Vrije Universiteit Brussel

Hopf algebras

S. Caenepeel and J. Vercruysse

Syllabus 106 bij WE-DWIS-12762 “Hopf algebras en quantum groepen - Hopf algebras and quantum groups”
Master Wiskunde Vrije Universiteit Brussel en Universiteit Antwerpen. 2013

Contents

Chapter 1

Basic notions from category theory

1.1 Categories and functors

1.1.1 Categories

A *category* $\mathcal{C}$ consists of the following data:

- a class $|\mathcal{C}| = \mathcal{C}_0 = \mathcal{C}$ of *objects*, denoted by $X, Y, Z, \ldots$;
- for any two objects X, Y, a set $\mathrm{Hom}_{\mathcal{C}}(X,Y) = \mathrm{Hom}(X,Y) = \mathcal{C}(X,Y)$ of morphisms;
- for any three objects X, Y, Z a composition law for the morphisms:
$$\circ : \mathrm{Hom}(X,Y) \times \mathrm{Hom}(Y,Z) \to \mathrm{Hom}(X,Z),\ (f,g) \mapsto g \circ f;$$
- for any object X a unit morphism on X, denoted by 1_X or X for short.

These data are subjected to the following compatibility conditions:

- for all objects X, Y, Z, U, and all morphisms $f \in \mathrm{Hom}(X,Y)$, $g \in \mathrm{Hom}(Y,Z)$ and $h \in \mathrm{Hom}(Z,U)$, we have
$$h \circ (g \circ f) = (h \circ g) \circ f;$$
- for all objects X, Y, Z, and all morphisms $f \in \mathrm{Hom}(X,Y)$ and $g \in \mathrm{Hom}(Y,Z)$, we have
$$Y \circ f = f \qquad g \circ Y = g.$$

Remark 1.1.1 In general, the objects of a category constitute a class, not a set. The reason behind this is the well-known set-theoretical problem that there exists no "set of all sets". Without going into detail, let us remind that a class is a set if and only if it belongs to some (other) class. For similar reasons, there does not exist a "category of all categories", unless this new category is "of a larger type". (A bit more precise: the categories defined above are Hom-Set categories, i.e. for any two objects X, Y, we have that $\mathrm{Hom}(X,Y)$ is a set. It is possible to build a category out of this type of categories that will no longer be a Hom-Set category, but a Hom-Class category: in a Hom-Class category $\mathrm{Hom}(X,Y)$ is a class for any two objects X and Y. On the other hand, if we restrict to so called *small* categories, i.e. categories with only a set of objects, then these form a Hom-Set category.)

Examples 1.1.2 1. The category $\underline{\underline{\mathsf{Set}}}$ whose objects are sets, and where the set of morphisms between two sets is given by all mappings between those sets.

2. Let k be a commutative ring, then $\mathcal{M}_k$ denotes the category with as objects all (right) k-modules, and with as morphisms between two k-modules all k-linear mappings.

3. If A is a non-commutative ring, we can consider also the category of right A-modules $\mathcal{M}_A$, the category of left A-modules ${}_A\mathcal{M}$, and the category of A-bimodules ${}_A\mathcal{M}_A$. If B is another ring, we can also consider the category of A-B bimodules ${}_A\mathcal{M}_B$. Remark that if A is commutative, then $\mathcal{M}_A$ and ${}_A\mathcal{M}$ coincide, but they are different from ${}_A\mathcal{M}_A$!

4. Top is the category of topological spaces with continuous mappings between them. Top_0 is the category of pointed topological spaces, i.e. topological spaces with a fixed base point, and continuous mappings between them that preserve the base point.

5. Grp is the category of groups with group homomorphisms between them.

6. $\underline{\underline{\mathrm{Ab}}}$ is the category of Abelian groups with group homomorphisms between them. Remark that $\underline{\underline{\mathrm{Ab}}} = \mathcal{M}_{\mathbb{Z}}$.

7. Rng is the category of rings with ring homomorphisms between them.

8. Alg_k is the category of k-algebras with k-algebra homomorphisms between them. We have $\mathsf{Alg}_{\mathbb{Z}} = \mathsf{Rng}$.

9. All previous examples are *concrete* categories: their objects are sets (with additional structure), i.e. they allow for a faithful forgetful functor to $\underline{\underline{\mathsf{Set}}}$ (see below). An example of a non-concrete category is as follows. Let M be a monoid, then we can consider this as a category with one object $*$, where $\mathrm{Hom}(*, *) = M$.

10. The trivial category $*$ has only one object $*$, and one morphism, the identity morphism of $*$ (this is the previous example with M the trivial monoid).

11. Another example of a non-concrete category can be obtained by taking a category whose class of objects is $\mathbb{N}_0$, and where $\mathrm{Hom}(n, m) = M_{n,m}(k)$: all $n \times m$ matrices with entries in k (where k is e.g. a commutative ring).

12. If $\mathcal{C}$ is a category, then $\mathcal{C}^{op}$ is the category obtained by taking the same class of objects as in $\mathcal{C}$, but by reversing the arrows, i.e. $\mathrm{Hom}_{\mathcal{C}^{op}}(X, Y) = \mathrm{Hom}_{\mathcal{C}}(Y, X)$. We call this the *opposite category* of $\mathcal{C}$.

13. If $\mathcal{C}$ and $\mathcal{D}$ are categories, then we can construct the product category $\mathcal{C} \times \mathcal{D}$, whose objects are pairs (C, D), with $C \in \mathcal{C}$ and $D \in \mathcal{D}$, and morphisms $(f, g) : (C, D) \to (C', D')$ are pairs of morphisms $f : C \to C'$ in $\mathcal{C}$ and $g : D \to D'$ in $\mathcal{D}$.

1.1.2 Functors

Let $\mathcal{C}$ and $\mathcal{D}$ be two categories. A (covariant) *functor* $F : \mathcal{C} \to \mathcal{D}$ consists of the following data:

- for any object $X \in \mathcal{C}$, we have an object $FX = F(X) \in \mathcal{D}$;
- for any morphism $f : X \to Y$ in $\mathcal{C}$, there is a morphism $Ff = F(f) : FX \to FY$ in $\mathcal{D}$;

satisfying the following conditions,

- for all $f \in \mathrm{Hom}(X, Y)$ and $g \in \mathrm{Hom}(Y, Z)$, we have $F(g \circ f) = F(g) \circ F(f)$;
- for all objects X, we have $F(1_X) = 1_{FX}$.

A *contravariant* functor $F : \mathcal{C} \to \mathcal{D}$ is a covariant functor $F : \mathcal{C}^{op} \to \mathcal{D}$. Most or all functors that we will encounter will be covariant, therefore if we say functor we will mean covariant functor, unless we say differently. For any functor $F : \mathcal{C} \to \mathcal{D}$, one can consider two functors $F^{op} : \mathcal{C}^{op} \to \mathcal{D}$ and $F^{cop} : \mathcal{C} \to \mathcal{D}^{op}$. Then F is contravariant if and only if F^{op} and F^{cop} are covariant (and visa versa). The functor $F^{op,cop} : \mathcal{C}^{op} \to \mathcal{D}^{op}$ is again contravariant.

Examples 1.1.3

1. The identity functor $1_\mathcal{C} : \mathcal{C} \to \mathcal{C}$, where $1_\mathcal{C}(C) = C$ for all objects $C \in \mathcal{C}$ and $1_\mathcal{C}(f) = f$ for all morphisms $f : C \to C'$ in $\mathcal{C}$.
2. The constant functor $\mathcal{C} \to \mathcal{D}$ at X, assigns to every object $C \in \mathcal{C}$ the same fixed object $X \in \mathcal{D}$, and assigns to every morphism f in $\mathcal{C}$ the identity morphism on X. Remark that defining the constant functor, is equivalent to choosing an object $D \in \mathcal{D}$.
3. The tensor functor $- \otimes - : \mathcal{M}_k \times \mathcal{M}_k \to \mathcal{M}_k$, associates two k-modules X and Y to their tensor product $X \otimes Y$ (see Section 1.3).
4. All "concrete" categories from Example 1.1.2 (1)–(8) allow for a forgetful functor to $\underline{\underline{\mathsf{Set}}}$, that sends the objects of the concrete category to the underlying set, and the homomorphisms to the underlying mapping between the underlying sets.
5. $\pi_1 : \mathsf{Top}_0 \to \mathsf{Grp}$ is the functor that sends a pointed topological space (X, x_0) to its fundamental group $\pi_1(X, x_0)$.
6. An example of a contravariant functor is the following $(-)^* : \mathcal{M}_k \to \mathcal{M}_k$, which assigns to every k-module X the dual module $X^* = \mathrm{Hom}(X, k)$.

All functors between two categories $\mathcal{C}$ and $\mathcal{D}$ are gathered in $\mathsf{Fun}(\mathcal{C}, \mathcal{D})$. In general, $\mathsf{Fun}(\mathcal{C}, \mathcal{D})$ is a class, but not necessarily a set. Hence, if one wants to define 'a category of all categories' where the morphisms are functors, some care is needed (see above).

1.1.3 Natural transformations

Let $F, G : \mathcal{C} \to \mathcal{D}$ be two functors. A *natural transformation* $\alpha : F \to G$ (sometimes denoted by $\alpha : F \Rightarrow G$), assigns to every object $C \in \mathcal{C}$ a morphism $\alpha_C : FC \to GC$ in $\mathcal{D}$ rendering for every $f : C \to C'$ in $\mathcal{C}$ the following diagram in $\mathcal{D}$ commutative,

$$\begin{tikzcd} FC \arrow[r, "Ff"] \arrow[d, "\alpha_C"'] & FC' \arrow[d, "\alpha_{C'}"] \\ GC \arrow[r, "Gf"'] & GC' \end{tikzcd}$$

Remark 1.1.4 If $\alpha : F \to G$ is a natural transformation, we also say that $\alpha_C : FC \to GC$ is a morphism that is *natural in* C. In such an expression, the functors F and G are often not explicitly predescribed. E.g. the morphism $X \otimes Y^* \to \mathrm{Hom}(Y, X),\ x \otimes f \mapsto (y \mapsto xf(y))$, is natural both in X and Y. Here X and Y are k-modules, $x \in X$, $y \in Y$, $f \in Y^* = \mathrm{Hom}(Y, k)$, the dual k-module of Y.

If α_C is an isomorphism in $\mathcal{D}$ for all $C \in \mathcal{C}$, we say that $\alpha : F \to G$ is a *natural isomorphism*.

Examples 1.1.5

1. If $F : \mathcal{C} \to \mathcal{D}$ is a functor, then $1_F : F \to F$, defined by $(1_F)_X = 1_{F(X)} : F(X) \to F(X)$ is the identity natural transformation on F.
2. The canonical injection $\iota_X : X \to X^{**}$, $\iota_X(x)(f) = f(x)$, for all $x \in X$ and $f \in X^*$, from a k-module X to the dual of its dual, defines a natural transformation $\iota : 1_{\mathcal{M}_k} \to (-)^{**}$. If we restrict to the category of finitely generated and projective k-modules, then ι is a natural isomorphism.

1.1.4 Adjoint functors

Let $\mathcal{C}$ and $\mathcal{D}$ be two categories, and $L : \mathcal{C} \to \mathcal{D}$, $R : \mathcal{D} \to \mathcal{C}$ be two functors. We say that (equivalently)

- L is a left adjoint for R;
- R is a right adjoint for L;
- (L, R) is an adjoint pair;
- the pair (L, R) is an adjunction,

if and only if any of following equivalent conditions hold:

(i) there is a natural isomorphism

$$\theta_{C,D} : \mathrm{Hom}_{\mathcal{D}}(LC, D) \to \mathrm{Hom}_{\mathcal{C}}(C, RD), \tag{1.1}$$

with $C \in \mathcal{C}$ and $D \in \mathcal{D}$;

(ii) there are natural transformations $\eta : 1_{\mathcal{C}} \to RL$, called the *unit*, and $\varepsilon : LR \to 1_{\mathcal{D}}$, called the *counit*, which render the following diagrams commutative for all $C \in \mathcal{C}$ and $D \in \mathcal{D}$,

$$
\begin{tikzcd}
LC \arrow[r, "L\eta_C"] \arrow[dr, equal] & LRLC \arrow[d, "\varepsilon_{LC}"] \\
& LC
\end{tikzcd}
\qquad
\begin{tikzcd}
RD \arrow[r, "\eta_{RD}"] \arrow[dr, equal] & RLRD \arrow[d, "R\varepsilon_D"] \\
& RD
\end{tikzcd}
$$

This means that we have the following identities between natural transformations: $1_L = \varepsilon L \circ L\eta$ and $1_R = R\varepsilon \circ \eta R$.

A proof of the equivalence between condition (i) and (ii) can be found in any standard book on category theory. We also give the following list of examples as illustration, without proof. Some of the examples will be used or proved later in the course.

Examples 1.1.6 1. Let $U : \mathsf{Grp} \to \underline{\underline{\mathsf{Set}}}$ be the forgetful functor that sends every group to the underlying set. Then U has a left adjoint given by the functor $F : \underline{\underline{\mathsf{Set}}} \to \mathsf{Grp}$ that associates to every set the free group generated by the elements of this set. Remark that equation (1.1) expresses that a group homomorphism (from a free group) is determined completely by its action on generators.

2. Let X be a k-module. The functor $- \otimes X : \mathcal{M}_k \to \mathcal{M}_k$ is a left adjoint for the functor $\mathrm{Hom}(X, -) : \mathcal{M}_k \to \mathcal{M}_k$.

3. Let X be an A-B bimodule. The functor $- \otimes_A X : \mathcal{M}_A \to \mathcal{M}_B$ is a left adjoint for the functor $\mathrm{Hom}_B(X, -) : \mathcal{M}_B \to \mathcal{M}_A$.

4. Let $\iota : B \to A$ be a morphism of k-algebras. Then the restriction of scalars functor $R : \mathcal{M}_A \to \mathcal{M}_B$ is a right adjoint to the induction functor $- \otimes_B A : \mathcal{M}_B \to \mathcal{M}_A$. Recall that for a right A-module X, $R(X) = X$ as k-module, and the B-action on $R(X)$ is given by the formula
$$x \cdot b = x\iota(b),$$
for all $x \in X$ and $b \in B$.

5. Let $k- : \mathsf{Grp} \to \mathsf{Alg}_k$ be the functor that associates to any group G the group algebra kG over k. Let $U : \mathsf{Alg}_k \to \mathsf{Grp}$ be the functor that associates to any k-algebra A its unit group $U(A)$. Then $k-$ is a left adjoint for U.

1.1.5 Equivalences and isomorphisms of categories

Let $F : \mathcal{C} \to \mathcal{D}$ be a functor. Then F induces the following morphism that is natural in $C, C' \in \mathcal{C}$,

$$F_{C,C'} : \mathrm{Hom}_{\mathcal{C}}(C, C') \to \mathrm{Hom}_{\mathcal{D}}(FC, FC').$$

The functor is said to be

- *faithful* if $F_{C,C'}$ is injective,

- *full* if $F_{C,C'}$ is surjective,
- *fully faithful* if $F_{C,C'}$ is bijective

for all $C, C' \in \mathcal{C}$.
If (L, R) is an adjoint pair of functors with unit η and counit ε, then L is fully faithful if and only if η is a natural isomorphism and R is fully faithful if and only if ε is an isomorphism.

Examples 1.1.7

1. All forgetful functors from a concrete category (as in Example 1.1.2 (1)–(8)) to $\underline{\underline{\mathsf{Set}}}$ are faithful (in fact, admitting a faithful functor to $\underline{\underline{\mathsf{Set}}}$, is the definition of being a concrete category, and this faithful functor to $\underline{\underline{\mathsf{Set}}}$ is then called the forgetful functor).
2. Let $\iota : B \to A$ be a surjective ring homomorphism, then the restriction of scalars functor $R : \mathcal{M}_A \to \mathcal{M}_B$ is full.
3. The forgetful functor $\underline{\underline{\mathrm{Ab}}} \to \mathsf{Grp}$ is fully faithful.

A functor $F : \mathcal{C} \to \mathcal{D}$ is called an *equivalence of categories* if and only if one of the following equivalent conditions holds:

1. F is fully faithful and has a fully faithful right adjoint;
2. F is fully faithful and has a fully faithful left adjoint;
3. F is fully faithful and essentially surjective, i.e. each object $D \in \mathcal{D}$ is isomorphic to an object of the form FC, for $C \in \mathcal{C}$;
4. F has a left adjoint and the unit and counit of the adjunction are natural isomorphisms;
5. F has a right adjoint and the unit and counit of the adjunction are natural isomorphisms;
6. there is a functor $G : \mathcal{D} \to \mathcal{C}$ and natural isomorphisms $GF \to 1_{\mathcal{C}}$ and $FG \to 1_{\mathcal{D}}$.

There is a subtle difference between an equivalence of categories and the following stronger notion: A functor $F : \mathcal{C} \to \mathcal{D}$ is called an isomorphism of categories if and only if there is a functor $G : \mathcal{D} \to \mathcal{C}$ such that $GF = 1_{\mathcal{C}}$ and $FG = 1_{\mathcal{D}}$.

Examples 1.1.8

1. Let k be a commutative ring and $R = M_n(k)$ the $n \times n$ matrix ring over k. Then the categories $\mathcal{M}_k$ and $\mathcal{M}_R$ are equivalent, (but not necessarily isomorphic if $n \neq 1$).
2. The categories $\underline{\underline{\mathrm{Ab}}}$ and $\mathcal{M}_{\mathbb{Z}}$ are isomorphic.
3. For any category $\mathcal{C}$, we have an isomorphism $\mathcal{C} \times * \cong \mathcal{C}$.

1.2 Abelian categories

1.2.1 Equalizers and coequalizers

Let $\mathcal{A}$ be any category and consider two (parallel) morphisms $f, g : X \to Y$ in $\mathcal{A}$. The *equalizer* of the pair (f, g), is a couple (E, e) consisting of an object E and a morphism $e : E \to X$, such that $f \circ e = g \circ e$, and that satisfies the following universal property. For all pairs $(T, t : T \to X)$, such that $f \circ t = g \circ t$, there must exist a unique morphism $u : T \to E$ such that $t = e \circ u$.

$$\begin{tikzcd} E \arrow[r, "e"] & X \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] & Y \\ T \arrow[u, dotted, "\exists! u"] \arrow[ur, "t"'] & & \end{tikzcd}$$

The dual notion of an equalizer is that of a *coequalizer*. Explicitly: the coequalizer of a pair (f, g) is a couple (C, c), consisting of an object C and a morphism $c : Y \to C$, such that $c \circ f = c \circ g$. Moreover, (C, c) is required to satisfy the following universal property. For all pairs $(T, t : Y \to C)$, such that $t \circ f = t \circ g$, there must exist a unique morphism $u : C \to T$ such that $t = u \circ c$.

$$\begin{tikzcd} X \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] & Y \arrow[r, "c"] \arrow[dr, "t"'] & C \arrow[d, dotted, "\exists! u"] \\ & & T \end{tikzcd}$$

By the universal property, it can be proved that equalizers and coequalizers, if they exist, are unique up to isomorphism. Explicitly, this property tells that if for a given pair (f, g), one finds to couples (E, e) and (E', e') such that $f \circ e = g \circ e$ and $f \circ e' = g \circ e'$ and both couples satisfy the universal property, then there exists an isomorphism $\phi : E \to E'$ in $\mathcal{A}$, such that $e = e' \circ \phi$.
Let (E, e) be the equalizer of a pair (f, g). An elementary but useful property of equalizers tells that e is always a monomorphism. Similarly, for a coequalizer (C, c), c is an epimorphism.

1.2.2 Kernels and cokernels

A *zero object* for a category $\mathcal{A}$, is an object 0 in $\mathcal{A}$, such that for any other object A in $\mathcal{A}$, $\mathrm{Hom}(A, 0)$ and $\mathrm{Hom}(0, A)$ consists of exactly one element. If it exits, the zero object of $\mathcal{A}$ is unique. Suppose that $\mathcal{A}$ has a zero object and let A and B be two objects of $\mathcal{A}$. A morphism $f : B \to A$ is called the zero morphism, if f factors trough 0, i.e. $f = f_1 \circ f_2$ where f_1 and f_2 are the unique elements in $\mathrm{Hom}(0, A)$ and $\mathrm{Hom}(B, 0)$, respectively. From now on, we denote any morphism from, to, or factorizing trough 0 also by 0.
The *kernel* of a morphism $f : B \to A$, is the equalizer of the pair $(f, 0)$. The *cokernel* of f is the coequalizer of the pair $(f, 0)$. Remark that in contrast with the classical definition, in the categorical definition of a kernel, a kernel consists of a pair (K, κ), where K is an object of $\mathcal{A}$, and $\kappa : K \to B$ is a morphism in $\mathcal{A}$. The monomorphism κ corresponds in the classical examples to the canonical embedding of the kernel.
The *image* of a morphism $f : B \to A$, is the cokernel of the kernel $\kappa : K \to B$ of f. The *coimage* is the kernel of the cokernel.

1.2.3 Limits and colimits

Limits unify the notions of kernel, product and several other useful (algebraic) constructions, such as pullbacks. Let $\mathcal{Z}$ be a small category (i.e. with only a set of objects), and consider a functor $F : \mathcal{Z} \to \mathcal{A}$. A cone on F is a couple (C, c_Z), consisting of an object $C \in \mathcal{A}$, and for each element $Z \in \mathcal{Z}$ a morphism $c_Z : C \to FZ$, such that for any morphism $f : Z \to Z'$, the following diagram commutes

$$\begin{tikzcd} C \arrow[r, "c_{Z'}"] \arrow[dr, "c_Z"'] & FZ' \\ & FZ \arrow[u, "Ff"'] \end{tikzcd}$$

The *limit* of F is a cone (L, l_Z), such that for any other cone (C, c_Z), there exists a unique morphism $u : C \to L$, such that for all $Z \in \mathcal{Z}$, $c_Z = l_Z \circ u$. If it exists, the limit of F is unique up to isomorphism in $\mathcal{A}$. We write $\lim F = \lim F(Z) = (L, l)$

Dually, a cocone on F, is a couple (M, m_Z), where $M \in \mathcal{A}$ and $m_Z : F(Z) \to M$ is a morphism in $\mathcal{A}$, for all $Z \in \mathcal{Z}$, such that

$$m_Z = m_{Z'} \circ F(f),$$

for all $f : Z \to Z'$ in $\mathcal{Z}$. The *colimit* of F is a cocone (C, c) on F satisfying the following universal property: if (M, m) is a cocone on F, then there exists a unique morhism such that

$$f \circ c_Z = m_Z,$$

for all $Z \in \mathcal{Z}$. If it exists, the colimit is unique up to isomorphism. We write $\mathrm{colim}\, F = \mathrm{colim}\, F(Z) = (C, c)$.

Different types of categories $\mathcal{Z}$ give rise to different types of (co)limits.

1. Let $\mathcal{Z}$ be a discrete category (i.e. $\mathrm{Hom}(Z, Z')$ is empty if $Z \neq Z'$ and exists of nothing but the identity morphism otherwise), then for any functor $F : \mathcal{Z} \to \mathcal{A}$, $\lim F = \prod_{Z \in \mathcal{Z}} F(Z)$, the product in $\mathcal{A}$ of all $F(Z) \in \mathcal{A}$ for all $Z \in \mathcal{Z}$ and $\mathrm{colim}\, F = \coprod_{Z \in \mathcal{Z}} F(Z)$, the coproduct in $\mathcal{A}$ of all $F(Z) \in \mathcal{A}$ for all $Z \in \mathcal{Z}$.

2. Let $\mathcal{Z}$ be a category consisting of two objects X and Y, such that $\mathrm{Hom}(X, X) = \{X\}$, $\mathrm{Hom}(Y, Y) = \{Y\}$, $\mathrm{Hom}(Y, X) = \emptyset$ and $\mathrm{Hom}(X, Y) = \{f, g\}$. Then for any functor $F : \mathcal{Z} \to \mathcal{A}$, $\lim F$ is the equalizer in $\mathcal{A}$ of the pair $(F(f), F(g))$ and $\mathrm{colim}\, F$ is the coequalizer in $\mathcal{A}$ of the pair $(F(f), F(g))$.

3. A category J is called *filtered* when

   - it is not empty,
   - for every two objects j and j' in J there exists an object k and two arrows $f : j \to k$ and $f' : j' \to k$ in J,
   - for every two parallel arrows $u, v : i \to j$ in J, there exists an object k and an arrow $w : j \to k$ such that $wu = wv$.

   Let I be a directed poset, the category associated to I, whose objects are the elements of I, and where $\mathrm{Hom}(i, j)$ is the singleton if $i \leq j$ and the singleton otherwise, is a filtered category. The (co)limit of a functor $F : J \to \mathcal{A}$, where J is a filtered category is called a filtered (co)limit.

1.2.4 Abelian categories and Grothendieck categories

A category is *preadditive* if it is enriched over the monoidal category $\underline{\underline{\mathrm{Ab}}}$ of abelian groups. This means that all Hom-sets are abelian groups and the composition of morphisms is bilinear.
A preadditive category$\mathcal{A}$ is called *additive* if every finite set of objects has a biproduct. This means that we can form finite direct sums and direct products (which are isomorphic as objects in $\mathcal{A}$).
An additive category is *preabelian* if every morphism has both a kernel and a cokernel.
Finally, a preabelian category is *abelian* if every monomorphism is a kernel of some morphism and every epimorphism is a cokernel of some morphism. In any preabelian category $\mathcal{A}$, one can construct for any morphism $f : A \to B$, the following diagram

$$\begin{tikzcd}
\mathsf{ker}(f) \arrow[r, "\kappa"] & A \arrow[r, "f"] \arrow[d, "\lambda"'] & B \arrow[r, "\pi"] & \mathsf{coker}(f) \\
& \mathsf{coim}(f) \arrow[r, "\bar{f}"] & \mathsf{im}(f) \arrow[u, "\mu"'] &
\end{tikzcd}$$

One can prove that $\mathcal{A}$ is abelian if and only if $\bar{f}$ is an isomorphism for all f.
The category $\underline{\underline{\mathrm{Ab}}}$ of abelian groups is the standard example of an abelian category. Other examples are $\mathcal{M}_k$, where k is a commutative ring, or more general, $\mathcal{M}_A$ and ${}_B\mathcal{M}_A$, where A and B are not necessarily commutative rings.
In any abelian category (in particular in $\mathcal{M}_k$), the equalizers of a pair (f, g) always exists and can be computed as the kernel of $f - g$. Dually, the coequalizer also exists for every pair (f, g) and can be computed as the cokernel of $f - g$, which is isomorphic to $Y/\mathrm{Im}\,(f - g)$.

1.2.5 Exact functors

Abelian categories provide a natural framework to study exact sequences and homology. In fact it is possible to study homology already in the more general setting of semi-abelian categories, of which the category of Groups form a natural example. For more details we refer to the course "semi-abelse categorieën" on this subject.
A sequence of morphisms

$$A \xrightarrow{f} B \xrightarrow{g} C$$

is called exact if $\mathsf{im}(f) = \mathsf{ker}(g)$. An arbitrary sequence of morphisms is called exact if every subsequence of two consecutive morphisms is exact.
Let $\mathcal{C}$ and $\mathcal{D}$ be two preadditive categories. Then a functor $F : \mathcal{C} \to \mathcal{D}$ is called additive if $F(f+g) = F(f)+F(g)$, for any two objects $A, B \in \mathcal{C}$ and any two morphisms $f, g \in \mathrm{Hom}(A, B)$.
Let $\mathcal{C}$ and $\mathcal{D}$ be two preabelian categories. A functor $F : \mathcal{C} \to \mathcal{D}$ is called right (resp. left) exact if for any sequence of the form

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0 \tag{1.2}$$

in $\mathcal{C}$, there is an exact sequence

$$F(A) \xrightarrow{F(f)} F(B) \xrightarrow{F(g)} F(C) \longrightarrow 0$$

in $\mathcal{D}$ (respectively, there is an exact sequence

$$0 \longrightarrow F(A) \xrightarrow{F(f)} F(B) \xrightarrow{F(g)} F(C)$$

in $\mathcal{D}$). A functor is exact if it is at the same time left and right exact, i.e. when the sequence

$$0 \longrightarrow F(A) \xrightarrow{F(f)} F(B) \xrightarrow{F(g)} F(C) \longrightarrow 0 \qquad (1.3)$$

is exact in $\mathcal{D}$.
If the functor F is such that for any sequence of the form (1.2) in $\mathcal{C}$, this sequence is exact in $\mathcal{C}$ if the sequence (1.3) is exact in $\mathcal{D}$, then we say that F *reflects* exact sequences.
Let A and B rings, and M an A-B-bimodule. Then the functor $- \otimes_A M : \mathcal{M}_A \to \mathcal{M}_B$ is right exact and the functor $\mathrm{Hom}_B(M, -) : \mathcal{M}_B \to \mathcal{M}_A$ is left exact. By definition, the functor $- \otimes_A M : \mathcal{M}_A \to \underline{\underline{\mathrm{Ab}}}$ is exact if and only if the left A-module M is *flat*. A module is called *faithfully flat*, if it is flat and the functor $- \otimes_A M : \mathcal{M}_A \to \underline{\underline{\mathrm{Ab}}}$ moreover reflects exact sequences. If A is a field, then any A-module is faithfully flat.
Let $\mathcal{A}$ be an abelian category, and consider a pair of parallel morphisms $f, g : X \to Y$. Then (E, e) is the equalizer of the pair (f, g) in $\mathcal{A}$ if and only if the row $0 \longrightarrow E \xrightarrow{e} X \xrightarrow{f-g} Y$ is exact (if and only if (E, e) is the kernel of the morphism $f - g$, see above). A dual statement relates coequalizers, right short exact sequences and cokernels in abelian categories. Hence an exact functor (resp. a functor that reflects exact sequences) between abelian categories preserves (resp. reflects) also equalizers and coequalizers. A left exact functor only preserves equalizers (in particular kernels), a right exact functor only preserves coequalizers (in particular cokernels).

1.2.6 Grothendieck categories

A *Grothendieck category* is an abelian category $\mathcal{A}$ such that

- $\mathcal{A}$ has a generator,
- $\mathcal{A}$ has colimits;
- filtered colimits are exact in the following sense: Let I be a directed set and

  $$0 \to A_i \to B_i \to C_i \to 0$$

  an exact sequence for each $i \in I$, then

  $$0 \to \mathsf{colim}\,(A_i) \to \mathsf{colim}\,(B_i) \to \mathsf{colim}\,(C_i) \to 0$$

  is also an exact sequence.

One of the basic properties of Grothendieck categories is that they also have limits.

Examples 1.2.1 • For any ring A, the category $\mathcal{M}_A$ of (right) modules over A is the standard example of a Grothendieck category. The forgetful functor $\mathcal{M}_A \to \underline{\underline{\mathrm{Ab}}}$ preserves and reflects exact sequences.

- If a coring $\mathfrak{C}$ is flat as a left A-module, then the category $\mathcal{M}^{\mathfrak{C}}$ of right $\mathfrak{C}$-comodules is a Grothendieck category. Moreover, in this case, the forgetful functor $\mathcal{M}^{\mathcal{C}} \to \mathcal{M}_A$ preserves and reflects exact sequences (hence (co)equalizers and (co)kernels), therefore, exactness, (co)equalizers and (co)kernels can be computed already in $\mathcal{M}_A$ (and even in $\underline{\underline{\mathrm{Ab}}}$).

1.3 Tensor products of modules

1.3.1 Universal property

Let k be a commutative ring, and let $\mathcal{M}_k$ be the category with objects (right) k-modules and morphisms k-linear maps. We denote the set of all k-linear maps between two k-modules X and Y by $\mathrm{Hom}(X, Y)$.
For any two k-modules X and Y, we know that the cartesian product $X \times Y$ is again a k-module where

$$(x, y) + (x', y') = (x + x', y + y') \quad \text{and} \quad (x, y) \cdot a = (xa, ya)$$

for all $x, x' \in X$, $y, y' \in Y$ and $a \in k$. For any third k-module Z, we can now consider the set $\mathsf{Bil}_k(X \times Y, Z)$ of k-bilinear maps from $X \times Y$ to Z. The *tensor product* of X and Y is defined as the unique k-module, denoted by $X \otimes Y$, for which there exists a bilinear map $\phi : X \times Y \to X \otimes Y$, such that the map

$$\Phi_Z : \mathrm{Hom}(X \otimes Y, Z) \to \mathsf{Bil}(X \times Y, Z),\ \Phi_Z(f) = f \circ \phi$$

is bijective for all k-modules Z. The uniqueness of the tensor product is reflected in the fact that it satisfies moreover the following universal property: if T is another k-module together with a k-bilinear map $\psi : X \times Y \to T$ such that the corresponding map $\Psi_Z : \mathrm{Hom}(T, Z) \to \mathsf{Bil}(X \times Y, Z)$ is bijective for all Z, then there must exist a unique k-linear map $\tau : X \otimes Y \to T$ such that $\psi = \tau \circ \phi$. Indeed, just take $\tau = \Phi_T^{-1}(\psi)$.
Remark that this universal property indeed implies that the tensor product is unique. (Prove this as exercise. In fact, many objects in category theory such as (co)equalisers, (co)products, (co)limits, are unique because they satisfy a similar *universal property*.)

1.3.2 Existence of tensor product

We will now provide an explicit construction for the tensor product, which explicitly implies the existence of (arbitrary) tensor products. Consider again k-modules X and Y. Let $(X \times Y)k$ be the free k-module generated by a basis indexed by all elements of $X \times Y$. I.e. elements of $(X \times Y)k$ are (finite) linear combinations of vectors $e_{(x,y)}$, where $x \in X$ and $y \in Y$. Now consider the submodule I generated by the following elements:

$$\begin{gathered}
e_{(x+x',y)} - e_{(x,y)} - e_{(x',y)}, \\
e_{(x,y+y')} - e_{(x,y)} - e_{(x,y')}, \\
e_{(xa,y)} - e_{(x,y)}a, \\
e_{(x,ya)} - e_{(x,y)}a.
\end{gathered}$$

We claim that $X \otimes Y = (X \times Y)k/I$. Indeed, there is a map

$$\phi : X \times Y \to X \otimes Y,\ \phi(x,y) = e_{x,y},$$

which is k-bilinear exactly because of the definition of I. Furthermore, for any k-module Z we can define $\Phi_Z^{-1} : \mathsf{Bil}(X \times Y, Z) \to \mathrm{Hom}(X \otimes Y, Z)$ as follows. For $f \in \mathsf{Bil}(X \times Y, Z)$, we put

$$\Phi_Z^{-1}(f)(e_{x,y}) = f(x,y)$$

and extend this linearly. Then it is straightforward to check that this defines indeed a two-sided inverse for Φ_Z.
From now on, we will denote the element $e_{x,y} \in X \otimes Y$ just by $x \otimes y \in X \otimes Y$. A general element of $X \otimes Y$ is therefore a finite sum of the form $\sum_i x_i \otimes y_i$, where $x_i \in X$ and $y_i \in Y$. Moreover, these elements satisfy the following relations:

$$\begin{aligned}
(x + x') \otimes y &= x \otimes y + x' \otimes y \\
x \otimes (y + y') &= x \otimes y + x \otimes y' \\
(xa) \otimes y &= x \otimes (ya) = (x \otimes y)a.
\end{aligned}$$

1.3.3 Iterated tensor products

A special tensor product is the tensor product where $Y = k$ (or $X = k$). Let us compute this particular case. Since X is a (right) k-module, multiplication with k provides a k-bilinear map

$$m : X \times k \to X,\ m(x,a) = ma.$$

By the universal property of the tensor product, this map can be transformed into a linear map $m' : X \otimes k \to X,\ m'(\sum_i x_i \otimes a_i) = \sum_i x_i a_i$. Now observe that the following map is k-linear:

$$r : X \to X \otimes k,\ r(x) = x \otimes 1.$$

Indeed, by the equivalence properties in the construction of the tensor product, we find that

$$r(xa) = xa \otimes 1 = (x \otimes 1)a = r(x)a.$$

Finally, we have that r and m are each others inverse:

$$\begin{aligned}
r \circ m(\sum_i x_i \otimes a_i) &= (\sum_i x_i a_i) \otimes 1 = \sum_i ((x_i a_i) \otimes 1) = \sum_i x_i \otimes a_i \\
m \circ r(x) &= m(x \otimes 1) = x1 = x
\end{aligned}$$

So we conclude that $X \otimes k \cong X$. Similarly, one shows that $k \otimes Y \cong Y$.
Consider now three k-modules X, Y and Z. Then we can construct the tensor products $X \otimes Y$ and $Y \otimes Z$. Now we can take the tensor product of these modules respectively with Z on the right and with X on the left. So we obtain $(X \otimes Y) \otimes Z$ and $X \otimes (Y \otimes Z)$. We claim that these modules are isomorphic. To prove this explicitly, we introduce the triple tensor product space with a similar universal property as for the usual tensor product. Let $\mathsf{Tri}(X \times Y \times Z, U)$

be the set of all tri-linear maps $f : X \times Y \times Z \to U$, where U is any fixed k-module. Then the k-module $\otimes(X, Y, Z)$ is defined to be the unique k-module for which there exists a trilinear map $\phi : X \times Y \times Z \to \otimes(X, Y, Z)$, such that for all k-modules U, the following map is bijective

$$\Phi_U : \mathrm{Hom}(\otimes(X, Y, Z), U) \to \mathsf{Tri}(X \times Y \times Z, U), \Phi_U(f) = f \circ \phi.$$

As for the usual tensor product, one can construct $\otimes(X, Y, Z)$ by dividing out the free module $k(X \times Y \times Z)$ by an appropriate submodule. It is an easy exercise to check that both $(X \otimes Y) \otimes Z$ and $X \otimes (Y \otimes Z)$ satisfy this universal property and therefore are isomorphic.
Of course, this procedure can be repeated to obtain iterated tensor products of any (finite) number of k-modules. Up to isomorphism, the order of constructing the iterated tensor product out of usual tensor products, is irrelevant.

1.3.4 Tensor products over fields

If k is a field, X and Y are vector spaces, then there is an easy expression for the basis of $X \otimes Y$. Let $\{e_\alpha\}_{\alpha \in A}$ be a basis for X and $\{b_\beta\}_{\beta \in B}$ be a basis for Y. Then $X \otimes Y$ has a basis $\{e_\alpha \otimes b_\beta \mid \alpha \in A, \beta \in B\}$. The universal property in this case can also easily be obtained assuming that $X \otimes Y$ has this basis. In particular, if X an Y are finite dimensional, then it follows that $\dim(X \otimes Y) = \dim X \cdot \dim Y$.

1.3.5 Tensor products over arbitrary algebras

Tensor products as a coequalizer

Let A be any (unital, associative) k-algebra. Consider a right A-module (M, μ_M) and a left A-module (N, μ_N). The tensor product of M and N over A is the k-module defined by the following coequalizer in $\mathcal{M}_k$,

$$\begin{tikzcd} M \otimes A \otimes N \arrow[r, shift left, "\mu_M \otimes N"] \arrow[r, shift right, "M \otimes \mu_N"'] & M \otimes N \arrow[r] & M \otimes_A N. \end{tikzcd}$$

(here the unadorned tensor product denotes the k-tensor product.)

Some basic properties

Consider three k-algebras A, B, C. One can check that the tensorproduct over B defines a functor

$$- \otimes_B - : {}_A\mathcal{M}_B \times {}_B\mathcal{M}_C \to {}_A\mathcal{M}_C,$$

where for all $M \in {}_A\mathcal{M}_B$ and $N \in {}_B\mathcal{M}_C$, the left A-action (resp. right C-action) on $M \otimes_B N$ are given by $\mu_{A,M} \otimes_B N$ (resp. $M \otimes_B \mu_{N,C}$).
For any k-algebra A and any left A-module (M, μ_M), we have $A \otimes_A M \cong M$. To prove this, it suffices to verify that (M, μ_M) is the coequalizer of the pair $(\mu_A \otimes M, A \otimes \mu_M)$. The statement follows by the uniqueness of the coequalizer.

1.4 Monoidal categories and algebras

1.4.1 Monoidal categories and coherence

Definition 1.4.1 *A monoidal category (sometimes also termed tensor category) is a sixtuple* $\mathcal{C} = (\mathcal{C}, \otimes, k, a, l, r)$ *where*

- $\mathcal{C}$ *is a category;*
- k *is an object of* $\mathcal{C}$*, called the unit object of* $\mathcal{C}$*;*
- $-\otimes - : \ \mathcal{C}\times\mathcal{C}\to\mathcal{C}$ *is a functor, called the (tensor) product;*
- $a : \ \otimes\circ(\otimes\times\mathrm{id})\to\otimes\circ(\mathrm{id}\times\otimes)$ *is a natural isomorphism;*
- $l : \ \otimes\circ(k\times\mathrm{id})\to\mathrm{id}$ *and* $r : \ \otimes\circ(\mathrm{id}\times k)\to\mathrm{id}$ *are natural isomorphisms.*

This means that we have isomorphisms

$$a_{M,N,P} : \ (M\otimes N)\otimes P\to M\otimes(N\otimes P);$$

$$l_M : \ k\otimes M\to M \ \ ; \ \ r_M : \ M\otimes k\to M$$

for all $M,N,P,Q\in\mathcal{C}$*. We also require that the following diagrams commute, for all* $M,N,P,Q\in\mathcal{C}$*:*

$$\begin{tikzcd}
((M\otimes N)\otimes P)\otimes Q \arrow[r, "a_{M\otimes N,P,Q}"] \arrow[d, "a_{M,N,P}\otimes Q"'] & (M\otimes N)\otimes(P\otimes Q) \arrow[r, "a_{M,N,P\otimes Q}"] & M\otimes(N\otimes(P\otimes Q)) \\
(M\otimes(N\otimes P))\otimes Q \arrow[rr, "a_{M,N\otimes P,Q}"] & & M\otimes((N\otimes P)\otimes Q) \arrow[u, "M\otimes a_{N,P,Q}"']
\end{tikzcd} \tag{1.4}$$

$$\begin{tikzcd}
(M\otimes k)\otimes N \arrow[rr, "a_{M,k,N}"] \arrow[dr, "r_M\otimes N"'] & & M\otimes(k\otimes N) \arrow[dl, "M\otimes l_N"] \\
& M\otimes N &
\end{tikzcd} \tag{1.5}$$

a is called the associativity constraint, and l and r are called the left and right unit constraints of $\mathcal{C}$.

