Normal forms in combinatorial algebra

Gioia, A.

Citation
Gioia, A. (2009). *Normal forms in combinatorial algebra*.

Version:	Not Applicable (or Unknown)
License:	License to inclusion and publication of a Bachelor or Master thesis in the Leiden University Student Repository
Downloaded from:	https://hdl.handle.net/1887/3597462

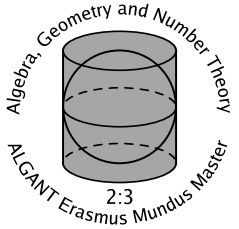
Note: To cite this publication please use the final published version (if applicable).

Alberto Gioia

Normal forms in combinatorial algebra

Master's thesis, defended on July 8, 2009

Thesis advisor: Hendrik Lenstra



Mathematisch Instituut

Universiteit Leiden

Contents

Introduction **iv**

1 Generators and relations **1**

1.1 Category theory 1

1.2 Free monoids 3

1.3 Relations 4

1.4 Free groups 6

1.5 Relations on groups 8

1.6 Free k-algebras 10

1.7 Relations on k-algebras 12

2 The monoid case **15**

2.1 The statement of the theorem 15

2.2 The proof of the theorem 17

2.3 Examples 19

3 The group case **27**

3.1 Van der Waerden's theorem 27

3.2 Examples 29

4 The ring case **32**

4.1 Van der Waerden's theorem 32

4.2 Examples 35

Bibliography **41**

Introduction

Let S be a set. An S-group is a group G together with a map $S \to G$, which we shall usually denote with the empty symbol (i.e. the image of $s \in S$ in G is denote s). A map of S-groups is a group homomorphism between two S-groups which respects this map. The free group $F(S)$ on S is universal among S-groups in the sense that given any S-group G there exists a unique S-groups map $F(S) \to G$ (section 1.4).

A set of group relations on S is a subset R of $F(S) \times F(S)$. An S-R-group G is an S-group such that, for $\varphi : F(S) \to G$ the unique map of S-groups, one has $\varphi(x) = \varphi(y)$ for all $(x, y) \in R$. There exist a universal S-R-group, unique up to unique S-group isomorphisms, which will be denoted $\langle S|R\rangle$ (section 1.5). The following theorem helps us to recognize $\langle S|R\rangle$ (theorem 3.1.1).

Theorem. *Let S be a set, and let R be a set of group relations on S. Let G be a set and let $1_G \in G$ be an element. Suppose for every $s \in S$ a bijection $\pi_s : G \to G$ is given. Then the following are equivalent:*

(1) *There is an S-R-group with underlying set G and neutral element 1_G such that for all $s \in S$ and $x \in G$ one has $sx = \pi_s(x)$. This S-R-group is isomorphic, as an S-R-group, to $\langle S|R\rangle$.*

(2) *The following three conditions are satisfied:*

   (i) *For each S-R-group G' there exists a map $\varphi : G \to G'$ such that $\varphi(1_G)$ is the neutral element of G' and one has $\varphi(\pi_s(x)) = s\varphi(x)$ for all $s \in S$ and $x \in G$.*

   (ii) *The group $\mathrm{Sym}(G)$ of all permutations of G together with the map $S \to \mathrm{Sym}(G)$ defined by $s \mapsto \pi_s$ is an S-R-group.*

   (iii) *The only subset $T \subseteq G$ with $1_G \in T$ such that for all $s \in S$ one has $\pi_s(T) = T$ is $T = G$.*

The main goal of this thesis is to give a proof of this theorem. The theorem is a formalized version of what is called "Van der Waerden's trick" which is used to check if a given set is a set of normal forms for the elements of

$\langle S|R\rangle$. In section 1.5 we will see that $\langle S|R\rangle$ is a quotient of $F(S)$ so we have a surjective map $F(S) \twoheadrightarrow \langle S|R\rangle$. We say that a subset V of $F(S)$ is a set of normal forms for the elements of $\langle S|R\rangle$ if the restriction of the above map to V is bijective. To do this in practice without using this method we should first find such a set and define a multiplication and then check if what we get is isomorphic to $\langle S|R\rangle$. Usually it is not easy to prove that the defined multiplication is associative. The idea of Van der Waerden allows us to prove that we can define an S-R-group structure on V such that it is isomorphic to $\langle S|R\rangle$, without proving associativity. In fact we do not even have to define a multiplication for every pair of elements, but only the left multiplication by a generator. If we do this and then we check that conditions (i), (ii) and (iii) are satisfied G has an S-R-group structure that is isomorphic to $\langle S|R\rangle$. Van der Waerden's method cannot be used to find such a structure, it is only useful to check, when we have a guess, if the guess is right.

The method can be applied not only to groups, but also to other associative algebraic structures which can be presented with generators and relations. In this thesis we will treat monoids, groups and rings. We will begin in the first chapter by proving the existence of structures as above for each S and R. Then we will go through the proof of the theorems and we present some examples. Originally Van der Waerden used his method for proving, more efficiently than had been done before, that we can give a normal form to the elements of the sum of groups (see [1]). Later he applied it to a construction regarding rings, namely the Clifford algebra (see [2]). The method has subsequently been used to prove that under certain assumptions we can find a normal form for the elements of an amalgamated sum of groups over a subgroup (this can be found in Serre's book [3] and Kurosh's [4], for example) and, also by Serre in the same book as an exercise, for some particular kind of amalgamated sums of rings. In the notes by Bergman ([6]) Van der Waerden's method is used frequently for proving normal forms for a lot of constructions of this kind in the case of groups, rings and also monoids. I could not find in the literature a statement of the method as a theorem valid for all sets S and for all sets of relations R, as the theorems we are proving in this thesis.

In section 2.3 we will build a normal form for the elments of some amalgamated sums of monoids over a submonoid. In this case we will not be able to give a completely explicit normal form, but we will show that we can understand the structure of the amalgamated sum by proving a theorem (theorem 2.3.8) about it. In section 4.2 we state a possible generalisation of Van der Waerden's discussion of Clifford Algebras.

Chapter 1

Generators and relations

Before introducing Van der Waerden's method we discuss free structures and structures presented by generators and relations. The theorem in fact, at least in the form we will state it, does not prove the existence of such structures. We prove it by showing how to build them up, but we will not be able to see what the elements of these structures look like. In order to understand what will follow, we first recall some basic facts about category theory that will be used in the following sections, before going into the details of each algebraic structure.

1.1 Category theory

Let us recall what a category is and then we will recall some other basic facts about categories.

Definition 1.1.1. (*Category*) A category consists of:

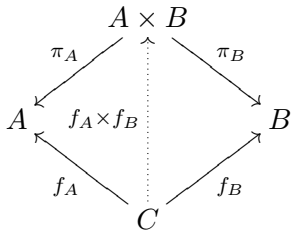
- A class $\mathscr{C}$, whose elements are called *objects*.
- For each pair of objects (A, B) a set $\mathrm{Hom}(A, B)$ whose elements are called *morphisms* and are denoted by *arrows*: $f \in \mathrm{Hom}(A, B)$ is denoted $f : A \to B$.
- For any three objects A, B and C an operation $\circ : \mathrm{Hom}(B, C) \times \mathrm{Hom}(A, B) \to \mathrm{Hom}(A, C)$, called *composition law*. As usual one writes $\circ(f, g) = f \circ g$.

The above items are such that the following conditions are satisfied:

(1). For each object A there is an element $\mathrm{Id}_A \in \mathrm{Hom}(A, A)$, called the identity of A, such that for each morphism $f \in \mathrm{Hom}(A, B)$ we have $f \circ \mathrm{Id}_A = f$ and for each morphism $g \in \mathrm{Hom}(B, A)$ we have $\mathrm{Id}_A \circ g = g$.

(2). The composition law is an associative operation.

As examples of categories think about sets and maps between sets, groups and homomorphisms of groups or, more generally, algebraic structures and set maps which respect the operations. Some definitions we give separately in different settings have a generalization in a general category. For example in set theory one defines the cartesian product of A and B by saying that it is the set of all pairs of elements in which the first one is in A and the second in B. One can then prove that this particular set has a *universal property*, namely: there are two maps $\pi_A : A \times B \to A$ and $\pi_B : A \times B \to B$ such that for each set C with two maps $f_A : C \to A$ and $f_B : C \to B$ there exists a unique map $f_A \times f_B : C \to A \times B$ such that the following diagram commutes



This property can be taken as a definition of the cartesian product of A and B. In general we say that two objects A and B of a category have a product and that their product is $A \prod B$ if this object satisfies the same universal property. For example for two groups their categorical product is their direct product.

If in a category we have an object with some universal property then it can be seen as an initial object in some ad hoc built category:

Definition 1.1.2. (*Initial objects*) Let $\mathscr{C}$ be a category and let A be one of its objects. We say that A is an *initial object* in $\mathscr{C}$ if for each object B there exists a unique morphism $A \to B$.

We did this brief introduction to category theory because all the structures presented by generators and relations have some universal property and to prove their existence we will use this idea: first define a category in which those structures are initial objects and then prove that there is such an object in these categories. To conclude the section we prove that initial objects are unique so that we will not have to prove uniqueness in each case in the rest of the chapter. First recall that an isomorphism between two objects A and B in a category is a morphism $f : A \to B$ such that there exists a morphism $g : B \to A$ such that the compositions $f \circ g$ and $g \circ f$ are both the identity (of B and A respectively).

Lemma 1.1.3. *Let $\mathscr{C}$ be a category and let A be an initial object. Then, if B is another initial object for $\mathscr{C}$, there exists a unique isomorphism $f : A \to B$.*

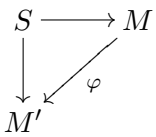
Proof. Since A is initial there is a unique morphism $A \to A$ and this must be the identity Id_A. The same is true for B. Moreover since they are both initial we have two unique morphisms $f : A \to B$ and $g : B \to A$. The compositions $f \circ g$ and $g \circ f$ are morphisms and they are $B \to B$ and $A \to A$ respectively. So it follows, from what we said before, that $f \circ g = \mathrm{Id}_B$ and $g \circ f = \mathrm{Id}_A$. Then f is a unique isomorphism from A to B. □

1.2 Free monoids

Let us start with the simplest structure for which we can use Van der Waerden's method, namely, monoids. We will first recall what a monoid is and then define the category of S-monoids, in which the free monoid is an initial object.

Definition 1.2.1. (*Category of monoids*) A monoid M is a set which has an associative operation (which we will usually denote multiplicatively) with a neutral element (which will usually be denoted by 1_M). If M' is also a monoid, a morphism $M \to M'$ is a map which respects both the multiplication and the unit element.

Definition 1.2.2. (*Category of S-monoids*) Given a set S, an S-monoid is a monoid M together with a map $S \to M$. This map will be usually denoted by the empty symbol (i.e. the image of $s \in S$ in M is denoted s). An S-monoid morphism (or S-map) $M \xrightarrow{\varphi} M'$ is a monoid morphism such that the following diagram commutes:



Notice that the identity $\mathrm{Id_M}$ of a monoid M is clearly an S-map which satisfies condition (1) in definition 1.1.1 and the composition of two S-maps, when possible, is again an S-map, so these define a category.

We remark that the map $S \to M$ is not assumed to be injective. The initial object, if it exists, in this category is the *free monoid* over the set S. We will denote such an object as $F_{\mathrm{Mon}}(S)$ or $F(S)$, if no confusion can arise. In the case of monoids is very easy to show that this object exists, and we will do it in the next proposition.

Proposition 1.2.3. *For each set S the category of S-monoids has an initial object.*

Proof. Since we do not have any relation we can just consider the set of all finite words taking S as an alphabet (we consider the empty word as a word of length zero); we will denote it again by $F(S)$. This is a monoid with concatenation of words as multiplication and the empty word as a neutral element. It is also an S-monoid by mapping $s \in S$ to the word of length one s in $F(S)$.

We now show it is initial in the category of S-monoids. First we notice that an element of $F(S)$ can be written as $s_1 \cdots s_n$, with each $s_i \in S$ and $n \geq 0$. We want to prove that given any S-monoid M, we have a unique map $\varphi : F(S) \to M$. We define that maps $\varphi(s_1 \cdots s_n)$ to be the product $s_1 \cdots s_n$ in M and the empty word in the neutral element of M. This is a monoid map, in fact the unit element is respected by definition and if $x = s_1 \cdots s_n$ and $y = s'_1 \cdots s'_n$ in $F(S)$ we have

$$\varphi(xy) = \varphi(s_1 \cdots s_n s'_1 \cdots s'_n) = s_1 \cdots s_n s'_1 \cdots s'_n \text{ (product in } M).$$

By the associative law in M we can consider the last product above as $(s_1 \cdots s_n)(s'_1 \cdots s'_n)$, which is $\varphi(x)\varphi(y)$ so also the multiplication is respected by φ. Moreover, by definition, if we take a word of length one then $\varphi(s) = s$ so φ is also an S-map. Let us suppose that ψ is another S-map from $F(S)$ to M. By definition we have $\psi(1) = 1 = \varphi(1)$ and $\psi(s) = s = \varphi(s)$ for $s \in S$. On a word $x = s_1 \cdots s_n$ with $n \geq 1$ we have, since ψ respects products:

$$\begin{aligned} \psi(x) = \psi(s_1 \cdots s_n) = \psi(s_1) \cdots \psi(s_n) = \\ = \varphi(s_1) \cdots \varphi(s_n) = \varphi(s_1 \cdots s_n) = \varphi(x). \end{aligned}$$

So $\psi = \varphi$ and φ is unique, so $F(S)$ is the initial object in the category of S-monoids. □

1.3 Relations

Before starting to consider further free structures we discuss relations on monoids. Someone who is familiar with relations on groups may be used to see relations given by one word. In the case of monoids this is not possible. A relation for us will then always be (even in the case of groups or rings) a pair of elements of the free object. More precisely:

Definition 1.3.1. (*Monoid relation on S*) Let S be a set. A monoid relation between the elements of S is an element of $F(S) \times F(S)$ (cartesian product); a set of monoid relations for the elements of S is then a set $R \subseteq F(S) \times F(S)$. In the following we will sometimes write *relations* for *monoid relations*, if no confusion can arise.

