Università di Pisa

Dipartimento di Matematica

Corso di Laurea in Matematica

Tesi di Laurea Triennale

The free exponential ring and the free exponential field

Candidato:

Silvio Martinico

Relatore:

Prof. Marcello Mamino

Anno Accademico 2019/2020

Contents

Introduction

The focus of this work is exponential rings and fields satisfying Schanuel's Condition.

Definition. *An exponential ring is a pair of a commutative ring R with* 1 *and a map* $E : R \longrightarrow R$ *such that:*

$$\forall\ x, y \in R\ E(x+y) = E(x) \cdot E(y)\,, \qquad E(0) = 1\,.$$

Definition. *An exponential ring R is said to satisfy Schanuel's Condition if it is a characteristic* 0 *domain and, whenever $\alpha_1, ..., \alpha_n \in R$ are linearly independent over $\mathbb{Q}$, the field $\mathbb{Q}(\alpha_1, ..., \alpha_n, E(\alpha_1), ..., E(\alpha_n))$ has transcendence degree $\geq n$ over $\mathbb{Q}$.*

Schanuel's Conjecture, formulated by Stephen Schanuel in the 1960s, says that $(\mathbb{C}, e^z)$ satisfies Schanuel's Condition. It can be seen as a generalization of Lindemann-Weierstrass Theorem, which states that if $\alpha_1, ..., \alpha_n$ are linearly independent algebraic numbers over $\mathbb{Q}$, then $e^{\alpha_1}, ..., e^{\alpha_n}$ are algebraically independent over $\mathbb{Q}$.

Currently, Schanuel's Conjecture is a fundamental open problem in the field of Transcendental Number Theory. Simple consequences of this conjecture are, for instance, that e^e, π^π, π^e are transcendental numbers or that π and e are algebraically independent over $\mathbb{Q}$, all of which are open problems in their own right.

A more profound consequence in Model Theory is the solution of Tarski's exponential function problem under Schanuel's Conjecture, due to A. J. Macintyre and A. Wilkie (1995) [4], that is the decidability of the first-order theory of the real exponential field $\mathbb{R}_{exp}$, namely the real field together with the exponential function e^x.

We want to investigate the consequences of Schanuel's Condition on exponential rings and exponential fields. We will formalize the intuition that an exponential ring, respectively

an exponential field, which satisfies Schanuel's Condition is "as free as possible", that is, the only relations it satisfies are the algebraic consequences of the defining equations for exponential rings or fields respectively. In Chapter 1 we introduce some notions of Universal Algebra, which we need to formalize the concepts of of free object and word problem. In particular, we introduce equational classes, that is, classes of algebras which can be described through a set of identities. We will see that an equational class with constant functions has a free object on every set, where a free object is an algebra that admits a morphism to every algebra of the class. We are interested in the study of the free object in the class of exponential rings which we call the *free exponential ring* $[\emptyset]^E$.

In Chapter 2 we focus on the free exponential ring. Our aim is to prove the following theorems:

Theorem 2.4. *The free exponential ring satisfies Schanuel's Condition.*

Theorem 2.10. *Let S be an E-ring which satisfies Schanuel's Condition. Let $S_0 \subset S$ be the exponential subring of S generated by* 1*. Then the natural E-morphism $\varphi : [\emptyset]^E \longrightarrow S_0$ is an isomorphism.*

Our approach is to rewrite the free exponential ring given by the general construction of the free algebra in Section 1.7 as a direct limit $[\emptyset]^E = \varinjlim R_n$ where the exponential map $E : [\emptyset]^E \longrightarrow [\emptyset]^E$ maps R_n to R_{n+1}. This construction enables us to prove both theorems by induction or recursion over the sequence $\{R_i\}_{i\in\mathbb{N}}$.

As opposed to rings' case, exponential fields don't form an equational class, as a consequence of Birkhoff's Theorem. Indeed one cannot even speak of "free field", let alone "free exponential field" (see Example 3.1). To tackle this case, in Chapter 3, we adopt the definition proposed by Macintyre [3]. This approach leads to an ad hoc construction which resembles the one for exponential rings explored in Chapter 2, however, unlike the case of exponential rings, it makes use of the axiom of choice.

Similarly to the rings' case we prove the following theorems:

Theorem 3.1. *The free exponential field $\langle\emptyset\rangle^E$ satisfies Schanuel's Condition.*

Theorem 3.2. *Let S be an E-field which satisfies Schanuel's Condition and let S_0 be the E-subfield generated by* 1*. Then $S_0 \simeq \langle\emptyset\rangle^E$.*

Finally, in Chapter 4 we study the word problem for the free exponential ring (field). The word problem for an algebra $\mathbf{A}$ is the decision problem of determining whether two terms in the language of $\mathbf{A}$ are equal in $\mathbf{A}$. For example, the word problem for the natural numbers in the language $\{0, 1, +, \cdot\}$ is decidable because the operations $+$ and $\cdot$ are computable. On the other hand, it was shown by Pyotr Novikov in 1955 that there exists a finitely presented group G such that the word problem for G is undecidable [5]. The example of the natural numbers demonstrates that if the basic operations of an algebra are computable then the word problem is decidable. This is indeed the case of the exponential rings. However, recalling that the free exponential field is constructed using the axiom of choice, it is not obvious how to represent it computably. For this case, even though we can't associate computably a normal form with each element, we exhibit an algorithm that, given two terms, can determine whether or not they are the same element of the field. Thus we conclude this work with the following results:

Theorem 4.1. *The word problem for the free exponential ring is decidable.*

Theorem 4.5. *The word problem for the free exponential field is decidable.*

Chapter 1

Equational classes and free objects

This chapter is devoted to the basic concepts of Universal Algebra, which is the study of algebras. An algebra in given by a set together with a family of operations, like groups, rings, fields, etc. The class of groups and the class of rings can be described by a set of identities. Classes that have this property are called equational classes. These classes are important to us because exponential rings form an equational class. We will see instead that fields and exponential fields don't form equational classes. For doing that, we exploit Birkhoff's Theorem, which gave us a characterization of equational classes in terms of closure under some operators.

We introduce the concept of *free object* for a class of algebras, that is, an object for which it exists a morphism from it to every algebra of the class. We show that, under opportune hypothesis, an equational class has a free object.

See [1] for further details on Universal Algebra.

1.1 Algebras and languages

One of the aims of universal algebra is to extract the common elements of different algebraic structures, such as groups, rings, etc., into the abstract concept of "algebra" as defined below.

Definition 1.1. A language of algebras is a set $\mathcal{F}$ of function symbols such that a natural number n is assigned to each member $f \in \mathcal{F}$. This natural number is called **arity** of f

and f is said to be an n-ary function symbol. Fixed $n \in \mathbb{N}$, we denote with $\mathcal{F}_n$ the subset of $\mathcal{F}$ containing only the function symbols of arity n.
If $\mathcal{F} = \{f_1, ..., f_k\}$ is finite of cardinality $k \in \mathbb{N}$ we call **signature** of $\mathcal{F}$ the k-tuple $(a_1, ..., a_k)$, where a_i is the arity of f_i.

Definition 1.2. Let $\mathcal{F}$ be a language of algebras. An algebra on the language $\mathcal{F}$ is an ordered pair $\mathbf{A} = (A, F)$ where A is a non-empty set called the universe of $\mathbf{A}$ and F is a family of operations called fundamental operations of $\mathbf{A}$ and indexed by the language $\mathcal{F}$ such that corresponding to each n-ary function symbol $f \in \mathcal{F}$ there is an n-ary operation $f^{\mathbf{A}} : A^n \longrightarrow A$ (note that an operation of arity 0 is a constant).
A subalgebra $\mathbf{B}$ of $\mathbf{A}$ is an algebra such that $B \subset A$ and, for all $f \in \mathcal{F}$, $f^{\mathbf{B}}$ is the restriction to B of $f^{\mathbf{A}}$. We write simply $\mathbf{B} \leq \mathbf{A}$ to indicate that $\mathbf{B}$ is a subalgebra of $\mathbf{A}$.

We now define the direct product of algebras and the morphisms between algebras, which will be useful later to introduce the concept of variety of algebras:

Definition 1.3. Let $\mathbf{A}_1$ and $\mathbf{A}_2$ be two algebras on the same language of algebras $\mathcal{F}$. The direct product $\mathbf{A}_1 \times \mathbf{A}_2$ is the algebra which universe is $A_1 \times A_2$ and such that, for every n and every $f \in \mathcal{F}_n$, given $a_i \in A_1$ and $a'_i \in A_2$ for $i = 1, ..., n$, we have the fundamental operation:

$$f^{\mathbf{A}_1 \times \mathbf{A}_2}((a_1, a'_1), ..., (a_n, a'_n)) = \left(f^{\mathbf{A}_1}(a_1, ..., a_n), f^{\mathbf{A}_2}(a'_1, ..., a'_n)\right) .$$

Definition 1.4. Let $\mathbf{A}$ and $\mathbf{B}$ be algebras over the language $\mathcal{F}$. A map $\alpha : A \longrightarrow B$ is called a morphism between $\mathbf{A}$ and $\mathbf{B}$ if $\forall\ f \in \mathcal{F}$ function symbol of arity n and $\forall\ a_1, ..., a_n \in A$ holds:

$$\alpha f^{\mathbf{A}}(a_1, ..., a_n) = f^{\mathbf{B}}(\alpha a_1, ..., \alpha a_n) .$$

A morphism between two algebras is an *embedding* if it is injective. An embedding that is also a surjective map is called an isomorphism.

Definition 1.5. Let X be a set whose elements are called variables. Let $\mathcal{F}$ be a language of algebras. The set $T(X)$ of terms on the language $\mathcal{F}$ over X is the smallest set such that:

i. $X \cup \mathcal{F}_0 \subset T(X)$;

ii. If $p_1, ..., p_n \in T(X)$ and $f \in \mathcal{F}_n$ then $f(p_1, ..., p_n) \in T(X)$.

Example 1.1. For example, if we take $X = \{1\}$ and $\mathcal{F} = \{+\}$ (+ has arity 2), the set of terms on the language $\mathcal{F}$ over X is $T(X) = 1, 2, 3, ... = \mathbb{N}\backslash\{0\}$.

Definition 1.6. Given a term $p(x_1, ..., x_n)$ on the language $\mathcal{F}$ over the set $X = \{x_i\}_{i\in I}$ of variables (I is a set of indexes) and given an algebra $\mathbf{A}$ on the language $\mathcal{F}$, we define the evaluation map $p^{\mathbf{A}} : A^n \longrightarrow A$ as follows:

- If p is a variable $x_i \in X$ then:

$$p^{\mathbf{A}}(a_1, ..., a_n) := a_i \qquad \text{for } a_1, ..., a_n \in A \ ;$$

- If p is of the form $f(p_1(x_1, ..., x_n), ..., p_k(x_1, ..., x_n))$, with $f \in \mathcal{F}_k$, then:

$$p^{\mathbf{A}}(a_1, ..., a_n) := f^{\mathbf{A}}(p_1^{\mathbf{A}}(a_1, ..., a_n), ..., p_k^{\mathbf{A}}(a_1, ..., a_n)) \, .$$

We now define subdirect products:

Definition 1.7. An algebra $\mathbf{A}$ is a subdirect product of an indexed family of algebras $(\mathbf{A}_i)_{i\in I}$ if:

i) $\mathbf{A} \leq \prod_{i\in I} \mathbf{A}_i$;

ii) $\pi_i(\mathbf{A}) = \mathbf{A}_i \ \forall \ i \in I$, where π_i is the projection map over the i-th component.

An embedding $\alpha : \mathbf{A} \longrightarrow \prod_{i\in I} \mathbf{A}_i$ is said a subdirect embedding if $\alpha(\mathbf{A})$ is a subdirect product of the $\mathbf{A}_i$.

1.2 Equational classes

Now we introduce the underlying concept for equational classes:

Definition 1.8. An **identity** on the language $\mathcal{F}$ over X is an expression of the form $p \approx q$, wheree $p, q \in T(X)$ (formally it is a pair $\{p, q\}$ with $p, q \in T(X)$).

Let $Id(X)$ be the set of identities on the language $\mathcal{F}$ over X. An algebra $\mathbf{A}$ on the language $\mathcal{F}$ satisfies an identity $p(x_1, ..., x_n) \approx q(x_1, ..., x_n)$, abbrevieted by $\mathbf{A} \models p(x_1, ..., x_n) \approx q(x_1, ..., x_n)$, or more briefly $\mathbf{A} \models p \approx q$, if for every choice of $a_1, ..., a_n \in A$ we have $p^{\mathbf{A}}(a_1, ..., a_n) = q^{\mathbf{A}}(a_1, ..., a_n)$.

A class of algebras K satisfies $p \approx q$, written $K \models p \approx q$, if every member of K satisfies $p \approx q$. If Σ is a set of identities we say that K satisfies Σ ($K \models \Sigma$) if K satisfies all the identities in Σ.

Definition 1.9. Given a class of algebras K and a set of variables X let $Id_K(X) := \{p \approx q \in Id(X) : K \models p \approx q\}$

Definition 1.10. Let Σ be a set of identities on the language $\mathcal{F}$ and $M(\Sigma)$ the class of algebras $\mathbf{A}$ on the language $\mathcal{F}$ which satisfy Σ. A class of algebras K is called an **equational class** if there is a set of identities Σ such that $K = M(\Sigma)$.

