Universidade Federal de Pernambuco
Centro de Ciências Exatas e da Natureza
Programa de Pós-Graduação em Matemática
Curso de Doutorado em Matemática

A Class of QFA Rings

por

Eudes Naziazeno Galvao

sob orientação do

Prof. Dr. Ruy de Queiroz

e co-orientação do

Prof. Ph.D. Thomas Scanlon

Tese apresentada ao Corpo Docente do Programa de Pós-Graduação em Matemática - CCEN - UFPE, como requisito parcial para obtenção do título de Doutor em Matemática.

Recife - PE
Fevereiro/2011

Catalogação na fonte
Bibliotecária Jane Souto Maior, CRB4-571

Galvão, Eudes Naziazeno
A class of QFA rings / Eudes Naziazeno - Recife: O Autor, 2011.
45 folhas.

Orientador: Ruy de Queiroz.
Tese (doutorado) Universidade Federal de Pernambuco. CCEN. Matemática, 2011.

Inclui bibliografia e apêndice.

1. Lógica matemática. 2. Teoria de modelos. 3. Lógica de primeira ordem. 4. Anéis QFA. I. Queiroz, Ruy de (orientador). II. Título.

511.3 CDD (22. ed.) MEI2011 – 065

Tese submetida ao Corpo Docente do Programa de Pós-graduação do Departamento de Matemática da Universidade Federal de Pernambuco como parte dos requisitos necessários para a obtenção do Grau de Doutorado em Matemática.

Aprovado: ______________________________

Thomas Scanlon, UC-Berkeley

Co-Orientador

____

Francisco Miraglia Neto, USP

Andre Luiz Meireles Araujo

____

André Luiz Meireles Araujo, UFPE

____

Maurício Ayala-Rincon, UnB

____

Marcelo Esteban Coniglio, UNICAMP

SOBRE UMA CLASSE DE ANÉIS QFA

Por

Eudes Naziazeno Galvão

UNIVERSIDADE FEDERAL DE PERNAMBUCO
CENTRO DE CIÊNCIAS EXATAS E DA NATUREZA
DEPARTAMENTO DE MATEMÁTICA
Cidade Universitária – Tels. (081) 2126.8415– Fax: (081) 2126.8410
RECIFE – BRASIL
Fevereiro – 2011

Sumário

Abstract

In this work, we prove that any infinite finitely generated integral domain is bi-interpretable with the structure of the natural numbers. Using this argument, we demonstrate that any infinite f.g. ring R which has nilpotent prime I such that R/I is an integral domain is Quasi-Finitely Axiomatizable (QFA).

Keywords: 1. Mathematical Logic. 2. Model Theory.
3. First Order Logic. 4. QFA Rings.

Resumo

Nesta tese, provamos que todo domínio infinito finitamente gerado é bi-interpretável com a estrutura dos números naturais. Usando este argumento, demonstramos que todo anel f.g. R que tem um ideal primo nilpotente I tal que R/I é um domínio é Quase-Finitamente Axiomatizável.

Palavras-chave: 1. Lógica Matemática. 2. Teoria de Modelos. 3. Lógica de Primeira Ordem. 4. Anéis QFA.

Capítulo 1

Preliminaries

Model Theory is the part of Mathematical Logic that deals with definability of mathematical objects. In other words, Model Theory classifies structures, functions and sets using logical formulae. For example, we may try to characterize a structure seeing which logical formulae are true in it and, on the other hand, we may look at a set of formulae and ask about whether there is a *model* of it, by some existential theorem or by construction of such one. We intend to introduce in this chapter basic definitions and results in Model Theory, likewise some useful results in algebra, in order to fully understand this work. The reader who is familiar with these concepts may skip this chapter. However, even for the reader that has never read anything about model theory we recommend to review a litte bit of ZFC, the axiomatization of Set Theory of Zermelo-Fraenkel with the Axiom of Choice.

1.1 First Order Logic

In this section, our intention is to present the basic definitions of first order logic: structures, signatures, models, terms, formulae, sentences, theories, homomorphisms, definable sets (for more details about it, see Hodges [Ho]). Then, we start with the definition of *structure*.

Definition 1.1.1 *We may define structure with few words saying that it is a mathematical object that consists of a set equiped with some logical symbols. Formally, a structure A have the following objects:*

1*)* **Domain of** A**.** *A set dom*(A)*, which is called domain of* A*. The el-*

ements in dom(A) are called the elements of the structure A. The cardinality of A, say $|A|$, is the cardinality of the set dom(A).

2*)* **Constants.** *Special elements in dom(A). We call them "constants." Each constant is named by one or more constant symbols. If c is a constant symbol, then we write c^A to denote the constant that is named by c in A.*

3*)* **Relations.** *For each natural number n, a set of n-ary relations over dom(A). Each relation is named by one or more relation symbols. If R is a constant symbol, then we write R^A to denote the relation that is named by R in A.*

4*)* **Functions.** *For each natural number n, a set of n-ary functions over dom(A). Each function is named by one or more function symbols. If F is a constant symbol, then we write F^A to denote the relation that is named by F in A.*

Note: Each set in 1), 2) or 3) above may be empty, and all structure is supposed to have "=" for equality of elements.

Definition 1.1.2 *The signature of a structure is just the union of the sets of constant symbols, relation symbols and function symbols of a structure A. If dom(A)=B and the signature of A is $L = \{C_1, \ldots, C_r, R_1, \ldots, R_s, F_1, \ldots, F_t\}$, then we write A as $(B, C_1, \ldots, C_r, R_1, \ldots, R_s, F_1, \ldots, F_t)$ and say that A is an L-structure.*

Example 1.1.1 (Graphs) *Let G a simple graph whose vertex set is V and edges set is E. How could we see G as a structure in the sense above? One way is to consider G as a structure such that dom$(G) = V$ and E is a binary relation symbol such that*

$$E^G(x, y) \Longleftrightarrow (x, y) \textit{ is an edge of } G.$$

Using the notation, we write structure G as $G = (V, E)$.

Example 1.1.2 (Rings) *Consider a ring R with unit. Then, we may see R as $(R, 0, 1, +\times)$, for which 0 is the constant symbol that names zero, 1 is* *the constant symbol that names the identity of R, $+$ is the function symbol for the sum in R, and finally $\times$ is the function symbol for the multiplication in R.*

Now we are going to introduce the definition of *homomorphism* of L-structures. Let A, B be L-structures. Then

Definition 1.1.3 *A homomorphism "$f : A \longrightarrow B$" is a function $f : dom(A) \longrightarrow dom(B)$ such that*

(1) For each constant symbol c of L, $f(c^A) = c^B$.

(2) For each $n > 0$, an n-ary relation symbol R of L, and an n-tuple $(a_1, \ldots, a_n)$ of $dom(A)$, then

$$(a_1, \ldots, a_n) \in R^A \Rightarrow (f(a_1), \ldots, f(a_n)) \in R^B. \tag{1.1.1}$$

(3) For each $n > 0$, an n-ary function symbol F of L, and an n-tuple $(a_1, \ldots, a_n)$ of $dom(A)$, then $f(F^A(a_1, \ldots, a_n)) = F^B(f(a_1), \ldots, f(a_n))$.

If a homomorphism $f : A \longrightarrow B$ is injective and we have "$\Leftrightarrow$" in (1.1.1) above, then we call it an **embedding**. Finally, a homomorphism $f : A \longrightarrow B$ is an **isomorphism** if it is a surjective embedding.

Aside from all these symbols, we may want to combine them with variables $x, y, s, t, \ldots$ to build more symbols. Then, we introduce the notion of *term* and *atomic formula*.

Definition 1.1.4 (Term) *We define term by induction:*
(a)Every variable is a term of L. (b) Every constant is a term of L. (c) If F is an n-ary function symbol, for some $n > 0$, and $t_1, \ldots, t_n$ are terms, then $F(t_1, \ldots, t_n)$ is a term of L.

Example 1.1.3 *y, 1, $\times(y, +(y, 1))$, and $\times(x, y)$ are terms of $L = \{0, 1, +, \times\}$. We will use "$x + y$" to say $+(x, y)$ and "$x \times y$" to say $\times(x, y)$*

Definition 1.1.5 (Atomic Formula) *We also define atomic formula by induction:*
(a) If s and t are terms of L, them $s = t$ is an atomic formula of L. (b) If R is an n-ary relation symbol, for some $n > 0$, and $t_1, \ldots, t_n$ are terms, then $R(t_1, \ldots, t_n)$ is an atomic formula of L. An atomic formula is called an **atomic sentence** *if it does not have variables on its composition.*

Example 1.1.4 *$y < 0$, $1+1=0$, and $y \times 1 < y$ are atomic formulae of $L = \{0,1,+,\times,<\}$.*

Finally, we introduce the *logic symbols*: $\neg$ (not), $\wedge$ (and), $\vee$ (or), $\forall$ (for all element...), $\exists$ (there is an element...) to contruct more sophisticated expressions. Now we are ready to define the class of formulae of a signature L, and then the first-order logic of L.

Definition 1.1.6 *The class of formulae of a signature L is the smallest class X such that:*
All atomic formulae of L are in X. If $\phi \in X$, then $\neg\phi \in X$ ($\neg\phi$ means "ϕ is false"). If $\Phi \subseteq X$, then $\bigvee \Phi$ and $\bigwedge \Phi$ are in X ($\bigvee \Phi$ means "at least one formula in Φ is true", and $\bigwedge \Phi$ means "all the formulae in Φ are true"). If $\phi \in X$ and x is a variable, then $\forall x\ \phi$ and $\exists x\ \phi$ are in X ($\forall x\ \phi$ means "ϕ is true for all x," and $\exists x\ \phi$ means "there is x such that ϕ is true").

Definition 1.1.7 (First-order Logic of L) *The First-order Logic of L is the subset of the class of formulae of L consisting of formulae that use a finite number of symbols of L and/or the logic symbols.*

Example 1.1.5 *Consider $L = \{0,1,+\times\}$ with the following list of axioms*

1) $\forall x,y,z\ (x+y)+z = x+(y+z),\ \ \forall x\ x+0 = x,\ \ \forall x,y\ x+y = y+x.$
2) $\forall x,y,z\ (x\times y)\times z = x\times(y\times z),\ \ \forall x\ x\times 1 = x,\ \ \forall x\ 1\times x = x.$
3) $\forall x,y,z\ x\times(y+z) = x\times y + x\times z,\ \ \forall x,y,z\ (x+y)\times z = x\times z + y\times z,$

Then the **first-order language of the rings**, *$\mathcal{L}_{ring}$, is the set of all finite formulas of such L equiped with this list of axioms.*

Let A be an L-structure and ϕ a formula of L. We say that A *is a model of* ϕ if ϕ is true in A. When this happens, we use the notation $A \models \phi$. A *theory* in L is a set of sentences of L. If a structure A is a model for all the sentences in a theory T, then we also use the notation $A \models T$ to say this. The *theory of an L- structure A*, Th(A), is the set of all sentences in the first-order logic of L that are true in A. Starting from this point, everytime we say "formula" we mean "first-order formula", "sentence" will mean "first-order sentence," and so on. We end this section with one of the most important definitions in model theory.

Definition 1.1.8 (Definable sets) *Let A be an L-structure and $B \subseteq dom(A)$. We say that B is definable if there is a formula $\varphi(x)$ such that*

$$x \in B \Longleftrightarrow \varphi(x)$$

A homomorphism $f : A \longrightarrow A$ is called **definable** if $\text{graph}(f) := \{(a, b) \, ; \, f(a) = b\}$ is definable. An element a of a structure A is definable if $\{a\}$ is definable.

Example 1.1.6 *Consider the structure of the natural numbers $(\mathbb{N}, 0, 1, +, \times)$. The set $S = \{$sums of the first n nonzero natural numbers$\}$ is definable. Indeed, since we know that $\sum_{i=1}^{n} i = \frac{n(n+1)}{2}$, then we define S by the formula $c \in S \Leftrightarrow \exists n \; 2c = n(n + 1)$.*

1.2 Interpretations

Now, we introduce the concept of interpretation and bi-interpretation of structures. Let K and L be signatures, A a K-structure, B an L-structure, and $n > 0$ an integer.

Definition 1.2.1 (Interpretation) *One n-dimentional interpretation Γ of B in A is defined by three ingredients:*

(1) One formula $\partial_\Gamma(x_0, \ldots, x_n)$. (this will specify the domain of the interpretation)

(2) For each formula $\phi(x_0, \ldots, x_n)$ in L of the form $x = y$, $c = y$, $F(x_0, \ldots, x_n) = y$, or $R(x_0, \ldots, x_n)$, for which $x, y, x_0, \ldots, x_n$ are variables, c is a constant symbol, F is a n-ary function symbol, and R is a n-ary relation symbol, we have a formula $\phi_\Gamma(\overline{x_0}, \ldots, \overline{x_n})$ of K, for which $\overline{x_i} := (x_i, 1, \ldots, x_i, n)$ for each i.

(3) A surjective function $f_\Gamma : \partial_\Gamma(A^n) \longrightarrow dom(B)$ such that for each formula ϕ in (2) and for all $\overline{a_i} \in \partial_\Gamma(A^n)$ we have that

$$B \models \phi(f_\Gamma\overline{a_0}, \ldots, f_\Gamma\overline{a_n}) \Longleftrightarrow A \models \phi_\Gamma(\overline{a_0}, \ldots, \overline{a_n})$$

for which $f_\Gamma\overline{a_i} := (f_\Gamma(a_{i,1}), \ldots, f_\Gamma(a_{i,n}))$ for each i.

This definition, seems to be complicated. Putting on simple terms, B is interpretable in A if we can define formulae to translate operations in B to operations in some power of A. We construct now an interpretation of the rational on the integrers.

Example 1.2.1 *For those who know basic commutative algebra, $\mathbb{Q}$ is the localization of $\mathbb{Z} \setminus \{0\}$ in $\mathbb{Z}$. For our intentions, we say that $\mathbb{Q}$ is formed by elements a/b such that $b \neq 0$ together with the operations $a/b + c/d = (ad+bc)/(cd)$ and $a/b \times c/d = (a \times c)/(c \times d)$. Since we are in $(\mathbb{Z}, 0, 1, +, \times)$, we need to find some "equivalent" formulae for these formulae in some power of $\mathbb{Z}$. Indeed, consider the formulae over $\mathbb{Z} \times \mathbb{Z}$:*

$$\partial_\Gamma(x_1, x_2) \iff \neg x_2 = 0$$

$$\iota_\Gamma(x_1, x_2, y_1, y_2) \iff \partial_\Gamma(x_1, x_2) \wedge \partial_\Gamma(y_1, y_2) \wedge x_1.y_2 = x_2.y_1$$

$$\alpha_\Gamma(x_1, x_2, y_1, y_2, z_1, z_2) \iff \iota_\Gamma(x_1.y_2 + x_2.y_1, x_2.y_2, z_1, z_2)$$

$$\mu_\Gamma(x_1, x_2, y_1, y_2, z_1, z_2) \iff \iota_\Gamma(x_1.y_1, x_2.y_2, z_1, z_2)$$

and

$$f : \partial_\Gamma(\mathbb{Z}^2) \longrightarrow \mathbb{Q}$$
$$(x_1, x_2) \mapsto \frac{x_1}{x_2}$$

Note that ι_Γ expresses equality in $\mathbb{Q}$, α_Γ expresses the graph of the addition function, and μ_Γ expresses the graph of the multiplication function. That is

$$a/b = c/d \text{ in } \mathbb{Q} \iff \iota_\Gamma(a, b, c, d) \text{ in } \mathbb{Z}$$

$$a/b + c/d = e/f \text{ in } \mathbb{Q} \iff \alpha_\Gamma(a, b, c, d, e, f) \text{ in } \mathbb{Z}$$

$$a/b \times c/d = e/f \text{ in } \mathbb{Q} \iff \mu_\Gamma(a, b, c, d, e, f) \text{ in } \mathbb{Z}$$

Thus, Γ is a bidimensional interpretation of $\mathbb{Q}$ in $\mathbb{Z}$.