We can now define the category of S-R-monoids, in which the monoid $\langle S|R\rangle_{\mathrm{Mon}}$, given with set of generators S and set of relations R, is an initial object.

Definition 1.3.2. (*Category of S-R-monoids*) Given a set S and a set R of relations on S an S-R-monoid M is an S-monoid with the property that for all pairs $(w_1, w_2) \in R$ the unique morphism $\varphi : F(S) \to M$ satisfies $\varphi(w_1) = \varphi(w_2)$. An S-R-monoid morphism is an S-monoid morphism between two S-R-monoids.

As before, if no confusion can arise, we will use the notation $\langle S|R\rangle$ for $\langle S|R\rangle_{\mathrm{Mon}}$. The existence of one initial object in this category is proved again by exhibiting one monoid with the required property; first we have to define, given a set of relations R, an equivalence relation on $F(S)$:

Definition 1.3.3. (*Relation $\sim_R$*) Let S be a set and let R be a set of relations for S. Let $x, y \in F(S)$ and define $x \sim_R y$ if and only if for all S-R-monoids M one has $\varphi(x) = \varphi(y)$, where φ is the map $F(S) \to M$.

Notice that by the definition of S-R-monoid we have that when the pair $(w_1, w_2) \in R$ then $\varphi(w_1) = \varphi(w_2)$ and so $w_1 \sim_R w_2$.

Proposition 1.3.4. *The relation $\sim_R$ is an equivalence relation and if $x \sim_R x'$ and $y \sim_R y'$ then $xy \sim_R x'y'$.*

Proof. Reflexivity, symmetry and transitivity are clear so it is an equivalence relation. Now suppose we have $x \sim_R x'$ and $y \sim_R y'$, then we can write:

$$\varphi(xy) = \varphi(x)\varphi(y) = \varphi(x')\varphi(y') = \varphi(x'y')$$

since φ is a homomorphism, so the proposition is proved. □

The property we proved implies that the operation on $F(S)$ induces an operation on $F(S)/\!\sim_R$ which becomes a monoid. Our claim is that $F(S)/\!\sim_R$ is the monoid $\langle S|R\rangle$.

Proposition 1.3.5. *For every set S the monoid $F(S)/\!\sim_R$ is an initial object in the category of S-R-monoids.*

Proof. We show first that $F(S)/\!\sim_R$ is an S-R-monoid and next that there is a unique morphism to each S-R-monoid. We can define the map from the set S by composing the map $S \to F(S)$ with the projection $F(S) \to F(S)/\!\sim_R$. Let us take a pair $(w_1, w_2) \in R$, we have to show that the unique S-map $\pi_R : F(S) \to F(S)/\!\sim_R$, which is the projection, satisfies $\pi_R(w_1) = \pi_R(w_2)$,

and this is true by the definition of $\sim_R$. So $F(S)/\sim_R$ is an S-R-monoid. We can notice that given any S-monoid M we have an injection

$$\mathrm{Hom}_S(F(S)/\sim_R, M) \hookrightarrow \mathrm{Hom}_S(F(S), M)$$

namely the one that sends a map f to the composition $\widetilde{f} = f \circ \pi_R$. So there is at most one map from $F(S)/\sim_R$ to any S-monoid, since the right hand side is a set with one element. We now show that we have at least one map from $F(S)/\sim_R$ to an S-R-monoid M. Let $\varphi : F(S) \to M$ be the unique S-map from $F(S)$ to M. It is clear from the definition of $\sim_R$ that the map $\widetilde{\varphi} : F(S)/\sim_R \to M$ induced by φ, namely the map $\widetilde{\varphi}([x]) = \varphi(x)$, is well defined. So there exist exactly one morphism from $F(S)/\sim_R$ to any S-R-monoid and so $F(S)/\sim_R$ is an initial object in the category of S-R-monoids, as we wanted to prove. □

We can now notice that, even if we proved the existence of $\langle S|R\rangle$ in every possible case, we do not have an idea what its elements look like. When we are able to guess a normal form for one of these monoids, Van der Waerden's method will help us checking if our guess is right. Before going on we prove some results that will be used later on.

Proposition 1.3.6. *Let M be a sub-S-monoid of $\langle S|R\rangle$. Then $M = \langle S|R\rangle$.*

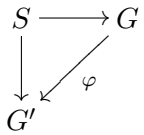
Proof. Since the multiplication in M is the same as in $\langle S|R\rangle$ the S-monoid M is also an S-R-monoid. So there exists a unique S-map $\langle S|R\rangle \to M$. Since M is a subset of $\langle S|R\rangle$ we also have the inclusion map $M \hookrightarrow \langle S|R\rangle$, which is also an S-map. The composition is an S-map from $\langle S|R\rangle$ in itself, so it must be the identity. So the inclusion is surjective and $M = \langle S|R\rangle$. □

Before stating and proving the main theorems we will discuss groups and rings presented by generators and relations.

1.4 Free groups

As for monoids we start by defining a category where the free group on the set S is an initial object.

Definition 1.4.1. (*Category of S-groups*) Given a set S an S-group is a group G together with a map $S \to G$. Morphisms (called also S-maps) are group morphisms $G \xrightarrow{\varphi} G'$ such that the following diagram commutes:



Since the identity is an S-map which satisfies condition (1) of definition 1.1.1 and the composition of two S-maps is an S-map these define a category.

We define the free group on a set S by taking a particular monoid $\langle \widetilde{S}|R\rangle_{\mathrm{Mon}}$ and showing that it is an initial object in the category of S-groups. The set $\widetilde{S}$ is the disjoint union of the set S with a set S^{-1} which is disjoint from it and is endowed with a bijection $S \to S^{-1}$ which will be denoted by $s \mapsto s^{-1}$. We will denote also the inverse map with the same symbol so that $(s^{-1})^{-1} = s$ for all $s \in \widetilde{S}$. The set of relations is the set

$$R = \{(ss^{-1}, 1) : s \in \widetilde{S}\}$$

which tells us that s and s^{-1} are inverses. Notice that this structure has a non-trivial set of relations, even if we claim it is the free group on the set S. This can be explained by considering that being "free" for an algebraic structure means that the only relations satisfied are the ones that follow from its defining properties. Then a structure which is free as a group is not free as a monoid because the relations that are necessary for groups (imposing that each element has an inverse) are not necessarily satisfied in a monoid. We will denote the monoid $\langle \widetilde{S}|R\rangle_{\mathrm{Mon}}$ as $F(S)_{\mathrm{Grp}}$ or only $F(S)$ if no confusion can arise. To show that the monoid defined above is the free group on the set S we first prove that it is a group and then that it is an initial object in the category of S-groups.

Proposition 1.4.2. *The monoid $\langle \widetilde{S}|R\rangle_{\mathrm{Mon}}$ is an S-group.*

Proof. We know that $\langle \widetilde{S}|R\rangle_{\mathrm{Mon}}$ is an S-monoid so we already have the map $S \to \langle \widetilde{S}|R\rangle_{\mathrm{Mon}}$ and then in order to conclude we just have to show that it is a group. Given any monoid M we can consider the set of invertible elements, denoted M^*, which is a group. The set $\widetilde{S}$ is contained, according to the relations, in $\langle \widetilde{S}|R\rangle^*_{\mathrm{Mon}}$ and by proposition 1.3.6 one has $\langle \widetilde{S}|R\rangle^*_{\mathrm{Mon}} = \langle \widetilde{S}|R\rangle_{\mathrm{Mon}}$ so $\langle \widetilde{S}|R\rangle_{\mathrm{Mon}}$ is a group. □

Proposition 1.4.3. *For every set S, the group $\langle \widetilde{S}|R\rangle_{\mathrm{Mon}} = F(S)_{\mathrm{Grp}}$ is an initial object in the category of S-groups.*

Proof. Let G be an S-group; the image of $s \in S$ is invertible in G, since it is a group, so there is a unique element s^{-1} in G which is the inverse of s. We can then build a map $\widetilde{S} \to G$, so G is an $\widetilde{S}$-monoid. The relations in R are satisfied in G (since $ss^{-1} = s^{-1}s = 1$ because s and s^{-1} are inverses) so G is also an $\widetilde{S}$-R-monoid. Then there is a unique $\widetilde{S}$-map $\varphi : \langle \widetilde{S}|R\rangle_{\mathrm{Mon}} \to G$. The map φ is also an S-map since S is a subset of $\widetilde{S}$ and the map $\widetilde{S} \to G$ coincides with $S \to G$ on S. So $\langle \widetilde{S}|R\rangle_{\mathrm{Mon}}$ is initial. □

At this point one can notice again that we do not have an idea of what the elements of this group look like. We know each is an equivalence class for

some equivalence relation on the free monoid $F(S)_{\mathrm{Mon}}$, but we do not know their shape. With Van der Waerden's method for groups we will be able to prove that each element has a normal form. More precisely we will prove that in each class we can choose a representative with the following form:

$$w = 1 \text{ or } w = x_1 x_2 \cdots x_n$$

with each $x_i \in \widetilde{S}$ and no two successive letters are inverse to each other.

1.5 Relations on groups

We can define S-R-groups and build the universal group with generators S and relations R exactly as we did for monoids, namely the group $\langle S|R\rangle_{\mathrm{Grp}}$ is a quotient of $F(S)_{\mathrm{Grp}}$. We start as before with the definition of relations.

Definition 1.5.1. (*Group relation on S*) Let S be a set. A group relation between the elements of S is an element of $F(S) \times F(S)$; a set of group relations for the elements of S is then a set $R \subseteq F(S) \times F(S)$. We will sometimes write *relations* for *group relations*, if no confusion can arise.

Definition 1.5.2. (*Category of S-R-groups*) Let S be a given set and let R be a set of group relations between the elements of S. An S-group G is called an S-R-group if for each pair $(w_1, w_2) \in R$ one has $\varphi(w_1) = \varphi(w_2)$ where φ is the unique morphism $F(S) \to G$. A morphism of S-R-groups is an S-map between two S-R-groups.

The definitions and the proofs are exactly as for monoids.

Definition 1.5.3. (*Relation $\sim_R$*) Let $x, y \in F(S)$ and define $x \sim_R y$ if and only if for every S-R-group G we have $\varphi(x) = \varphi(y)$ where φ is the unique map $F(S) \to G$.

Proposition 1.5.4. *The relation $\sim_R$ is an equivalence relation and if $x \sim_R x'$ and $y \sim_R y'$ then $xy \sim_R x'y'$.*

Proposition 1.5.4 implies that the quotient $F(S)/\!\sim_R$ is a group, and of course also an S-group. One can prove as before that $F(S)/\!\sim_R$ is also an S-R-group and then that it is an initial object in the category of S-R-groups.

Proposition 1.5.5. *For every set S and for every set of group relations R on S, the group $F(S)/\!\sim_R$ is an initial object in the category of S-R-groups.*

Proof. The proof goes exactly as for monoids. As we said $F(S)/\!\sim_R$ is an S-group and the fact that the relations in R are respected follows, as we did for monoids, from the definition of $\sim_R$, since the unique S-map

$F(S) \to F(S)/\sim_R$ is the projection so $F(S)/\sim_R$ is also an S-R-group. Given any S-group G we have an injection

$$\mathrm{Hom}_S(F(S)/\sim_R, G) \hookrightarrow \mathrm{Hom}_S(F(S), G)$$

so there is at most one map from $F(S)/\sim_R$ to any S-group. We can exhibit one map from $F(S)/\sim_R$ to G, when G is an S-R-group, as before. Let $\varphi : F(S) \to G$ be the unique S-map from $F(S)$; by the definition of the relation $\sim_R$ the map $\widetilde{\varphi} : F(S)/\sim_R \to G$ induced by φ is well defined so it is in $\mathrm{Hom}_S(F(S)/\sim_R, G)$. So there exists exactly one morphism from $F(S)/\sim_R$ to any S-R-group and so $F(S)/\sim_R$ is an initial object, as we wanted to prove. □

It can be interesting at this point to show that the usual way of presenting groups with generators and relations is in fact equivalent to the one we defined. This is what the following proposition states.

Proposition 1.5.6. *Let S be a set and R a set of group relations on S. Let M be the group $\langle S|R\rangle$ and H be the smallest normal subgroup of $F(S)$ containing the elements which can be written xy^{-1} with the pair (x, y) in R. Then M is isomorphic to $F(S)/H$.*

Proof. We want to show that $F(S)/H$ is an initial S-R-group. Let M' be an S-R-group. Since M' is an S-group there exist a unique S-map $\varphi : F(S) \to M'$. We want to show that this induces a map $\psi : F(S)/H \to M'$ so we have to show that $\varphi(x) = 1$ for x in H. We show that this is true for the generators of H and this implies the claim. Let xy^{-1} be a generator of H so $(x, y) \in R$ and then, by the definition of $\sim_R$, we have $\varphi(x) = \varphi(y)$ so $\varphi(xy^{-1}) = 1$. Then there exists a map ψ as above. This is an S-group map since $\psi([s]) = \varphi(s) = s$ and we show that it is unique. Let ψ' be another S-map from $F(S)/H$ to M'. Then we have:

$$\begin{aligned}\psi'([s_1 \cdots s_n]) = \psi'([s_1] \cdots [s_n]) = \psi'([s_1]) \cdots \psi'([s_n]) = s_1 \cdots s_n = \\ = \varphi(s_1) \cdots \varphi(s_n) = \varphi(s_1 \cdots s_n) = \psi([s_1 \cdots s_n]).\end{aligned}$$

So $F(S)/H$ is initial and hence isomorphic to M. □

As we did for monoids we prove here that the set S generates the group $\langle S|R\rangle$.

Proposition 1.5.7. *Let G be a sub-S-group of $\langle S|R\rangle$. Then $G = \langle S|R\rangle$.*

Proof. Can be done as for monoids. The multiplication in G is the same as in $\langle S|R\rangle$ so it is also an S-R-group. Then there exists a unique S-map $\langle S|R\rangle \to G$, but G is a subset of $\langle S|R\rangle$ so there exists also the inclusion map

$M \hookrightarrow \langle S|R\rangle$, which is an S-map. The composition is also an S-map from $\langle S|R\rangle$ in itself, so it must be the identity. So the inclusion is surjective and $G = \langle S|R\rangle$.