Example 1.2. Examples of equational classes are:

- Semigroups: they form an equational class on the language $\mathcal{F} = \{\cdot\}$ (a binary operation) with the identity:
  - $\triangleright$ $x(yz) = (xy)z$.
- Groups: they form an equational class on the language $\mathcal{F} = \{\cdot, ^{-1}, 1\}$ (a binary operation, the inverse operation of arity 1 and the identity operation of arity 0) with the following identities identities:
  - $\triangleright$ $x(yz) = (xy)z$;
  - $\triangleright$ $1x = x1 = x$;
  - $\triangleright$ $xx^{-1} = x^{-1}x = 1$.
- Rings: they form an equational class on the language $\mathcal{F} = \{+, \cdot, ^{-1}, 0, 1\}$ (which correspond respectively to a binary sum, a binary product, the inverse operation of arity 1, the sum identity of arity 0 and the product identity of arity 0) with the following identities:

- $\triangleright$ $(x + y) + z = x + (y + z)$;
- $\triangleright$ $x + y = y + x$;
- $\triangleright$ $0 + x = x + 0 = x$;
- $\triangleright$ $x + (-x) = (-x) + x = 0$;
- $\triangleright$ $(x \cdot y) \cdot z = x \cdot (y \cdot z)$;
- $\triangleright$ $x \cdot (y + z) = x \cdot y + x \cdot z$;
- $\triangleright$ $(x + y) \cdot z = x \cdot z + y \cdot z$.

Definition 1.11. We define the class of exponential rings as the class of algebras on the language $\mathcal{F} = \{+, \cdot, E, ^{-1}, 0, 1\}$, namely the language of rings to which we add an unary exponential operation, which satisfies the ring identity plus the following operations:

- $\triangleright$ $E(x + y) = E(x) \cdot E(y)$;
- $\triangleright$ $E(0) = 1$.

Fields and exponential fields don't form equational classes because it's not possible to express the existence of the product inverse for every non-zero element with a universally verified identity. We will soon this formally, as a consequence of **Birkhoff's Theorem**.

1.3 Class operators

Our aim is now to characterize equational classes as those close under subalgebras, homomorphic images and direct products.

Definition 1.12. Given a class of algebras K, we define the following operators:

- $\mathbf{A} \in I(K) \iff \mathbf{A}$ is isomorphic to some member of K;
- $\mathbf{A} \in S(K) \iff \mathbf{A}$ is a subalgebra of some member of K;
- $\mathbf{A} \in H(K) \iff \mathbf{A}$ is the homomorphic image of some member of K;
- $\mathbf{A} \in P(K) \iff \mathbf{A}$ is the direct product of a non-empty family of algebras in K;

- $\mathbf{A} \in P_S(K) \iff \mathbf{A}$ is the subdirect product of a non-empty family of algebras in K;

Given two operators O_1 and O_2 we write O_1O_2 for their composition and we write that $O_1 \leq O_2$ if for all classes K it holds $O_1(K) \subset O_2(K)$. An operator O is said to be idempotent if $O^2 = O$ and a class K is said closed under and opertor O if $O(K) \subset K$.

Definition 1.13. A non-empty class of algebras K on the language $\mathcal{F}$ is called **variety** if it's closed under the operators S, H and P.

It's not hard to see that every class of algebras on the same language is contained in a variety (trivially, the classes of every algebras on a fixed language forms a variety) and that the intersection of varieties is still a variety, so, given a class of algebras K, there exist the smallest variety the contains K and we write it as $V(K)$.

Lemma 1.1. *The following inequalities between operators hold:*

$$SH \leq HS, \quad PS \leq SP, \quad PH \leq HP\,.$$

Furthermore the operators H, S and IP are idempotent.

Proof

We will show only the first inequality, the remaining two are similiar.
Let $\mathbf{A} \in SH(K)$. Then there exist a morphism β (which we can consider, without loss of generality, to be surjective) and an algebra $\mathbf{B} \in K$, with $\beta : \mathbf{B} \longrightarrow \mathbf{C}$ such that $\mathbf{A} \leq \mathbf{C}$, so, in particular, $\mathbf{A} = \beta(\beta^{-1}(\mathbf{A}))$, i.e. $\mathbf{A}$ is an homomorphic image of a subalgebra of $\mathbf{B} \in K$ (and clearly $\beta^{-1}(\mathbf{A})$ is a subalgebra of $\mathbf{B}$), i.e. $\mathbf{A} \in HS(K)$. This shows the first inequality.

□

The lemma above shows that of all the six possible orders of composition of H, S and P, HSP is the largest operator (in terms of the $\leq$ relation). Indeed, Tarski's Theorem shows that the operators HSP and V coincide.

Theorem 1.2.

$$V = HSP\,.$$

Proof

We note that the following equalities chain holds:

$$HV = SV = PV = V\,, \tag{1.1}$$

in fact we clearly have $V \leq HV, SV, PV$ and, from the fact that $V(K)$ is a variety for every class K, we have $HV, SV, PV \leq V$.
Surely we have $HSP \leq HSPV$ and furthermore, thanks to (1.1), we have:

$$V = HV = HSV = HSPV\,,$$

and so:

$$HSP \leq V\,. \tag{1.2}$$

We now need the opposite inequalities. From Lemma 1.1 the following facts follow:

- $H(HSP) = HSP$ thanks to the fact that H is idempotent;
- $S(HSP) \leq HSSP = HSP$ thanks to the facts that $SH \leq HS$ and S is idempotent;
- The following inequalities chain holds:

$$\begin{aligned} P(HSP) &\overset{PH\leq HP}{\leq} HPSP \overset{PS\leq SP}{\leq} HSPP \overset{*}{\leq} HSIPIP \overset{(IP)^2=IP}{\leq} \\ &\overset{(IP)^2=IP}{\leq} HSIP \overset{I\leq H}{\leq} HSHP \overset{SH\leq HS}{\leq} HHSP \overset{H^2=H}{=} HSP\,, \end{aligned}$$

  where the passage marked with "*" is valid because for each class K it holds $K \leq I(K)$ (each element is isomorphic at least to itself).

These three facts tell us that HSP is closed under H, S and P so, for each class K, $HSP(K)$ is a variety which contains K, i.e.:

$$V \leq HSP\,. \tag{1.3}$$

Then, putting together (1.2) and (1.3), we have the thesis.

□

1.4 Birkhoff's Theorem

One last lemma is needed in order to prove Birkhoff's Theorem.

Lemma 1.3. *For every class K of algebras on the same language $\mathcal{F}$ the classes K, $I(K)$, $S(K)$, $H(K)$, $P(K)$ and $V(K)$ satisfy the same identities over every set of variables X.*

Proof

Clearly K and $I(K)$ satisfy the same identities.

Since $I \leq IS$, $I \leq H$ and $I \leq IP$ the following containments apply:

$$Id_K(X) \supset Id_{S(K)}(X), \tag{1.4}$$

$$Id_K(X) \supset Id_{H(K)}(X), \tag{1.5}$$

$$Id_K(X) \supset Id_{P(K)}(X), \tag{1.6}$$

where $Id_K(X) := \{p \approx q \in Id(X) : K \models p \approx q\}$.

We proceed to show the opposite containments, so as we have the equalities and therefore the thesis. We show only the first containment, that is the opposite of the containment in (1.4), the others are similar.

Let $p \approx q \in Id_K(X)$, then $K \models p(x_1, ..., x_n) \approx q(x_1, ..., x_n)$. Let $\mathbf{B} \leq \mathbf{A} \in K$ and $b_1, ..., b_n \in B \subset A$. So we have:

$$p^{\mathbf{A}}(b_1, ..., b_n) = q^{\mathbf{A}}(b_1, ..., b_n)\,,$$

but then, by the definition of subalgebra, it also holds:

$$p^{\mathbf{B}}(b_1, ..., b_n) = p^{\mathbf{A}}(b_1, ..., b_n) = q^{\mathbf{B}}(b_1, ..., b_n) = q^{\mathbf{B}}(b_1, ..., b_n)\,,$$

i.e. $\mathbf{B} \models p \approx q$ and so $Id_K(X) \subset Id_{S(K)}(X)$, which, together with (1.4), it implies that $Id_K(X) = Id_{S(K)}(X)$.

From Tarski's Theorem we have $V = HSP$ and, using the equalities we have just showed, we obtain:

$$Id_{V(K)}(X) = Id_{HSP(K)}(X) = Id_{SP(K)}(X) = Id_{P(K)}(X) = Id_K(X)\,.$$

□

We can then go on to state and prove the **Birkhoff's Theorem**:

Theorem 1.4. *K is an equational class $\iff$ K is a variety.*

Proof

K is an equational class so there exists a set of identities Σ such that $K = M(\Sigma)$. Then, by Lemma 1.3 it holds that K and $V(K)$ satisfy the same identities, so $V(K)$ satisfies every identity in Σ, i.e. $V(K) \models \Sigma$; this implies that $V(K) \subset M(\Sigma) = K$. But then, given that by definition $K \subset V(K)$, we have double containment and therefore the equality:

$$V(K) = K\,,$$

i.e. K is a variety.

We will show the other arrow of the theorem at the end of this chapter, since it requires some tools and notions which we have yet to introduce.

□

Corollary 1.1. *The class of fields and the class of exponential fields are not closed under P, thus, in particular, not equational.*

Proof

Given two fields F_1 and F_2 we have that for $x \in F_1$ and $y \in F_2$ with $x, y \neq 0$, $(x, 0)\cdot(0, y) = (x \cdot 0, 0 \cdot y) = (0, 0)$, so the direct product of two fields is not an integral domain and therefore it is not a field.

If by contraddition we suppose that the class of fields or the class of exponential fields are equational then, by Birkhoff's Theorem they would be varieties and this is not possible because they would be closed under direct product.

□

1.5 Free objects

We now want to give a formal definition of free object on a certain set of generators to finally see that an equational class always admits a free object on every set of generators X

such that $T(X) \neq \emptyset$. This will enable us, for instance, to say that the class of exponential rings has a free object on no generators (i.e. a free object on the empty set).

Fix a language of algebras $\mathcal{F}$ and a set X, we define the *term algebra* of X over the language $\mathcal{F}$, written $\mathbf{T}(X) = (T(X), F_T)$ (under the hypothesis that $T(X) \neq \emptyset$), where $T(X)$ is the set of terms of X over the language of algebras $\mathcal{F}$ and F_T is the set of fundamental operations such that:

$$f^{\mathbf{T}(X)} : (p_1, ..., p_n) \mapsto f(p_1, ..., p_n)$$

for $f \in \mathcal{F}_n$ and $p_i \in T(X)$ for $i = 1, ..., n$.

Definition 1.14. Given an algebra $\mathbf{A} = (A, F)$ on $\mathcal{F}$, we say that $B \subset A$ is a subuniverse of $\mathbf{A}$ if B is closed under the opertions of $\mathbf{A}$, i.e. if given an operation of a certain arity n of $\mathbf{A}$ and given $a_1, ..., a_n \in B$, we have $f(a_1, ..., a_n) \in B$.

Definition 1.15. For every $X \subset A$ we define the subuniverse generated by X as:

$$Sg(X) := \bigcap \{B : X \subset B \text{ and } B \text{ is a subuniverse of } A\},$$

which is none other than the smallest subuniverse that contains X.

If $Sg(X) = A$ we say that X generates $\mathbf{A}$.
We observe that $\mathbf{T}(X)$ is generated by X.

Let K be a class of algebras on the language $\mathcal{F}$ and let $\mathbf{U}(X)$ be an algebra generated by X on the language $\mathcal{F}$. If $\forall\ \mathbf{A} \in K$ and $\forall\ \alpha : X \longrightarrow A$ there exists a morphism $\beta : \mathbf{U}(X) \longrightarrow A$ such that β extends α then we say that $\mathbf{U}(X)$ has the **universal mapping property** for K over X, X is called a set of free generators of $\mathbf{U}(X)$ and $\mathbf{U}(X)$ is said to be the *free object* generated by X.
We observe that the extension β is unique because a morphism is uniquely determined by the generators.

Theorem 1.5. *For any languange of algebras $\mathcal{F}$ and set X of variables, where $X \neq \emptyset$ if $\mathcal{F}_0 = \emptyset$, the term algebra $\mathbf{T}(X)$ has the universal mapping property for the class of all algebras on the language $\mathcal{F}$ over X.*

Proof

Let $\alpha : X \longrightarrow A$, where $\mathbf{A}$ is an algebra on $\mathcal{F}$. We define:

$$\beta : T(X) \longrightarrow A$$

recursively by:

- $\beta x = \alpha x$ for $x \in X$;
- $\beta(f(p_1, ..., p_n)) = f^{\mathbf{A}}(\beta p_1, ..., \beta p_n)$ for $p_1, ..., p_n \in T(X)$ and $f \in \mathcal{F}_n$.

Then $\beta(p(x_1, ..., x_n)) = p^{\mathbf{A}}(\alpha x_1, ..., \alpha x_n)$ and it's a morphism extending α.

□

1.6 Congruences

Definition 1.16. Let $\mathbf{A}$ be an algebra on the language $\mathcal{F}$ and let θ be an equivalence relation over A. θ is said to be a congruence over $\mathbf{A}$ if $\forall$ $f \in \mathcal{F}$ n-ary function symbol and $\forall$ $a_1, ..., a_n, b_1, ..., b_n \in A$ holds:

$$\forall\ i = 1, ..., n a_i \theta b_i \implies f^{\mathbf{A}}(a_1, ..., a_n) \theta f^{\mathbf{A}}(b_1, ..., b_n)\,.$$

We denote with $Con(\mathbf{A})$ the set of all congruences over $\mathbf{A}$ and we define the quotient algebra of $\mathbf{A}$ over θ, for a certain $\theta \in Con(\mathbf{A})$, as follows:

Definition 1.17. The quotient algebra of $\mathbf{A}$ over θ, written as $\mathbf{A}/\theta$, is the algebra whose universe is A/θ equipped with the fundamental operations that satisfy:

$$f^{\mathbf{A}/\theta}(a_1/\theta, ..., a_n/\theta) = f^{\mathbf{A}}(a_1, ..., a_n)/\theta\,,$$

where $a_1, ..., a_n \in A$ and f is an n-ary function symbol in $\mathcal{F}$.