Interpretations are very useful, for we can express sentences about other structures through them. We now show that we can interpret the localization of a multiplicative set S of a commutative ring R, and then we prove that we can interpret finite degree extentions of the field of fractions of some ring in such ring. Then, we present an example: one interpretation of $(\mathbb{Q}(\sqrt{2}), +, \times)$ in $(\mathbb{Z}, +, \times)$.

Lemma 1.2.1 *There are formulae $E(x_1, x_2, y_1, y_2)$, $A(x_1, x_2, y_1, y_2, z_1, z_2)$, and $M(x_1, x_2, y_1, y_2, z_1, z_2)$ so that for any commutative ring R and multiplicative set $S \subseteq R$, if S is definable by the formula $F(x)$, then the localization $S^{-1}R$ is interpretable in R as $\{(x, y) \in R^2; S(y)\}/E$, and the graph of addition is the image of A under E and of multiplication is M under E.*

Proof: Define

$$E(x_1, x_2, y_1, y_2) \Leftrightarrow \exists t\ F(t) \wedge F(x_2) \wedge F(y_2) \wedge (t.(x_1.y_2 - x_2.y_1) = 0)$$

$$A(x_1, x_2, y_1, y_2, z_1, z_2) \Leftrightarrow E(x_1.y_2 + x_2.y_1, x_2.y_2, z_1, z_2)$$

$$M(x_1, x_2, y_1, y_2, z_1, z_2) \Leftrightarrow E(x_1.y_1, x_2.y_2, z_1, z_2)$$

Then, if we define

$$(x_1, x_2) \sim_\Gamma (y_1, y_2) \Leftrightarrow E(x_1, x_2, y_1, y_2)$$

$$X = (x_1, x_2),\ Y = (y_1, y_2),\ Z = (z_1, z_2)$$

$$X \oplus_\Gamma Y = Z \Leftrightarrow A(X, Y, Z)$$

$$X \otimes_\Gamma Y = Z \Leftrightarrow M(X, Y, Z)$$

As we did in the Example (1.2.1), we use the same arguments to ensure that Γ is an interpretation of R_S in R, that is, $(R^2/\sim, \overline{0}, \overline{1}, \oplus_S, \otimes_S) \simeq (R_S, 0, 1, +, \times)$ □

Corollarium 1.2.1 *There is a uniform interpretation of the field of fractions of R, say* Frac(R)*, across the class of integral domains R.*

Proof: Set $F(x) \Leftrightarrow \neg\ x = 0$ and apply the lemma for $S = \{x;\ F(x)\}$. ■

Lemma 1.2.2 *For any fixed positive integer d, there is a formula E_d (in d^3 variables indexed as $a = (a_{i,j,k})$) and formulae $A_d(x_1..., x_d, y_1...y_d, z_1...z_d; a)$ and $M_d(x, y, x; a)$ so that for each a if $E_d(a)$ holds, then $A_d(x, y, z; a)$ defines the graph of a binary operation $+_a$ on R^d and $M(x, y, z; a)$ defines the graph of a binary operation $\times_a$ on R^d so that identifying R with $R \times (0, ..., 0)$, the structure $(R^d, +_a, \times_a)$ is an integral domain extending R. Moreover, every such integral domain which is free of rank d over R is encoded by some a satisfying $E_d(a)$.*

Proof: Suppose that R' is a degree-d extension of a ring R generated by the basis $\{e_1, \cdots, e_d\}$. Then, to understand how is the multiplication in R' we see what happens in its generators. Indeed, we have for $i, j \in \{1, \cdots, d\}$ the equality

$$e_i.e_j = a_{i,j,1}e_1 + a_{i,j,2}e_2 + \cdots + a_{i,j,d}e_d \ ,$$

for which $a_{i,j,k} \in R$ is the coefficient of $e_i.e_j$ related to e_k. Since R' is commutative, then $\forall i, j, k \ \ a_{i,j,k} = a_{j,i,k}$. The relations among $e_1, \cdots, e_d$ will uniquely determine these $a_{i,j,k}$. Therefore, we may suppose that we know all the d^3-matrix $a = (a_{i,j,k})$. With this matrix in hand, define

$$A_d(x_1, ..., x_d, y_1, ..., y_d, z_1, ..., z_d; a) \Leftrightarrow \bigwedge_{i=1}^{d} x_i + y_i = z_i$$

$$M_d(x_1, ..., x_d, y_1, ..., y_d, z_1, ..., z_d; a)$$

$$\Updownarrow$$

$$\bigwedge_{l=1}^{d} \sum_{j=1}^{d} \sum_{i=1}^{d} x_j \times (y_i \times a_{j,i,l}) = z_l$$

Finally, considering $X := (x_1, ..., x_d)$, $Y := (y_1, ..., y_d)$, and $Z := (z_1, ..., z_d)$, we abbreviate these formulas to

$$X \oplus_d Y = Z \ \Leftrightarrow A_d(X, Y, Z; a)$$

$$X \otimes_d Y = Z \ \Leftrightarrow M_d(X, Y, Z; a)$$

Then, we define $E_d(a)$ by

$$\begin{cases} \forall A, B, C, X, Y, Z \ \big(Y \otimes_a Z = A \ \wedge X \otimes_d A = B \ \wedge X \otimes_d Y = C\big) \Rightarrow C \otimes_d Z = B \\ \forall A, B \ \big(A \otimes_d B = 0\big) \Rightarrow A = 0 \vee B = 0 \\ \forall A, B \ A \otimes_d B = B \otimes_d A \end{cases}$$

(Note: We did not add the distributive property of $\otimes_d$ over $\oplus_d$, because they follow from the definition.). Then, if $a = (a_{i,j,k})$ is such that $E_d(a)$, it follows that $(R^{d^2}, \oplus_d, \otimes_d)$ is a degree-d extension of R which is an integral domain. In order to see R as a subring, of this degree-d extension, isomorphic to $R \times (0, \cdots, 0)$, we add the formula

$$\forall i, j, k \ (j \neq k \Rightarrow a_{1,j,k} = 0) \wedge (j = k \Rightarrow a_{1,j,k} = 1)$$

to $E_d(a)$. So, with these definitions, we have that $(R^{d^2}, \oplus_d, \otimes_d)$ is a degree-d extension of R such that R is viewed as $R \times (0, \cdots, 0)$. $\square$

Example 1.2.2 *Suppose we are in* $(\mathbb{Z}, 0, 1, +, \times)$ *and want to express the sentence "there is an* x *in* $\mathbb{Q}[\sqrt{2}]$ *such that* $x^2 - 2 = 0$*."Then, we first see the elements of* $\mathbb{Q}[\sqrt{2}]$ *as elements of* $\mathbb{Z}^4$ *with the operations*

$$\left(\frac{x_{1,1}}{x_{2,1}} + \frac{x_{1,2}}{x_{2,2}}\sqrt{2}\right) \oplus \left(\frac{y_{1,1}}{y_{2,1}} + \frac{y_{1,2}}{y_{2,2}}\sqrt{2}\right) = \left(\frac{z_{1,1}}{z_{2,1}} + \frac{z_{1,2}}{z_{2,2}}\sqrt{2}\right)$$

defined by

$$\frac{z_{1,1}}{z_{2,1}} = \frac{x_{1,1}}{x_{2,1}}+\frac{y_{1,1}}{y_{2,1}} := \frac{x_{1,1}\cdot y_{2,1} + x_{2,1}\cdot y_{1,1}}{x_{2,1}\cdot y_{2,1}} \;\;\&\;\; \frac{z_{1,2}}{z_{2,2}} = \frac{x_{1,2}}{x_{2,2}}+\frac{y_{1,2}}{y_{2,2}} := \frac{x_{1,2}\cdot y_{2,2} + x_{2,2}\cdot y_{1,2}}{x_{2,2}\cdot y_{2,2}}$$

and

$$\left(\frac{x_{1,1}}{x_{2,1}} + \frac{x_{1,2}}{x_{2,2}}\sqrt{2}\right) \otimes \left(\frac{y_{1,1}}{y_{2,1}} + \frac{y_{1,2}}{y_{2,2}}\sqrt{2}\right) = \left(\frac{z_{1,1}}{z_{2,1}} + \frac{z_{1,2}}{z_{2,2}}\sqrt{2}\right)$$

defined by

$$\frac{z_{1,1}}{z_{2,1}} = \frac{x_{1,1}\cdot y_{1,1}.x_{2,2}\cdot y_{2,2} + 2.x_{1,2}\cdot y_{1,2}.x_{2,1}\cdot y_{2,1}}{x_{2,1}\cdot y_{2,1}.x_{2,2}\cdot y_{2,2}} \;\;\&\;\; \frac{z_{1,2}}{z_{2,2}} = \frac{x_{1,1}\cdot y_{1,2}.x_{2,2}\cdot y_{2,1} + .x_{1,2}\cdot y_{1,1}.x_{2,1}\cdot y_{2,2}}{x_{2,1}\cdot y_{2,2}.x_{2,2}\cdot y_{2,1}}$$

or equivalently

$$\left(\frac{x_{1,1}}{x_{2,1}} + \frac{x_{1,2}}{x_{2,2}}\sqrt{2}\right)\otimes\left(\frac{y_{1,1}}{y_{2,1}} + \frac{y_{1,2}}{y_{2,2}}\sqrt{2}\right) := \left(\frac{x_{1,1}\cdot y_{1,1}}{x_{2,1}\cdot y_{2,1}} + \frac{x_{1,1}\cdot y_{1,2}}{x_{1,2}\cdot y_{2,2}}\sqrt{2}\right)\oplus\left(\frac{2.x_{1,2}\cdot y_{1,2}}{x_{2,2}\cdot y_{2,2}} + \frac{x_{1,2}\cdot y_{1,1}}{x_{2,2}\cdot y_{2,1}}\sqrt{2}\right)$$

Therefore, we can define

$$\iota((x_{1,1}, x_{2,1}, x_{1,2}, x_{2,2}), (y_{1,1}, y_{2,1}, y_{1,2}, y_{2,2}))$$

$$\Updownarrow$$

$$(\neg\; x_{2,1}.x_{2,2}\cdot y_{2,1}\cdot y_{2,2} = 0) \wedge (x_{1,1}\cdot y_{2,1} = x_{2,1}\cdot y_{1,1}) \wedge (x_{1,2}\cdot y_{2,2} = x_{2,2}\cdot y_{1,2})$$

(we will use this "ι" to talk about equalities of members of $\mathbb{Q}[\sqrt{2}]$*), and*

$$\alpha((x_{1,1}, x_{2,1}, x_{1,2}, x_{2,2}), (y_{1,1}, y_{2,1}, y_{1,2}, y_{2,2}), (z_{1,1}, z_{2,1}, z_{1,2}, z_{2,2}))$$

$$\Updownarrow$$

$$\iota((x_{1,1}\cdot y_{2,1}+x_{2,1}\cdot y_{1,1}, x_{2,1}\cdot y_{2,1}, x_{1,2}\cdot y_{2,2}+x_{2,2}\cdot y_{1,2}, x_{2,2}.x_{2,2}), (z_{1,1}, z_{2,1}, z_{1,2}, z_{2,2}))$$

(we use "'α" as the definition of sum in $\mathbb{Q}[\sqrt{2}]$*), and, finally,*

$$\mu((x_{1,1}, x_{2,1}, x_{1,2}, x_{2,2}), (y_{1,1}, y_{2,1}, y_{1,2}, y_{2,2}), (z_{1,1}, z_{2,1}, z_{1,2}, z_{2,2}))$$

$$\Updownarrow$$

$$\alpha((x_{1,1}.y_{1,1}, x_{2,1}.y_{2,1}, x_{1,1}.y_{1,2}, x_{2,1}.y_{2,2}), (2.x_{1,2}.y_{1,2}, x_{2,2}.y_{2,2}, x_{1,2}.y_{1,1}, x_{2,2}.y_{2,1}), (z_{1,1}, z_{2,1}, z_{1,2}, z_{2,2}))$$

(to talk about multiplication).Therefore, to say "there is an x in $\mathbb{Q}[\sqrt{2}]$ such that $x^2 - 2 = 0$"we use the translation

$$\exists x_{1,1}, x_{2,1}, x_{1,2}, x_{2,2} \quad \mu((x_{1,1}, x_{2,1}, x_{1,2}, x_{2,2}), (x_{1,1}, x_{2,1}, x_{1,2}, x_{2,2}), (2, 1, 0, 0))$$

Moreover, we can abbreviate these sentences, by using $X = (x_{1,1}, x_{2,1}, x_{1,2}, x_{2,2})$, $Y = (y_{1,1}, y_{2,1}, y_{1,2}, y_{2,2})$ and $Z = (z_{1,1}, z_{2,1}, z_{1,2}, z_{2,2})$ and defining $X \oplus Y = Z \Leftrightarrow \alpha(X, Y, Z)$ and $X \otimes Y = Z \Leftrightarrow \mu(X, Y, Z)$. So, the translation of some sentence about $(\mathbb{Q}(\sqrt{2}), 0, 1, +, \times)$ is just changing 0 by $(0, 1)$, 1 by $(1, 1)$, the variables by "their capital letters", and "+" and "×" by "⊕" and "⊗". □

We end this section with the notion of bi-interpretation.

Definition 1.2.2 (Bi-interpretation) *Let K and L be signatures, A a K-structure, and B an L-structure. We say that A is bi-interpretable with B if there is an interpretation Γ_A of A in B and there is an interpretation Γ_B of B in A such that the composition of Γ_A and Γ_B is definable in B and the composition of Γ_B and Γ_A is definable in A.*

For counterexamples of bi-interpretability, we assert that $\mathbb{Z}[\varepsilon]/(\varepsilon^2)$ is not bi-interpretable with $\mathbb{Z}$. The Appendix contains a proof of this fact. Now, we go to next section that says that if we add a definable symbol to the language, then we essentially do not change the class of definable sets.

1.3 Definitional Expansions

Definition 1.3.1 *Let L and L' be signaturess such that $L \subseteq L'$, and T' a theory in L'. For an n-ary relation symbol R of L', we say that a formula φ of L is an* **explicit definition** *of R relative to T' if T' proves*

$$\forall x_1, \cdots, x_n \;\; R(x_1, \cdots, x_n) \longleftrightarrow \varphi(x_1, \cdots, x_n)$$

Analogously, if c is a constant and F is a n-ary function symbol, then their explicit definitions in L would be formulae ϕ and ψ (respectively) of L such that T' proves

$$\forall x \;\; c = x \longleftrightarrow \phi(x)$$

$$\forall x_1, \cdots, x_n, y \;\; F(x_1, \cdots, x_n) = y \longleftrightarrow \psi(x_1, \cdots, x_n, y)$$

Definitional expansions are used in most cases to avoid writing extremely long sentences when we have this possibility of abbreviation. For example, in $T' = Th(\mathbb{Z}, 0, 1, +, \times)$ we can use "$x < y$" to say $\exists n_1, n_2, n_3, n_4 \;\; y = x + n_1^2 + n_2^2 + n_3^2 + n_4^2 + 1$. The following results about definitional expansions have simple proofs (they are the theorems 2.6.3 and 2.6.4 of [Hö]).