Examples 1.4.2 1) ($\underline{\text{Sets}}, \times, \{*\}$) is a monoidal category. Here $\{*\}$ is a fixed singleton.
2) For a commutative ring k, $({}_k\mathcal{M}, \otimes, k)$ is a monoidal category.
3) Let G be a monoid. Then $({}_{kG}\mathcal{M}, \otimes, k)$ is a monoidal category

In both examples, the associativity and unit constraints are the natural ones. For example, given 3 sets M, N and P, we have natural isomorphisms

$$a_{M,N,P} : \ (M\times N)\times P\to M\times(N\times P), \ \ a_{M,N,P}((m,n),p) = (m,(n,p)),$$

$$l_M : \ \{*\}\times M\to M, \ \ l_M(*,m) = m.$$

In many, but not all, important examples of monoidal categories, the associativity and unit constraints are trivial.
If the maps underlying the natural isomorphisms a, l and r are the identity maps, then we say that the monoidal category is strict. We mention (without proof) the Theorem, sometimes referred to as *Mac Lane's coherence Theorem* that every monoidal category is monoidally equivalent to a strict monoidal category. It states more precisely that for every monoidal category $(\mathcal{C}, \otimes, I, a, l, r)$, there exists a strict monoidal category $(\mathcal{C}', \otimes', I', a', l', r')$ together with an equivalence of categories $F : \mathcal{C} \to \mathcal{C}'$, where F is a strong monoidal functor. Since a', l' and r' are identities, there is no need to write them. Moreover, every diagram that is constructed out of these trivial morphisms will automatically commute (as it consists only of identities). By the (monoidal) equivalence of categories $\mathcal{C} \simeq \mathcal{C}'$, also every diagram in $\mathcal{C}$, constructed out of a, l and r will be commutative, this clarifies the name 'coherence'. As a consequence of this Theorem, we will omit to write the data a, l, r in the remaining of this section, a monoidal category will be shortly denoted by $(\mathcal{C}, \otimes, I)$. We will make computations and definitions as if $\mathcal{C}$ was strict monoidal, however, by coherence, everything we do and prove remains valid in the non-strict setting.

1.4.2 Monoidal functors

Definition 1.4.3 *Let $\mathcal{C}_1$ and $\mathcal{C}_2$ be two monoidal categories. A monoidal functor or tensor functor from $\mathcal{C}_1 \to \mathcal{C}_2$ is a triple (F, φ_0, φ) where*

- *F is a functor;*
- *$\varphi_0 :\ k_2 \to F(k_1)$ is a $\mathcal{C}_2$-morphism;*
- *$\varphi :\ \otimes \circ (F, F) \to F \circ \otimes$ is a natural transformation between functors $\mathcal{C}_1 \times \mathcal{C}_1 \to \mathcal{C}_2$ - so we have a family of morphisms*

$$\varphi_{M,N} :\ F(M) \otimes F(N) \to F(M \otimes N)$$

such that the following diagrams commute, for all $M, N, P \in \mathcal{C}_1$:

$$\begin{tikzcd}
(F(M) \otimes F(N)) \otimes F(P) \arrow[r, "a_{F(M),F(N),F(P)}"] \arrow[d, "\varphi_{M,N} \otimes F(P)"'] & F(M) \otimes (F(N) \otimes F(P)) \arrow[d, "F(M) \otimes \varphi_{P,Q}"] \\
F(M \otimes N) \otimes F(P) \arrow[d, "\varphi_{M \otimes N,P}"'] & F(M) \otimes F(N \otimes P) \arrow[d, "\varphi_{M,N \otimes P}"] \\
F((M \otimes N) \otimes P) \arrow[r, "F(a_{M,N,P})"] & F(M \otimes (N \otimes P))
\end{tikzcd} \tag{1.6}$$

$$\begin{tikzcd}
k_2 \otimes F(M) \arrow[r, "l_{F(M)}"] \arrow[d, "\varphi_0 \otimes F(M)"'] & F(M) \\
F(k_1) \otimes F(M) \arrow[r, "\varphi_{k_1,M}"] & F(k_1 \otimes M) \arrow[u, "F(l_M)"']
\end{tikzcd}
\qquad
\begin{tikzcd}
F(M) \otimes k_2 \arrow[r, "r_{F(M)}"] \arrow[d, "F(M) \otimes \varphi_0"'] & F(M) \\
F(M) \otimes F(k_1) \arrow[r, "\varphi_{M,k_1}"] & F(M \otimes k_1) \arrow[u, "F(r_M)"']
\end{tikzcd} \tag{1.7}$$

If φ_0 is an isomorphism, and φ is a natural isomorphism, then we say that F is a strong monoidal functor. If φ_0 and the morphisms underlying φ are identity maps, then we say that F is strict monoidal.
A functor $F : \mathcal{C} \to \mathcal{D}$ between the monoidal categories $(\mathcal{C}, \otimes, I)$ and $(\mathcal{D}, \odot, J)$ is called an op-monoidal, if and only if $F^{op,cop} : \mathcal{C}^{op} \to \mathcal{D}^{op}$ has the structure of a monoidal functor. Hence an op-monoidal functor consists of a triple (F, ψ_0, ψ), where $\psi_0 : F(I) \to J$ is a morphism in $\mathcal{D}$ and $\psi_{X,Y} : F(X \otimes Y) \to F(X) \odot F(Y)$ are morphisms in $\mathcal{D}$, natural in $X, Y \in \mathcal{C}$, satisfying suitable compatibility conditions.
A strong monoidal functor (F, ϕ_0, ϕ) is automatically op-monoidal. Indeed, one can take $\psi_0 = \phi_0^{-1}$ and $\psi = \phi^{-1}$.

Example 1.4.4 1) Consider the functor $k- : \underline{\text{Sets}} \to {}_k\mathcal{M}$ mapping a set X to the vector space kX with basis X. For a function $f : X \to Y$, the corresponding linear map kf is given by the formula

$$kf(\sum_{x \in X} a_x x) = \sum_{x \in X} a_x f(x).$$

The isomorphism $\varphi_0 : k \to k*$ is given by $\varphi_0(a) = a^*$.

$$\varphi_{X,Y} : kX \otimes kY \to k(X \times Y)$$

is given by $\varphi_{X,Y}(x \otimes y) = (x, y)$, for $x \in X$, $y \in Y$. Hence the linearizing functor $k-$ is strongly monoidal.

2) Let G be a monoid. The forgetful functor $U : {}_{kG}\mathcal{M} \to {}_k\mathcal{M}$ is strongly monoidal. The maps $\varphi : k \to U(k) = k$ and $\varphi_{M,N} : U(M) \otimes U(N) = M \otimes N \to U(M \otimes N) = M \otimes N$ are the identity maps. So U is a strict monoidal functor.

3) $\mathrm{Hom}(-, k) : \underline{\underline{\mathsf{Set}}}^{op} \to \mathcal{M}_k$ is a monoidal functor.

1.4.3 Symmetric and braided monoidal categories

Monoidal categories can be viewed as the categorical versions of monoids. Now we investigate the categorical notion of commutative monoid. It appears that there are two versions. We state our definition only for strict monoidal categories; it is left to the reader to write down the appropriate definition in the general case.

Definition 1.4.5 *Let $(\mathcal{C}, \otimes, k)$ be a strict monoidal category, and consider the switch functor*

$$\tau : \mathcal{C} \times \mathcal{C} \to \mathcal{C} \times \mathcal{C}; \;\; \tau(C, C') = (C', C), \;\; \tau(f, f') = (f', f).$$

A braiding on $\mathcal{C}$ is a natural isomorphism $\gamma : \mathrm{id} \Rightarrow \tau$ such that $\gamma_{k,C} = \gamma_{C,k} = C$ and the following diagrams commute, for all $C, C', C'' \in \mathcal{C}$.

$$\begin{tikzcd} C \otimes C' \otimes C'' \arrow[rr, "\gamma_{C,C'\otimes C''}"] \arrow[dr, "\gamma_{C',C}\otimes C''"'] & & C' \otimes C'' \otimes C \\ & C' \otimes C \otimes C'' \arrow[ur, "C'\otimes\gamma_{C,C''}"'] & \end{tikzcd}$$

$$\begin{tikzcd}
C \otimes C' \otimes C'' \arrow[rr, "\gamma_{C\otimes C',C''}"] \arrow[dr, "C\otimes\gamma_{C',C''}"'] & & C'' \otimes C \otimes C' \\
& C \otimes C'' \otimes C' \arrow[ur, "\gamma_{C,C''}\otimes C'"'] &
\end{tikzcd}$$

γ is called a symmetry if $\gamma^{-1}_{C,C'} = \gamma_{C',C}$, for all $C, C' \in \mathcal{C}$.

A monoidal category with a braiding (resp. a symmetry) is called a braided monoidal category (resp. a symmetric monoidal category).

Examples 1.4.6 1. $\underline{\underline{\mathrm{Set}}}$ is a symmetric monoidal category, where the symmetry is given by the swich map $\gamma_{X,Y} : X \times Y \to Y \times X, \gamma_{X,Y}(x, y) = (y, x)$.

2. $\mathcal{M}_k$ is a symmetric monoidal category, where the symmetry is given by $\gamma_{X,Y} : X \otimes Y \to Y \otimes X,\ \gamma_{X,Y}(x \otimes y) = y \otimes x$ (and linearly extended).

3. In general, there is no braiding on ${}_A\mathcal{M}_A$, the category of A-bimodules.

Let $(\mathcal{C}, \otimes, I, \gamma$ and $(\mathcal{D}, \odot, J, \delta)$ be (strict) braided monoidal categories. A monoidal functor $(F, \varphi_0, \varphi) : (\mathcal{C}, \otimes, I) \to (\mathcal{D}, \odot, J)$ is called braided if it preserves the braiding, meaning that the following diagram commutes, for all $X, Y \in \mathcal{C}$:

$$\begin{tikzcd}
F(X) \odot F(Y) \arrow[r, "\delta_{F(X),F(Y)}"] \arrow[d, "\phi_{X,Y}"'] & F(Y) \odot F(X) \arrow[d, "\phi_{Y,X}"] \\
F(X \otimes Y) \arrow[r, "F(\gamma_{X,Y})"'] & F(Y \otimes X)
\end{tikzcd}$$

Chapter 2

Hopf algebras

2.1 Monoidal categories and bialgebras

Let k be a field (or, more generally, a commutative ring). Recall that a k-algebra is a k-vector space (a k-module in the case where we work over a commutative ring) A with an associative multiplication $A \times A \to A$, which is a k-bilinear map, and with a unit 1_A. The multiplication can be viewed as a k-linear map $A \otimes A \to A$, because of the universal property of the tensor product. Examples of k-algebras include the $n \times n$-matrix algebra $\mathrm{M}_n(k)$, the group algebra kG, and many others.
Recall that kG is the free k-module with basis $\{\sigma \mid \sigma \in G\}$ and with multiplication defined on the basic elements by the multiplication in G. The group algebra kG is special in the sense that it has the following property: if M and N are kG-modules, then $M \otimes N$ is also a kG-module. The basic elements act on $M \otimes N$ as follows:

$$\sigma(m \otimes n) = \sigma m \otimes \sigma n.$$

This action can be extended linearly to the whole of kG. Also k is a kG-module, with action

$$(\sum_{\sigma \in G} a_\sigma \sigma)x = \sum_{\sigma \in G} \sigma x.$$

We will now investigate whether there are other algebras that have a similar property.

Now let A be a k-algebra, and assume that we have a monoidal structure on ${}_A\mathcal{M}$ such that the forgetful functor $U: {}_A\mathcal{M} \to {}_k\mathcal{M}$ is strongly monoidal, in such a way that the maps φ_0 and $\varphi_{M,N}$ are the identity maps, as in Example 1.4.4 (2). This means in particular that the unit object of ${}_A\mathcal{M}$ is equal to k (after forgetting the A-module structure), and that the tensor product of $M, N \in {}_A\mathcal{M}$ is equal to $M \otimes N$ as a k-module. Also it follows from the commuting diagrams in Definition 1.4.3 that the associativity and unit constraints in ${}_A\mathcal{M}$ are the same as in ${}_k\mathcal{M}$.

$A \in {}_A\mathcal{M}$ via left multiplication. Thus $A \otimes A \in {}_A\mathcal{M}$. Consider the k-linear map

$$\Delta: A \to A \otimes A, \quad \Delta(a) = a(1 \otimes 1).$$

For $a \in A$, we have that $\Delta(a) = \sum_i a_i \otimes a'_i$, with $a_i, a'_i \in A$. It is incovenient that the a_i and a'_i are not uniquelly determined: an element in the tensor product of two modules can usually be written in several different ways as a sum of tensor monomials. We will have situations where the map Δ will be applied several times, leading to multiple indices. In order to avoid this notational complication, we introduce the following notation:

$$\Delta(a) = \sum_{(a)} a_{(1)} \otimes a_{(2)}.$$

This notation is usually refered to as the *Sweedler-Heyneman notation*. It can be simplified further by omitting the summation symbol. We then obtain

$$\Delta(a) = a_{(1)} \otimes a_{(2)}.$$

The reader has to keep in mind that the right hand side of this notation is in general not a monomial: the presence of the Sweedler indices (1) and (2) implies implicitly that we have a (finite) sum of monomials.

Once Δ is known, the A-action on $M \otimes N$ is known for all $M, N \in {}_A\mathcal{M}$. Indeed, take $m \in M$ and $n \in N$, and consider the left A-linear maps

$$f_m : A \to M, \;\; f_m(a) = am \;\; ; \;\; g_n : A \to N, \;\; g_n(a) = an.$$

From the functoriality of the tensor product, it follows that $f_m \otimes g_n$ is a morphism in ${}_A\mathcal{M}$, i.e. $f_m \otimes g_n$ is left A-linear. In particular

$$\begin{aligned} a(m \otimes n) &= a((f_m \otimes g_n)(1 \otimes 1)) = (f_m \otimes g_n)(a(1 \otimes 1)) = (f_m \otimes g_n)(\Delta(a)) \\ &= (f_m \otimes g_n)(a_{(1)} \otimes a_{(2)}) = a_{(1)}m \otimes a_{(2)}n. \end{aligned}$$

We conclude that

$$a(m \otimes n) = a_{(1)}m \otimes a_{(2)}n. \tag{2.1}$$

The associativity constraint $a_{A,A,A} : (A \otimes A) \otimes A \to A \otimes (A \otimes A)$ is also morphism in ${}_A\mathcal{M}$. Hence

$$a(1 \otimes (1 \otimes 1)) = a_{(1)} \otimes a_{(2)}(1 \otimes 1) = a_{(1)} \otimes \Delta(a_{(2)})$$

is equal to

$$a(a_{A,A,A}((1\otimes 1)\otimes 1)) = a_{A,A,A}(a((1\otimes 1)\otimes 1)) = a_{A,A,A}(a_{(1)}(1\otimes 1)\otimes a_{(2)}) = a_{A,A,A}(\Delta(a_{(1)})\otimes a_{(2)}).$$

We conclude that

$$a_{(1)} \otimes \Delta(a_{(2)}) = \Delta(a_{(1)}) \otimes a_{(2)}. \tag{2.2}$$

This property is called the *coassociativity* of A. It can also be expressed as

$$(A \otimes \Delta) \circ \Delta = (\Delta \otimes A) \circ \Delta$$

We also use the following notation:

$$a_{(1)} \otimes \Delta(a_{(2)}) = \Delta(a_{(1)}) \otimes a_{(2)} = \Delta^2(a) = a_{(1)} \otimes a_{(2)} \otimes a_{(3)}.$$

We also know that $k \in {}_A\mathcal{M}$. Consider the map

$$\varepsilon : \ A \to k, \ \ \varepsilon(a) = a \cdot 1_k.$$

Since the left unit map $l_A : \ k \otimes A \to A$, $l_A(x \otimes a) = xa$ is left A-linear, we have

$$a = al_A(1_k \otimes 1_A) = l_A(a(1_k \otimes 1_A) = l_A(\varepsilon(a_{(1)}) \otimes a_{(2)}) = \varepsilon(a_{(1)})a_{(2)}.$$

We conclude that

$$\varepsilon(a_{(1)})a_{(2)} = a = a_{(1)}\varepsilon(a_{(2)}). \tag{2.3}$$

The second equality follows from the left A-linearity of r_A. This property is called the *counit property*.
We can also compute

$$\begin{aligned}
&\Delta(ab) = (ab)(1 \otimes 1) = a(b(1 \otimes 1)) = a(b_{(1)} \otimes b_{(2)}) = a_{(1)}b_{(1)} \otimes a_{(2)}b_{(2)};\\
&\Delta(1) = 1(1 \otimes 1) = 1 \otimes 1;\\
&\varepsilon(ab) = (ab) \cdot 1_k = a \cdot (b \cdot 1_k) = a \cdot \varepsilon(b) = \varepsilon(a)\varepsilon(b)\\
&\varepsilon(1) = 1 \cdot 1_k = 1_k.
\end{aligned}$$

These four equalities can be expressed as follows: the maps Δ and ε are algebra maps. Here $A \otimes A$ is a k-algebra with the following multiplication:

$$(a \otimes b)(a' \otimes b') = aa' \otimes bb'.$$

Theorem 2.1.1 *Let A be a k-algebra. There is a bijective correspondence between*

- *monoidal structures on ${}_A\mathcal{M}$ that are such that the forgetful functor ${}_A\mathcal{M} \to {}_k\mathcal{M}$ is strict monoidal, and φ_0 and $\varphi_{M,N}$ are the identity maps;*
- *couples of k-algebra maps $(\Delta : \ A \to A \otimes A, \ \varepsilon : \ A \to k)$ satisfying the coassociativity property (2.2) and the counit property (2.3).*

Proof. We have already seen how we construct Δ and ε if a monoidal structure is given. Conversely, given Δ and ε, a left A-module structure is defined on $M \otimes N$ by (2.1). k is made into a left A-module by the formula $a \cdot x = \varepsilon(a)x$. It is straightforward to verify that this makes ${}_A\mathcal{M}$ into a monoidal category. □

Definition 2.1.2 *A k-bialgebra is a k-algebra together with two k-algebra maps $\Delta : \ A \to A \otimes A$ and $\varepsilon : \ A \to k$ satisfying the coassociativity property (2.2) and the counit property (2.3). Δ is called the comultiplication or the diagonal map. ε is called the counit or augmentation map.*

Example 2.1.3 Let G be a monoid. Then kG is a bialgebra. The comultiplication Δ and the augmentation ε are given by the formulas

$$\Delta(\sigma) = \sigma \otimes \sigma \ \ ; \ \ \varepsilon(\sigma) = 1$$

A k-module C together with two k-linear maps $\Delta: C \to C \otimes C$ and $\varepsilon: C \to k$ satisfying the coassociativity property (2.2) and the counit property (2.3) is called a *coalgebra*.

A k-linear map $f: C \to D$ between two coalgebras is called a coalgebra map if $\varepsilon_D \circ f = \varepsilon_C$ and $\Delta_D \circ f = (f \otimes f) \circ \Delta_C$, that is

$$\varepsilon_D(f(c)) = \varepsilon_C(c) \text{ and } f(c)_{(1)} \otimes f(c)_{(2)} = f(c_{(1)}) \otimes f(c_{(2)}).$$

Thus a bialgebra A is a k-module with simultaneously a k-algebra and a k-coalgebra structure, such that Δ and ε are algebra maps, or, equivalently, the multiplication $m: A \otimes A \to A$ and the unit map $\eta: k \to A$, $\eta(x) = x1$ are coalgebra maps.

Let A and B be bialgebras. A k-linear map $f: A \to B$ is called a bialgebra map if it is an algebra map and a coalgebra map.

2.2 Hopf algebras and duality

2.2.1 The convolution product, the antipode and Hopf algebras

Let C be a coalgebra, and A an algebra. We can now define a product $*$ on $\mathrm{Hom}(C, A)$ as follows: for $f, g: C \to A$, let $f * g$ be defined by

$$f * g = m_A \circ (f \otimes g) \circ \Delta_C \tag{2.4}$$

or

$$(f * g)(c) = f(c_{(1)})g(c_{(2)}) \tag{2.5}$$

$*$ is called the *convolution product*. Observe that $*$ is associative, and that for any $f \in \mathrm{Hom}(C, A)$, we have that

$$f * (\eta_A \circ \varepsilon_C) = (\eta_A \circ \varepsilon_C) * f = f$$

so the convolution product makes $\mathrm{Hom}_k(C, A)$ into a k-algebra with unit.
Now suppose that H is a bialgebra, and take $H = A = C$ in the above construction. If the identity H of H has a convolution inverse $S = S_H$, then we say that H is a Hopf algebra. $S = S_H$ is called the *antipode* of H. The antipode therefore satisfies the following property: $S * H = H * S = \eta \circ \varepsilon$ or

$$h_{(1)}S(h_{(2)}) = S(h_{(1)})h_{(2)} = \eta(\varepsilon(h)) \tag{2.6}$$

for all $h \in H$. A bialgebra homomorphism $f: H \to K$ is called a Hopf algebra homomorphism if $S_K \circ f = f \circ S_H$.

Proposition 2.2.1 *Let H and K be Hopf algebras. If $f: H \to K$ is a bialgebra map, then it is a Hopf algebra map.*

Proof. We show that $S_K \circ f$ and $f \circ S_H$ have the same inverse in the convolution algebra $\mathrm{Hom}(H, K)$. Indeed, for all $h \in H$, we have

$$\begin{aligned}((S_K \circ f) * f)(h) &= S_K(f(h_{(1)}))f(h_{(2)}) = S_K(f(h)_{(1)})f(h)_{(2)} \\ &= \varepsilon_K(f(h))1_K = \varepsilon_H(h)1_K.\end{aligned}$$

and

$$\begin{aligned}(f*(f\circ S_H))(h) &= f(h_{(1)})f(S_H(h_{(2)}))=f(h_{(1)}S_H(h_{(2)})\\ &= f(\varepsilon_H(h)1_H)=\varepsilon_H(h)1_K.\end{aligned}$$

This shows that $S_K\circ f$ is a left inverse of f, and $f\circ S_H$ is a right inverse of f. If an element of an algebra has a left inverse and a right inverse, then the left and right inverse are equal, and are a two-sided inverse. Indeed, if $xa=ay=1$, then $xay=x1=x$ and $xay=1y=y$. □

Example 2.2.2 Let G be a group. The group algebra kG is a Hopf algebra: the antipode S is given by the formula

$$S(\sum_{\sigma\in G}a_\sigma\sigma)=\sum_{\sigma\in G}a_\sigma\sigma^{-1}.$$

Proposition 2.2.3 *Let H be a Hopf algebra.*

1. $S(hg)=S(g)S(h)$*, for all* $g,h\in H$*;*
2. $S(1)=1$*;*
3. $\Delta(S(h))=S(h_{(2)})\otimes S(h_{(1)})$*, for all* $h\in H$*;*
4. $\varepsilon(S(h))=\varepsilon(h)$*.*

In other words, $S:\ H\to H^{\rm op}$ *is an algebra map, and* $S:\ H\to H^{\rm cop}$ *is a colagebra map.*

Proof. 1) We consider the convolution algebra $\mathrm{Hom}(H\otimes H,H)$. Take $F,G,M:\ H\otimes H\to H$ defined by

$$F(h\otimes g)=S(g)S(h);\ \ G(h\otimes g)=S(hg);\ \ M(h\otimes g)=hg.$$

A straightforward computation shows that M is a left inverse for F and a right inverse for G. This implies that $F=G$, and the result follows.
2) $1=\varepsilon(1)1=S(1_{(1)})1_{(2)}=S(1)$.
3) Now we consider the convolution algebra $\mathrm{Hom}(H,H\otimes H)$, and $F,G:\ H\to H\otimes H$ given by

$$F(h)=\Delta(S(h));\ \ G(h)=S(h_{(2)})\otimes S(h_{(1)}).$$

Then Δ is a left inverse for F and a right inverse for G, hence $F=G$.
4) Apply ε to the relation $h_{(1)}S(h_{(2)})=\varepsilon(h)1$. This gives

$$\varepsilon(h)=\varepsilon(h_{(1)})\varepsilon(S(h_{(2)}))=\varepsilon(S(\varepsilon(h_{(1)})h_{(2)}))=\varepsilon(S(h)).$$

□

Proposition 2.2.4 *Let H be a Hopf algebra. The following assertions are equivalent.*

1. $S(h_{(2)})h_{(1)}=\varepsilon(h)1$*, for all* $h\in H$*;*
2. $h_{(2)}S(h_{(1)})=\varepsilon(h)1$*, for all* $h\in H$*;*

3. $S \circ S = H$.

Proof. $1) \Rightarrow 3)$. We show that $S^2 = S \circ S$ is a right convolution inverse for S. Since H is a (left) convolution inverse of S, it then follows that $S \circ S = H$.

$$\begin{aligned}(S * S^2)(h) = S(h_{(1)})S^2(h_{(2)}) &= S(S(h_{(2)})h_{(1)}) \\ &= S(\varepsilon(h)1) = \varepsilon(h)1.\end{aligned}$$

$3) \Rightarrow 1)$. Apply S to the equality $S(h_{(1)})h_{(2)} = \varepsilon(h)1$.
$2) \Rightarrow 3)$. We show that $S^2 = S \circ S$ is a leftt convolution inverse for S.
$3) \Rightarrow 2)$. Apply S to the equality $h_{(1)}S(h_{(2)}) = \varepsilon(h)1$. □

Corollary 2.2.5 *If H is commutative or cocommutative, then $S \circ S = H$.*

2.2.2 Projective modules

Let V be a k-module. Recall that V is projective if it has a dual basis; this is a set

$$\{(e_i, e_i^*) \mid i \in I\} \subset V \times V^*$$

such that for each $v \in V$

$$\#\{i \in I \mid \langle e_i^*, v\rangle \neq 0\} < \infty$$

and

$$v = \sum_{i \in I} \langle e_i^*, v\rangle e_i \tag{2.7}$$

If I is a finite set, then V is called finitely generated projective.
Let V and W be k-modules. Then we have a natural map

$$i: \ V^* \otimes W^* \to (V \otimes W)^*$$

given by

$$\langle i(v^* \otimes w^*), v \otimes w\rangle = \langle v^*, v\rangle\langle w^*, w\rangle$$

If k is a field, then every k-vector space is projective, and a vector space is finitely generated projective if and only if it is finite dimensional. If this is the case, then we have for all $v \in V$ and $v^* \in V^*$:

$$\langle v^*, v\rangle = \sum_i \langle e_i^*, v\rangle\langle v^*, e_i\rangle$$

hence

$$v^* = \sum_i \langle v^*, e_i\rangle e_i^*. \tag{2.8}$$

Proposition 2.2.6 *A k-module M is finitely generated projective if and only if the map*

$$\iota: \ M \otimes M^* \to \mathrm{End}(M), \ \ \iota(m \otimes m^*)(n) = \langle m^*, n\rangle m$$

is bijective.

Proof. First assume that ι is bijective. Let $\iota^{-1}(M) = \sum_i e_i \otimes e_i^*$. Then for all $m \in M$,

$$m = \iota(\sum_i e_i \otimes e_i^*)(m) = \sum_i \langle e_i^*, m\rangle e_i$$

so $\{(e_i, e_i^*)\}$ is a finite dual basis of M.
Conversely, take a finite dual basis $\{(e_i, e_i^*)\}$ of M, and define

$$\kappa : \ \mathrm{End}(M) \to M \otimes M^*$$

by

$$\kappa(f) = \sum_i f(e_i) \otimes e_i^*.$$

For all $f \in \mathrm{End}(M)$, $m, n \in M$ and $m^* \in M^*$, we have

$$\begin{aligned}
\iota(\kappa(f))(n) &= \sum_i \langle e_i^*, n\rangle f(e_i) \\
&= f(\sum_i \langle e_i^*, n\rangle e_i) = f(n); \\
\kappa(\iota(m \otimes m^*)) &= \sum_i \iota(m \otimes m^*)(e_i) \otimes e_i^* \\
&= \sum_i \langle m^*, e_i\rangle m \otimes e_i^* \\
&= m \otimes \sum_i \langle m^*, e_i\rangle e_i^* = m \otimes m^*,
\end{aligned}$$

and this shows that κ is the inverse of ι. □

Proposition 2.2.7 *If V and W are finitely generated projective, then $i : \ V^* \otimes W^* \to (V \otimes W)^*$ is bijective.*

Proof. Let $\{(e_i, e_i^*) \mid i \in I\} \subset V \times V^*$ and $\{(f_j, f_j^*) \mid j \in J\} \subset W \times W^*$ be finite dual bases for V and W. We define i^{-1} by

$$i^{-1}(\varphi) = \sum_{i,j} \langle \varphi, e_i \otimes f_j\rangle e_i^* \otimes f_j^*$$

A straightforward computation shows that i^{-1} is the inverse of i. □

2.2.3 Duality

Our next aim is to give a categorical interpretation of the definition of a Hopf algebra.

Definition 2.2.8 *A monoidal category $\mathcal{C}$ has left duality if for all $M \in \mathcal{C}$, there exists $M^* \in \mathcal{C}$ and two maps*

$$\mathrm{coev}_M : \ k \to M \otimes M^* \ \ ; \ \ \mathrm{ev}_M : \ M^* \otimes M \to k$$

such that

$$(M \otimes \mathrm{ev}_M) \circ (\mathrm{coev}_M \otimes M) = M \text{ and } (\mathrm{ev}_M \otimes M^*) \circ (M^* \otimes \mathrm{coev}_M) = M^*$$

This means that the two following diagrams are commutative:

$$\begin{tikzcd} M \arrow[r, "\mathrm{coev}_M \otimes M"] \arrow[dr, "="'] & M \otimes M^* \otimes M \arrow[d, "M \otimes \mathrm{ev}_M"] \\ & M \end{tikzcd} \qquad \begin{tikzcd} M^* \arrow[r, "M^* \otimes \mathrm{coev}_M"] \arrow[dr, "="'] & M^* \otimes M \otimes M^* \arrow[d, "\mathrm{ev}_M \otimes M^*"] \\ & M^* \end{tikzcd}$$

Example 2.2.9 ${}_k\mathcal{M}^f$, the full subcategory of ${}_k\mathcal{M}$ consisting of finitely generated projective k-modules, is a category with left duality. $M^* = \mathrm{Hom}(M, k)$ is the linear dual of M and the evaluation and coevaluation maps are given by the formulas

$$\mathrm{ev}_M(m^* \otimes m) = \langle m^*, m\rangle \;\; ; \;\; \mathrm{coev}(1_k) = \sum_i e_i \otimes e_i^*,$$

where $\{(e_i, e_i^*)\}$ is a finite dual basis of M.

Proposition 2.2.10 *For a Hopf algebra H, the category ${}_H\mathcal{M}^f$ of left H-modules that are finitely generated and projective as a k-module has left duality.*

Proof. Take a left H-module M. It is easy to see that M^* is a right H-module as follows:

$$\langle m^* \leftharpoonup h, m\rangle = \langle m^*, hm\rangle.$$

But we have to make M^* into a *left* H-module. To this end, we apply the antipode:

$$h \cdot m^* = m^* \leftharpoonup S(h),$$

or

$$\langle h \cdot m^*, m\rangle = \langle m^*, S(h)m\rangle.$$

We are done if we can show that ev_M and coev_M are left H-linear. We first prove that ev_M is left H-linear:

$$\begin{aligned} \mathrm{ev}_M(h \cdot (m^* \otimes m)) &= \mathrm{ev}_M(h_{(1)} \cdot m^* \otimes h_{(2)}m) \\ &= \langle h_{(1)} \cdot m^*, h_{(2)}m\rangle = \langle m^*, S(h_{(1)})h_{(2)}m\rangle = \varepsilon(h)\mathrm{ev}_M(m^* \otimes m). \end{aligned}$$

Before we show that coev_M is left H-linear, we observe that $\mathrm{End}(M)$ is a left H-module under the following action:

$$(h \cdot f)(n) = h_{(1)}f(S(h_{(2)})n).$$

This action is such that $\iota : M \otimes M^* \to \mathrm{End}(M)$ is an isomorphism of left H-modules. Indeed, for all $m, n \in M$ and $m^* \in M^*$, we have

$$\begin{aligned} \iota(h(m \otimes m^*))(n) &= \iota(h_{(1)}m \otimes h_{(2)}m^*)(n) \\ &= \langle m^*, S(h_{(2)})n\rangle h_{(1)}m = (h \cdot \iota(m \otimes m^*))(n). \end{aligned}$$

Now it suffices to show that $\iota \circ \mathrm{coev}_M : k \to \mathrm{End}(M)$ is left H-linear. For $x \in k$, we have that $(\iota \circ \mathrm{coev}_M)(x) = xI_M$, multiplication by the scalar $x \in k$. Here we wrote I_M for the identity of M. It is now easy to compute that

$$((h \cdot (\iota \circ \mathrm{coev}_M))(x))(m) = (h \cdot xI_M)(m) = h_{(1)}xS(h_{(2)})m = x\varepsilon(h)m,$$

hence

$$(h \cdot (\iota \circ \mathrm{coev}_M))(x) = x\varepsilon(h)I_M = (\iota \circ \mathrm{coev}_M)(\varepsilon(h)x),$$

as needed. □

2.3 Properties of coalgebras

2.3.1 Examples of coalgebras

Examples 2.3.1 1) Let S be a nonempty set, and let $C = kS$ be the free k-module with basis S. Define Δ and ε by

$$\Delta(s) = s \otimes s \ \text{ and } \ \varepsilon(s) = 1$$

for all $s \in S$. Then (C, Δ, ε) is a coalgebra.

2) Let C be the free k-module with basis $\{c_m \mid m \in \mathbb{N}\}$. Now define Δ and ε by

$$\Delta(c_m) = \sum_{i=0}^{m} c_i \otimes c_{m-i} \ \text{ and } \ \varepsilon(c_m) = \delta_{0,m}$$

This coalgebra is called the *divided power coalgebra*.

3) k is a coalgebra; Δ and ε are the canonical isomorphisms.

4) Let $\mathrm{M}^n(k)$ be free k-module of dimension n^2 with k-basis $\{e_{ij} \mid i, j = 1, \cdots, n\}$. We define a comultiplication Δ and a counit ε by the formulas

$$\Delta(e_{ij}) = \sum_{k=1}^{n} e_{ik} \otimes e_{kj} \ \text{ and } \ \varepsilon(e_{ij}) = \delta_{ij}$$

$\mathrm{M}^n(k)$ is called the matrix coalgebra.

5) Let C be the free k-module with basis $\{g_m, d_m \mid m \in \mathbb{N}^*\}$.We define a comultiplication Δ and a counit ε by the formulas

$$\Delta(g_m) = g_m \otimes g_m \ ; \ \varepsilon(g_m) = 1$$

$$\Delta(d_m) = g_m \otimes d_m + d_m \otimes g_{m+1} \ ; \ \varepsilon(d_m) = 0$$

6) Let C be the free k-module with basis $\{s, c\}$. We define $\Delta : C \to C \otimes C$ and $\varepsilon : C \to k$ by

$$\Delta(s) = s \otimes c + c \otimes s \ ; \ \varepsilon(s) = 0$$

$$\Delta(c) = c \otimes c + s \otimes s \;\; ; \;\; \varepsilon(c) = 1$$

C is called the trigonometric coalgebra.

7) Let $C = (C, \Delta, \varepsilon)$. Then $C^{\rm cop} = (C, \Delta^{\rm cop} = \tau \circ \Delta, \varepsilon)$ is also a coalgebra, called the opposite coalgebra. The comultiplication in $C^{\rm cop}$ is given by the formula

$$\Delta^{\rm cop}(c) = c_{(2)} \otimes c_{(1)}$$

8) If C and D are coalgebra, then $C \otimes D$ is also coalgebra. The structure maps are

$$\varepsilon_{C\otimes D} = \varepsilon_C \otimes \varepsilon_D \;\text{ and }\; \Delta_{C\otimes D} = (I_C \otimes \tau \otimes I_D) \circ \Delta_C \otimes \Delta_D$$

that is,

$$\varepsilon_{C\otimes D}(c \otimes d) = \varepsilon_C(c)\varepsilon_D(d) \;\text{ and }\; \Delta_{C\otimes D}(c \otimes d) = (c_{(1)} \otimes d_{(1)}) \otimes (c_{(2)} \otimes d_{(2)})$$

$g \in C$ is called a grouplike element if $\Delta(g) = g \otimes g$ and $\varepsilon(g) = 1$ (see Example 1.4.2 1). The set of grouplike elements of C is denoted by $G(C)$.
Let g and h be grouplike elements. $x \in C$ is called (g,h)-primitive if $\Delta(x) = g \otimes x + x \otimes h$ and $\varepsilon(x) = 0$. A $(1,1)$-primitive element is called primitive. The set of (g,h)-primitive elements of C is denoted $P_{g,h}(C)$.

Duality

Let C be a coalgebra. Then C^* is an algebra, with multiplication

$$m_{C^*} = \Delta^* \circ i : \; C^* \otimes C^* \to (C \otimes C)^* \to C^*$$

and unit ε. C^* is called the *dual algebra* of C. The multiplication is given by

$$(c^* * d^*)(c) = \langle c^*, c_{(1)} \rangle \langle d^*, c_{(2)} \rangle$$

This multiplication is called the convolution.

Conversely, let A be an algebra that is finitely generated and projective as a k-module. Then A^* is a coalgebra, with comultiplication

$$\Delta_{A^*} = i^{-1} \circ m_A^* : \; A^* \to (A \otimes A)^* \to A^* \otimes A^*$$

and counit

$$\varepsilon_{A^*}(a^*) = \langle a^*, 1 \rangle.$$

The comultiplication Δ_{A^*} can be described explicitly in terms of the dual basis $\{(e_i, e_i^*)\}$ of A:

$$\Delta(h^*) = \sum_{i,j} \langle h^*, e_i e_j \rangle e_i^* \otimes e_j^*. \tag{2.9}$$

Examples 2.3.2 1) Let S be a set, and consider the coalgebra kS from Example 2.3.1 1). Then $(kS)^*$ is isomorphic to $\mathrm{Map}(S,k)$, the algebra of functions from S to k: to a morphism $f \in (kS)^*$, we associate its restriction to S, and, conversely, a map $f:\ S \otimes k$ can be extended linearly to a map $kS \to k$. The multiplication on $\mathrm{Map}(S,k)$ is then just pointwise multiplication. If S is finite then $(kS)^*$ is isomorphic as an algebra to the direct sum of a number of copies of k indexed by S.
2) Consider the coalgebra C from Example 2.3.1 2). The multiplication on C^* is given by

$$(f * g)(c_m) = \sum_{i=0}^{m} f(c_i)g(c_{m-i})$$

As an algebra, $C^* \cong k[[X]]$, the algebra of formal power series in one variable. The connecting isomorphism ϕ is given by

$$\phi(f) = \sum_{n=0}^{\infty} f(c_n)X^n$$

3) Consider the matrix coalgebra $\mathrm{M}^n(k)$. Its dual is isomorphic to the matrix algebra $\mathrm{M}_n(k)$. This can be seen as follows: define $e_{ij}^*:\ \mathrm{M}^n(k) \to k$ by

$$\langle e_{ij}^*, e_{kl} \rangle = \delta_{ik}\delta_{jl}$$

Then It can be verified immediately that the e_{ij}^* multiply under convolution as elementary matrices.
4) Let A be a finitely generated projective k-algebra. Then $G(A^*) = \mathrm{Alg}(A,k)$.

2.3.2 Subcoalgebras and coideals

Let $C = (C, \Delta, \varepsilon)$ be a coalgebra, and D a k-submodule of C. D is called a subcoalgebra of C if the comultiplication Δ restricts and corestricts to

$$\Delta_{|D}:\ D \to D \otimes D$$

in this case, $D = (D, \Delta_{|D}, \varepsilon_{|D})$ is itself a coalgebra.

Exercise 2.3.3 Let $(C_i)_{i\in I}$ be a family of subcoalgebras of C. Show that $\sum_{i\in I} C_i$ is a again a subcoalgebra of C.

A k-submodule I of C is called
- a left coideal if $\Delta(I) \subset C \otimes I$;
- a right coideal if $\Delta(I) \subset I \otimes C$;
- a coideal if $\Delta(I) \subset I \otimes C + C \otimes I$ and $\varepsilon(I) = 0$.

Exercise 2.3.4 Let k be a field, I be a left and right coideal of the coalgebra C; show that I is a subcoalgebra. Use the following property. If $X \subset V$ and $Y \subset W$ are vector spaces, then $(V \otimes Y) \cap (X \otimes W) = X \otimes Y$.

The following result is called the Fundamental Theorem of Coalgebras; it illustrates the intrinsic finiteness property of coalgebras.

Theorem 2.3.5 *Let C be a coalgebra over a field k. Every element $c \in C$ is contained in a finite dimensional subcoalgebra of C.*

Proof. Fix a basis $\{c_i \mid i \in I\}$ of C; we can write

$$(I \otimes \Delta)\Delta(c) = \sum_{i,j \in I} c_i \otimes x_{ij} \otimes c_j. \tag{2.10}$$

Only a finite number of the x_{ij} are different from 0. Let X be the subspace of C generated by the x_{ij}. Applying $\varepsilon \otimes C \otimes \varepsilon$ to (2.10), we find that

$$c = \sum_{i,j} \varepsilon(c_i)\varepsilon(c_j) \in X.$$

From the coassociativity of Δ, it follows that

$$\sum_{i,j \in I} c_i \otimes \Delta(x_{ij}) \otimes c_j = \sum_{i,j \in I} \Delta(c_i) \otimes x_{ij} \otimes c_j$$

Since $\{c_j \mid j \in I\}$ is linearly independent, we have, for all $j \in I$

$$\sum_{i \in I} c_i \otimes \Delta(x_{ij}) = \sum_{i \in I} \Delta(c_i) \otimes x_{ij}$$

It follows that $\sum_{i \in I} c_i \otimes \Delta(x_{ij}) \in C \otimes C \otimes X$, and, because $\{c_i \mid i \in I\}$ is linearly independent,

$$\Delta(x_{ij}) \in C \otimes X$$

In a similar way, we prove that $\Delta(x_{ij}) \in X \otimes C$ and it follows that

$$\Delta(x_{ij}) \in C \otimes X \cap X \otimes C = X \otimes X$$

and X is a finite dimensional subcoalgebra of C containing c. □

Exercise 2.3.6 Let $f : C \to D$ be a morphism of coalgebras. Prove that $\mathrm{Im}\,(f)$ is a subcoalgebra of D and $\mathrm{Ker}\,(f)$ is a coideal in C.