In general, the Kernel of a morphism between algebras is a congruence, more precisely:

Definition 1.18. Let $\mathbf{A}$ and $\mathbf{B}$ be two algebras on the language $\mathcal{F}$ and let $\alpha : \mathbf{A} \longrightarrow \mathbf{B}$ be a morphism. Then we define the Kernel of α as follows:

$$\ker \alpha := \{(x, y) \in \mathbf{A} \times \mathbf{A} : \varphi(x) = \varphi(y)\}$$

Theorem 1.6. *Let* $\alpha : \mathbf{A} \longrightarrow \mathbf{B}$ *be a morphism between algebras. Then* $\ker\alpha$ *is a congruence on* $\mathbf{A}$*.*

Proof

If $(a_i, b_i) \in \ker\alpha$ for $i = 1, ..., n$ and $f \in \mathcal{F}$ is a function symbol of arity n, then:

$$\begin{aligned} \alpha f^{\mathbf{A}}(a_1, ..., a_n) &\overset{\alpha \text{ morphism}}{=} f^{\mathbf{B}}(\alpha a_1, ..., \alpha a_n) \\ &\overset{(a_i,b_i)\in\ker\alpha}{=} f^{\mathbf{B}}(\alpha b_1, ..., \alpha b_n) \\ &\overset{\alpha \text{ morphism}}{=} \alpha f^{\mathbf{A}}(b_1, ..., b_n) \end{aligned}$$

so $(f^{\mathbf{A}}(a_1, ..., a_n), f^{A}(b_1, ..., b_n)) \in \ker\alpha$. Furthermore $\ker\alpha$ is clearly an equivalence relation and so we have that $\ker\alpha$ is a congruence.

□

Proposition 1.7. *Let* $\mathbf{A}, \mathbf{B}, \mathbf{C}$ *be algebras on the same language* $\mathcal{F}$*. Let* $\alpha : \mathbf{A} \longrightarrow \mathbf{B}$ *and* $\beta : \mathbf{A} \longrightarrow \mathbf{C}$ *such that* $\ker\beta = \ker\alpha$ *and* β *is surjective. Then there exists a morphism* $\gamma : \mathbf{C} \longrightarrow \mathbf{B}$ *such that* $\alpha = \gamma \circ \beta$*.*

Proof

Let $c \in C$. β in surjective, so $\exists\ a \in A : c = \beta(a)$. Then we define $\gamma(c) := \alpha(a)$ and show that γ is well defined (i.e. it doesn't depend on the choice of a) and it's a morphism.

- If we suppose $c = \beta(a) = \beta(a')$ then $(a, a') \in \ker\beta \subset \ker\alpha$ so $\alpha(a) = \alpha(a')$ and γ is well defined.

- Let $f \in \mathcal{F}_n$ and let $b_1 = \beta(a_1), ..., b_n = \beta(a_n) \in B$. Then we have:

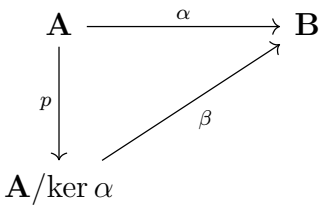
$$\begin{aligned} \gamma f^{\mathbf{C}}(c_1, ..., c_n) \ &= \ \gamma f^{\mathbf{C}}(\beta(a_1), ..., \beta(a_n)) \\ &\overset{\beta \text{ morphism}}{=} \gamma \circ \beta f^{\mathbf{A}}(a_1, ..., a_n) \\ &\overset{\gamma\circ\beta=\alpha}{=} \alpha f^{\mathbf{A}}(a_1, ..., a_n) \\ &\overset{\alpha \text{ morphism}}{=} f^{\mathbf{B}}(\alpha a_1, ..., \alpha a_n) \ = \ f^{\mathbf{B}}(\gamma c_1, ..., \gamma c_n)\,, \end{aligned}$$

  So γ is a morphism and we are done.

□

We now show that for the morphisms between algebras it holds the classic **Isomorphism Theorem**:

Theorem 1.8. *Let $\alpha : \mathbf{A} \longrightarrow \mathbf{B}$ be a morphism between algebras. Then there is an isomorphism $\beta : \mathbf{A}/\ker\alpha \longrightarrow \mathbf{B}$ defined by $\alpha = \beta \circ p$, where p is the natural projection morphism, i.e. β makes the following diagram to commute:*



Proof

Let $\ker\alpha = \theta$. First of all we notice that if $\alpha = \beta \circ p$ then we must have $\beta(a/\theta) = \alpha(a)$, so we define β in this way and we show that it's an isomorphism: β is clearly a bijection so we have to prove that it's morphism, i.e. we have to show that, taken an n-ary function symbol $f \in \mathcal{F}$ and $a_1, ..., a_n \in A$ we have:

$$\beta f^{\mathbf{A}/\theta}(a_1/\theta, ..., a_n/\theta) = f^{\mathbf{B}}(\beta(a_1/\theta), ..., \beta(a_n/\theta)) .$$

In fact we have:

$$\begin{aligned}
\beta f^{\mathbf{A}/\theta}(a_1\theta, ..., a_n\theta) &\overset{\theta \in Con\mathbf{A}}{=} \beta(f^{\mathbf{A}}(\alpha a_1, ..., \alpha a_n)/\theta) \\
&\overset{\beta(a/\theta)=\alpha(a)}{=} \alpha(f^{\mathbf{A}}(\alpha a_1, ..., \alpha a_n)) \\
&\overset{\alpha \text{ morphism}}{=} f^{\mathbf{B}}(\alpha a_1, ..., \alpha a_n) \\
&\overset{\alpha=\beta\circ p}{=} f^{\mathbf{B}}(\beta(a_1\theta), ..., \beta(a_n\theta))
\end{aligned}$$

and we have the thesis.

□

We therefore have all we need to show that an equational class admits a free object on any set X such that $T(X) \neq \emptyset$.

1.7 Free algebras

Definition 1.19. Let K be a class of algebras on the language $\mathcal{F}$ and let X be a set of variables. We define the congruence $\theta_K(X)$ on $\mathbf{T}(X)$ by:

$$\theta_K(X) := \bigcap \phi_K(X)\,,$$

where $\phi_K(X) := \{\phi \in Con\mathbf{T}(X) : \mathbf{T}(X)/\phi \in IS(K)\}$.
So we can define the K-free algebra over $\overline{X}$ as:

$$\mathbf{F}_K(\overline{X}) := \mathbf{T}(X)/\theta_K(X)\,,$$

where $\overline{X} := X/\theta_K(X)$.

We observe that:

i) $\mathbf{F}_K(\overline{X})$ exists $\iff$ $\mathbf{T}(X)$ exists $\iff$ $X \neq \emptyset$ or $\mathcal{F}_0 \neq \emptyset$;

ii) If $\mathbf{F}_K(\overline{X})$ exists then $\overline{X}$ is a set of generators.

The following theorem tells us that $\mathbf{F}_K(\overline{X})$ is the free object we are looking for:

Theorem 1.9. *Let's suppose that $T(X)$ exists. Then $\mathbf{F}_K(\overline{X})$ has the universal mapping property for K over $\overline{X}$.*

Proof

Given an algebra $\mathbf{A} \in K$, let $\alpha : \overline{X} \longrightarrow A$. Let $\nu : \mathbf{T}(X) \longrightarrow \mathbf{F}_K(\overline{X})$ be the natural projection morphism. Then $\alpha \circ \nu$ is a map from X to A, so, by the universal mapping property of $\mathbf{T}(X)$ (Theorem 1.5) there exists a morphism $\mu : \mathbf{T}(X) \longrightarrow \mathbf{A}$ extending $\alpha \circ \nu\big|_X$. It's clear that, thanks to the Isomorphism Theorem for algebras, $\ker\mu \in \phi_K(X)$, which implies that $\theta_K(X) \subset \ker\mu$. Thus, by Proposition 1.7, there is a morphism $\beta : \mathbf{F}_K(\overline{X}) \longrightarrow \mathbf{A}$ such that $\mu = \beta \circ \nu$. But then, for $x \in X$, we have:

$$\beta(\overline{x}) \;=\; \beta \circ \nu(x) \;=\; \mu(x) \;=\; \alpha \circ \nu(x) \;= \alpha(\overline{x})\,,$$

so β is a morphism which extends α and we can conclude that $\mathbf{F}_K(\overline{X})$ has the universal mapping property for K over $\overline{X}$.

□

Corollary 1.2. *If K is a class of algebras on the language $\mathcal{F}$ and $\mathbf{A} \in K$, then there exists a set X such that $\mathbf{A} \in H(\mathbf{F}_K(\overline{X}))$.*

Proof

Take X such that $|\overline{X}| \geq |A|$ and let $\alpha : \overline{X} \longrightarrow A$ be a surjective map. Then, by the universal mapping property of $\mathbf{F}_K(\overline{X})$ over $\overline{X}$, there exists a morphism $\beta : \mathbf{F}_K(\overline{X}) \longrightarrow \mathbf{A}$ which extends α, so it's surjective and $\mathbf{A}$ is the homomorphic image of $\mathbf{F}_K(\overline{X})$.

□

The next theorem (more precisely, its corollary) tells us that the free object that we have found belongs to K. But first we see a lemma that will be useful for the proof of the theorem.

Lemma 1.10. *Let $\mathbf{A}$ be an algebra and let $\theta_i \in Con(\mathbf{A})\ \forall\ i \in I$. Let $\theta = \bigcap_{i\in I} \theta_i$. Then $\mathbf{A}/\theta$ can be subdirectly embedded in $\prod_{i\in I} \mathbf{A}/\theta_i$.*

Proof

We want to find an embedding $\alpha : \mathbf{A}/\theta \longrightarrow \prod_{i\in I} \mathbf{A}/\theta_i$ such that $\alpha(\mathbf{A}/\theta)$ is a subdirect product of $\{\mathbf{A}/\theta_i\}_{i\in I}$, i.e. such that:

- $\alpha(\mathbf{A}/\theta) \leq \prod_{i\in I} \mathbf{A}/\theta_i$;
- $\pi_i(\alpha(\mathbf{A}/\theta)) = \mathbf{A}/\theta_i\ \forall\ i \in I$.

We define:

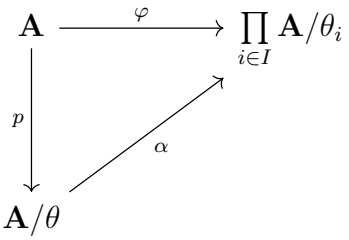
$$\varphi : \mathbf{A} \longrightarrow \prod_{i\in I} \mathbf{A}/\theta_i$$

$$a \longmapsto (a/\theta_i)_i$$

where (a/θ_i) is the I-tuple which i-th component is a/θ_i.

It is clear that $\ker \varphi = \bigcap_{i\in I} \theta_i$.

Then thanks to the Isomorphism Theorem 1.8 there exists a morphism between $\mathbf{A}/\theta$ and $\prod_{i\in I} \mathbf{A}/\theta_i$ such that $\alpha : \mathbf{A}/\theta \longrightarrow Im(\varphi)$ is an isomorphism and such that the following diagram commutes:



where p is the natural projection map. So α is the embedding we are looking for because $\alpha(\mathbf{A}/\theta) = Im(\varphi)$ is a subalgebra of $\prod_{i\in I} \mathbf{A}/\theta_i$ and it's easy to see that $\pi_i(\alpha(\mathbf{A}/\theta)) = \mathbf{A}/\theta_i$.

□

Theorem 1.11. *Let's assume that* $\mathbf{T}(X)$ *exists. Then, if* $K \neq \emptyset$, $\mathbf{F}_K(\overline{X}) \in ISP(K)$.

Proof

Due to te facts that $\mathbf{F}_K(\overline{X}) = \mathbf{T}(X)/\theta_K(X)$ and $\theta_K(X) = \bigcap \phi_K(X)$, where $\phi_K(X) \in Con\mathbf{T}(X)$, thanks to Lemma 1.10 we have $\mathbf{F}_K(\overline{X}) \in IP_S(\{\mathbf{T}(X)/\theta : \theta \in \phi_K(X)\})$.
Remembering that $\phi_K(X) = \{\phi \in Con\mathbf{T}(X) : \mathbf{T}(X)/\phi \in IS(K)\}$, we have the following containment: $\{\mathbf{T}(X)/\theta : \theta \in \phi_K(X)\} \subset IS(X)$, which implies:

$$\mathbf{F}_K(\overline{X}) \in IP_S IS(K)\,.$$

We observe that $P_S \leq SP$, so we have:

$$\mathbf{F}_K(\overline{X}) \in ISPIS(K)\,.$$

We now want to show that $ISPIS \subset ISPS(K)$.
Let $\mathbf{A} \in ISPIS(K)$, which means that $\mathbf{A}$ is isomorphic to a subalgebra of a direct product of algebras $(\mathbf{B}_i)_{i\in I}$ that are isomorphic to subalgebras $(\mathbf{C}_i)_{i\in I}$ of algebras in K, i.e. $\mathbf{A}$ is isomorphic to a subalgebra of $\prod_{i\in I} \mathbf{B}_i$, where for each $i \in I$ it hold $\mathbf{B}_i \simeq \mathbf{C}_i$ and $\mathbf{C}_i \leq \mathbf{D}_i$, for some algebras $\mathbf{D}_i \in K$. Summarizing we have:

$$\mathbf{A} \;\simeq\; \mathbf{B} \;\leq\; \prod_{i\in I} \mathbf{B}_i \;\simeq\; \prod_{i\in I} \mathbf{C}_i \;\leq\; \mathbf{D}_i \in K\,.$$

But therefore $\mathbf{A}$ is isomorphic to a subalgebra $\mathbf{C}$ of $\prod_{i\in I} \mathbf{C}_i$, i.e. it holds:

$$\mathbf{A} \;\simeq\; \mathbf{C} \;\leq\; \prod_{i\in I} \mathbf{C}_i \;\leq\; \mathbf{D}_i \in K\,,$$

that is, $\mathbf{A} \in ISPS(K)$.