Proposition 1.3.1 *Let L and L' be signatures such that $L \subseteq L'$ and T' a theory in L'. Let M and N be L'-structures which are models of T', R a relation symbol of L' and φ an explicit definition of R relative to T'. If for every $a \in M^n = N^n$ we have that $M \models \varphi(a) \Longleftrightarrow N \models \varphi(a)$, then $R^M = R^N$. The same occurs for constants and function symbols.*

This proposition is just a restatement of Definition 1.3.1.

Theorem 1.3.1 *Let L and L' be signatures such that $L \subseteq L'$, and T' a theory in L'. Suppose that for each symbol S of $L' \setminus L$ we have an explicit definition φ_S of S relative to T'. Consider $U := \{\forall x_1, \cdots, x_m \; S(x_1, \cdots, x_n) \leftrightarrow \varphi(x_1, \cdots, x_n)$; S is in $L' \setminus L\}$. Then, if M is a model of U, then for each formula $\psi(x_1, \cdots, x_n)$ of L' there is a formula $\psi^*(x_1, \cdots, x_n)$ of L such that*

$$M \models \forall(a_1, \cdots, a_n) \;\; \psi(a_1, \cdots, a_n) \Leftrightarrow \psi^*(a_1, \cdots, a_n) \; .$$

We also say that φ is an **explicit definition of S in a structure** M if φ is an explicit definition of S relative to $\mathrm{Th}(M)$. Then, if we consider M' as M expanded with S in its signature, then we say that M' is a **definitional expansion** of M. The theorem above ensures that when we take definitional expansions M' of a structure M the changes in the language are not significant to $\mathrm{Th}(M)$, because any sentence in $L' \setminus L$ can be reduced to a sentence in L. Moreover, this kind of change in the language does not cause an essential change to the class of definable sets, since if $A \in dom(M') = dom(M)$ is a definable set of M', then, by the last theorem, we can build a definition of A in M by replacing the definable symbol with its explicit definition.

Example 1.3.1 *We can define divisibility on the natural numbers* $(\mathbb{N}, 0, 1, +, \times)$ *by writing*

$$x | y \Longleftrightarrow \exists m \;\; y = mx$$

So, we may consider the definitional expansion $(\mathbb{N}, 0, 1, +, \times, \; | \;)$ *and define a prime number by*

$$x \textit{ is prime} \Longleftrightarrow \neg p = 1 \;\wedge\; \forall a, b \; x|(a.b) \Rightarrow (x|a \vee x|b)$$

Hence, as we suggested before, the following formulae are equivalent

$$(\exists m\ a.b = m.x) \Rightarrow ((\exists n\ a = n.x) \vee (\exists o\ b = o.x))$$

$$x|(a.b) \Rightarrow (x|a \vee x|b)$$

This Example (1.3.1) ilustrates how useful the usage of definitional expansions is to write sentences of the theory of some structure. In the next chapter, we will use definitional expantions of the first-order language of rings to contruct sentences to characterize some rings in a specific class.

1.4 Gödel Coding

In this section we describe the Gödel Coding, or Gödel β-functions, in $\mathbb{N}$. More specifically, we will show how we can code finite sequences over the natural numbers, and then we will present the sentences that are true in every model of PA^-, the finitely many basic algebraic axioms for *Peano Arithmetic* (see [Ka] for details and proofs). At the end of this section, we provide one example to ilustrate how important is the Gödel Coding, by proving that if a infinite finitely generated ring R is interpretable with $\mathbb{N}$, then there is a formula $\varphi(x, y)$ that defines "there is an automorphism $\sigma : R \longrightarrow R$ such that $\sigma(x) = y$".

Let $x_0, \cdots, x_{n-1}$ be a finite sequence of natural numbers. Now we are going to say how to code in this sequence in $\mathbb{N}$ with a natural number that can be used to recover the sequence. Consider $b = \max(n, x_0, \cdots, x_{n-1})$; and $m = b!$, the factorial of b.

Claim 1: *The finite sequence $m + 1, 2m + 1, \cdots, nm + 1$ is pairwise coprime.*

Proof: Suppose that there is a prime number p and $i, j \in \{0, \cdots, n\}$ such that $i < j$, $p|(im+1)$ and $p|(jm+1)$. Then, we have that $p|(j-i)m$ and $j-i < n \leq b$. Since p is prime, $p|(j-i)$ or $p|m$. Since $m = b(b-1). \cdots .(j-i). \cdots .1$, then $p|(j-i) \Rightarrow p|m$. In any case we have that $p|m$. Hence, $p|im$. Since $p|(im+1)$, then $p|(im+1-im)$, that is, $p|1$. This a contradiction with the fact that p is prime. □

Now, suppose that we have a system

$$\begin{cases} x \equiv x_0 \mod(m+1) \\ x \equiv x_1 \mod(2m+1) \\ \vdots \qquad\qquad \vdots \\ x \equiv x_{n-1} \mod(nm+1) \end{cases}$$

So, since Claim 1 holds, the *Chinese remainder theorem* ensures that there is a solution $a \in \mathbb{N}$ for this system (see [IR]). Thus, consider $a \in \mathbb{N}$ a solution of this system. We claim that the pair (a, m) *codes* the sequence $x_0, \cdots, x_{n-1}$, that is, we can recover this sequence from the pair (a, m). Indeed, for each $i \in \{0, \cdots, n\}$ we have that x_i is the remainder when we divide a by $m(i+1)+1$, that is, $a \equiv x_i \mod(m(i+1)+1)$ (a is a solution of the system). Therefore, given such pair (a, m) we can find its sequence $x_0, \cdots, x_n$. Since we want to use just a single natural number to encode one sequence, we will use the *pairing function* $< ., . >$ over $\mathbb{N} \times \mathbb{N}$ given by

$$< x, y >= \frac{(x+y).(x+y+1)}{2} + y$$

Claim 2: *The pairing function is a bijection between* $\mathbb{N} \times \mathbb{N}$ *and* $\mathbb{N}$.

Proof: Since for all $x, y \in \mathbb{N}$ we have an even number in the set $\{x + y, x+y+1\}$, then $\mathrm{Im}(< ., . >) \subseteq \mathbb{N}$. We now prove that the pairing function is injective. Suppose that $< x, y >=< u, v >$. Then, $x + y = u + v$. Indeed, suppose $x + y < u + v$. So, $x + y + 1 \leq u + v$. Hence,

$$< x, y >= \frac{(x+y).(x+y+1)}{2} + y < \frac{(x+y).(x+y+1)}{2} + y + 1 =$$

$$\frac{(x+y+1).(x+y+2)}{2} \leq \frac{(u+v).(u+v+2)}{2} + v =< u, v >=< x, y >$$

which is an absurd. Using this same argument when supposing that $u + v < x + y$, we have another absurd. Therefore, $x + y = u + v$. Now it is just note that

$$y =< x, y > - \frac{(x+y).(x+y+1)}{2} =< u, v > - \frac{(u+v).(u+v+1)}{2} = v.$$

and since $x + y = u + v$, $x = u$. Then, the pairing function is intective. Now we prove by induction on n that there is $x, y \in \mathbb{N}$ such that $< x, y >= n$. If $n = 0$, then take $x = 0$ and $y = 0$, and we are done. Suppose that there is

$x, y \in \mathbb{N}$ such that $< x, y >= n - 1$. If $x > 0$, then $x - 1 \geq 0$ and we can consider

$$n + 1 = \frac{((x-1) + (y+1).((x-1) + (y+1) + 1)}{2} + y + 1$$

that is, $n + 1 =< x - 1, y + 1 >$. If $x = 0$, then

$$n = n - 1 + 1 =< 0, y > +1 = \frac{y(y+1)}{2} + y + 1 =$$

$$\frac{y(y+1) + 2y + 2}{2} = \frac{(y+1).(y+2)}{2} =< y + 1, 0 >$$

Therefore, we have the surjectivity of $< ., . >$, and then the pairing function is a bijection. □

So, there is an injection

$$\begin{aligned} \{\text{finite sequences of } \mathbb{N}\} &\longrightarrow \mathbb{N} \\ \{x_0, \cdots, x_{n-1}\} &\longmapsto < a, m >. \end{aligned}$$

We summarize now what we used to ensure we can code a sequence $x_0, \cdots, x_{n-1}$ into one single number: we had to find a number m such that the elements in the sequence $m + 1, \cdots, nm + 1$ are pairwise coprime; we had to find a solution to the system $\bigwedge_{i=0}^{n-1} x \equiv x_i \mod((i+1)m + 1)$; and we had to define a bijective pairing function. It is true that we can define all these steps in any model of PA. Since this is not the main object of this work, we will skip the proof of this fact (for more details, see [Ka]). Nevertheless, we present now the powerful tool that ensure we can do the same thing as above but in any model of PA.

Proposition 1.4.1 (Gödel's Lemma) *Let M be a model of PA, and $n \in \mathbb{N}$ such that $x_0, \cdots, x_{n-1} \in M$. Then, there exists a formula $(x)_y = z$ and $u \in M$ such that $M \models (u)_i = x_i$ for all $i < n$.*

The formulae $(x)_y = z$ are known by "Gödel's β-functions," for they are frequently written as $\beta(x, y) = z$. Since we are dealing with sequences, we will use the notation $(x)_y = z$.

In the Chapter 4, we will be widely using Gödel coding to express formulas to define some sets and homomorphisms. Here is an example of the power of Gödel coding:

Proposition 1.4.2 *Let R be a ring that is generated by $a_1, \cdots, a_n$. If R is bi-interpretable in $\mathbb{Z}$, then there is a formula $\phi(x, y)$ defining the graph of $\sigma \in \mathrm{Aut}(R)$.*

Proof: Since R is bi-interpretable with $\mathbb{Z}$, we have a definable copy of R, say $(\mathbb{Z}, \oplus_R, \otimes_R)$, and the elements $a_1, \cdots, a_n, \sigma(a_1), \cdots, \sigma(a_n)$ are definable. Since $\mathbb{N}$ is definable in $\mathbb{Z}$, we can translate the Gödel coding to talk about sequences in R. For our convenience, we save the length of the sequence in the first slot of the sequence. So, suppose that $(x)_i =_R y$ is the translated Gödel coding in the copy of R and set the formula

$$\Gamma(\tau, x_1, \cdots, x_n) \Longleftrightarrow \forall m \; 0 < m \leq (\tau)_0 \Rightarrow \bigwedge_{i=1}^{n} (\tau) =_R x_i \vee$$

$$\exists j, l < m \begin{pmatrix} (\tau)_m =_R (\tau)_j \oplus_R (\tau)_l \\ (\tau)_m =_R (\tau)_j \otimes_R (\tau)_l \\ (\tau)_m \oplus_R (\tau)_l =_R (\tau)_j \end{pmatrix}$$

It is true that if $x \in R$ is the image of $(a_1, \cdots, a_n)$ by some $f \in \mathbb{Z}[t_1, \cdots, t_n]$, then $\sigma(x) = f(\sigma(a_1), \cdots, \sigma(a_n))$ for which σ is an automorphism of R. Then, consider $\Psi(\tau, y_1, \cdots, y_n; y) : \Gamma(\tau, y_1, \cdots, y_n) \wedge (\tau)_{(\tau)_0} = y$. Then we define the formula $\phi(x, y)$ by

$\phi(x, y) \Longleftrightarrow$
(1) $\exists \tau \Psi(\tau, a_1, \cdots, a_n; x) \Longrightarrow \Psi(\tau, \sigma(a_1), \cdots, \sigma(a_n); y)$.

(2)$\forall a, b, c \; \big(\exists \tau \rho$
$\Psi(\tau, a_1, \cdots, a_n; a) \wedge \Psi(\rho, a_1, \cdots, a_n; b) \wedge \Psi(\tau, \sigma(a_1), \cdots, \sigma(a_n); c) \wedge \Psi(\rho, \sigma(a_1), \cdots, \sigma(a_n); c)\big)$
$\Longrightarrow a = b$. (injectivity of σ)

(3) $\forall y \exists x, \tau \; \Psi(\tau, a_1, \cdots, a_n; x) \wedge \Psi(\tau, \sigma(a_1), \cdots, \sigma(a_n); y)$. (surjectivity of σ)

In other words, the sentence above says that (x, y) is in graph(σ) iff (1) there is a polynomial $f \in \mathbb{Z}[x_1, \cdots, x_n]$ such that $f(a_1, \cdots, a_n) = x$ and $f(\sigma(a_1), \cdots, \sigma(a_n)) = y$; (2) for all a,b,c if there is $f, g \in \mathbb{Z}[x_1, \cdots, x_n]$ such that $f(a_1, \cdots, a_n) = a$, $g(a_1, \cdots, a_n) = b$, $f(\sigma(a_1), \cdots, \sigma(a_n)) = c$ and $g(\sigma(a_1), \cdots, \sigma(a_n)) = c$, then $a = b$; (3) for all y there is $f(x_1, \cdots, x_n) \in \mathbb{Z}[x_1. \cdots, x_n]$ and $x \in R$ such that $f(a_1, \cdots, a_n) = x$ and $f(\sigma(a_1), \cdots, \sigma(a_n)) = y$. This is exactly the description of σ as an automorphism over R. Therefore, any $\sigma \in \mathrm{Aut}(R)$ is definable if R is bi-interpretable with $\mathbb{Z}$. ■

This are the preliminaries in model theory necessary to understand the following chapters. In the next chapter, interpretations and definitional expansions will be widely used. We introduce the definition of *QFA-rings* and use these concepts to provide some examples of QFA-rings.

Capítulo 2

Quasi-finitely Axiomatizable Rings

2.1 QFA Rings

In this chapter, we are going to define and present some instances of an intersting class of structures, the *quasi-finitely axiomatizable* rings.

Definition 2.1.1 *Let $\mathcal{L}_{ring}$ be the language of first order of the rings and $\mathcal{K}$ be the class of the finitely generated commutative rings. We say that $S \in \mathcal{K}$ is quasi-finitely axiomatizable, or QFA, if there is a sentence $\varphi \in \mathcal{L}_{ring}$ such that $S \models \varphi$ and if $A \in \mathcal{K}$ is such that $A \models \varphi$, then we have $A \simeq S$. If $S \in \mathcal{K}$ is QFA and $\varphi \in \mathcal{L}_{ring}$ is such sentence, we also say that S is QFA via φ or that φ is a QFA-sentence for S.*

Note that if $S \in \mathcal{K}$ is QFA via ϕ and also via φ, then every model of ϕ that is in $\mathcal{K}$ is a model of φ (and vice & versa). In 2004, O. Belegradek raised the question "which f.g. rings are QFA." Note that, since $\mathbb{Z}[x_1, \cdots, x_n]$ is noetherian and $\mathbb{Z}[x_1, \cdots, x_n]$ is the free ring in n variables, each f.g. ring is noetherian.