Proposition 2.3.7 *Let I be a coideal in a coalgebra C, and $p : C \to C/I$ the canonical projection.*
1) There exists a unique coalgebra structure on C/I such that p is a coalgebra map.
2) If $f : C \to D$ is a coalgebra morphism with $I \subset \mathrm{Ker}\,(f)$, then f factors through C/I: there exists a unique coalgebra morphism $\overline{f} : C/I \to D$ such that $\overline{f} \circ p = f$.

Corollary 2.3.8 *Let $f : C \to D$ be a surjective coalgebra map. Then we have a canonical coalgebra isomorphism $C/\mathrm{Ker}\,(f) \cong D$.*

2.4 Comodules

The definition of a comodule over a coalgebra is a dual version of the definition of module over an algebra. Let k be a commutative ring, and C a k-coalgebra. A right C-comodule (M, ρ) is a k-module M together with a k-linear map $\rho : M \to M \otimes C$ such that the following diagrams commute:

$$\begin{tikzcd} M \arrow[r, "\rho"] \arrow[d, "\rho"'] & M \otimes C \arrow[d, "\rho\otimes C"] \\ M \otimes C \arrow[r, "M\otimes\Delta"] & M \otimes C \otimes C \end{tikzcd} \qquad \begin{tikzcd} M \arrow[r, "\rho"] \arrow[d, "M"'] & M \otimes C \arrow[d, "M\otimes\varepsilon"] \\ M \arrow[r, "r_M"] & M \otimes k \end{tikzcd}$$

We will also say that C coacts on M, or that ρ defines a coaction on M. We will use the following version of the Sweedler-Heynemann notation: if M is a comodule, and $m \in M$, then we write

$$\rho(m) = m_{[0]} \otimes m_{[1]}$$

$$(\rho \otimes I_C)\rho(m) = (I_M \otimes \Delta)\rho(m) = m_{[0]} \otimes m_{[1]} \otimes m_{[2]}$$

and so on. The second commutative diagram takes the form

$$\varepsilon(m_{[1]})m_{[0]} = m$$

A morphism between two comodules M and N is a k-linear map $f : M \to N$ such that

$$\rho(f(m)) = f(m)_{[0]} \otimes f(m)_{[1]} = f(m_{[0]}) \otimes m_{[1]}$$

for all $m \in M$. We say that f is C-colinear. The category of right C-comodules and C-colinear maps will be denoted by $\mathcal{M}^C$. We can also define left C-comodules. If ρ defines a left C-coaction on M, then we write

$$\rho(m) = m_{[-1]} \otimes m_{[0]} \in C \otimes M$$

Let C and D be coalgebras. If we have a left C-coaction ρ^l and a right D-coaction ρ^r on a k-module M such that

$$(\rho^l \otimes I_D) \circ \rho^r = (I_C \otimes \rho^r) \circ \rho^l$$

then we call (M, ρ^l, ρ^r) a (C, D)-bicomodule. We then write

$$(\rho^l \otimes I_D)\rho^r(m) = (I_C \otimes \rho^r)\rho^l(m) = m_{[-1]} \otimes m_{[0]} \otimes m_{[1]}$$

Examples 2.4.1 1) (C, Δ) is a right (and left) C-comodule.
2) Let V be a k-module. Then $(V \otimes C, I_V \otimes \Delta)$ is a right C-comodule.

Let S be a set. An S-graded k-module is a k-module M together with a decomposition as a direct sum of submodules indexed by S:

$$M = \oplus_{s\in S} M_s$$

This means that every $m \in M$ can be written in a unique way as a sum $m = \sum_{s\in S} m_s$ with m_s in M_s. m_s is called the homogeneous component of degree s of m, and we write $\deg(m_s) = s$. A map between two S-graded modules M and N is called graded if it preserves the degree, that is $f(M_s) \subset N_s$. The category of S-graded k-modules and graded homomorphisms is denoted gr^S.

Proposition 2.4.2 *Let S be a set and k a commutative ring. The category gr^S of graded modules is isomorphic to the category $\mathcal{M}^{kS}$ of right kS-comodules.*

Proof. We define a functor $F: \mathrm{gr}^S \to \mathcal{M}^{kS}$ as follows: $F(M)$ is M as a k-module, with coaction given by

$$\rho(m) = \sum_{s\in S} m_s \otimes s$$

if $m = \sum_{s\in S} m_s$ is the homogeneous decomposition of $m \in M$. F is the identity on the morphisms. Straightforward computations show that F is a well-defined functor.
Now we define a functor $G: \mathcal{M}^{kS} \to \mathrm{gr}^S$. Take a right kS-comodule M, and let

$$M_s = \{m \in M \mid \rho(m) = m \otimes s\}$$

Let $m \in M$, and write $\rho(m) = \sum_{s\in S} m_s \otimes s$. From the coassociativity of the coaction, it follows that

$$\sum_{s\in S} \rho(m_s) \otimes s = \sum_{s\in S} m_s \otimes s \otimes s$$

in $M \otimes kS \otimes kS$. Since S is a free basis of kS, it follows that $\rho(m_s) = m_s \otimes s$ for every $s \in S$, hence $m_s \in M_s$. Therefore

$$m = (I_M \otimes \varepsilon)\rho(m) = \sum_{s\in S} m_s\varepsilon(s) = \sum_{s\in S} m_s \in \sum_{s\in S} M_s$$

and this proves that $M = \sum_{s\in S} M_s$. This is a direct sum: if $m \in M_s \cap M_t$, then $\rho(m) = m \otimes s = m \otimes t$, and from the fact that kS is free with basis S, it follows that $m = 0$ or $s = t$. Thus we have defined a grading on M, and $G(M)$ will be M as a k-module with this grading. G is the identity on the morphisms.
G is a well-defined functor, and F and G are each others inverses. □

Proposition 2.4.3 *Let C be a coalgebra over a commutative ring k. Then we have a functor $F: \mathcal{M}^C \to {}_{C^*}\mathcal{M}$. If C is finitely generated and projective as a k-module, then F is an isomorphism of categories.*

Proof. Take a right C-comodule M, and let $F(M) = M$ as a k-module, with left C^*-action given by

$$c^* \cdot m = \langle c^*, m_{[1]}\rangle m_{[0]}.$$

It is straightforward to verify that this is a well-defined C^*-action. Furthermore, if $f: M \to N$ is right C-colinear, then f is also left C^*-linear; so we define $F(f) = f$ on the level of the morphisms, and we obtain a functor F.
Suppose that C is finitely generated and projective, and let $\{(c_i, c_i^*) \mid i = 1, \cdots, n\}$ be a finite dual basis for C. We define a functor $G: {}_{C^*}\mathcal{M} \to \mathcal{M}^C$ as follows: $G(M) = M$, with right C-coaction

$$\rho(m) = \sum_{i=1}^{n} c_i^* \cdot m \otimes c_i.$$

A straightforward computation shows that G is a functor, which is inverse to F. □

Theorem 2.4.4 *Let C be a coalgebra over a field k, and $M \in \mathcal{M}^C$. Then any element $m \in M$ is contained in a finite dimensional subcomodule of M.*

Proof. Let $\{c_i \mid i \in I\}$ be a basis of C, and write

$$\rho(m) = \sum_{i\in I}{}' m_i \otimes c_i,$$

where only finitely many of the m_i are different from 0. The subspace N of M spanned by the m_i is finite dimensional. We can write

$$\Delta(c_i) = \sum_{j,k} a_{ijk} c_j \otimes c_k,$$

and then

$$\sum_i \rho(m_i) \otimes c_i = \sum_{i,j,k} m_i \otimes a_{ijk} c_j \otimes c_k,$$

hence

$$\rho(m_k) = \sum_{i,j} m_i \otimes a_{ijk} c_j \in N \otimes C,$$

so N is a subcomodule of M. □

Proposition 2.4.5 *Let C be a coalgebra. Then the categories $\mathcal{M}^C$ and ${}^{C^{\mathrm{cop}}}\mathcal{M}$ are isomorphic.*

Proposition 2.4.6 *If $N \subset M$ is a subcomodule, then M/N is also a comodule.*

Proposition 2.4.7 *Let $f : M \to N$ be right C-colinear. Then $\mathrm{Im}\,(f)$ is a C-comodule. If C is flat as a k-module, then $\mathrm{Ker}\, f$ is also a C-comodule.*

Proof. The first statement is straightforward: for any $m \in M$, we have

$$\rho_N(f(m)) = (f \otimes C)(\rho_M(m)) \in \mathrm{Im}\, f \otimes C.$$

To prove the second statement, we proceed as follows. We have an exact sequence of k-modules

$$0 \to \mathrm{Ker}\, f \to M \xrightarrow{f} N$$

Since C is flat, the sequence

$$0 \to \mathrm{Ker}\, f \otimes C \to M \otimes C \xrightarrow{f\otimes C} N \otimes C$$

is also exact, hence $\mathrm{Ker}\, f \otimes C = \mathrm{Ker}\,(f \otimes C)$. If $m \in \mathrm{Ker}\, f$, then

$$f(m_{[0]}) \otimes m_{[1]} = \rho_N(f(m)) = 0,$$

hence $\rho_M(m) \in \mathrm{Ker}\,(f \otimes C) = \mathrm{Ker}\, f \otimes C$, as needed. □

Proposition 2.4.8 *Assume that $C \in \mathcal{M}$ is flat, and let $f : M \to N$ in $\mathcal{M}^C$. There exists a unique isomorphism $\overline{f} : M/\mathrm{Ker}\, f \to \mathrm{Im}\, f$ in $\mathcal{M}^C$ such that the diagram*

$$\begin{tikzcd} M \arrow[r, "f"] \arrow[d, "p"'] & N \\ M/\mathrm{Ker}\, f \arrow[r, "\overline{f}"] & \mathrm{Im}\,(f) \arrow[u, "i"'] \end{tikzcd}$$

commutes, where p is the canonical projection, and i is the inclusion.

Proposition 2.4.9 *The category $\mathcal{M}^C$ has coproducts.*

Proof. Let $\{M_i \mid i \in I\}$ be a family of right C-comodules, with structure maps ρ_i. Let $\oplus_{i\in I} M_i$ be the coproduct of the M_i in $\mathcal{M}$, and $q_j : M_j \to \oplus_{i\in I} M_i$ the canonical injection. By the definition of the coproduct, there exists a unique k-linear map $\rho : \oplus_{i\in I} M_i \to \oplus_{i\in I} M_i \otimes C$ such that for every $j \in I$, the diagram

$$\begin{tikzcd} M_j \arrow[r, "q_j"] \arrow[dr, "(q_j\otimes C)\circ\rho_j"'] & \oplus_{i\in I} M_i \arrow[d, "\rho"] \\ & \oplus_{i\in I} M_i \otimes C \end{tikzcd}$$

commutes. It is easy to check that ρ is a coaction on $\oplus_{i\in I} M_i$, and that $\oplus_{i\in I} M_i$ is the coproduct of the M_i in $\mathcal{M}^C$. $\square$

Corollary 2.4.10 *If C is flat, then $\mathcal{M}^C$ is an abelian category. In particular, if k is a field, then $\mathcal{M}^C$ is an abelian category.*

Troughout the rest of this Section, k will be a field. Let C be a coalgebra, and M a vector space. We have a k-linear map

$$\psi : \mathrm{Hom}(M, M \otimes C) \to \mathrm{Hom}(C^* \otimes M, M)$$

defined as follows: if $\omega(m) = \sum_i m_i \otimes c_i$, then

$$\psi_\omega(c^* \otimes m) = \sum_i \langle c^*, c_i\rangle m_i.$$

Proposition 2.4.11 *(M, ω) is a right C-comodule if and only if (M, ψ_ω) is a left C^*-module.*

Proposition 2.4.12 *The map*

$$\mu_M : M \otimes C \to \mathrm{Hom}(C^*, M), \quad \mu_M(m \otimes c)(c^*) = \langle c^*, c\rangle m$$

is injective.

Proof. Let $\{c_i \mid i \in I\}$ be a basis of C, and let $c_i^* : C \to k$ be the projection defined by

$$\langle c_i^*, c_j\rangle = \delta_{ij}.$$

If $\sum_i m_i \otimes c_i \in \operatorname{Ker} \mu_M$, then for all $j \in I$:

$$0 = \mu_M(\sum_i m_i \otimes c_i)(c_j^*) = \sum_i \langle c_j^*, c_i \rangle m_i = m_j,$$

hence $m_j = 0$, and $\sum_i m_i \otimes c_i = 0$. □

Let M be a left C^*-module, with action $\psi : C^* \otimes M \to M$. Consider the map

$$\rho_M : M \to \operatorname{Hom}(C^*, M), \quad \rho_M(m)(c^*) = c^* m.$$

We say that M is a *rational* C^*-module if ρ_M factorizes through μ_M, that is, $\rho_M(M) \subset \mu_M(M \otimes C)$. This means that, for all $m \in M$, there exists

$$\sum_i m_i \otimes c_i \in M \otimes C$$

such that

$$c^* m = \sum_i \langle c^*, c_i \rangle m_i,$$

for all $c^* \in C^*$. It follows from the fact that μ_M is injective that $\sum_i m_i \otimes c_i \in M \otimes C$ is unique. $\operatorname{Rat}({}_{C^*}\mathcal{M})$ will be the full subcategory of ${}_{C^*}\mathcal{M}$ consisting of rational left C^*-modules.

Theorem 2.4.13 *Let k be a field. Then the categories $\mathcal{M}^C$ and $\operatorname{Rat}({}_{C^*}\mathcal{M})$ are isomorphic.*

Proof. We know from Proposition 2.4.3 that we have a functor $F : \mathcal{M}^C \to {}_{C^*}\mathcal{M}$, and it follows immediately from the construction of F that $F(M)$ is a rational C^*-module if M is a right C-comodule.
Now let M be a rational left C^*-module. Then the map $\rho_M : M \to \operatorname{Hom}(C^*, M)$ factorizes through a unique map $\rho : M \to M \otimes C$. Then

$$\psi_\rho(c^* \otimes m) = \sum_i \langle c^*, c_i \rangle m_i = c^* m,$$

and it follows from Proposition 2.4.11 that (M, ρ) is a comodule. We define $G(M) = (M, \rho)$. Then observe that $\rho(m) = m_{[0]} \otimes m_{[1]}$ if and only if

$$c^* m = \langle c^*, m_{[1]} \rangle m_{[0]}, \tag{2.11}$$

for all $c^* \in C^*$.
Let $f : M \to N$ be a C^*-linear map between two rational left C^*-modules, and let us show that f is right C-colinear. This is equivalent to

$$\rho(f(m)) = f(m_{[0]}) \otimes m_{[1]},$$

for all $m \in M$; using (2.11), this is equivalent to

$$c^* f(m) = \langle c^*, m_{[1]} \rangle f(m_{[0]}),$$

for all $m \in M$ and $c^* \in C^*$. This is easily verified:

$$c^* f(m) = f(c^* m) = f(\langle c^*, m_{[1]} \rangle m_{[0]}) = \langle c^*, m_{[1]} \rangle f(m_{[0]}).$$

□

2.5 Examples of Hopf algebras

Proposition 2.5.1 *Let H be a bialgebra that is finitely generated and projective as a k-module. Then H^* is also a bialgebra.*

Proof. We have seen that H^* is an algebra and a coalgebra. Let us show that $\Delta_{H^*} = m^*$ respects the convolution product, that is,

$$\Delta_{H^*}(h^*) * \Delta_{H^*}(k^*) = \Delta_{H^*}(h^* * k^*).$$

Indeed, for all $h, k \in H$, we have

$$\begin{aligned} \langle \Delta_{H^*}(h^*) * \Delta_{H^*}(k^*), h \otimes k\rangle &= \langle \Delta_{H^*}(h^*), h_{(1)} \otimes k_{(1)}\rangle\langle \Delta_{H^*}(k^*), h_{(2)} \otimes k_{(2)}\rangle \\ &= \langle h^*, h_{(1)}k_{(1)}\rangle\langle k^*, h_{(2)}k_{(2)}\rangle = \langle h^*, (hk)_{(1)}\rangle\langle k^*, (hk)_{(2)}\rangle \\ &= \langle h^* * k^*, hk\rangle = \langle \Delta_{H^*}(h^* * k^*), h \otimes k\rangle. \end{aligned}$$

□

Proposition 2.5.2 *Let H be a Hopf algebra which is finitely generated and projective as a k-module, then H^* is a Hopf algebra with antipode S^*.*

Proof. We have to show that

$$S^*(h^*_{(1)}) * h^*_{(2)} = \langle h^*, 1\rangle\varepsilon.$$

Indeed, for all $h \in H$, we have

$$\begin{aligned} \langle S^*(h^*_{(1)}) * h^*_{(2)}, h\rangle &= \langle S^*(h^*_{(1)}), h_{(1)}\rangle\langle h^*_{(2)}, h_{(2)}\rangle = \langle h^*_{(1)}, S(h_{(1)})\rangle\langle h^*_{(2)}, h_{(2)}\rangle \\ &= \langle h^*, S(h_{(1)})h_{(2)}\rangle = \langle h^*, \varepsilon(h)1\rangle = \langle h^*, 1\rangle\varepsilon(h) \end{aligned}$$

□

Let H be a Hopf algebra. $g \in H$ is called grouplike if $\Delta(g) = g \otimes g$ and $\varepsilon(g) = 1$. The product of two grouplike elements is again grouplike. If g is grouplike, then $gS(g) = S(g)g = 1$, hence $G(H)$, the set of grouplike elements of H, is a group.

Example 2.5.3 Let G be a group. Then the groupring kG is a Hopf algebra. The comultiplication and counit are given by

$$\Delta(g) = g \otimes g \ \text{ and } \ \varepsilon(g) = 1,$$

for all $g \in G$. The antipode is given by

$$S(g) = g^{-1}.$$

If G is a finite group, then we can consider the dual Hopf algebra $(kG)^* = Gk$. We have that

$$(kG)^* = \bigoplus_{g \in G} kv_g,$$

with $v_g : kG \to k$ the projection onto the g-component:

$$\langle v_g, h\rangle = \delta_{g,h}.$$

The v_g form a set of orthogonal idempotents in $(kG)^*$:

$$\sum_{g\in G} v_g = \varepsilon \text{ and } v_g * v_h = \delta_{g,h} v_g.$$

The comultiplication on $(kG)^*$ is given by the formula

$$\Delta(v_g) = \sum_{x\in G} v_x \otimes v_{x^{-1}g}.$$

The antipode is

$$S^*(v_g) = v_{g^{-1}}.$$

If G is a finite abelian group, then Gk is again a group ring, if the order of G is invertible in k, and if k contains enough roots of unity. Before we show this, let us recall the following elementary Lemma.

Lemma 2.5.4 *Let k be a commutative ring in which the positive integer n is not a zero-divisor. If k contains a primitive n-th root of unity η, then*

$$(1-\eta)(1-\eta^2)\cdots(1-\eta^{n-1}) = n \tag{2.12}$$

If the greatest common divisor of n and i equals 1, then $1+\eta+\eta^2+\cdots+\eta^{i-1}$ is invertible in k.

Proof. In $k[x]$, we have that

$$x^n - 1 = (x-1)(x-\eta)\cdots(x-\eta^{n-1})$$

and

$$x^{n-1} + x^{n-2} + \cdots + 1 = (x-\eta)\cdots(x-\eta^{n-1})$$

(2.12) follows after we take $x = 1$. If $(n,i) = 1$, then

$$\{1, \eta, \eta^2, \ldots, \eta^{n-1}\} = \{1, \eta^i, \eta^{2i}, \ldots, \eta^{(n-1)i}\}$$

and

$$(x-1)(x-\eta)\cdots(x-\eta^{n-1}) = (x-1)(x-\eta^i)\cdots(x-\eta^{(n-1)i})$$

and

$$\frac{x-\eta^i}{x-\eta}\frac{x-\eta^{2i}}{x-\eta^2}\cdots\frac{x-\eta^{(n-1)i}}{x-\eta^{n-1}} = 1$$

Take $x = 1$. The first factor of the left hand side is $1+\eta+\eta^2+\cdots+\eta^{i-1}$, and divides 1. $\square$

Theorem 2.5.5 *Let k be a connected commutative ring, and G a finite abelian group such that $|G|$ is invertible in k, and such that k has a primitive $\exp(G)$-th root of unity. Then we have an isomorphism*

$$kG \cong k(G^*) \cong Gk$$

Proof. Recall that $G^* = \mathrm{Hom}(G, \mathbb{G}_m(k))$. If k has enough roots of unity, then $G \cong G^*$. Consider the map

$$f: \; k(G^*) \to (kG)^*$$

defined as follows: for $\sigma^* \in G^*$, we define $f(u_{\sigma^*})$ by

$$\langle f(u_{\sigma^*}), u_\tau \rangle = \langle \sigma^*, \tau \rangle.$$

We will show that f is an isomorphism of Hopf algebras. It is clear that f is a Hopf algebra homomorphism. Indeed, it preserves multiplication, and also comultiplication, since u_{σ^*} and $f(u_{\sigma^*})$ are both grouplike elements. $f(u_{\sigma^*})$ is grouplike because it is a multiplicative map. It suffices now to show that f is bijective, in the case where $G = C_q$, the cyclic group of order q, where q is a primary number. Indeed, since G is a finite abelian group, we have

$$\begin{array}{rcl} G = C_{q_1} \times C_{q_2} \times \cdots \times C_{q_r} & ; & kG = kC_{q_1} \otimes kC_{q_2} \otimes \cdots \otimes kC_{q_r} \\ G^* = C^*_{q_1} \times C^*_{q_2} \times \cdots \times C^*_{q_r} & ; & (kG)^* = (kC_{q_1})^* \otimes (kC_{q_2})^* \otimes \cdots \otimes (kC_{q_r})^* \end{array}$$

From now on, let us assume that $G = C_q =< \sigma >$, with q a primary number. Let η be a primitive q-th root of unity in k, and define $\sigma^* \in G^*$ by $\langle \sigma^*, \sigma \rangle = \eta$. In the sequel, we will write $u = f(u_{\sigma^*}) \in (RG)^*$. It is clear that $G^* =< \sigma^* >\cong G$.
To show that f is bijective, it will be sufficient to show that $\{u^i | i = 0, 1, \ldots, q-1\}$ is a basis of the free k-module $Gk = (kG)^*$, or, equivalently, that every v_{σ^k} may be written in a unique way as a linear combination of the u^i. This comes down to showing that the equation

$$\sum_{i=0}^{q-1} \alpha_i u^i = v_{\sigma^k}$$

has a unique solution for every k. This is equivalent to showing that the linear system

$$\sum_{i=0}^{q-1} \alpha_i \langle u^i, u_{\sigma^j} \rangle = \langle v_{\sigma^k}, u_{\sigma^j} \rangle$$

or

$$\sum_{i=0}^{q-1} \alpha_i \eta^{ij} = \delta_{kj} \tag{2.13}$$

has a unique solution for every $k \in \{0, 1, \ldots, q-1\}$. The determinant D of (2.13) is a Vandermonde determinant and is equal to

$$D = \prod_{0<i<j<q} (\eta^i - \eta^j)$$

To show that D is invertible, it suffices to show that every factor of D is invertible. Dividing by the powers of η, it follows that it suffices to show that for all $i = 1, 2, \ldots, q-1$, $1 - \eta^i$ is invertible, or, equivalently, that

$$\prod_{0<i<q} (1 - \eta^i) = q$$

is invertible. q is invertible by assumption. □

Example 2.5.6 (Tensor algebra) Let M be a k-module. Recall the definition of the tensor algebra

$$T(M) = \bigoplus_{n=0}^{\infty} T^n(M),$$

with $T^0(M) = k$ and $T^{n+1}(M) = T^n(M) \otimes M$. The multiplication is the following: if $x = m_1 \otimes \cdots \otimes m_n \in T^n(M)$ and $y = h_1 \otimes \cdots \otimes h_r \in T^r(M)$, then

$$x \cdot y = m_1 \otimes \cdots \otimes m_n \otimes h_1 \otimes \cdots \otimes h_r \in T^{n+r}(M).$$

The multiplication of two arbitrary elements is then obtained by linearity. $1 \in k = T^0(M)$ is the unit element, and we have a k-linear map $i: M = T^1(M) \to T(M)$, and $i(M) = T^1(M)$ generates $T(M)$ as a k-algebra.
The tensor algebra can be defined using its universal property: if A is a k-algebra, and $f: M \to A$ is a k-linear map, then there exists a unique algebra map $\overline{f}: T(M) \to A$ such that the following diagram commutes:

$$\begin{tikzcd} M \arrow[r, "i"] \arrow[dr, "f"'] & T(M) \arrow[d, "\overline{f}"] \\ & A \end{tikzcd}$$

Another way of introducing T is the following: $T: \mathcal{M} \to \underline{\underline{Alg}}$ is a functor, and is the left adjoint of the forgetful functor $U: \underline{\underline{Alg}} \to \mathcal{M}$.
We will show that $T(M)$ is a Hopf algebra. The tensor product of $T(M)$ with itself will be denoted by $T(M)\overline{\otimes}T(M)$. Using the universal property, we can extend the k-linear map

$$i: M \to T(M)\overline{\otimes}T(M), \;\; i(m) = m\overline{\otimes}1 + 1\overline{\otimes}m$$

to a k-algebra map

$$\Delta: T(M) \to T(M)\overline{\otimes}T(M).$$

Let us show that Δ is coassociative, or

$$(\Delta\overline{\otimes}T(M))\overline{\otimes}\Delta = (T(M)\overline{\otimes}\Delta)\overline{\otimes}\Delta.$$

The maps on both sides are algebra maps, so it suffices to show that they are equal on a set of algebra generators of $T(M)$, namely M. For $m \in M$, we have

$$\begin{aligned}(\Delta\overline{\otimes}T(M))(\Delta(m)) &= (\Delta\overline{\otimes}T(M))(m\overline{\otimes}1 + 1\overline{\otimes}m) \\ &= m\overline{\otimes}1\overline{\otimes}1 + 1\overline{\otimes}m\overline{\otimes}1 + 1\overline{\otimes}1\overline{\otimes}m \\ &= (T(M)\overline{\otimes}\Delta)(m\overline{\otimes}1 + 1\overline{\otimes}m) \\ &= (T(M)\overline{\otimes}\Delta)(\Delta(m)).\end{aligned}$$

The counit $\varepsilon: T(M) \to k$ is obtained by extending the null morphism $0: M \to k$ using the universal property. Let us show that

$$(\varepsilon\overline{\otimes}T(M)) \circ \Delta = T(M).$$

The maps on both sides are algebra maps, so it suffices to show this on M. For $m \in M$, we have

$$(\varepsilon\overline{\otimes}T(M))(\Delta(m)) = \varepsilon(m)\overline{\otimes}1 + \varepsilon(1)\overline{\otimes}m = 1\overline{\otimes}m = m,$$

as needed. In a similar way, we prove that

$$(T(M)\overline{\otimes}\varepsilon) \circ \Delta = T(M).$$

We now construct the antipode. Consider the k-linear map

$$g : M \to T(M)^{\mathrm{op}}, \ \ g(m) = -m.$$

From the universal property, it follows that there exists an algebra morphism

$$S : T(M) \to T(M)^{\mathrm{op}}$$

such that $S(m) = -m$, for every $m \in T^1(M)$. For $m_1 \otimes \cdots \otimes m_n \in T^n(M)$, we have $S(m_1 \otimes \cdots \otimes m_n) = (-1)^n m_1 \otimes \cdots \otimes m_n$. For $m \in T^1(M)$, we have

$$m_{(1)} \otimes m_{(2)} = m\overline{\otimes}1 + 1\overline{\otimes}m \ \text{ and } \ \varepsilon(m) = 0,$$

hence

$$S(m_{(1)})m_{(2)} = m_{(1)}S(m_{(2)}) = \varepsilon(m)1.$$

The property for the antipode thus holds for a set of algebra generators, hence for the whole of $T(M)$, by Lemma 2.5.7.

Lemma 2.5.7 *Let H be a bialgebra, and $S : H \to H$ an algebra antimorphism. Let $a, b \in H$. If a and b satisfy the equation*

$$S(x_{(1)})x_{(2)} = x_{(1)}S(x_{(2)}) = \varepsilon(x)1,$$

then ab also satisfies this equation.

Example 2.5.8 (Symmetric algebra) Let M be a k-module. We recall the definition of the *symmetric algebra* $S(M)$. Consider the ideal I of $T(M)$ generated by elements of the form $x\otimes y - y\otimes x$, and let $S(M) = T(M)/I(M)$. The map $j = p \circ i : M \to T(M) \to S(M)$ is injective. $S(M)$ satisfies the following universal property: if A is a commutative algebra, and $f : M \to A$ is k-linear, then there exists a unique algebra map $\overline{f} : S(M) \to A$ such that $\overline{f} \circ j = f$.
S is a left adjoint of the forgetful functor from commutative k-algebras to k-modules.
We will show that $S(M) = T(M)/I$ is a Hopf algebra. It suffices to show that I is a Hopf ideal. We have to show that

$$\Delta(x) \in I\overline{\otimes}T(M) + T(M)\overline{\otimes}I, \ \ \varepsilon(x) = 0, \ \ S(x) \in I$$

for all $x \in I$. Since Δ and ε are multiplicative and S is antimultiplicative, it suffices to show this for the generators of I. Indeed, for $m, n \in M$, we have

$$\begin{aligned}
\Delta(m \otimes n - n \otimes m) &= \Delta(m)\Delta(n) - \Delta(n)\Delta(m) \\
&= (m\overline{\otimes}1 + 1\overline{\otimes}m)(n\overline{\otimes}1 + 1\overline{\otimes}n) - (n\overline{\otimes}1 + 1\overline{\otimes}n)(m\overline{\otimes}1 + 1\overline{\otimes}m) \\
&= (m \otimes n - n \otimes m)\overline{\otimes}1 + 1\overline{\otimes}(m \otimes n - n \otimes m) \in I\overline{\otimes}T(M) + T(M)\overline{\otimes}I.
\end{aligned}$$

Moreover,

$$\varepsilon(m \otimes n - n \otimes m) = \varepsilon(m)\varepsilon(n) - \varepsilon(n)\varepsilon(m) = 0,$$

and

$$S(m \otimes n - n \otimes m) = S(n)S(m) - S(m)S(n) = (-n) \otimes (-m) - (-m) \otimes (-n) \in I.$$

Observe that $S(M)$ is a commutative and cocommutative Hopf algebra.

Example 2.5.9 (Enveloping algebra of a Lie algebra) Let L be a Lie algebra. The *enveloping algebra* of the Lie algebra L is the factor algebra $U(L) = T(L)/I$, where I is the ideal generated by elements of the form $[x, y] - x \otimes y + y \otimes x$, with $x, y \in L$. We can then show that

$$\Delta([x,y]-x\otimes y+y\otimes x) = ([x,y]-x\otimes y+y\otimes x)\overline{\otimes}1 = 1\overline{\otimes}([x,y]-x\otimes y+y\otimes x) \in I\otimes T(M)+T(M)\otimes I$$

$$\varepsilon([x, y] - x \otimes y + y \otimes x) = 0$$

$$S([x, y] - x \otimes y + y \otimes x) = -([x, y] - x \otimes y + y \otimes x) \in I$$

Hence I is a Hopf ideal and $U(L)$ is a (cocommutative) Hopf algebra.

Example 2.5.10 (Sweedler's 4-dimensional Hopf algebra) Let k be a field of characteristic different from 2. Let H be generated as a k-algebra by x and c, with multiplication rules

$$c^2 = 1,\ x^2 = 0,\ xc = -cx.$$

We define a comultiplication and counit on H as follows:

$$\Delta(c) = c \otimes c,\ \ \Delta(x) = c \otimes x + x \otimes 1$$

$$\varepsilon(c) = 1,\ \ \varepsilon(x) = 0.$$

i.e. c is grouplike and x is $(c, 1)$-primitive. Then H is a bialgebra. The antipode of H is given by the formulas

$$S(c) = c,\ \ S(x) = -cx.$$

Example 2.5.11 (Taft algebra) Let $n \geq 2$, en k a field with characteristic prime to n, and with a primite n-th root of unity η. Let H be the algebra with generators c and x, and multiplication rules

$$c^n = 1,\ \ x^n = 0,\ \ xc = \lambda cx.$$

Comultiplication:

$$\Delta(c) = c \otimes c,\ \ \Delta(x) = c \otimes x + x \otimes 1$$

Counit:

$$\varepsilon(c) = 1,\ \ \varepsilon(x) = 0$$

Antipode:

$$S(c) = c^{-1},\ \ S(x) = -c^{-1}x.$$

Example 2.5.12 Let k be a commutative domain, with $2 \neq 0$. Assume that we have a factorization $2 = ab$ in k. Consider the commutative k-algebra

$$H_a = k[X]/(X^2 + aX)$$

with comultiplication and counit

$$\Delta(x) = 1 \otimes x + x \otimes 1 + bx \otimes x, \;\; \varepsilon(x) = 0$$

Observe that $u = 1 + bx$ is grouplike.

$$S(x) = x.$$

Exercise 2.5.13 Let k be a field. Classify all Hopf algebras of dimension 2.

Sketch of solution. Let H be Hopf algebra of dimension 2. Then $H = k \oplus \operatorname{Ker}\varepsilon$. Hence $\dim \operatorname{Ker}\varepsilon = 1$. Take a basis $\{x\}$ of $\operatorname{Ker}\varepsilon$. Since $\operatorname{Ker}\varepsilon$ is an ideal, $x^2 = ax$.
We can write

$$\Delta(x) = \alpha 1 \otimes 1 + \beta x \otimes 1 + \gamma 1 \otimes x + \delta x \otimes x$$

Applying the counit property, we find that

$$\alpha = 0, \;\; \beta = \gamma = 1$$

Now from $\Delta(x^2) = \Delta(x)\Delta(x) = \Delta(ax)$, it follows that

$$a\delta = -1 \;\text{ or }\; a\delta = -2$$

From $S(x_{(1)})x_{(2)} = 0$, it follows that $a\delta = -1$ is impossible, hence $a\delta = -2$.
1) $\mathrm{char} k \neq 2$. Then $a \neq 0$, and 1 and $1 - \frac{2}{a}x$ are two distinct grouplike elements of H, so $H \cong kC_2$.
2) $\mathrm{char} k = 2$. Then $a\delta = 0$.
a) $a = 0$, $\delta \neq 0$. Then 1 and $1 + \delta x$ are grouplike elements of H, so $H \cong kC_2$.
b) $a = \delta = 0$. Then $x^2 = 0$, and x is primitive:

$$\Delta(x) = 1 \otimes x + x \otimes 1$$

The antipode is given by $S(x) = x$. This Hopf algebra is selfdual.
c) $a \neq 0$, $\delta = 0$. Replacing x by x/a, we may assume that $a = 1$. Thus we have a Hopf algebra with

$$x^2 = x, \;\; \Delta(x) = 1 \otimes x + x \otimes 1, \;\; \varepsilon(x) = 0$$

This Hopf algebra is the dual of kC_2.

Chapter 3

Hopf modules and integral theory

3.1 Integrals and separability

Let A be a k-algebra. A *Casimir element* is an element $e = e^1 \otimes e^2 \in A \otimes A$ (summation implicitely understood) such that

$$ae^1 \otimes e^2 = e^1 \otimes e^2 a \tag{3.1}$$

for all $a \in A$. The k-module consisting of all Casimir elements will be denote by W_A.
A is called a *separable* if there exists $e \in W_A$ such that

$$e^1 e^2 = 1. \tag{3.2}$$

In this situation, e is called a *separability idempotent*. It is an idempotent element of the algebra $A \otimes A^{\text{op}}$. Indeed, in $A \otimes A^{\text{op}}$, we have

$$ee = (e^1 \otimes e^2) \cdot (E^1 \otimes E^2) = e^1 E^1 \otimes E^2 e^2 = E^1 \otimes E^2 e^1 e^2 = E^1 \otimes E^2 = e.$$

Here $e = E^1 \otimes E^2$ is a second copy of e.
A is called a *Frobenius algebra* if there exists $e \in W_A$ and $\nu \in A^*$ such that

$$e^1 \nu(e^2) = \nu(e^1) e^2 = 1. \tag{3.3}$$

Let A be a k-algebra. Then A^* is an A-bimodule:

$$\langle a \cdot a^* \cdot b, c \rangle = \langle a^*, bca \rangle.$$

Proposition 3.1.1 *For a k-algebra A, the following assertions are equivalent*

1. *A is Frobenius;*
2.
   a) *A is finitely generated and projective as a k-module;*
   b) *A and A^* are isomorphic as right A-modules;*
3.
   a) *A is finitely generated and projective as a k-module;*
   b) *A and A^* are isomorphic as left A-modules.*

Proof. $\underline{1) \Longrightarrow 2)}$. For all $a \in A$, we have that

$$e^1\nu(e^2a) = ae^1\nu(e^2) = a,$$

so $\{(e^1, \nu(e^2-))\}$ is a finite dual basis for A. Define

$$\phi:\ A^* \to A,\ \ \phi(a^*) = \langle a^*, e^1\rangle e^2;$$

$$\psi:\ A \to A^*,\ \ \langle \psi(a), b\rangle = \langle \nu, ab\rangle.$$

φ and ψ are right A-linear:

$$\phi(a^* \cdot a) = \langle a^*, ae^1\rangle e^2 = \langle a^*, e^1\rangle e^2 a = \phi(a^*)a;$$

$$\langle \psi(ac), b\rangle = \nu(acb) = \langle \psi(a), cb\rangle = \langle \psi(a)\cdot c, b\rangle.$$

ϕ and ψ are inverses:

$$(\phi\circ\psi)(a) = \langle \psi(a), e^1\rangle e^2 = \nu(ae^1)e^2 = \nu(e^1)e^2a = a$$

$$\begin{aligned}\langle(\psi\circ\phi)(a^*), a\rangle &= \langle \nu, \phi(a^*)a\rangle = \langle \nu, \langle a^*, e^1\rangle e^2 a)\rangle \\ &= \ \langle a^*, e^1\rangle\langle \nu, e^2a\rangle = \langle a^*, ae^1\langle \nu, e^2\rangle)\rangle = \langle a^*, a\rangle.\end{aligned}$$

$\underline{2) \Longrightarrow 1)}$. Suppose that $\phi:\ A^* \to A$ is an isomorphism in $\mathcal{M}_A$, with inverse ψ. Let $\underline{\{(e_i, e_i^*) \mid i = 1, \cdots, n\}}$ be a finite dual basis of A. Let $\nu = \psi(1)$, and $y_i = \phi(e_i^*)$. Then $e_i^* = \psi(y_i) = \psi(1)\cdot y_i = \nu\cdot y_i$. For all $a \in A$, we have

$$a = \sum_i e_i\langle e_i^*, a\rangle = \sum_i e_i\langle \nu, y_ia\rangle.$$

Taking $a = 1$, we obtain that

$$\sum_i e_i\langle \nu, y_i\rangle = 1.$$

Since A is finitely generated and projective, we have an isomorphism

$$i:\ A\otimes A^* \to \mathrm{End}_k(A),\ \ i(a\otimes a^*)(b) = \langle a^*, b\rangle a.$$

The inverse of i is given by the formula

$$i^{-1}(f) = \sum_i f(e_i)\otimes e_i^*.$$

Now consider the isomorphism

$$\Phi = i\circ(A\otimes\psi):\ A\otimes A \to \mathrm{End}_k(A).$$

Φ and Φ^{-1} are described by the following formulas:

$$\Phi(a\otimes b)(c) = a\nu(bc)\ \ ;\ \ \Phi^{-1}(f) = \sum_i f(e_i)\otimes y_i.$$

For all $a, b \in A$, we have

$$a \otimes b = (\Phi^{-1} \circ \Phi)(a \otimes b) = \sum_i a\nu(be_i) \otimes y_i = \sum_i a \otimes \nu(be_i)y_i.$$

Taking $a = b = 1$, we find

$$1 \otimes 1 = 1 \otimes \sum_i \nu(e_i)y_i,$$

and it follows that $1 = \sum_i \nu(e_i)y_i$. We are done if we can show that $e = \sum_i e_i \otimes y_i$ is a Casimir element. We compute that

$$\begin{aligned}
\Phi(\sum_i ae_i \otimes y_i)(b) &= \sum_i ae_i\nu(y_ib) = ab; \\
\Phi(\sum_i e_i \otimes y_ia)(b) &= \sum_i e_i\nu(y_iab) = \sum_i ae_i\nu(y_ib) = ab.
\end{aligned}$$

It follows that $\Phi(\sum_i ae_i \otimes y_i) = \Phi(\sum_i e_i \otimes y_ia)$, and $\sum_i ae_i \otimes y_i = \sum_i e_i \otimes y_ia$, since Φ is injective.
$\underline{1) \Longleftrightarrow 3)}$ is proved in a similar way. $\square$

Integrals can be used as tools to discuss when a Hopf algebra is separable or Frobenius.
$t \in H$ is called a *left* (resp. *right*) *integral* in H if

$$ht = \varepsilon(h)t \quad \text{resp.} \quad th = \varepsilon(h)t$$

for all $h \in H$. $\int_H^l$ (resp. $\int_H^r$) denote the k-modules consisting respectively of left and right integrals in H. In a similar way, we introduce left and right integral in H^* (or *on* H). These are functionals $\varphi \in H^*$ that have to verify respectively

$$h^* * \varphi = \langle h^*, 1\rangle\varphi \quad \text{resp.} \quad \varphi * h^* = \langle h^*, 1\rangle\varphi$$

for all $h^* \in H^*$. The k-modules consisting of left and right integral in H^* are denoted by $\int_{H^*}^l$ and $\int_{H^*}^r$.

Proposition 3.1.2 *Let H be a Hopf algebra. We have the following maps*

$$p: W_H \to \int_H^l \quad ; \quad p(e) = e^1\varepsilon(e^2)$$

$$p': W_H \to \int_H^r \quad ; \quad p'(e) = \varepsilon(e^1)e^2$$

$$i: \int_H^l \to W_H \quad ; \quad i(t) = t_{(1)} \otimes S(t_{(2)})$$

$$i': \int_H^r \to W_H \quad ; \quad i'(t) = S(t_{(1)}) \otimes t_{(2)}$$

satisfying

$$(p \circ i)(t) = t \quad ; \quad (p' \circ i')(t) = t$$

for every left (resp. right) integral t.