So we have obtained $\mathbf{F}_K(\overline{X}) \in ISPS(K)$. Now, remembering that thanks to Lemma 1.1 it holds $PS \leq SP$, we have $\mathbf{F}_K(\overline{X}) \in ISSP(K)$ and, again thanks to Lemma 1.1, it holds that S is idempotent, i.e. $S^2 = S$. So we can conclude that $ISSP(K) = ISP(K)$ and we finally have the thesis.

□

Corollary 1.3. *For every set X, an equational class $K \neq \emptyset$ on an a language of algebras $\mathcal{F}$ such that $\mathcal{F}_0 \neq \emptyset$ has a free object over $\overline{X}$.*

Proof

$\mathcal{F}_0 \neq \emptyset \implies T(X) \neq \emptyset \implies \mathbf{F}_K(\overline{X})$ exists. Furthermore, by Theorem 1.9, $\mathbf{F}_K(\overline{X})$, has the universal mapping property for K over $\overline{X}$.

Thanks to Birkhoff's Theorem an equational class K is a variety of algebras, i.e. a class of algebras closed under H, S and P and so, in particular, closed under I, S and P. Thus, by Theorem 1.11 we have $\mathbf{F}_K(\overline{X}) \in ISP(K) \subset K$, where the last containment follows from the closure under I, S e P.

□

Corollary 1.4. *The class of exponential rings has a free object over the empty set.*

Proof

Let $\mathcal{F}$ be the language of the class of exponential rings. Then $\mathcal{F}_0 \neq \emptyset$ and so, by Corollary 1.3, the class of exponential rings has a free object over $\overline{X}$, and, since $X = \emptyset$, $\overline{X} = \emptyset$. Thus we have the thesis.

□

We call this object the **Free Exponential Ring** and we write it as $[\emptyset]^E$.

1.8 Birkhoff's Theorem and free algebras

Finally we can now prove the other arrow of Birkhoff's Theorem. For doing that, we need first some results about free algebras.

Proposition 1.12. *If K is a class of algebras on the language $\mathcal{F}$ and $p \approx q$ is an identity on the language $\mathcal{F}$ over X, then: $K \models p \approx q \iff$ for every $\mathbf{A} \in K$ and for every morphism $\alpha : \mathbf{T}(X) \longrightarrow \mathbf{A}$ we have $\alpha p = \alpha q$.*

Proof

- " $\Longrightarrow$ " Let $p = p(x_1, ..., x_n), q = q(x_1, ..., x_n)$. Suppose $K \models p \approx q$ and let $\mathbf{A} \in K$ and $\alpha : \mathbf{T}(X) \longrightarrow \mathbf{A}$ be a morphism. Then:

$$\begin{aligned} & p^{\mathbf{A}}(\alpha x_1, ..., \alpha x_n) \;=\; q^{\mathbf{A}}(\alpha x_1, ..., \alpha x_n) \\ \Longrightarrow\; & \alpha p^{\mathbf{T}(X)}(x_1, ..., x_n) \;=\; \alpha q^{\mathbf{T}(X)}(x_1, ..., x_n) \\ \Longrightarrow\; & \alpha p = \alpha q\,. \end{aligned}$$

- " $\Longleftarrow$ " Let $\mathbf{A} \in K$ and $a_1, ..., a_n \in A$. By the universal mapping property of $\mathbf{T}(X)$ there is a morphism $\alpha : \mathbf{T}(X) \longrightarrow \mathbf{A}$ such that $\alpha x_i = a_i$ for $i = 1, ..., n$. Thus:

$$\begin{aligned} p^{\mathbf{A}}(a_1, ..., a_n) \;&=\; p^{\mathbf{A}}(\alpha x_1, ..., \alpha x_n) \\ &=\; \alpha p \;=\; \alpha q \\ &=\; q^{\mathbf{A}}(\alpha x_1, ..., \alpha x_n) \\ &=\; q^{\mathbf{A}}(a_1, ..., a_n)\,, \end{aligned}$$

  so $K \models p \approx q$.

□

Proposition 1.13. *Given a class of algebras K on the language $\mathcal{F}$ and two terms $p, q \in T(X)$ on $\mathcal{F}$, it holds:*

$$K \models p \approx q \iff \mathbf{F}_K(\overline{X}) \models p \approx q \iff \overline{p} = \overline{q} \text{ in } \mathbf{F}_K(\overline{X}) \iff \langle p, q \rangle \in \theta_K(X)\,.$$

Proof

Let $\mathbf{F} = \mathbf{F}_K(\overline{X})$, $p = p(x_1, ..., x_n)$, $q = q(x_1, ..., x_n)$, and let:

$$\nu\mathbf{T}(X) \longrightarrow \mathbf{F}$$

be the natural projection morphism. Since $\mathbf{F} \in ISP(K)$, by 1.3 $K \models p \approx q$ implies $\mathbf{F} \models p \approx q$.

Suppose now that $\mathbf{F} \models p \approx q$. Then:

$$p^{\mathbf{F}}(\overline{x}_1, ..., \overline{x}_n) \;=\; q^{\mathbf{F}}(\overline{x}_1, ..., \overline{x}_n)\,,$$

hence $\overline{p} = \overline{q}$. Sequently, suppose $\overline{p} = \overline{q}$ in $\mathbf{F}$. Then it holds:

$$\nu(p) = \overline{p} = \overline{q} = \nu(q)\,,$$

so $\langle p, q\rangle \in \ker \nu = \theta_K(X)$.

Finally, suppose $\langle p, q\rangle \in \theta_K(X)$. Given $\mathbf{A} \in K$ and $a_1, ..., a_n \in A$, choose $\alpha : \mathbf{T}(X) \longrightarrow \mathbf{A}$ such that $\alpha x_i = a_i$ for $i = 1, ..., n$. Since $\ker \alpha \in \phi_K(X)$, we have:

$$\ker \alpha \supset \ker \nu = \theta_K(X)\,,$$

so it follows from Proposition 1.7 that there is a morphism $\beta : \mathbf{F} \longrightarrow \mathbf{A}$ such that $\alpha = \beta \circ \nu$. Then it holds:

$$\alpha(p) \;=\; \beta \circ \nu(p) \;=\; \beta \circ \nu(q) \;=\; \alpha(q)\,.$$

Consequently, by Proposition 1.12, $K \models p \approx q$.

□

Proposition 1.14. *Let K be a class of algebras on the language $\mathcal{F}$ and $p, q \in T(X)$. Then, for any set of variables Y with $|Y| \geq |X|$ we have:*

$$K \models p \approx q \iff \mathbf{F}_K(\overline{Y}) \models p \approx q\,.$$

Proof

- " $\Longrightarrow$ " This arrow is obvious because $\mathbf{F}_K(\overline{Y}) \in ISP(K)$ and by 1.3 K and $ISP(K)$ satisfy the same identities.
- " $\Longleftarrow$ " Take $X_0 \supset X$ such that $|X_0| = |Y|$. Then $\mathbf{F}_K(\overline{X}_0) \cong \mathbf{F}_K(\overline{Y})$ and, since by Proposition 1.13 we have:

  $$K \models p \approx q \iff \mathbf{F}_K(\overline{X}_0) \models p \approx q$$

  it follows the thesis.

□

Proposition 1.15. *Suppose K is a class of algebras on the language $\mathcal{F}$ and X is a set of variables. Then for any infinite set of variables Y it holds:*

$$Id_K(X) \;=\; Id_{\mathbf{F}_K(\overline{Y})}(X)\,.$$

Proof

For $p \approx q \in Id_K(X)$, with $p = p(_1, ..., x_n), q = q(x_1, ..., x_n)$, we have $p, q \in T(\{x_1, ..., x_n\})$. As $|\{x_1, ..., x_n\}| < |Y|$, by Proposition 1.14 we have:

$$K \models p \approx q \iff \mathbf{F}_K(\overline{y}) \models p \approx q\,,$$

so we have the thesis.

□

We now have all is needed to prove that a variety is an equational class.

Theorem 1.16. *Let V be a variety of algebras on the language $\mathcal{F}$. Then V is an equational class.*

Proof

We show that $V = M(Id_K(X))$ for any infinite set of variables X.
Let $V' := M(Id_K(X))$. Clearly V is a variety, in fact, by 1.3 it's closed under H, S and P.
$V \subset V'$ because every algebra in V satisfies the identities of $Id_V(X)$, so it is in V'. We now show the opposite containment so that we have equality.
We observe that $Id_{V'}(X) = Id_V(X)$, so, by Proposition 1.13, we have:

$$\mathbf{F}_{V'}(\overline{X}) = \mathbf{F}_V(\overline{X})\,. \tag{1.7}$$

Taken an infinite set of variables Y, by Proposition 1.15 we have:

$$Id_{V'}(Y) \overset{1.15}{=} Id_{\mathbf{F}_{V'}(\overline{X})}(Y) \overset{1.7}{=} Id_{\mathbf{F}_V(\overline{X})}(Y) \overset{1.15}{=} Id_V(Y)\,.$$

Again, by Proposition 1.13, we have $\theta_{V'}(Y) = \theta_{V'}(Y)$, which implies that $\mathbf{F}_{V'}(\overline{Y}) = \mathbf{F}_V(\overline{Y})$.

Now, taken $\mathbf{A} \in V'$, by Corollary 1.2, for a suitable infinite set Y, we have that $\mathbf{A} \in H(\mathbf{F}_{V'}(\overline{Y}))$, so, thanks to 1.7, $\mathbf{A} \in H(\mathbf{F}_V(\overline{Y}))$. But, remembering the result in Corollary 1.3 and since V is a variety, $\mathbf{F}_V(\overline{Y}) \in V$. Thanks again to the fact that V is a variety, we have that $H(\mathbf{F}_V(\overline{Y})) \subset V$. So $\mathbf{A} \in V$. Thus $V' \subset V$ and we have the thesis.

□

Chapter 2

Schanuel's Condition and free exponential rings

Schanuel's Conjecture has several consequences in the field of Transcendental Number Theory. It is a tough open problem in this field. For example we don't know if e^e or π^π are transcendental. In this case Schanuel's Conjecture solves these problems. Inspired by Schanuel's Conjecture we define the Schanuel's Condition:

Definition 2.1. We say that an E-ring R satisfies **Schanuel's Condition** if R is a characteristic 0 domain and, whenever $\alpha_1, ..., \alpha_n \in R$ are linearly independent over $\mathbb{Q}$, then $\mathbb{Z}[\alpha_1, ..., \alpha_n, E(\alpha_1), ..., E(\alpha_n)]$ has transcendence degree $\geq n$ over $\mathbb{Z}$.

We observe that it's equivalent to ask that $\mathbb{Q}(\alpha_1, ..., \alpha_n, E(\alpha_1), ..., E(\alpha_n))$ has transcendence degree $\geq n$ over $\mathbb{Q}$ (we will use this version for fields).

Schanuel's Conjecture states that the exponential field $(\mathbb{C}, e^z)$ satisfies Schanuel's Condition.

Let's see two examples of how to exploit Schanuel's Conjecture to solve the above problems:

Example 2.1.

e^e: If we take $\alpha_1 = 1$ and $\alpha_2 = e$ and $E(x) = e^x$, by Schanuel's Conjecture we have that the transcendence degree over $\mathbb{Q}$ of $\mathbb{Q}(1, e, e^1, e^e)$ is at least 2, but $e^1 = e$ and $1 \in \mathbb{Q}$, so we have that $\mathbb{Q}(e, e^e)$ has transcendence degree ≥ 2 over $\mathbb{Q}$, thus e^e is transcendental.

Example 2.2.

π^π: We put $\alpha_1 = \log(\log \pi)$, $\alpha_2 = \log \pi$, $\alpha_3 = \pi \log \pi$ and $\alpha_4 = i\pi$, so $e^{\alpha_1} = \log \pi$, $e^{\alpha_2} = \pi$, $e^{\alpha_3} = \pi^\pi$ and $e^{\alpha_4} = -1$. Now we observe that $e^{\alpha_1} = \alpha_2$, π and $i\pi$ are not algebraically independent, $-1 \in \mathbb{Q}$ and α_2, α_3 and α_4 are linearly independent but not algebraically independent because $\alpha_3 = (\alpha_2 \cdot \alpha_4)/i$. So we can conclude by Schanuel's Condition.

In a similar way we can show that π^e or $\pi^{\pi^{\pi^\pi}}$ are transcendental under Schanuel's Conjecture.

Let's look at a lemma that will be useful later on:

Lemma 2.1. *Let S be an E-ring which satisfies Schanuel's condition. If R is an E-subring of S then R satisfies Schanuel's condition too.*

Proof.

The proof is trivial. Surely if S is a characteristic 0 domain, R is too; furthermore, given $\alpha_1, ..., \alpha_n \in R$ linearly independent over $\mathbb{Q}$, they belongs to S too and so, due to the fact that S satisfies Schanuel's condition, $\mathbb{Q}(\alpha_1, ..., \alpha_n, E(\alpha_1), ..., E(\alpha_n))$ has transcendence degree $\geq n$ over $\mathbb{Q}$.

□

2.1 The free exponential ring

We now give a construction of the free object over the empty set in the class of E-rings. We will see that $[\emptyset]^E$, as ring, will be got as $\lim_{n\in\mathbb{N}} R_n$ and E will be defined as the limit of the functions E_n. We define:

$$R_{-1} := \{0\}, \quad R_0 = B_0 := \mathbb{Z} \ .$$

Let Γ_n be a multiplicative group with an isomorphism $exp_n : B_n \longrightarrow \Gamma_n$ from the additive group B_n to Γ_n. Having defined B_0 we therefore have Γ_0. Hence we can define B_{n+1} as the free R_n-module over $\Gamma_n \backslash \{1\}$ and R_{n+1} as the group ring $R_n[\Gamma_n]$. We now define

$E_n : R_n \longrightarrow R_{n+1}$. Put $E_{-1} : \{0\} \longrightarrow \mathbb{Z}$ as the function such that $E_{-1}(0) = 1$. Therefore we define:

$$E_{n+1} := E_n \oplus exp_n : R_{n-1} \oplus B_n \longrightarrow R_n[\Gamma_n] \ .$$

So we have that $\varinjlim R_n$ with $E = \varinjlim E_n$ is free over the empty set (where $\varinjlim$ is the direct limit).