Example 2.1.1 *As a very first example, we claim that $(\mathbb{Z}/2\mathbb{Z}, 0, 1, +, \cdot)$ is QFA via the sentence*

$$\varphi_{\mathbb{Z}_2} : \quad (\neg 0 = 1) \wedge (\forall x \quad x = 0 \vee x = 1)$$

If we suppose that $A \in \mathcal{K}$ is a model of $\varphi_{\mathbb{Z}_2}$, then A have exactly two elements. Indeed, since $0 \neq 1$, we have that $1+1 \neq 1$, and that $1+1=0$. Then there is an isomorphism $\psi : \mathbb{Z}_2 \longrightarrow A$ (note that any homomorphism has to be an isomorphism in this case).

Roughly speaking, a ring is QFA if we can describe it in $\mathcal{K}$, up to isomorphism, just by asserting properties holding among its elements usings only a finite number of words built from terms and the logical symbols in the first order language of rings. We may be using here definitional expantions of $\mathcal{L}_{ring}$ without mentioning it. There is also an equivalent notion for QFA groups. Some authors, like Andre Nies, have developed some work in this direction (see [An]). However, in this text we will concentrate in the ring case. To be QFA is a very strong characteristic for a ring to have. For instance, to be QFA implies categoricity in some sense. For the next sections we will show some samples of nontrivial QFA structures and prove that in fact they are QFA by building isomorphisms in each case. It is not too hard to see that we can contruct to each finite structure, as we did with $\mathbb{Z}_2$, its QFA-sentence (for example, see [Vää]). That is why we just treat infinite structures in the following.

2.2 The integers

The ring of integers is the most important mathematical structure that anyone would study. Therefore, it does make sense to ask whether $(\mathbb{Z}, 0, 1, +, \times)$ is QFA in order to go on investigating through $\mathcal{K}$. In 2004, Sabbagh proved (see [Ni]) that $\mathbb{Z}$ is QFA by using Gödel coding to define the factorial function $n \mapsto n!$, but we decided to present a more elementary sentence.

Proposition 2.2.1 *The integers are QFA.*

Proof: Firstly, we want to define an order $x < y \Leftrightarrow$ "$y - x - 1$ is a natural number". Every natural number is the sum of four squares (Lagrange's Theorem, see [IR]). Then, we can define the natural numbers in $\mathbb{Z}$ by

$$\mathbb{N} = \{x \in \mathbb{Z} \ ; \ \exists n_1, n_2, n_3, n_4 \ \ x = n_1^2 + n_2^2 + n_3^2 + n_4^2\}$$

With this definition of $\mathbb{N}$, we define the order "<" by

$$\forall x, y, z \ \ x < y \ \Leftrightarrow \exists n_1, n_2, n_3, n_4 \ \ y = x + 1 + n_1^2 + n_2^2 + n_3^2 + n_4^2$$

$$(x < y) \wedge (y < z) \ \Rightarrow x < z$$

$$(0 < z) \wedge (x < y) \;\Rightarrow zx < zy$$

$$x < y \;\Rightarrow x + z < y + z$$

Now we add a sentence to say that the model is "discrete"

$$\forall x, y \;\; (x < y)\dot{\vee}(x = y)\dot{\vee}(x = y + 1)\dot{\vee}(y + 1 < x)$$

for which "$\phi\dot{\vee}\psi \Leftrightarrow (\phi\wedge\neg\psi)\vee(\neg\phi\wedge\psi)$" is the *exclusive or* (we can ensure that the positive elements of a model in $\mathcal{K}$ for these sentences satisfies PA^-; PA^- consists of the finitely many basic algebraic axioms for Peano Arithmetic, see [Ka], and so it can be considered as a single sentence). Actually some of those, like $(x < y) \wedge (y < z) \;\Rightarrow x < z$, are part of PA^-. Therefore a model in $\mathcal{K}$ of these sentences is a model of Th($\mathbb{Z}$)) and finally a sentence ϕ to say that for all elements of the model there is a bigger element that is equivalent to a power of 2.

$$\psi(w): \;\; \forall x \;\; 1 < x \Rightarrow ((\exists r \;\; w = rx) \Rightarrow (\exists s \;\; x = 2s))$$

$$\phi: \;\; \forall z \exists w \;\; (z < w) \wedge \psi(w).$$

Claim: *The conjunction $\phi \wedge \overline{PA^-}$ is a QFA-sentence for $\mathbb{Z}$, for which $\overline{PA^-}$ is the relativisation of PA^- to the set $\{a \in M \; ; \; \exists n_1, n_2, n_3, n_4 \;\; x = n_1^2 + n_2^2 + n_3^2 + n_4^2\}$.*

Proof: Let $M \in \mathcal{K}$ be such that $M \models \phi \wedge \overline{PA^-}$. Since $M \models \overline{PA^-}$, M is an ordered rings. Now we will prove that the natural map $\mathbb{Z} \to M$ is an isomorphism. Since M is ordered, this map is injective. Suppose that this map is not surjective. We will use the following theorem (see [Ka]) to ensure that there is an element in M that is greater than all integers.

Theorem 2.2.1 (Thm. 2.2 in [Ka]) *Let $M \models PA^-$. Then the map $\mathbb{N} \to M$ given by $n \mapsto n^M$ is an embedding sending $\mathbb{N}$ onto an initial segment of M.*

Since the map is not surjective, then, by Theorem 2.2.1, there is $\alpha \in M$ such that $\forall n \; n < \alpha$. So, by ϕ there is an element $\theta_0 \in |M|$ such that $(\alpha < \theta_0) \wedge \psi(\theta_0)$. Hence, ψ ensures the following lemma.

Lemma 2.2.1 *For all $i \in \mathbb{N}$ we have that 2^i divides θ_0.*

Proof: (Lema 2.2.1) We prove this lemma by induction on $i \in \mathbb{N}$. Since $\theta_0 = 2^0.\theta_0$, then we have that the base case holds. Suppose that θ_0 is divisible by 2^n, that is, that there exists θ_n such that $\theta_0 = 2^n.\theta_n$. Since θ_0 is greater that all integers, so is θ_n. Thus, $\theta_n > 1$ and $\psi(\theta_0)$ implies that there exists θ_{n+1} such that $\theta_n = 2.\theta_{n+1}$. Hence, $\theta_0 = 2^n.\theta_n = 2^n.2.\theta_{n+1} = 2^{n+1}.\theta_{n+1}$, that is, θ_0 is divisible by 2^{n+1}. Therefore, the lemma follows, by induction. □

Suppose that we have all the sequence $\{\theta_i\}_{i\in\mathbb{N}}$ from Lemma 2.2.1. Then, we can build a properly ascending chain of ideals

$$(\theta_1) \subset (\theta_2) \subset (\theta_3) \subset \cdots \subset (\theta_n) \subset \cdots$$

Since all the θ_i's are transcendent, this chain goes on forever. So, M is not a Noetherian ring, which is a contradiction with the fact that $M \in \mathcal{K}$ (M is finitely generated). □

Hence, if we consider

$$\begin{aligned}\varphi_{\mathbb{Z}}:\ & \forall x,y,z\ (x<y \ \Leftrightarrow \exists n_1,n_2,n_3,n_4\ \ y = x+1+n_1^2+n_2^2+n_3^2+n_4^2)\wedge \\ & ((x<y)\wedge(y<z)\ \Rightarrow x<z)\wedge \\ & ((0<z)\wedge(x<y)\ \Rightarrow zx<zy)\wedge \\ & (x<y\ \Rightarrow x+z<y+z)\wedge \\ & ((x<y)\dot{\vee}(x=y)\dot{\vee}(x=y+1)\dot{\vee}(y+1<x))\wedge \\ & (\forall z\exists w\ \ z<w \wedge (\forall x\ \ 1<x \Rightarrow ((\exists r\ \ w=rx) \Rightarrow (\exists s\ \ x=2s))))\end{aligned} \tag{2.2.1}$$

then the arguments above ensure that if $S \in \mathcal{K}\ \wedge\ S \models \varphi_{\mathbb{Z}}$, then $S \simeq \mathbb{Z}$. So, $\varphi_{\mathbb{Z}}$ is a QFA-sentence for $\mathbb{Z}$. ■

Now we go on investigating other interesting cases.

2.3 The rings $\mathbb{Z}[\varepsilon]/(\varepsilon^2)$ and $\mathbb{Z}[\varepsilon]/(\varepsilon^3)$.

At first, we can uniquely represent elements of $\mathbb{Z}[\varepsilon]/(\varepsilon^2)$ and $\mathbb{Z}[\varepsilon]/(\varepsilon^3)$, respectively, by $a+b\varepsilon$ and $r+s\varepsilon+t\varepsilon^2$, for which $a,b,r,s,t \in \mathbb{Z}$ and ε is a distinguished element of the ring satisfying $\varepsilon \neq 0$ and $\varepsilon^2 = 0$. Nevertheless, these sentences describing how the elements in these rings are have sentences $\ulcorner a,b\in\mathbb{Z}\urcorner$ and $\ulcorner a,b,c\in\mathbb{Z}\urcorner$ that depend on a predicate for $\mathbb{Z}$. Therefore, we should have a explicit definition of $\mathbb{Z}$ in $\mathrm{Th}(\mathbb{Z}[\varepsilon]/(\varepsilon^2))$. With this purpose, we could try to find such definition $\varphi(x) \in \mathcal{L}_{ring}$ of $\mathbb{Z}$ valid in $\mathbb{Z}[\varepsilon]/(\varepsilon^2)$, *id est* $\ulcorner\varphi(x) \Leftrightarrow x\in\mathbb{Z}\urcorner$, and then say that

$$\mathbb{Z}[\varepsilon]/(\varepsilon^2) = \{a+b\varepsilon\ ;\ \varphi(a)\wedge\varphi(b)\wedge\neg\varepsilon=0\wedge\varepsilon^2=0\}$$

However, the integers $\mathbb{Z}$ unfortunately (or fortunately) are not definable in $\mathbb{Z}[\varepsilon]/(\varepsilon^2)$ (the arguments for this last claim will be presented in the first section of the appendix). But fortunately we can at least interpret $\mathbb{Z}$ in $\mathbb{Z}[\varepsilon]/(\varepsilon^2)$, and we shall use one interpretation to construct a QFA-sentence $\varphi_{\mathbb{Z}[\varepsilon]/(\varepsilon^2)}$ for $\mathbb{Z}[\varepsilon]/(\varepsilon^2)$. Indeed, we first add the sentence $\theta :\ \ulcorner\exists\epsilon\ \ \neg\epsilon = 0 \wedge \epsilon^2 = 0\urcorner$ and then define the equivalence relation $x \overset{\mathbb{Z}}{\sim} y$ by the following sentence

$$\forall x, y\ \ x \overset{\mathbb{Z}}{\sim} y\ \Leftrightarrow \exists m\ \ x = y + m\epsilon$$

for which ϵ is given by θ. And now, to say that $\overset{\mathbb{Z}}{\sim}$ induces an interpretation of $\mathbb{Z}$, we consider a QFA-sentence of $\mathbb{Z}$, say $\varphi_{\mathbb{Z}}$, and relativise it by substitution of the symbol "$=$" by "$\overset{\mathbb{Z}}{\sim}$", say $\tilde{\varphi}_{\mathbb{Z}}$. Thus, if $S \in \mathcal{K}$ satisfies these sentences, then necessarily $S/\overset{\mathbb{Z}}{\sim}\ \simeq \mathbb{Z}$ via $\overline{1_S} \mapsto 1_{\mathbb{Z}}$. To complete our sentence $\varphi_{\mathbb{Z}[\varepsilon]/(\varepsilon^2)}$, we add just one more sentence, namely $\forall x, y\ \ \epsilon x = \epsilon y \Rightarrow x \overset{\mathbb{Z}}{\sim} y$. Putting everything together, our QFA-sentence for $\mathbb{Z}[\varepsilon]/(\varepsilon^2)$ is given by

$$\begin{aligned}
\varphi_{\mathbb{Z}[\varepsilon]/(\varepsilon^2)} :\ & (\exists\epsilon\ \ \neg\epsilon = 0 \wedge \epsilon^2 = 0)\wedge \\
& \forall x, y, z\ \ (x \overset{\mathbb{Z}}{\sim} y\ \Leftrightarrow \exists m\ \ x = y + m\epsilon)\wedge \\
& (x < y\ \Leftrightarrow \exists n_1, n_2, n_3, n_4\ \ y \overset{\mathbb{Z}}{\sim} x + 1 + n_1^2 + n_2^2 + n_3^2 + n_4^2)\wedge \\
& ((x < y) \wedge (y < z)\ \Rightarrow x < z)\wedge \\
& ((0 < z) \wedge (x < y)\ \Rightarrow zx < zy)\wedge \\
& (x < y\ \Rightarrow x + z < y + z)\wedge \\
& ((x < y)\dot{\vee}(x \overset{\mathbb{Z}}{\sim} y)\dot{\vee}(x \overset{\mathbb{Z}}{\sim} y + 1)\dot{\vee}(y + 1 < x))\wedge \\
& (\forall z \exists w\ \ z < w \wedge (\forall x\ \ 1 < x \Rightarrow ((\exists r\ \ w \overset{\mathbb{Z}}{\sim} rx) \Rightarrow (\exists s\ \ x \overset{\mathbb{Z}}{\sim} 2s))))\wedge \\
& (\epsilon x = \epsilon y \Rightarrow x \overset{\mathbb{Z}}{\sim} y)
\end{aligned} \tag{2.3.1}$$

Note that we introduced the definable symbols $\overset{\mathbb{Z}}{\sim}$ and $<$. Hence, $\varphi_{\mathbb{Z}[\varepsilon]/(\varepsilon^2)}$ is actually a sentence of the definitional expansion $(\mathbb{Z}[\varepsilon]/(\varepsilon^2), 0, 1, , \overset{\mathbb{Z}}{\sim}, <)$. Now we are going to prove that $\varphi_{\mathbb{Z}[\varepsilon]/(\varepsilon^2)}$ works.

Proposition 2.3.1 *Let $\varphi_{\mathbb{Z}[\varepsilon]/(\varepsilon^2)} \in \mathcal{L}_{ring}(\overset{\mathbb{Z}}{\sim}, <)$ be as above. Then, $\mathbb{Z}[\varepsilon]/(\varepsilon^2)$ is QFA via $\varphi_{\mathbb{Z}[\varepsilon]/(\varepsilon^2)}$.*

Proof: Let $S \in \mathcal{K}$ be a model of $\varphi_{\mathbb{Z}[\varepsilon]/(\varepsilon^2)}$. Since $S/\overset{\mathbb{Z}}{\sim} \models \varphi_{\mathbb{Z}}$, we have that $n.1_S$ corresponds to n in the quotient and for each $x \in S$ there is a unique $n \in \mathbb{Z}$ for which $x \overset{\mathbb{Z}}{\sim} n$. We define the map $\Phi : \mathbb{Z}[\varepsilon] \longrightarrow S$ such that $1_{\mathbb{Z}} \mapsto 1_S$ and $\varepsilon \mapsto \epsilon$. From the definition, we conclude directly that Φ is a homomorphism. Moreover, Φ induces a homomorphism $\Psi : \mathbb{Z}[\varepsilon]/(\varepsilon^2) \longrightarrow S$ given by

$$a + b\varepsilon \longmapsto a.1_S + b.1_S.\epsilon$$

So, as an isomorphism is a surjective embedding, it suffices to prove that Ψ is bijective.