□

1.6 Free k-algebras

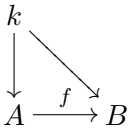
In the remainder of this chapter we will discuss rings presented by generators and relations. By a ring we will always mean an associative ring with a multiplicative neutral element, but not necessarily commutative. Since the theory for rings (which are $\mathbb{Z}$-algebras) is not easier than the more general theory for k-algebras where k is a commutative ring, we will consider this latter case. We will then from now on suppose to have a fixed commutative base ring k. We start by giving some definitions.

Definition 1.6.1. (*Center of a ring*) Let A be any ring. The *center* of A is the subset of the elements which commute with all the elements in A:

$$Z(A) = \{x \in A | \forall y \in A, xy = yx\}$$

It is a commutative subring of A.

Definition 1.6.2. (*Category of k-algebras*) An object in the category of k-algebras is a ring A together with a ring homomorphism $f : k \to A$ such that $f(k) \subseteq Z(A)$. A morphism between two k-algebras A and B is a ring homomorphism $f : A \to B$ such that the following diagram commutes:



Definition 1.6.3. (*Category of S-k-algebras*) Given a set S we define an S-k-algebra A to be a k-algebra together with a map $S \to A$. As usual morphisms of S-k-algebras are morphisms of k-algebras which respect this map.

Definition 1.6.4. (*Free k-algebra over S*) Given a set S an initial object in the category of S-k-algebras is called the free k-algebra over the set S and is denoted $k\langle S\rangle$.

In order to prove the existence of free k-algebras we will make use of free modules over a ring. We then recall briefly the definition of a module and the construction of a free module.

Definition 1.6.5. (*A-module*) Let A be a ring. We define a left module M over A to be an abelian group together with a map $f : A \times M \to M$, which is denoted with the empty symbol so that $f(a, m) = am$, such that the following conditions are satisfied:

- $1_A m = m$ for every $m \in M$.
- $(a + b)m = am + bm$ for every $m \in M$ and $a, b \in A$.
- $(ab)m = a(bm)$ for every $m \in M$ and $a, b \in A$.
- $a(m + m') = am + am'$ for every $m, m' \in M$ and $a \in A$.

Remark 1.6.6.

1. Let us notice that each k-algebra A is a k-module with the multiplication defined by $hx = f(h)x$ where $h \in k$, the map $f : k \to A$ is the map that gives A the structure of a k-algebra and the multiplication in the right hand side is taken in A. All the properties are trivial and follow from the definition of a ring.

2. On a general ring A one can define similarly right A-modules and A-A-bimodules. Bimodules have both a structure of right and left A-module and these structures are compatible in the sense that $a(xb) = (ax)b$ for every $a, b \in A$ and x in the module. It is important for us to point out that in the case A is a k-algebra over a commutative ring k if we define a left k-module structure as we saw above and a right k-module structure in a similar way then, since k maps to the center by definition, these structures coincide and give A the structure of a k-k-bimodule.

We now recall the definition of a free left A-module over some set S. Before giving the definition recall that given a collection of left modules over the same ring A we can build their direct sum (as abelian groups) and give it a left A-module structure in this way:

$$ax = a(x_1 + \ldots + x_n) = ax_1 + \ldots + ax_n.$$

The verifications of the properties are straightforward.

Definition 1.6.7. (*free left A-module over the set S*) Let A be a ring and S be a set. We can define the category of S-A-modules as we did for monoids and groups, so the objects are A-modules M with a map $S \to M$ and morphism are maps of modules that respect the map from S. The initial object in this category is called the free left A-module over the set S and can be realized by considering the abelian group

$$M = \bigoplus_{s \in S} A$$

with multiplication induced by the multiplication in A. One can show that this A-module is an S-A-module with the map $s \mapsto 1_A$ (in the copy of A corresponding to the element s) and that it is initial.

With these constructions we are now able to prove existence of free k-algebras.

Proposition 1.6.8. *Let S be a set and let k be a commutative ring. Then there exists an initial object in the category of S-k-algebras.*

Proof. Let us consider the free monoid $F(S)$ and denote by $k\langle S\rangle$ the free k-module over $F(S)$. If w and w' are elements of $F(S)$ and h and h' are elements of k we define a multiplication on $k\langle S\rangle$ in this way: $(hw)(h'w') = (hh')(ww')$. Extending this multiplication by k-linearity, one can show that this is a k-algebra with the map $h \in k \mapsto h1 \in k\langle S\rangle$ (as usual 1 denotes the empty word). We can define a map $S \to k\langle S\rangle$ by sending $s \in S$ to $1_k s$, so that $k\langle S\rangle$ is an S-k-algebra. Now we want to show that given any S-k-algebra A there is a unique map $\varphi : k\langle S\rangle \to A$. Let us prove existence first. We need to make both these diagrams commutative:

We can see that the multiplicative monoid of any S-k-algebra A is naturally an S-monoid and we denote it by M. Since M is an S-monoid there exists a unique map $\varphi_M : F(S) \to M$. We define φ over $1_k F(S)$ to be $\varphi(1_k w) = \varphi_M(w)$. In particular $\varphi(1_k s) = \varphi_M(s) = g_S(s)$ so the first diagram is commutative. We extend φ by k-linearity (so that $\varphi(h_1 x_1 + \ldots + h_n x_n) = h_1\varphi(x_1) + \ldots h_n\varphi(x_n)$) and we get the commutativity of the second diagram:

$$\varphi(h1) = h\varphi(1) = h\varphi_M(1) = h1_A = g(h)1_A = g(h).$$

So φ becomes a map of S-k-algebras defined on the whole $k\langle S\rangle$.

We now want to show that φ is unique. Suppose that φ' is another S-k-algebra morphism from $k\langle S\rangle$ to A. For the commutativity of the diagrams above we must have $\varphi'(1_k s) = \varphi(1_k s)$ for all $s \in S$. Since φ' has to respect the multiplication in $k\langle S\rangle$ we get that φ' is equal to φ on the whole subset $1_k F(S)$. Then $\varphi' = \varphi$ everywhere since φ' is k-linear. □

1.7 Relations on k-algebras

We have now a definition of free k-algebra on a set for every S and we want to introduce relations on it. The way we do it is very similar to what we did for monoids and groups.

Definition 1.7.1. (k-algebra relation on S) Let S be a set. A k-algebra relation on S is an element of $k\langle S\rangle \times k\langle S\rangle$. A set of k-algebra relations is then a subset of $k\langle S\rangle \times k\langle S\rangle$. We will sometimes write *relation* for *k-algebra relation*, if no confusion can arise.

Definition 1.7.2. (Category of S-R-k-algebras) Given a set S and a set of relations on $k\langle S\rangle$ we define an S-R-k-algebra to be an S-k-algebra A such that the unique map $\varphi : k\langle S\rangle \to A$ satisfies $\varphi(x) = \varphi(y)$ for every pair $(x, y) \in R$. A morphism of S-R-k-algebras is a morphism of S-k-algebras between two S-R-k-algebras.

Definition 1.7.3. (Relation $\sim_R$) Let S be a set and let R be a set of relations on $k\langle S\rangle$. We define an equivalence relation $\sim_R$ on $k\langle S\rangle$, by saying that $x \sim_R y$ if and only if for all S-R-k-algebras A one has $\varphi(x) = \varphi(y)$ where φ is the unique S-k-algebra morphism $k\langle S\rangle \to A$.

We can prove that we can define a k-algebra structure on the quotient of $k\langle S\rangle$ by $\sim_R$. We do this in the following proposition.

Proposition 1.7.4. *The relation $\sim_R$ is an equivalence relation and if $x \sim_R x'$ and $y \sim_R y'$ then $x + y \sim_R x' + y'$ and $xy \sim_R x'y'$.*

Proof. The fact that $\sim_R$ is an equivalence relation is clear. The other properties follow from the fact that φ is a morphism of rings. □

We want now to show that the k-algebra that we have just defined is an initial object in the category of S-R-k-algebras. The way we will do it is very similar to what we did for monoids and groups.

Proposition 1.7.5. *For every set S the k-algebra $k\langle S\rangle/\sim_R$ is an initial object in the category of S-R-k-algebras.*

Proof. It is clear from proposition 1.7.4 that $k\langle S\rangle/\sim_R$ is an S-R-k-algebra. Let A be any S-k-algebra, we have an injection

$$\mathrm{Hom}(k\langle S\rangle/\sim_R, G) \hookrightarrow \mathrm{Hom}(k\langle S\rangle, G)$$

so there exists at most one S-R-k-algebra map from $k\langle S\rangle/\sim_R$ to any S-k-algebra. Suppose now that A is an S-R-k-algebra. We can induce a map $k\langle S\rangle/\sim_R \to A$ from the unique map $k\langle S\rangle \to A$, and this is a well defined S-R-k-algebra map. By what we said it is unique so the proof is complete. □

As for groups also in the case of k-algebras, since congruences correspond to two sided ideals, we could have defined the relation $\sim_R$ to be the congruence corresponding to the smallest two sided ideal of $k\langle S\rangle$ consisting of all the elements $k_1x_1 + \ldots + k_nx_n - k'_1y_1 - \ldots - k'_my_m$ if the pair $(k_1x_1 + \ldots + k_nx_n, k'_1y_1 + \ldots + k'_my_m)$ is in $\sim_R$. We state the proposition without proof:

Proposition 1.7.6. *Let S be a set and R a set of k-algebra relations on S. Let A be the k-algebra $\langle S|R\rangle$ and I be the two-sided ideal of $k\langle S\rangle$ generated by the elements $x - y$ with x and y in $k\langle S\rangle$ such that $(x, y) \in R$. Then A is isomorphic to $k\langle S\rangle/I$.*

We conclude this section by proving a proposition similar to proposition 1.3.6, which we will use in proving theorem 4.1.1.

Proposition 1.7.7. *Let A be a sub-S-k-algebra of $\langle S|R\rangle$. Then $A = \langle S|R\rangle$.*

Proof. The proof is the same as the one we did in the monoid case. The multiplication in A is the same as in $\langle S|R\rangle$ so A is also an S-R-k-algebra. So there exist a unique morphism $\langle S|R\rangle \to A$. Since A is contained in $\langle S|R\rangle$ we also have the inclusion map $A \hookrightarrow \langle S|R\rangle$. This is clearly a morphism and so it is the composition. Since the composition is a morphism of $\langle S|R\rangle$ in itself, it must be the identity. Then the inclusion is surjective and $A = \langle S|R\rangle$. □

Chapter 2

The monoid case

2.1 The statement of the theorem

Let us begin by stating the theorem. After the statement we will give some examples to understand what the conditions we require mean in practice and then we will proceed to the proof. From now on we use the convention that an empty product is equal to the neutral element of the structure it belongs to. So in the next theorem when $n = 0$ the composition $\pi_{s_1} \circ \ldots \circ \pi_{s_n}$ is equal to Id_M and the product $s_1 \cdots s_n$ equals 1. In the same way when we will state the theorem for rings an empty sum will be the zero element.

Theorem 2.1.1. *Let S be a set, and let R be a set of monoid relations on S. Let M be a set and let $1_M \in M$ be an element. Suppose for every $s \in S$ a map $\pi_s : M \to M$ is given. Then the following are equivalent:*

(1) *There exists an S-monoid structure on M such that the multiplication $* : M \times M \to M$ has neutral element 1_M and satisfies $s * x = \pi_s(x)$ for all $s \in S$ and $x \in M$, and the pair $(M, S \to M)$ is a universal S-R-monoid.*

(2) *The following three conditions are satisfied:*

   (i) *For all S-R-monoids M' there exists a map $\varphi : M \to M'$ such that $\varphi(1_M) = 1_{M'}$ and $\varphi(\pi_s(x)) = s\varphi(x)$ for all $s \in S$ and $x \in M$.*

   (ii) *The collection of maps $(\pi_s)_{s \in S}$ has the following property: if the pair $(s_1 \cdots s_n, s'_1 \cdots s'_m) \in R$ for $n, m \geq 0$ then $\pi_{s_1} \circ \ldots \circ \pi_{s_n} = \pi_{s'_1} \circ \ldots \circ \pi_{s'_m}$ in M^M.*

   (iii) *The only subset $T \subseteq M$ with $1_M \in T$ such that for all $s \in S$ one has $\pi_s(T) \subseteq T$ is $T = M$.*

Moreover if there exists an S-monoid structure on M, with the required unit and translations, then it is unique.

As we already have mentioned Van der Waerden's method (theorem 2.1.1) is used, when we think that a certain set is a set of normal forms for the elements of a monoid given by generators and relations, to check if this is true. In the theorem the set of generators is S and the set of relations is R. So we are given the monoid $\langle S|R\rangle$ and our goal is to find a normal form for it. To do this we need a candidate and this is the role of the set M, in the notation of theorem 2.1.1. In this set we are requested to choose a unit element and to define the left multiplication by a generator. If we do that, by verifying properties (i), (ii) and (iii), we prove that condition (1) is true and so M has a monoid structure and is a universal S-R-monoid so M is in particular isomorphic to $\langle S|R\rangle$. If one among properties (i), (ii) and (iii) is not satisfied we should change the set of normal forms. We see now three examples to see that none of the three conditions is implied by the other two.

Example 2.1.2. In this example we will show that condition (i) does not follow from the other two.
Let $S = \{s\}$ and $R = \emptyset$. Let us take as M the set $\{1_M\}$ and $\pi_s = \mathrm{Id}_M$. Then if we take in property (i) the S-R-monoid M' to be the free monoid $F(S)$ we are not able to construct a map $\varphi : M \to F(S)$ with the required properties. In fact there is only one map $M \to F(S)$ such that $1_M \mapsto 1$ and we have $\varphi(\pi_s(1_M)) = \varphi(1_M) = 1 \neq s = s1 = s\varphi(1_M)$. Notice that both conditions (ii) and (iii) are clearly satisfied here. In this case M is an S-R-monoid which is not isomorphic to $\langle S|R\rangle$ since the map $\langle S|R\rangle \twoheadrightarrow M$ is surjective but not injective because we know that $\langle S|R\rangle \neq \{1\}$.