This object is clearly an exponential ring and it's easy to see that it is a free object, in fact it is generated by the empty set (the only subuniverse of $[\emptyset]^E$ is $[\emptyset]^E$ itself so it coincides with $Sg(X)$). Furthermore it trivially has the universal mapping property because $X = \emptyset$. What we are going to see is that not only this object maps itself in every exponential ring but it even can be embedded in every exponential ring which satisfies Schanuel's Condition. We can therefore state the fundamental theorem of this chapter which we will prove later:

Theorem 2.2. *Let S be an E-ring which satisfies Schanuel's Condition. Let $S_0 \subset S$ be the exponential subring of S generated by 1. Then the natural E-morphism $\varphi : [\emptyset]^E \longrightarrow S_0$ is an isomorphism.*

The object we have just constructed satisfies Schanuel's Condition, to prove it we first see a lemma:

Lemma 2.3. *Let $\beta_1, ..., \beta_n \in [\emptyset]^E$ such that $\beta_i \neq \beta_j$ for $i \neq j$. Therefore $E(\beta_1), ..., E(\beta_n)$ are linearly independent over $\mathbb{Q}$.*

Proof

We proceed by induction on n:

- $\mathbf{n = 1}$: This case is trivial;
- $\mathbf{n - 1 \implies n}$: Let's suppose by contradiction that $\lambda_1 E(\beta_1) + ... + \lambda_n E(\beta_n) = 0$, then, if $\lambda_1 \neq 0$, we have:

$$\lambda_1 E(\beta_1) \left(1 + \frac{\lambda_2}{\lambda_1} E(\beta_2 - \beta_1) + ... + \frac{\lambda_n}{\lambda_1} E(\beta_n - \beta_1)\right) \ = \ 0 \, ,$$

which, due to the fact that $[\emptyset]^E$ is an integral domain and that we have supposed $\lambda_1 \neq 0$, implies:

$$1 + \frac{\lambda_2}{\lambda_1} E(\beta_2 - \beta_1) + ... + \frac{\lambda_n}{\lambda_1} E(\beta_n - \beta_1) = -1\,, \tag{2.1}$$

which is a contradiction because the LHS (left-hand side) of (2.1) is a sum of elements in the various B_i with $i > 0$, while the RHS (right-hand side) is -1, i.e. it belongs to $\mathbb{Z} = B_0$ which is in direct sum with the other B_is for $i \neq 0$. Therefore $\lambda_1 = 0$ and we have:

$$\lambda_2 E(\beta_2) + ... + \lambda_n E(\beta_n) = 0$$

and this, by inductive hypothesis, implies that $\lambda_2 = ... = \lambda_n = 0$, so we have the thesis.

□

Theorem 2.4. $[\emptyset]^E$ *satisfies Schanuel's Condition.*

Proof.

We observe that $[\emptyset]^E$ is clearly a characteristic 0 integral domain.
We now want to show that, taken $\alpha_1, ..., \alpha_n \in [\emptyset]^E$ linearly independent over $\mathbb{Q}$, the field $\mathbb{Q}(\alpha_1, ..., \alpha_n, E(\alpha_1), ..., E(\alpha_n))$ has transcendence degree $\geq n$ over $\mathbb{Q}$.
Let's prove by contradition that $\{E(\alpha_1), ..., E(\alpha_n)\}$ is algebraically independent. Suppose that it isn't, so we have that $\exists\, p \in \mathbb{Q}[x_1, ..., x_n]$ such that $p \neq 0$ and $p(E(\alpha_1), ..., E(\alpha_n)) = 0$ and p is of the form:

$$p(x_1, ..., x_n) \;=\; \sum_{i=1}^{m} \lambda_i \cdot x_1^{e_{1,i}} \cdot ... \cdot x_n^{e_{n,i}} \quad \text{with } \lambda_i \in \mathbb{Q}\ \forall\ i\,,$$

then $p(E(\alpha_1), ..., E(\alpha_n)) \;=\; \sum_{i=1}^{m} \lambda_i \cdot E(c_i)$, where the c_is are a linear combination with integer coefficients of the α_is, so $c_i \neq c_k$ for $i \neq k$, which implies, thanks to Lemma 2.3, that the $E(c_i)$s are linearly independent over $\mathbb{Q}$ and so $\lambda_i = 0\ \forall\ i$, i.e. $p = 0$ and we have reached a contradiction.

□

2.2 Control operators

We now define two operators $\mathscr{D}$ and $\mathscr{E}$ over the set of finite subsets of $[\emptyset]^E$, which we will need to have a "control" on the elements of $[\emptyset]^E$. We define them on singletons and we can then extend them to every finite subset through union, i.e. $\forall\ A_1, A_2 \subset [\emptyset]^E$ finite subsets of $[\emptyset]^E$ we have:

$$\mathscr{D}(A_1 \cup A_2) = \mathscr{D}(A_1) \cup \mathscr{D}(A_2) \quad \text{and} \quad \mathscr{E}(A_1 \cup A_2) = \mathscr{E}(A_1) \cup \mathscr{E}(A_2)\ .$$

Let $\alpha \in [\emptyset]^E$ and let $n := \min\{k \in \mathbb{N} \mid \alpha \in R_k\}$. Then we write:

$$\alpha = \sum_{k=0}^{n} \alpha_k \quad \text{with } \alpha_k \in B_k\ \forall\ k \in \{0, ..., n\}\ .$$

We define the operators on the α_k and then define:

$$\mathscr{D}(\{\alpha\}) = \bigcup_{k=0}^{n} \mathscr{D}(\{\alpha_k\}) \quad \text{e} \quad \mathscr{E}(\{\alpha\}) = \bigcup_{k=0}^{n} \mathscr{E}(\{\alpha_k\})\ .$$

For $k > 0$ we write:

$$\alpha_k = \sum_{d \in B_{k-1}} c_d \cdot E(d)\ , \quad \text{with } c_d \in R_{k-1}\ .$$

In this case we define:

$$\mathscr{D}(\{\alpha_k\}) := \{d \mid c_d \neq 0\} \cup \{c_d \mid d \neq 0\}\ , \qquad \mathscr{E}(\{\alpha_k\}) := \{d \mid c_d \neq 0\}\ .$$

For $k = 0$, $a_k \in \mathbb{Z}$, so we put:

$$\mathscr{D}(\{\alpha_0\}) := \{\alpha_0\}\ , \qquad \mathscr{E}(\{\alpha_0\}) := \{0\}\ .$$

Given $A \subset [\emptyset]^E$ a finite subset and $n \in \mathbb{N}$ the minimum for which $A \subset R_n$, we lastly define for $0 \leq k < n$:

$$A^{(0)} = A_{(0)} := A\ , \quad A^{(k+1)} := \mathscr{D}(A^{(k)})\ , \quad A_{(k+1)} := \mathscr{E}(A^{(k)})\ .$$

Given $\alpha \in [\emptyset]^E$ and $A = \{\alpha\}$ we observe that $\alpha \in \mathbb{Z}[A^{(1)}, E(A_{(1)})]$.

2.3 Pure submodules

We now introduce a key property for modules that will be useful to us later on: the purity.

Definition 2.2. Let R be a ring and M an R-module. A submodule P of M is said to be pure in M if, called $i : P \longrightarrow M$ the inclusion map, for every R-module X the map induced by i on the tensor product $i \otimes id_X : P \otimes X \longrightarrow M \otimes X$ is injective.

Equivalently:

Definition 2.3. A short exact sequence of R-modules:

$$0 \longrightarrow P \xrightarrow{f} M \xrightarrow{g} C \longrightarrow 0$$

is said to be pure exact if the sequence stays exact when tensored with any R-module X.

The definition through exact sequences is equivalent to saying that $f(P)$ is a pure submodule of M.

Let's see a useful property that makes it easier to show that a given submodule is pure:

Proposition 2.5. *If $M = \bigoplus_{j \in J} P_j$, where the P_js are submodules of M, then P_j is pure in M for all $j \in J$.*

Proof

Let's fix an index $k \in J$ and show that P_k is pure in M. Let

$$i_k : P_k \longrightarrow M = \bigoplus_{j \in J} P_j$$

be the natural inclusion map, i.e. i maps an element $p \in P_k$ in the element whose components are 0 in every P_j with $j \neq k$, while the component in P_k is equal to p.
Then, taken an R-module X, we have:

$$M \otimes X \;=\; (\bigoplus_{j \in J} P_j) \otimes X \;=\; \bigoplus_{j \in J} (P_i \otimes X)$$

so the map induced by i_k is clearly injective because it's none other than the map that send an element $p \otimes a \in P_k \otimes X$ in the respective component of the direct sum, just like the map i_k does.

□

Thanks to Proposition 2.5 we have that the B_is are pure submodules of $[\emptyset]^E$ because, as additive group, $[\emptyset]^E = \bigoplus_{i\geq 0} B_i$.
It is not hard to see that the intersection of pure submodules is still pure, so we can give the following definition:

Definition 2.4. Given an R-module M and a subset $X \subset M$, we define the **pure closure** of X in M as the smallest pure submodule P in M which contains X and we write it as X^*.

Given an element $\alpha \in [\emptyset]^E$ and putting $A = \{\alpha\}$, we want to find a $\mathbb{Z}$-basis Δ_j of the pure closure of $C_j := A_{(n)} \cup ... \cup A_{(j)}$ in $[\emptyset]^E$ (as $\mathbb{Z}$-module) for $j = 0, ..., n$.
Let's see two lemmas which will be useful to this purpose:

Lemma 2.6. *Let $k \in \mathbb{Z}\backslash\{0\}$. Then the pure closure of $\{k\}$ in $[\emptyset]^E$ is $\mathbb{Z}$.*

Proof

Clearly $\mathbb{Z}$ is a $\mathbb{Z}$-submodule of $[\emptyset]^E$. We remind moreover that $\mathbb{Z}$ is pure in $[\emptyset]^E$ because $\mathbb{Z} = B_0$. So $\{k\}^* \subset \mathbb{Z}$ and it's a pure submodule of $\mathbb{Z}$ which contains k so it can't be the trivial submodule $\{0\}$. Then $\{k\}^* = \mathbb{Z}$ in that the submodules of $\mathbb{Z}$ are the $n\mathbb{Z}$s and for $n \neq 0, 1$ they aren't pure submodules because, if we suppose by contraddition that $n\mathbb{Z}$s are pure, then the exact sequence:

$$0 \longrightarrow n\mathbb{Z} \longrightarrow \mathbb{Z} \longrightarrow \mathbb{Z}/n\mathbb{Z} \longrightarrow 0$$

would split [2], i.e. we would have $\mathbb{Z} \simeq n\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z} \simeq n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$, which is not possible because $\mathbb{Z}$ hasn't non-trivial finite order elements while $n\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ has torsion elements.

□

Lemma 2.7. *Let $\alpha = \lambda \cdot E(\beta)$, where $\lambda \in \mathbb{Z}$ and $\beta \in R_{n-1}\backslash R_{n-2}$ (so $\alpha \in B_n$) with $n > 0$. Then the pure closure of $\{\alpha\}$ in $[\emptyset]^E$ is $\mathbb{Z} \cdot E(\beta)$.*

Proof

B_n is pure in $[\emptyset]^E$ so surely $\{\alpha\}^* \subset B_n$. $\mathbb{Z} \cdot E(\beta)$ is clearly a submodule of $[\emptyset]^E$ and it is the smallest submodule of $[\emptyset]^E$ which contains $E(\beta)$. Furthermore he is pure in that:

$$B_n = \bigoplus_{\beta \in R_{n-1}\backslash R_{n-2}} (\mathbb{Z} \cdot E(\beta))$$

and the B_ns are direct addends of $[\emptyset]^E$.

But then the pure closure of α is contained in $\mathbb{Z} \cdot E(\beta)$ and rather they coincide because the submodules of $\mathbb{Z} \cdot E(\beta)$ are of the form $n(\mathbb{Z} \cdot E(\beta)) \simeq n\mathbb{Z}$ and therefore the same considerations apply as in the case of $\mathbb{Z}$.

□

Taken an $\alpha \in B_n$ it can be written as the sum of a finite number of elements of the form $\lambda_i \cdot E(\beta_i)$ of Lemma 2.7 and therefore, as we have just seen, the pure closure of $\{\alpha\}$ will be given by the direct sum of the pure closure of the single terms, as this sum will be a sub-module of B_n, it is clearly pure because it's a direct sum of direct addends of B_n and it will therefore be itself a direct addendum and it's the smallest pure submodule containing $\{\alpha\}$ because it coincides with the submodule generated by the various $E(\beta_i)$s.

We now introduce a last operator that will be useful to describe the Δ_is. Let $\alpha \in [\emptyset]^E$. As we have already done we define the new operator $\tilde{\mathscr{E}}$ on singletons and then extend it through the union. Let n be the minimum such that $\alpha \in R_n$. This time we write:

$$\alpha = \sum_{i \in I_\alpha} \lambda_i \cdot E(d_i), \quad \text{where } \lambda_i \in \mathbb{Z} \text{ and } d_i \in R_{n-1} \ .$$

Therefore we define:

$$\tilde{\mathscr{E}}(\{\alpha\}) \ := \ \{d_i \mid i \in I_\alpha\} \ .$$

After the considerations we have made, we can therefore state the following proposition:

Proposition 2.8. *Let $\alpha \in [\emptyset]^E \backslash \{0\}$ and let n be the minimum such that $\alpha \in R_n$. Therefore, for all $i = 1, ..., n$, it holds:*

$$\Delta_i \ = \ \Delta_{i+1} \cup \{E(\tilde{\mathscr{E}}(\beta)) \mid \beta \in A_{(i)}\} \quad \textit{with } \Delta_n = \{1\}$$

is a $\mathbb{Z}$-basis of the pure closure of $A_{(n)} \cup ... \cup A_{(i)}$ in $[\emptyset]^E$.