Lemma 2.3.1 $\Psi : \mathbb{Z}[\varepsilon]/(\varepsilon^2) \longrightarrow S$ *is surjective.*

Proof: Take $y \in S$. So, there is a representative $a.1_S \in S$ for the class that has y. Hence, since y and $a.1_S$ are in the same class, there is $m \in S$ such that $y = a.1_S + m\epsilon$. Analogously, there is a representative $b.1_S \in S$ for the class that has m. Like before, there is $n \in S$ such that $m = b.1_S + n\epsilon$. Thus, we can express y as $y = a.1_S + m\epsilon = a.1_S + (b.1_S + n\epsilon)\epsilon = a.1_S + b.1_S\epsilon + n\epsilon^2$. Since $S \models \varphi_{\mathbb{Z}[\varepsilon]/(\varepsilon^2)}$, then $\epsilon^2 = 0$. Hence, $y = a.1_S + b.1_S\epsilon$. Then, if we consider $x = a + b\varepsilon \in \mathbb{Z}[\varepsilon]/(\varepsilon^2)$ such that $a, b \in \mathbb{Z}$ are such as in the definition of Ψ, we have that $\Psi(x) = y$. $\square$

Lemma 2.3.2 $\Psi : \mathbb{Z}[\varepsilon]/(\varepsilon^2) \longrightarrow S$ *is injective.*

Proof: Suppose that $x = a + b\varepsilon$ is such that $\Psi(a + b\varepsilon) = 0$. So, $a.1_S - 0 = -b\epsilon \;\therefore\; a.1_S \overset{\mathbb{Z}}{\sim} 0 \;\therefore a = 0$. Then, we have that $b.1_S\epsilon = 0.\epsilon$. By $\varphi_{\mathbb{Z}[\varepsilon]/(\varepsilon^2)}$, we have $b.1_S \overset{\mathbb{Z}}{\sim} 0 \;\therefore b = 0$. Therefore, $x = 0$. $\square$

Then, $S \simeq \mathbb{Z}[\varepsilon]/(\varepsilon^2)$ and the proposition is proved. ■

Analogously, we can build $\varphi_{\mathbb{Z}[\varepsilon]/(\varepsilon^3)}$ such that the ring $\mathbb{Z}[\varepsilon]/(\varepsilon^3)$ is QFA via $\varphi_{\mathbb{Z}[\varepsilon]/(\varepsilon^3)}$. Just by changing and adding sentences to the last sentence we built, we find

$$\begin{array}{rl}
\varphi_{\mathbb{Z}[\varepsilon]/(\varepsilon^3)}: & (\exists\epsilon \;\; \neg\epsilon = 0 \wedge \neg\epsilon^2 = 0 \wedge \epsilon^3 = 0)\wedge \\
& \forall x, y, z \;\; (x \overset{\mathbb{Z}}{\sim} y \;\Leftrightarrow \exists m \;\; x = y + m\epsilon)\wedge \\
& (x < y \;\Leftrightarrow \exists n_1, n_2, n_3, n_4 \;\; y \overset{\mathbb{Z}}{\sim} x + 1 + n_1^2 + n_2^2 + n_3^2 + n_4^2)\wedge \\
& ((x < y) \wedge (y < z) \;\Rightarrow x < z)\wedge \\
& ((0 < z) \wedge (x < y) \;\Rightarrow zx < zy)\wedge \\
& (x < y \;\Rightarrow x + z < y + z)\wedge \\
& ((x < y)\dot{\vee}(x \overset{\mathbb{Z}}{\sim} y)\dot{\vee}(x \overset{\mathbb{Z}}{\sim} y + 1)\dot{\vee}(y + 1 < x))\wedge \\
& (\forall z \exists w \;\; z < w \wedge (\forall x \;\; 1 < x \Rightarrow ((\exists r \;\; w = rx) \Rightarrow (\exists s \;\; x = 2s))))\wedge \\
& (\epsilon^2 x = \epsilon^2 y \Rightarrow x \overset{\mathbb{Z}}{\sim} y)
\end{array} \tag{2.3.2}$$

Claim: $\mathbb{Z}[\varepsilon]/(\varepsilon^3)$ *is QFA via* $\varphi_{\mathbb{Z}[\varepsilon]/(\varepsilon^3)}$.

Proof: Suppose that $S \in \mathcal{K}$ is a model of $\varphi_{\mathbb{Z}[\varepsilon]/(\varepsilon^3)}$. We build, like before, a homomorphism $\Psi : \mathbb{Z}[\varepsilon]/(\varepsilon^3) \longrightarrow S$ given by

$$a + b\varepsilon + c\varepsilon^2 \longmapsto a.1_S + b.1_S\epsilon + c.1_S\epsilon^2$$

Once again, it is enough to prove that Ψ is a bijection. The surjectivity follows analogously as before. Take $y \in S$. Then, since $S/\overset{\mathbb{Z}}{\sim} \simeq \mathbb{Z}$, $y \in \overline{a.1_S}$ for some $a \in \mathbb{Z}$. Then, there is $m \in S$ such that $y = a.1_S + m\epsilon$. Since $m \in \overline{b.1_S}$ for some $b \in \mathbb{Z}$, there is $n \in S$ such that $m = b.1_S + n\epsilon$. Analogously, there is $q \in S$ such that $n = c.1_S + q\epsilon$ and $n \in \overline{c.1_S}$. Thus, we write $y = a.1_S + (b.1_S + (c.1_S + q\epsilon)\epsilon)\epsilon = a.1_S + b.1_S\epsilon + c.1_S\epsilon^2 + q\epsilon^3$. Since $S \models \varphi_{\mathbb{Z}[\varepsilon]/(\varepsilon^3)}$, then $\epsilon^3 = 0$. Hence, $y = a.1_S + b.1_S\epsilon + c.1_S\epsilon^2$. Then, taking $x = a + b\varepsilon + c\varepsilon^2 \in \mathbb{Z}[\varepsilon]/(\varepsilon^3)$, $\Psi(x) = y$ and the surjectivity of Ψ follows.

The argument for the injectivity is similar. Suppose that $x = a + b\varepsilon + c\varepsilon^2$ is such that $\Psi(x) = a.1_S + b.1_S\epsilon + c.1_S\epsilon^2 = 0$. If we multiply the last equation by ϵ^2, we have that $a.1_S\epsilon^2 = 0$, since $\epsilon^3 = 0$. So, $a.1_S \overset{\mathbb{Z}}{\sim} 0 \;\therefore a = 0$. Now, the equation becomes $b.1_S\epsilon + c.1_S\epsilon^2 = 0$. So, if we multiply by ϵ, then we have that $b.1_S.\epsilon^2 = 0$. So, $b.1_S \overset{\mathbb{Z}}{\sim} 0 \;\therefore b = 0$. Now the equation is just $c.1_S\epsilon = 0$, and then $c.1_S \overset{\mathbb{Z}}{\sim} 0 \;\therefore c = 0$. Therefore, $x = 0$ and the injectivity of Ψ follows.
■

2.4 The rings $\mathbb{Z}[\varepsilon]/(\varepsilon^4, 5\varepsilon^3)$ and $\mathbb{Z}[\varepsilon, \eta]/(\varepsilon^3, \eta^3, \varepsilon\eta^2)$

At this point, the reader probably is thinking "why more examples?" One possible answer for this question is that we are considering these other examples to exhibit some of the complications which may arise.

Consider $S_1 := \mathbb{Z}[\varepsilon]/(\varepsilon^4, 5\varepsilon^3)$ and $S_2 := \mathbb{Z}[\varepsilon, \eta]/(\varepsilon^3, \eta^3, \varepsilon\eta^2)$. We shall present QFA-sentences φ_{S_1} and φ_{S_1} for S_1 and S_2, respectively. Once again, we produce a sentence very close to the previous ones. We leave the proof to the reader that S_1 is QFA via

$$\begin{aligned}
\varphi_{S_1}:\ & (\exists \epsilon\ \ \neg\epsilon^3 = 0 \wedge 5\epsilon^3 = 0 \wedge \epsilon^4 = 0)\wedge \\
& \forall x, y, z\ \ (x \overset{\mathbb{Z}}{\sim} y\ \Leftrightarrow \exists m\ \ x = y + m\epsilon)\wedge \\
& (x < y\ \Leftrightarrow \exists n_1, n_2, n_3, n_4\ \ y \overset{\mathbb{Z}}{\sim} x + 1 + n_1^2 + n_2^2 + n_3^2 + n_4^2)\wedge \\
& ((x < y) \wedge (y < z)\ \Rightarrow x < z)\wedge \\
& ((0 < z) \wedge (x < y)\ \Rightarrow zx < zy)\wedge \\
& (x < y\ \Rightarrow x + z < y + z)\wedge \\
& ((x < y)\dot{\vee}(x \overset{\mathbb{Z}}{\sim} y)\dot{\vee}(x \overset{\mathbb{Z}}{\sim} y + 1)\dot{\vee}(y + 1 < x))\wedge \\
& (\forall z \exists w\ \ z < w \wedge (\forall x\ \ 1 < x \Rightarrow ((\exists r\ \ w \overset{\mathbb{Z}}{\sim} rx) \Rightarrow (\exists s\ \ x \overset{\mathbb{Z}}{\sim} 2s))))\wedge \\
& (\epsilon x = \epsilon y \Rightarrow x \overset{\mathbb{Z}}{\sim} y)\wedge \\
& (\epsilon^2 x = \epsilon^2 y \Rightarrow x \overset{\mathbb{Z}}{\sim} y) \\
& (\epsilon^3 x = \epsilon^3 y \Rightarrow \exists m\ \ x \overset{\mathbb{Z}}{\sim} y + 5m)
\end{aligned} \tag{2.4.1}$$

In the case of S_2, it seems to be more complicated. Nevertheless, it also follows from the same argument, but with a bigger, and slightly more difficult, sentence. Indeed, we can define

$$\begin{aligned}
\varphi_{S_2}: \;& (\exists\epsilon \;\; \neg\epsilon^2 = 0 \wedge \epsilon^3 = 0)\wedge \\
& (\exists n \;\; \neg n^2 = 0 \wedge n^3 = 0)\wedge \\
& (\neg\epsilon^2 n = 0 \wedge \epsilon n^2 = 0)\wedge \\
& \forall x, y, z \;\; (x \overset{\mathbb{Z}}{\sim} y \;\Leftrightarrow \exists r, s \;\; x = y + r\epsilon + sn)\wedge \\
& (x < y \;\Leftrightarrow \exists m_1, m_2, m_3, m_4 \;\; y \overset{\mathbb{Z}}{\sim} x + 1 + m_1^2 + m_2^2 + m_3^2 + m_4^2)\wedge \\
& ((x < y) \wedge (y < z) \;\Rightarrow x < z)\wedge \\
& ((0 < z) \wedge (x < y) \;\Rightarrow zx < zy)\wedge \\
& (x < y \;\Rightarrow x + z < y + z)\wedge \\
& ((x < y)\dot{\vee}(x \overset{\mathbb{Z}}{\sim} y)\dot{\vee}(x \overset{\mathbb{Z}}{\sim} y + 1)\dot{\vee}(y + 1 < x))\wedge \\
& (\forall z \exists w \;\; z < w \wedge (\forall x \;\; 1 < x \Rightarrow ((\exists r \;\; w \overset{\mathbb{Z}}{\sim} rx) \Rightarrow (\exists s \;\; x \overset{\mathbb{Z}}{\sim} 2s))))\wedge \\
& (\epsilon x + ny = \epsilon p + nq \Rightarrow ((x \overset{\mathbb{Z}}{\sim} p) \wedge (y \overset{\mathbb{Z}}{\sim} q))\wedge \\
& (\epsilon^2 x = \epsilon^2 y + nq \Rightarrow x \overset{\mathbb{Z}}{\sim} y)\wedge \\
& (n^2 x = n^2 y + \epsilon p \Rightarrow x \overset{\mathbb{Z}}{\sim} y)\wedge \\
& (\epsilon n x = \epsilon n y \Rightarrow x \overset{\mathbb{Z}}{\sim} y)\wedge \\
& (\epsilon^2 n x = \epsilon^2 n y \Rightarrow x \overset{\mathbb{Z}}{\sim} y)
\end{aligned} \tag{2.4.2}$$

Proposition 2.4.1 *S_2 is QFA via φ_{S_2}.*

Proof: Let $S \in \mathcal{K}$ be a model of φ_2. Since $S_2/\overset{\mathbb{Z}}{\sim} \simeq \mathbb{Z}$, we construct a map $\Phi : \mathbb{Z}[\varepsilon, \eta] \longrightarrow S$ such that

$$(1, \varepsilon, \eta) \mapsto (1_S, \epsilon, n)$$

Like before, Φ induces a homomorphism $\Psi : S_2 \longrightarrow S$, and it suffices to show that Ψ is bijective to be an isomorphism. Let y be an element of S. We can use the same argument of taking fixed representatives of classes in $S_2/\overset{\mathbb{Z}}{\sim}$ to write $y = a_0.1_S + a_1.1_S\epsilon + a_2.1_S n + a_{2,0}.1_S\epsilon^2 + a_{1,1}.1_S\epsilon n + a_{0,2}.1_S n^2 + a_{2,1}.1_S\epsilon^2 n$. So, setting $x = a_0 + a_1\varepsilon + a_2\eta + a_{2,0}\varepsilon^2 + a_{1,1}\varepsilon\eta + a_{0,2}\eta^2 + a_{2,1}\epsilon^2\eta \in S_2$, we have $\Psi(x) = y$ and then Ψ is surjective. We shall shorten the proof of injectivity of Ψ too. Suppose that $\Psi(x) = \Psi(y)$ for some $x, y \in S_2$. So,

$$a_0^x.1_S + a_1^x.1_S\epsilon + a_2^x.1_S n + a_{2,0}^x.1_S\epsilon^2 + a_{1,1}^x.1_S\epsilon n + a_{0,2}^x.1_S n^2 + a_{2,1}^x.1_S\epsilon^2 n =$$

$$a_0^y.1_S + a_1^y.1_S\epsilon + a_2^y.1_S n + a_{2,0}^y.1_S\epsilon^2 + a_{1,1}^y.1_S\epsilon n + a_{0,2}^y.1_S n^2 + a_{2,1}^y.1_S\epsilon^2 n.$$

Therefore

$$a_0^x.1_S - a_0^y.1_S = (a_1^y.1_S - a_1^x.1_S + (a_{2,0}^y.1_S - a_{2,0}^x.1_S)\epsilon + (a_{1,1}^y.1_S - a_{1,1}^x.1_S)n)\epsilon +$$
$$a_2^y.1_S - a_2^x.1_S + (a_{0,2}^y.1_S - a_{0,2}^x.1_S)n + (a_{2,1}^y.1_S - a_{2,1}^x.1_S)\epsilon^2)n.$$