Example 2.1.3. In this example we will show that condition (ii) does not follow from the other two.
Let $S = \{s\}$ and $R = \{(s, 1)\}$. Let us take as M the set $F(S)$, with $1_M = 1$ and π_s the usual multiplication on the left by s in $F(S)$. Then condition (ii) is not satisfied since $\pi_s \neq \mathrm{Id_M}$. Condition (iii) is clearly true. Also condition (i) is satisfied since if M' is a S-R-monoid there is a unique S-map $M \to M'$, since M is the free monoid on the set S. In this case M is a monoid with a surjective map $M \twoheadrightarrow \langle S|R\rangle$ which is not injective.

Example 2.1.4. In this example we will show that condition (iii) does not follow from the other two.
Let $S = \emptyset$ and $R = \emptyset$. Let us take as M the set $F(\{x\})$, where x is some symbol, with unit element 1. Then condition (iii) is not satisfied since the requirement $\pi_s(T) \subseteq T$ for all $s \in S$ is empty so the set $T = \{1\}$ is a strict subset of M containing the neutral element and satisfying the above condition. Notice that here (ii) is empty and in (i) we can take $\phi(w) = 1_{M'}$ for every S-R-monoid M'. In this case M is an S-R-monoid and the map

$\langle S|R\rangle \hookrightarrow M$ is injective but not surjective.

We can now go on with the proof of the theorem and then we will see how to apply it in practice.

2.2 The proof of the theorem

The implication (1)⇒(2) is easy. The idea of the proof of the converse is the following: we prove that there is a submonoid of the monoid of all maps $M \to M$, namely the submonoid generated by the π_s, which is in bijection with M and so we have an induced multiplication on M. Then we prove that this multiplication makes M into an initial object in the category of S-R-monoids. This is the generalization of the idea of Van der Waerden on the free product of groups. The most useful feature of this method is that, since we define the multiplication on the set of normal forms from the composition on M^M, we do not have to prove associativity. We now see the proof in detail and then we will give an example to understand how to use it.

Proof. Assume (1) holds. Then (i) comes from the universal property, even with a unique φ. For (ii) suppose the pair $(x, y) \in R$ and let τ_x and τ_y be the left multiplication maps by x and by y respectively, in M^M. These maps are equal, since $x = y$ in M so, if $x = s_1 \cdots s_n$ and $y = s'_1 \cdots s'_m$, we have

$$\pi_{s_1} \circ \ldots \circ \pi_{s_n} = \tau_x = \tau_y = \pi_{s'_1} \circ \ldots \circ \pi_{s'_m}.$$

This is true also if one among x and y is the empty word. Let now T be a set satisfying the conditions in (iii). Then the set $\{x \in M | xT \subseteq T\}$ is a submonoid of M containing S and so, by proposition 1.3.6, it is equal to M. So for all $x \in M$ the element $x = x1_M$ is in the set xT and so it is in T. Then $x \in T$, and condition (iii) holds.
Now assume the three conditions (i), (ii) and (iii) are satisfied. Let us consider the set $M^M = L$ of the set maps $M \to M$. This set is clearly a monoid (the neutral element is Id_M and the operation is the composition) and the map $s \mapsto \pi_s$ makes it into an S-R-monoid by condition (ii). So from condition (i) we have a map $\varphi : M \to L$ such that $\varphi(1_M) = \mathrm{Id}_M$ and $\varphi(\pi_s(x)) = \pi_s \circ \varphi(x)$ for $s \in S$ and $x \in M$. Let $H = \langle \pi_s : s \in S \rangle$ be the submonoid of L generated by the maps π_s. We want to show that $\varphi(M) = H$. Let us consider the set $\{f \in L | f \circ \varphi(M) \subseteq \varphi(M)\}$. This is clearly a submonoid of L and it contains Id_M and all the maps π_s for $s \in S$, since $\pi_s \circ \varphi(M) = \varphi \circ \pi_s(M)$, so it contains the set H. Then we have: $H = H \circ \mathrm{Id}_M \subseteq \varphi(M)$. To prove the converse we prove that $M = \varphi^{-1}(H)$.

Let us consider the set $T = \varphi^{-1}(H)$ and apply condition (iii). We have that $1_M \in T$ and if $x \in T$ and $s \in S$ then also $\pi_s(x) \in T$ since:

$$x \in T \Leftrightarrow x \in \varphi^{-1}(H) \Leftrightarrow \varphi(x) \in H \Rightarrow \pi_s \circ \varphi(x) \in H \Leftrightarrow$$
$$\Leftrightarrow \varphi(\pi_s(x)) \in H \Leftrightarrow \pi_s(x) \in \varphi^{-1}(H) \Leftrightarrow \pi_s(x) \in T.$$

By condition (iii) we then get $T = M$ and we proved that $\varphi(M) \subseteq H$ and so they are equal since we proved the other inclusion before.
Define now the map $\psi : L \to M$ by $f \mapsto f(1_M)$. We claim that this map is a left inverse for φ. We use again condition (iii), on the set

$$T = \{x \in M : \psi \circ \varphi(x) = x\}.$$

It is clear that $1_M \in T$ since $\psi \circ \varphi(1_M) = \psi(\mathrm{Id}_M) = \mathrm{Id}_M(1_M) = 1_M$. Let now $x \in M$ and $s \in S$; we have:

$$x \in T \Leftrightarrow \varphi(x)(1_M) = x \Rightarrow (\pi_s \circ \varphi(x))(1_M) = \pi_s(x) \Leftrightarrow$$
$$\Leftrightarrow \varphi(\pi_s(x))(1_M) = \pi_s(x) \Leftrightarrow \pi_s(x) \in T.$$

So $T = M$ and ψ is a left inverse for φ.
From this we know that the restriction $\psi : H \to M$ is bijective and its inverse is φ. This fact allow us to conclude the proof. Since H is an S-R-monoid we can induce a monoid multiplication on M, namely $x_1 * x_2 = \psi(\varphi(x_1) \circ \varphi(x_2))$ and this multiplication makes M also into an S-R-monoid. The map from S comes from the map $S \to H$ so it is the map $s \mapsto \psi(s)$. Since H is generated by the π_s we have that M is generated by the image of S in M and from this we get that the map in (i) is unique and hence M is a universal S-R-monoid. We notice explicitly that the translation maps are as we wanted:

$$s * x = \psi(\pi_s \circ \varphi(x)) = \psi(\varphi(\pi_s(x))) = \pi_s(x).$$

We still have to prove the uniqueness of the S-monoid structure. Suppose that $\#$ also makes M into a universal S-R-monoid, with the required unit and translations. Then the map $S \to M$ must be the same by the condition on the translations applied to $x = 1_M$ in fact

$$s * 1_M = \pi_s(1_M) = s \# 1_M.$$

We now prove that the multiplications coincide. Let us consider, for each $x \in M$, the set $T_y = \{x \in M : x * y = x \# y\}$. For all $y \in M$ one has $1 \in T_y$ and:

$$x * y = x \# y \Rightarrow \pi_s(x * y) = \pi_s(x \# y) \Leftrightarrow s * (x * y) = s \# (x \# y) \Leftrightarrow$$
$$\Leftrightarrow (s * x) * y = (s \# x) \# y \Leftrightarrow (\pi_s(x)) * y = (\pi_s(x)) \# y$$

so from condition (iii) we get, for every $x \in M$, that $T_y = M$. So $\# = *$. $\square$

2.3 Examples

Amalgamated sum

We will consider the amalgamated sum of monoids. In general by amalgamated sum we mean the colimit of a diagram of this kind

$$\varphi_i : H \to M_i$$

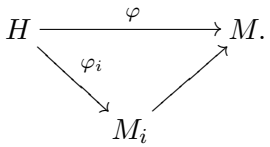
for each i in a given set I. The situation is then the following: we have a collection of monoids and they all have a map from a fixed monoid H. Clearly in the category of monoids, as in the category of groups, this colimit always exists, and it is also clear how to present it, as we are going to explain here. We choose a presentation for the monoids involved: $H = \langle H|R_H\rangle$, and $M_i = \langle M_i|R_i\rangle$ where

$$R_H = \{(xy, z) \text{ if } xy = z \text{ in } H\} \sqcup \{(1_H, 1)\}$$

with 1 the empty word in $F_{\mathrm{Mon}}(H)$, and R_i is defined in the same way for the monoids M_i. The symbol $\sqcup$ denotes the disjoint union. With this presentation the amalgamated sum of the M_i over H is the monoid

$$M = \left\langle H \sqcup \bigsqcup_{i\in I} M_i | R_H \sqcup \bigsqcup_{i\in I} R_i \sqcup R_\varphi \right\rangle$$

where $R_\varphi = \{(x, \varphi_j(x))|i \in I, x \in H\}$. We will from now on write $M = \langle S|R\rangle$. The fact that this presentation is correct can be seen very easily. The colimit of a diagram as the one we are considering in the category of monoids is a monoid together with a monoid map from every M_i, a monoid map $\varphi : H \to M$ and all these maps, should be compatible in the sense that all the squares like the one below commute



The colimit should also be universal with respect to this property which means that for every monoid M' satisfying the same requirements there should be a unique monoid map $M \to M'$ which respect all the maps involved. This is equivalent to look for an initial object in a category where objects are monoids given together with monoid maps from all M_i and from H with compatibility requirements. It is not difficult to realize that this is exactly the category of S-R-monoids. Giving a map $M_i \to M$ and a map from H makes M into an S-monoid and the fact that these must be monoid

morphisms makes M into an S-R'-monoid where $R' = R \setminus R_\varphi$. Finally, the relations in R_φ are equivalent to the commutativity of the diagrams above.

We will consider the case in which H is a subgroup and all φ_i are injective maps. We will show, using theorem 2.1.1, that in this case we can give a more explicit form to this monoid which will help to prove some properties about the amalgamated sum. The construction is the same as the one for groups, but in that case what we get is a completely explicit form (in the sense that it is in bijection with the set of equivalence classes), because of the fact that the action of a subgroup on a group is free. We will see later on how this is related to the word problem. Let us start constructing the set of normal forms by defining our main tool.

Definition 2.3.1. (*H-sets and compositions*) Let H be a group and X be a set. We say that X is a left H-set if we have an action of H on X which is a map $H \times X \to X$ (the image of (h, x) is denoted hx) such that $1_H x = x$ for all $x \in X$ and $h(h'x) = (hh')x$ for $h, h' \in H$ and $x \in X$. One can define right H-set in a similar way. We also have a notion of a H-G-biset (where G is another group, possibly equal to H) which are sets with a left H-action and a right G-action such that $h(xg) = (hx)g$ where h is an element of H, where x is in X and $g \in G$. If X is a right H-set and Y is a left H-set then $X \times_H Y$ is called the *composition* of X and Y over H and is defined to be the quotient of $X \times Y$ under the left action of H defined in this way:

$$\sigma(x, y) = (x\sigma^{-1}, \sigma y).$$

It is easily verified that this is a left action of H on $X \times Y$. When one among X and Y is a biset we can give more structure to $X \times_H Y$. For example if X is a G-H-biset then $X \times_H Y$ is a left G-set with the action given by

$$g[x, y] = [gx, y].$$

It is easy to verify that this is a well-defined left action of G on $X \times_H Y$. If Y is an H-K-biset we can define in a similar way a right action of K on $X \times_H Y$. Finally, if both X and Y are bisets as above, then their composition is a G-K-biset.

Notice that in $X \times_H Y$ we have $[x\sigma, y] = [x, \sigma y]$ since $\sigma(x\sigma, y) = (x\sigma\sigma^{-1}, \sigma y)$ and this is $(x, \sigma y)$. We will use this property very often in the construction of the amalgamated sum. We remark that one can define also an action of a monoid on a set, in the same way as for groups, but in general if M is a monoid acting on the left on X the relation $x \sim y$ if and only if there exists $\sigma \in M$ such that $x = \sigma y$ is not an equivalence relation. In particular we cannot define a composition as we did for groups.

Definition 2.3.2. (*Morphism of H-sets*) Let X and Y be two left H-sets. A morphism of H-sets is a map $f : X \to Y$ such that $f(hx) = hf(x)$ for

each $h \in H$ and $x \in X$. Similarly we define morphisms of right H-sets and of H-G-bisets.

With the definitions we gave left H-sets form a category, and so it is for right H-sets and bisets over two fixed groups. In our discussion we will use bisets which have both the left and the right action on the same group H. In the following propositions we will prove some properties of the above constructions which we will use later on.