Proof

We use the principle of induction on $k = n - i$.

- $k = 0$: $A_{(n)} \subset \mathbb{Z}$ and, since $\alpha \neq 0$ and n is the minimum such that $\alpha \in R_n$, then $A_{(n)} \neq \{0\}$. So, thanks to Lemma 2.6, $(A_{(n)})^* = \mathbb{Z}$ and so $\{1\}$ is a $\mathbb{Z}$-basis;

- $k-1 \Rightarrow k$: By induction hypothesis we have that Δ_{i+1} is a basis of the pure closure of $A_{(n)} \cup ... \cup A_{(i+1)}$. As stated in the Lemma 2.7 and in the consideration below it, we just need to add to Δ_{i+1} the elements of the set $\{E(\tilde{\mathscr{E}}(\beta)) \mid \beta \in A_{(i)}\}$.

□

2.4 Embedding of the free exponential ring

Let's see a lemma that we will need for the proof of the next theorem:

Lemma 2.9. $\{\Delta_{n-k}, E(\Delta_{n-k})\}$ *is algebraic over* $\{E(\Delta_{n-k})\}$.

Proof

We first show that $A^{(n-k)}$ is algebraic over $E(\Delta_{n-k-1})$.

We proceed by induction on k. The base case is trivial because $A^{(n)} \subset \mathbb{Z}$. We then proceed with the inductive step. Let $\alpha \in A^{(n-k)}$. We write: $\alpha = \alpha_0 + ... + \alpha_n$ like we did in the definition of the control operators. Therefore we have:

$$\alpha = \sum_d c_d \cdot E(d) \tag{2.2}$$

and so the c_ds belong to $A^{(n-k+1)} = A^{(n-(k-1))}$ which, by inductive hypothesis, is algebraic over $E((\Delta_{n-k}) \subset E((\Delta_{n-k-1})$. Meanwhile each d belongs to $\mathscr{E}(A^{(n-k)}) = A_{(n-k+1)}$ which is $\mathbb{Z}$-generated by $\Delta_{n-k+1} \subset \Delta_{n-k-1}$ and thus $E(d)$ is algebraic over $E(\Delta_{n-k-1})$ (passing to exponentials the $\mathbb{Z}$-generability translates into algebraicity). So we have done because sums and products preserve the algebraicity.

Taking advantage of this fact, we now show the thesis.

Again we proceed by induction on k. The base case is trivial because $\Delta_n = \{1\}$. Remembering that $\Delta_{n-k} = \Delta_{n-(k-1)} \cup \{E(\tilde{\mathscr{E}}(A_{(n-k)}))\}$, let's see the inductive step: by inductive hypothesis $\Delta_{n-(k-1)}$ is algebraic over $E(\Delta_{n-(k-1)}) \subset E(\Delta_{n-k})$. The only thing left to prove is that $\{E(\tilde{\mathscr{E}}(A_{(n-k)}))\}$ is algebraic over $E(\Delta_{n-k})$. Let $\alpha \in A_{(n-k)}$; we write it as follows:

$$\alpha = \sum_{i \in I_\alpha} \lambda_i \cdot E(d_i), \quad \text{with } \lambda_i \in \mathbb{Z}$$

and $E(\tilde{\mathscr{E}}(A_{(n-k)}))\}$ is none other than the set of the $E(d_i)$'s with $\alpha \in A^{(n-k)}$.

This time we write

$$\alpha = \sum_d c_d \cdot E(d)$$

as we made before in (2.2) and we observe that every d belongs to $A_{(n-(k-1))}$ wich is $\mathbb{Z}$-generated by $\Delta_{n-(k-1)}$ and so, as we have seen before, $E(d)$ is algebraic over $E(\Delta_{n-(k-1)}) \subset E(\Delta_{n-k})$. The c_ds insted belongs to $A^{(n-k+1)}$ which we have just proved to be algebraic over $E(\Delta_{n-k})$. Also in this case we conclude because sums and products preserve algebraicity.

□

Theorem 2.10. *Let S be an E-ring which satisfies Schanuel's Condition. Let $S_0 \subset S$ be the exponential subring of S generated by 1. Then the natural E-morphism $\varphi : [\emptyset]^E \longrightarrow S_0$ is an isomorphism.*

Proof

First of all, we note that φ is a morphism of exponential rings, so $\varphi\left([\emptyset]^E\right)$ is an exponential subring of S and it contains the 1_S because $\varphi(1) = 1_S$. Therefore $\varphi\left([\emptyset]^E\right)$ contains the exponential subring of S generated by 1, so φ is surjective. So the injectivity is left to prove. For this purpose, we show that the Kernel of φ is trivial.

Let $\alpha \in [\emptyset]^E$ and $A := \{\alpha\}$. As we have seen before $\alpha \in \mathbb{Z}\left[A^{(1)}, E(A_{(1)})\right]$. It will therefore suffice to show the injectivity of the restriction of φ to this set.

Let $n := \min\{k \in \mathbb{N} \mid \alpha \in R_k\}$. Then $A_{(n)} \subset B_0 = \mathbb{Z}$ and $A_{(n-k)} \subset B_k$ and, more generally, $A_{(j)} \subset B_{(n-j)}$.

Let $A^*_{(j)}$ be the pure closure of $A_{(j)}$ in $[\emptyset]^E$. $A^*_{(j)} \subset B_{(n-j)}$ because $B_{(n-j)}$ is pure.

Let us now distinguish two cases: if $A^*_{(n)} = \{0\}$ then $A_{(n)} = \{0\}$ and so we have $\alpha = 0$ and there is nothing to say as $0 \in Ker(\varphi)$. Otherwise $A^*_{(n)} \subset \mathbb{Z}$ and so Δ_n has cardinality 1. Let's define then $d_j := |\Delta_{n-j}|$.

Now let's show something more than what we need (in order to exploit the induction principle to our advantage), i.e. we will show that $\forall\ j\ :\ 0 \leq j \leq n$, the restriction of φ to $\mathbb{Z}[A^{(n)}, ..., A^{(n-j)},\ A^*_{(n)}, ..., A^*_{(n-j)}]$ is injective. Indeed, if this were true, we would have concluded because $\alpha \in \mathbb{Z}[A^{(n)}, ..., A^{(n-j)},\ A^*_{(n)}, ..., A^*_{(n-j)}]$ for $j = n$.

We proceed by induction on j:

- $\mathbf{j = 0}$: This case is trivial because both $A^{(n)}$ and $A_{(n)}$ are contained in $\mathbb{Z}$ and so $A^*_{(n)} \subset \mathbb{Z}$ too and, as we have said before, the restriction of φ to $\mathbb{Z}$ is clearly injective.

- $\mathbf{j = k + 1}$: Let's suppose that the result is true for $j = k$. Δ_{n-k} is $\mathbb{Z}$-independent in that it's a $\mathbb{Z}$-basis, $\varphi(\Delta_{n-k})$ is independent too because φ is a morphism and so it preserve the independence. But then, due to the fact that by hypothesis S satisfies Schanuel's Condition, $\mathbb{Q}(\{\varphi(\Delta_{n-k}),\ E(\varphi(\Delta_{n-k}))\})$ has transcendence degree $\geq d_k$ over $\mathbb{Q}$; thanks to Theorem 2.4 $[\emptyset]^E$ satisfies Schanuel's Condition too and so $\mathbb{Q}(\{\Delta_{n-k},\ E(\Delta_{n-k})\})$ has transcendence degree $\geq d_k$ over $\mathbb{Q}$ too.

  Now $\{\Delta_{n-k},\ E(\Delta_{n-k})\}$ is algebraic over $\{E(\Delta_{n-k})\}$ thanks to Lemma 2.9, so $\{E(\Delta_{n-k})\}$ is algebraically independent (otherwise we would have that the degree of transcendence over $\mathbb{Q}$ of $\{\Delta_{n-k},\ E(\Delta_{n-k})\}$ is $< d_k$). Since φ is a morphism, $\{\varphi(\Delta_{n-k}), E(\varphi(\Delta_{n-k}))\}$ is algebraic over$\{E(\varphi(\Delta_{n-k}))\}$ and therefore the latter is algebraically independent for the same reason as before. This implies the injectivity of the restriction of φ to $\mathbb{Z}[E(\Delta_{n-k})]$ and therefore also that of the restriction on its relative algebraic closure in $[\emptyset]^E$ (thanks to the action of φ on minimum polynomials). But then we finished because the elements of $\mathbb{Z}[A^{(n)}, ..., A^{(n-j)}, A^*_{(n)}, ..., A^*_{(n-j)}]$ are algebraic over $\mathbb{Z}[E(\Delta_{n-k})]$. In fact Δ_{n-k} generates $A_{(n)} = \mathscr{E}(A^{(n-1)}), ..., A_{(n-k)} = \mathscr{E}(A^{(n-k-1)})$ and so $A^{(n)}, A^{(n-1)}, ..., A^{(n-k-1)}$ are algebraic over $E(\Delta_{n-k})$. For the $A_{(i)}$s it's sufficient to observe that they are contained in the $A^{(i)}$s and so this holds for their pure closures too, which are still algebraic over $\mathbb{Z}[E(\Delta_{n-k})]$.

□

Chapter 3

Exponential fields

As we have seen in Section 1.4, E-fields (or exponential fields), unlike E-rings, don't form an equational class. Furthermore, the definition of free object we have seen does not fit in this case because we can't divide by 0, but in the term algebra this is possible because in the language of E-fields we have both $0 \in \mathcal{F}_\prime$ and $^{-1} \in \mathcal{F}_1$. Therefore, the notion of *free* is delicate and we need to take a different path than in the case of the rings.
Moreover, also the notion of morphism between algebras we gave doesn't work. In fact, if we take an exponential field that satisfies Schanuel's Condition, there isn't any morphism between it and an exponential field that doesn't satisfy Schanuel's Condition.

Example 3.1. Take (F_1, E) a field that satisfies Schanuel's Condition and $(F_2, E') = (\mathbb{R}, 2^x)$. Clearly (F_2, E') doesn't satisfy Schanuel's Condition, in fact $2^2 = 4 \in \mathbb{Q}$.
If we take a morphism of exponential fields:

$$\varphi : (F_1, E) \longrightarrow (\mathbb{R}, 2^x)$$

it is in particular a morphism of fields and so it must be injective. But

$$\varphi(E(1) - 2) \;=\; \varphi(E(1)) - 2\varphi(1) \;=\; 2^{\varphi(1)} - 2\varphi(1) \;=\; 2 - 2 = 0\,,$$

while $E(1) - 2 \neq 0$ thanks to the hypothesis that (F_1, E) satisfies Schanuel's Condition. So a morphism of exponential fields between (F_1, E) and (F_2, E') can't exist.

Not even a morphism between exponential fields which don't satisfy Schanuel's Condition is guaranteed to exist, in fact if we take $\varphi : (F_1, E) = (\mathbb{R}, 3^x) \longrightarrow (F_2, E') = (\mathbb{R}, 2^x)$

clearly $2 - E(1) = -1$ and $\varphi(2 - E(1)) = 2 - E'(1) = 2 - 2 = 0$ but again φ must be injective.

Thus, we need a weaker notion of morphism too. We use some definitions given by A. Macintyre in [3] for defining those maps and the free exponential field and then we give an explicit construction for the latter.

3.1 Partial E-rings and $\mathscr{R}$-fields

Definition 3.1. A partial E-ring is a triple (R, A, E) where R is a commutative ring with identity, A is an additive subgroup of R and $E : A \longrightarrow R$ is a map such that $E(0) = 1$ and $E(x + y) = E(x) \cdot E(y)$.

A morphism between two partial E-rings $\mathscr{R} = (R, A, E)$ and $\mathscr{R}' = (R', A', E)$, is a morphism of rings φ which make the following diagram commutes:

$$\begin{array}{ccc} R & \xrightarrow{\varphi} & R' \\ {\scriptstyle E}\uparrow & & \uparrow{\scriptstyle E} \\ A & \xrightarrow[\varphi]{} & A' \end{array}$$

Definition 3.2. Let $\mathscr{R}$ be a partial E-ring. An $\mathscr{R}$-field is an ordered pair (K, ψ) where K is an E-field and $\psi : \mathscr{R} \longrightarrow K$ is a morphism of partial E-rings such that $\psi(\mathscr{R})$ generates K as an E-field.

We will then have the following commutative diagram:

$$\begin{array}{ccc} R & \xrightarrow{\psi} & K \\ {\scriptstyle E}\uparrow & & \uparrow{\scriptstyle E} \\ A & \xrightarrow[\psi]{} & K \end{array}$$

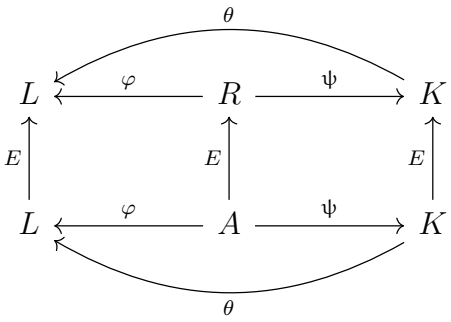
3.2 The category of $\mathscr{R}$-fields

Fixed a partial E-ring $\mathscr{R} = (R, A, E)$ we want to define a category which objects are $\mathscr{R}$-fields. Before saying who are the morphisms between objects, let's give a definition:

Definition 3.3. Let $\mathscr{R}$ and $\mathscr{S}$ be two partial E-rings. A specialization from $\mathscr{R}$ to $\mathscr{S}$ is an ordered pair $(\mathscr{R}_0, \theta)$ where $\mathscr{R}_0$ is an E-subring of $\mathscr{R}$ and $\theta : \mathscr{R}_0 \longrightarrow \mathscr{S}$ is a morphism of partial E-rings such that if $t \in \mathscr{R}_0$ is invertible in $\mathscr{R}$ then $\theta(t) = 0$ if $t^{-1} \notin \mathscr{R}_0$.