Hence, $a_0^x.1_S \overset{\mathbb{Z}}{\sim} a_0^y.1_S \ \therefore\ a_0^x.1_S = a_0^y.1_S \ \therefore\ a_0^x = a_0^y$. Simplifying and rearranging the first identity, it follows that

$$(a_1^x.1_S + a_{2,0}^x.1_S\epsilon + a_{1,1}^x.1_S n)\epsilon + (a_2^x.1_S + a_{0,2}^x.1_S n + a_{2,1}^x.1_S\epsilon^2)n =$$
$$(a_1^y.1_S + a_{2,0}^y.1_S\epsilon + a_{1,1}^y.1_S n)\epsilon + (a_2^y.1_S + a_{0,2}^y.1_S n + a_{2,1}^y.1_S\epsilon^2)n.$$

Thus $r_{a_1^x} \overset{\mathbb{Z}}{\sim} r_{a_1^y} \wedge a_2^x.1_S \overset{\mathbb{Z}}{\sim} a_2^y.1_S \ \therefore\ a_1^x.1_S = a_1^y.1_S \wedge a_2^x.1_S = a_2^y.1_S \ \therefore$ $a_1^x = a_1^y \wedge a_2^x = a_2^y$. After canceling the commom terms, we can see that

$$(a_{2,0}^x - a_{2,0}^y).1_S\epsilon^2 = ((a_{1,1}^y - a_{1,1}^x)1_S\epsilon + (a_{0,2}^y - a_{0,2}^x)1_S n + (a_{2,1}^y - a_{2,1}^x)1_S\epsilon^2)n$$

and

$$(a_{0,2}^x - a_{0,2}^y).1_S n^2 = (a_{2,0}^y - a_{2,0}^x)1_S\epsilon + (a_{1,1}^y - a_{1,1}^x)1_S n + (a_{2,1}^y - a_{2,1}^x)1_S\epsilon n)\epsilon$$

Then $a_{2,0}^x.1_S \overset{\mathbb{Z}}{\sim} a_{2,0}^y.1_S \wedge a_{0,2}^x.1_S \overset{\mathbb{Z}}{\sim} a_{0,2}^y.1_S$ implies that $a_{2,0}^x.1_S = a_{2,0}^y.1_S \wedge a_{0,2}^x.1_S = a_{0,2}^y.1_S$ and, then, $a_{2,0}^x = a_{2,0}^y \wedge a_{0,2}^x = a_{0,2}^y$. Now, it remains

$$\epsilon n(a_{1,1}^x.1_S + a_{2,1}^x.1_S\epsilon) = \epsilon n(a_{1,1}^y.1_S + a_{2,1}^y.1_S\epsilon)$$

It follows that $(a_{1,1}^x.1_S + a_{2,1}^x.1_S\epsilon) \overset{\mathbb{Z}}{\sim} (a_{1,1}^y.1_S + a_{2,1}^y.1_S\epsilon) \ \therefore\ a_{1,1}^x.1_S \overset{\mathbb{Z}}{\sim} a_{1,1}^y.1_S \ \therefore$ $\therefore\ a_{1,1}^x.1_S = a_{1,1}^y.1_S \ \therefore a_{1,1}^x = a_{1,1}^y$. Finally,

$$a_{2,1}^x.1_S\epsilon^2 n = a_{2,1}^y.1_S\epsilon^2 n$$

and $a_{2,1}^x.1_S \overset{\mathbb{Z}}{\sim} a_{2,1}^y.1_S \ \therefore\ a_{2,1}^x.1_S = a_{2,1}^y.1_S \ \therefore a_{2,1}^x = a_{2,1}^y$. So,

$$a_0^x + a_1^x\varepsilon + a_2^x\eta + a_{2,0}^x\varepsilon^2 + a_{1,1}^x\varepsilon\eta + a_{0,2}^x\eta^2 + a_{2,1}^x\varepsilon^2\eta =$$
$$= a_0^y + a_1^y\varepsilon + a_2^y\eta + a_{2,0}^y\varepsilon^2 + a_{1,1}^y\varepsilon\eta + a_{0,2}^y\eta^2 + a_{2,1}^y\varepsilon^2\eta$$

and then we have that Ψ is injective. Therefore, $S \simeq S_2$. □

This ends with our list of examples to understand what is done when proving that some f.g. ring is QFA. In the next chapter, we will start with a theorem that says that *if R is a f.g. ring which is an integral domain, then R is bi-interpretable with $\mathbb{N}$. Moreover, if $a_1, \cdots, a_n$ are generators of R, then there is a formula $F(x_1, \cdots, x_n)$ such that R is a model of $F(a_1, \cdots, a_n)$ and, if S is a integral domain with $b_1, \cdots, b_n \in S$, then $S \models f(b_1, \cdots, b_n) \iff$ there is an isomorphism $R \longrightarrow S$ such that $a_i \mapsto b_i$ for $i \leq n$.* As a sequel, we use this result to obtain a generalization for the previous examples, proving one theorem about a class of QFA rings.

Capítulo 3

Integral Domains and the General Case

As we mentioned at the end of the last chapter, we need an auxiliary result to present QFA-formulas for the class of f.g. rings we are studying. Thus, we divide this chapter into two sections: the first one presents an important result about f.g. rings which are integral domains, and the second one has some comments about those examples in the last chapter and provides a theorem that says that a certain class of f.g. rings is QFA.

3.1 Infinite f.g. integral domains are bi-interpretable with $\mathbb{Z}$

For the result of this section, we firstly tried to prove our claims using elementary arguments. However, some parts still need more research to pull them down to simpler proofs. In the meanwhile, we are using a result due to Björn Poonen in *Uniform First-Order Definitions in Finitely Generated Fields*, in Duke Math. J. (see [Po]).

Theorem 3.1.1 *if R is an infinite f.g. ring which is an integral domain, then R is bi-interpretable with $\mathbb{N}$. Moreover, if $a_1, \cdots, a_n$ are generators of R, then there is a formula $F_R(x_1, \cdots, x_n)$ such that R is a model of $F_R(a_1, \cdots, a_n)$ and, if S is a integral domain with $b_1, \cdots, b_n \in S$, then $S \models F_R(b_1, \cdots, b_n) \iff$ there is an isomorphism $R \longrightarrow S$ such that $a_i \mapsto b_i$ for each $i \in \{1, \cdots, n\}$.*

Proof: We proceed by induction on $n = trdeg_{\mathbb{Z}}(R)$.

Case $n = 0$ and $n = 1$: If char$(R) = 0$, then the base case is $n = 0$, that is, R is an integral domain and Frac(R) is a global field. If char$(R) = p$, then the base case is $n = 1$, that is, R is an integral domain and Frac(R) is a function field (if $n = 0$, then R would be finite). Both cases were solved in [Ru]. □

Case $n + 1$: Suppose the result is true for all f.g. integral domains R with $trdeg_{\mathbb{Z}}(R) = n$, that is, that R is bi-interpretable with $\mathbb{N}$ and if $a_1, \cdots, a_n$ are generators of R, then there is a formula $F_R(x_1, \cdots, x_n)$ such that R is a model of $F_R(a_1, \cdots, a_n)$ and, if S is a f.g. integral domain with $b_1, \cdots, b_n \in S$, then $S \models F_R(b_1, \cdots, b_n) \iff$ there is an isomorphism $R \longrightarrow S$ such that $a_i \mapsto b_i$. We are going to separate into two cases, and then we prove that all cases can be reduced to these two.

Case 1: *$R' = R[x]$ and R' is relatively algebraically closed over R.*

We will prove that $R' := R[x]$ is bi-interpretable with $\mathbb{N}$ by proving the following steps:

Step 1: R is definable. We prove *Step 1* with two claims. The arguments in Claim 1 are a variant of the arguments we can find in [Ni].

Claim 1: *$R[x]/(p)$ is R-isomorphic to $R \iff p = ax + b$ with $b \in R$ and $a \in R$ invertible.*

Proof of Claim 1: ($\Leftarrow$) Suppose that $p = ax + b$ with $b \in R$ and a invertible. Then, we can build the homomorphism

$$\begin{aligned} R[x] &\longrightarrow R \\ f &\mapsto f(-a^{-1}b) \end{aligned}$$

Using the canonical projection $R[x] \longrightarrow R[x]/(p)$ and the Isomorphism Theorem, we can conclude that $R[x]/(p)$ is isomorphic to R. Moreover, it is not hard to see that R is fixed by this isomorphism. Hence, $R[x]/(p)$ is R-isomorphic to R.

($\Rightarrow$) Suppose that we have an isomorphism $R \longrightarrow R[x]/(p)$ that fixes R. Thus, p cannot be a constant, otherwise we could not have injectivity. Since R is fixed by this surjective homomorphism, we have that each equivalence class in $R[x]/(p)$ has to have one constant (actually it is just one). So, for the element x there is a constant c and a polynomial $h(x)$ such that $x - c = h(x).p \in R[x]$. Since we have an equality between polynomials in R and p is not a constant, then $h(x)$ is a constant, say $A \in R$, and $p = ax+b$ for some $a, b \in R$. Then, $x - c = (A.a)x + A.b$ and, therefore, we have $A.a = 1$. Thus, $p = ax + b$ with $b \in R$ and a invertible. This ends the proof of ($\Rightarrow$), and therefore this proves Claim 1. □

Using the definition $x =_p y \Leftrightarrow \exists m \;\; x = y + m.p$ likewise functions $\oplus_p$ and $\otimes_p$, we can interpret $R[x]/(p)$ with $(R[x], \oplus_p, \otimes_p)$. Relativising the formula F_R in the interpretation, we have a formula to define the set

$$C = \{p = ax + b \; ; \; b \in R \; \wedge \exists A \; A.a = 1\}$$

Using this auxiliary set, we can define R in $R[x]$ with the formula

$$r \in R \Longleftrightarrow \forall y \in C \;\; y + r^2 \in C$$

Indeed, if $r \in R$, then $y + r^2 \in C$ for all $y \in C$. If $\forall y \in C \;\; y + r^2 \in C$, then $x + r^2 \in C$. Hence $\deg_R(r) = 0$, otherwise $\deg_R(x + r^2) > 1$, which is a contradiction with $x + r^2 \in C$. So, $r \in R$. □(Step 1)

Step 2: There is a copy R^* of $R[x]$ interpretable in R.

Proof: Since R is interpretable in $\mathbb{N}$, we can relativize the Gödel coding of $\mathbb{N}$ to the interpretation of R in $\mathbb{N}$, namely $(\mathbb{N}, \oplus_R, \otimes_R)$. Each finite sequence of R will have its length saved in the first slot of its code. Then, we define the interpretation with

$$x =_\sim y \Longleftrightarrow \forall i \; (x)_i =_R (y)_i$$

$$x \oplus_\sim y =_\sim z \Longleftrightarrow \forall i \neq 0 \; (x)_i \oplus_R (y)_i =_R (z)_i$$

and

$$x \otimes_\sim y =_\sim z$$

$$\Updownarrow$$

$$\forall i \leq (x)_0 + (y)_0$$

$$\Big(\exists s \; \forall j \; (j = 0 \Rightarrow (s)_j = 0) \wedge (j < i \Rightarrow (s)_{j+1} = (s)_j \oplus_R (x)_{i-j}.(y)_{j+1})\Big)$$

$$\wedge \; (z)_i = (s)_i$$

Thus, we are interpreting $(R[x], +, \times)$ in $\mathbb{N}$ as $(\{\text{finite sequences of } R\}, \oplus_\sim, \otimes_\sim)$. Since R interprets $\mathbb{N}$, we relativize all above formulae to have the formulae of the interpretation of this copy, say R^*, in R. $\square$(Step 2)

Step 3: There is a definable (in R) embedding $\Omega : R \longrightarrow R^*$ identifying R with the constant polynomials.

Proof: Define the graph of $\Omega : R \longrightarrow R^*$ by

$$\text{graph}(\Omega) := \{(a,b)\ ;\ (b)_0 = 1 \wedge (b)_1 = a\}.$$

Note that this definition says that b just has the constant coefficient and that this coefficient is a. So, it does its work. $\square$(Step 3)

Step 4: $R^* \times R \xrightarrow{\Phi} R$ with $(f,a) \mapsto f(a)$ is definable in R.

The graph(Φ) is definable by

$$\{(f,a,b)\,;\, \ulcorner a \in R\urcorner \wedge \ulcorner b \in R\urcorner \wedge (\forall x\ (x)_0 = 1 \wedge (x)_1 = 1 \Rightarrow \ulcorner (x - a^*)|^*(f - b^*)\ \mathit{in}\ R^{*}\urcorner)\}$$

for which the formula $\ulcorner (x - a^*)|^*(f - b^*)\ \mathit{in}\ R^*\urcorner$ is the interpretation of $\ulcorner (x - a)|(f - b)\ \mathit{in}\ R[x]\urcorner$ in $R^* = (\{\text{finite sequences of } R\}, \oplus_\sim, \otimes_\sim)$, since "|" is definable and so is R, and $a^* = \Omega(a)$ and $b^* = \Omega(b)$. $\square$(Step 4)

Step 5: $R[x] \times R \xrightarrow{\Gamma} R$ with $(f,a) \mapsto f(a)$ is definable in $R[x]$.

Analogously, we have

$$\text{graph}(\Gamma) = \{(f,a,b)\ ;\ \ulcorner a \in R\urcorner \wedge \ulcorner b \in R\urcorner \wedge (x-a)|(f-b)\ \mathit{in}\ R\}.$$

Step 6: R^* and $R' = R[x]$ are definably isomorphic in R'.

We construct such isomorphism by doing

$$\begin{gathered} R^* \xrightarrow{\Theta} R[x] \\ f \mapsto g \end{gathered}$$

such that

$$\text{graph}(\Theta) =$$
$$\{(f,g)\ ;\ (\ulcorner (f,a,b) \in\ \text{graph}(\Phi)\urcorner \wedge \ulcorner (g,a,c) \in\ \text{graph}(\Gamma)\urcorner) \Rightarrow b = c\}.$$

Since all these formulae are definable, then we have Step 6 done. $\square$

Gathering the steps: we have that Step 2 and Step 3 together imply that R^*

is bi-interpretable with R, and Step 5 says that R^* is definably isomorphic to $R' = R[x]$. Therefore, $R[x]$ is bi-interpretable with $\mathbb{N}$.

Since $R[x]$ is bi-interpretable with $\mathbb{N}$, then we can build the formula $F_x(x_1, \cdots, x_{n+1})$ using the formulae that define the interpretation of R in $\mathbb{N}$, together with the formula interpreting $\mathbb{N}$ in R, and the formula that defines the isomorphism between R and the interpreted copy of R in the interpreted copy of $\mathbb{N}$[1]. With this, Case 1 holds.$\square$

Case 2: *$R' = R[s,t]/g(s,t)$, R is relatively algebraically closed in R', and g is absolutely irreducible over $R[s,t]$.*

First, as we did before, we want to define R in R'. For this, we make use of the following result we mentioned in the beginning of the chapter.