Proposition 2.3.3. *Let X be a K_1-H-biset, Y an H-G-biset and let Z be a G-K_2-biset, then there exists an isomorphism of K_1-K_2-bisets $X \times_H (Y \times_G Z) \cong (X \times_H Y) \times_G Z$.*

Proof. We show that both $(X \times_H Y) \times_G Z$ and $X \times_H (Y \times_G Z)$ are in bijection with the same quotient of $X \times Y \times Z$. Let us consider the case $(X \times_H Y) \times_G Z$. We have surjective maps

$$\begin{array}{ccccc} X \times Y \times Z & \overset{f_1}{\twoheadrightarrow} & (X \times_H Y) \times Z & \overset{f_2}{\twoheadrightarrow} & (X \times_H Y) \times_G Z \\ (x,y,z) & \mapsto & ([x,y],z) & \mapsto & [[x,y],z]. \end{array}$$

We then know that the right hand side is a quotient of $X \times Y \times Z$ and we want now to show that it is a quotient modulo a left action of $H \times G$. We know that to make the map induced on the quotient by $f = f_2 \circ f_1$ into an isomorphism we have to consider the equivalence relation $(x,y,z) \sim (x',y',z')$ if and only if $f(x,y,z) = f(x',y',z')$. Let us suppose that $f_1(x,y,z) = f_1(x',y',z')$. Then we must have $z = z'$ and there exists an $h \in H$ such that $x' = xh^{-1}$ and $y' = hy$. Similarly $f_2([x,y],z) = f_2([x',y'],z')$ if and only if there exists a $g \in G$ such that $[x',y'] = [x,y]g^{-1} = [x,yg^{-1}]$ and $z' = gz$. The first condition is equivalent to the existence of an $h \in H$ such that $x' = xh^{-1}$ and $y' = hyg^{-1}$. We can notice that $f(x,y,z) = f(x',y',z')$ if and only if the conditions for f_2 are satisfied, since the conditions on f_1 are more restrictive. Then the equivalence class of the element (x,y,z) in $X \times Y \times Z$ is the set (xh^{-1}, hyg^{-1}, gz) and we can consider $(X \times_H Y) \times_G Z$ as the quotient of $X \times Y \times Z$ by the action of $H \times G$ defined $(h,g)(x,y,z) = (xh^{-1}, hyg^{-1}, gz)$. Exactly the same argument prove that the same is true also for $X \times_H (Y \times_G Z)$ so they are in bijection, and the map is $[[x,y],z] \mapsto [x,[y,z]]$. The fact that the actions are respected is straightforward. □

Proposition 2.3.4. *Let X, X' be right K_1-H-sets and Y, Y' be left H-K_2-sets. Let $f : X \to X'$ and $g : Y \to Y'$ be morphisms of K_1-H-bisets and H-K_2-bisets respectively. Then the map $f \times g : X \times_H Y \to X' \times_H Y'$ defined $f \times g([x,y]) = [f(x), g(y)]$ is a morphism of K_1-K_2-bisets.*

Proof. It is clear that $f \times g$ is well defined. We prove that it respects the actions of K_1 and K_2: let $\sigma \in K_1$ and $\tau \in K_2$, we then have

$$f \times g(\sigma[x,y]\tau) = f \times g([\sigma x, \tau y]) = [f(\sigma x), g(\tau y)] = \\ = [\sigma f(x), g(y)\tau] = \sigma[f(x), g(y)]\tau = \sigma f \times g([x,y])\tau$$

for $x \in X$ and $y \in Y$. So $f \times g$ is a morphism of K_1-K_2-bisets as we wanted to show. □

Proposition 2.3.5. *Let I be a set of indices and $X = \bigsqcup_{i\in I} X_i$ be a K_1-H-set such that also X_i is a K_1-H-biset for each $i \in I$. Let Y be an H-K_2-set. Then we have a K_1-K_2-biset isomorphism $X \times_H Y \cong \bigsqcup_{i\in I}(X_i \times_H Y)$.*

Proof. The map f, gluing of the immersions of all the sets X_i in X times the identity of Y, namely the map

$$[x,y] \in \bigsqcup_{i\in I}(X_i \times_H Y) \mapsto [x,y] \in X \times_H Y$$

is a well defined bijection. The fact that it respects the actions of K_1 and K_2 follows immediately: let $h \in K_1$ and $g \in K_2$ and let x, y in X and Y respectively, we have

$$f(h[x,y]g) = f([hx, yg]) = [hx, yg] = h[x,y]g = hf([x,y])g$$

so the proposition is proved. □

Proposition 2.3.6. *Let K be a group isomorphic to H and let X be an H-H-biset. Then K is an H-H-biset and we have $K \times_H X \cong X$ as H-H-bisets.*

Proof. Let us fix an isomorphism $\varphi : H \to K$. We give to K an H-H-biset structure induced from φ, namely $hkg = \varphi(h)k\varphi(g)$. This makes φ^{-1} into an H-H-biset morphism since, for $k \in K$ and $h, g \in H$ we have

$$\varphi^{-1}(gkh) = \varphi^{-1}(\varphi(h)k\varphi(g)) = h\varphi^{-1}(k)g.$$

Let $k \in K$ and $x \in X$, we have $[k,x] = [1_K\varphi^{-1}(k), x] = [1_K, \varphi^{-1}(k)x]$ and we define a map f which sends $[k,x] \in K \times_H X$ to $\varphi^{-1}(k)x \in X$. The map f is well defined since $f([kh,x]) = \varphi^{-1}(kh)x = \varphi^{-1}(k)hx = f([k,hx])$. The map f is surjective since $x = f([1_K, x])$. Suppose $f([k,x]) = f([k',x'])$ then we have $\varphi^{-1}(k)x = \varphi^{-1}(k')x'$ and so $[k,x] = [1_K, \varphi^{-1}(k)x] = [1_K, \varphi^{-1}(k')x'] = [k',x']$ so f is also injective. We conclude by proving that f is also a morphism of H-H-bisets: for $h, g \in H$ we have

$$f(h[k,x]g) = f([hk, xg]) = f([h, \varphi^{-1}(k)(xg)]) = \\ = f([1_K, h\varphi^{-1}(k)(xg)]) = h\varphi^{-1}(k)(xg) = h(\varphi^{-1}(k)x)g = hf([k,x])g.$$

□

We are now ready to start the construction of the amalgamated sum of monoids. We recall that we have a collection of monoids M_i, for i in a set of indices I and each of these monoids has a subgroup isomorphic to a fixed group H via an injection $H \to M_i$ which we denote φ_i. Let us consider the set Σ of all words w on the alphabet I with the following property:

$$w = i_1 \cdots i_n \text{ with } n \geq 0, \text{ with } i_k \in I \text{ for } k = 1, \ldots, n$$
$$\text{and } i_k \neq i_{k+1} \text{ for all } k = 1, \ldots, n-1.$$

For $n = 0$ the word w is the empty word 1. For $i \in I$ we will denote with Σ_i the set of words in Σ which do not start with i. Now to each $w \in \Sigma$ we associate an H-H-set L_w. We define it by induction:

- For $w = 1$ we define $L_1 = H$.
- If $w = i$ is a word of length 1 we define $L_i = M_i \setminus \varphi_i(H)$ and we point out explicitly that this, since H is a group, is an H-H-biset; this may not be true if H is a general submonoid.
- If L_w is defined and is an H-H-biset for some word w of length $n-1$ (not starting with i) then we define $L_{iw} = L_i \times_H L_w$, which is again an H-H-biset.

By the same argument that we used in proposition 2.3.3 we can prove that each composition over H of three or more H-H-bisets can be seen as a quotient of the cartesian product of the underlying sets. In particular here we have a surjective map $L_{i_1} \times \ldots \times L_{i_n} \twoheadrightarrow L_w$ for every $w = i_1 \cdots i_n \in \Sigma$. We will write $x = [x_1, \ldots, x_n]$ for $x \in L_w$.

We now want to prove that we can give a more explicit form to the amalgamated sum of the monoids M_i over the subgroup H using Van der Waerden's method. This will be done in the following theorem:

Theorem 2.3.7. *Let H be a group and I be a set. For each $i \in I$ let M_i be a monoid given together with an injective map $\varphi_i : H \to M_i$. Let M be the amalgamated sum of the monoids M_i over the subgroup H. Then for every $w = i_1 \cdots i_n \in \Sigma$ there exists a unique bijection f making the following diagram commutative:*

$$\begin{array}{ccccc} L_{i_1} \times \ldots \times L_{i_n} & \twoheadrightarrow & L_w & \hookrightarrow & \bigsqcup_{v \in \Sigma} L_v \\ \downarrow & & & \nearrow_{f} & \\ M_{i_1} \times \ldots \times M_{i_n} & \longrightarrow & M & & \end{array}$$

where the map $L_{i_1} \times \ldots \times L_{i_n} \twoheadrightarrow L_w$ is the projection, the map $M_{i_1} \times \ldots \times M_{i_n} \to M$ is the map $(x_1, \ldots, x_n) \mapsto x_1 \cdots x_n$ where the product is taken in M and all the products are considered to be H if $n = 0$.

Proof. We want to prove this theorem using theorem 2.1.1. We denote with M the set $\bigsqcup_{v\in\Sigma} L_v$ and we prove that we can endow it with an S-R-monoid structure making it universal. To apply the theorem we first need to define the maps π_g for g in some set M_i or in H and to choose a neutral element for M. As neutral element we take the element $1_H \in L_1$. To define the translations we define the H-H-bisets

$$X_i = \bigsqcup_{w\in\Sigma_i} L_w \qquad \text{and} \qquad Z_i = \bigsqcup_{w\in\Sigma_i} L_{iw}.$$

We are now going to build an H-H-bisets isomorphism $\lambda_i : M_i \times_H X_i \to M$ for each $i \in I$. By proposition 2.3.5 we have $M_i \times_H X_i = (L_i \sqcup \varphi_i(H)) \times_H X_i \cong (L_i \times_H X_i) \sqcup (\varphi_i(H) \times_H X_i)$ and

$$Z_i = \bigsqcup_{w\in\Sigma_i} L_{iw} = \bigsqcup_{w\in\Sigma_i} (L_i \times_H L_w) \cong L_i \times_H \Big(\bigsqcup_{w\in\Sigma_i} L_w \Big) \cong L_i \times_H X_i.$$

So we have

$$M_i \times_H Y_i \cong (L_i \times_H X_i) \sqcup (\varphi_i(H) \times_H X_i) \cong Z_i \sqcup X_i = M.$$

Here we used in the last isomorphism proposition 2.3.6. The H-H-bisets isomorphism above is the map

$$\lambda_i([\sigma, x]) = \begin{cases} \varphi_i^{-1}(\sigma)x \in L_w & \text{if } \sigma \in \varphi_i H \\ [\sigma, x] \in L_{iw} & \text{if } \sigma \in L_i \end{cases}$$

for $x \in L_w$ with $w \in \Sigma_i$ and $\sigma \in M_i$. Now that we have these bijections λ_i we can induce maps π_s with $s \in M_i$ and, by using different λ_i's, we are able to define all the translations for $s \in M_i$. We will use, for $s \in M_i$, the map $\pi'_s : M_i \times_H X_i \to M_i \times_H X_i$ defined $\pi'_s([\sigma, x]) = [s\sigma, x]$, so we have $\pi_s(x) = \lambda_i(\pi'_s(\lambda_i^{-1}(x)))$. If $s \in H$ we define π_s to be just the left action of H that we have on the set M.
We now have to prove that conditions (i), (ii) and (iii) of theorem 2.1.1 are satisfied. Let us start with condition (iii). Let T be a subset of M and suppose that $T \ni 1_H$ and $\pi_s(T) \subseteq T$ for all $s \in S$. Every element of M can be built by multiplication from the left by elements in the monoids M_i or in H, so by the properties of T every element of M is in T and $T = M$. We now prove condition (i). Let M' be an S-R-monoid. We want to build a map $\varphi : M \to M'$ such that $\varphi(\pi_s(x)) = s\varphi(x)$ for all $s \in S$ and $\varphi(1_H) = 1_{M'}$. We define φ on 1_H to be $1_{M'}$ and we define $\varphi(x) = x$ for each x in L_1 or in L_i for some $i \in I$. We define φ on L_w by induction on the length of w. Supposing it is defined on L_w for w a word of length n, let $[x, x'] \in L_{iw}$. We define $\varphi([x, x'])$ to be $\varphi(x)\varphi(x')$. Notice that φ is an H-H-biset map. Then we have

$$\varphi([x\sigma, \sigma^{-1}x']) = \varphi(x\sigma)\varphi(\sigma^{-1}x) = \varphi(x)\sigma\sigma^{-1}\varphi(x') = \varphi(x)\varphi(x') = \varphi([x, x'])$$

so φ is well defined. We have to show that φ respects the action of M_i on M for all $i \in I$. We notice first that for the maps λ_i we have:

$$\pi_s(\lambda_i([\sigma, y])) = \lambda_i(\pi'_s(\lambda_i^{-1}(\lambda_i([\sigma, y])))) = \lambda_i(\pi'_s([\sigma, x]))$$

so the maps λ_i respect the action of M_i on $M_i \times_H Y_i$, given by the π'_s. We now consider the composition $f = \varphi \circ \lambda_i$. If we prove that f is an M_i-morphism then we are done since $\varphi = f \circ \lambda_i^{-1}$ is a composition of M_i-maps and hence an M_i-map. Given $[\sigma, y] \in M_i \times_H Y_i$ we have

$$[\sigma, y] \mapsto \begin{cases} \varphi_i^{-1}(\sigma)y & \mapsto \quad \varphi_i^{-1}(\sigma)\varphi(y) = \sigma\varphi(y) = \sigma y \quad \text{if } \sigma \in \varphi_i(H) \\ [\sigma, y] & \mapsto \quad \varphi(\sigma)\varphi(y) = \sigma y \qquad\qquad\quad \text{otherwise.} \end{cases}$$

So f is in either case the map $[\sigma, y] \mapsto \sigma y$. It is very easy now to see that this map respects the action of M_i since

$$f(\pi'_s([\sigma, y])) = f([s\sigma, y]) = (s\sigma)y = s(\sigma y) = sf([\sigma, y]).$$

So (i) is proved. To show that M has property (ii) we note that we have two kinds of relations: relations in R_i and in R_H and relations in R_φ. Regarding the first set of relations is easy to see that if $s_1 s_2 = s_3$ in one of the M_i or in H then $\pi_{s_1} \circ \pi_{s_2} = \pi_{s_3}$ (this is true for the π'_s and hence it is true for π_s). The fact that the second kind of relations is respected follows easily from the fact that the λ_i are H-set morphisms: for all $i \in I$ we have

$$\pi_{\varphi_i(h)}(x) = \lambda_i \circ \pi'_{\varphi_i(h)} \circ \lambda_i^{-1}(x) = \lambda_i(h\lambda_i^{-1}(x)) = h\lambda_i(\lambda_i^{-1}(x)) = hx.$$

So M has a structure which makes it in a universal S-R-monoid. We still have to prove that the diagram above commutes. In particular we should prove that given $x = (x_1, \ldots, x_n) \in L_{i_1} \times \ldots \times L_{i_n}$ and we map it to L_w and then to M we get the same as if we map x to $M_{i_1} \times \ldots \times M_{i_n}$ and then to M with the multiplication map. We can prove it by induction on n. If $n = 0$ then $x \in H$ and there is nothing to prove. Let us suppose that the statement is true for $n < m$ and suppose that $x = (x_1, \ldots, x_m)$. Let $x' = (x_2, \ldots, x_m)$, we know by induction hypothesis that x' has the same image in M if we take it in the two different ways. This means that the product $x_2 \cdots x_m$ equals $[x_2, \ldots, x_m]$ in M. Then we can write

$$x_1 \cdots x_m = x_1(x_2 \cdots x_m) = x_1[x_2, \ldots, x_m] = \pi_{x_1}([x_2, \ldots, x_m]) = [x_1, \ldots, x_m]$$

since $w \in \Sigma$. So the proof is complete. □

These easy verifications that we have done imply that the set M, with the multiplication induced by the maps π_s, is the initial object among S-R-monoids and so it is the amalgamated sum of the M_i with amalgamated

subgroup H. In the general case this is not a completely explicit form, in the sense that we still can have two words x_1 and x_2 in M which are different, but represent the same element. When the action of H over the monoids M_i is free (for example if all the monoids are cancellative, which means that $xa = ya$ implies $x = y$ and $ax = ay$ implies $x = y$ for all x, y, a in M_i) we can take a unique representative for each element of the amalgamated sum. To do this first we should choose a representative for each left coset of H in each of the M_i. For each $x \in M_i$ we can see in which coset of H it is and consider the chosen representative, which will be denoted by $\overline{x}$. Since in this case the action is free, there exists a unique $h \in H$ such that $x = h\overline{x}$. In this way, given $x \in M$, we can find a process to write it in a unique way in the form $x = h[\overline{y}_1, \ldots, \overline{y}_n]$.
What we are going to do in the following is to prove a theorem about this amalgamated sum in the general case to see that even if we are not dealing with a completely explicit form we are able to understand some of its structure.