Given two $\mathscr{R}$-fields (K, ψ) and (L, φ), these are in particular two partial E-rings (K, K, E) and (L, L, E) and we can therefore consider a specialization with a morphism θ between them. If we require that $dom(\theta) \supset \psi(R)$ we can thus define an equivalence relation over specializations: we will say that two specializations $(\mathscr{R}_0, \theta)$ and $(\mathscr{R}_0', \theta')$ are equivalent if θ and θ' coincide on $\mathscr{R}_0 \cap \mathscr{R}_0'$. It's not hard to verify that the one just defined is an equivalence relation. For simplicity, from now on with specialization we will indicate an entire equivalence class.

At this point we have a category where the objects are $\mathscr{R}$-fields and the morphisms $(K, \psi) \to (L, \varphi)$ are specialization θ with $dom(\theta) \supset \psi(R)$ and such that $\theta\psi = \varphi$.



Definition 3.4. A universal $\mathscr{R}$-field is an initial object in the category of $\mathscr{R}$-fields.

3.3 The free exponential field

Let's now take the partial E-ring $\mathscr{R} = (\mathbb{Q}, \{0\}, E)$ and see the construction of a universal $\mathscr{R}$-field which we will write as $\langle\emptyset\rangle^E$.

$\langle\emptyset\rangle^E$ qua field will be taken as $\lim_{\to n\in\mathbb{N}} R_n$, where the R_ns are fields that we will define soon and E will be the limit of the functions $E_n : R_n \longrightarrow R_{n+1}$. We put:

$$R_{-1} := \{0\}\,, \qquad R_0 := \mathbb{Q}\,, \qquad E_{-1}(0) = 1\ .$$

For $n \geq 0$ R_{n+1} will be taken as the field of fractions of the group ring $R_n[\Gamma_n]$, where Γ_n is a torsion-free divisible abelian group to be specified below.

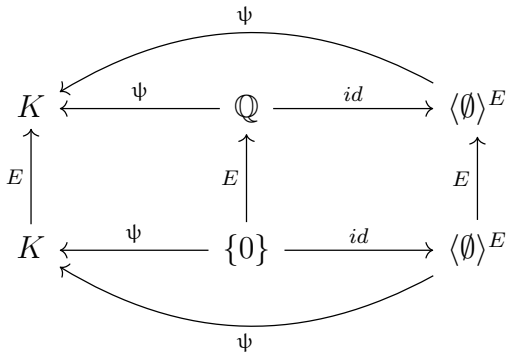
Assume inductively that we have defined R_n, E_n, B_n with $R_n = R_{n-1} \oplus B_n$ as $\mathbb{Q}$-spaces. Therefore Γ_n is a multiplicative group with an isomorphism:

$$exp_n : B_n \longrightarrow \Gamma_n \, .$$

As stated above, through R_n and Γ_n we define R_{n+1} and furthermore we define $E_{n+1} := E_n \oplus exp_n$. At this point we take a $\mathbb{Q}$-space B_{n+1} such that $R_{n+1} = R_n \oplus B_{n+1}$.

As $\mathscr{R}$-field, $\langle\emptyset\rangle^E$ coincide with the pair $(\langle\emptyset\rangle^E, id)$, where $id : \mathbb{Q} \longrightarrow \langle\emptyset\rangle^E$ is the identity which maps $\mathbb{Q}$ into his copy in $\langle\emptyset\rangle^E$.

We notice that $\langle\emptyset\rangle^E$ is an initial object in the category of $\mathscr{R}$-fields. In fact, taken an $\mathscr{R}$-field (K, ψ) we have that ψ is a specialization between $\langle\emptyset\rangle^E$ and (K, ψ) and it's clearly unique because (this holds more generally for the $\mathscr{R}$-fields and not only for $\langle\emptyset\rangle^E$) if by contradiction there are two specializations they would coincide on a set which generates and so they would coincide everywhere.



So we have seen that there is an initial object in the case of $\mathscr{R} = (\mathbb{Q}, \{0\}, E)$. We now show that it's unique: if we suppose by contradiction that there are two initial objects I_1 and I_2 then there would exist a unique morphism $\theta_1 : I_1 \longrightarrow I_2$ and a unique morphism $\theta_2 : I_2 \longrightarrow I_1$, but then $\theta_2\theta_1$ would be a morphism from I_1 to itself and, by uniqueness it would be the identity; for the same reason $\theta_1\theta_2$ would be a morphism from I_2 to itself and again, by uniqueness it would be the identity, so I_1 and I_2 are isomorphic.

After we have proved that $\langle\emptyset\rangle^E$ is a universal $\mathscr{R}$-field (and it's the only one up to isomorphism), we can go on with a theorem which is the equivalent for E-fields of Theorem

2.10. But first, we see another fundamental theorem:

Theorem 3.1. *$\langle\emptyset\rangle^E$ satisfies Schanuel's Condition.*

Proof

This proof resembles to that of the equivalent theorem for rings, i.e. Theorem 2.4.

□

3.4 Embedding of the free exponential field

Theorem 3.2. *Let S be an E-field which satisfies Schanuel's Condition and let S_0 be the E-subfield generated by 1. Then $S_0 \simeq \langle\emptyset\rangle^E$.*

Proof

S_0 and $\langle\emptyset\rangle^E$ are $\mathscr{R}$-fields with $\mathscr{R} = (\mathbb{Q}, \{0\}, E)$, so there is a unique (equivalence class of) specialization $\varphi : \langle\emptyset\rangle^E \longrightarrow S_0$ and φ is clearly surjective because $1 \in Imm(\varphi)$. We now have to show the injectivity.

Let $\alpha \in \langle\emptyset\rangle^E$, then $\alpha = \frac{a}{b}$ where a and b are exponential polynomials with rational coefficients. Thus we define the control operators in the following way:

$$\mathscr{D}(\alpha) = \mathscr{D}(a) \cup \mathscr{D}(b)\,, \qquad \mathscr{E}(\alpha) = \mathscr{E}(a) \cup \mathscr{E}(b)\,.$$

Let n be the minimum such that $\alpha \in R_n$. The sets $A^{(i)}$ and $A_{(i)}$ are defined in the usual way and Δ_i this time is just a $\mathbb{Q}$-basis of $A_{(n)} \cup ... \cup A_{(i)}$ (the purity is a useless concept now that we are working in $\mathbb{Q}$).

So we have that α belongs to the field of fractions of $\mathbb{Q}[A^{(1)}, A_{(1)}]$.

We now show by induction on $0 \leq j < n$ that the restriction of φ to the field of fractions of $\mathbb{Q}[A^{(n)}, ..., A^{(n-j)}, A_{(n)}, ..., A_{(n-j)}]$ is injective:

- $j = 0$: This case is trivial because both $A^{(n)}$ and $A_{(n)}$ are contained in $\mathbb{Q}$ and so their field of fractions does too and the restriction of φ to $\mathbb{Q}$ is injective.

- $j = k + 1$: We suppose the thesis holds for $j = k$. Δ_{n-k} is $\mathbb{Q}$-independent in that it's a $\mathbb{Q}$-basis, so $\varphi(\Delta_{n-k})$ is independent too because φ is a morphism and so it

preserves the independence. But then, since by hypothesis S satisfies Schanuel's Condition, $\mathbb{Q}(\{\varphi(\Delta_{n-k}),\ E(\varphi(\Delta_{n-k}))\})$ has transcendence degree $\geq d_k$ over $\mathbb{Q}$; $\mathbb{Q}(\{\Delta_{n-k},\ E(\Delta_{n-k})\})$ has transcendence degree $\geq d_k$ over $\mathbb{Q}$ too because, by Theorem 3.1, $\langle\emptyset\rangle^E$ satisfies Schanuel's Condition.

Now $\{\Delta_{n-k},\ E(\Delta_{n-k})\}$ is algebraic over $\{E(\Delta_{n-k})\}$ by Lemma 2.9 (in reality the situation is slightly different, we would need that exponentials of rational linear combinations of elements w_i are algebraic on $E(w_i)$, but this is actually obvious because the rational coefficients $a^{\frac{1}{k}w_i}$ at the exponents are simply obtained with the roots $\sqrt[k]{a^{w_i}}$, while for the numerators we proceed as on $\mathbb{Z}$), so $\{E(\Delta_{n-k})\}$ is algebraically independent (otherwise we would have that the transcendence degree over $\mathbb{Q}$ of $\{\Delta_{n-k},\ E(\Delta_{n-k})\}$ is $< d_k$). Since φ is a morphism, $\{\varphi(\Delta_{n-k}), E(\varphi(\Delta_{n-k}))\}$ is algebraic over $\{E(\varphi(\Delta_{n-k}))\}$ and therefore the latter is algebraically independent for the same reason just seen. This implies the injectivity of the restriction of φ to $\mathbb{Q}[E(\Delta_{n-k})]$ and so to the respective field of fractions and to its relative algebraic closure in $\langle\emptyset\rangle^E$ too (thanks to the action of φ on minimum polynomials). But then we are done because the elements of the field of fractions of $\mathbb{Q}[A^{(n)}, ..., A^{(n-j)}, A_{(n)}, ..., A_{(n-j)}]$ are algebraic over $\mathbb{Q}[E(\Delta_{n-k})]$.

□

Chapter 4

Word problem for exponential constants

We want to introduce the concept of "word problem" and then we want to prove that the free exponential ring and the free exponential field have a decidable word problem. Informally, the word problem consists of deciding whether two terms on a language are equal or not.

4.1 The word problem

Definition 4.1. An algebra (A, F) on the language $\mathcal{F}$ is the *reduct* of an algebra (A, F^*) (on the language $\mathcal{F}^*$) to $\mathcal{F}$ if $\mathcal{F} \subset \mathcal{F}^*$ and F is the restriction of F^* to $\mathcal{F}$.

Given a language of algebras $\mathcal{F}$ and a variety of algebras V on $\mathcal{F}$ we define a *presentation* as follows:

Definition 4.2. A presentation of an algebra $\mathbf{A} \in V$ in an ordered pair $\langle G, R\rangle$, where G is a set of *generators* and R a set of *defining relations* such that the following hold:

i) R is a set of identities $p(g_1, ..., g_n) \approx q(g_1, ..., g_n)$ on the language $\mathcal{F} \cup G$ (we assume $\mathcal{F} \cap G = \emptyset$) with $g_1, ..., g_n \in G$;

ii) If $\hat{V}$ is the variety on the language $\mathcal{F} \cup G$ defined by $\Sigma \cup R$, where Σ is a set of equations defining V, then $\mathbf{A}$ is the reduct of $\mathbf{F}_{\hat{V}}(\emptyset)$ to the language of V.

When the above holds we write $\mathcal{P}_V(G, R)$ for $\mathbf{A}$ and we say that it is the algebra in V freely generated by G subject to the relations R.

We observe that if $R = \emptyset$ we just obtain $\mathbf{F}_V(G)$.

The **word problem** for a given presentation $\langle G, R\rangle$ in V asks if there is an algorithm to determine, for any pair of terms $r(g_1, ..., g_n)$ and $s(g_1, ..., g_n)$, whether or not:

$$\mathbf{F}_V(\emptyset) \models r(g_1, ..., g_n) \approx s(g_1, ..., g_n)\,.$$

4.2 Word problem for the free exponential ring

If we take V as the class of exponential rings, $\langle \emptyset, \emptyset\rangle$ is a presentation of $[\emptyset]^E$ in V. The word problem for this presentation consists of determine, for any pair of terms t_1 and t_2 on the empty set in the language of exponential rings, whether or not $\mathbf{F}_V(\emptyset) \models t_1 \approx t_2$, but $\mathbf{F}_V(\emptyset) = [\emptyset]^E$, so we are wondering if, given two terms that are obtained only from a finite number of iterations of the fundamental operations of an exponential ring starting from the empty set, they are equal or not.
From the construction of $[\emptyset]^E$ we can see that the word problem is decidable.

Theorem 4.1. *The word problem for $[\emptyset]^E$ is decidable.*

Proof

Let $\alpha_1, \alpha_2 \in [\emptyset]^E$. Then $\alpha_1 = \alpha_2 \iff \alpha := \alpha_1 - \alpha_2 = 0$
Let n be the minimum such that $\alpha \in R_n$. We proceed by induction on n.
If $n = 0$ then $\alpha \in \mathbb{Z}$ and this case is trivial.
Let's suppose the thesis holds for n. Then we can write:

$$\alpha = \sum_{i=1}^{m} \lambda_i \cdot E(d_i), \quad \text{where } \lambda_i \in \mathbb{Z} \text{ and } d_i \in R_{n-1}\,,$$

and, by induction hypothesis, we can suppose that $d_i \neq d_j$ for $i \neq j$ because $d_i \in R_n \; \forall \; i$.
We show by induction on m that $\alpha = 0 \iff \lambda_i = 0 \; \forall \; i = 1, ..., m$.
If $m = 1$ $\alpha = \lambda_1 E(d_1) = 0 \iff \lambda_1 = 0$ because $[\emptyset]^E$ is an integral domain and $E(d) \neq 0 \forall d \in [\emptyset]^E$.