Proof. We will show that $i(t) \in W_H$ if t is a left integral, and leave all the other assertions to the reader.

$$\begin{aligned} ht_{(1)} \otimes S(t_{(2)}) &= h_{(1)}t_{(1)} \otimes S(t_{(2)})S(h_{(2)})h_{(3)} \\ &= (h_{(1)}t)_{(1)} \otimes S((h_{(1)}t)_{(2)})h_{(2)} \\ &= (\varepsilon(h_{(1)})t)_{(1)} \otimes S((\varepsilon(h_{(1)})t)_{(2)})h_{(2)} \\ &= t_{(1)} \otimes S(t_{(2)})h \end{aligned}$$

□

Corollary 3.1.3 *A Hopf algebra H is separable if and only if there exists a (left or right) integral $t \in H$ such that $\varepsilon(t) = 1$.*

Proof. If t is a left integral with $\varepsilon(t) = 1$, then $e = i(t) \in W_H$ satisfies $\sum e^1 e^2 = \sum t_{(1)}S(t_{(2)}) = \varepsilon(t) = 1$. The converse is similar: if $\sum e^1 e^2 = 1$, then $\varepsilon(p(e)) = \sum \varepsilon(e^1 e^2) = 1$. □

Proposition 3.1.4 *A separable algebra A over a field k is semisimple.*

Proof. Let $e = \sum e^1 \otimes e^2 \in A \otimes A$ be a separability idempotent and N an A-submodule of a right A-module M. As k is a field, the inclusion $i: N \to M$ splits in the category of k-vector spaces. Let $f: M \to N$ be a k-linear map such that $f(n) = n$, for all $n \in N$. Then

$$\tilde{f}: M \to N, \quad \tilde{f}(m) = \sum f(me^1)e^2$$

is a right A-module map that splits the inclusion i. Thus N is an A-direct factor of M, and it follows that M is completely reducible. This shows that A is semisimple. □

Corollary 3.1.5 *A finite dimensional Hopf algebra H over a field k is semisimple if and only if there exists a (left or right) integral $t \in H$ such that $\varepsilon(t) = 1$.*

Proof. One direction follows immediately from Corollary 3.1.3 and Proposition 3.1.4. Conversely, if H is semisimple, then $H = I \oplus \operatorname{Ker}(\varepsilon)$ for some left ideal I of H. We claim that $I \subset \int_H^l$: For $z \in I$, and $h \in H$, we have $h - \varepsilon(h) \in \operatorname{Ker}(\varepsilon)$, so $(h - \varepsilon(h))z \in I \cap \operatorname{Ker}\varepsilon = \{0\}$, hence $hz = \varepsilon(h)z$, and z is a left integral. Choose $z \neq 0$ in I (this is possible since I is one-dimensional). $\varepsilon(z) \neq 0$ since $z \notin \operatorname{Ker}(\varepsilon)$, and $t = z/\varepsilon(z)$ is a left integral with $\varepsilon(t) = 1$. □

3.2 Hopf modules and the fundamental theorem

A *Hopf module* is a k-module together with a right H-action and a right H-coaction such that

$$\rho(mh) = m_{[0]}h_{(1)} \otimes m_{[1]}h_{(2)}, \tag{3.4}$$

for all $m \in M$ and $h \in H$. A morphism between two Hopf modules is a k-linear map that is H-linear and H-colinear. $\mathcal{M}_H^H$ is the category of Hopf modules and morphisms between Hopf modules.

Let $N \in \mathcal{M}$. Then $N \otimes H$, with H-action and H-coaction induced by the multiplication and comultiplication on H, namely

$$(n \otimes h)k = n \otimes hk \ ; \ \rho(n \otimes h) = n \otimes h_{(1)} \otimes h_{(2)},$$

is a Hopf module. This construction is functorial, so we have a functor

$$F = - \otimes H : \ \mathcal{M} \to \mathcal{M}_H^H.$$

If M is a Hopf module, then

$$M^{\mathrm{co}H} = \{m \in M \mid \rho(m) = m \otimes 1\}$$

is a k-module. This construction is also functorial, so we have a functor

$$G = (-)^{\mathrm{co}H} : \ \mathcal{M}_H^H \to \mathcal{M}.$$

Proposition 3.2.1 (F, G) *is a pair of adjoint functors.*

Proof. The unit and the counit of the adjunction are defined as follows. For $M \in \mathcal{M}_H^H$, let

$$\varepsilon_M : \ FG(M) = M^{\mathrm{co}H} \otimes H \to M, \ \ \varepsilon_M(m \otimes h) = mh.$$

It is obvious that ε_M is right H-linear; it follows from (3.4) that ε_M is right H-colinear. For $N \in \mathcal{M}$, let

$$\eta_N : \ N \to (N \otimes H)^{\mathrm{co}H}, \ \ \eta_N(n) = n \otimes 1.$$

An easy verification shows that

$$\varepsilon_{N \otimes H} \circ \eta_N \otimes H = N \otimes H;$$

$$\varepsilon_M^{\mathrm{co}H} \circ \eta_{M^{\mathrm{co}H}} = M^{\mathrm{co}H},$$

for all $M \in \mathcal{M}_H^H$ and $N \in \mathcal{M}$, and this proves that (F, G) is an adjoint pair of functors. □

Theorem 3.2.2 (Fundamental Theorem for Hopf modules) (F, G) *is a pair of inverse equivalences. In other words, η and ε are natural isomorphisms.*

Proof. Let M be a Hopf module. For any $m \in M$, $m_{[0]}S(m_{[1]}) \in M^{\mathrm{co}H}$, since

$$\begin{aligned}
\rho(m_{[0]}S(m_{[1]})) &= m_{[0][0]}S(m_{[1]})_{(1)} \otimes m_{[0][1]}S(m_{[1]})_{(2)} \\
&= m_{[0]}S(m_{[3]}) \otimes m_{[1]}S(m_{[2]}) = m_{[0]}S(m_{[2]}) \otimes \varepsilon(m_{[1]})1_H \\
&= m_{[0]}S(m_{[1]}) \otimes 1
\end{aligned}$$

Now define $\alpha : \ M \to M^{\mathrm{co}H} \otimes H$ as follows:

$$\alpha(m) = m_{[0]}S(m_{[1]}) \otimes m_{[2]}$$

α is the inverse of ε_M: for all $m \in M$, we have

$$(\varepsilon \circ \alpha)(m) = m_{[0]}S(m_{[1]})m_{[2]} = m,$$

and, for $m' \in M^{\mathrm{co}H}$,

$$\alpha(\varepsilon_M(m' \otimes h)) = m'_{[0]}h_{(1)}S(m'_{[1]}h_{(2)}) \otimes m'_{[2]}h_{(3)} = m'h_{(1)}S(h_{(2)}) \otimes h_{(3)} = m' \otimes h.$$

Now take $N \in \mathcal{M}$, and $q = \sum_i n_i \otimes h_i \in (N \otimes H)^{\mathrm{co}H}$. We then have that

$$\rho(q) = \sum_i n_i \otimes h_{i(1)} \otimes h_{i(2)} = q \otimes 1 = \sum_i n_i \otimes h_i \otimes 1.$$

We apply $N \otimes \varepsilon \otimes H$ to both sides of this equation. We then find that

$$q = \sum_i n_i \otimes h_i = \sum_i n_i \otimes \varepsilon(h_i) \otimes 1.$$

Now define

$$\beta : (N \otimes H)^{\mathrm{co}H} \to N, \ \ \beta(\sum_i n_i \otimes h_i) = \sum_i n_i \otimes \varepsilon(h_i).$$

β and η_N are inverses. For all $n \in N$, we have

$$(\beta \circ \eta_N)(n) = \beta(n \otimes 1) = n,$$

and for all $q = \sum_i n_i \otimes h_i \in (N \otimes H)^{\mathrm{co}H}$, we have

$$(\eta_N \circ \beta)(q) = \sum_i n_i \otimes \varepsilon(h_i) \otimes 1 = q.$$

□

An immediate application is the following:

Proposition 3.2.3 *Let H be a finitely generated projective Hopf algebra. H^* is a left H^*-module (by multiplication), and therefore a right H-comodule. It is also a right H-module, we let*

$$\langle h^* \leftharpoonup h, k\rangle = \langle h^*, kS(h)\rangle$$

for all $h^* \in H^*$, and $h, k \in H$. With these structure maps, H^* is a right-right Hopf module, and $(H^*)^{\mathrm{co}H} \cong \int_{H^*}^l$. Consequently we have an isomorphism

$$\alpha : \int_{H^*}^l \otimes H \to H^* \quad ; \quad \alpha(\varphi \otimes h) = \varphi \leftharpoonup h \tag{3.5}$$

of right-right Hopf modules. In particular, it follows that $\int_{H^*}^l$ is a rank one projective k-module. Similar results hold for the right integral space.

Proof. Remark that the right H-action on H^* is not the usual one. Recall that the usual H-bimodule structure on H^* is given by

$$\langle h \cdot h^* \cdot k, l\rangle = \langle h^*, klh\rangle$$

an we see immediately that

$$h^* \leftharpoonup h = S(h) \cdot h^*$$

Also observe that the right H-coaction on H^* can be rewritten in terms of a dual basis $\{(h_i, h_i^*) \mid i = 1, \cdots, n\}$ of H:

$$\rho(h^*) = \sum_i h_i^* * h^* \otimes h_i$$

The only thing we have to check is the Hopf compatibility relation for H^*, i.e.

$$\rho(h^* \leftharpoonup h) = h^*_{[0]} \leftharpoonup h_{(1)} \otimes h^*_{[1]} h_{(2)}$$

for all $h \in H$, $h^* \in H^*$. It suffices to prove that

$$\langle (h^* \leftharpoonup h)_{[0]}, k \rangle (h^* \leftharpoonup h)_{[1]} = \langle h^*_{[0]} \leftharpoonup h_{(1)}, k \rangle h^*_{[1]} h_{(2)} \tag{3.6}$$

for all $k \in H$. We first compute the left hand side:

$$\rho(h^* \leftharpoonup h) = \sum_i (h_i^* * S(h) \cdot h^*) \otimes h_i$$

so

$$\begin{aligned} \langle (h^* \leftharpoonup h)_{[0]}, k \rangle (h^* \leftharpoonup h)_{[1]} &= \sum_i \langle h_i^* * S(h) \cdot h^*, k \rangle h_i \\ &= \sum_i \langle h_i^*, k_{(1)} \rangle \langle h^*, k_{(2)} S(h) \rangle h_i = \langle h^*, k_{(2)} S(h) \rangle k_{(1)} \end{aligned}$$

The right hand side of (3.6) equals

$$\begin{aligned} \sum_i \langle h_i^* * h^*, kS(h_{(1)}) \rangle h_i h_{(2)} &= \langle h_i^*, k_{(1)} S(h_{(2)}) \rangle \langle h^*, k_{(2)} S(h_{(1)}) \rangle h_i h_{(3)} \\ &= \langle h^*, k_{(2)} S(h_{(1)}) \rangle k_{(1)} S(h_{(2)}) h_{(3)} = \langle h^*, k_{(2)} S(h_{(1)}) \rangle k_{(1)} \end{aligned}$$

as needed. □

As an application of Proposition 3.2.3, we can prove that the antipode of a finitely generated projective Hopf algebra is always bijective.

Proposition 3.2.4 *The antipode of a finitely generated projective Hopf algebra is bijective.*

Proof. We know from Proposition 3.2.3 that $J = \int_{H^*}^l$ is projective of rank one. This implies that we have an isomorphism

$$J^* \otimes J \to k \quad ; \quad p \otimes \varphi \mapsto p(\varphi)$$

Let $\sum_l p_l \otimes \varphi_l$ be the inverse image of 1:

$$\sum_l p_l(\varphi_l) = 1$$

The isomorphism α of Proposition 3.2.3 induces another isomorphism

$$\widetilde{\alpha}:\ H \to J^* \otimes H^* \quad ; \quad \widetilde{\alpha}(h) = \sum_l p_l \otimes \alpha(\varphi_l \otimes h) = \sum_l p_l \otimes S(h) \cdot \varphi_l$$

If $S(h) = 0$, then it follows from the above formula that $\widetilde{\alpha}(h) = 0$, hence $h = 0$, since $\widetilde{\alpha}$ is injective. Hence S is injective.
The fact that S is surjective follows from a local global argument. Let $Q = \mathrm{Coker}\,(S)$. For every prime ideal p of k, $\mathrm{Coker}\,(S_p) = Q_p$, since localization at a prime ideal is an exact functor. Now H_p/pH_p is a finite dimensional Hopf algebra over the field k_p/pk_p, with antipode induced by S_p, the antipode of the localized k_p-Hopf algebra H_p. The antipode of H_p/pH_p is injective, hence bijective, by counting dimensions. Nakayama's Lemma implies that S_p is surjective, for all $p \in \mathrm{Spec}\,(k)$, and it follows that S is bijective. □

Here is another application of Proposition 3.2.3:

Proposition 3.2.5 *Let H be a finitely generated projective Hopf algebra. Then there exist $\varphi_j \in \int_{H^*}^l$ and $h_j \in H$ such that*

$$\sum_j \langle \varphi_j, h_j \rangle = 1$$

and $t_j \in \int_H^l$ and $h_j^* \in H^*$ such that

$$\sum_j \langle h_j^*, t_j \rangle = 1$$

Proof. Take $\alpha^{-1}(\varepsilon) = \sum_j \varphi_j \otimes S^{-1}(h_j)$ (the antipode is bijective by Proposition 3.2.4). Then

$$1_k = \langle \varepsilon_H, 1_H \rangle = \sum_j \langle \varphi_j \leftharpoonup S^{-1}(h_j), 1_H \rangle = \sum_j \langle \varphi_j, h_j \rangle$$

the second statement follows after we apply the first one with H replaced by H^*. □

The main result is now the following:

Theorem 3.2.6 *For a Hopf algebra H, the following assertions are equivalent:*
1) H/k is Frobenius;
2) H is finitely generated and projective, and H^*/k is Frobenius;
3) H is finitely generated and projective, and $\int_H^l$ is free of rank one;
4) H is finitely generated and projective, and $\int_H^r$ is free of rank one;
5) H is finitely generated and projective, and $\int_{H^*}^l$ is free of rank one;
6) H is finitely generated and projective, and $\int_{H^*}^r$ is free of rank one.

Proof. $\underline{1) \Rightarrow 3)}$. There exist $\nu \in H^*$ and $e \in W_A$ such that $\nu(e^1)e^2 = e^1\nu(e^2) = 1$. Take $t = p(e) = \varepsilon(e^2)e^1 \in \int_H^l$. We claim that $\int_H^l$ is free with basis $\{t\}$. Take another left integral $u \in \int_H^l$. Then

$$\begin{aligned} u &= ue^1\nu(e^2) = e^1\nu(e^2u) = e^1\nu(\varepsilon(e^2)u) \\ &= \varepsilon(e^2)e^1\nu(u) = \nu(u)t \end{aligned}$$

and it follows that the map $k \to \int_H^l$ sending $x \in k$ to xt is surjective. This map is also injective: if

$$xt = x\varepsilon(e^2)e^1 = 0$$

then

$$0 = \nu(x\varepsilon(e^2)e^1) = \nu(e^1)x\varepsilon(e^2) = x\varepsilon(e^2\nu(e^1)) = x$$

$\underline{5) \Rightarrow 2)}$ and $\underline{5) \Rightarrow 1)}$. Assume that $\int_{H^*}^l = k\varphi$, with φ a left integral, and consider the Hopf module isomorphism

$$\alpha : \; k\varphi \otimes H \to H^*$$

from Proposition 3.2.3. We first consider the map

$$\Theta : \; H \to H^* \quad ; \quad \Theta(h) = \alpha(\varphi \otimes h) = S(h) \cdot \varphi$$

α and Θ are right H-colinear, hence left H^*-linear. Θ is therefore an isomorphism of left H^*-modules, and it follows that H^* is Frobenius.
A slightly more subtle argument shows that H is Frobenius: we consider the map

$$\phi = \Theta \circ S^{-1} : \; H \to H^*, \; \text{ i.e. } \phi(h) = h \cdot \varphi$$

We know from Proposition 3.2.4 that S is bijective, so ϕ is well-defined, and is a bijection. ϕ is left H-linear since

$$\phi(kh) = (kh) \cdot \varphi = k \cdot (h \cdot \varphi) = k \cdot \phi(h)$$

All the other implications follow after we apply the above implications $\underline{1) \Rightarrow 3)}$ an $\underline{5) \Rightarrow 1)}$ with H replaced by H^* (H is finitely generated and projective) or by H^{op} (the Frobenius property is symmetric). □

Assume that H is Frobenius and that we know a generator φ for $\int_{H^*}^l$. We want to answer the following questions.

1. How do we find a generator t for $\int_H^l$?
2. Can we explicitly describe a Frobenius system for H?
3. What is the inverse of the isomorphism $\phi : \; H \to H^*$?

Before answering this question, we make two observations that are valid in any Hopf algebra.

Lemma 3.2.7 *Let H be a Hopf algebra with invertible algebra $\varphi \in \int_{H^*}^l$ and $t \in \int_H^l$. For every $h \in H$, we have that*

$$\langle \varphi, h_{(2)} \rangle S^{-1}(h_{(1)}) = \langle \varphi, h \rangle 1. \tag{3.7}$$

Moreover, $t_{(2)} \otimes S^{-1}(t_{(1)}) \in W_H$.

Proof. If $\varphi \in \int_{H^*}^l$, then $\langle \varphi, h_{(2)} \rangle h_{(1)} = \langle \varphi, h \rangle 1$, for all $h \in H$, hence

$$\langle \varphi, h_{(2)} \rangle S^{-1}(h_{(1)}) = \langle \varphi, h \rangle S^{-1}(1) = \langle \varphi, h \rangle 1.$$

From Proposition 3.1.2 we know that $t_{(1)} \otimes S(t_{(2)}) \in W_H$. Applying this property to the Hopf algebra $H^{\rm cop}$, and keeping in mind that the antipode of $H^{\rm cop}$ is S^{-1}, we find that $t_{(2)} \otimes S^{-1}(t_{(1)}) \in W_H$. This can also be proved directly: for all $h \in H$, we have

$$\begin{aligned}
& ht_{(2)} \otimes S^{-1}(t_{(1)}) = h_{(3)}t_{(2)} \otimes S^{-1}(t_{(1)})S^{-1}(h_{(2)})h_{(1)} \\
= \;& (h_{(2)}t)_{(2)} \otimes S^{-1}(h_{(2)}t)_{(1)})h_{(1)} \\
= \;& \langle \varepsilon, h\rangle t_{(2)} \otimes S^{-1}(t_{(1)})h_{(1)} \\
= \;& t_{(2)} \otimes S^{-1}(t_{(1)})h.
\end{aligned}$$

□

Recall from the proof of $5) \Rightarrow 1)$ in Theorem 3.2.6 that we have an isomorphism of left H-modules

$$\phi: \; H \to H^* \;\; ; \;\; \phi(h) = h \cdot \varphi$$

Let $\phi^{-1}(\varepsilon) = t$, this means that $\phi(t) = t \cdot \varphi = \varepsilon$, or

$$\varphi(ht) = \varepsilon(h)$$

for all $h \in H$. In particular, we have that

$$\langle \varphi, t\rangle = 1. \tag{3.8}$$

We claim that t is a free generator for $\int_H^l$.
First, t is a left integral, since

$$\begin{aligned}
\langle \phi(ht), k\rangle &= \langle (ht) \cdot \varphi, k\rangle = \langle t \cdot \varphi, kh\rangle \\
&= \varepsilon(kh) = \varepsilon(k)\varepsilon(h) = \varepsilon(h)\langle \phi(t), k\rangle
\end{aligned}$$

for all $h, k \in H$, implying that $\phi(ht) = \varepsilon(h)\phi(t)$, and $ht = \varepsilon(h)t$, and t is an integral.
If u is another left integral, then

$$\begin{aligned}
\langle \phi(u), h\rangle &= \langle u \cdot \varphi, h\rangle = \langle \varphi, hu\rangle = \varepsilon(h)\langle \varphi, u\rangle = \langle \varphi, ht\rangle\langle \varphi, u\rangle \\
&= \langle \varphi, h\varphi(u)t\rangle = \langle (\varphi(u)t) \cdot \varphi, h\rangle = \langle \phi(\varphi(u)t), h\rangle
\end{aligned}$$

implying $\phi(u) = \phi(\varphi(u)t)$ and $u = \varphi(u)t$.
Assume that $xt = 0$, for some $x \in k$. Then $\phi^{-1}(x\varepsilon) = 0$, hence $x\varepsilon = 0$, and $x = 0$. This proves that t is a free generator for $\int_H^l$.
In the proof of $5) \Rightarrow 2)$ of Theorem 3.2.6, we constructed a left H^*-linear isomorphism $\Theta : H \to H^*$. We write down this map, but for the Hopf algebra H^* instead of H. Since t is a free generator of $\int_H^l$, we find a left H-linear isomorphism

$$\Lambda: \; H^* \to H, \;\; \Lambda(h^*) = S^*(h^*) \bullet t = \langle h^*, S(t_{(2)})\rangle t_{(1)}.$$

Now take this isomorphism, applied to the Hopf algebra $H^{\rm cop}$. Since the antipode of $H^{\rm cop}$ is S^{-1} and the left H-action on H and H^* only involves the algebra action on H, we find a left H-linear isomorphism

$$\Omega: \; H^* \to H, \;\; \Omega(h^*) = \langle h^*, S^{-1}(t_{(1)})\rangle t_{(2)}.$$

We now show that ϕ is left inverse of Ω. Indeed, for all $h \in H$ and $h^* \in H^*$, we have

$$\begin{aligned}
\langle(\phi\circ\Omega)(h^*),h\rangle = \langle\Omega(h^*)\cdot\varphi,h\rangle & \\
= \quad & \langle\varphi,ht_{(2)}\rangle\langle h^*,S^{-1}(t_{(1)})\rangle \\
\stackrel{*}{=} \quad & \langle\varphi,t_{(2)}\rangle\langle h^*,S^{-1}(t_{(1)})h\rangle \\
\stackrel{(3.7)}{=} \quad & \langle h^*,\langle\varphi,t\rangle h\rangle \\
\stackrel{(3.7)}{=} \quad & \langle h^*,h\rangle.
\end{aligned}$$

Since ϕ and Ω are isomorphisms, ϕ is also a right inverse of Ω, and we conclude that $\Omega = \phi^{-1}$. In particular,

$$1 = (\Omega\circ\phi)(1) = \Omega(\varphi) = \langle\varphi,S^{-1}(t_{(1)})\rangle t_{(2)}. \tag{3.9}$$

It now follows that $(t_{(2)}\otimes S^{-1}(t_{(1)}),\varphi)$ is a Frobenius system for H. Indeed, we have seen in Lemma 3.2.7 that $t_{(2)}\otimes S^{-1}(t_{(1)}) \in W_H$. From (3.7-3.8), it follows that $\langle\varphi,t_{(2)}\rangle S^{-1}(t_{(1)}) = 1$, and finally we have (3.9). We summarize our results as follows.

Theorem 3.2.8 *Let H be a Frobenius Hopf algebra, and assume that φ is a free generator of $\int_{H^*}^l$. Then*

$$\phi:\ H\to H^*\ \ ;\ \ \phi(h) = h\cdot\varphi$$

is a left H-linear isomorphism. $t = \phi^{-1}(\varepsilon)$ is a free generator for $\int_H^l$, and

$$\phi^{-1}:\ H^*\to H,\ \ \phi^{-1}(h^*) = \langle h^*,S^{-1}(t_{(1)})\rangle t_{(2)}.$$

Moreover $\langle\varphi,t\rangle = 1$, and $(t_{(2)}\otimes S^{-1}(t_{(1)}),\varphi)$ is a Frobenius system for H.

Theorem 3.2.9 *A Hopf algebra H (with bijective antipode) is Frobenius if and only if there exist $t\in\int_H^l$ and $\varphi\in\int_{H^*}^l$ such that $\langle\varphi,t\rangle = 1$.*

Proof. One application already follows from Theorem 3.2.8. Conversely, assume that there exist $t\in\int_H^l$ and $\varphi\in\int_{H^*}^l$ such that $\langle\varphi,t\rangle = 1$. It follows from (3.7) that

$$\langle\varphi,t_{(2)}\rangle S^{-1}(t_{(1)}) = 1. \tag{3.10}$$

We will show that $S^{-1}(t)$ is a free generator of $\int_H^r$. Then the proof will be finished after we apply Theorem 3.2.6. For $v\in\int_H^r$, we have

$$\begin{aligned}
v \quad \stackrel{(3.10)}{=} \quad & \langle\varphi,t_{(2)}\rangle S^{-1}(t_{(1)})v \stackrel{(*)}{=} \langle\varphi,vt_{(2)}\rangle S^{-1}(t_{(1)}) \\
\stackrel{(**)}{=} \quad & \langle\varphi,\varepsilon(t_{(2)})v\rangle S^{-1}(t_{(1)}) = \langle\varphi,v\rangle S^{-1}(t).
\end{aligned}$$

$(*)$: we used Lemma 3.2.7; $(**)$: t is a right integral. This shows that the map $k\to\int_H^r$ mapping x to $xS^{-1}(t)$ is surjective. Let us show that it is also injective. If $xS^{-1}(t) = 0$, then

$$\begin{aligned}
0 \quad &= \quad S(xS^{-1}(t)) = xt = x\langle\varepsilon,S^{-1}(t_{(1)})\rangle t_{(2)}; \\
0 \quad &= \quad x\langle\varepsilon,S^{-1}(t_{(1)})\rangle\langle\varphi,t_{(2)}\rangle \stackrel{(3.10)}{=} x\langle\varepsilon,1\rangle = x.
\end{aligned}$$

□

Remark 3.2.10 1) It follows from the preceding Theorem that any finite dimensional Hopf algebra over a field k is Frobenius.
2) In Proposition 3.1.2, we have seen that we have a map $p:\ W_A\to\int_H^l$, with a right inverse i. The map p is not an isomorphism. To see this, take a Frobenius Hopf algebra H (e.g. any finite dimensional Hopf algebra over a field).
First we observe that, if H is finitely generated and projective, we have an isomorphism

$$W_A\cong \mathrm{Hom}_H(H^*,H).$$

Actually, this isomorphism is used implicitly in the proof of Proposition 3.1.1. To see this, we define first

$$\varphi:\ W_A\to \mathrm{Hom}_H(H^*,H),\ \ \varphi(e^1\otimes e^2)(h^*)=\langle h^*,e_1\rangle e_2.$$

Let us check that $\varphi(e^1\otimes e^2)$ is right H-linear:

$$\varphi(e^1\otimes e^2)(h^*\cdot h)=\langle h^*,he_1\rangle e_2=\langle h^*,e_1\rangle e_2h=\varphi(e^1\otimes e^2)(h^*)h.$$

Next we define

$$\psi:\ \mathrm{Hom}_H(H^*,H)\to W_A,\ \ \psi(f)=\sum_i h_i\to f(h_i^*),$$

where $\{(h_i,h_i^*)\mid i=1,\cdots,n\}$ is a finite dual basis of H. Let us show that $\psi(f)\in W_A$. Since

$$\sum_i h_i\langle h_i^*,hk\rangle=hk=\sum_i hh_i\langle h_i^*,k\rangle,$$

for all $h,k\in H$, we have, for all $h\in H$:

$$\sum_i h_i\otimes h_i^*\cdot h=\sum_i hh_i\otimes h_i^*,$$

hence

$$\sum_i hh_i\otimes f(h_i^*)=\sum_i h_i\otimes f(h_i^*\cdot h)=\sum_i h_i\otimes f(h_i)h.$$

Now ψ and φ are inverses:

$$(\psi\circ\varphi)(e^1\otimes e_2)=\sum_i h_i\otimes\langle h_i^*,e^1\rangle e_2=e^1\otimes e_2;$$

$$((\varphi\circ\psi)(f))(h^*)=\varphi(\sum_i h_i\otimes f(h_i^*))(h^*)=\sum_i\langle h^*,h_i\rangle f(h_i^*)=f(h^*).$$

Using the fact that $H^*\cong H$ as right H-modules (see Proposition 3.1.1), we now find

$$W_A\cong\mathrm{Hom}_H(H^*,H)\cong\mathrm{Hom}_H(H,H)\cong H$$

and the rank of W_1 equals the rank of H as a k-module.
As we have seen, the rank of $\int_H^l$ is one.

3) Assume that H is Frobenius, and that ψ is a free generator of $\int_{H^*}^r$. Then we have a right H-linear isomorphism

$$\Psi: \ H \to H^*, \ \ \Psi(h) = \psi \cdot h.$$

$\Psi^{-1}(\varepsilon) = u$ is then a free generator of $\int_H^r$, and $\langle \psi, u \rangle = 1$. Now let φ and t as in Theorems 3.2.8 and 3.2.9. Then take $u = S(t)$ and $\psi = \varphi \circ S^{-1}$. It is clear that u and ψ are right integrals, and that $\langle \psi, u \rangle = 1$. We also have a commutative diagram

$$\begin{tikzcd}
H \arrow[r, "\phi"] \arrow[d, "S"'] & H^* \arrow[d, "(S^*)^{-1}"] \\
H \arrow[r, "\Psi"] & H^*
\end{tikzcd}$$

We can easily compute Ψ^{-1}:

$$\Psi^{-1}(h^*) = (S \circ \phi^{-1})(h^* \circ S) = \langle h^*, t_{(1)} \rangle S(t_{(2)}) = \langle h^*, S^{-1}(u_{(2)}) \rangle u_{(1)}.$$

$(t_{(1)} \otimes S(t_{(2)}) = S^{-1}(u_{(2)}) \otimes u_{(1)}, \varphi \circ S^{-1} = \psi)$ is a Frobenius system for H.

We generalize the definition of integrals as follows: take $\alpha \in \mathrm{Alg}(H, k)$ and $g \in G(H)$, and define

$$\int_\alpha^l = \{t \in H \mid ht = \alpha(h)t, \text{ for all } h \in H\}$$

$$\int_\alpha^r = \{t \in H \mid th = \alpha(h)t, \text{ for all } h \in H\}$$

$$\int_g^l = \{\varphi \in H^* \mid h^* * \varphi = \langle h^*, g \rangle \varphi, \text{ for all } h^* \in H^*\}$$

$$\int_g^r = \{\varphi \in H^* \mid \varphi * h^* = \langle h^*, g \rangle \varphi, \text{ for all } h^* \in H^*\}$$

Of course we recover the previous definitions if $\alpha = \varepsilon$ and $g = 1$. We have the following generalization of Theorem 3.2.6.

Proposition 3.2.11 *Let H be a Hopf algebra, and assume that H/k is Frobenius. Then for all $\alpha \in \mathrm{Alg}(H, k)$ and $g \in G(H)$, the integral spaces $\int_\alpha^l$, $\int_\alpha^l$, $\int_g^l$ and $\int_g^r$ are free k-modules of rank one.*

Proof. Take $t = \alpha(e^1)e^2$. Arguments almost identical to the ones used in the proof of $1) \Rightarrow 3)$ in Theorem 3.2.6 prove that t is a free generator of $\int_\alpha^l$. The statements for the other integral spaces follow by duality arguments. $\square$

Now assume that H is Frobenius, and write $\int_H^l = kt$. It is easy to prove that $th \in \int_H^l$, for all $h \in H$. Indeed,

$$k(th) = (kt)h = \varepsilon(k)th$$

for all $k \in H$. It follows that there exists a unique $\alpha(h) \in k$ such that

$$th = \alpha(h)t$$

$\alpha: H \to k$ is multiplicative, so we can restate our observation by saying that $t \in \int_\alpha^r$. We call α the *distinguished element* of H^*. If $\alpha = \varepsilon$, then we say that H is *unimodular*.

Proposition 3.2.12 *Let H be a Frobenius Hopf algebra, and $\alpha \in H^*$ the distinguished element. Then $\int_\alpha^r = \int_H^l$, and H is unimodular if and only if*

$$\int_H^r = \int_H^l$$

Proof. We know from Proposition 3.2.11 that $\int_\alpha^r = kt'$ is free of rank one. For all $h \in H$, we have that $ht' \in \int_\alpha^r$, hence we find a unique multiplicative map $\beta: H \to k$ such that

$$ht' = \beta(h)t'$$

for all $h \in H$. Now we have that $t = xt'$ for some $x \in k$, since $t \in \int_\alpha^r$. Thus

$$\varepsilon(h)t = ht = xht' = x\beta(h)t' = \beta(h)t$$

for all $h \in H$. This implies that $\beta = \varepsilon$, since t is a free generator of $\int_H^l$. It follows that $t' \in \int_H^l$, proving the first statement.
If $\alpha = \varepsilon$, then it follows that $\int_H^r = \int_H^l$. Conversely, if $\int_H^r = \int_H^l$, then $t \in \int_H^r$, and this means that the distinguished element is equal to ε. $\square$

Chapter 4

Galois Theory

4.1 Algebras and coalgebras in monoidal categories

Let $\mathcal{C} = (\mathcal{C}, \otimes, k)$ be a monoidal category. An *algebra* in $\mathcal{C}$ is a triple $A = (A, m, \eta)$, where $A \in \mathcal{C}$ and $m : A \otimes A \to A$ and $\eta : k \to A$ are morphisms in $\mathcal{C}$ such that the following diagrams commute:

$$\begin{tikzcd} A \otimes A \otimes A \arrow[r, "m\otimes A"] \arrow[d, "A\otimes m"'] & A \otimes A \arrow[d, "m"] \\ A \otimes A \arrow[r, "m"] & A \end{tikzcd} \qquad \begin{tikzcd} k \otimes A \arrow[r, "\eta\otimes A"] \arrow[dr, "l_A"'] & A \otimes A \arrow[d, "m"] & A \otimes k \arrow[l, "A\otimes\eta"'] \arrow[dl, "r_A"] \\ & A & \end{tikzcd}$$

A *coalgebra* in $\mathcal{C}$ is an algebra in the opposite category $\mathcal{C}^{\mathrm{op}}$.

Example 4.1.1 Let k be a commutative ring. An algebra in $\mathcal{M}_k$ is a k-algebra, and a coalgebra in $\mathcal{M}_k$ is a k-coalgebra.

Example 4.1.2 An algebra in <u>Sets</u> is a monoid. Every set X has a unique structure of coalgebra in <u>Sets</u>. The comultiplication $\Delta : X \to X \times X$ is the diagonal map $\Delta(x) = (x, x)$, and the counit is the unique map $\varepsilon : X \to \{*\}$.
It is easy to see that (X, Δ, ε) is a coalgebra. Conversely, let (X, Δ, ε) is a coalgebra. Then ε is the unique map $X \to \{*\}$. Take $x \in X$, and assume that $\Delta(x) = (a, b)$. From the left counit property, it follows that

$$x = ((\varepsilon \times X) \circ \Delta)(x) = b.$$

In a similar way, we find that $x = a$, hence $\Delta(x) = (x, x)$.

A (co)algebra in $\mathcal{C}$ is also called a (co)monoid in $\mathcal{C}$

Example 4.1.3 Let A be a ring with unit. The category of bimodules ${}_A\mathcal{M}_A$ is a monoidal category; the tensor is given by the tensor product $\otimes_A$, and the unit object A. An algebra in ${}_A\mathcal{M}_A$ is called an A-ring, and a coalgebra in ${}_A\mathcal{M}_A$ is called an A-coring. Corings will be studied in Section 4.2.

Example 4.1.4 Let H be a bialgebra. We know that ${}_H\mathcal{M}$ is a monoidal category. An algebra A in ${}_H\mathcal{M}$ is called a left H-module algebra. Then A is a left H-module, and a k-algebra such that the multiplication and unit maps are left H-linear, which comes down to

$$h \cdot (ab) = (h_{(1)} \cdot a)(h_{(2)} \cdot b) \ ; \ h \cdot 1_A = \varepsilon(h)1_A.$$

A coalgebra in in ${}_H\mathcal{M}$ is called a left H-module coalgebra.
For a monoid G, a left kG-module algebra is a left G-module algebra in the classical sense, that is, it is an algebra with a left G-action such that

$$\sigma \cdot (ab) = (\sigma \cdot a)(\sigma \cdot b) \ ; \ \sigma \cdot 1_A = 1_A.$$

Of course, we can also consider right H-module (co)algebras.

Example 4.1.5 Let H be a bialgebra, and consider the category of right H-comodules $\mathcal{M}^H$. It is also a monoidal category, with tensor $\otimes_k$ and unit object k. For $M, N \in \mathcal{M}^H$, $M \otimes N$ is again a right H-comodule, with right H-coaction

$$\rho(m \otimes n) = m_{[0]} \otimes n_{[0]} \otimes m_{[1]}n_{[1]}.$$

$k \in \mathcal{M}^H$ with right H-coaction $\rho(1_k) = 1_k \otimes 1_A$.
An algebra A in $\mathcal{M}^H$ is called a right H-comodule algebra. Then A is a right H-comodule, and a k-algebra, such that the multiplication and unit maps are right H-colinear, which comes down to

$$\rho(ab) = a_{[0]}b_{[0]} \otimes a_{[1]}b_{[1]} \ ; \ \rho(1_A) = 1_A \otimes 1_H.$$

For a monoid G, a kG-comodule algebra A is a G-graded ring A, that is,

$$A = \bigoplus_{\sigma \in G} A_\sigma,$$

with

$$A_\sigma A_\tau \subset A_{\sigma\tau} \ ; \ 1_A \in A_e.$$

A coalgebra in $\mathcal{M}^H$ is called a right H-comodule coalgebra. Of course, we can also consider right H-comodule (co)algebras.

4.2 Corings

Let A be a ring with unit. An A-coring is a triple $\mathbb{C} = (\mathbb{C}, \Delta_\mathbb{C}, \varepsilon_\mathbb{C})$, where

- $\mathbb{C}$ is an A-bimodule;
- $\Delta_\mathbb{C} : \mathbb{C} \to \mathbb{C} \otimes_A \mathbb{C}$ is an A-bimodule map;
- $\varepsilon_\mathbb{C} : \mathbb{C} \to A$ is an A-bimodule map

such that

$$(\Delta_{\mathbb{C}} \otimes_A I_{\mathbb{C}}) \circ \Delta_{\mathbb{C}} = (I_{\mathbb{C}} \otimes_A \Delta_{\mathbb{C}}) \circ \Delta_{\mathbb{C}}, \tag{4.1}$$

and

$$(I_{\mathbb{C}} \otimes_A \varepsilon_{\mathbb{C}}) \circ \Delta_{\mathbb{C}} = (\varepsilon_{\mathbb{C}} \otimes_A I_{\mathbb{C}}) \circ \Delta_{\mathbb{C}} = I_{\mathbb{C}}. \tag{4.2}$$

Sometimes corings are considered as coalgebras over noncommutative rings. This point of view is not entirely correct: a coalgebra over a commutative ring k is a k-coring, but not conversely: it could be that the left and and right action of k on the coring are different.

The Sweedler-Heyneman notation is also used for a coring $\mathbb{C}$, namely

$$\Delta_{\mathbb{C}}(c) = c_{(1)} \otimes_A c_{(2)},$$

where the summation is implicitely understood. (4.2) can then be written as

$$\varepsilon_{\mathbb{C}}(c_{(1)})c_{(2)} = c_{(1)}\varepsilon_{\mathbb{C}}(c_{(2)}) = c.$$

This formula looks like the corresponding formula for usual coalgebras. Notice however that the order matters in the above formula, since $\varepsilon_{\mathbb{C}}$ now takes values in A which is noncommutative in general. Even worse, the expression $c_{(2)}\varepsilon_{\mathbb{C}}(c_{(1)})$ makes no sense at all, since we have no well-defined switch map $\mathbb{C} \otimes_A \mathbb{C} \to \mathbb{C} \otimes_A \mathbb{C}$.
A morphism between two corings $\mathbb{C}$ and $\mathcal{D}$ is an A-bimodule map $f:\ \mathbb{C} \to \mathcal{D}$ such that

$$\Delta_{\mathcal{D}}(f(c)) = f(c_{(1)}) \otimes_A f(c_{(2)}) \ \text{ and } \ \varepsilon_{\mathcal{D}}(f(c)) = \varepsilon_{\mathbb{C}}(c),$$

for all $c \in \mathbb{C}$. A right $\mathbb{C}$-comodule $M = (M, \rho)$ consists of a right A-module M together with a right A-linear map $\rho:\ M \to M \otimes_A \mathbb{C}$ such that:

$$(\rho \otimes_A I_{\mathbb{C}}) \circ \rho = (I_M \otimes_A \Delta_{\mathbb{C}}) \circ \rho, \tag{4.3}$$

and

$$(I_M \otimes_A \varepsilon_{\mathbb{C}}) \circ \rho = I_M. \tag{4.4}$$

We then say that $\mathbb{C}$ coacts from the right on M. Left $\mathbb{C}$-comodules and $\mathbb{C}$-bicomodules can be defined in a similar way. We use the Sweedler-Heyneman notation also for comodules:

$$\rho(m) = m_{[0]} \otimes_A m_{[1]}.$$

(4.4) then takes the form $m_{[0]}\varepsilon_{\mathbb{C}}(m_{[1]}) = m$. A right A-linear map $f:\ M \to N$ between two right $\mathbb{C}$-comodules M and N is called right $\mathbb{C}$-colinear if $\rho(f(m)) = f(m_{[0]}) \otimes m_{[1]}$, for all $m \in M$.

Example 4.2.1 Let $i:\ B \to A$ be a ring morphism; then $\mathcal{D} = A \otimes_B A$ is an A-coring. We define

$$\Delta_{\mathcal{D}}:\ \mathcal{D} \to \mathcal{D} \otimes_A \mathcal{D} \cong A \otimes_B A \otimes_B A$$

and

$$\varepsilon_{\mathcal{D}}:\ \mathcal{D} = A \otimes_B A \to A$$

by

$$\Delta_{\mathcal{D}}(a \otimes_B b) = (a \otimes_B 1_A) \otimes_A (1_A \otimes_B b) \cong a \otimes_B 1_A \otimes_B b$$

and

$$\varepsilon_{\mathcal{D}}(a \otimes_B b) = ab.$$

Then $\mathcal{D} = (\mathcal{D}, \Delta_{\mathcal{D}}, \varepsilon_{\mathcal{D}})$ is an A-coring. It is called the *Sweedler canonical coring* associated to the ring morphism i.