Theorem 2.3.8. *Let M be the amalgamated sum of the monoids $(M_i)_{i\in I}$ with amalgamated subgroup H. Let M^* be the subgroup of invertible elements of M, let M_r^* be the submonoid of elements of M which have a right inverse and M_l^* the submonoid of elements of M which have a left inverse. Then M^* is equal to the amalgamated sum of the monoids M_i^* over the subgroup H and similarly for M_r^* and M_l^*.*

Proof. Let $x \in M$ and suppose that $x \in L_w$ and that $y \in L_v$ is such that $xy = 1_H$. We have to show that if $x = [x_1, \ldots, x_n]$ then each of letters $x_k \in M_{i_k}$ for $k = 1, \ldots, n$ has a right inverse. Since the statement is clear if $x \in H$ or if $x \in L_i$ for some $i \in I$, let us suppose that w is a word of length at least 2 and that the statement is true for w of length strictly less than n. Let $y \in M$ be $[y_m, \ldots, y_1]$. We know that $m \geq 1$ since if y is in H and x is not, as we supposed, it cannot be $xy = 1_H$. Moreover we have that x_n and y_m must be in the same monoid M_{i_n} and the product $x_n y_n$ in this monoid is an element of $\varphi_{i_n}(H)$ (but not necessarily $\varphi_{i_n}(1_H)$) because we need x_n to cancel out. We will denote the product $x_n y_m$ by h_n. This implies that x_n has a right inverse in M_{i_n} since

$$x_n(y_m h_n^{-1}) = (x_n y_m)h_n^{-1} = h_n h_n^{-1} = 1_{M_{i_n}}.$$

Now $x' = [x_1, \ldots, x_{n-1}]$ is in $L_{w'}$ where w' is w without the last letter i_n. Since w' has length strictly less than n and $y' = [h_n y_{m-1}, \ldots, y_1]$ is a right inverse for x' all the elements x_k for $k = 1, \ldots, n-1$ are right invertible by the induction hypothesis and so we proved our claim.
The part concerning elements with a left inverse can be shown in the same way. For invertible elements we just have to put the results together since an element is invertible if and only if it has both a right and a left inverse. □

Chapter 3

The group case

3.1 Van der Waerden's theorem

Let us now consider the case of Van der Waerden's theorem for groups. The proof of the theorem is very similar to the one we gave for monoids.

Theorem 3.1.1. *Let S be a set, and let R be a set of group relations on S. Let G be a set and let $1_G \in G$ be an element. Suppose for every $s \in S$ a bijection $\pi_s : G \to G$ is given. Then the following are equivalent:*

(1) *There exists an S-group structure on G such that the multiplication $* : G \times G \to G$ has neutral element 1_G and satisfies $s * x = \pi_s(x)$ for all $s \in S$ and $x \in G$ and the pair $(G, S \to G)$ is a universal S-R-group.*

(2) *The following three conditions are satisfied:*

   (i) *For all S-R-group G' there exists a map $\varphi : G \to G'$ such that $\varphi(1_G) = 1_{G'}$ and $\varphi(\pi_s(x)) = s\varphi(x)$ for all $s \in S$ and $x \in G$.*

   (ii) *Let $s_i, s'_j \in S$ for $i = 1, \ldots, n$ and $j = 1, \ldots, m$ with $n, m \geq 0$ and let $(s_1^{\varepsilon_1} \cdots s_n^{\varepsilon_n}, s_1'^{\delta_1} \cdots s_m'^{\delta_m})$ be in R with ε_i, δ_j equal plus or minus 1 for every $i = 1, \ldots, n$ and $j = 1, \ldots, m$. Then $\pi_{s_1}^{\varepsilon_1} \circ \ldots \circ \pi_{s_n}^{\varepsilon_n} = \pi_{s'_1}^{\delta_1} \circ \ldots \circ \pi_{s'_m}^{\delta_m}$ in $\mathrm{Sym}(G)$.*

   (iii) *The only subset $T \subseteq G$ with $1_G \in T$ such that for all $s \in S$ one has $\pi_s(T) = T$ is $T = G$.*

Moreover if there exists an S-group structure on G, with the required unit and translations, then it is unique.

Proof. The implication (1)⇒ (2) can be done exactly as for monoids. In fact condition (i) comes also in this case immediately from the universal

property. Condition (ii) can be verified again using the translation maps for G as we did in the monoid case. To prove condition (iii) let T be a set satisfying the conditions in (iii). Here we take the set $\{x \in G | xT = T\}$ and this is a subgroup of G containing S and so, by proposition 1.5.7, it is equal to G. Then we conclude that $T = G$ as we did for monoids.
Now assume the three conditions (i), (ii) and (iii) are satisfied. We consider the set $\mathrm{Sym}(G) = L$ of the set bijections $G \to G$. This set is clearly a group and by condition (ii) the map $s \mapsto \pi_s$ makes it into an S-R-group. So from condition (i) we have a map $\varphi : G \to L$ such that $\varphi(1_G) = \mathrm{Id}_G$ and $\varphi(\pi_s(x)) = \pi_s \circ \varphi(x)$ for $s \in S$ and $x \in G$. We call H the subgroup of L generated by the maps π_s, namely the set $\langle \pi_s : s \in S \rangle$. We want to show that $\varphi(G) = H$. Since π_s is surjective, we have $\pi_s(G) = G$ so $\varphi(G) = \varphi(\pi_s(G)) = \pi_s \circ \varphi(G)$ and since $\mathrm{Id}_G \in \varphi(G)$ this implies that $\pi_s \in \varphi(G)$ for all $s \in S$ so $H \subseteq \varphi(G)$. To prove the converse we prove that $G = \varphi^{-1}(H)$. Let us consider the set $T = \varphi^{-1}(H)$ and apply condition (iii). We have that $1_G \in T$ and $x \in T$ if and only if $\pi_s(x) \in T$ for $s \in S$ in fact:

$$x \in T \Leftrightarrow x \in \varphi^{-1}(H) \Leftrightarrow \varphi(x) \in H \Leftrightarrow \pi_s \circ \varphi(x) \in H \Leftrightarrow$$
$$\Leftrightarrow \varphi(\pi_s(x)) \in H \Leftrightarrow \pi_s(x) \in \varphi^{-1}(H) \Leftrightarrow \pi_s(x) \in T.$$

So by condition (iii) we get $T = G$ and we proved that $\varphi(G) \subseteq H$ and so they are equal.
We define now the map $\psi : f \in L \mapsto f(1_G) \in G$ and we claim that also in this case ψ is a left inverse for φ. We use again condition (iii), on the set

$$T = \{x \in G : \psi \circ \varphi(x) = x\}.$$

We clearly have $1_G \in T$ and if $x \in G$ and $s \in S$ we have:

$$x \in T \Leftrightarrow \varphi(x)(1_G) = x \Leftrightarrow (\pi_s \circ \varphi(x))(1_G) = \pi_s(x) \Leftrightarrow$$
$$\Leftrightarrow \varphi(\pi_s(x))(1_G) = \pi_s(x) \Leftrightarrow \pi_s(x) \in T.$$

So $T = G$ and ψ is a left inverse for φ.
By this as for monoids we know that the restriction $\psi : H \to G$ is bijective and its inverse is φ and also in this case this allows us to conclude the proof. Since H is an S-R-group we can induce a group multiplication on G, namely $x_1 * x_2 = \psi(\varphi(x_1) \circ \varphi(x_2))$ and this multiplication makes G also into an S-R-group, since H was an S-R-group. The map from S comes from the map $S \to H$ so it is the map $s \mapsto \psi(s)$. Since H is generated by the π_s we have that G is generated by the image of S in G and from this we get that the map in (i) is unique and hence G is a universal S-R-group. We prove again explicitly that the translation maps are as we wanted:

$$s * x = \psi(\pi_s \circ \varphi(x)) = \psi(\varphi(\pi_s(x))) = \pi_s(x).$$

We still have to prove the uniqueness of the S-group structure. Suppose

that # also makes G into a universal S-R-group, with the required unit and translations. Then the map $S \to G$ must be the same by the condition on the translations applied to $x = 1_G$ in fact

$$s * 1_G = \pi_s(1_G) = s\#1_G.$$

We now prove that the multiplications coincide. Let us consider, for each $x \in G$, the set $T_y = \{x \in G : x * y = x\#y\}$. For all $y \in G$ one has $1 \in T_y$ and:

$$\begin{aligned} x * y = x\#y \Leftrightarrow \pi_s(x * y) = \pi_s(x\#y) \Leftrightarrow s * (x * y) = s\#(x\#y) \Leftrightarrow \\ \Leftrightarrow (s * x) * y = (s\#x)\#y \Leftrightarrow (\pi_s(x)) * y = (\pi_s(x))\#y \end{aligned}$$

so from condition (iii) we get, for every $x \in G$, that $T_y = G$. So $\# = *$. □

3.2 Examples

Free group

As we said when discussing free groups let us start by discussing the normal form for the group $F(S)$. In 1.4 we showed that the initial object in the category of S-groups is the monoid $\langle \widetilde{S}|R\rangle_{\mathrm{Mon}}$ where $\widetilde{S}$ was the disjoint union of the set S and a set of "inverses" for the elements of S and R was the set of relations which told us that $ss^{-1} = s^{-1}s = 1$. We want now to give to this group an explicit presentation. Let us consider the set of words in the alphabet $\widetilde{S}$ with the property that two characters which are next to each other are never equal one to s and the other one to s^{-1} for some $s \in \widetilde{S}$. We call this set G and we define the translations in the obvious way: for $s_1, \ldots, s_n \in \widetilde{S}$ we have

$$\pi_s(s_1 s_2 \cdots s_n) = \begin{cases} s_2 \cdots s_n & \text{If } s_1 = s^{-1} \\ s s_1 s_2 \cdots s_n & \text{otherwise.} \end{cases}$$

We have to show that all these maps are bijections $G \to G$. We show that each π_s is invertible and its inverse is $\pi_{s^{-1}}$. Let $w = s_1 \cdots s_n \in G$, we have

$$\pi_s(\pi_{s^{-1}}(w)) = \begin{cases} \pi_s(s_2 \cdots s_n) = s s_2 \cdots s_n = w & \text{If } s_1 = s \\ \pi_s(s^{-1} w) = w & \text{otherwise.} \end{cases}$$

notice that $s_2 \neq s^{-1}$ in the first case since if it is so then the word $w \notin G$. We have now to verify conditions (i), (ii) and (iii). Condition (ii) is empty, since there are no relations. Condition (iii) can be easily shown by induction on the length of a word. For condition (i) we can define $\varphi : G \to G'$ for an S-R-group G' to be $1_{G'}$ on 1_G and $\varphi(s_1 \cdots s_n) = \varphi(s_1) \cdots \varphi(s_n)$ where

$\varphi(s) = s$ for $s \in S$. To prove the condition on the translation maps we should distinguish two cases. Suppose first that $s = s_1^{-1}$ then we have:

$$\begin{aligned}\varphi(\pi_s(s_1 \cdots s_n)) = \varphi(s_2 \cdots s_n) = \varphi(s_2) \cdots \varphi(s_n) = s_2 \cdots s_n = \\ = (ss_1)s_2 \cdots s_n = s(s_1 \cdots s_n) = s\varphi(s_1 \cdots s_n).\end{aligned}$$

If $s \neq s_1^{-1}$ we have

$$\varphi(\pi_s(s_1 \cdots s_n)) = \varphi(ss_1 \cdots s_n) = \varphi(s)\varphi(s_1) \cdots \varphi(s_n) = s\varphi(s_1 \cdots s_n).$$

This concludes the proof of the normal form for the free group.