If we suppose the thesis for m then we have two cases: if $\exists\ j$ such that $d_j = 0$ then we have:

$$\sum_{i=1, i\neq j}^{m} \lambda_i \cdot E(d_i) = -\lambda_j$$

that, since the LHS belongs to the union of some B_i with $i \neq 0$ and the RHS belongs to B_0, implies that $\lambda_j = 0$ and so, by induction hypothesis, the LHS is 0 if and only if $\lambda_i = 0\ \forall\ i$ and we have the thesis.

If $d_j \neq 0\ \forall\ j$ then we can reduce to the previous case by writing:

$$\alpha = E(d_1)\left(\lambda_1 + \sum_{j=2}^{m+1} \lambda_j \cdot E(d_j - d_1)\right)$$

and it's 0 if and only if $\lambda_1 + \sum_{j=2}^{m+1} \lambda_j \cdot E(d_j - d_1) = 0$.

□

4.3 Word problem for the free exponential field

In the last section we gave a formalization of what is the word problem in universal algebra. However we can ask ourselves if this type of problem is decidable in general. We are interested in investigating the word problem for exponential rational terms, i.e. the elements of $\langle\emptyset\rangle^E$.

Given two terms $\alpha_1, \alpha_2 \in \langle\emptyset\rangle^E$ we don't have a normal form like in the case of $[\emptyset]^E$. In fact, we remember that in the construction of $\langle\emptyset\rangle^E$, we take it as the direct limit of R_n which is defined inductively starting from $\mathbb{Q}$ and taking R_{n+1} as the field of fractions of the group ring $R_n[\Gamma_n]$, where Γ_n is a group isomorphic to B_n. The problem is that we take B_{n+1} as the complement of R_n in R_{n+1} and, for doing that, we use the Axiom of Choice and we don't give an explicit description for it.

We see a term as the result of a finite number of iterations of the operations $\{+, -, \cdot, ^{-1}, E\}$ on the set $\{1\}$.

Before showing the procedures we define the level of a term as the maximum number of E nestled in it. We define the level of a finite set of terms as the maximum level of its elements.

PROCEDURE 1: EQUALS

Input: pair of terms x, y in the form:

$$x = \sum_{i=1}^{k_1} \frac{\lambda_i E(a_i)}{p_i} \qquad y = -\sum_{i=k_1+1}^{k} \frac{\lambda_i E(a_i)}{p_i}\,,$$

where the λ_is are integers, the a_is are terms and the p_is are exponential polynomials, i.e. terms of the form:

$$\sum_j \mu_j E(c_j)\,,$$

where $\mu_j \in \mathbb{Z}\ \forall\ j$ and the c_js are terms.

Output: "true" if $x = y$, "false" if $x \neq y$, "error" if one of the terms is not valid (i.e. there is a denominator $= 0$).

i. $x = y \iff t := x - y = 0$, so we have

$$t = \sum_{i=1}^{k} \frac{\lambda_i E(a_i)}{p_i}\,, \qquad p_i = \sum_j \mu_j E(c_j)\,.$$

ii. We check if any of the p_is is equal to 0. To do so, we find a basis of each p_i through the procedure "basis", if the basis is the empty set then $p_i = 0$ and the result of this procedure is "error", otherwise it's $\neq 0$.

iii. If each p_i is $\neq 0$ the term has sense, so the output will be "true" or "false". We use the procedure "basis" on the term t, if the basis is the empty set then $t = 0$ and the result of this procedure is "true", otherwise we have $t \neq 0$, so $x \neq y$ and the result is "false".

PROCEDURE 2: BASIS

Input: List of terms $t_1, ..., t_n$ in the form:

$$t_i = \sum_{j=1}^{k_i} \frac{\lambda_{ij} \cdot E(a_{ij})}{p_{ij}}\,,$$

where $\lambda_{ij} \in \mathbb{Z}\ \forall\ i, j$, a_{ij}s are terms and p_{ij}s are exponential polynomials with coefficients in $\mathbb{Z}$.

Output: "Error" if there is a term which is not valid, else a minimal generating sublist and coordinates for the t_is with respect to this list.

i. We check if any of the p_{ij}s is equal to 0. To do so, we find a basis of each p_i through this procedure, if the basis is the empty set then $p_i = 0$ and the result of this procedure is "error", otherwise it's $\neq 0$.

ii. We take the set of exponents of the numerators $A = \{a_{ij}\}$. For doing that, we have to check if the a_{ij} are all different. To do so, we use the procedure 1 on the a_{ij}s which are on a lower level of exponentiation. If there exist two elements of A which are equal we take only one of them. We now have $A = \{a_1, ..., a_s\}$ where s is the cardinality of A.

iii. The denominators are exponential polynomials of the form:

$$p_{ij} = \sum_{k=1}^{m_{ij}} \mu_{ijk} E(b_{ijk}) \,,$$

where $\mu_{ijk} \in \mathbb{Z} \; \forall \; i, j, k$ and the b_{ijk}s are terms. Then we take the exponents $B = \{b_{ijk}\}$ as we did in the previous step. We now have $B = \{b_1, ..., b_r\}$ where r is the cardinality of B;

iv. We define $C := A \cup B$;

v. If $C = \{0\}$ (in this case $t_i \in \mathbb{Q} \; \forall \; i$) return $\emptyset$ if $\sum_j \lambda_{ij} = 0 \; \forall \; i$, else return 1 as the basis and $\frac{\sum_j \lambda_{ij}}{\sum_{j,k} \mu_{ijk}}$ as coordinates for t_i with respect to the basis $\{1\}$. For this step we use the procedure 1 on c_i and 0 for $i = 1, ..., d$.

vi. Else, if $C \neq \{0\}$, we take a basis $\{c_1, ..., c_d\}$ of C together with coordinates by recalling this procedure on it (terms in C are on a lower level of exponentiation).

vii. Now we have the writing of each a_{ij} and b_{ijk} with respect to the basis:

$$a_{ij} = \sum_{f=1}^{d} \alpha_{ij,f} \cdot c_f \qquad b_{ijk} = \sum_{f=1}^{d} \beta_{ijk,f} \cdot c_f$$

where $\forall \; i, j, k, f \; \alpha_{ij,f}, \beta_{ijk,f} \in \mathbb{Q}$;

viii. We write each $\alpha_{ij,f}$ and each $\beta_{ijk,f}$ as a fraction in lowest terms, respectively $\frac{n_{ij,f}}{d_{ij,f}}$ and $\frac{n_{ijk,f}}{d_{ijk,f}}$. Let $Y = \{\frac{n_1}{d_1}, ..., \frac{n_h}{d_h}\}$ be the set of these fractions and we take, for each $f = 1, ..., d$, d_f as the least common multiple among the d_i regarding c_f.

ix. For all $i = 1, ..., n$ and for all $j = 1, ..., k_i$ we write

$$E(a_{ij}) = \prod_{k=1}^{d} \left(E\left(\frac{c_k}{d_k}\right)\right)^{n_{ij,k} \cdot \frac{d_f}{d_{ij,k}}}$$

and

$$E(b_{ijk}) = \prod_{m=1}^{d} \left(E\left(\frac{c_m}{d_m}\right)\right)^{n_{ijk,m} \cdot \frac{d_f}{d_{ijk,m}}} ;$$

x. For each $i = 1, ..., d$ we associate to $E(\frac{c_i}{d_i})$ an indeterminate and so we write each t_i as a member of $\mathbb{Q}(x_1, ..., x_d)$.

xi. We use the procedure 3 for taking a minimal subset of generators with the respective coordinates and then we return the correspondent subset of terms with the same coordinates.

PROCEDURE 3: POLYNOMIALS BASIS

Input: List of fractions of rational polynomials well defined (i.e. the denominators are not 0) $f_1 = \frac{p_1}{q_1}, ..., f_n = \frac{p_n}{q_n}$ in d variables $x_1, ..., x_d$;

Output: A minimal generating sublist and coordinates for each f_i with respect to this list.

i. We multiply each f_i for the product of the q_is:

$$g_i = f_i \cdot \prod_{i=1}^{n} q_i \, .$$

ii. The g_is are polynomials, so we can write them as vectors and extract a minimal subset of generators $\{g_{i_1}, ..., g_{i_k}\}$ and the respective coordinates for each g_i with respect to this subset.

iii. We return the subset $\{f_{i_1}, ..., f_{i_k}\}$ and the same coordinates of the previous step.

Proposition 4.2. *Procedure 3 is correct.*

Proof

We supposed that the input fractions are well defined, i.e. $q_i \neq 0 \ \forall \ i = 1, ..., n$, so the product $P := \prod_{i=1}^{n} q_i$ is $\neq 0$ as well. Then, given a subset of $\{g_{i_j}\}_{j=1,...,k}$ it is linearly independent if and only if the set $\{f_{i_j}\}_{j=1,...,k}$ is linearly independent. In fact, if we take a rational linear combination of the g_{i_j}s we have:

$$\begin{aligned} & c_1 g_{i_1} + ... + c_k g_{i_k} \\ = \ & c_1 f_{i_1} P + ..., c_k f_{i_k} P \\ = \ & P \cdot (c_1 f_{i_1} + ..., c_k f_{i_k}) \end{aligned}$$

and, since $P \neq 0$, we have:

$$c_1 g_{i_1} + ... + c_k g_{i_k} = 0 \iff c_1 f_{i_1} + ..., c_k f_{i_k} = 0 \, .$$

The coordinates for the g_is with respect to the subset $\{g_{i_j}\}_{j=1,...,k}$ are the same coordinates of the f_is with respect to the subset $\{f_{i_j}\}_{j=1,...,k}$. In fact, if $g_j = c_{j,1} g_{i_1} + ... + c_{j,k} g_{i_k}$ then we have:

$$\begin{aligned} P \cdot f_j \ = \ g_j \ &= \ c_{j,1} g_{i_1} + ... + c_{j,k} g_{i_k} \\ &= \ c_{j,1} f_{i_1} P + ... + c_{j,k} f_{i_k} P \\ &= \ P \cdot (c_{j,1} f_{i_1} + ... + c_{j,k} f_{i_k}) \end{aligned}$$

and so, since $P \neq 0$, $f_j = c_{j,1} f_{i_1} + ... + c_{j,k} f_{i_k}$.

□

Proposition 4.3. *Procedure 2 is correct.*

Proof

Let k be the level of $t_1, ..., t_n$. We proceed by induction on k.

- $k = 0$: in this case $\forall i = 1, ..., n \ t_i \in \mathbb{Q}$. The procedure enters the step i. If one of the p_is is 0 then the call of the procedure with input p_i returns $\emptyset$ thanks to step v. and so, by step i., the result is "error". If $\forall \ i = 1, ..., n \ p_i \neq 0$ then, the call of the procedure with input p_i returns 1 by step v. and so the procedure continues. Note that from now we are looking at the procedure with input p_i.

We arrive to step v. with $C = \{0\}$. If $\forall\ i = 1, ..., n\ t_i = 0$, then $\forall\ i = 1, ..., n\ \sum_j \lambda_{ij} = 0$ and the procedure returns $\emptyset$, else it returns 1 that is a $\mathbb{Q}$-basis for t_is. So for $k = 0$ the procedure works.

- $k \implies k+1$: The procedure enters the step i. and it calls itself with input p_i. Each p_i has as denominators 1 because it is an exponential polynomial with coefficients in $\mathbb{Z}$ and so the subprocedure continue.

  Steps ii. and iii. works by inductive hypothesis because a_{ij}s and b_{ijk}s are on a lower level (they are exponents).

  Step iv. is simply a union.

  Step v. works by inductive hypothesis. If p_i is a constant then $C = \{0\}$ and, if $p_i = 0$, the procedure returns $\emptyset$, so we return to step i. and the main procedure returns "error". If $p_i \neq 0$ the procedure returns 1 and the coordinates for p_i and the main procedure continues.

  If p_i isn't constant, then $C \neq \{0\}$ and step vi. works by inductive hypothesis.

  Now that we have a basis we recall the fact that $\langle\emptyset\rangle^E$ satisfies Schanuel's Condition and so the set $\left\{E\left(\frac{c_k}{d_k}\right) : k = 1, ..., d\right\}$ is algebraically independent and so it doesn't satisfies any polynomial equation. Then we can treat these elements as indeterminates and we conclude by the correctness of procedure 2.

  Lastly, after we have checked that each p_{ij} is $\neq 0$, we return to step i. and we proceed with the main procedure in the same way.

□

Proposition 4.4. *Procedure 1 is correct.*

Proof

By the correctness of procedure 2 the step ii. returns "error" if there exists an index i such that $p_i = 0$. Otherwise the terms are well defined and we proceed with step iii. Again, by procedure 2, procedure 1 returns "true" if $t = 0$, i.e. if $x = y$ and false otherwise.

□

So we can conclude this work with this result:

Theorem 4.5. *The word problem for* $\langle \emptyset \rangle^E$ *is decidable.*

Proof

It follows directly from the correctness of procedures 1, 2 and 3.

□

Bibliography

[1] S. Burris and H.P. Sankappanavar. *A Course in Universal Algebra*. Graduate Texts in Mathematics. Springer New York, 2011. ISBN: 9781461381327.

[2] Tsit-Yuen Lam. *Lectures on Modules and Rings*. Graduate Texts in Mathematics. Springer-Verlag New York, 1999. ISBN: 978-1-4612-0525-8.

[3] Angus Macintyre. "Schanuel's conjecture and free exponential rings". In: *Annals of Pure and Applied Logic* 51.3 (1991), pp. 241–246. ISSN: 0168-0072. DOI: https://doi.org/10.1016/0168-0072(91)90017-G.

[4] Angus Macintyre and Alex J. Wilkie. "On the Decidability of the Real Exponential Field". In: *Kreiseliana. About and Around Georg Kreisel*. Ed. by Piergiorgio Odifreddi. A K Peters, 1996, pp. 441–467.

[5] P. S. Novikov. "Algorithmic Unsolvability of the Word Problem in Group Theory". In: *Journal of Symbolic Logic* 23.1 (1958), pp. 50–52. DOI: 10.2307/2964487.