Example 4.2.2 Let k be a commutative ring, G a finite group, and A a G-module algebra. Let $\mathcal{C} = \oplus_{\sigma \in G} A v_\sigma$ be the left free A-module with basis indexed by G, and let $p_\sigma : \mathcal{C} \to A$ be the projection onto the free component Av_σ. We make $\mathcal{C}$ into a right A-module by putting

$$v_\sigma a = \sigma(a) v_\sigma.$$

A comultiplication and counit on $\mathcal{C}$ are defined by putting

$$\Delta_{\mathcal{C}}(av_\sigma) = \sum_{\tau \in G} av_\tau \otimes_A v_{\tau^{-1}\sigma} \text{ and } \varepsilon_{\mathcal{C}} = p_e,$$

where e is the unit element of G. It is straightforward to verify that $\mathcal{C}$ is an A-coring. Notice that, in the case where A is commutative, we have an example of an A-coring, which is not an A-coalgebra, since the left and right A-action on $\mathcal{C}$ do not coincide.
Let us give a description of the right $\mathcal{C}$-comodules. Assume that $M = (M, \rho)$ is a right $\mathcal{C}$-comodule. For every $m \in M$ and $\sigma \in G$, let $\overline{\sigma}(m) = m_\sigma = I_M \otimes_A p_\sigma)(\rho(m))$. Then we have

$$\rho(m) = \sum_{\sigma \in G} m_\sigma \otimes_A v_\sigma.$$

$\overline{e}$ is the identity, since $m = (I_M \otimes_A \varepsilon_{\mathcal{C}}) \circ \rho(m) = m_e$. Using the coassociativity of the comultiplication, we find

$$\sum_{\sigma \in G} \rho(m_\sigma) \otimes v_\sigma = \sum_{\sigma, \tau \in G} m_\sigma \otimes_A v_\tau \otimes_A v_{\tau^{-1}\sigma} = \sum_{\rho, \tau \in G} m_{\tau\rho} \otimes_A v_\tau \otimes_A v_\rho,$$

hence $\rho(m_\sigma) = \sum_{\tau \in G} m_{\tau\sigma} \otimes_A v_\tau$, and $\overline{\tau}(\overline{\sigma}(m)) = m_{\tau\sigma} = \overline{\tau\sigma}(m)$, so G acts as a group of k-automorphisms on M. Moreover, since ρ is right A-linear, we have that

$$\rho(ma) = \sum_{\sigma \in G} \overline{\sigma}(ma) \otimes_A v_\sigma = \sum_{\sigma \in G} \overline{\sigma}(m) \otimes_A v_\sigma a = \sum_{\sigma \in G} \overline{\sigma}(m)\sigma(a) \otimes_A v_\sigma$$

so $\overline{\sigma}$ is A-semilinear: $\overline{\sigma}(ma) = \overline{\sigma}(m)\sigma(a)$, for all $m \in M$ and $a \in A$. Conversely, if G acts as a group of right A-semilinear automorphims on M, then the formula

$$\rho(m) = \sum_{\sigma \in G} \overline{\sigma}(m) \otimes_A v_\sigma$$

defines a right $\mathcal{C}$-comodule structure on $\mathcal{M}$.

Example 4.2.3 Now let k be a commutative ring, G an arbitrary group, and A a G-graded k-algebra. Again let $\mathcal{C}$ be the free left A-module with basis indexed by G:

$$\mathcal{C} = \oplus_{\sigma\in G} A u_\sigma$$

Right A-action, comultiplication and counit are now defined by

$$u_\sigma a = \sum_{\tau\in G} a_\tau u_{\sigma\tau} \ ; \ \Delta_{\mathcal{C}}(u_\sigma) = u_\sigma \otimes_A u_\sigma \ ; \ \varepsilon_{\mathcal{C}}(u_\sigma) = 1.$$

$\mathcal{C}$ is an A-coring; let $M = (M, \rho)$ be a right A-comodule, and let $M_\sigma = \{m \in M \mid \rho(m) = m \otimes_A u_\sigma\}$. It is then clear that $M_\sigma \cap M_\tau = \{0\}$ if $\sigma \neq \tau$. For any $m \in M$, we can write in a unique way:

$$\rho(m) = \sum_{\sigma\in G} m_\sigma \otimes_A u_\sigma.$$

Using the coassociativity, we find that $m_\sigma \in M_\sigma$, and using the counit property, we find that $m = \sum_\sigma m_\sigma$. So $M = \oplus_{\sigma\in G} M_\sigma$. Finally, if $m \in M_\sigma$ and $a \in A_\tau$, then it follows from the right A-linearity of ρ that

$$\rho(ma) = (m \otimes_A u_\sigma)a = ma \otimes_A u_{\sigma\tau},$$

so $ma \in M_{\sigma\tau}$, and $M_\sigma A_\tau \subset M_{\sigma\tau}$, and M is a right G-graded A-module. Conversely, every right G-graded A-module can be made into a right $\mathcal{C}$-comodule.

Example 4.2.4 Let H be a bialgebra over a commutative ring k, and A a right H-comodule algebra. Now take $\mathcal{C} = A \otimes H$, with A-bimodule structure

$$a'(b \otimes h)a = a'ba_{[0]} \otimes ha_{[1]}.$$

Now identify $(A \otimes H) \otimes_A (A \otimes H) \cong A \otimes H \otimes H$, and define the comultiplication and counit on $\mathcal{C}$, by putting $\Delta_{\mathcal{C}} = I_A \otimes \Delta_H$ and $\varepsilon_{\mathcal{C}} = I_A \otimes \varepsilon_H$. Then $\mathcal{C}$ is an A-coring. The category $\mathcal{M}^{\mathcal{C}}$ is isomorphic to the category of relative Hopf modules. These are k-modules M with a right A-action and a right H-coaction ρ, such that

$$\rho(ma) = m_{[0]}a_{[0]} \otimes_A m_{[1]}a_{[1]}$$

for all $m \in M$ and $a \in A$.

Duality

If $\mathcal{C}$ is an A-coring, then its left dual ${}^*\mathcal{C} = {}_A\mathrm{Hom}(\mathcal{C}, A)$ is a ring, with (associative) multiplication given by the formula

$$f\#g = g \circ (I_{\mathcal{C}} \otimes_A f) \circ \Delta_{\mathcal{C}} \ \text{ or } \ (f\#g)(c) = g(c_{(1)}f(c_{(2)})), \tag{4.5}$$

for all left A-linear $f, g : \ \mathcal{C} \to A$ and $c \in \mathcal{C}$. The unit is $\varepsilon_{\mathcal{C}}$. We have a ring homomorphism $i : \ A \to {}^*\mathcal{C}, \ \ i(a)(c) = \varepsilon_{\mathcal{C}}(c)a$. We easily compute that

$$(i(a)\#f)(c) = f(ca) \ \text{ and } \ (f\#i(a))(c) = f(c)a, \tag{4.6}$$

for all $f \in {}^*\mathcal{C}$, $a \in A$ and $c \in \mathcal{C}$. We have a functor $F: \mathcal{M}^{\mathcal{C}} \to \mathcal{M}_{^*\mathcal{C}}$, where $F(M) = M$ as a right A-module, with right ${}^*\mathcal{C}$-action given by $m \cdot f = m_{[0]} f(m_{[1]})$, for all $m \in M$, $f \in {}^*\mathcal{C}$. If $\mathcal{C}$ is finitely generated and projective as a left A-module, then F is an isomorphism of categories: given a right ${}^*\mathcal{C}$-action on M, we recover the right $\mathcal{C}$-coaction by putting $\rho(m) = \sum_j (m\cdot f_j) \otimes_A c_j$, where $\{(c_j, f_j) \mid j = 1, \cdots, n\}$ is a finite dual basis of $\mathcal{C}$ as a left A-module. ${}^*\mathcal{C}$ is a right A-module, by (4.6): $(f \cdot a)(c) = f(c)a$, and we can consider the double dual $({}^*\mathcal{C})^* = \mathrm{Hom}_A({}^*\mathcal{C}, A)$. We have a canonical morphism $i: \mathcal{C} \to ({}^*\mathcal{C})^*$, $i(c)(f) = f(c)$, and we call $\mathcal{C}$ reflexive (as a left A-module) if i is an isomorphism. If $\mathcal{C}$ is finitely generated projective as a left A-module, then $\mathcal{C}$ is reflexive. For any $\varphi \in ({}^*\mathcal{C})^*$, we then have that $\varphi = i(\sum_j \varphi(f_j)c_j)$.

Grouplike elements

Let $\mathcal{C}$ be an A-coring, and suppose that $\mathcal{C}$ coacts on A. Then we have a map $\rho: A \to A \otimes_A \mathcal{C} \cong \mathcal{C}$. The fact that ρ is right A-linear implies that ρ is completely determined by $\rho(1_A) = x$: $\rho(a) = xa$. The coassociativity of the coaction yields that $\Delta_{\mathcal{C}}(x) = x \otimes_A x$ and the counit property gives us that $\varepsilon_{\mathcal{C}}(x) = 1_A$. We say that x is a *grouplike element* of $\mathcal{C}$ and we denote $G(\mathcal{C})$ for the set of all grouplike elements of $\mathcal{C}$. If $x \in G(\mathcal{C})$ is grouplike, then the associated $\mathcal{C}$-coaction on A is given by $\rho(a) = xa$.

If $x \in G(\mathcal{C})$, then we call $(\mathcal{C}, x)$ a *coring with a fixed grouplike element*. For $M \in \mathcal{M}^{\mathcal{C}}$, we call

$$M^{\mathrm{co}\mathcal{C}} = \{m \in M \mid \rho(m) = m \otimes_A x\}$$

the submodule of coinvariants of M; note that this definition depends on the choice of the grouplike element. Also observe that

$$A^{\mathrm{co}\mathcal{C}} = \{b \in A \mid bx = xb\}$$

is a subring of A.

An adjoint pair of functors

Let $i: B \to A$ be a ring morphism. i factorizes through $A^{\mathrm{co}\mathcal{C}}$ if and only if

$$x \in G(\mathcal{C})^B = \{x \in G(\mathcal{C}) \mid xb = bx, \text{ for all } b \in B\}.$$

We then have a pair of adjoint functors (F, G) between the categories $\mathcal{M}_B$ and $\mathcal{M}^{\mathcal{C}}$. For $N \in \mathcal{M}_B$ and $M \in \mathcal{M}^{\mathcal{C}}$,

$$F(N) = N \otimes_B A \text{ and } G(M) = M^{\mathrm{co}\mathcal{C}}.$$

The unit and counit of the adjunction are

$$\nu_N: N \to (N \otimes_B A)^{\mathrm{co}\mathcal{C}},\ \nu_N(n) = n \otimes_B 1;$$

$$\zeta_M: M^{\mathrm{co}\mathcal{C}} \otimes_B A \to M,\ \zeta_M(m \otimes_B a) = ma.$$

We want to discuss when (F, G) is a category equivalence. We will do this first in the case where $\mathcal{C}$ is the Sweedler canonical coring, and $x = 1 \otimes_B 1$.

4.3 Faithfully flat descent

Let $i : B \to A$ be a ring morphism. The problem of descent theory is the following: suppose that we have a right A-module M. When do we have a right B-module N such that $N = M \otimes_B A$?

Let $\mathcal{D} = A \otimes_B A$ be the associated Sweedler canonical coring. Let $M = (M, \rho)$ be a right $\mathcal{D}$-comodule. We will identify $M \otimes_A \mathcal{D} \cong M \otimes_B A$ using the natural isomorphism. The coassociativity and the counit property then take the form

$$\rho(m_{[0]}) \otimes m_{[1]} = m_{[0]} \otimes_B 1_A \otimes_B m_{[1]} \ \text{ and } \ m_{[0]} m_{[1]} = m. \tag{4.7}$$

$1_A \otimes_B 1_A$ is a grouplike element of $\mathcal{D}$. As we have seen at the end of Section 4.2, we havea pair of adjoint functors, between $\mathcal{M}_B$ and $\mathcal{M}^{\mathcal{D}}$, which we will denote by (K, R). The unit and counit of the adjunction will be denoted by η and ε. K is called the comparison functor. If (K, R) is an equivalence of categories, then the "descent problem" is solved: $M \in \mathcal{M}_A$ is isomorphic to some $N \otimes_B A$ if and only if we can define a right $\mathcal{D}$-coaction on M.

Proposition 4.3.1 *If $A \in {}_B\mathcal{M}$ is flat, then R is fully faithful, that is, ε_M is bijective, for all $M \in \mathcal{M}^{\mathcal{D}}$.*

Proof. Consider the map

$$i_M : M \to M \otimes_B A, \ \ i_M(m) = m \otimes_B 1.$$

Then $M^{\mathrm{co}\mathcal{D}} = \{m \in M \mid \rho(m) = m \otimes_B 1\}$ fits into the exact sequence

$$0 \longrightarrow M^{\mathrm{co}\mathcal{D}} \xrightarrow{\ \ j\ \ } M \underset{i_M}{\overset{\rho}{\rightrightarrows}} M \otimes_B A$$

Since $A \in {}_B\mathcal{M}$ is flat, we have an exact sequence

$$0 \longrightarrow M^{\mathrm{co}\mathcal{D}} \otimes_B A \xrightarrow{\ j \otimes_B A\ } M \otimes_B A \underset{i_M \otimes_B A}{\overset{\rho \otimes_B A}{\rightrightarrows}} M \otimes_B A \otimes_B A$$

Now ρ corestricts to $\rho : M \to M^{\mathrm{co}\mathcal{D}} \otimes_B A$. Indeed, for all $m \in M$, we have, using (4.7)

$$(\rho \otimes_B A)(m_{[0]} \otimes_B m_{[1]}) = m_{[0]} \otimes 1 \otimes_B m_{[1]} = (i_M \otimes_B A)(m_{[0]} \otimes_B m_{[1]}).$$

This corestriction of ρ is the inverse of ε_M: $(\varepsilon_M \circ \rho)(m) = m$ by the counit property (4.7), and for all $m \in M^{\mathrm{co}\mathcal{D}}$ and $a \in A$, we have that

$$(\rho \circ \varepsilon_M)(m \otimes_B a) = \rho(ma) = m_{[0]} \otimes_B m_{[1]} a = m \otimes_B a.$$

□

Proposition 4.3.2 *Assume that $A \in {}_B\mathcal{M}$ is flat. Then the following assertions are equivalent.*

1. *$A \in {}_B\mathcal{M}$ is faithfully flat;*

2. (K, R) *is a pair of inverse equivalences.*

Proof. $\underline{1) \Longrightarrow 2)}$. We know form Proposition 4.3.1 that R is fully faithful, so we only need to show that K is fully faithful, that is, η_N is bijective for all $N \in {}_B\mathcal{M}$. We will show that $i_N : N \to N \otimes_B A$ is injective. Since $A \in {}_B\mathcal{M}$ is faithfully flat, it suffices to show that $i_N \otimes_B A : N \otimes_B A \to N \otimes_B A \otimes_B A$ is injective. Assume that

$$0 = (i_N \otimes_B A)(\sum_i n_i \otimes_B a_i) = \sum_i n_i \otimes_B 1 \otimes_B a_i.$$

Multiply the second and third tensor factor. It then follows that $\sum_i n_i \otimes_B a_i = 0$. We have a commutative diagram

$$\begin{tikzcd} N \arrow[r, "\eta_N"] \arrow[dr, "i_N"'] & (N \otimes_B A)^{\mathrm{co}\mathcal{D}} \arrow[d, "\subset"] \\ & N \otimes_B A \end{tikzcd}$$

and it follows that η_N is injective. In order to prove that η_N is surjective, take $a = \sum_i n_i \otimes_B a_i \in (N \otimes_B A)^{\mathrm{co}\mathcal{D}}$. Then

$$\rho(q) = \sum_i n_i \otimes_B a_i \otimes_B 1 = \sum_i n_i \otimes_B 1 \otimes_B a_i. \tag{4.8}$$

Now let $P = (N \otimes_B A)/i(N)$, and let $\pi : N \otimes_B A \to P$ be the canonical projection. Apply $\pi \otimes_B A$ to (4.8):

$$\pi(q) \otimes_B 1 = \sum_i \pi(n_i \otimes_B 1) \otimes_B a_i = 0 \in P \otimes_B A.$$

Since i_P is injective, it follows that $\pi(q) = 0$, so $q \in \mathrm{Im}\,(i_N)$.

$\underline{2) \Longrightarrow 1)}$. If $A \in {}_B\mathcal{M}$ is flat, then $\mathcal{D} = A \otimes_B A \in {}_A\mathcal{M}$ is flat, and $\mathcal{M}^{\mathcal{D}}$ is an abelian category, in such a way that the forgetful functor $\mathcal{M}^{\mathcal{D}} \to \mathcal{M}_A$ is exact. The proof is similar to the proof of Corollary 2.4.10. Now let

$$N' \xrightarrow{f} N \xrightarrow{g} N''$$

be a sequence in ${}_B\mathcal{M}$ and assume that

$$N' \otimes_B A \xrightarrow{f \otimes_B A} N \otimes_B A \xrightarrow{g \otimes_B A} N'' \otimes_B A$$

is exact in $\mathcal{M}_A$. Then this sequence is also exact in $\mathcal{M}^{\mathcal{D}}$, since the forgetful functor is faithfully exact. Now (K, R) is a pair of inverse equivalences. In particular, R is a right adjoint of K, so R preserves kernels. R is also a left adjoint of K, so R also preserves cokernels (see prref3.3.3). So R is exact, and

$$0 \longrightarrow N' \xrightarrow{f} N \xrightarrow{g} N'' \longrightarrow 0$$

is exact in $\mathcal{M}_B$. $\square$

Proposition 4.3.3 *Let (F, G) be a pair of adjoint functors between the categories $\mathcal{C}$ and $\mathcal{D}$. Then F preserves cokernels and G preserves kernels.*

Proof. One of the equivalent characterizations of adjoint functors is the following: for $C \in \mathcal{C}$ and $D \in \mathcal{D}$, we have isomorphisms

$$\alpha_{C,D} : \operatorname{Hom}_{\mathcal{D}}(F(C), D) \to \operatorname{Hom}_{\mathcal{C}}(C, G(D)),$$

natural in C and D. The naturality in C and D means the following: for $f : C \to C'$ in $\mathcal{C}$, and $g : F(C) \to D$, $h : D \to D'$ in $\mathcal{D}$, we have

$$\alpha_{C',D'}(h \circ g \circ F(f)) = G(h) \circ \alpha_{C,D}(g) \circ f. \tag{4.9}$$

Take $f : C \to C'$ in $\mathcal{C}$, with cokernel $k : C' \to K$. We will show that the cokernel of $F(f)$ is $F(k)$. It is clear that $F(k) \circ F(f) = F(k \circ f) = 0$.
Assume that $g : F(C') \to D$ is such that $g \circ F(f) = 0$:

$$\begin{tikzcd}
F(C) \arrow[r, "F(f)"] & F(C') \arrow[r, "F(k)"] \arrow[dr, "g"'] & F(K) \\
& & D
\end{tikzcd}$$

Then $0 = \alpha_{C,D}(g \circ F(f)) \stackrel{(4.9)}{=} \alpha_{C',D}(g) \circ f$. Since k is the cokernel of f, there exists a unique $l : K \to G(D)$ such that the diagram

$$\begin{tikzcd}
C \arrow[r, "f"] & C' \arrow[r, "k"] \arrow[dr, "\alpha_{C',D}(g)"'] & K \arrow[d, "\exists! l"] \\
& & G(D)
\end{tikzcd}$$

commutes. Now

$$g = \alpha^{-1}_{C',D}(\alpha_{C',D}(g)) = \alpha^{-1}_{C',D}(l \circ k) \stackrel{(4.9)}{=} \alpha^{-1}_{K,D}(l) \circ F(k),$$

so $\alpha^{-1}_{K,D}(l)$ makes the following diagram commute:

$$\begin{tikzcd}
F(C) \arrow[r, "F(f)"] & F(C') \arrow[r, "F(k)"] \arrow[dr, "g"'] & F(K) \arrow[d, "\alpha^{-1}_{K,D}(l)"] \\
& & D
\end{tikzcd}$$

We still have to show that this is the unique map that makes the diagram commutative. Assume that $m : F(k) \to D$ is such that $g = m \circ F(k)$. Then

$$l \circ k = \alpha_{C',D}(g) \stackrel{(4.9)}{=} \alpha_{K,D}(m) \circ k.$$

From the uniqueness of l, it follows that $l = \alpha_{K,D}(m)$, and $\alpha^{-1}_{K,D}(l) = m$. $\square$

The commutative case

Now we consider the special case where A and B are commutative. In this situation, an alternative description of the category $\mathcal{M}^{\mathcal{D}}$ can be given. For $M \in \mathcal{M}_A$, we consider $A \otimes_B M$ and $M \otimes_B M$ as right $A \otimes_B A$-modules.

Lemma 4.3.4 *We have an isomorphism* $\alpha : \operatorname{Hom}_A(M, M \otimes_B A) \to \operatorname{Hom}_{A\otimes_B A}(A \otimes_B M, M \otimes_B A)$.

Proof. For $\rho : M \to M \otimes_B A$, $\alpha(\rho) = g$ is given by

$$g(a \otimes_B m) = m_{[0]}a \otimes_B m_{[1]},$$

where we denote $\rho(m) = m_{[0]} \otimes m_{[1]}$. Conversely, given $g \in \operatorname{Hom}_{A\otimes_B A}(A \otimes_B M, M \otimes_B A)$, we let $\alpha^{-1}(g) = \rho$ given by $\rho(m) = g(1 \otimes_B m)$. □

For $g \in \operatorname{Hom}_{A\otimes_B A}(A \otimes_B M, M \otimes_B A)$, we can consider the three following morphisms of $A \otimes_B \otimes_B A$-modules:

$$g_1 = A \otimes_B g : A \otimes_B A \otimes_B M \to A \otimes_B M \otimes_B A$$
$$g_3 = g \otimes_B A : A \otimes_B M \otimes_B A \to M \otimes_B A \otimes_B A$$
$$g_2 : A \otimes_B A \otimes_B M \to M \otimes_B A \otimes_B A$$

g_2 is given by the formula

$$g(a \otimes_B a' \otimes_B m) = m_{[0]}a \otimes_B a' \otimes_B m_{[1]}$$

Lemma 4.3.5 *Take* $\rho \in \operatorname{Hom}_A(M, M \otimes_B A)$*, and let* $g = \alpha(\rho)$.

1. *ρ is coassociative if and only if $g_2 = g_3 \circ g_1$;*
2. *ρ has the counit property if and only if $(\psi_M \circ g)(1 \otimes_B m) = m$, for all $m \in M$. $\psi_M : M \otimes_B A \to M$ is the right A-action on M.*

Proof. 1) We easily compute that

$$g_2(1 \otimes_B 1 \otimes_B m) = m_{[0]} \otimes_B 1 \otimes_B m_{[1]}$$
$$(g_3 \circ g_1)(m) = g_3(1 \otimes_B m_{[0]} \otimes_B m_{[1]}) = \rho(m_{[0]}) \otimes_B m_{[1]}$$

and the first assertion follows.
2) is obvious. □

If the conditions of Lemma 4.3.5 are satisfied, then (M, g) is called a descent datum. Let $\underline{\mathrm{Desc}}(A/B)$ be the category with descent data as objects. A morphism $(M, g) \to (M', g')$ consists of a morphism $f : M \to M'$ in $\mathcal{M}_A$ such that the diagram

$$\begin{tikzcd} A \otimes_B M \arrow[r, "g"] \arrow[d, "A\otimes_B f"'] & M \otimes_B A \arrow[d, "f\otimes_B A"] \\ A \otimes_B M' \arrow[r, "g'"] & M' \otimes_B A \end{tikzcd}$$

commutes.

Proposition 4.3.6 *The categories* $\underline{\mathrm{Desc}}(A/B)$ *and* $\mathcal{M}^{\mathcal{D}}$ *are isomorphic.*

Proof. $(M,\rho) \in \mathcal{M}^{\mathcal{D}}$ is sent to $(M,\alpha(\rho)) \in \mathcal{M}^{\mathcal{D}}$. If $f: M \to M'$ is a morphism in $\mathcal{M}^{\mathcal{D}}$, then it is also a morphism in $\underline{\mathrm{Desc}}(A/B)$. □

Proposition 4.3.7 *Assume that* $g \in \mathrm{Hom}_{A\otimes_B A}(A \otimes_B M, M \otimes_B A)$ *satisfies the condition* $g_2 = g_3 \circ g_1$. *Then condition 2) of Lemma 4.3.5 is satisfied if and only if* g *is a bijection.*

Proof. $\underline{\Longrightarrow}$. The inverse of g is given by the formula

$$g^{-1}(m \otimes_B a) = m_{[1]} \otimes m_{[0]}a.$$

Indeed:

$$\begin{aligned}
(g^{-1} \circ g)(a \otimes_B m) = g^{-1}(m_{[0]}a \otimes_B m_{[1]}) &= m_{[0][1]}a \otimes_B m_{[0][0]}m_{[1]} \\
&= a \otimes_B m_{[0]}m_{[1]} \\
&= a \otimes_B m \\
(g \circ g^{-1})(m \otimes_B a) = g(m_{[1]} \otimes_B m_{[0]}a) &= m_{[0][0]}m_{[1]} \otimes_B m_{[0][1]}a \\
&= m_{[0]}m_{[1]} \otimes_B a \\
&= m \otimes_B a
\end{aligned}$$

$\underline{\Longleftarrow}$. We compute that

$$\begin{aligned}
g(1 \otimes_B m_{[0]}m_{[1]}) &= m_{[0][0]} \otimes_B m_{[0][1]}m_{[1]} \\
&= m_{[0]} \otimes_B m_{[1]} = g(1 \otimes_B m).
\end{aligned}$$

Since g is bijective, it follows that

$$1 \otimes_B m_{[0]}m_{[1]} = 1 \otimes_B m$$

and $m_{[0]}m_{[1]} = m$. □

If (M,g) is a decent datum, then the descended module $M^{\mathrm{co}\mathcal{D}}$ is given by the formula

$$M^{\mathrm{co}\mathcal{D}} = \{m \in M \mid g(1 \otimes_B m) = m \otimes_B 1\}.$$

4.4 Galois corings

Let $(\mathcal{C},x)$ be an A-coring with a fixed grouplike element x, and let $i: B \to A^{\mathrm{co}\mathcal{C}}$ be a ring morphism. Then we have a morphism of corings

$$\mathrm{can}: \mathcal{D} = A \otimes_B A \to \mathcal{C}, \ \mathrm{can}(a \otimes_B a') = axa'.$$

Recall from Section 4.2 that we have a pair of adjoint functors (F,G) between $\mathcal{M}_B$ and $\mathcal{M}^{\mathcal{C}}$.

Proposition 4.4.1 *1) If F is fully faithful, then $i:\ B\to A^{\mathrm{co}\mathcal{C}}$ is an isomorphism;*
2) if G is fully faithful, then can *is an isomorphism.*

Proof. 1) $\nu_B=i$ is an isomorphism.
2) $(\mathcal{C},\Delta)$ is a right $\mathcal{C}$-comodule. The map

$$f:\ A\to\mathcal{C}^{\mathrm{co}\mathcal{C}},\ \ f(ax)$$

is an (A,B)-bimodule isomorphism; the inverse g is the restriction of ε to $\mathcal{C}^{\mathrm{co}\mathcal{C}}$. Indeed, $(g\circ f)(a)=\varepsilon(ax)=a\varepsilon(x)=a$. If $c\in\mathcal{C}^{\mathrm{co}\mathcal{C}}$, then $\Delta(c)=c\otimes_A x$, so $\varepsilon(c)x=\varepsilon(c_{(1)})c_{(2)}=c$. Then we find that

$$(f\circ g)(c)=f(\varepsilon(c))=\varepsilon(c)x=c.$$

Now we compute that

$$(\zeta_{\mathcal{C}}\circ(f\otimes_B A))(a\otimes_B a')=\zeta_{\mathcal{C}}(ax\otimes_B a')=axa'=\mathrm{can}(a\otimes_B a'),$$

so $\mathrm{can}=\zeta_{\mathcal{C}}\circ(f\otimes_B A)$ is an isomorphism. □

Proposition 4.4.1 leads us to the following Definition.

Definition 4.4.2 *Let $(\mathcal{C},x)$ be an A-coring with a fixed grouplike, and let $B=A^{\mathrm{co}\mathcal{C}}$. We call $(\mathcal{C},x)$ a Galois coring if the canonical coring morphism* $\mathrm{can}:\ \mathcal{D}=A\otimes_B A\to\mathcal{C}$, $\mathrm{can}(a\otimes_B b)=axb$ *is an isomorphism.*

Let $i:\ B\to A$ be a ring morphism. If $x\in G(\mathcal{C})^B$, then we can define a functor

$$\Gamma:\ \mathcal{M}^{\mathcal{D}}\to\mathcal{M}^{\mathcal{C}},\ \ \Gamma(M,\rho)=(M,\widetilde{\rho})$$

with $\widetilde{\rho}(m)=m_{[0]}\otimes_A xm_{[1]}\in M\otimes_A\mathcal{C}$ if $\rho(m)=m_{[0]}\otimes_B m_{[1]}\in M\otimes_B A$. It is easy to see that $\Gamma\circ K=F$, and therefore we have the following result.

Proposition 4.4.3 *Let $(\mathcal{C},x)$ be a Galois A-coring. Then Γ is an isomorphism of categories. Consequently R (resp. K) is fully faithful if and only if G (resp. F) is fully faithful.*

Proposition 4.4.4 *Let $(\mathcal{C},x)$ be an A-coring with fixed grouplike element, and $B=A^{\mathrm{co}\mathcal{C}}$. Assume that A is flat as a left B-module. Then the following statements are equivalent.*

1. *$(\mathcal{C},x)$ is Galois;*
2. *G is fully faithful.*

Proof. $\underline{1)\Rightarrow 2)}$ follows from Propositions 4.3.1 and 4.4.3. $\underline{2)\Rightarrow 1)}$ follows from Proposition 4.4.1. □

Proposition 4.4.5 *Let $(\mathcal{C},x)$ be an A-coring with fixed grouplike element, and $B=A^{\mathrm{co}\mathcal{C}}$. Assume that A is flat as a left B-module. Then the following statements are equivalent.*

1. *$(\mathcal{C},x)$ is Galois and A is faithfully flat as a left B-module;*
2. *(F,G) is a pair of inverse equivalences.*

Proof. The equivalence of 1) and 2) follows from Propositions 4.3.2 and 4.4.3. □

4.5 Morita Theory

Definition 4.5.1 *Let A and B be rings. A Morita context connecting A and B is a sixtuple (A, B, P, Q, f, g) where*

- $P \in {}_A\mathcal{M}_B$, $Q \in {}_B\mathcal{M}_A$;
- $f: P \otimes_B Q \to A$ *in* ${}_A\mathcal{M}_A$, $g: Q \otimes_A P \to B$ *in* ${}_B\mathcal{M}_A$;
- *the following two diagrams are commutative:*

$$\begin{tikzcd} Q \otimes_A P \otimes_B Q \arrow[r, "g\otimes_B Q"] \arrow[d, "Q\otimes_A f"'] & B \otimes_B Q \arrow[d, "\cong"] \\ Q \otimes_A A \arrow[r, "\cong"] & Q \end{tikzcd} \qquad \begin{tikzcd} P \otimes_B Q \otimes_A P \arrow[r, "f\otimes_A P"] \arrow[d, "P\otimes_B g"'] & A \otimes_A P \arrow[d, "\cong"] \\ P \otimes_B B \arrow[r, "\cong"] & P \end{tikzcd}$$

or

$$qf(p \otimes_B q') = g(q \otimes_A p)p' \;\; ; \;\; pg(q \otimes_A p') = f(p \otimes_B q)p', \tag{4.10}$$

for all $p, p' \in P'$ and $q, q' \in Q$.

Recall that $M \in {}_A\mathcal{M}$ is called a *generator* of ${}_A\mathcal{M}$ if there exist $m_i \in M$ and $f_i \in {}_A\mathrm{Hom}(M, A)$ such that $\sum_i f_i(m_i) = 1_A$.

Theorem 4.5.2 *Let (A, B, P, Q, f, g) be a Morita context, and assume that f is surjective. Then we have the following properties.*

1. *f is bijective;*
2. *$P \in {}_A\mathcal{M}$ and $Q \in \mathcal{M}_A$ are generators;*
3. *$P \in \mathcal{M}_B$ and $Q \in {}_B\mathcal{M}$ are finitely generated projective;*
4. *$P \cong {}_B\mathrm{Hom}(Q, B)$ in ${}_A\mathcal{M}_B$ and $Q \cong \mathrm{Hom}_B(P, B)$ in ${}_B\mathcal{M}_A$;*
5. *$A \cong {}_B\mathrm{End}(Q)^{\mathrm{op}} \cong \mathrm{End}_B(P)$ as rings;*
6. *$(\tilde{F} = - \otimes_A P, \tilde{G} = - \otimes_B Q)$ is a pair of adjoint functors between $\mathcal{M}_A$ and $\mathcal{M}_B$;*
7. *$M \otimes_B Q \cong M \otimes_B \mathrm{Hom}_B(P, B) \cong \mathrm{Hom}_B(P, M)$, for all $M \in \mathcal{M}_B$; in other words, the functor $\tilde{G}$ is isomorphic to $\mathrm{Hom}_B(-, M)$.*

Proof. Since f is surjective, we know that there exist $p_i \in P$, $q_i \in Q$ ($i = 1, \cdots, n$) such that

$$\sum_{i=1}^{n} f(p_i \otimes_B q_i) = 1_A. \tag{4.11}$$

1) If $\sum_j p'_j \otimes_B q'_j \in \mathrm{Ker}\,(f)$, then

$$\begin{aligned}\sum_j p'_j \otimes_B q'_j &\overset{(4.11)}{=} \sum_{i,j} p'_j \otimes_B q'_j f(p_i \otimes_B q_i)\\ &\overset{(4.10)}{=} \sum_{i,j} p'_j \otimes_B g(q'_j \otimes_A p_i) q_i = \sum_{i,j} p'_j g(q'_j \otimes_A p_i) \otimes_B q_i\\ &\overset{(4.10)}{=} \sum_{i,j} f(p'_j \otimes_B q'_j) p_i \otimes_B q_i = 0.\end{aligned}$$

2) For $i = 1, \cdots, n$, define $f_i \in {}_A\mathrm{Hom}(P, A)$ by $f_i(p) = f(p \otimes_B q_i)$. Then

$$\sum_{i=1}^n f_i(p_i) = \sum_{i=1}^n f(p_i \otimes_B q_i) \overset{(4.11)}{=} 1_A,$$

so $P \in {}_A\mathcal{M}$ is a generator.

3) For all $p \in P$, we have

$$p = \sum_i f(p_i \otimes_B q_i) p \overset{(4.10)}{=} p_i g(q_i \otimes_A p),$$

and it follows that $\{(p_i, g(q_i \otimes_A -) \mid i = 1, \cdots, n\}$ is a finite dual basis of $P \in \mathcal{M}_B$.

4) ${}_B\mathrm{Hom}(Q, B) \in {}_A\mathcal{M}_B$, with the following left A-action and right B-action:

$$(a \cdot \varphi \cdot b)(q) = \varphi(qa)b,$$

for all $a \in A$, $b \in B$, $q \in Q$ and $\varphi \in {}_B\mathrm{Hom}(Q, B)$. Now we define

$$\alpha :\ P \to {}_B\mathrm{Hom}(Q, B)$$

as follows:

$$\alpha(p)(q) = g(q \otimes_A p).$$

α is an (A, B)-bimodule map since

$$\alpha(apb)(q) = g(q \otimes_A apb) = g(qa \otimes_A p)b = (\alpha(p)(qa))b = (a \cdot \alpha(p) \cdot b)(q).$$

α is injective: if $\alpha(p) = 0$, then

$$p = \sum_i f(p_i \otimes_B q_i) p = \sum_i p_i g(q_i \otimes_A p) = \sum_i p_i(\alpha(p)(q_i)) = 0.$$

α is surjective: for $\psi \in {}_B\mathrm{Hom}(Q, B)$, we have

$$\varphi(q) \;=\; \sum_i \varphi(q f(p_i \otimes_B q_i))$$

$$
\begin{aligned}
&= \sum_i \varphi(g(q \otimes_A p_i)q_i) \\
&= \sum_i g(q \otimes_A p_i)\varphi(q_i) \\
&= g(q \otimes \sum_i p_i\varphi(q_i)) \\
&= \alpha(\sum_i p_i\varphi(q_i))(q).
\end{aligned}
$$

hence $\varphi = \alpha(\sum_i p_i\varphi(q_i))$.
In a similar way, $\mathrm{Hom}_B(P, B) \in {}_B\mathcal{M}_A$ via

$$(b \cdot \psi \cdot a)(p) = b\psi(ap),$$

and the isomorphism $\beta :\ Q \to \mathrm{Hom}_B(P, B)$ is given by the formula

$$\beta(q)(p) = g(q \otimes_A p).$$

5) The map

$$\gamma :\ A \to {}_B\mathrm{End}(Q)^{\mathrm{op}},\ \ \gamma(a)(q) = qa$$

is a ring morphism:

$$\gamma(ab)(q) = qab = (\gamma(b) \circ \gamma(a))(q).$$

γ is injective: if $\gamma(a) = 0$, then

$$a = \sum_i f(p_i \otimes_B q_i)a = \sum_i f(p_i \otimes_B q_ia) = \sum_i f(p_i \otimes_B \gamma(a)(q_i)) = 0.$$

γ is surjective: for $k \in {}_B\mathrm{End}(Q)^{\mathrm{op}}$, we have

$$
\begin{aligned}
k(q) &= \sum_i k(qf(p_i \otimes_B q_i)) \\
&= \sum_i k(g(q \otimes_A p_i)q_i) \\
&= \sum_i g(q \otimes_A p_i)k(q_i) \\
&= \sum_i qf(p_i \otimes_B k(q_i)) \\
&= \gamma(\sum_i f(p_i \otimes_B k(q_i)))(q),
\end{aligned}
$$

so $k = \gamma(\sum_i f(p_i \otimes_B k(q_i)))$.
The other ring automorphism is

$$\delta :\ A \to \mathrm{End}_B(P),\ \ \delta(a)(p) = ap.$$

6) The unit and the counit of the adjunction are defined as follows:

$$\eta_N = \eta \otimes_A f^{-1} : \; N \otimes N \otimes_A P \otimes_B Q \;\; ; \;\; \varepsilon_M = M \otimes_B g : \; M \otimes_B Q \otimes_A \to M,$$

for $N \in \mathcal{M}_A$ and $M \in \mathcal{M}_B$. F is fully faithful since η_N is bijective.

7) For $M \in \mathcal{M}_B$, we have an homomorphism

$$\alpha_M : \; M \otimes_B \mathrm{Hom}_B(P, B) \to \mathrm{Hom}_B(P, M), \;\; \alpha_M(m \otimes_B f) = \varphi,$$

with $\varphi(p) = mf(p)$. Now we know that $P \in \mathcal{M}_B$ is finitely generated projective, with finite dual basis $\{(p_i, f_i = g(q_i \otimes_A -) \mid i = 1, \cdots, n\}$. The inverse of α_M is now given by the formula

$$\alpha_M^{-1}(\varphi) = \sum_i \varphi(p_i) \otimes_B f_i.$$

□

A left (resp.) right A-module that is finitely generated and projective and a generator is called a left (resp. right) A-*progenerator* A Morita context (A, B, P, Q, f, g) is called *strict* if f and g are surjective. In this case, both f and f and g are injective, and P and Q are A- and B-progenerators. In this case the adjunction $(\tilde{F}, \tilde{G})$ of Theorem 4.5.2 6) is a pair of inverse equivalences.

The Morita context associated to a module

Let B be a ring, and $P \in \mathcal{M}_B$. We construct a Morita context as follows. Let $A = \mathrm{End}_B(P)$, $Q = \mathrm{Hom}_B(P, B)$. Then P is an (A, B)-bimodule, with left A-action

$$a \cdot p = a(p);$$

Q is a (B, A)-bimodule with actions

$$(b \cdot q)(p) = bq(p) \;\; ; \;\; q \cdot a = q \circ a.$$

Then the maps

$$f : \; P \otimes_B Q \to A, \;\; f(p \otimes_B q)(p') = pq(p');$$
$$g : \; Q \otimes_A P \to B, \;\; g(q \otimes_A p) = g(p)$$

are well-defined bimodule maps.

Proposition 4.5.3 *With notation as above, (A, B, P, Q, f, g) is a Morita context.*
The map f is surjective if and only if $P \in \mathcal{M}_B$ is finitely generated projective.
The map g is surjective if and only if $P \in \mathcal{M}_B$ is a generator.
Consequently, the Morita context is strict if and only if P is a right B-progenerator.