Theorem 3.1.2 *(Thm. 1.4 in [Po]) For each n natural number, there exists a formula $\psi_n(t_1, \cdots, t_n)$ that when interpreted in a finitely generated field K is true if and only if $t_1, \cdots, t_n$ are algebraically dependent over k.*

As we did in Chapter 1, we can interpret the field of fractions of R', namely $\overline{R'} := Frac(R')$, using formulas to define $\oplus_{\overline{R'}}$ and $\otimes_{\overline{R'}}$ such that $(R', \oplus_{\overline{R'}}, \otimes_{\overline{R'}}) \simeq (\overline{R'}, +, \times)$. Since equality in $\overline{R'}$ is interpreted in R' with the formula $(x_1, x_2) \sim (y_1, y_2) \Leftrightarrow x_1.y_2 = x_2.y_1$, then $\ulcorner x \in R' \urcorner$ is definable in $\overline{R'}$ by $(x_1, x_2) \in R' \Leftrightarrow \exists y \;\; y.x_2 = 1$ (x_2 is invertible). Now, fix generators $a_1, \cdots, a_n$ of R and take a formula $\psi_{n+1}(t_1, \cdots, t_{n+1})$ given by Theorem 3.1.2. Now, do

$$x \in R \Longleftrightarrow \overline{R'} \models (x \in R') \wedge \psi_m(a_1, \cdots, a_m, x)$$

Thus, R is definable in R'. It follows that R' is bi-interpretable with the structure $(R', +, \times, \mathcal{R})$, for which $\mathcal{R}$ is a predicate for R. Let R'' be the interpreted copy of R' in R. Hence, R'' can be viewed as a set of functions on the curve defined by $g(x,y) = 0$. Now, if we define the evaluation $R' \longrightarrow R$ such that $f \mapsto f(p)$ (some p on the curve defined by g), then we can identify R' and R'' by the way they act on the curve. Possibly, we have to consider we are in some degree-d extension of the field of fractions of R, say Frac(R). Let's construct these formulae now. First, to interpret Frac(R) in R', we can use, like in Chapter 1, the formulae

$$E(x_1, x_2, y_1, y_2) \Leftrightarrow \mathcal{R}(x_2) \wedge \mathcal{R}(y_2) \wedge (\neg x_2.y_2 = 0) \wedge (x_1.y_2 = x_2.y_1)$$

[1] This formula will be included in the next version of this thesis.

$$A(x_1, x_2, y_1, y_2, z_1, z_2) \Leftrightarrow E(x_1.y_2 + x_2.y_1, x_2.y_2, z_1, z_2)$$
$$M(x_1, x_2, y_1, y_2, z_1, z_2) \Leftrightarrow E(x_1.y_1, x_2.y_2, z_1, z_2)$$

Then, we use the notation $X := (x_1, x_2),\ Y := (y_1, y_2),\ Z := (z_1, z_2),\ \tilde{0} := (0, 1),\ \tilde{1} := (1, 1)$ to abbreviate the formulae

$$X \oplus Y = Z \Leftrightarrow A(X, Y, Z)$$
$$X \otimes Y = Z \Leftrightarrow M(X, Y, Z)$$

With this considerations, we see that $((R')^2, \tilde{0}, \tilde{1}, \oplus, \otimes) = (\text{Frac}(R), 0, 1, +, \times)$.

Now, for a fixed d, we can build a formula to talk about the total space of all degree-d extentions of Frac(R). Like in chapter zero, we have to build a formula with parameters $\{a_{i,j,k}\}$ which define the multiplication in the degree-d extention. So, we do

$$A_d((X_1, ..., X_d), (Y_1, ..., Y_d), (Z_1, ..., Z_d); \{a_{i,j,k}\}) \Leftrightarrow \bigwedge_{i=1}^{d} X_i \oplus Y_i = Z_i$$

$$M_d((X_1, ..., X_d), (Y_1, ..., Y_d), (Z_1, ..., Z_d); \{a_{i,j,k}\})$$
$$\Updownarrow$$
$$\bigwedge_{l=1}^{d} \sum_{j=1}^{d} \sum_{i=1}^{d} X_j \otimes (Y_i \otimes a_{j,i,l}) = Z_l$$

for which $\sum_{i=1}^{d} B_i := B_1 \oplus B_2 \oplus \cdots \oplus B_d$.
Finally, considering $\tilde{X} := (X_1, ..., X_d)$, $\tilde{Y} := (Y_1, ..., Y_d)$, and $\tilde{Z} := (Z_1, ..., Z_d)$, we define

$$\tilde{X} \oplus_d \tilde{Y} = \tilde{Z} \ \Leftrightarrow A_d(\tilde{X}, \tilde{Y}, \tilde{Z}; \{a_{i,j,k}\})$$
$$\tilde{X} \otimes_d \tilde{Y} = \tilde{Z} \ \Leftrightarrow M_d(\tilde{X}, \tilde{Y}, \tilde{Z}; \{a_{i,j,k}\})$$
$$\forall A, B, C, X, Y, Z \ \big(Y \otimes_a Z = A \wedge X \otimes_d A = B \wedge X \otimes_d Y = C\big) \Rightarrow C \otimes_d Z = B$$
$$\forall A, B \ \big(A \otimes_d B = 0\big) \Rightarrow A = 0 \vee B = 0$$
$$\forall A, B \ A \otimes_d B = B \otimes_d A$$

(Note: We did not add the distributive property of $\otimes_d$ over $\oplus_d$, because they follow from the definition.). In order to see R' as a subring, of this degree-d extension, isomorphic to $R' \times (0, \cdots, 0)$, we add the formula

$$\Big(\bigwedge_{\{(i,j,k)\ ;\ 1 \leq i,j,k \leq n\ \&\ j \neq k\}} a_{i,j,k} = 0 \Big) \wedge \Big(\bigwedge_{\{(i,j,k)\ ;\ 1 \leq i,j,k \leq n\}} a_{i,j,j} = 1 \Big)$$

So, with these definitions, we have that $((R')^{d^2}, \otimes_d, \otimes_d)$ is a degree-d extension of $Frac(R)$ such that R' is viewed as $R' \times (0, \cdots, 0)$.

Since R is bi-int. with $\mathbb{N}$ and $\mathbb{N}$ interprets $R[s,t]/(g(s,t)$, then R interprets $R[s,t]/(g(s,t))$ (we can see $R[x,t]$ as finite sequences with indices from $\mathbb{N} \times \mathbb{N}$ of elements of R equiped with specific sum and product, and then we consider the equivalence relation $x \sim y \Leftrightarrow \exists m \ \ x - y = m.g$). So, let R'' be the interpreted copy of R' in R. Then, construct the isomorphism

$$R' \longrightarrow R''$$

$$f \mapsto h$$

iff for each s and t satisfying $g_a(s,t) = 0$, s and t in some degree-d extension of Frac(R) we have that $f_a(s,t) = h_a(s,t)$. So, the graph of the isomorphism is defined by

$$\{(f,h) \ ; \exists((a_1, a_2)_{i,j,k}) \ \forall i,j,k \ \mathcal{R}((a_1)_{i,j,k}) \wedge \mathcal{R}((a_2)_{i,j,k}) \wedge \neg(a_2)_{i,j,k} = 0$$

$$\& \ \exists A, B \ g_d(x,y) = A(x-s) + B(y-t) \Rightarrow$$
$$\exists C, D \ f_d(x,y) - h_d(x,y) = C(x-s) + D(y-t)\}$$

for which g_d, f_d, h_d are g, f, h when viewed (interpreted) in the degree-d extension of Frac(R) (whose multiplication is defined by the $a_{i,j,k}$), and A, B, C, D lie on this extension. To end with this definition, we just use a definition for the graph of the evaluation map $f_d \mapsto f_d(x,y) = z\}$[2] . With these considerations, we proved that $R[s,t]/(g(s,t))$ is bi-int. with $\mathbb{N}$.

Since $R[s,t]/(g(s,t))$ is bi-interpretable with $\mathbb{N}$, we can proceed with the same argument of Case 1 to construct the QFA-formula $F_{R[s,t]/(g(s,t))}(x_1, \cdots, x_{n+1})$. With this, Case 2 holds. □

Now, we show that any case can be reduced to these two.

Lemma 3.1.1 *If R' is a f.g. integral domain of $trdeg_{\mathbb{Z}}(R') = n+1$, then there is a relatively algebraically closed subring R and two elements $s, t \in R'$ such that $R' = R[s]$ or R[s,t]/(g(s,t)) as an abstract ring.*

Proof: Take $a_1, \cdots, a_{n+1}$ generators of R'. Consider R the algebraic closure of $\{a_1, \cdots, a_n\}$. Since $a_1, \cdots, a_{n+1}$ are generators of R', then $R \subseteq R'$. If a_{n+1} is algebraically independent of R, then $R' = R[a_{n+1}]$ and we are done.

[2] This definition is being fixed and will be included in the next version of this thesis.

If not, then there is some relation $g(a_1, \cdots, a_n, a_{n+1}) = 0$ in R'. We may assume this is the only relation over the generators we have (otherwise we decrease the transcendence degree of R'). Consider $\tilde{R}$ the algebraic closure of $\{a_1, \cdots, a_{n-1}\}$. Now, consider $\tilde{g}(a_n, a_{n+1}) := g(a_1, \cdots, a_n, a_{n+1})$. Therefore, $R' = \tilde{R}[a_n, a_{n+1}]/(g(a_n, a_{n+1}))$, and we are done. □

So, any case can be viewed like the cases above, and then the result holds by the induction principle. ∎

3.2 The General Case

As we mentioned before, all of the previous examples of QFA rings have something in commom. We shall now make explicit their similarity. In this section, we will consider finitely generated rings R' such that there is a nilpotent prime ideal $I \subset R'$, *id est* there is $n > 0$ such that $I^n = 0$ and $R'/I = R$ is an integral domain. Observe that, for instance, the last ring of the last chapter is the case for which $R' := \mathbb{Z}[\varepsilon, \eta]/(\varepsilon^3, \eta^3, \varepsilon\eta^2)$, $I = (\varepsilon, \eta)$, and $R = \mathbb{Z}$. Now, let's think about what is going on among the already presented arguments. All of the constructions of the QFA-sentences until now involve relations between the elements $x_1, \cdots, x_l$ induced by the ideals I, I^2,$\cdots$, I^{n-1}. Furthermore, one can realize that we always added the sentences

$$\begin{aligned}\varphi_{\mathbb{Z}}: \ & \forall x, y, z \ \ (x < y \ \Leftrightarrow \exists n_1, n_2, n_3, n_4 \ \ y \overset{\mathbb{Z}}{\sim} x + 1 + n_1^2 + n_2^2 + n_3^2 + n_4^2) \wedge \\ & ((x < y) \wedge (y < z) \ \Rightarrow x < z) \wedge ((0 < z) \wedge (x < y) \ \Rightarrow zx < zy) \wedge \\ & (x < y \ \Rightarrow x + z < y + z) \wedge \\ & ((x < y) \dot{\vee} (x = y) \dot{\vee} (x = y + 1) \dot{\vee} (y + 1 < x)) \wedge \\ & (\forall z \exists w \ \ z < w \wedge (\forall x \ \ 1 < x \Rightarrow ((\exists r \ \ w = rx) \Rightarrow (\exists s \ \ x = 2s))))\end{aligned} \tag{3.2.1}$$

whose relativisation was used to state that the equivalent classes interpret the rational integers. With $\varphi_{\mathbb{Z}}$ in hands we used the relations induced by those ideals to build our sentences.

Due to Theorem 3.1.1, we will assume that in the general case we know $F_R(x_1, \cdots, x_l)$, and then try to find a QFA-formula for R'. For this, we will use some already known facts of Computational Algebra we find in [BV]. Indeed, since $R[x_1, \cdots, x_l]$ is a R-module and, for each $1 \leq j \leq n-1$, I^j/I^{j+1} is a R-submodule of $R[x_1, \cdots, x_l]$, then we can find, with Buchberger's algorithm, generators for I^j/I^{j+1}. Using this, we have

Theorem 3.2.1 *Let $\mathcal{K}$ be the class of finitely generated rings. Consider $R' \in \mathcal{K}$ such that R' is finitely generated over R, an integral domain, by elements $x_1, ..., x_n$ of R' and that $I = (x_1, ..., x_n)$ is a nilpotent, prime ideal for which $R'/I = R$ (as an R-algebra). Then, we can contruct a QFA-formula for R'.*

Proof: By the theorem about integral domains, we have a QFA-formula for R and a set of generators $(a_1, \cdots, a_l)$, namely $F_R(x_1, \cdots, x_l)$. We want to construct a QFA-formula for R', namely $F_{R'}(s_1, \cdots, s_l, t_1, \cdots, t_n)$. Consider the ideal $I(x_1, \cdots, x_n/R) := \{f \in R[y_1, \cdots, y_n] \; ; \; f(x_1, \cdots, x_n) = 0 \textit{ in } R'\}$. Since $I(x_1, \cdots, x_n/R)$ is f.g., we can take generators $g_1(y_1, \cdots, y_n)$,..., $g_k(y_1, \cdots, y_n)$ for $I(x_1, \cdots, x_n/R)$. For each i, we rewrite the g_i's as $g_i(y_1, \cdots, y_n) = h_i(y_1, \cdots, y_n, a_1, \cdots, a_l)$, for which the h_i's are in $\mathbb{Z}[x_1, \cdots, x_{n+l}]$. Then, we could define $F_{R'}(s_1, \cdots, s_l, t_1, \cdots, t_n)$ as

$$\begin{aligned} F_{R'}(s_1, \cdots, s_l, t_1, \cdots, t_n) : \; & \tilde{F_R}(s_1, \cdots, s_l) \wedge \\ & \bigwedge_{i=1}^{k} h_i(t_1, \cdots, t_n, a_1, \cdots, a_l) \wedge \\ & \ulcorner \textit{there is no other relation} \urcorner \end{aligned} \tag{3.2.2}$$

for which $\tilde{F_R}(x_1, \cdots, x_l)$ is the relativization of $F_R(x_1, \cdots, x_l)$ when equality is replaced by $\sim$ such that $x \sim y \Leftrightarrow x - y \in I$ ($\ulcorner f \in I \urcorner$ is definable by $\exists (a_\beta)_{0<|\beta|<n, \beta \in n^\ell} \; f = \sum a_\beta x^\beta$). Then, if we define $\ulcorner$*there is no other relations*$\urcorner$, we are done. Indeed, we can do this by defining $\ulcorner x$ is R-linearly independent on $u_1, \cdots, u_p \urcorner$, for we could say "there is not a relation h such that h is R-independent on the h_i's". Remember that I, as an R-module, is isomorphic to its graded ring $\mathrm{gr}(I) = I/I^2 \oplus I^2/I^3 \oplus ... \oplus I^{n-1}/I^n$. Indeed, we can use Buchberger's algorithm to find a basis $x_{(1,1)}, \cdots, x_{(1,e_1)}$ for I/I^2 starting from $(x_1, \cdots, x_n)$. Using the same argument, we can extract a basis $x_{(2,1)}, \cdots, x_{(2,e_2)}$ for I^2/I^3 from $(x_1^2, x_1x_2, x_1x_3, ..., x_1x_n, x_2^2, ..., x_nx_{n-1}, x_n^2)$. We repeat this argument until we get a basis $(x_{(n-1,1)}, \cdots, x_{(n-1,e_{n-1})})$ for $I^{n-1}/I^n = I^{n-1}$. So, if we set $B = (x_{(1,1)}, \cdots, x_{(1,e_1)}, \ldots, x_{(n-1,1)}, \cdots, x_{(n-1,e_{n-1})})$, then for each $i \in \{1, \cdots, n-1\}$ the reduction maps $B_i := (x_{(i,1)}, \cdots, x_{(1,e_i)}) \longrightarrow B_i/I^{i+1}$ are one-to-one. Therefore, B is a basis to I. Now, we define I with $x \in I \Leftrightarrow \exists m_1, \cdots, m_n \;\; x = \sum_{q=1}^{n} m_q.B|_q$, for which $B|_q$ is the q^{th} coordinate of B. Likewise, the sentences $\ulcorner x \in I^j \urcorner$ are definable for each j. Furthermore, we can define $x \in I^j/I^{j+1}$ by

$$x \in I^j/I^{j+1} \Longleftrightarrow \exists m_1, \cdots, m_{e_i} \;\; x = \sum_{z=1}^{e_i} m_z x_{(i,z)}$$

So, for each $d > 0$ and $j \in \{1, \cdots, n{-}1\}$ we can define sentences $\delta_j(\rho_1, \cdots, \rho_d)$ that say "$\rho_1, \cdots, \rho_d \in I^j/I^{j+1}$ are R-linearly independent " by

$$\delta_j(\rho_1, \cdots, \rho_d) \Longleftrightarrow \ \exists b_1, \cdots, b_d \ (b_1\rho_1 + \cdots + b_d\rho_d \in I^{j+1} \Rightarrow \bigwedge_{i=1}^{d} b_i \in I^{j+1})$$

Therefore, since $I \simeq \mathrm{gr}(I)$ as R'/I-modules and $R'/I = R$, then "$\rho_1, \cdots, \rho_d$ are R-linearly independent " is equivalent to

$$\bigwedge_{j=1}^{n-1} \delta_j(\rho_1, \cdots, \rho_d)$$

Hence, for each $d > 0$ the sentences $\Theta_d(\rho_1, \cdots, \rho_d)$: $\ulcorner \rho_1, \cdots, \rho_d$ are R-linearly independent$\urcorner$ is definable, and so is $\ulcorner$*there is no other relations*$\urcorner$.