Sum of groups

In this example we will consider the case of the sum of a family of groups, what Van der Waerden called *free product*. This case is easier than the one we did in section 2.3, but it is important since is the one we find in the original paper by Van der Waerden ([1]). Let us suppose to have a collection of groups $(G_i)_{i \in I}$ for some index set I. We want to construct their *sum*, also called coproduct in categorical terms. The idea is similar to what we did for amalgamated sum of monoids and in fact this can be viewed as an amalgamated sum with amalgamated subgroup isomorphic to the trivial group. Let us take a presentation of the groups $G_i = \langle G_i | R_i \rangle$ where $R_i = \{(xy, z) | xy = z \text{ as a product in } G_i\}$. With this presentation for the groups the sum can be presented as $\langle S = \bigsqcup_{i \in I} G_i | R = \bigsqcup_{i \in I} R_i \rangle$, and we can prove this as we did for the amalgamated sum of monoids. We now want to find a set of normal forms for this group. Consider the set Σ of all words $w = x_1 \cdots x_n$ with $x_k \in I$ for $k = 1, \ldots, n$ and $n \geq 0$ such that for each k we have $x_k \neq x_{k+1}$. We will denote by Σ_i the set of words in Σ which do not start with $i \in I$. Let $w \in \Sigma$ be the word $x_1 \cdots x_n$, we define L_w to be the product $L_{x_1} \times \ldots \times L_{x_n}$ where $L_i = G_i \setminus \{1_{G_i}\}$ for every $i \in I$ and $L_1 = \{1\}$. We define as for monoids the sets G and X_i as follows:

$$G = \bigsqcup_{w \in \Sigma} L_w \qquad\qquad X_i = \bigsqcup_{w \in \Sigma_i} L_w.$$

We define now a bijection $\lambda_i : G_i \times X_i \to G$ for each $i \in I$ in the following way: let $g \in G_i$ and $w \in X_i$ then

$$\lambda_i(g, w) = \begin{cases} (g, w) & \text{if } g \neq 1_{G_i} \\ w & \text{if } g = 1_{G_i}. \end{cases}$$

In this case it is easy to prove that the maps λ_i are bijective. We can then induce for each $s \in S$, using the maps π'_s defined as we did above, a map $\pi_s : G \to G$ which is our multiplication by s in G. Defined in this way,

namely $\pi_s(x) = \lambda_i(\pi'_s(\lambda_i^{-1}(x)))$ for $s \in G_i$, it is clear that π_s is invertible, since it is the composition of invertible maps. So we can go on with the verification of conditions (i), (ii) and (iii). Condition (iii) can be proved as for monoids. Let G' be an S-R-group and we define the map φ to be $\varphi(1) = 1'_G$ on L_1, on words of length one $\varphi(x) = x$ and on longer words $\varphi(x_1, \ldots, x_n) = x_1 \cdots x_n$. Let us fix an arbitrary $s \in L_i$ (since if $s = 1_{G_i}$ the property is clearly satisfied) and take an element $x = (x_1, \ldots, x_n) \in G$. Suppose first that x_1 is not in L_i; we have:

$$\begin{aligned}\varphi(\pi_s(x_1, \ldots, x_n)) &= \varphi(\lambda_i(\pi'_s(\lambda_i^{-1}(x_1, \ldots, x_n)))) = \varphi(\lambda_i(\pi'_s(1, x_1, \ldots, x_n)))= \\ &= \varphi(\lambda_i(s, x_1, \ldots, x_n)) = \varphi(s, x_1, \ldots, s_n) = sx_1 \cdots x_n = \\ &= s(x_1 \cdots x_n) = s\varphi(x_1, \ldots, x_n).\end{aligned}$$

In case $x_1 \in L_i$ and the product $sx_1 \neq 1_{G_i}$ we can write:

$$\begin{aligned}\varphi(\pi_s(x_1, \ldots, x_n)) &= \varphi(\lambda_i(\pi'_s(\lambda_i^{-1}(x_1, \ldots, x_n)))) = \varphi(\lambda_i(\pi'_s(x_1, \ldots, x_n))) = \\ &= \varphi(\lambda_i((sx_1), \ldots, x_n)) = \varphi((sx_1), \ldots, x_n) = \\ &= (sx_1) \cdots x_n = s(x_1 \cdots x_n) = s\varphi(x_1, \ldots, x_n).\end{aligned}$$

The only remaining case is when $x_1 \in L_i$ and $s = x_1^{-1}$. We have:

$$\begin{aligned}\varphi(\pi_s(x_1, \ldots, x_n)) &= \varphi(\lambda_i(\pi'_s(\lambda_i^{-1}(x_1, \ldots, x_n)))) = \varphi(\lambda_i(\pi'_s(x_1, \ldots, x_n))) = \\ &= \varphi(\lambda_i(1_{G_i}, \ldots, x_n)) = \varphi(x_2, \ldots, x_n) = x_2 \cdots x_n = \\ &= x_1^{-1}x_1x_2 \cdots x_n = s\varphi(x_1, \ldots, x_n).\end{aligned}$$

So condition (i) is satisfied. We still need to prove condition (ii), which follows immediately from the fact that $\pi'_{s_1} \circ \pi'_{s_2} = \pi'_{s_3}$ if $s_1s_2 = s_3$ in one of the G_i.

Amalgamated sum

We could also build amalgamated sum for groups, but there is no difference with the construction we saw in the monoid case. As we pointed out in section 2.3 in the case of an amalgamated sum of groups we get a completely explicit form, after we choose representatives for the left cosets of the amalgamated subgroup H in the G_i. Van der Waerden's method was used in this case also by Serre (see [3]) and Kurosh (see [4]).

Chapter 4

The ring case

4.1 Van der Waerden's theorem

We now discuss the version of Van der Waerden's theorem in the case of rings. As we already discussed in section 1.6 we will consider the more general case of k-algebras over a fixed commutative ring k. Let us start by stating Van der Waerden's theorem in this case. To simplify the notation in condition (ii) we will write π_x for $x \in F(S)_{\mathrm{Mon}} \backslash \{1\}$ meaning the composition $\pi_{s_1} \circ \ldots \circ \pi_{s_n}$ if $x = s_1 \cdots s_n$ for $n \geq 1$.

Theorem 4.1.1. *Let S be a set, k a commutative ring and let R be a set of k-algebra relations on S. Let A be a k-module and let $1_A \in A$ be an element. Suppose for every $s \in S$ a k-module morphism $\pi_s : A \to A$ is given. Then the following are equivalent:*

(1) *There exists an S-k-algebra structure on A such that the k-module structure is preserved and the multiplication $* : A \times A \to A$ has neutral element 1_A and satisfies $s * x = \pi_s(x)$ for all $s \in S$ and $x \in A$ and the pair $(A, S \to A)$ is a universal S-R-k-algebra.*

(2) *The following three conditions are satisfied:*

   (i) *For all S-R-k-algebras A' there exists a k-linear map $\varphi : A \to A'$ such that $\varphi(1_A) = 1_{A'}$ and $\varphi(\pi_s(x)) = s\varphi(x)$ for all $s \in S$ and $x \in A$.*

   (ii) *The collection of maps $(\pi_s)_{s \in S}$ has the following property: if the pair $(h_1 x_1 + \ldots + h_n x_n, h'_1 y_1 + \ldots + h'_m y_m) \in R$, for some x_i and y_j in $F(S)$, the h_i and h'_j in k for $i = 1, \ldots, n$ and $j = 1, \ldots, m$ and for $n, m \geq 0$, then $h_1 \pi_{x_1} + \ldots + h_n \pi_{x_n} = h'_1 \pi_{y_1} + \ldots + h'_m \pi_{y_m}$ in $\mathrm{End}_k(A)$.*

(iii) *The only k-submodule $T \subseteq A$ with $1_A \in T$ such that for all $s \in S$ one has $\pi_s(T) \subseteq T$ is $T = A$.*

Moreover if there exists an S-structure on A, with the required unit and translations, then it is unique.

The proof of theorem 4.1.1 is done in the same way as the one we did for monoids and we are going to write it down explicitly. Before starting with the proof let us make some remarks about the theorem. Notice that in this case the set of normal forms is required to have more structure than for monoids and groups, it should be a k-module and the translation maps should respect this further structure. The key point is that Van der Waerden's theorem is useful to define associative multiplications. So, if we want to apply it, we should have an object such that if we add an associative multiplication it becomes the algebraic structure we wanted. So for monoids we just need a set with a unit and translations can be just maps. For groups we need again a set, but when defining translations we should require them to be bijections in order to ensure an inverse for each element of the group. For k-algebras we need to start with a k-module and the multiplication that we are going to define needs to be distributive with respect to the addition in its abelian group structure and this is exactly what is encoded in the k-linearity requirement. To simplify the theorem we start with a lemma

Lemma 4.1.2. *Let M be a k-module. The set of k-linear maps $M \to M$, denoted $\mathrm{End}_k(M) = L$ is a k-algebra.*

Proof. Let us denote the neutral element of M by 0_M. We define the map $\underline{0}_M$ which sends every $x \in M$ to 0_M which is a k-linear map. We define an addition on L induced from the one in M, namely $(f+g)(x) = f(x)+g(x)$. It is clear that the map $f+g$ is again a k-linear map and that $\underline{0}_M$ is a neutral element for this addition. Each map $f \in L$ has an additive inverse, namely the map $x \mapsto -f(x)$ so L is an abelian group. One can show that the composition of maps is distributive with respect to this addition and that Id_L is a neutral element for the composition so L is a ring.
We define a map $k \to L$ by sending $h \in k$ to the multiplication by h, which is a k-linear map since k is commutative, in fact if f is the multiplication by h we have:

$$f(h'x) = h(h'x) = hh'x = h'hx = h'(hx) = h'f(x).$$

It is again easy to show that the image of the map $k \to L$ is contained in the center of the ring L so the lemma is proved. □

We can now start with the proof of theorem 4.1.1.

Proof. Assume (1) holds. Then (i) comes immediately from the universal property. For (ii) we consider the map $A \to \mathrm{End}_k(A)$ which sends each element $a \in A$ to the multiplication by a. This is a k-algebra homomorphism and respects the set S (the element $\pi_s(1_A) \in A$ is sent to the multiplication by $\pi_s(1_A)$ so to the map π_s) so also $\mathrm{End}_k(A)$ is an S-R-k-algebra and (ii) is satisfied. Let now T be a set that satisfies the requirements of condition (iii). Then the set $\{x \in A | xT \subseteq T\}$ is a subalgebra of A containing S and so, by proposition 1.7.7, it is equal to A. So for all $x \in A$ the element $x = x1_A$ is in the set xT and so it is in T. Then $x \in T$, and condition (iii) holds.
Now assume the three conditions (i), (ii) and (iii) are satisfied. Let us consider the set $\mathrm{End}_k(A) = L$ of k-linear maps $A \to A$. This set is a k-algebra by lemma 4.1.2 and the map $s \mapsto \pi_s$ makes it into an S-R-k-algebra by condition (ii). So from condition (i) we have a map $\varphi : A \to L$ such that $\varphi(1_A) = \mathrm{Id}_A$ and $\varphi(\pi_s(x)) = \pi_s \circ \varphi(x)$ for $s \in S$ and $x \in A$. Let $H = \langle \pi_s : s \in S \rangle$ be the subalgebra of L generated by the maps π_s. We want to show that $\varphi(A) = H$. Let us consider the set $\{f \in L | f \circ \varphi(A) \subseteq \varphi(A)\}$. This is a subalgebra of L and it contains all the maps π_s for $s \in S$, so it contains the set H. Then we have: $H = H \circ \mathrm{Id}_A \subseteq \varphi(A)$. To prove the converse we prove that $A = \varphi^{-1}(H)$. Let us consider the set $T = \varphi^{-1}(H)$ and apply condition (iii). We have that $1 \in T$ and if $x \in T$ and $s \in S$ then also $\pi_s(x) \in T$ since

$$x \in T \Leftrightarrow x \in \varphi^{-1}(H) \Leftrightarrow \varphi(x) \in H \Rightarrow \pi_s \circ \varphi(x) \in H \Leftrightarrow$$
$$\Leftrightarrow \varphi(\pi_s(x)) \in H \Leftrightarrow \pi_s(x) \in \varphi^{-1}(H) \Leftrightarrow \pi_s(x) \in T.$$

By condition (iii) we then have $T = A$ and we proved that $\varphi(A) \subseteq H$ and so they are equal.

Define now the map $\psi : L \to A$ which sends a map f to its value on the element of A we have chosen as a unit, so $f \mapsto f(1_A)$. We claim that this map is a left inverse for φ. We use again condition (iii), on the set

$$T = \{x \in A : \psi \circ \varphi(x) = x\}.$$

It is clear that $1_A \in T$ since $\psi \circ \varphi(1_A) = \psi(\mathrm{Id}_A) = \mathrm{Id}_A(1_A) = 1_A$. Let now $x \in A$ and $s \in S$; we have:

$$x \in T \Leftrightarrow \varphi(x)(1_A) = x \Rightarrow (\pi_s \circ \varphi(x))(1_A) = \pi_s(x) \Leftrightarrow$$
$$\Leftrightarrow \varphi(\pi_s(x))(1_A) = \pi_s(x) \Leftrightarrow \pi_s(x) \in T.$$

So $T = A$ and ψ is a left inverse for φ.

By this we know that the restriction $\psi : H \to A$ is bijective and its inverse is φ. As for monoids this is all that we need to finish the proof. Since H is an S-R-k-algebra we can induce a k-bilinear multiplication on A, namely $x_1 * x_2 = \psi(\varphi(x_1) \circ \varphi(x_2))$ which makes A into an S-R-k-algebra. The map

from S comes from the map from S in H so it is the map $s \mapsto \psi(s)$. Since H is generated by the π_s we have that A is generated by the image of S in A and from this we get that the map in (i) is unique and hence A is a universal S-R-monoid. We notice explicitly that the translation maps are as we wanted:

$$s * x = \psi(\pi_s \circ \varphi(x)) = \psi(\varphi(\pi_s(x))) = \pi_s(x).$$

We still have to prove the uniqueness of $*$. Suppose that $\#$ also makes A into a universal S-R-k-algebra, with the required unit and multiplication. Let us consider, for each $y \in A$, the set $T_y = \{x \in A : x * y = x\#y\}$. For all $y \in A$ one has $1 \in T_y$ and:

$$\begin{aligned} x * y = x\#y \Rightarrow \pi_s(x * y) = \pi_s(x\#y) \Leftrightarrow s * (x * y) = s\#(x\#y) \Leftrightarrow \\ \Leftrightarrow (s * x) * y = (s\#x)\#y \Leftrightarrow (\pi_s(x)) * y = (\pi_s(x))\#y \end{aligned}$$

so from condition (iii) we get, for every $x \in A$, that $T_y = A$. So $\# = *$.