Proof. The proof of the first statement is straightforward.
If f is surjective, then it follows from Theorem 4.5.2 3) that $P \in \mathcal{M}_B$ is finitely generated projective. Conversely, assume that $\{(p_i, q_i) \mid i = 1, \cdots, n\}$ is a finite dual basis of P. For all $p' \in P$, we have that

$$f(\sum_i p_i \otimes_B q_i)(p') = f(\sum_i p_i \otimes_B q_i)p' = \sum_i p_i g(q_i \otimes_A p') = \sum_i p_i q_i(p') = p',$$

hence $f(\sum_i p_i \otimes_B q_i) = 1_A$, and f is surjective.
If g is surjective, then it follows from Theorem 4.5.2 2) that $P \in \mathcal{M}_B$ is a generator. Conversely, if P is a generator, then there exist $p_i \in P_i$ and $q_i \in Q = \mathrm{Hom}_B(P, B)$ such that

$$1_B = \sum_i q_i(p_i) = g(\sum_i q_i \otimes_A p_i),$$

and it follows that g is surjective. □

Progenerators are faithfully flat

Proposition 4.5.4 *Let $M \in \mathcal{M}_A$ be finitely generated projective. Then M is a flat left A-module.*

Proof. Let $\{(m_i, f_i) \mid i = 1, \cdots, n\}$ is a finite dual basis of M. Let $\varphi: \ P \to Q$ be a monomorphism in ${}_A\mathcal{M}$. We have to show that $\varphi \otimes_A M: \ P \otimes_M \to Q \otimes_A M$ is a monomorphism of abelian groups. Take $\sum_j n_j \otimes_A p_j \in \mathrm{Ker}\,(\varphi \otimes_A M)$. Then

$$0 = r(\varphi \otimes_A M)(\sum_j n_j \otimes_A p_j) = \sum_j m_j \otimes_A \varphi(p_j).$$

It follows that we have, for all $f \in \mathrm{Hom}_A(M, A)$:

$$0 = \sum_j f(m_j)\varphi(p_j) = \varphi(\sum_j f(m_j)p_j),$$

and, since φ is injective,

$$\sum_j f(m_j)p_j = 0.$$

We now conclude that

$$\sum_j n_j \otimes_A p_j = \sum_{i,j} m_i f_i(n_j) \otimes_A p_j = \sum_i m_i \otimes_A \sum_j f_i(n_j)p_j = 0.$$

□

Proposition 4.5.5 *Let $M \in \mathcal{M}_A$ be a generator. Then $M \otimes_A - : \ {}_A\mathcal{M} \to \underline{\underline{\mathrm{Ab}}}$ reflects exact sequences.*

Proof. Since M is a generator, there exist $m_i \in M$, $f_i \in \mathrm{Hom}_A(M, A)$ such that $\sum_i f_i(m_i) = 1$. Consider a sequence

$$P \xrightarrow{\varphi} Q \xrightarrow{\psi} R \tag{4.12}$$

in $\mathcal{M}_A$, and assume that

$$M \otimes_A P \xrightarrow{M \otimes_A \varphi} M \otimes_A Q \xrightarrow{M \otimes_A \psi} M \otimes_A R$$

is exact in $\underline{\underline{\mathrm{Ab}}}$. Then we have to show that (4.12) is exact.
We first show that $\psi \circ \varphi = 0$. For all $p \in P$, we have

$$0 = ((M \otimes_A \psi) \circ (M \otimes_A \varphi))(m_i \otimes_A p) = m_i \otimes_A (\psi \circ \varphi)(p),$$

hence

$$(\psi \circ \varphi)(p) = \sum_i f_(m_i)(\psi \circ \varphi)(p) = 0.$$

Next, assume that $q \in \mathrm{Ker}\,(\psi)$. Then $(M \otimes_A \psi)(m_i \otimes_A q) = 0$, so there exists $\sum_j n_j \otimes_A p_j \in M \otimes_A P$ such that

$$m_i \otimes_A q = (M \otimes_A \varphi)(\sum_j n_j \otimes_A p_j) = \sum_j n_j \otimes_A \varphi(p_j).$$

Then

$$q = \sum_i f_i(m_i)q = \sum_{i,j} f_i(n_j)\varphi(p_j) = \varphi(\sum_{i,j} f_i(n_j)p_j) \in \mathrm{Im}\,(\varphi).$$

□

Corollary 4.5.6 *If $M \in \mathcal{M}_A$ is a progenerator, then $M \in \mathcal{M}_A$ is faithfully flat.*

Progenerators over commutative rings

Let M be a finitely generated projective module over a commutative ring k. We will show that M is a generator if and only if M is faithful. We introduced the following ideals of k:

$$\mathrm{Ann}_k(M) = \{x \in k \mid Mx = 0\}$$

$$\mathrm{Tr}_k(M) = \{\sum_i \langle m^*, m\rangle \mid m_i \in M, m_i^* \in M^*\}$$

$\mathrm{Ann}_k(M)$ is called the *annihiliator* of M, and $\mathrm{Tr}_k(M)$ is called the *trace ideal* of M. Clearly M is faithful if and only if $\mathrm{Ann}_k(M) = 0$, and M is a generator if and only if $\mathrm{Tr}_k(M) = k$.

Proposition 4.5.7 *Let I be an ideal of k, and M a finitely generated k-module. Then*

$$MI = M \iff I + \mathrm{Ann}_k(M) = k.$$

Proof. $\Longleftarrow$. There exist $x \in I$ and $y \in \mathrm{Ann}_k(M)$ such that $x + y = 1$. Then for all $m \in M$ we have that $m = mx + my = mx \in MI$.

$\Longrightarrow$. Let $\{m_1, m_2, \cdots m_n\}$ be a set of generators of M. For $i = 1, \cdots, n$, let

$$M_i = m_i k + m_{i+1} k + \cdots + m_n k$$

be the submodule of M generated by $\{m_i, m_{i+1}, \cdots, m_n\}$. Let $M_{n+1} = 0$. We will prove the following statement:

$$\forall i \in \{1, \cdots, n+1\} : \ \exists x_i \in I : \ \ M(1 - x_i) \subset M_i. \tag{4.13}$$

We construct the x_i recursevely. Let $x_1 = 0$. Assume that we have found $x_i \in I$ such that (4.13) is satisfied. Then

$$M(1 - x_i) = MI(1 - x_i) = M(1 - x_i)I \subset M_i I,$$

so there exist $x_{ji} \in I$ such that

$$m_i(1 - x_i) = \sum_{j=i}^{n} m_j x_{ji},$$

and

$$m_i(1 - x_i - x_{ii}) = \sum_{j=i+1}^{n} m_j x_{ji} \in M_{i+1}.$$

Then it follows that

$$M(1 - x_i)(1 - x_i - x_{ii}) \subset M_i(1 - x_i - x_{ii}) \subset M_{i+1},$$

or

$$M(1 - (2x_i + x_{ii} - x_i^2 - x_i x_{ii})) \subset M_{i+1}.$$

Then $x_{i+1} = 2x_i + x_{ii} - x_i^2 - x_i x_{ii} \in I$ satisfies (4.13).
Now $M(1 - x_{n+1}) \subset M_{n+1} = 0$, hence $1 = x_{n+1} + (1 - x_{n+1}) \in I + \mathrm{Ann}_k(M)$. $\square$

Corollary 4.5.8 (Nakayama Lemma) *Let M be a finitely generated k-module. If $M\mathfrak{m} = M$ for every maximal ideal $\mathfrak{m}$ of k, then $M = 0$.*

Proof. If $M \neq 0$, then $\mathrm{Ann}_k(M) \neq k$, so there exists a maximal ideal $\mathfrak{m}$ of k containing $\mathrm{Ann}_k(M)$. Then $\mathfrak{m} + \mathrm{Ann}_k(M) = \mathfrak{m} \neq k$, and it follows from Proposition 4.5.7 that $M\mathfrak{m} \neq M$. $\square$

Proposition 4.5.9 *Let M be a finitely generated projective k-module. Then*

$$\mathrm{Tr}_k(M) \oplus \mathrm{Ann}_k(M) = k.$$

Consequently M is a generator if and only if M is faithful.

Proof. Let $\{(m_i, m_i^*) \mid i = 1, \cdots n\}$ be a finite dual basis of M. For all $m \in M$, we have

$$m = \sum_{i=1}^{n} \langle m_i^*, m \rangle m_i \in \mathrm{Tr}_k(M)M,$$

so $M = \mathrm{Tr}_k(M)M$, and it follows from Proposition 4.5.7 that

$$\mathrm{Tr}_k(M) + \mathrm{Ann}_k(M) = k.$$

We are left to show that this sum is direct. For all $x \in \mathrm{Ann}_k(M)$, $m \in M$ and $m^* \in M^*$, we have

$$\langle m^*, m \rangle x = \langle m^*, mx \rangle = 0,$$

so $\mathrm{Tr}_k(M)\mathrm{Ann}_k(M) = 0$. There exist $t \in \mathrm{Tr}_k(M)$ and $a \in \mathrm{Ann}_k(M)$ such that $t + m = 1$. If $x \in \mathrm{Tr}_k(M) \cap \mathrm{Ann}_k(M)$, then

$$x = xt + xu = 0.$$

$\square$

The Eilenberg-Watts Theorem

We have seen that a strict Morita context connecting two rings A and B gives rise to a pair of inverse equivalences between the categories of modules over A and B. We will now prove the converse result: every pair of inverse equivalences between module categories comes from a strict Morita context. First we need a few classical results from category theory.
We first recall one of the characterizing properties of pairs of adjoint functors. Let $F: \mathcal{A} \to \mathcal{B}$ and $G: \mathcal{B} \to \mathcal{A}$ be two functors. Then (F, G) is an adjoint pair of functors if and only if for every $A \in \mathcal{A}$, $B \in \mathcal{B}$, we have an isomorphism

$$\theta_{A,B}: \ \mathrm{Hom}_{\mathcal{B}}(F(A), B) \to \mathrm{Hom}_{\mathcal{A}}(A, G(B))$$

that is natural in A and B. The naturality means the following: for all $f: A' \to A$ in $\mathcal{A}$ and $g: B \to B'$ in $\mathcal{B}$, we have

$$\theta_{A',B'}(g \circ \varphi \circ F(f)) = G(g) \circ \theta_{A,B}(\varphi) \circ f. \tag{4.14}$$

We also recall the definition of the coproduct. Let $(A_i)_{i \in I}$ be a family of objects in the category. A coproduct $\coprod_{i \in I} A_i$ is an object $A = \coprod_{i \in I} A_i \in \mathcal{A}$ together with morphisms $p_i: A_i \to A$ such that the following universal property holds: given $A' \in \mathcal{A}$ and a collection of morphisms $q_i: A_i \to A'$, there exists a unique $l: A \to A'$ such that the diagram

$$\begin{tikzcd} A_i \arrow[r, "p_i"] \arrow[dr, "q_i"'] & A \arrow[d, "\exists! l"] \\ & A' \end{tikzcd} \tag{4.15}$$

commutes.

Proposition 4.5.10 *Let (F, G) be an adjoint pair of functors between the categories $\mathcal{A}$ and $\mathcal{B}$. If $(A_i)_{i\in I}$ is a family of objects in $\mathcal{A}$ such that the coproduct $\coprod_{i\in I} A_i$ exists in $\mathcal{A}$, then the coproduct $\coprod_{i\in I} F(A_i)$ exists in $\mathcal{B}$, and*

$$\coprod_{i\in I} F(A_i) = F(\coprod_{i\in I} A_i).$$

Proof. Let $A = \coprod_{i\in I} A_i$. We will show that the family of morphisms $F(p_i) : F(A_i) \to F(A)$ in $\mathcal{B}$ satisfies the necessary universal property. Take $B \in \mathcal{B}$, and assume that we have a family of morphisms $q_i : F(A_i) \to B$ in $\mathcal{B}$. Let $r_i = \theta_{A_i,B}(q_i) : A_i \to G(B)$. By the universal property of the coproduct $\coprod_{i\in I} A_i$, there exists a unique $l : A \to G(B)$ making the diagram

$$\begin{tikzcd}
A_i \arrow[r, "p_i"] \arrow[dr, "r_i"'] & A \arrow[d, "\exists! l"] \\
& G(B)
\end{tikzcd}$$

Then

$$q_i = \theta^{-1}_{A_i,B}(r_i) = \theta^{-1}_{A_i,B}(l \circ p_i) \overset{(4.14)}{=} \theta^{-1}_{A,B}(l) \circ F(p_i),$$

so the diagram

$$\begin{tikzcd}
F(A_i) \arrow[r, "F(p_i)"] \arrow[dr, "q_i"'] & F(A) \arrow[d, "\theta^{-1}_{A,B}(l)"] \\
& B
\end{tikzcd}$$

commutes. We are done if we can prove the uniqueness of the map making the diagram commutative. Assume that $k : F(A) \to B$ is such that $k \circ F(P_i) = q_i$, for all $i \in I$. Then

$$r_i = \theta_{A_i,B}(q_i) \overset{(4.14)}{=} \theta_{A,B}(k) \circ p_i,$$

and, by the uniqueness in (4.15), $l = \theta_{A,B}(k)$, and $k = \theta^{-1}_{A,B}(l)$. □

Proposition 4.5.11 *Let (F, G) and (F', G') be two adjoint pairs of functors between the categories $\mathcal{A}$ and $\mathcal{B}$, and let $(A_i)_{i\in I}$ be a family of objects in $\mathcal{A}$ such that the coproduct $A = \coprod_{i\in I} A_i$ exists in $\mathcal{A}$. If $\gamma : F \to F'$ is a natural transformation such that γ_{A_i} is an isomorphism for each i, then $\gamma_A : F(A) \to F(A')$ is also an isomorphism.*

Proof. For all $i \in I$, we consider the commutative diagram

$$\begin{tikzcd}
F(A_i) \arrow[r, "\gamma_{A_i}"] \arrow[d, "F(p_i)"'] & F'(A_i) \arrow[d, "F'(p_i)"] \\
F(A) \arrow[r, "\gamma_A"] & F'(A)
\end{tikzcd}$$

Since $F'(A) = \coprod_{i\in I} F'(A_i)$, there exists a morphism $\psi : F'(A) \to F(A)$ in $\mathcal{B}$ such that

$$\psi \circ F'(p_i) = F(p_i) \circ \gamma^{-1}_{A_i}.$$

Then

$$F(p_i) = \psi \circ F'(p_i) \circ \gamma_{A_i} = \psi \circ \gamma_A \circ F(p_i).$$

From the uniqueness in the universal property of the coproduct $F(A) = \coprod_{i \in I} F(A_i)$, it follows that $\psi \circ \gamma_A = F(A)$.
We also have

$$\gamma_A \circ \psi \circ F'(p_i) = \gamma_A \circ F(p_i) \circ \gamma_{A_i}^{-1} = F'(p_i) \circ \gamma_{A_i} \circ \gamma_{A_i}^{-1} = F'(p_i).$$

From the uniqueness in the universal property of the coproduct $F'(A) = \coprod_{i \in I} F'(A_i)$, it follows that $\gamma_A \circ \psi = F'(A)$. $\square$

We have seen in Proposition 4.5.10 that left adjoints preserve coproducts. Similar arguments show that they also preserve cokernels.

Proposition 4.5.12 *Let (F, G) be an adjoint pair of functors between the categories $\mathcal{A}$ and $\mathcal{B}$. Let $f : A_1 \to A_2$ be a morphism in $\mathcal{A}$ with cokernel $u : A_2 \to f$. Then* $\mathrm{Coker}\,(F(f)) = F(\mathrm{Coker}\,(f)) = F(u) : F(A_2) \to F(E)$.

Proof. It is clear that $F(u) \circ F(f) = F(u \circ f) = 0$, so it suffices to show that the universal property of cokernels holds. Let $g : F(A_2) \to B$ be a morphism in $\mathcal{B}$ such that $g \circ F(f) = 0$. Let $h = \theta_{A_2,B}(g)$. Then

$$h \circ f = \theta_{A_2,B}(g) \circ f \overset{(4.15)}{=} \theta_{A_1,B}(g \circ F(f)) = 0,$$

so there exists a unique morphism $h' : E \to G(B)$ in $\mathcal{A}$ making the diagram

$$\begin{tikzcd} A_1 \arrow[r, "f"] & A_2 \arrow[r, "u"] \arrow[dr, "h"'] & E \arrow[d, "\exists! h'"] \\ & & G(B) \end{tikzcd}$$

commutative. Then

$$g = \theta^{-1}_{A_2,B}(h) \overset{(4.15)}{=} \theta^{-1}_{E,B}(h') \circ F(u),$$

hence the diagram

$$\begin{tikzcd} F(A_1) \arrow[r, "F(f)"] & F(A_2) \arrow[r, "F(u)"] \arrow[dr, "g"'] & F(E) \arrow[d, "\theta^{-1}_{E,B}(h')"] \\ & & B \end{tikzcd}$$

commutes. We still have to prove the unicity. Suppose that $v' : F(E) \to B$ is such that $v' \circ F(u) = g$. Then

$$h = \theta_{A_2,B}(g) \overset{(4.15)}{=} \theta_{E,B}(v') \circ u,$$

and it follows from the unicity of h' that $h' = \theta_{E,B}(v')$ and $v' = \theta^{-1}_{E,B}(h')$. $\square$

Proposition 4.5.13 *Let (F, G) and (F', G') be two adjoint pairs of functors between the categories $\mathcal{A}$ and $\mathcal{B}$, and $\gamma : F \to F'$ a natural transformation such that γ_{A_i} is an isomorphism $(i = 1, 2)$. Let $f : A_1 \to A_2$ be a morphism in $\mathcal{A}$ with cokernel $u : A_2 \to f$. Then $\gamma_E : F(E) \to F(E')$ is also an isomorphism.*

Proof. Consider the commutative diagram

$$\begin{tikzcd}
F(A_1) \arrow[r, "F(f)"] \arrow[d, "\gamma_{A_1}"] & F(A_2) \arrow[r, "F(f')"] \arrow[d, "\gamma_{A_2}"] & F(E) \arrow[d, "\gamma_E"] \\
F'(A_1) \arrow[r, "F'(f)"] & F'(A_2) \arrow[r, "F'(u)"] & F'(E)
\end{tikzcd}$$

Then

$$F(u) \circ \gamma_{A_2}^{-1} \circ F(f') = F(u) \circ F(f) \circ \gamma_{A_1} = 0,$$

hence there exists $\psi : \; F'(E) \to F(E)$ such that

$$F(u) \circ \gamma_{A_2}^{-1} = \psi \circ F(u'),$$

hence

$$F(u) = \psi \circ F(u') \circ \gamma) A_2 = \psi \circ \gamma_E \circ F(u),$$

and it follows from the uniqueness in the universal property of the cokernel that

$$\psi \circ \gamma_E = F(E).$$

We also have

$$\gamma_E \circ \psi \circ F(u') = \gamma_E \circ F(u) \circ \gamma_{A_2}^{-1} = F(u') \circ \gamma_{A_2} \circ \gamma_{A_2}^{-1} = F(u'),$$

and it follows, again using the uniqueness in the universal property of the cokernel, that

$$\gamma_E \circ \psi = F'(E).$$

□

Theorem 4.5.14 (Eilenberg-Watts) *Suppose that A and B are rings, and that $F : \; \mathcal{M}_A \to \mathcal{M}_B$ is a functor with a right adjoint G. Then $F(A) = M \in {}_A\mathcal{M}_B$ and there is a natural isomorphism between the functors F and $- \otimes_A M$.*

Proof. $F(A) = M \in \mathcal{M}_B$. We have an isomorphism

$$l : \; A \to \mathrm{Hom}_A(A, A), \;\; l(a)(b) = ab.$$

It is clear that $l(a) \circ l(a') = l(aa')$. Now since F is a functor, we also have a map

$$F : \; \mathrm{Hom}_A(A, A) \to \mathrm{Hom}_B(F(A), F(A)) = \mathrm{End}_B(M).$$

We define $am = F(l(a))(m)$, for all $a \in A$, $m \in M$. This makes M an (A, B)-bimodule since

$$a(mb) = F(l(a))(mb) = (F(l(a))(m))b = (am)b;$$

$$(aa')m = F(l(aa'))(m) = F(l(a) \circ l(a'))(m) = (F(l(a)) \circ F(l(a')))(m) = a(a'm).$$

Now take $X \in \mathcal{M}_A$. We have an isomorphism

$$\xi:\ X \to \mathrm{Hom}_A(A, X),\ \ \xi(x)(a) = xa,$$

and $\xi(axa') = l(a) \circ \xi(x) \circ l(a')$. We also have

$$F:\ \mathrm{Hom}_A(A, X) \to \mathrm{Hom}_B(M, F(X)).$$

We define

$$\beta_X:\ X \to \mathrm{Hom}_B(M, F(X)),\ \ \beta_X(x) = F(\xi(x)).$$

β_X is right A-linear:

$$\beta_X(xa) = F(\xi(xa)) = F(\xi(x) \circ l(a)) = F(\xi(x)) \circ F(l(a)) = \beta_X(x) \circ F(l(a)),$$

hence

$$\beta_X(xa)(m) = \beta_X(x)(am)$$

and

$$\beta_X(xa) = \beta(x)a.$$

Now we claim that β is an natural transformation from the identity functor on $\mathcal{M}_A$ to the functor $\mathrm{Hom}_B(M, F(-))$. Let $f\ :\ X \to X'$ in $\mathcal{M}_A$. It is easy to see that, for all $x \in X$, we have $f \circ \xi(x) = \xi(f(x))$. Now we show that the diagram

$$\begin{tikzcd}
X \arrow[r, "f"] \arrow[d, "\beta_X"'] & X' \arrow[d, "\beta_{X'}"] \\
\mathrm{Hom}_B(M, F(X)) \arrow[r, "F(f)\circ-"] & \mathrm{Hom}_B(M, F(X'))
\end{tikzcd}$$

commutes: for all $x \in X$, we have

$$F(f) \circ \beta_X(x) = F(f) \circ F(\xi(x)) = F(f \circ \xi(x)) = F(\xi(f(x))) = \beta_{X'}(f(x)).$$

Now $\mathrm{Hom}_B(M, -):\ \mathcal{M}_B \to \mathcal{M}_A$ is a right adjoint of $- \otimes_A M$, so we have a isomorphism

$$\mathrm{Hom}_A(X, \mathrm{Hom}_B(M, F(X))) \cong \mathrm{Hom}_B(X \otimes_A M, F(X))$$

that is natural in X. The image of β_X is a map

$$\gamma_X:\ X \otimes_A M \to F(X)$$

in $\mathcal{M}_B$, and γ is natural in X. γ_X is given by the formula

$$\gamma_X(x \otimes_A m) = \beta_X(x)(m) = F(\xi(x))(m).$$

So we have a natural transformation

$$\gamma:\ - \otimes_A M \to F.$$

We find that

$$\gamma_A(a \otimes_A m) = F(l(a))(m) = am,$$

so $\gamma_A : A \otimes_A M \to M$ is the natural isomorphism. It follows from Proposition 4.5.11 that $\gamma_{A^{(I)}}$ is an isomorphism, for every index set I. Now for $X \in \mathcal{M}_A$ arbitrary, we can find a exact sequence

$$A^{(J)} \to A^{(I)} \to X \to 0.$$

It then follows from Proposition 4.5.13 that γ_X is an isomorphism, hence $\gamma : - \otimes_A M \to F$ is a natural isomorphism. □

Theorem 4.5.15 *Suppose that A and B are rings, and that (F, G) is a pair of inverse equivalences between $\mathcal{M}_A$ and $\mathcal{M}_B$. Then (F, G) is induced by a strict Morita context connecting A and B.*

Proof. It follows from Theorem 4.5.14 that $F = - \otimes_A M$, and $G = \otimes_B N$, with $M = F(A)$, $N = G(B)$. Consider the unit η and counit ε of the adjunction (F, G):

$$\eta_X : X \to X \otimes_A M \otimes_B N, \quad \varepsilon_Y : Y \otimes_B N \otimes_A M \to Y.$$

For $x \in X$, consider the A-linear map $\xi(x)$ as in the proof of Theorem 4.5.14. From the naturality of η, we have a commutative diagram

$$\begin{tikzcd} A \arrow[r, "\eta_A"] \arrow[d, "\xi(x)"'] & A \otimes_A M \otimes_B N \arrow[d, "\xi(x) \otimes_A M \otimes_B N"] \\ X \arrow[r, "\eta_X"] & X \otimes_A M \otimes_B N \end{tikzcd}$$

Taking $X = A$, and $x = a$ in this diagram, we see that η_A is left A-linear. It follows that $\eta_X(x) = x \otimes_A \eta_A(1)$, hence $\eta_X = X \otimes_A \eta_A$. In a similar way, we prove that ε_B is right B-linear, and $\varepsilon_Y = Y \otimes_B \varepsilon_B$. Because (F, G) is an adjoint pair, we have two commutative diagrams, for every $X \in \mathcal{M}_A$ and $Y \in \mathcal{M}_B$:

$$\begin{tikzcd} F(X) \arrow[r, "F(\eta_X)"] \arrow[dr, "="'] & FGF(X) \arrow[d, "\varepsilon_{F(X)}"] \\ & F(X) \end{tikzcd} \qquad \begin{tikzcd} G(Y) \arrow[r, "\eta_{G(Y)}"] \arrow[dr, "="'] & GFG(Y) \arrow[d, "G(\varepsilon_Y)"] \\ & G(Y) \end{tikzcd}$$

Take $X = A$ and $Y = B$:

$$\begin{tikzcd} M \arrow[r, "\eta_A \otimes_A M"] \arrow[dr, "="'] & M \otimes_B N \otimes_A M \arrow[d, "M \otimes_B \varepsilon_B"] \\ & M \end{tikzcd} \qquad \begin{tikzcd} N \arrow[r, "N \otimes_A \eta_A"] \arrow[dr, "="'] & N \otimes_A M \otimes_B N \arrow[d, "\varepsilon_B \otimes_B N"] \\ & N \end{tikzcd}$$

It follows that $(A, B, M, N, \eta_A^{-1}, \varepsilon_B)$ is a strict Morita context. □

4.6 Galois corings and Morita theory

Let $(\mathcal{C}, x)$ be an A-coring with a fixed grouplike element. We let $B = A^{\mathrm{co}\mathcal{C}}$. We consider the left dual ${}^*\mathcal{C} = {}_A\mathrm{Hom}(\mathcal{C}, A)$. Recall (4.5-4.6) that ${}^*\mathcal{C}$ is an A-ring. As before, $\mathcal{D} = A \otimes_B A$ is the Sweedler canonical coring. Now consider the left dual of the canonical map

$$\mathrm{can}: \ \mathcal{D} \to \mathcal{C}, \ \ \mathrm{can}(a \otimes_B a') = axa'.$$

$${}^*\mathrm{can}: \ {}^*\mathcal{C} \to {}^*\mathcal{D} = {}_A\mathrm{Hom}(A \otimes_B A, A), \ \ {}^*\mathrm{can}(f)(a \otimes_B a') = (f \circ \mathrm{can})(a \otimes_B a') = f(axa').$$

Let us give an easy description of ${}^*\mathcal{D}$.

Lemma 4.6.1 *We have an isomorphism of A-rings*

$$\lambda: \ {}^*\mathcal{D} \to {}_B\mathrm{End}(A)^{\mathrm{op}}, \ \ \lambda(\phi)(a) = \phi(1 \otimes_B a).$$

Proof. It is straightforward to see that λ is an isomorphism of abelian groups: the inverse of λ is defined by

$$\lambda^{-1}(\varphi)(a \otimes_B a') = a\varphi(a').$$

Let us next show that λ transforms multiplication into opposite composition. For $\phi, \Psi \in {}^*\mathcal{D}$, we have

$$(\phi\#\Psi)(a \otimes_B a') = \Psi(a \otimes_B \phi(1 \otimes_B a')),$$

hence

$$\lambda(\phi\#\Psi)(a) = (\phi\#\Psi)(1 \otimes_B a) = \Psi(1 \otimes_B \phi(1 \otimes_B a)) = (\lambda(\Psi) \circ \lambda(\phi))(a),$$

and $\lambda(\phi\#\Psi) = \lambda(\Psi) \circ \lambda(\phi)$.
Finally, we show that λ is an isomorphism of A-rings.

$$r: \ A \to {}_B\mathrm{End}(A)^{\mathrm{op}}, \ \ r(a)(a') = a'a$$

is a ring morphism, making ${}_B\mathrm{End}(A)^{\mathrm{op}}$ into an A-ring. Also recall that

$$i: \ A \to {}^*\mathcal{D}, \ \ i(a)(a' \otimes_B a'') = \varepsilon_{\mathcal{D}}(a' \otimes_B a'')a = a'a''a$$

is a ring morphism. Now

$$\lambda(i(a))(a'') = i(a)(1 \otimes_B a') = a'a = r(a)(a'),$$

so $\lambda \circ i = r$, as needed. □

The composition $\lambda \circ {}^*\mathrm{can}$ will also be denoted by ${}^*\mathrm{can}$. So we obtain a morphism of A-rings

$${}^*\mathrm{can}: \ {}^*\mathcal{C} \to {}_B\mathrm{End}(A)^{\mathrm{op}}, \ \ {}^*\mathrm{can}(f)(a) = f(xa).$$

The following result is now obvious.

Proposition 4.6.2 *If $(\mathcal{C}, x)$ is a Galois coring, then* ${}^*\mathrm{can}$ *is an isomorphism. Conversely, if $\mathcal{C}, \mathcal{D} \in {}_A\mathcal{M}$ are finitely generated projective, and* ${}^*\mathrm{can}$ *is an isomorphism, then* can *is an isomorphism, and $(\mathcal{C}, x)$ is a Galois coring.*
If $A \in {}_B\mathcal{M}$ is finitely generated projective, then $\mathcal{D} = A \otimes_B A \in {}_A\mathcal{M}$ is finitely generated projective.

Our next aim will be to associate a Morita context to a coring with a fixed grouplike element. This Morita context will connect B and ${}^*\mathcal{C}$.

Lemma 4.6.3 *The abelian group*

$$Q = \{q \in {}^*\mathcal{C} \mid c_{(1)}q(c_{(2)}) = q(c)x, \ \ \forall\, c \in \mathcal{C}\}$$

is a $({}^*\mathcal{C}, B)$-bimodule.

Proof. For all $f \in {}^*\mathcal{C}$, $q \in Q$ and $c \in \mathcal{C}$, we have

$$\begin{aligned} c_{(1)}(f\#q)(c_{(2)}) &= c_{(1)}q(c_{(2)}f(c_{(3)})) \\ &= (c_{(1)}f(c_{(2)}))_{(1)}q((c_{(1)}f(c_{(2)}))_{(2)}) \\ &= q(c_{(1)}f(c_{(2)}))x = (f\#q)(c)x, \end{aligned}$$

so $f\#q \in Q$, and Q is a left ideal in ${}^*\mathcal{C}$. For $b \in B$, we have

$$c_{(1)}(q\#i(b))(c_{(2)}) = c_{(1)}q(c_{(2)})b = q(c)xb = q(c)bx = (q\#i(b))(c)x,$$

so $q\#i(b) \in Q$, and Q is a right B-module. The fact that Q is a bimodule follows immediately from the associativity of $\#$. □

Lemma 4.6.4 *A is a $(B, {}^*\mathcal{C})$-bimodule.*

Proof. $A \in \mathcal{M}^{\mathcal{C}}$ via $\rho(a) = 1 \otimes_A xa$. Hence $A \in \mathcal{M}_{{}^*\mathcal{C}}$ via

$$a \cdot f = f(xa).$$

Clearly is a left B-module, via left multiplication. Finally

$$b(a \cdot f) = bf(xa) = f(bxa) = f(xba) = (ba) \cdot f.$$

□

Lemma 4.6.5 *The map*

$$\tau: \ A \otimes_{{}^*\mathcal{C}} Q \to B, \ \ \tau(a \otimes_{{}^*\mathcal{C}} q) = a \cdot q = q(xa)$$

is a well-defined morphism of (B, B)-bimodules.

Proof. τ is well-defined: for all $a \in A$, $q \in Q$ and $f \in {}^*\mathcal{C}$, we have

$$\tau(a \cdot f \otimes q) = \tau(f(xa) \otimes q) = q(xf(xa)) = (f\#q)(a) = \tau(a \otimes (f\#q)).$$

τ is left and right B-linear: for all $a \in A$, $q \in Q$ and $b \in B$, we have

$$\tau(ba \otimes_{^*\mathcal{C}} q) = q(xba) = q(bxa) = bq(xa) = b\tau(a \otimes_{^*\mathcal{C}} q);$$

$$\tau(a \otimes_{^*\mathcal{C}} q\#i(b)) = (q\#i(b))(xa) = q(xa)b = \tau(a \otimes_{^*\mathcal{C}} q)b.$$

□

Lemma 4.6.6 *The map*

$$\mu : \ Q \otimes_B A \to {}^*\mathcal{C}, \ \ \mu(q \otimes_B a) = q\#i(a)$$

is a well-defined morphism of (A, A)*-bimodules.*

Proof. μ is well-defined: for all $q \in Q$, $a \in A$ and $b \in B$, we have

$$\mu((q\#i(b)) \otimes a) = q\#i(b)\#i(a) = q\#i(ba) = \mu(q \otimes ba).$$

μ is left ${}^*\mathcal{C}$-linear: for all $q \in Q$, $a \in A$ and $f \in {}^*\mathcal{C}$, we have

$$\mu((f\#q) \otimes a) = f\#q\#i(a) = f\#\mu(q \otimes_B a).$$

Finally we show that μ is right ${}^*\mathcal{C}$-linear. We have to show that

$$\mu(q \otimes_B (a \cdot f)) = \mu(q \otimes_B f(xa)) = q\#i(f(xa))$$

is equal to

$$\mu(q \otimes_B a)\#f = q\#i(a)\#f.$$

or

$$q\#i(a)\#f = q\#i(f(xa)). \tag{4.16}$$

Indeed, for all $c \in \mathcal{C}$, we have

$$\begin{aligned}(q\#i(a)\#f)(c) &= f(c_{(1)}(q\#i(a))(c_{(2)})) = f(c_{(1)}q(c_{(2)})a) \\ &= f(q(c)xa) = q(c)f(xa) = (q\#i(f(xa)))(c).\end{aligned}$$

□

Proposition 4.6.7 *With notation as above,* $(B, {}^*\mathcal{C}, A, Q, \tau, \mu)$ *is a Morita context.*

Proof. Let us first show that

$$\mu(q \otimes_B a)\#q' = q\#i(\tau(a \otimes_{^*\mathcal{C}} q'.$$

We easily compute that

$$\mu(q \otimes_B a)\#q' = q\#i(a)\#q'$$

and

$$q\#i(\tau(a \otimes_{^*\mathcal{C}} q'. = q\#i(a \cdot q') = q\#i(q'(xa)),$$

and we have already computed that these are equal, see (4.16). Finally we compute that

$$\begin{aligned} a \cdot \mu(q \otimes_N a') &= a \cdot (q\#i(a')) = (q\#i(a'))(xa) \\ &= \quad q(xa)a' = \tau(a \otimes_{^*\mathcal{C}} q)a'. \end{aligned}$$

□

Proposition 4.6.8 *Let $(\mathcal{C}, x)$ be an A-coring with a fixed grouplike element, and consider the Morita context $(B, {}^*\mathcal{C}, A, Q, \tau, \mu)$ from Proposition 4.6.7. Then the following assertions are equivalent.*

1. *τ is surjective;*
2. *$\exists \Lambda \in Q$: $\Lambda(x) = 1$;*
3. *the map*
$$\omega_M : \ M \otimes_{^*\mathcal{C}} Q \to M^{^*\mathcal{C}}, \ \ \omega_M(m \otimes q) = m \cdot q$$
is bijective, for every $M \in \mathcal{M}_{^*\mathcal{C}}$.

Proof. $1) \Longrightarrow 2)$. Since τ is surjective, there exist $a_j \in A$, $q_j \in Q$ such that

$$1 = \tau(\sum_j a_j \otimes q_j) = \sum_j q_j(xa_j) = (\sum_j i(a_j)\#q_j)(x).$$

Now let $\Lambda = \sum_j i(a_j)\#q_j \in Q$.

$2) \Longrightarrow 3)$. $M^{^*\mathcal{C}}$ is defined as follows:

$$M^{^*\mathcal{C}} = \{m \in M \mid m \cdot f = mf(x), \text{ for all } f \in {}^*\mathcal{C}\}.$$

The map

$$\theta_M : \ M^{^*\mathcal{C}} \to M \otimes_{^*\mathcal{C}} Q, \ \ \theta_M(m) = m \otimes_{^*\mathcal{C}} \Lambda$$

is the inverse of ω_M. Indeed, for all $m \in M^{^*\mathcal{C}}$, we have

$$\omega_M \circ \theta_M)(m) = m \cdot \Lambda = m\Lambda(x) = m.$$

For all $m \in M$ and $q \in Q$, we have

$$(\eta_M \circ \omega_M)(m \otimes_{^*\mathcal{C}} q) = \theta_M(m \cdot q) = m \cdot q \otimes_{^*\mathcal{C}} \Lambda = m \otimes_{^*\mathcal{C}} q\#\Lambda = m \otimes_{^*\mathcal{C}} q,$$

where we used the fact that $q\#\Lambda = q$. Indeed, for all $c \in \mathcal{C}$:

$$(q\#\Lambda)(c) = \Lambda(c_{(1)}q(c_{(2)})) = \Lambda(q(c)x) = q(c)\Lambda(x) = q(c).$$

$3) \Longrightarrow 1)$. It suffices to observe that $\tau = \omega_A$. □

Proposition 4.6.9 *For all $M \in \mathcal{M}^{\mathcal{C}}$, we have that $M^{\mathrm{co}\mathcal{C}} \subset M^{*\mathcal{C}}$. If τ is surjective, then $M^{*\mathcal{C}} = M^{\mathrm{co}\mathcal{C}}$.*

Proof. Take $m \in M^{\mathrm{co}\mathcal{C}}$. Then $\rho(m) = m \otimes_A x$, hence $m \cdot f = mf(x)$, for all $f \in {}^*\mathcal{C}$.
Conversely, assume that τ is surjective. Then there exists $\Lambda \in Q$ such that $\Lambda(x) = 1$. Take $m \in M^{*\mathcal{C}}$. Then

$$m = m\Lambda(x) = m \cdot \Lambda = m_{[0]}\Lambda(m_{[1]}),$$

hence

$$\begin{aligned}
\rho(m) &= \rho(m_{[0]}\Lambda(m_{[1]})) \\
&= m_{[0]} \otimes_A m_{[1]}\Lambda(m_{[2]}) \\
&= m_{[0]} \otimes_A \Lambda(m_{[1]})x \ \ (\text{since } \Lambda \in Q) \\
&= m_{[0]}\Lambda(m_{[1]}) \otimes_A x = m \otimes_A x
\end{aligned}$$

hence $m \in M^{\mathrm{co}\mathcal{C}}$. $\square$

Proposition 4.6.10 *We have that*

$$Q \subset Q' = \{q \in {}^*\mathcal{C} \mid q\#f = q\#i(f(x)),\ \text{for all } f \in {}^*\mathcal{C}\}.$$

If $\mathcal{C} \in {}_A\mathcal{M}$ is finitely generated projective, then $Q = Q'$.

Proof. Take $q \in Q$. Then $c_{(1)}q(c_{(2)}) = q(c)x$, for all $c \in \mathcal{C}$, hence

$$(q\#f)(c) = f(c_{(1)}q(c_{(2)})) = f(q(c)x) = q(c)f(x) = (q\#i(f(x)))(c),$$

and it follows that $q \in Q'$.
Conversely, assume that $\mathcal{C} \in {}_A\mathcal{M}$, and take a dual basis $\{(c_j, f_j) \mid j = 1, \cdots, n\}$ of $\mathcal{C}$. If $q \in Q'$, then

$$\begin{aligned}
c_{(1)}q(c_{(2)}) &= \sum_j f_j(c_{(1)}q(c_{(2)}))c_j \\
&= \sum_j (q\#f_j)(c)c_j \\
&= \sum_j (q\#i(f_j(x)))(c)c_j \\
&= \sum_j f_j(q(c)x)c_j = q(c)x.
\end{aligned}$$

$\square$

We have a pair of adjoint functors $(F = - \otimes_B A, G = (-)^{\mathrm{co}\mathcal{C}})$ between $\mathcal{M}_B$ and $\mathcal{M}^{\mathcal{C}}$ (see the end of Section 4.2).
We also have a pair of functors $(\tilde{F} = - \otimes_B A, \tilde{G} = -\otimes_{^*\mathcal{C}})$ between $\mathcal{M}_B$ and $\mathcal{M}_{^*\mathcal{C}}$. $(\tilde{F}, \tilde{G})$ is an adjoint pair if τ is surjective (see Theorem 4.5.26)).

If $\mathcal{C} \in {}_A\mathcal{M}$ is finitely generated projective, then the categories $\mathcal{M}^{\mathcal{C}}$ and $\mathcal{M}_{^*\mathcal{C}}$ are isomorphic. If, moreover, τ is surjective, then $G(M) = \tilde{G}(M)$, for all $M \in \mathcal{M}^{\mathcal{C}} \cong \mathcal{M}_{^*\mathcal{C}}$.

$$\begin{tikzcd}
\mathcal{M}_B \arrow[r, shift left, "F"] \arrow[d, "="'] & \mathcal{M}^{\mathcal{C}} \arrow[l, shift left, "G"] \arrow[d, "\cong"] \\
\mathcal{M}_B \arrow[r, shift left, "\tilde{F}"] & \mathcal{M}_{^*\mathcal{C}} \arrow[l, shift left, "\tilde{G}"]
\end{tikzcd} \tag{4.17}$$

This proves the following.

Proposition 4.6.11 *If $\mathcal{C} \in {}_A\mathcal{M}$ is finitely generated projective and τ is surjective, then $(\tilde{F}, \tilde{G})$ is a pair of inverse equivalences (i.e. the Morita context associated to $(\mathcal{C}, x)$ is strict) if and only if (F, G) is a pair of inverse equivalences.*

We now consider the Sweedler canonical coring $\mathcal{D} = A \otimes_B A$. We assume that $A \in {}_B\mathcal{M}$ is faithfully flat, and compute the Morita context associated to $(\mathcal{D}, 1 \otimes_B 1)$.

It follows from Proposition 4.3.2 that $\eta_B : \ B \to A^{\mathrm{co}\mathcal{D}} = \{b \in A \mid b \otimes_B 1 = 1 \otimes_B b\}$ is bijective.

Recall from Lemma 4.6.1 that we have an isomorphism of A-rings

$$\lambda : \ {}^*\mathcal{D} = {}_A\mathrm{Hom}(A \otimes_B A, A) \to S = {}_B\mathrm{End}(A)^{\mathrm{op}}, \ \ \lambda(\phi)(a) = \phi(1 \otimes_B a).$$

We will write $\lambda(\phi) = \varphi$.

We first show that

$$\lambda(Q) = \tilde{Q} = {}_B\mathrm{Hom}(A, B).$$

Indeed, take $q \in Q$, and let $\tilde{q} = \lambda(q)$. Then for all $a, a' \in A$, we have

$$a' \otimes_B q(1 \otimes_B a) = (a' \otimes_B 1)q(1 \otimes_B a) = q(a' \otimes_B a)(1 \otimes_B 1) = q(a' \otimes_B a) \otimes_B 1.$$

Take $a = 1$. Then we find

$$1 \otimes_B \tilde{q}(a) = \tilde{q}(a) \otimes_B 1,$$

hence $\tilde{q}(a) \in B$, and $\tilde{q} : \ A \to B$.