Finally, let S be a f.g. ring with $c_1, \cdots, c_l, b_1, \cdots, b_n \in S$.
If $S \models F_{R'}(c_1, \cdots, c_l, b_1, \cdots, b_n)$, then, by $\tilde{F_R}(c_1, \cdots, c_l)$, we have that $c_1, \cdots, c_l$ are generators of $S/(b_1, \cdots, b_n)$ and there is an isomorphism $S/(b_1, \cdots, b_n) \longrightarrow R$ such that $c_i \mapsto a_i$ for each i. By the other part of $F_{R'}(c_1, \cdots, c_l, b_1, \cdots, b_n)$ ensures that $b_1, \cdots, b_n$ satisfy the same relations over $S/(b_1, \cdots, b_n) \simeq R$ that the fixed generators $g_1, \cdots, g_n$ of I in R'. Then, $R \longrightarrow S$ defined by $a_i \mapsto c_i$ and $g_i \mapsto b_i$ is an isomorphism. Since the converse is trivial, we have that $F_{R'}(s_1, \cdots, s_l, t_1, \cdots, t_n)$ is a QFA-formula for R' ■

Capítulo 4

Appendix

4.1 $\mathbb{Z}[\varepsilon]/(\varepsilon^2)$ is not biinterpretable with $\mathbb{Z}$

Now we are going to prove the assertion that name this section. For this, we are going to present arguments we got from "*(Non)-bi-interpretability of infinite finitely generated commutative rings with* $\mathbb{N}$", through pritave communication, due to Matthias Aschenbrenner & Thomas Scanlon.

Suppose that $\phi_{\mathbb{Z}}$ is a QFA-sentence for $\mathbb{Z}$. As we know, we can use $\phi_{\mathbb{Z}}$ to construct a QFA-sentence for the ring $S = \mathbb{Z}[\varepsilon]/(\varepsilon^2)$. However, we afirmed that there is not a biinterpretation between S and $\mathbb{Z}$. Now we are going to prove this in the following proposition as a consequence of lemmas.

Proposition 4.1.1 $\mathbb{Z}[\varepsilon]/(\varepsilon^2)$ *is not biinterpretable with* $\mathbb{Z}$*, even using parameters.*

Proof: Let's begin with this lemma

Lemma 4.1.1 *Let k be an integral domain of characteristic zero, R a finitely generated k-algebra which is also an integral domain of characteristic zero, and $t \in R$ transcendental over k. Then, there exists a k-derivation $\partial : R \to R$ such that $\partial t \neq 0$.*

Proof: (Lemma 4.1.1) Let $t_1, \cdots, t_n$ be a system of generators for R over k with $t_1 = t$. Let K be the field of fractions of R. Then, as $\mathrm{char}(k) = 0$ and t is transcendental over k, then there exists a k-derivative $D : K \longrightarrow K$

with $D(t) = 1$ and $D(t_i) = \frac{a_i}{b_i}$ for some $a_i, b_i \in R$. Consider

$$\widetilde{D} := \left(\prod_{i=1}^{n} b_i\right) \cdot D$$

Thus, $\widetilde{D} : K \longrightarrow K$ is still a k-derivative and $\partial := \widetilde{D}|_R : R \longrightarrow K$ actually takes values in R. Indeed, if $\alpha \in R$, then we may write $\alpha = f(t_1, \cdots, t_n)$ for some polynomial $f \in k[X_1, \cdots, X_n]$. So,

$$\widetilde{D}(\alpha) = \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(t_1, \cdots, t_n) \cdot \widetilde{D}(t_i) = \sum_{i=1}^{n} \frac{\partial f}{\partial x_i}(t_1, \cdots, t_n) \cdot \left(\prod_{i=1}^{n} b_i\right) \cdot a_i$$

which is in R and, moreover, $\widetilde{D}(t) = \prod_{i=1}^{n} b_i \neq 0$. □

Lemma 4.1.2 *If k is an integral domain of characteristic zero, R is also an integral of characteristic zero, $k \subseteq R$ is a subring of R, $t \in R$ transcendental over k, then there is a limit ultrapower ${}^*\mathcal{R} \succeq R$ and a k-derivation $\partial : {}^*\mathcal{R} \to {}^*\mathcal{R}$ such that $\partial t \neq 0$.*

Proof: (Lemma 4.1.2) Consider $I := \{S \subseteq R \,;\, S\ is\ f.g.\ k{-}algebra\ and\ t \in S\}$. For $S \in I$, set $(S) := \{T \subseteq R \,;\, T \in I\ and\ S \subseteq T\}$. Let $\mathcal{C}$ be the filter generated by $\{(S) \,;\, S \in I\}$. Then, there is an ultrafilter $\mathcal{U}$ that has $\mathcal{C}$. For $S \in I$ let $D_S : S \longrightarrow S$ be a k-derivation with $D_S(t) \neq 0$, provided by Lemma 4.1.1. Note that $\prod_{S \in I}{}_{\mathcal{U}}\, S \subseteq R^{\mathcal{U}}$, for which $R^{\mathcal{U}}$ is the ultrapower of R relative to $\mathcal{U}$. Hence, $\prod_{\mathcal{U}} D_S$ is a partial function $R^{\mathcal{U}} \longrightarrow R^{\mathcal{U}}$ whose domain is $\prod_{S \in I}{}_{\mathcal{U}}\, S$. Via the diagonal embedding

$$\Delta : R \longrightarrow R^{\mathcal{U}}$$

$$r \mapsto (r)_{S \in I}$$

we have that $\Delta(R) \subseteq \prod_{S \in I}{}_{\mathcal{U}}\, S$ since k and r are in R $(k[t, r]) \in \mathcal{C} \subseteq \mathcal{U}$. Recall that we define $\mathcal{U}lt(R, \alpha)$ by considering: for $\alpha = 0$, put $\mathcal{U}lt(R, 0) := R$; given this definition for some α, then for its successor put $\mathcal{U}lt(R, \alpha^+) := \mathcal{U}lt(R, \alpha)^{\mathcal{U}}$; and finally $\mathcal{U}lt(R, \lambda) := \varinjlim_{\alpha < \lambda} \mathcal{U}lt(R, \alpha)$ for λ a limit when the limit is taken along the diagonal embeddings. Define $D : R \longrightarrow R^{\mathcal{U}} = \mathcal{U}lt(R,1)$ as the composit of $P := \prod_{S \in I}^{\mathcal{U}} D_S$ with the diagonal embedding

$$\begin{tikzcd}
R \arrow[r, "\Delta"] \arrow[dr, "D"'] & R^{\mathcal{U}} \arrow[d, "P"] \\
 & R^{\mathcal{U}}
\end{tikzcd}$$

by the above considerations, D is a k-derivation over R and by Łoś's theorem, $Dt \neq 0$.

Let $\partial := \mathcal{U}lt(D,\omega) : \mathcal{U}lt(R,\omega) \longrightarrow \mathcal{U}lt(R^{\mathcal{U}},\omega) = \mathcal{U}lt(R,\omega)$. Then, the diagram

$$\begin{tikzcd}
R \arrow[r, "D"] \arrow[d] & R^{\mathcal{U}} \arrow[d, "\iota"] \\
\mathcal{U}lt(R,\omega) \arrow[r, "\partial"] & \mathcal{U}lt(R^{\mathcal{U}},\omega)
\end{tikzcd}$$

commutes and, hence, $\partial(t) \neq 0$. □

Lemma 4.1.3 (Beth definability) *Let M be an L-structure and $A \subseteq M$ some subset. If A is L-definable, then if P is a new predicate, M is considered as a $L(P)$-structure via $P(M) := A$ and, moreover, if $N \succeq_{L(P)} M$ is any elementary extension of M in $L(P)$ and $\sigma : N \to N$ is an L-automorphism of N, then one must have $\sigma(P(N)) \subseteq P(N)$.*

The proof of this lemma can be found in Hodges [Ho].

Lemma 4.1.4 *If the $\mathcal{L}$-structure M is biinterpretable with $(\mathbb{Z}, +, \cdot, 0, 1)$, $f : M \to M$ is a $\mathcal{L}$-definable function and $a \in M$, then $\mathcal{O}_f(a) := \{f^{on}(a);\ n \in \mathbb{N}\}$ is $\mathcal{L}$-definable.*

Proof: (Lemma 4.1.4) Using Gödel coding of sequences in $\mathbb{N}$, one sees that the orbit of a point under a definable function is definable in the interpretation of M in $\mathbb{N}$. By biinterpretability, any set defined in the interpretation is already $\mathcal{L}$-definable. □

Lemma 4.1.5 *If $(\mathbb{Z}[\varepsilon]/(\varepsilon^2), +, \cdot, 0, 1, \varepsilon)$ were biinterpretable with $\mathbb{N}$, then $\mathbb{Z}$ considered as a subring of $\mathbb{Z}[\varepsilon]/(\varepsilon^2)$ would be $\mathcal{L}$-definable.*

Proof: (Lemma 4.1.5) Using the notation like in Lemma 4, we have that

$$\mathbb{Z} = \mathcal{O}_{x\mapsto x+1}(0) \cup \mathcal{O}_{x\mapsto x-1}(0)$$

Applying Lemma 4 for these two orbits, we have that $\mathbb{Z}$ would be $\mathcal{L}$-definable. □

Lemma 4.1.6 *There exists a limit ultrapower* $^*\mathbb{Z} \succeq \mathbb{Z}$ *of* $\mathbb{Z}$ *with a non trivial derivative* $D :^*\mathbb{Z} \to^*\mathbb{Z}$.

Proof: (Lemma 4.1.6) Let $R \succ \mathbb{Z}$ be any proper ultrapower of $\mathbb{Z}$ with $t \in R \setminus \mathbb{Z}$. Thus, we can apply Lemma 4.1.2 for$R$, t and $k = \mathbb{Z}$. □

Lemma 4.1.7 *There exists a limit ultrapower* $^*R \succeq \mathbb{Z}[\varepsilon]/(\varepsilon^2)$ *and an automorphism* $\sigma :^*R \to^*R$ *fixing* $\mathbb{Z}[\varepsilon]/(\varepsilon^2)$ *pointwise but having* $\sigma(^*\mathbb{Z}) \not\subseteq^*\mathbb{Z}$.

Proof: (Lemma 4.1.7) Let $D : {}^*\mathbb{Z} \to {}^*\mathbb{Z}$ be the derivation of Lemma 4.1.6. Then,

$$\sigma : (^*\mathbb{Z})[\varepsilon]/(\varepsilon^2) \longrightarrow (^*\mathbb{Z})[\varepsilon]/(\varepsilon^2)$$
$$x + \varepsilon y \mapsto x + (Dx + y)\varepsilon$$

is an automorphism with inverse $x+\varepsilon y \mapsto x+(y-Dx)\varepsilon$. Since D is nontrivial, there exists $t \in^*\mathbb{Z}$ with $Dt \neq 0$. So,

$$\sigma(t) = t + Dt\varepsilon \notin^*\mathbb{Z} \quad \square.$$

Finally, we can go back to prove the proposition.

Proof: (Proposition) Suppose that $\mathbb{Z}[\varepsilon]/(\varepsilon^2)$ is biinterpretable with $\mathbb{Z}$. By Lemma 4.1.5, $\mathbb{Z}$ is definable. Choosing P as a new predicate to $\mathbb{Z}$, by Beth definability, if $N \succeq_{\mathcal{L}(P)} M$ is any elementary extension of M in $\mathcal{L}(P)$ and $\sigma : N \to N$ is an $\mathcal{L}$-automorphism of N, then one must have $\sigma(P(N)) \subseteq P(N)$. But this contradicts Lemma 4.1.7, that says that $\exists^*\mathcal{R} \succeq \mathbb{Z}[\varepsilon]/(\varepsilon^2)$, $\sigma \in\ Aut(^*\mathcal{R})$, and $\sigma(^*\mathbb{Z}) \not\subseteq^* \mathbb{Z}$. Then the proposition is true. ■

References

[Ju] Robinson, J. *Definability and decision problems in arithmetic*, J. Symb. Logic vol. 14 (1949) pp. 98-114.

[Vää] Väänänen, J. *A Short Course on Finite Model Theory*, available on: www.math.helsinki.fi/logic/people/jouko.vaananen/shortcourse.pdf .

[SM] Scanlon, T. & Aschenbrenner, M. *(Non)-bi-interpretability of infinite finitely generated commutative rings with* $\mathbb{N}$, in preparation.

[Ho] Hodges, W. *Model theory*, Cambridge Univ. Press.

[Sc] Scanlon, T. *Infinite finitely generated fields are biinterpretable with* $\mathbb{N}$, J. Amer. Math. Soc. 21 (2008) 893-908.

[Po] Poonen, B. *Uniform first-order definitions in finitely generated fields*, Duke Math. J. Volume 138, Number 1 (2007), 1-21.

[Ra] Robinson, R.M. *Undecidable rings*, Trans. Amer. Math. Soc. vol. 70 (1951) pp. 137-159.

[Ru] Rumely, R.S. *Undecidability and definability for the theory of global fields*, Trans. Amer. Math. Soc. 262 (1980) (1), pp. 195-217

[Ni] Nies, A. *Describing Groups.* Bull. Symb. Logic 13 no 3 (2007), 305-339

[BV] Becker, T & Weispfenning, V. *Gröbner Bases*, Springer Graduate Texts in Mathematics 141.(1998).

[Ka] Kaye, R. *Models of Peano Arithmetic*, Clarendon Press, Oxford University Press edition (1991).

[IR] Ireland, K.F. & Rosen, M.I. *A classical introduction to modern number theory*, Springer Science & Business, 1990.