□

4.2 Examples

Tensor Algebra

In this example we define the tensor algebra of a k-module over k. Given a commutative ring k let M be a left k-module. The tensor algebra of M over k is defined to be the k-module $T = \bigoplus_{n \geq 0} M^{\otimes n}$. This is a k-algebra with the obvious multiplication and we can see that it can be presented as $\langle M|R\rangle$ with

$$\begin{aligned} R = \{(x + y, w) | x, y, w \in M, \text{ if } x + y = w \text{ in } M\} \cup \\ \cup \{(hx, z) | x, z \in M, h \in k, \text{ if } hx = z \text{ in } M\} \end{aligned}$$

using theorem 4.1.1. Notice that in R we have Let us consider the k-module T with neutral element 1_k and translations given by $\pi_x(y) = x \otimes y$ for every $y \in T$ and $x \in M$. The verifications of property (i), (ii) and (iii) are very easy. For (i) let T' be an M-R-k-algebra and define $\varphi : T \to T'$, by

$$\varphi(h_0 + h_1 y_1^1 + \ldots + h_n y_n^1 \otimes \ldots \otimes y_n^n) = h_0 + h_1 y_1^1 + \ldots + h_n y_n^1 \cdots y_n^n$$

with all y_i^j in M and h_r in k for $r = 0, \ldots, n$. For $x \in M$ it is very easy, using the defining properties of a ring, to prove that $\varphi(\pi_x(y)) = x\varphi(y)$ for every $y \in T$. Condition (ii) follows from the properties of the tensor product: let y be in T and let $m, m' \in M$ with $m + m' = z$, we have:

$$\begin{aligned}\pi_m(y) + \pi_{m'}(y) &= m \otimes (h_0 + h_1 y_1^1 + \ldots + h_n y_n^1 \otimes \ldots \otimes y_n^n) + \\ &+ m' \otimes (h_0 + h_1 y_1^1 + \ldots + h_n y_n^1 \otimes \ldots \otimes y_n^n) = \\ &= (m + m')h_0 + h_1(m + m') \otimes y_1^1 + \ldots + \\ &+ h_n(m + m') \otimes y_n^1 \otimes \ldots \otimes y_n^n = \pi_{m+m'}(y) = \pi_z(y).\end{aligned}$$

We can do in a similar way also for the other relations, for $h \in k$ and $m \in M$ and for $hm = w$ we have:

$$\begin{aligned}h\pi_m(y) &= hm \otimes (h_0 + h_1 y_1^1 + \ldots + h_n y_n^1 \otimes \ldots \otimes y_n^n) = \\ &= (hm) \otimes (h_0 + h_1 y_1^1 + \ldots + h_n y_n^1 \otimes \ldots \otimes y_n^n) = \\ &= \pi_{hm}(y) = \pi_w(y).\end{aligned}$$

Condition (iii) follows by induction: let S be a submodule of T with $1 \in S$ and $\pi_x(S) \subseteq S$. Let us suppose that all the elements of $M^{\otimes n}$ are in S for some n. Then also $M^{\otimes n+1}$ is contained is S since all the generators of its k-module structure can be written as $\pi_x(w)$ for some $x \in M$ and some $w \in M^{\otimes n}$. So S equals T because it is a submodule and it contains all the sets $M^{\otimes n}$ so it contains also sums of elements of those sets and their multiplications by elments of k. So we can define an M-k-algebra structure on T and T with this structures will be isomorphic to $\langle M|R\rangle$. We have to show that the multiplication induced on T by these translations is the one that we have on the tensor algebra but this is clear since the neutral element and the translations are the same.

Amalgamated sum

As for groups and monoids also in the case of k-algebras we can prove a normal form theorem for some particular kind of amalgamated sum. We will not discuss it in great detail, but we will give an idea of how this can be done. We will do it in the case which is considered also by Serre in [3], but we point out that in the paper by Cohn, see [5], a normal form is found also in a more general case. Let us suppose to have a collection of k-algebras R_i for i in some index set I and let us suppose that there exist a k-algebra K with an injective morphism of k-algebras, denoted φ_i, to each of the R_i. Since in this case we cannot generalize the construction if we just consider the set-theoretic difference $R_i \setminus \varphi_i(K)$, we can ask the further requirement that $R_i = \varphi_i(K) \oplus B_i$ as K-K-bimodules for some complementary K-K-bimodule B_i. If we make this assumption the construction and the proofs can be done exactly as for monoids and for groups by considering the tensor product over K in the place of the H-H-bisets composition. Notice that, as required by the theorem, in this case all the objects we are considering are modules over K and so they are also modules over k and the π_s are endomorphisms of

k-modules. What is made weaker by Cohn is the requirement that for all i the sub-K-K-bimodule $\varphi_i(K)$ is a direct summand of R_i, by requiring that the K-K-bimodule $R_i/\varphi_i(K)$ is left flat which means that the sequence

$$0 \to M' \otimes_K (R_i/\varphi_i(K)) \to M \otimes_K (R_i/\varphi_i(K))$$

is an exact sequence of right K-modules for all right K-modules M, M' such that M' is a submodule of M.

Clifford algebras

In this example we will consider briefly the case of Clifford algebras treated by Van der Waerden in [2] and then we will discuss a possible generalization. In his article Van der Waerden considers the case of a vector space V over a field k given together with a quadratic form Q with values in the field. A quadratic form on a vector space is a map $Q : V \to k$ such that $Q(hx) = h^2Q(x)$ for all $h \in k$ and $x \in V$ and such that the map $L_Q : V \times V \to k$ defined $L_Q(x, y) = Q(x + y) - Q(x) - Q(y)$ is a k-bilinear map. Suppose now that $v_1, \ldots, v_n$ form a basis for V over k. Here one defines the Clifford algebra corresponding to Q to be the quotient C of the tensor algebra of V by the two sided ideal I, generated by the elements $x \otimes x - Q(x)$ for $x \in V$. In the article Van der Waerden proves that the elements $v_{i_1} \otimes v_{i_2} \otimes \ldots \otimes v_{i_k}$ with $k = 1, \ldots, n$, $i_j \in \{1, \ldots, n\}$ for all j and such that $i_j < i_{j+1}$ for all j, form a basis of C over k. This was proved before, with a different method, by Chevalley in [7] and according to Van der Waerden the proof by Chevalley was the first one which was valid in the case of fields of characteristic 2. The difference between the two cases is that in characteristic different from 2 it is possible to diagonalize the quadratic form Q and the computations become easier. In the article of Van der Waerden he uses instead his method on the k-algebra with generators $v_1, \ldots, v_n$ (which is isomorphic to the tensor algebra of V) and with the relations that we can derive from $x \otimes x - Q(x) = 0$, namely:

$$v_k v_k = Q(v_k) \qquad \text{and} \qquad v_i v_k + v_k v_i = L_Q(v_i, v_k).$$

The second type of relations is obtained by considering the quadratic form on $x + y$ and the relation on x^2 in this way:

$$Q(x + y) = (x + y)(x + y) = x^2 + xy + yx + y^2 = Q(x) + Q(y) + xy + yx.$$

We will not discuss this case in further detail, but we suggest a generalization of this example. Suppose that we are given a module M over a commutative ring k together with a linear form $T : M \to k$ and a quadratic form $Q : M \to k$. We define a quadratic form on a module as we did for vector spaces over fields. We consider the tensor algebra of M over k and we quotient by

the two sided ideal generated by the elements $x^2 - T(x)x + Q(x)$ for $x \in M$. For some M it should be possible to prove a theorem similar to the one proved by Van der Waerden. Let us consider for example M free of rank 2 over k. Let a, b be generators for M, we can prove that the k-algebra

$$\langle a, b | (a^2, T(a)a - Q(a)), (b^2, T(b)b - Q(b)), (ab + ba, T(b)a + T(a)b - L_Q(a, b)) \rangle$$

has the set $\{1, a, b, ab\}$ as a basis over k (the other relations follows from the ones that we have written above). To simplify notations we will write the above as $\langle a, b | R \rangle$ where

$$R = \{(a^2, t_a a - q_a), (b^2, t_b b - q_b), (ab + ba, t_b a + t_a b - l)\} \qquad (*)$$

for some arbitrary t_a, t_b, q_a, q_b and l in k. To explain how this example can arise let us consider the matrix ring $M_2(k)$ of two by two matrices with coefficients in k as M and the trace and the determinant as T and Q respectively. By Cayley-Hamilton theorem we have $X^2 - \mathrm{Tr}(X)X + \det(X) = 0$ for all $X \in M_2(k)$ so the relations above are satisfied with $t_a = T(X)$ and so on. We can see that the matrix ring $M_2(k)$ can be generated as a k-module by the set $\{\mathrm{Id}, X, Y, XY\}$ if X and Y are generators of the ring. Using Van der Waerden's method we will prove that in the more general case of a k-algebra with generators and relations as above the set {1,a,b,ab} is a k-basis for the ring A.

Theorem 4.2.1. *The k-module structure of the k-algebra $\langle a, b | R \rangle$ with the notation we defined in (*) is free with basis $\{1, a, b, ab\}$.*

Proof. Let A be the free k-module over the set $\{1, a, b, ab\}$. Since we want to apply Van der Waerden's method we need to choose a neutral element and some translations π_a and π_b. As neutral element we choose the element 1. We define the translations and prove condition (i) at the same time. Given an (a, b)-R-k-algebra A' we define a k-linear map $\varphi : A \to A'$: on the basis it is

$$\varphi(1) = 1_{A'}, \quad \varphi(a) = a, \quad \varphi(b) = b, \quad \varphi(ab) = ab$$

and we extend it on A' by k-linearity. We have from the relations that $a^2 = t_a a - q_a$ in A' so we have:

$$\varphi(t_a a - q_a) = t_a \varphi(a) - q_a \varphi(1) = t_a a - q_a = a^2 = aa = a\varphi(a).$$

Then if we define $\pi_a(a) = t_a a - q_a$ we get $\varphi(\pi_a(a)) = a\varphi(a)$ for every A'. Similarly for $\pi_a(ab)$ we have

$$\varphi(t_a ab - q_a b) = t_a \varphi(ab) - q_a \varphi(b) = t_a ab - q_a b = a^2 b = a(ab) = a\varphi(ab)$$

and if we define $\pi_a(ab) = t_a ab - q_a b$ we get $\varphi(\pi_a(ab)) = a\varphi(ab)$. So we can define π_a on the basis:

$$\begin{cases} \pi_a(1) = a \\ \pi_a(a) = t_a a - q_a \\ \pi_a(b) = ab \\ \pi_a(ab) = t_a ab - q_a b \end{cases}$$

and extend it by k-linearity on the whole A. For π_b we can proceed in the same way. By the relations we have that $ba = -ab + t_b a + t_a b - l$ in A' so we have:

$$\begin{aligned} \varphi(-ab + t_b a + t_a b - l) &= -\varphi(ab) + t_b\varphi(a) + t_a\varphi(b) - l = \\ &= -ab + t_b a + t_a b - l = ba = b\varphi(a) \end{aligned}$$

and by the same reasoning as above we define $\pi_b(a) = -ab + t_b a + t_a b - l$. For $\pi_b(ab)$ we consider the product bab in A'. We have

$$\begin{aligned} b(ab) = (ba)b = (-ab + t_b a + t_a b - l)b = \\ = -a(t_b b - q_b) + t_b ab + t_a(t_b b - q_b) - lb = -t_a q_b + q_b a + (t_a t_b - l)b \end{aligned}$$

and with the same argument we get

$$\begin{cases} \pi_b(1) = b \\ \pi_b(a) = -ab + t_b a + t_a b - l \\ \pi_b(b) = t_b b - q_b \\ \pi_b(ab) = -t_a q_b + q_b a + (t_a t_b - l)b \end{cases}$$

which we extend by k-linearity to A. Then we have defined the translation and the proof of (i) follows immediately. We have now to show that conditions (ii) and (iii) are satisfied. For proving condition (iii) let T be a submodule of A with $1 \in T$ and suppose that $\pi_a(T) \subseteq T$ and $\pi_b(T) \subseteq T$. Then we have $a \in T$ since $a = \pi_a(1)$ and also $b \in T$ since $b = \pi_b(1)$. Then also $ab \in T$ since $ab = \pi_a(b)$. So T is a submodule of A and contains all the elements of a basis so $T = A$. Let us now consider condition (ii). We have to show that $\pi_a \circ \pi_a(x) = t_a\pi_a(x) - q_a\mathrm{Id}(x)$ for all $x \in A$ and similarly for π_b and also that $\pi_a \circ \pi_b(x) + \pi_b \circ \pi_a(x) = t_b\pi_a(x) + t_a\pi_b(x) - l$. We prove that this is true on the elements of the basis. It is clear for $\pi_a(\pi_a(1))$ and $\pi_b(\pi_b(1))$. For the first kind of relations the other cases are similar and we are going to write explicitly only $\pi_b(\pi_b(ab))$. We have:

$$\begin{aligned} \pi_b(\pi_b(ab)) &= \pi_b(-t_a q_b + q_b a + (t_a t_b - l)b) = \\ &= -t_a q_b b + q_b(-ab + t_b a + t_a b - l) + (t_a t_b - l)(t_b b - q_b) = \\ &= t_b(-t_a q_q + q_b a + (t_a t_b - l)b) - q_b ab = \\ &= t_b\pi_b(ab) - q_b\mathrm{Id}(ab). \end{aligned}$$

Also for the other relation we have to prove the equalities above for the basis elements. We do it for ab:

$$\begin{aligned}\pi_a(\pi_b(ab)) + \pi_b(\pi_a(ab)) &= \pi_a(-t_a q_b + q_h a + t_a t_b b - lb) + \pi_b(t_a ab - q_a b) = \\ &= -q_b q_a + t_a t_b ab - lab + t_a \pi_b(ab) - q_a(t_b b - q_b) = \\ &= t_a \pi_b(ab) + t_b(t_a ab - q_a b) - lab = t_a \pi_b(ab) + t_b \pi_a(ab) + l\mathrm{Id}(ab).\end{aligned}$$

So we proved the claim and A with the multiplication induced by the maps π_a and π_b is the (a,b)-R-k-algebra $\langle a, b | R\rangle$. □

Even for free modules computations in the higher dimensional case can be very long, but it should be possible in general to have a normal form as the one above.

Bibliography

[1] B.L. Van der Waerden, *Free products of groups*, *Amer. J. Math.*, Vol. 70, 1948, pp. 527–528

[2] B.L. Van der Waerden, *On Clifford algebras*, *Indag. Math.*, Vol. 28, 1966, pp. 78–83

[3] J.P. Serre, *Arbres, amalgames, SL2*, Astérisque n. 46, Soc. math. France, 1977

[4] A.G. Kurosh, *The theory of groups*, Vol. II, Chelsea publishing company, New York, 1955

[5] P.M. Cohn, *On the free product of associative rings*, *Mathematische Zeitschrift*, Vol. 71, 1959, pp. 380–398

[6] G.M. Bergman, *An Invitation to General Algebra and Universal Constructions*, http://math.berkeley.edu/∼gbergman/245/

[7] C. Chevalley, *Algebraic Theory of Spinors*, New York, Columbia University Press, 1954