A is a $(B, {}^*\mathcal{D})$-bimodule (Lemma 4.6.4), hence A is also a (B, S)-bimodule, with right S-action

$$a \cdot \varphi = a \cdot \phi = \phi(1 \otimes_B a) = \varphi(a).$$

Q is a $({}^*\mathcal{D}, B)$-bimodule (Lemma 4.6.3), hence $\tilde{Q} = {}_B\mathrm{Hom}(B, A)$ is an $(S = {}_B\mathrm{End}(A)^{\mathrm{op}}, B)$-bimodule. We compute the left S-action and the right B-action:

$$\varphi \cdot \tilde{q} = \lambda(\phi \# q) = \tilde{q} \circ \varphi$$

$$\tilde{q} \cdot b = \lambda(q \# i(b))$$

Now

$$(q\#i(b))(a' \otimes_B a) \overset{(4.6)}{=} q(a' \otimes_B a)b,$$

hence

$$(\tilde{q} \cdot b)(a) = q(a)b.$$

We have a (B, B)-bimodule map

$$\tilde{\tau} = \tau \circ (A \otimes \lambda^{-1}) : \ A \otimes_S \tilde{Q} \to A \otimes_{{}^*\mathcal{D}} Q \to B.$$

We compute that

$$\tilde{\tau}(a \otimes \tilde{q}) = \tau(a \otimes q) = q(1 \otimes a) = \tilde{q}(a).$$

We have an (S, S)-bimodule map

$$\tilde{\mu} = \lambda \circ \mu \circ (\lambda^{-1} \otimes A) : \ \tilde{Q} \otimes_B A \to Q \otimes_B A \to {}^*\mathcal{D} \to S.$$

We compute that

$$\begin{aligned} \tilde{\mu}(\tilde{q} \otimes_B a)(a') &= \lambda(\mu(q \otimes a))(a') = \mu(q \otimes a)(1 \otimes a') \\ &= (q\#i(a))(1 \otimes a') \overset{(4.6)}{=} q(1 \otimes a')a = \tilde{q}a' \end{aligned}$$

We then obtain a Morita context $(B, {}_B\mathrm{End}(A)^{\mathrm{op}}, A, {}_B\mathrm{Hom}(A, B), \tilde{\tau}, \tilde{\mu})$, that is isomorphic to the Morita context $(B, {}^*\mathcal{D}, A, Q, \tau, \mu)$ associated to $(\mathcal{D}, 1 \otimes_B 1)$. This Morita context is precisely the Morita context associated to the left B-module A. From Proposition 4.5.3, it follows that this Morita context is strict if and only if A is a left B-progenerator.

Proposition 4.6.12 *Let $i : B \to A$ be a ring morphism, and assume that $A \in {}_B\mathcal{M}$ is faithfully flat. Then the Morita context associated to the coring $(A \otimes_B A, 1 \otimes_B 1)$ is isomorphic to the Morita context associated to A considered as a left B-module. This Morita context is strict if and only if A is a left B-progenerator.*

Proposition 4.6.13 *Let $i : B \to A$ be a ring morphism. If $A \in {}_B\mathcal{M}$ is faithfully flat, and $\mathcal{D} = A \otimes_B A \in {}_A\mathcal{M}$ is a progenerator, then $A \in {}_B\mathcal{M}$ is a progenerator.*

Proof. Consider the diagram

$$\begin{tikzcd} \mathcal{M}_B \arrow[r, "K"] \arrow[d, "="'] & \mathcal{M}^{\mathcal{D}} \arrow[d] \\ \mathcal{M}_B \arrow[r, "\tilde{K}"] & \mathcal{M}_{{}^*\mathcal{D}} \cong \mathcal{M}_{{}_B\mathrm{End}(A)^{\mathrm{op}}} \end{tikzcd}$$

The functor $\mathcal{M}^{\mathcal{D}} \to \mathcal{M}_{{}^*\mathcal{D}}$ is an isomorphism of categories, since $\mathcal{D}$ is a left A-progenerator. $K = - \otimes_B A$ is an equivalence of categories (by Proposition 4.3.2 and because $A \in {}_B\mathcal{M}$ is faithfully flat. Then $\tilde{K} = - \otimes_B A$ is also an equivalence of categories, and then $A \in {}_B\mathcal{M}$ is a progenerator. □

Theorem 4.6.14 *Let $(\mathcal{C}, x)$ be an A-coring with a fixed grouplike element. We assume that $\mathcal{C}$ is a left A-progenerator. Let $B = A^{\mathrm{co}\mathcal{C}}$ and $i : B' \to B$ a ring morphism. Let $\mathcal{D}' = A \otimes_{B'} A$, and* $\mathrm{can}' : \mathcal{D}' \to \mathcal{C}$, $\mathrm{can}'(a \otimes_{B'} a') = axa'$. *Then the following assertions are equivalent.*

1. • can' *is an isomorphism (of A-corings);*
• *A is faithfully flat as a left B'-module;*

2. • ${}^*\mathrm{can}'$ *is an isomorphism (of A-rings);*
• *A is a left B'-progenerator;*

3. • $i: B \to B'$ *is an isomorphism (hence we can take $B = B'$);*
• *the Morita context associated to $(\mathcal{C}, x)$ is strict;*

4. • $i: B \to B'$ *is an isomorphism;*
• *the adjunction (F, G) between $\mathcal{M}_B$ and $\mathcal{M}^{\mathcal{C}}$ is a pair of inverse equivalences.*

Proof. $\underline{1) \Longrightarrow 2)}$. If can' is an isomorphism, then its dual map ${}^*\mathrm{can}'$ is also an isomorphism. Since $\mathrm{can}'\ \mathcal{D}' \to \mathcal{C}$ is an isomorphism of corings, and hence of left A-modules, $\mathcal{D}'$ is a left A-progenerator, and it follows from Proposition 4.6.13 that A is a left B'-progenerator.

$\underline{1) \Longrightarrow 3)}$. We have that

$$B = A^{\mathrm{co}\mathcal{C}} = A^{\mathrm{co}\mathcal{D}'} = B'.$$

The second equality follows from the fact that $\mathcal{C}$ and $\mathcal{D}'$ are isomorphic A-corings, and the third equality from the fact that $A \in {}_{B'}\mathcal{M}$ is faithfully flat.
Since A is a left B-progenerator, the Morita context associated to $(\mathcal{D}, 1 \otimes_B 1)$ is strict (see Proposition 4.6.12). Since $\mathcal{C}$ and $\mathcal{D}$ are isomorphic corings, the Morita contexts associated to $(\mathcal{C}, x)$ and $(\mathcal{D}, 1 \otimes_B 1)$ are isomorphic, hence The Morita context associated to $(\mathcal{C}, x)$ is strict.

$\underline{3) \Longrightarrow 4)}$. The Morita context $(B, {}^*\mathcal{C}, A, Q, \tau, \mu)$ associated to $(\mathcal{C}, x)$ is strict, and it follows from Theorem 4.5.2 that A is a left B-progenerator, and then from Corollary 4.5.6 that A is faithfully flat as a left B-module.
It follows from Proposition 4.6.11 that (F, G) is a pair of inverse equivalences.

$\underline{4) \Longrightarrow 1)}$. It follows from Proposition 4.4.1 that $\mathrm{can} = \mathrm{can}'$ is an isomorphism. Since $\mathcal{C} \in {}_A\mathcal{M}$ is finitely generated projective, $\mathcal{M}^{\mathcal{C}} \cong \mathcal{M}_{{}^*\mathcal{C}}$. Since $- \otimes_B A:\ {}_B\mathcal{M} \to \mathcal{M}^{\mathcal{C}}$ is an equivalence, A is a left B-progenerator, and it follows from Corollary 4.5.6 that A is faithfully flat as a left B'-module.
□

4.7 Hopf-Galois extensions

Let H be a Hopf algebra with a bijective antipode, and A a right H-comodule algebra. Recall (see Example 4.2.4) that $\mathcal{C} = A \otimes H$ is an H-coring. $x = 1_A \otimes 1_H$ is a grouplike element of $A \otimes H$. This makes A into a right $A \otimes H$-comodule, and the $A \otimes H$-coaction coincides with the right H-action in the following sense: $\rho:\ A \to A \to_A A \otimes H \cong A \otimes H$, $\rho(a) = a_{[0]} \otimes_A (1 \otimes a_{[1]} \cong a_{[0]} \otimes a_{[1]}$. Then

$$A^{\mathrm{co}A \otimes H} = \{a \in A \mid \rho(a) = a \otimes 1_H\}.$$

Definition 4.7.1 *A is called a Hopf-Galois extension of B if $(A\otimes H, 1_A\otimes 1_H)$ is a Galois coring, or, equivalently,*

$$\mathrm{can}:\ A\otimes_B A\to A\otimes H,\ \ \mathrm{can}(a\otimes_B a')=a(1_A\otimes 1_H)a'=aa'_{[0]}\otimes a'_{[1]}$$

is an isomorphism of corings.

Proposition 4.4.5 then specifies to the following result.

Proposition 4.7.2 *Let A be right H-comodule algebra, and $B=A^{\mathrm{co}H}$. Assume that A is flat as a left B-module. Then the following statements are equivalent.*

1. *A is a Hopf-Galois extension of B and A is faithfully flat as a left B-module;*
2. *$(F=-\otimes_B A, G=(-)^{\mathrm{co}H}$ is a pair of inverse equivalences between $\mathcal{M}_B$ and the category of relative Hopf modules $\mathcal{M}_A^H$.*

Let A be a right H-module algebra. The *smash product* $H\#A$ is defined as follows: as a k-module, it is equal to $H\otimes A$, with multiplication given by the formula

$$(h\#a)(k\#b)=hk_{(1)}\#(a\cdot k_{(2)})b.$$

A straightforward computation shows that this is an associative multiplication. $1_H\#1_A$ is a unit for this multiplication, so $H\#A$ is a k-algebra. The maps

$$A\to H\#A,\ \ a\mapsto 1_H\#a\ \ ;\ \ H\to H\#A,\ \ h\mapsto h\#1_A$$

are algebra morphisms.

Now we assume that H is a k-progenerator, and let A be a right H-comodule algebra. Then $A\otimes H$ is a left A-progenerator. Let $\{(h_i,h_i^*)\mid i=1,\cdots,n\}$ be a finite dual basis for H. A is a right H-comodule algebra, hence it is a left H^*-module algebra, and a right $(H^*)^{\mathrm{op}}$-module algebra, and we can consider the smash product $(H^*)^{\mathrm{op}}\#A$. We have isomorphisms of k-modules

$$H^*\otimes A\to \mathrm{Hom}(H,A)\to {}_A\mathrm{Hom}(A\otimes H,A).$$

The composition of these two compositions will be called α. Then we have

$$\alpha(h^*\otimes a)(a'\otimes b)=\langle h^*,h\rangle a'a.$$

Proposition 4.7.3 *$\alpha:\ (H^*)^{\mathrm{op}}\#A\to {}_A\mathrm{Hom}(A\otimes H,A)$ is an isomorphism of A-rings.*

Proof. Take $h^*,k^*\in H^*$, $a,b\in A$. Let $\varphi=\alpha(h^*\#a)$, $\psi=\varphi(k^*\#b)$. Then

$$(h^*\#a)(k^*\#b)=k^*_{(1)}*h^*\#(a\cdot k^*_{(2))})b=k^*_{(1)}*h^*\#\langle k^*_{(2)},a_{[1]}\rangle a_{[0]}b,$$

hence

$$\begin{aligned}\alpha((h^*\#a)(k^*\#b))(a'\otimes h)&=\langle k^*_{(1)}*h^*,h\rangle\langle k^*_{(2)},a_{[1]}\rangle a'a_{[0]}b\\ &=\langle k^*_{(1)},h_{(1)}\rangle\langle h^*,h_{(2)}\rangle\langle k^*_{(2)},a_{[1]}\rangle a'a_{[0]}b\\ &=\langle k^*,h_{(1)}a_{[1]}\rangle\langle h^*,h_{(2)}\rangle a'a_{[0]}b.\end{aligned}$$

$$\begin{aligned}(\varphi\#\psi)(a'\otimes h) &= \psi((a'\otimes h_{(1)})\varphi(1\otimes h_{(2)}))\\ &= \psi((a'\otimes h_{(1)})\langle h^*, h_{(2)}\rangle a)\\ &= \psi(\langle h^*, h_{(2)}\rangle a'a_{[0]}\otimes h_{(1)}a_{[1]})\\ &= \langle h^*, h_{(2)}\rangle\langle k^*, h_{(1)}a_{[1]}\rangle a'a_{[0]}b,\end{aligned}$$

and it follows that α preserves the multiplication. Now let us also show that α respects the algebra morphisms

$$i:\ A\to {}_A\mathrm{Hom}(A\otimes H, A),\ \ i(a)(a'oth)=\varepsilon_{\mathcal{C}}(a'\otimes h)a=\varepsilon(h)a'a;$$

$$i':\ A\to (H^*)^{\mathrm{op}}\#A,\ \ i'(a)=\varepsilon\#a.$$

indeed,

$$\alpha'(i(a))(a'\otimes h)=\alpha(\varepsilon\#a)(a'\#h)=\varepsilon(h)a'a=i(a)(a'\otimes h).$$

so $\alpha\circ i'=i$, as needed. □

Recall that the dual of the map $\mathrm{can}:\ A\otimes_B A\to\mathcal{C}=A\otimes H$ is

$${}^*\mathrm{can}:\ {}^*\mathcal{C}={}_A\mathrm{Hom}(A\otimes H, A)\to {}_A\mathrm{Hom}(A\otimes_B A, A)={}_B\mathrm{End}(A)^{\mathrm{op}},$$

given by

$${}^*\mathrm{can}(f)(a')=f(xa')=f(a'_{[0]}\otimes a'_{[1]}).$$

Let us compute

$${}^*\widetilde{\mathrm{can}}={}^*\mathrm{can}\circ\alpha:\ (H^*)^{\mathrm{op}}\#A\to {}_B\mathrm{End}(A)^{\mathrm{op}}.$$

$${}^*\widetilde{\mathrm{can}}(h^*\#a)(a')=\alpha(h^*\#a)(a'_{[0]}\otimes a'_{[1]})=\langle h^*, a'_{[1]}\rangle a'_{[0]}a=(a'\cdot h^*)a.$$

Recall from Proposition 4.6.10 that

$$Q=Q'=\{q\in {}^*\mathcal{C}\mid q\#f=q\#i(f(x)),\ \text{for all}\ f\in {}^*\mathcal{C}\}.$$

We compute $\hat{Q}=\alpha^{-1}(Q)\subset (H^*)^{\mathrm{op}}\#A$.

$$\begin{aligned} y=\sum_i h_i^*\#a_i\in\hat{Q}\ &\Longleftrightarrow\ q=\alpha(y)\in Q'=Q\\ &\Longleftrightarrow\ q\#f=q\#i(f(x)),\ \ \forall f\in {}^*\mathcal{C}\\ &\Longleftrightarrow\ y(h^*\#a)=yi'(\langle h^*,1\rangle a),\ \ \forall h^*\in H^*, a\in A\\ &\Longleftrightarrow\ (\sum_i h_i^*\#a_i)(h^*\#a)=(\sum_i h_i^*\#a_i)(\varepsilon\#\langle h^*,1\rangle a)\\ &\Longleftrightarrow\ \sum_i h^*_{(1)}*h_i^*\#\langle h^*_{(2)}, a_{i[1]}\rangle a_{i[0]}a=\sum_i h_i^*\#\langle h^*,1\rangle a_i a,\ \ \forall h^*\in H^*, a\in A\\ &\Longleftrightarrow\ \sum_i h^*_{(1)}*h_i^*\#\langle h^*_{(2)}, a_{i[1]}\rangle a_{i[0]}=\sum_i h_i^*\#\langle h^*,1\rangle a_i,\ \ \forall h^*\in H^*\\ &\Longleftrightarrow\ y(h^*\#1)=\langle h^*,1\rangle y,\ \ \forall h^*\in H^*.\end{aligned}$$

We conclude that

$$\hat{Q} = \{y \in (H^*)^{\mathrm{op}}\#A \mid y(h^*\#1) = \langle h^*, 1\rangle y,\ \ \forall h^* \in H^*\}.$$

Consider the maps

$$\hat{\tau} = \tau \circ (A \otimes \alpha) :\ A\#_{(H^*)^{\mathrm{op}}\#A}\hat{Q} \to A \otimes_{^*\mathcal{C}} Q \to B,\ \tau(a \otimes y) = {}^*\widetilde{\mathrm{can}}(y)(a);$$

$$\hat{\mu} = \mu \circ (\alpha \otimes A) :\ \hat{Q} \otimes_B A \to Q \otimes_B A \to B,\ \mu(y \otimes a) = y(\varepsilon\#a).$$

Then $(B, (H^*)^{\mathrm{op}}\#A, A, \hat{Q}, \hat{\tau}, \hat{\mu})$ is a Morita context.

Applying Theorem 4.6.14, we now obtain the following result.

Theorem 4.7.4 *Let H be a Hopf algebra, and assume that H is a progenerator as a k-module. Let A be a right H-comodule algebra, $B = A^{\mathrm{co}H}$, $i :\ B' \to B$ a ring morphism. Then the following assertions are equivalent.*

1.
   - $\mathrm{can}' :\ A \otimes_{B'} A \to A \otimes H,\ \ \mathrm{can}'(a' \otimes_B a) = a'a_{[0]} \otimes a_{[1]}$ *is bijective;*
   - *A is faithfully flat as a left B'-module.*
2.
   - ${}^*\widetilde{\mathrm{can}}' :\ (H^*)^{\mathrm{op}}\#A \to {}_{B'}\mathrm{End}(A)^{\mathrm{op}},\ \ {}^*\widetilde{\mathrm{can}}'(h^*\#a)(b) = (h^*\rightharpoonup b)a$ *is an isomorphism;*
   - *A is a left B'-progenerator.*
3.
   - *$B = B'$;*
   - *the Morita context $(B, (H^*)^{\mathrm{op}}\#A, A, \hat{Q}, \hat{\tau}, \hat{\mu})$ is strict.*
4.
   - *$B = B'$;*
   - *the adjoint pair of functors $(F = \bullet \otimes A, G = (\bullet)^{\mathrm{co}H})$ is an equivalence between the categories $\mathcal{M}_B$ and $\mathcal{M}_A^H$.*

In Theorem 4.7.4, we can take $B' = k$. If the equivalent conditions of Theorem 4.7.4 are satisfied, then $A^{\mathrm{co}H} = k$; then we say that A is an H-*Galois object.*

4.8 Strongly graded rings

As in Example 4.2.3, let G be a group, and A a G-graded ring, and $\mathcal{C} = \oplus_{\sigma\in G}Au_\sigma$. Fix $\lambda \in G$, and take the grouplike element $u_\lambda \in G(\mathcal{C})$. Then $M^{\mathrm{co}\mathcal{C}} = M_\lambda$, for any right G-graded A-module, and $B = A^{\mathrm{co}\mathcal{C}} = A_e$. Also

$$\mathrm{can} :\ A \otimes_B A \to \oplus_{\sigma\in G}Au_\sigma,\ \ \mathrm{can}(a' \otimes a) = \sum_{\sigma\in G} a'a_\sigma u_{\lambda\sigma}.$$

Proposition 4.8.1 *With notation as above, the following assertions are equivalent.*

1. *A is strongly G-graded, that is, $A_\sigma A_\tau = A_{\sigma\tau}$, for all $\sigma, \tau \in G$;*

2. *the pair of adjoint functors $(F = \bullet \otimes_B A, G = (\bullet)_\lambda)$ is an equivalence between $\mathcal{M}_B$ and $\mathcal{M}_A^G$, the category of G-graded right A-modules;*

3. *$(\mathcal{C}, u_\lambda)$ is a Galois coring.*

In this case A is faithfully flat as a left (or right) B-module.

Proof. $\underline{1) \Rightarrow 2)}$ is a well-known fact from graded ring theory. We sketch a proof for completeness sake. The unit of the adjunction between $\mathcal{M}_B$ and $\mathcal{M}_A^G$ is given by

$$\eta_N : \; N \to (N \otimes_B A)_\lambda, \;\; \eta_N(n) = n \otimes_B 1_A.$$

η_N is always bijective, even if A is not strongly graded. Let us show that the counit maps $\zeta_M : M_\lambda \otimes_B A \to M$, $\zeta_M(m \otimes_B a) = ma$ are surjective. For each $\sigma \in G$, we can find $a_i \in A_{\sigma^{-1}}$ and $a_i' \in A_\sigma$ such that $\sum_i a_i a_i' = 1$. Take $m \in M_\tau$ and put $\sigma = \lambda^{-1}\tau$. Then $m = \zeta_M(\sum_i m a_i \otimes_B a_i')$, and ζ_M is surjective.
If $m_j \in M_\lambda$ and $c_j \in A$ are such that $\sum_j m_j c_j = 0$, then for each $\sigma \in G$, we have

$$\sum_j m_j \otimes c_{j\sigma} = \sum_{i,j} m_j \otimes c_{j\sigma} a_i a_i' = \sum_{i,j} m_j c_{j\sigma} a_i \otimes a_i' = 0.$$

hence $\sum_j m_j \otimes c_j = \sum_{\sigma \in G} = \sum_j m_j \otimes c_{j\sigma} = 0$, so ζ_M is also injective.
$\underline{2) \Rightarrow 3)}$ follows from Proposition 4.4.1.
$\underline{3) \Rightarrow 1)}$. Take $a \in A_{\sigma\tau}$ Since can is a bijection, there exist $a_i', a_i \in A$ such that

$$a u_{\lambda\tau} = \mathrm{can}(\sum_i a_i' \otimes a_i) = \sum_{\rho \in G} \sum_i a_i' (a_i)_\tau u_{\lambda\rho}.$$

This implies that

$$\sum_i a_i'(a_i)_\tau = a.$$

Since the right hand side is homogeneous of degree $\sigma\tau$, the left hand side is also homogeneous of degree $\sigma\tau$, and therefore equal to its homogeneous part of degree $\sigma\tau$:

$$a = \sum_i (a_i')_\sigma (a_i)_\tau \in A_\sigma A_\tau.$$

We prove the final statement as follows. We knwo from 2) that the counit map

$$\zeta_A : \; A_\lambda \otimes_B A \to A$$

is an isomorphism. For every $\sigma \in G$, it restricts to an isomorphism $A_\lambda \otimes_B A_\sigma \to A_{\lambda\sigma}$. We consider the isomorphisms

$$f : \; A_\lambda \otimes_B A_{\lambda^{-1}} \to A_e = B \;\text{ and }\; g : \; A_{\lambda^{-1}} \otimes_B A_\lambda \to A_e = B.$$

These are part of a strict Morita context $(B, B, A_\lambda, A_{\lambda^{-1}}, f, g)$. It follows from Theorem 4.5.2 that every A_λ is a progenerator as a (left and right) B-module, and hence, by Corollary 4.5.6, that A_λ is faithfully flat as a (left and right) B-module. Then $A = \bigoplus_{\lambda \in G} A_\lambda$ is also faithfully flat. □

Notice that, in this situation, the fact that $(\mathcal{C}, u_\lambda)$ is Galois is independent of the choice of λ.

4.9 Classical Galois theory

Let G be a finite group, and A a left G-module algebra. We consider the A-coring $\mathcal{C} = \bigoplus_{\sigma\in G} Av_\sigma$ from Example 4.2.2. Recall the formulas

$$v_\sigma a = \sigma(a)v_\sigma \;\; ; \;\; \Delta(v_\sigma) = \sum_\lambda v_\lambda \otimes v_{\lambda^{-1}\rho}.$$

We also have that $x = \sum_{\sigma\in G} v_\sigma \in G(\mathcal{C})$ is a grouplike element. Recall that the category $\mathcal{M}^{\mathcal{C}}$ is isomorphic to the category of right A-modules on which G acts as a group of right A-semilinear automorphisms. For $m \in \mathcal{M}^{\mathcal{C}}$, we have

$$\begin{aligned} m \in M^{\mathrm{co}\mathcal{C}} &\iff \rho(m) \sum_{\sigma\in G} \sigma(m) \otimes v_\sigma = m \otimes \sum_\sigma \in G v_\sigma \\ &\iff \sigma(m) = m,\ \forall \sigma \in G \iff m \in M^G. \end{aligned}$$

We conclude that $M^{\mathrm{co}\mathcal{C}} = M^G$, the submodule of G-invariants. In particular, we have that $B = A^G$. We will apply Theorem 4.6.14 in this situation, in the particular case where $B' = k$. First we compute the canonical map

$$\mathrm{can}' :\; A \otimes A \to \bigoplus_{\sigma\in G} Av_\sigma.$$

$$\mathrm{can}'(a\otimes a') = \sum_{\sigma\in G} av_\sigma a' = \sum_{\sigma\in G} a\sigma(a')v_\sigma.$$

Our next aim is to compute ${}^*\mathcal{C}$.

Proposition 4.9.1 *${}^*\mathcal{C} \cong \bigoplus_{\sigma\in G} u_\sigma A$ is the free right A-module with basis $\{u_\sigma \mid \sigma \in G\}$ and multiplication rule*

$$(u_\sigma a)(u_\tau a') = u_{\tau\sigma}\tau(a)b. \tag{4.18}$$

Proof. For every $\tau \in G$, we consider the projection

$$p_\tau :\; \bigoplus_{\sigma\in G} Av_\sigma \to A,\;\; p_\tau(\sum_{\sigma\in G} a_\sigma v_\sigma = a_\tau.$$

It is clear that $p_\tau \in {}^*\mathcal{C} = {}_A\mathrm{Hom}(\bigoplus_{\sigma\in G} Av_\sigma, A)$. Using (4.5), we find that

$$(p_\sigma \# p_\tau)(av_\rho) = \sum_\lambda p_\tau(av_\lambda p_\sigma(v_{\lambda^{-1}\rho})) = p_\tau(av_{\rho\sigma^{-1}}) = \delta_{\tau\sigma,\rho}a = p_{\tau\sigma}(av_\rho),$$

hence

$$p_\sigma \# p_\tau = p_{\tau\sigma}. \tag{4.19}$$

For $a \in A$, $i(a) :\; \mathcal{C} \to A$ is given by

$$i(a)(\sum_{\sigma\in G} a_\sigma v_\sigma) = \varepsilon(\sum_{\sigma\in G} a_\sigma v_\sigma)a = a_e a.$$

Using (4.6), we compute

$$(i(a)\#p_\sigma)(a'v_\rho) = p_\sigma(a'v_\rho a) = p_\sigma(a'\rho(a)v_\rho) = a'\sigma(a)\delta_{\rho\sigma} = p_\sigma(a'v_\rho)\sigma(a) = (p_\sigma\#i(\sigma(a)))(a'v_\rho),$$

hence

$$i(a)\#p_\sigma = p_\sigma\#i(\sigma(a)). \tag{4.20}$$

This shows that

$$\alpha : \bigoplus_{\sigma\in G} u_\sigma A \to {}^*\mathcal{C},\ \alpha(u_\sigma a) = p_\sigma\#i(a)$$

is an algebra homomorphism. For $f \in {}^*\mathcal{C}$, we have

$$f(av_\tau) = af(v_\tau) = \sum_{\sigma\in G} p_\sigma(av_\tau)f(v_\sigma) \overset{(4.6)}{=} \sum_{\sigma\in G}(p_\sigma\#i(f(v_\sigma)))(av_\tau),$$

hence

$$f = \sum_{\sigma\in G}(p_\sigma\#i(f(v_\sigma))) = \alpha(\sum_{\sigma\in G} u_\sigma f(v_\sigma)),$$

and it follows that f is surjective. f is also injective: suppose that

$$\alpha(\sum_{\sigma\in G} u_\sigma a_\sigma) = \sum_{\sigma\in G} p_\sigma\#i(a_\sigma) = 0,$$

then

$$0 = (\sum_{\sigma\in G} p_\sigma\#i(a_\sigma))(v_\rho) = \sum_{\sigma\in G} p_\sigma(v_\sigma)a_\rho,$$

for all $\rho \in G$, hence $\sum_{\sigma\in G} u_\sigma a_\sigma = 0$. □

We can now easily compute the composition $\gamma = {}^*\mathrm{can}' \circ \alpha :\ \bigoplus_{\sigma\in G} u_\sigma A \to \mathrm{End}(A)^{\mathrm{op}}$:

$$\gamma(u_\sigma a)(a') = (p_\sigma\#i(a))(\sum_{\tau\in G} v_\tau a') = (p_\sigma\#i(a))(\sum_{\tau\in G} \tau(a')v_\tau) = \sigma(a')a.$$

Proposition 4.9.2 $\alpha^{-1}(Q) = \{\sum_{\sigma\in G} u_\sigma\sigma(a) \mid a \in A\}$.

Proof. Take $q \in Q$. We know from the proof of Proposition 4.9.1 that $q = \sum_{\tau\in G} p_\tau\#i(a_\tau)$, with $a_\tau = q(v_\tau)$, and $\alpha^{-1}(q) = \sum_{\tau\in G} u_\tau a_\tau$. Fix $\sigma \in G$. Since $q \in Q$, we know that

$$q(v_\sigma)x = \sum_{\rho\in G} a_\sigma v_\rho$$

equals

$$(v_\sigma)_{(1)}q((v_\sigma)_{(2)}) = \sum_{\rho,\tau\in G} v_\rho(p_\tau(v_{\rho^{-1}\sigma})a_\tau = \sum_\rho v_\rho a_{\rho^{-1}\sigma} = \sum_\rho \rho(a_{\rho^{-1}\sigma})v_\rho.$$

This implies that $a_\sigma = \rho(a_{\rho^{-1}\sigma})$, for all $\rho \in G$. In particular, if we take $\rho = \sigma$, we obtain that $a_\sigma = \sigma(a_e)$. Then $\alpha^{-1}(q) = \sum_{\tau\in G} u_\tau\tau(a_e)$, as needed.

Conversely, let $q = \sum_{\sigma\in G} p_\sigma\#i(\sigma(a)) = \alpha(\sum_{\sigma\in G} u_\sigma\sigma(a)$. Then we prove that $q \in Q$: for all $c = \sum_{\rho\in G} a'_\rho v_\rho \in \mathcal{C}$, we have

$$c_{(1)}q(c_{(2)}) = \sum_{\rho,\tau,\sigma\in G} a'_\rho v_\tau p_\sigma(v_{\tau^{-1}\rho})\sigma(a) = \sum_{\rho,\tau\in G} a'_\rho v_\tau(\tau^{-1}\rho)(a) = \sum_{\rho,\tau\in G} a'_\rho \rho(a)v_\tau;$$

$$q(c)x = (\sum_{\sigma,\rho\in G} a'_\rho p_\sigma(v_\rho)\sigma(a))x = (\sum_{\rho\in G} a'_\rho\rho(x))(\sum_{\tau\in G} v_\tau) = \sum_{\rho,\tau\in G} a'_\rho\rho(a)v_\tau.$$

□

It follows from Propositions 4.9.1 and 4.9.2 that we have a k-linear isomorphism

$$\lambda:\ A \to Q,\ \ \lambda(a) = \sum_{\sigma\in G} p_\sigma\#i(\sigma(a)).$$

The $({}^*\mathcal{C}, B)$-bimodule structure on Q can be transported into a $(\bigoplus_{\sigma\in G} u_\sigma A, B)$-bimodule structure on A. The right B-action is given by multiplication. The left action by $\bigoplus_{\sigma\in G} u_\sigma A$ is given by the formula

$$(u_\tau a)\cdot a' = \tau^{-1}(aa').$$

Indeed,

$$(p_\tau\#i(a))\lambda(a') = \sum_\sigma (p_\tau\#i(a))(p_\sigma\#i(\sigma(a'))) = \sum_{\sigma\in G} u_{\sigma\tau}\#i(\sigma(aa'))$$

equals

$$\lambda(\tau^{-1}(aa')) = \sum_{\rho\in G}(\rho\tau^{-1})(aa').$$

On the other hand, we know that A is also a $(B, {}^*\mathcal{C})$-module. Hence it is also a $(B, \bigoplus_{\sigma\in G} u_\sigma A)$-bimodule. The left B-action is given by multiplication. Let us compute the right action by $\bigoplus_{\sigma\in G} u_\sigma A$:

$$a'\cdot(u_\sigma a) = (p_\sigma\#i(a))(xa') = \sum_{\tau\in G}(p_\sigma\#i(a))(v_\tau a') = \sum_{\tau\in G} p_\sigma(\tau(a')v_\tau)a = \sigma(a')a.$$

Now we compute the (B, B)-bimodule map

$$\overline{\tau} = \tau\circ(A\otimes\lambda):\ A\otimes_{\bigoplus_{\sigma\in G} u_\sigma A} A \to A\otimes_{{}^*\mathcal{C}} Q \to B.$$

$$\overline{\tau}(a'\otimes a) = \tau\Big(a'\otimes\sum_{\sigma\in G} p_\sigma\#i(\sigma(a))\Big) = \sum_{\sigma\in G}\sigma(a')\sigma(a) = \sigma(a'a).$$

Finally, we have the $(\bigoplus_{\sigma\in G} u_\sigma A, \bigoplus_{\sigma\in G} u_\sigma A)$-bimodule map

$$\overline{\mu} = \alpha^{-1}\circ\mu\circ(\lambda\otimes A):\ A\otimes_B A \to Q\otimes_B A \to {}^*\mathcal{C} \to \bigoplus_{\sigma\in G} u_\sigma A,$$

$$\overline{\mu}(a\otimes a') = \sum_{\sigma\in G} u_\sigma\sigma(a)a'.$$

We conclude that we have a Morita context $(B = A^G, \bigoplus_{\sigma\in G} u_\sigma A, A, A, \overline{\tau}, \overline{\mu})$. From Theorem 4.6.14 we obtain the following result.

Theorem 4.9.3 *Let G be a finite group, k a commutative ring and A a G-module algebra. Then the following statements are equivalent:*

1.
   - $\mathrm{can}' : A \otimes A \to \bigoplus_{\sigma \in G} Av_\sigma$, $\mathrm{can}'(a \otimes a') = \sum_{\sigma \in G} a\sigma(a')v_\sigma$, *is an isomorphism;*
   - *A is faithfully flat as a k-module.*
2.
   - $\gamma : \bigoplus_{\sigma \in G} u_\sigma A \to \mathrm{End}(A)^{\mathrm{op}}$, $\gamma(u_\sigma a)(a') = \sigma(a')a$ *is an isomorphism;*
   - *A is a k-progenerator.*
3.
   - $A^G = k$*;*
   - *the Morita context $(B = A^G, \bigoplus_{\sigma \in G} u_\sigma A, A, A, \overline{\tau}, \overline{\mu})$ is strict.*
4.
   - $A^G = k$*;*
   - *the adjoint pair of functors $(F = \bullet \otimes A, G = (\bullet)^G)$ is a pair of inverse equivalences between the categories of k-modules and right A-modules on which G acts as a group of right A-semilinear automorphisms.*

Theorem 4.9.4 *Let G be a finite group, k a commutative ring and A a commutative faithful G-module algebra. Then the statements of Theorem 4.9.3 are equivalent to*

5.
   - $A^G = k$*;*
   - *for each non-zero idempotent $e \in A$ and $\sigma \neq \tau \in G$, there exists $a \in A$ such that $\sigma(a)e \neq \tau(a)e$;*
   - *A is a separable k-algebra.*
6.
   - $A^G = k$*;*
   - $v_e \in \mathrm{Im}\,(\mathrm{can}')$*; this means that there exist $x_1, \cdots, x_n, y_1, \cdots y_n \in A$ such that*

     $$\sum_{j=1}^{n} x_j \sigma(y_j) = \delta_{\sigma,e} \qquad (4.21)$$

     for all $\sigma \in G$.
7.
   - $A^G = k$*;*
   - can' *is an isomorphism;*
8.
   - $A^G = k$*;*
   - *for each maximal ideal m of A, and for each $\sigma \neq e \in G$, there exists $x \in A$ such that $\sigma(x) - x \notin m$.*

Proof. 5. $\Longrightarrow$ 6. Let $e = \sum_{i=1}^{n} x_i \otimes y_i \in A \otimes A$ be a separability idempotent. Then for all $\sigma \in G$ $\sum_{i=1}^{n} x_\sigma(y_i) \in A$ is an idempotent. For all $a \in A$, we have

$$a \sum_{i=1}^{n} x_\sigma(y_i) = \sum_{i=1}^{n} x_\sigma(y_i a) = \sum_{i=1}^{n} x_\sigma(y_i)\sigma(a) = \sigma(a) \sum_{i=1}^{n} x_\sigma(y_i),$$

and it follows from the second condition in 5. that $\sum_{i=1}^n x_\sigma(y_i) = 0$ if $\sigma \neq e$. We also have that $\sum_{i=1}^n x_i y_i = 1$, and (4.21) follows.

<u>6. $\Longrightarrow$ 1.</u> $(\mathrm{can}')^{-1}$ is given by the formula

$$(\mathrm{can}')^{-1}(av_\tau) = \sum_{i=1}^n a\tau(x_i) \otimes y_i.$$

Indeed,

$$\begin{aligned}
(\mathrm{can}' \circ (\mathrm{can}')^{-1})(av_\tau) &= \mathrm{can}(\sum_{i=1}^n a\tau(x_i) \otimes y_i) \\
&= \sum_{\sigma\in G}\sum_{i=1}^n a\tau(x_i)\sigma(y_i)v_\sigma = a\sum_{\sigma\in G}\tau\Big(\sum_{i=1}^n x_i(\tau^{-1}\sigma)(y_i)\Big)v_\sigma \\
&\overset{(4.21)}{=} a\sum_{\sigma\in G}\tau(\delta_{\tau^{-1}\sigma,e})v_\sigma = av_\tau; \\
((\mathrm{can}')^{-1} \circ \mathrm{can})(a\otimes a') &= (\mathrm{can}')^{-1}(\sum_{\sigma\in G} a\sigma(a')v_\sigma) \\
&= \sum_{i=1}^n\sum_{\sigma\in G} a\sigma(a')\sigma(x_i)\otimes y_i = \sum_{i=1}^n a\sum_{\sigma\in G}\sigma(a'x_i)\otimes y_i \\
&= \sum_{i=1}^n a\sum_{\sigma\in G}\sigma(x_i)\otimes y_i a'_i = \sum_{i=1}^n a\otimes\sum_{\sigma\in G}\sigma(x_i)y_i a'_i \\
&\overset{(4.21)}{=} a\otimes\sum_{\sigma\in G}\delta_{\sigma,e}a'_i = a\otimes a'.
\end{aligned}$$

We used the fact that $\sum_{\sigma\in G}\sigma(a) \in A^G = k$.
Now define $x_i^* \in A^*$ by the formula

$$\langle x_i^*, a\rangle = \sum_{\sigma\in G}\sigma(ay_i) \in A^G = k.$$

For all $a \in A$, we have

$$\sum_{i=1}^n \langle x_i^*, a\rangle x_i = \sum_{i=1}^n\sum_{\sigma\in G}\sigma(ay_i)x_i = \sum_{\sigma\in G}\sigma(a)\sum_{i=1}^n\sigma(ay_i)x_i = \sum_{\sigma\in G}\sigma(a)\delta_{\sigma,e} = a,$$

so $\{(x_i, x_i^*) \mid i = 1, \cdots, n\}$ is a finite dual basis for A, and A is finitely generated and projective. By assumption, A is faithful, hence A is a k-progenerator, and faithfully flat as a k-module.

<u>1. $\Longrightarrow$ 7. $\Longrightarrow$ 6.</u> is obvious.

<u>6. $\Longrightarrow$ 5.</u> In the proof of <u>6. $\Longrightarrow$ 1.</u>, we have seen that

$$\sum_{j=1}^n \tau(x_j)\sigma(y_j) = \delta_{\sigma,\tau} \tag{4.22}$$

$\sum_{i=1}^n x_i\otimes y_i$ is a separability idempotent: first, we have $\sum_{i=1}^n x_iy_i=1$.
Since $\sum_{\sigma\in G}\sigma(ax_iy_j)\in A^G=k$, we have that

$$\sum_{i=1}^n\sum_{j=1}^n\sum_{\sigma\in G}\sigma(ax_iy_j)x_j\otimes y_i=\sum_{i=1}^n\sum_{j=1}^n x_j\otimes\sum_{\sigma\in G}\sigma(ax_iy_j)y_i$$

Now

$$\begin{aligned}\sum_{i=1}^n\sum_{j=1}^n\sum_{\sigma\in G}\sigma(ax_iy_j)x_j\otimes y_i&=\sum_{i=1}^n\sum_{\sigma\in G}\sigma(ax_i)\sum_{j=1}^n\sigma(y_j)x_j\otimes y_i\\ &\overset{(4.21)}{=}\sum_{i=1}^n\sum_{\sigma\in G}\sigma(ax_i)\delta_{\sigma,e}\otimes y_i=\sum_{i=1}^n ax_i\otimes y_i;\\ \sum_{i=1}^n\sum_{j=1}^n x_j\otimes\sum_{\sigma\in G}\sigma(ax_iy_j)y_i&=\sum_{j=1}^n x_j\otimes\sum_{\sigma\in G}\sigma(ay_j)\sum_{i=1}^n\sigma(x_i)y_i\\ &\overset{(4.22)}{=}\sum_{j=1}^n x_j\otimes\sum_{\sigma\in G}\sigma(ay_j)\delta_{\sigma,e}=\sum_{j=1}^n x_j\otimes y_ja;\end{aligned}$$

we find that $\sum_{i=1}^n ax_i\otimes y_i=\sum_{j=1}^n x_j\otimes y_ja$, as needed. Now let $\sigma,\tau\in G$, and assume that $e\neq 0$ is an idempotent in A such that $\sigma(a)e=\tau(a)e$, for all $a\in A$. Then

$$\delta_{\sigma,\tau}e\overset{(4.22)}{=}\sum_{i=1}^n\tau(x_i)\sigma(y_i)e=\sum_{i=1}^n\tau(x_i)\tau(y_i)e\overset{(4.22)}{=}e,$$

hence $e=0$ or $\sigma=\tau$.

<u>6. $\Longrightarrow$ 8.</u> If $\sigma\neq e$ is such that $(e-\sigma)(S)\subset m$, then m contains

$$\sum_{i=1}^n x_i(y_i-\sigma(y_i))=\sum_{i=1}^n x_iy_i-\sum_{i=1}^n x_i\sigma(y_i)=1,$$

which contradicts the fact that m is a proper ideal of A.

<u>8. $\Longrightarrow$ 6.</u> Let $\mathcal{G}$ be the set of subsets $V\subset G$ satisfying the following properties

1. $e\in V$;

2. there exist $n\in\mathbb{N}$, $x_1,\cdots,x_n,y_1,\cdots,y_n\in A$ such that

$$\sum_{i=1}^n x_i\sigma(y_i)=\delta_{\sigma,e}.$$

for all $\sigma\in V$.

1) For all $\sigma \neq e \in G$, $\{e, \sigma\} \in \mathcal{G}$. The ideal of A generated by

$$\{a(e - \sigma)(b) \mid a, b \in A\}$$

is the whole of A. This implies that there exist $x_1, \cdots, x_n, y_1, \cdots, y_n \in A$ such that

$$\sum_{i=1}^{n} x_i y_i - \sum_{i=1}^{n} x_i \sigma(y_i) = 1.$$

Now let $x_{n+1} = \sum_{i=1}^{n} x_i \sigma(y_i)$ and $y_{n+1} = 1$. Then we see easily that

$$\sum_{i=1}^{n+1} x_i \sigma(y_i) = \delta_{\sigma,e}.$$

2) If $V, W \in \mathcal{G}$, then $V \cup W \in \mathcal{G}$. Obviously $e \in V \cup W$. There exist $n, m \in \mathbb{N}$, $x_1, \cdots, x_n, y_1, \cdots, y_n, x'_1, \cdots, x'_m, y'_1, \cdots, y'_m \in A$ such that

$$\sum_{i=1}^{n} x_i \sigma(y_i) = \delta_{\sigma,e}, \quad \forall \sigma \in V$$

$$\sum_{j=1}^{m} x'_j \sigma(y'_j) = \delta_{\tau,e}, \quad \forall \sigma \in W$$

Then we have for all $\sigma \in V \cup W$ that

$$\sum_{i=1}^{n} \sum_{j=1}^{m} x_i x'_j \sigma(y_i y'_j) = \Big(\sum_{i=1}^{n} x_i \sigma(y_i)\Big)\Big(\sum_{j=1}^{m} x'_j \sigma(y'_j)\Big) = \delta_{\sigma,e}.$$

$\square$

Chapter 5

Examples from (non-commutative) geometry

5.1 The general philosophy

In 1872 Felix Klein published a research program, entitled *Vergleichende Betrachtungen ber neuere geometrische Forschungen*, that had a major influence on the research in geometry ever since. This Erlangen Program (*Erlanger Programm*) – Klein was then at Erlangen – proposed a new solution to the problem how to classify and characterize geometries on the basis of *projective geometry* and *group theory*. Let us focus on this second part of the program.
Klein proposed that group theory was the most useful way of organizing geometrical knowledge: it provides algebraic methods to abstract the idea of (geometric) symmetries. With every geometry, Klein associated an underlying group of symmetries. The hierarchy of geometries is thus mathematically represented as a hierarchy of these groups, and hierarchy of their invariants. For example, lengths, angles and areas are preserved with respect to the Euclidean group of symmetries, while only the incidence structure and the cross-ratio are preserved under the more general projective transformations. A concept of parallelism, which is preserved in affine geometry, is not meaningful in projective geometry. Then, by abstracting the underlying groups of symmetries from the geometries, the relationships between them can be re-established at the group level. Since the group of affine geometry is a subgroup of the group of projective geometry, any notion invariant in projective geometry is a priori meaningful in affine geometry; but not the other way round. If you add required symmetries, you have a more powerful theory but fewer concepts and theorems.
In the modern and more abstract approach to the Erlangen program, geometry or *geometrical spaces*, are studied as spaces (i.e. sets, sometimes endowed with additional structure, such as a vector space, a Banach space, a topological space, etc.) together with a (predescribed) group that acts on this space (this action has to respect the additional structure of the set, i.e. it is, respectively, a linear map, a bounded linear map or a linear contraction, a continuous map, etc). Explicitly, let X be a set and G a group, we say that G acts on X if there is a map

$$\mathsf{m} : X \times G \to X,\ \mathsf{m}(x, g) = x \cdot g$$

such that $(x \cdot g) \cdot h = x \cdot (gh)$ and $x \cdot e = x$, for all $x \in X$ and $g, h \in G$ and the unit element $e \in G$. We call then X a G-space. The group G is considered as the symmetry group of the space X.

In the language of monoidal categories and Hopf algebras, developed above, remark that the group G is exactly a Hopf algebra in $\underline{\underline{\mathsf{Set}}}$ and X is a G-module, and even a G-module coalgebra (as any set has a trivial coalgebra structure in $\underline{\underline{\mathsf{Set}}}$).
As natural examples, one can consider any known "geometric" space X, take G it's usual group of symmetries and m as the usual action. In the next few sections we study which algebraic properties correspond to some (interesting) properties that those (classical) geometric examples share.

Homogeneous spaces

A G-space X is called *homogeneous* if the action of G on X is transitive, i.e. for all pairs $(x, y) \in X \times X$, there exists an element $g \in G$ such that $x = y \cdot g$.
All "classical spaces" are homogeneous spaces. E.g. if you consider an affine n-dimensional (real or complex) space $\mathbb{A}^n$, then the affine group (which is exactly a direct sum $GL(n)$ with the group of translations) acts transitively on $\mathbb{A}^n$.

Principal homogeneous spaces

A G-space X is called a *principal homogeneous space*, if X is a homogeneous space for G such that the stabilizer subgroup G_x of any point $x \in X$ is trivial. Recall that the *stabilizer subgroup* is defined as follows

$$G_x = \{g \in G \mid gx = x\} \subset G$$

Recall that an action of G on X is called *free* if for any two distinct g, h in G and all x in X we have $g \cdot x \neq h \cdot x$; or equivalently, if $g \cdot x = x$ for some x then $g = e$.
The following proposition provides a characterization for principal homogeneous spaces.

Proposition 5.1.1 *Let G be a group and X a G-space. The following assertions are equivalent.*

(i) X is a principal homogeneous space;

(ii) the action of G on X is free and transitive (i.e. the action of G is regular *or* simply transitive*);*

(iii) the canonical map $\chi : X \times G \to X \times X, \chi(x, g) = (x \cdot g, x)$ is bijective.

Proof. $\underline{(i) \Leftrightarrow (ii)}$. Trivial.
$\underline{(ii) \Leftrightarrow (iii)}$. It is easily verified that the surjectivity of χ is equivalent with the action of G on X being transitive, and that the injectivity of χ is equivalent with the action of G on X being free. $\square$

Algebraic groups as Hopf algebras in Aff

Similarly to $\underline{\underline{\mathsf{Set}}}$, $(\underline{\underline{\mathsf{Aff}}}, \times, \{P_*\})$ is a symmetric monoidal category, where $\{P_*\}$ is a (fixed) affine space with 1 point P_*. Hence it makes sense to define algebras, coalgebras, bialgebras and Hopf algebras in $\underline{\underline{\mathsf{Aff}}}$. Again similarly to $\underline{\underline{\mathsf{Set}}}$, the coalgebras in $\underline{\underline{\mathsf{Aff}}}$ are trivial: every affine space X can be endowed with a unique structure of a coalgebra, by means of the diagonal map $\Delta : X \to X \times X, \Delta(P) = (P, P)$ for all points $P \in X$. The next interesting structures are the Hopf algebras in $\underline{\underline{\mathsf{Aff}}}$. These are exactly the *algebraic groups*. I.e. an affine space $G \in \underline{\underline{\mathsf{Aff}}}$ is a Hopf algebra in

$\underline{\underline{\mathsf{Aff}}}$ if it has moreover a group structure, and the multiplication and morphism of taking inverses are regular (i.e. polynomial) functions.
Furthermore if X is another affine space, and the algebraic group G acts on X by means of a regular function, i.e. the action morphism $\mathsf{m}_X : X \times G \to G$ is a morphism in $\underline{\underline{\mathsf{Aff}}}$, then X becomes a G-module coalgebra in $\underline{\underline{\mathsf{Aff}}}$.
As we have now translated the algebro-geometric notions (of algebraic group, action of a group on an affine set) into general notions inside monoidal categories (a Hopf algebra, a comodules algebra), we can apply the machinery of monoidal functors, to show that the coordinate algebras on the objects that we have will carry over these structures, and therefore fit in the theory (of Hopf-Galois extensions) we have developed during this course.

5.2 Hopf algebras in algebraic geometry

5.2.1 Coordinates as monoidal functor

Troughout this section, let k be an infinite field. Recall from the course on algebraic geometry that there is a contravariant functor

$$\Gamma : \underline{\underline{\mathsf{Aff}}} \to \mathsf{Alg}_k$$

taking an n-dimensional affine variety $V \subset \mathbb{A}^n$ to its coordinate algebra $\Gamma(X) = k[X_1, \ldots, X_n]/I$, where I is the ideal consisting of all polynomials $f \in k[X_1, \ldots, X_n]$ for which $f(P) = 0$ for all $P \in X$. The aim of this section is to provide the categorical machinery that turns the 'coordinate algebra' really into an 'algebra', and to proof that it allows to construct Hopf algebras out of algebraic groups. The main idea is that the functor Γ is strict monoidal. However, since Γ is contravariant, it will be more suitable to consider Γ as a covariant functor, i.e. we will consider

$$\Gamma : \underline{\underline{\mathsf{Aff}}}^{op} \to \mathsf{Alg}_k.$$

(So, as mentioned in Section 1.1.2, we consider in fact the functor Γ^{op}, but we will omit to write the "op".)

Lemma 5.2.1 *For any $n, m \in \mathbb{N}$, there is a natural isomorphism*

$$\phi : k[X_1, \ldots, X_n] \otimes k[Y_1, \ldots, Y_m] \to k[X_1, \ldots, X_n, Y_1, \ldots, Y_m].$$

Proof. Consider any two elements

$$\begin{aligned} f(X_1, \ldots, X_n) &= \sum a_{i_1 \ldots i_n} X_1^{i_1} \cdots X_n^{i_n} \in k[X_1, \ldots, X_n]; \\ g(Y_1, \ldots, Y_m) &= \sum b_{j_1 \ldots j_m} Y_1^{j_1} \cdots Y_m^{j_m} \in k[Y_1, \ldots, Y_m]. \end{aligned}$$

We can define a new polynomial $F \in k[X_1, \ldots, X_n, Y_1, \ldots, Y_m]$, by

$$F(X_1, \ldots, X_n, Y_1, \ldots, Y_m) = \sum a_{i_1 \ldots i_n} b_{j_1 \ldots j_m} X_1^{i_1} \cdots X_n^{i_n} Y_1^{j_1} \cdots Y_m^{j_m}.$$

This defines a well-defined map ϕ as in the statement of the theorem. Conversely, take any $F = \sum a_{i_1\dots i_{n+m}} X_1^{i_1}\cdots X_n^{i_1} Y_1^{i_{n+1}}\cdots Y_m^{i_{n+m}}$, then we can construct the following element in $k[X_1,\dots,X_n]\otimes k[Y_1,\dots,Y_m]$:

$$\bar\phi(F) = \sum a_{i_1\dots i_{n+m}} X_1^{i_1}\cdots X_n^{i_1}\otimes Y_1^{i_{n+1}}\cdots Y_m^{i_{n+m}}.$$

A straightforward calculation shows that ϕ and $\bar\phi$ are mutual inverses. $\square$

Remark that ϕ is defined in such a way, that for any two points $P\in\mathbb{A}^n$ and $P'\in\mathbb{A}^m$ (i.e. $(P.P')\in\mathbb{A}^n\times\mathbb{A}^m$), and any $f\in\Gamma(\mathbb{A}^n)=k[X_1,\dots,X_n]$ and $g\in\Gamma(\mathbb{A}^m)=k[Y_1,\dots,Y_m]$,

$$\varphi(f\otimes g)(P,P') = f(P)g(P) \tag{5.1}$$

Lemma 5.2.2 *Consider vectorspaces $V,W,U,Z\in\mathcal{M}_k$ and linear maps $f:V\to W$ and $g:U\to Z$. Then* $\ker(f\otimes g)=(\ker f\otimes V)+(U\otimes\ker g)$.

Proof. Let $(v_\alpha)_{\alpha\in A_1}$ be a basis of $\ker f$, which we complete with $(v_\alpha)_{\alpha\in A_2}$ to form a basis of V. Then $f(v_\alpha)_{\alpha\in A_2}$ is a linearly independent subset of W. Analogously, let $(u_\beta)_{\beta\in B_1}$ be a basis of $\ker g$, which we complete with $(u_\beta)_{\beta\in B_2}$ to a basis of U. Again, $(g(u_\beta))_{\beta\in B_2}$ is a linearly independent family in Z. Consider

$$q = \sum_{\substack{\alpha\in A_1\cup A_2\\ \beta\in B_1\cup B_2}} c_{\alpha\beta} v_\alpha\otimes u_\beta \in \ker(f\otimes g).$$

Then

$$\sum_{\substack{\alpha\in A_1\cup A_2\\ \beta\in B_1\cup B_2}} c_{\alpha\beta} f(v_\alpha)\otimes g(u_\beta) = 0.$$

By the linearly independence of the family $(f(v_\alpha)\otimes g(u_\beta))_{\alpha\in A_2,\beta\in B_2}$, it follows that $c_{\alpha\beta}=0$ for any $\alpha\in A_2$ and $\beta\in B_2$. Then $q\in\ker f\otimes U+V\otimes\ker g$, and we obtain that

$$\ker(f\otimes g)\subseteq(\ker f\otimes V)+(U\otimes\ker g).$$

The reverse inclusion is clear. $\square$

Theorem 5.2.3 *The functor $\Gamma:\underline{\underline{\mathsf{Aff}}}^{op}\to\mathcal{M}_k$ defined above is a strong, symmetric monoidal functor.*

Proof. Consider two affine varieties $X\subset\mathbb{A}^n$ and $Y\subset\mathbb{A}^m$. Then we have $\Gamma(X)=k[X_1,\dots,X_n]/I$, and $\Gamma(Y)=k[Y_1,\dots,Y_m]/J$ where I and J is the ideal of all polynomials vanishing respectively on X and Y. We can construct the variety $X\times Y\subset\mathbb{A}^n\times\mathbb{A}^m\cong\mathbb{A}^{m+n}$. Hence $\Gamma(X\times Y)=k[X_1,\dots,X_n,Y_1,\dots,Y_m]/L$, where L is the ideal consisting of all polynomials vanishing on $X\times Y$. It is our aim to construct an isomorphism

$$\Phi_{X,Y}: k[X_1,\dots,X_n]/I\otimes k[Y_1,\dots,Y_m]/J\cong k[X_1,\dots,X_n,Y_1,\dots,Y_m]/L.$$

Take any generator $f\otimes g\in k[X_1,\dots,X_n]/I\otimes k[Y_1,\dots,Y_m]/J$. We will define $\Phi_{X,Y}(f\otimes g)=\phi(f\otimes g)$, where ϕ is the morphism from Lemma 5.2.1. Let us check that $\Phi_{X,Y}$ is well defined.

Consider the projection $\pi_I : k[X_1, \ldots, X_n] \to k[X_1, \ldots, X_n]/I$. Then $I = \ker \pi_I$. Similarly, $J = \ker \pi_J$, where $\pi_J : k[Y_1, \ldots, Y_m] \to k[Y_1, \ldots, Y_m]/J$. Now consider the exact row

$$k[X_1, \ldots, X_n] \otimes k[Y_1, \ldots, Y_m] \xrightarrow{\pi_I \otimes \pi_J} k[X_1, \ldots, X_n]/I \otimes k[Y_1, \ldots, Y_m]/J \longrightarrow 0$$

Since this row is exact,

$$\begin{aligned} k[X_1, \ldots, X_n]/I \otimes k[Y_1, \ldots, Y_m]/J &= (k[X_1, \ldots, X_n] \otimes k[Y_1, \ldots, Y_m])/\ker(\pi_I \otimes \pi_J) \\ &\cong (k[X_1, \ldots, X_n] \otimes k[Y_1, \ldots, Y_m])/(I \otimes k[Y_1, \ldots, Y_m] + k[X_1, \ldots, X_n] \otimes J), \end{aligned}$$

where the last isomorphism follows by Lemma 5.2.2.
Consequently, to verify wether $\Phi_{X,Y}$ is well defined, it suffices to check wether for any $\sum f_i \otimes g_i \in (I \otimes k[Y_1, \ldots, Y_m] + k[X_1, \ldots, X_n] \otimes J)$, we have that $\phi(\sum f_i \otimes g_i) \in L$. By definition, the latter is true if and only if $\phi(\sum f_i \otimes g_i)(P, P') = 0$ for all $(P, P') \in X \times Y$. By (5.1), this is equivalent with $\sum f_i(P) g_i(P') = 0$ for all $P \in X$ and $P' \in Y$. Since for all choices of i, we have that either $f_i \in I$ or $g_i \in J$, each term in this sum equals zero, and $\Phi_{X,Y}$ is well defined.
Conversely, we define

$$\begin{aligned} \bar{\Phi}_{X,Y} : k[X_1, \ldots, X_n, Y_1, \ldots, Y_m]/L &\to k[X_1, \ldots, X_n]/I \otimes k[Y_1, \ldots, Y_m]/J \\ &\cong (k[X_1, \ldots, X_n] \otimes k[Y_1, \ldots, Y_m])/(I \otimes k[Y_1, \ldots, Y_m] + k[X_1, \ldots, X_n] \otimes J) \end{aligned}$$

by $\bar{\Phi}_{X,Y}(F) = \phi^{-1}(F)$. Again, we have to check wether $\bar{\Phi}_{X,Y}$ is well-defined. So take an element $F \in L$, we will verify if $\phi^{-1}(F) = \sum f_i \otimes g_i \in (I \otimes k[Y_1, \ldots, Y_m] + k[X_1, \ldots, X_n] \otimes J)$. Consider all indices i such that $g_i(P') = 0$ for all points $P' \in Y$, and denote these indices from now on by ℓ. Then this means exactly that $g_\ell \in J$ and so $f_\ell \otimes g_\ell \in k[X_1, \ldots, X_n] \otimes J$. Denote the remaining indices by q, then

$$\phi^{-1}(F) = \sum f_i \otimes g_i = \sum f_\ell \otimes g_\ell + \sum f_q \otimes g_q,$$

where $\sum f_\ell \otimes g_\ell \in k[X_1, \ldots, X_n] \otimes J$ we will be done if we show that $\sum f_q \otimes g_q \in I \otimes k[Y_1, \ldots, Y_m]$.
By definition of F and ϕ, and our construction above, we find for all $P \in X$ and $P' \in Y$ that

$$0 = F(P, P') = \sum_i f_i(P) g_i(P') = \sum_q f_q(P) g_q(P').$$

Hence, for any fixed $P' \in Y$, we have that $\sum_q g_q(P') f_q \in I$. Since all $g_q \notin J$, and there are only a finite number of indices q, there exists a $P' \in Y$ such that $g_q(P') \neq 0$ for all q, fix such a P'. We can write

$$g_q = \sum b^q_{j_1 \ldots j_m} Y_1^{j_1} \cdots Y_m^{j_m} = \sum g_q(P') \tilde{b}^q_{j_1 \ldots j_m} Y_1^{j_1} \cdots Y_m^{j_m}.$$

where $\tilde{b}^q_{j_1 \ldots j_m} = b^q_{j_1 \ldots j_m}/g_q(P')$. Then we find

$$\begin{aligned} \sum_q f_q \otimes g_q &= \sum_q f_q \otimes \sum_{j_1, \ldots, j_m} g_q(P') \tilde{b}^q_{j_1 \ldots j_m} Y_1^{j_1} \cdots Y_m^{j_m} \\ &= \sum_{j_1, \ldots, j_m} (\sum_q g_q(P') f_q) \otimes \tilde{b}^q_{j_1 \ldots j_m} Y_1^{j_1} \cdots Y_m^{j_m} \in I \otimes k[Y_1, \ldots, Y_m]. \end{aligned}$$

Finally, $\Phi_0 : \Gamma(\{P_*\}) = k$ by definition, so Γ is a strict monoidal functor. It is easily verified that Γ is also symmetric. $\square$

As announced, we have now an explanation for the following known result.

Corollary 5.2.4 *For any affine space X, $\Gamma(X)$ is a (commutative) k-algebra. Hence the functor Γ can be corestricted to a functor $\Gamma : \underline{\underline{\mathsf{Aff}}} \to \mathsf{Alg}_k$.*

Proof. Consider any affine space X. As mentioned at the end of Section 5.1, X is a coalgebra in $\underline{\underline{\mathsf{Aff}}}$, with comultiplication $\Delta : X \to X \times X,\ \Delta(P) = (P, P)$ and counit $\pi : X \to \{P_*\},\ \pi(P) = P_*$. Hence X is an algebra in $\underline{\underline{\mathsf{Aff}}}^{op}$ and therefore, as we know by Theorem 5.2.3 that Γ is a monoidal functor, $(\Gamma(X), \Gamma(\Delta), \overline{\Gamma(\pi)})$ is an algebra in $\mathcal{M}_k$, since by Theorem **??**, monoidal functors preserve algebras. This is exactly the classical, commutative coordinate algebra of X, with multiplication

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

and unit $1(P) = 1$ for all $P \in X$. $\square$

Remark 5.2.5 Remark that the commutativity of $\Gamma(X)$ is a consequence of the cocommutativity of X as coalgebra in $\underline{\underline{\mathsf{Aff}}}$.

Algebro-geometric Hopf algebras and their coactions

Subsuming the results developed in previous sections, we arrive at the following important theorem, that translates the geometric concepts of Section 5.1 in Hopf-algebraic terms.

Theorem 5.2.6 *[(i)]*

If G is an algebraic group, then $\Gamma(G)$ is a k-Hopf algebra.

2. *If an algebraic group G has a regular action m_X on an affine space X, then $\Gamma(X)$ is a comodule algebra over the Hopf algebra $\Gamma(G)$.*

Proof. (i) Suppose that G is an algebraic group, hence a Hopf algebra in $\underline{\underline{\mathsf{Aff}}}$, then G is also a Hopf algebra in $\underline{\underline{\mathsf{Aff}}}^{op}$ and, by Theorem 5.2.3 and Theorem **??**, $\Gamma(G)$ is a Hopf algebra in $\mathcal{M}_k$. The comultiplication is given by $\Gamma(\mathsf{m}_G)$ (where m_G denotes the multiplication map of G) and the antipode is given by $\Gamma(\mathsf{inv})$ (where $\mathsf{inv} : G \to G,\ \mathsf{inv}(g) = g^{-1}$).
(ii) As explained at the end of Section 5.1, the action of the group G on X, can be seen as a G-module coalgebra structure on X on $\underline{\underline{\mathsf{Aff}}}$, hence as a G-comodule algebra structure on X in $\underline{\underline{\mathsf{Aff}}}^{op}$. Similar to Theorem **??**, one proves that this structure is preserved by the strong, symmetric monoidal functor Γ. Therefore, $A = \Gamma(X)$ is an $H = \Gamma(G)$-comodule algebra in $\mathcal{M}_k$, with $\rho^A = \Gamma(\mathsf{m}_X)$. $\square$

Theorem 5.2.7 *If X is a principal homogeneous G-space then $A = \Gamma(X)$ is a Galois object for $H = \Gamma(G)$, i.e. $A^{coH} \cong k$ and $k \to A$ is a (faithfully flat) H-Galois extension.*

Proof. Consider the map $\pi_X : G \times X \to X, \pi_X(g,x) = x$, the projection on X. Then consider the coequalizer in $\underline{\underline{\mathsf{Aff}}}$ of the pair (m_X, π_X), where we denote by m_X the action of G on X, i.e.

$$X \times G \underset{\pi_X}{\overset{\mathsf{m}_X}{\rightrightarrows}} X \longrightarrow X/G.$$

An easy computation shows that this coequalizer is the quotient of X by the action of G, consisting of all orbits. Hence by transitivity, the coequalizer is the singleton $\{P_*\}$. Applying the monoidal functor Γ on this coequalizer, we obtain the following equalizer in $\mathcal{M}_k$.

$$\Gamma(\{P_*\}) \cong k \longrightarrow \Gamma(X) = A \underset{\Gamma(\pi_X)\simeq A\otimes\eta_H}{\overset{\Gamma(\mathsf{m}_X)\simeq\rho^A}{\rightrightarrows}} \Gamma(X \times G) \cong A \otimes H$$

Which shows, by uniqueness of the equalizer, that the coinvariants of $A = \Gamma(X)$ are isomorphic to k.
By Proposition 5.1.1, we know that the map $\chi : X \otimes G \to X \times X$ is bijective. Hence $\Gamma(\chi)$ will be an isomorphism in $\mathcal{M}_k$, we claim that $\Gamma(\chi) = \mathrm{can} : \Gamma(X \times X) \cong A \otimes A \to \Gamma(X \times G) \cong A \otimes H$. Indeed, we can write $\chi = (X \times \mathsf{m}_X) \circ (\Delta_X \times G)$. So, using the contravariancy of Γ we find

$$\begin{aligned}\Gamma(\chi) &= \Gamma(\Delta_X \times G) \circ \Gamma(X \times \mathsf{m}_X) = (\Gamma(\Delta_X) \otimes \Gamma(G)) \circ (\Gamma(X) \otimes \Gamma(m_X)) \\ &= (\mu_A \otimes H) \circ (A \otimes \rho^A) = \mathrm{can}\end{aligned}$$

where we used the monoidality of Γ in the second equality, and the definition of can in the last equality.
Since we work over a field k, and the coinvariants of A are exactly k, the faithful flatness condition is trivial. □

An elaborated example: The unit circle and the orthogonal group

In this section we illustrate Theorem 5.2.7 with one of the most immediate examples: the orthogonal group G of 2-by-2 matrices acting on the unit circle C. The orthogonal group acts on C by counter-clockwise rotation of the points. This action is obviously transitive and free, hence C is a principal homogeneous G-space. Consequently, $\Gamma(C)$ will be a $\Gamma(G)$ Galois object. We will explicitly compute these structures. It is not our aim to provide the shortest possible proofs for the statements (as everything follows immediately from the theorems in the previous section), but to provide a guiding frame to compute more (complicated) examples.
Consider

$$G = \mathsf{SO}_2(\mathbb{R}) = \{A \in \mathsf{Mat}_2(\mathbb{R}) \mid A^tA = I_2 = AA^t, \det(A) = 1\}$$

This can be considered as a subspace of $\mathbb{A}^4$, and we find

$$H = \Gamma(G) = \mathbb{R}[a,b,c,d]/(a^2 + b^2 - 1, c^2 + d^2 - 1, ac + bd, ad - bc - 1).$$

Let us calculate the coalgebra structure on H. Recall that $\Gamma(G)$ can be interpreted as the algebra of regular functions on the affine space G. With this interpretation, a set of generators for the algebra H is given by a, b, c, d, defined by

$$a(A) = a_{11},\ b(A) = a_{12},\ c(A) = a_{21},\ d(A) = a_{22},$$

where $A = \begin{pmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{pmatrix} \in \mathsf{Mat}_2(\mathbb{R})$. Because monoidality of the functor Γ, we have $\Gamma(G\times G) \cong \Gamma(G) \otimes \Gamma(G)$, so we can define $\Delta(a)$ be evaluating it in a pair (A, B). Since the comultiplication on H is constructed by dualizing the multiplication on G, we have

$$\Delta(a)(A, B) = a(A.B) = a_{11}b_{11} + a_{12}b_{21} = a(A)a(B) + b(A)c(B) = (a \otimes a + b \otimes c)(A, B),$$

hence $\Delta(a) = a\otimes a+b\otimes c$. Similar computations show that $\Delta(b) = a\otimes b+b\otimes d$, $\Delta(c) = c\otimes a+d\otimes c$ and $\Delta(d) = c \otimes b + d \otimes d$. Then can be compressed in the following formal expression

$$\Delta \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{5.2}$$

Using the fact that Δ needs to be an algebra morphism, these expressions define $\Delta(f)$ for any $f \in \Gamma(G)$. We should check wether Δ is well-defined, i.e. if $\Delta(f) \in I \otimes \mathbb{R}[a, b, c, d] + \mathbb{R}[a, b, c, d] \otimes I$ (or zero in $H \otimes H$) for any $f \in I = (a^2 + b^2 - 1, c^2 + d^2 - 1, ac + bd, ad - bc - 1)$. Let us verify this explicitly for $f = a^2 - b^2 - 1$. We can compute in $H \otimes H$,

$$\begin{aligned}
\Delta(a^2 + b^2 - 1) \;\; = \;\; & \Delta(a)\Delta(c) + \Delta(b)\Delta(d) \\
& = (a \otimes a + b \otimes c)(a \otimes a + b \otimes c) + (a \otimes b + b \otimes d)(a \otimes b + b \otimes d) - 1 \otimes 1 \\
& = (a^2 \otimes a^2 + 2ab \otimes ac + b^2 \otimes c^2) + (a^2 \otimes b^2 + 2ab \otimes bd + b^2 \otimes d^2) - 1 \otimes 1 \\
& = (a^2 \otimes a^2 + 2ab \otimes ac + b^2 \otimes c^2) + (a^2 \otimes b^2 + 2ab \otimes bd + b^2 \otimes d^2) - 1 \otimes 1 \\
& = a^2 \otimes (a^2 + b^2) + b^2 \otimes (c^2 + d^2) + 2ab \otimes (ac + bd) - 1 \otimes 1 \\
& = a^2 \otimes 1 + b^2 \otimes 1 - 1 \otimes 1 = 0
\end{aligned}$$

Let us now construct the counit. Recall that $k \cong \Gamma\{P_*\}$, and $\varepsilon = \Gamma(\pi)$, where $\pi : G \to \{P_*\}$ is the canonical projection. Take again the generator $a \in H$, then we have

$$\varepsilon(a)(P_*) = a(I_2) = 1.$$

Similarly, $\varepsilon(b) = b(I_2) = 0$, $\varepsilon(c) = c(I_2) = 0$ and $\varepsilon(d) = d(I_2) = 1$. This can be subsumed in the formal expression

$$\varepsilon \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}. \tag{5.3}$$

Next, we compute the antipode.

$$S(a)(A) = a(A^{-1}) = a(A^t) = a_{11} = a(A)$$

So $S(a) = a$. Similarly, $S(b) = c$, $S(c) = b$ and $S(d) = d$. In short,

$$S \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & c \\ b & d \end{pmatrix}. \tag{5.4}$$

Let us check that the antipode is well-defined. The only problem is to verify that $S(ac+bd) = S(c)S(a)+S(d)S(b) = ba+dc = 0$ (the antipode must be an anti-algebra morphism, however as our algebra is commutative, S is just an algebra morphism). This can be seen as follows,

$$\begin{aligned} 0 &= ac+bd, && \text{multiply by } bc, \\ &= abc^2+b^2cd, && c^2 = 1-d^2,\ b^2 = 1-a^2 \\ &= ab-abd^2+cd-a^2cd \\ &= ab+cd-ad(bd+ac), && bd+ac=0 \\ &= ab+cd \end{aligned}$$

Now consider the circle $C \subset \mathbb{A}^2$. Algebraic geometry tells us that $A = \Gamma(C) = \mathbb{R}[x,y]/(x^2+y^2-1)$. We know by Theorem 5.2.6 $\Gamma(C)$ is an H-comodule algebra. The explicit formula for the coaction can be computed by similar method as above. First, consider coorinates on points of the cirle, $P = P(X,Y)$, and define the generators x, y in A as follows,

$$x(P) = X,\ y(P) = Y.$$

Since the coaction ρ is the dual of the action m of G on C, we find that

$$\begin{aligned} \rho(x)(P,A) &= x(P\cdot A) = x(Xa_{11}+Ya_{21}, Xa_{21}+Ya_{22}) = Xa_{11}+Ya_{21} \\ &= x(P)a(A)+y(P)c(A) = (x\otimes a+y\otimes c)(P,A), \end{aligned}$$

so $\rho(x) = x\otimes a+y\otimes c$. Similarly, $\rho(y) = x\otimes b+y\otimes d$, and therefore we write

$$\rho\begin{pmatrix} x & y \end{pmatrix} = \begin{pmatrix} x & y \end{pmatrix} \otimes \begin{pmatrix} a & b \\ c & d \end{pmatrix} \tag{5.5}$$

There is a deeper reason why it is possible to define the comultiplication, counit, antipode and coaction in this example by means of the compact formula (5.2), (5.3), (5.4) and (5.5). Although we will not go into the details of this mechanism, let us just mention that it is a consequence of a universal property of polynomial rings and this mechanism makes it possible to construct in an easy way more examples of Hopf algebras and bialgebras, and comodule algebras over these, starting from subgroups of matrix groups acting on affine spaces.

Finally, let us check that A is a H-Galois object. To this end, let us recall the form of the map $\chi : C\times G \to C\times C, \chi(P,g) = (P, P\cdot g)$ in this situation. Similar computations as above then gives the explicit form of $\mathrm{can} : A\otimes A \to A\otimes H$, as the dualization of χ, on the generators $1\otimes x, 1\otimes y, x\otimes 1$ and $y\otimes 1$ of $A\otimes A$,

$$\begin{aligned} \mathrm{can}(1\otimes x) &= x\otimes a+y\otimes c && (5.6) \\ \mathrm{can}(1\otimes y) &= x\otimes b+y\otimes d && (5.7) \\ \mathrm{can}(x\otimes 1) &= x\otimes 1 && (5.8) \\ \mathrm{can}(y\otimes 1) &= y\otimes 1 && (5.9) \end{aligned}$$

To see that can is bijective and to compute its inverse, let us first compute the inverse of χ. The coordinates (X,Y) of a point P of C can be written as $X = \cos\alpha$, $Y = \sin\alpha$. For a second point

$P' = P'(X', Y')$, we can write $X' = \cos\beta$ and $Y' = \sin\beta$. Hence, $\chi^{-1}(P, P') = (P, g)$, where g is a rotation over $\beta - \alpha$ (via right multiplication), i.e.

$$\begin{aligned} g &= \begin{pmatrix} \cos(\beta-\alpha) & \sin(\beta-\alpha) \\ -\sin(\beta-\alpha) & \cos(\beta-\alpha) \end{pmatrix} = \begin{pmatrix} \sin\alpha\sin\beta + \cos\alpha\cos\beta & \cos\alpha\sin\beta - \sin\alpha\cos\beta \\ \sin\alpha\cos\beta - \sin\beta\cos\alpha & \sin\alpha\sin\beta + \cos\alpha\cos\beta \end{pmatrix} \\ &= \begin{pmatrix} YY' + XX' & XY' - YX' \\ YX' - Y'X & YY' + XX' \end{pmatrix} \end{aligned}$$

Similar computations as above then lead to the following form for the inverse of can

$$\begin{aligned} \mathrm{can}^{-1}(x \otimes 1) &= x \otimes 1 \\ \mathrm{can}^{-1}(y \otimes 1) &= y \otimes 1 \\ \mathrm{can}^{-1}(1 \otimes a) &= y \otimes y + x \otimes x \\ \mathrm{can}^{-1}(1 \otimes b) &= x \otimes y - y \otimes x \\ \mathrm{can}^{-1}(1 \otimes c) &= y \otimes x - x \otimes y \\ \mathrm{can}^{-1}(1 \otimes d) &= y \otimes y + x \otimes x \end{aligned}$$

We leave it to the reader to check that can and can^{-1} are indeed mutual inverses. Remark that the relations in H imply that $d = a$ and $b = -c$.

5.3 A glimpse on non-commutative geometry

5.3.1 Non-commutative geometry by Hopf (Galois) theory

All initial examples of Hopf algebras (e.g. group algebras, tensor algebras, universal enveloping algebras of a Lie algebra, regular functions on an algebraic group,...) are either commutative or cocommutative. For some time, it was therefore thought that all Hopf algebras needed to be commutative or cocommutative. This turned out to be false, with as a first counterexample Sweedler's four-dimensional Hopf algebra. Some of most intensively studied Hopf algebras today, are classes of non-commutative, non-cocommutative Hopf algebras, called quantum groups. These originate in the study of (non-commutative) geometry, as the symmetries of a non-commutative space.
As we have explained in Section 5.1, we understand a group G exactly as the symmetries of a certain space X upon which this group acts. Next, we have translated the group structure of G into the structure of a (commutative) Hopf algebra H and encoded the space X by its (commutative) coordinate algebra A. If G acts on X, then A is a comodule algebra over H. Still, we can understand H to describe the "symmetries" of the "space" A. At this point the occuring algebras are all commutative. This was explained by the fact that the functor Γ is a strong monoidal functor, and the underlying sets of G and X posses a trivial, hence cocommutative, coalgebra structure. The idea is now to extend the functor $\Gamma : \underline{\underline{\mathsf{Aff}}} \to \mathcal{M}_k$, in such a way, that its image will reach also non-commutative algebras. The functor Γ will then origin in the category of 'non-commutative spaces'. However, to describe the category of non-commutative spaces in an appropriate way, that allows a nice geometric interpretation and such that the functor Γ satisfies all desired properties seems a very difficult (and doubtful) job. Therefore, we will mainly concentrate on the image

of Γ and we will understand a non-commutative space, as being completely described by its non-commutative "coordinate algebra" A. The symmetries of the non-commutative space are described by a non-commutative, non-cocommutative Hopf algebra H, over which A is a comodule algebra. Following this philosophy, we say that A is a quantum principle homegeneous space, exactly when A is an H-Galois object.
More generally an H-Galois extension $B \to A$, corresponds to a *quantum principle bundle*.

5.3.2 Deformations of algebraic groups: algebraic quantum groups

A general manner to construct examples of quantum groups and the non-commutative space upon which they act, is to deform classical spaces, as we have studied in Section 5.2. By deforming, we refer to a procedure that changes the multiplication of the algebra, in order to make it non-commutative, but does not change the algebra as a vector space, nor the unit element.
One of the most well known examples is the so-called quantum plane. We will give an explicit form of the quantum plane, and of a Hopf algebra of quantum symmetries. Let $q \in k^*$ be an invertible element of the field k. We denote by I_q the two-sided ideal of the free algebra $k\langle x, y\rangle$ generated by the element $yx - qxy$. The quantum plane is the quotient algebra

$$A = k_q[x, y] = k\langle x, y\rangle / I_q.$$

If $q = 1$, then $A = k[x, y]$ the polynomial algebra (i.e. the coordinate algebra of the affine plane $\mathbb{A}^2$), otherwise, A is non-commutative.
Next, we construct the algebra $M_q(2) = k\langle a, b, c, d\rangle / J_q$, of (dual) quantum matrices. Here J_q is the ideal of the free algebra $k\langle a, b, c, d\rangle$ generated by the relations

$$\begin{aligned} ba &= qab, & db &= qbd \\ ca &= qac, & dc &= qcd, \\ bc &= cb, & ad - da &= (q^{-1} - q)bc \end{aligned}$$

This algebra is a in fact a bialgebra. Comultiplication Δ and counit ε are given by the following formula on the generators

$$\Delta\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \otimes \begin{pmatrix} a & b \\ c & d \end{pmatrix} \qquad \varepsilon\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}.$$

Moreover, the quantum plane A is an $M_q(2)$-comodule algebra, with coaction given by

$$\rho\begin{pmatrix} x & y \end{pmatrix} = \begin{pmatrix} x & y \end{pmatrix} \otimes \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

Next, we will construct a Hopf algebra, coacting on the quantum plane. Consider the algebra $SL_q(2) = M_q(2)/(da - qbc - 1)$. One can check that the comultiplication Δ, counit ε and coaction ρ, as defined above, behave well with respect to the ideal $(da - qbc - 1)$. Moreover, by defining an antipode

$$S\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} d & -q^{-1}c \\ -qb & a \end{pmatrix}.$$

we find that $SL_q(2)$ becomes a Hopf algebra, and the quantum plane is a $SL_q(2)$-comodule algebra. In an appropriate way, one can define quantum circles, higher dimensional variants and their symmetries.

5.3.3 More quantum groups

The procedure described above, provides an approach towards non-commutative geometry starting from the point of view of algebraic geometry. There is another approach possible, based rather on differential geometry. In this approach, one considers smooth manifolds, whose symmetries are described by Lie groups. As generally known, associated to a Lie group G, there is a Lie algebra $\mathfrak{g}$ (and visa versa). The universal enveloping algebra $U(\mathfrak{g})$ of the Lie algebra $\mathfrak{g}$ is a cocommutative Hopf algebra. Furthermore, if the Lie group G is compact, one can consider the algebra $\mathsf{Rep}(G)$ of representable complex-valued functions on G, this is again a Hopf algebra (very similar to the Hopf algebra of regular functions on an algebraic group). Moreover, the Hopf algebras $\mathsf{Rep}(G)$ and $U(\mathfrak{g})$ are in a dual pairing (The concept of a dual pairing for Hopf algebras generalises the fact that the dual of a finite dimensional Hopf algebra is again a Hopf algebra. If two finite dimensional Hopf algebras A and B are in a dual pairing, then $A \cong B^*$). If X is a smooth space, then it is possible to construct an algebra of functions on X, that becomes a comodule algebra over $\mathsf{Rep}(G)$, and a module algebra over $U(\mathfrak{g})$. Many of the considered algebras in this setting have an additional structure of $*$-algebra or C^*-algebra.
The approach to non-commutative algebra is now to consider non-commutative (C^*-)algebras, and non-commutative, non-cocommutative Hopf algebras that (co-)act on these and that are deformations of the above. In particular, it is possible to construc quantized enveloping algebras $U_q(\mathfrak{g})$. Many quantum groups and non-commutative spaces can be studied both in algebraic and differential geometric framework. For example, the Hopf algebra $U_q(\mathfrak{sl}_2)$ acts on the quantum plane.

Index

Bibliography

[1] E. Abe, Hopf Algebras, Cambridge University Press, Cambridge, 1977.

[2] H. Bass, Algebraic K-theory, Benjamin, New York, 1968.

[3] F. Borceux, Handbook of categorical algebra 1, Encyclopedia Math. Appl. **50**, Cambridge University Press, Cambridge, 1994.

[4] F. Borceux, Handbook of categorical algebra 2, Encyclopedia Math. Appl. **51**, Cambridge University Press, Cambridge, 1994.

[5] S. Dăscălescu, C. Năstăsescu and Ş. Raianu, "Hopf algebras: an Introduction", *Monographs Textbooks in Pure Appl. Math.* **235** Marcel Dekker, New York, 2001.

[6] C. Kassel, "Quantum Groups", *Graduate Texts Math.* **155**, Springer Verlag, Berlin, 1995.

[7] S. Mac Lane, Categories for the working mathematician. Second edition. *Graduate Texts Math.* **5**, Springer Verlag, Berlin, 1998.

[8] S. Majid, "Foundations of quantum group theory", Cambridge Univ. Press, 1995.

[9] S. Montgomery, "Hopf algebras and their actions on rings", American Mathematical Society, Providence, 1993.

[10] M. E. Sweedler, "Hopf algebras", Benjamin, New York, 1969.