

UTRECHT UNIVERSITY

DEPARTMENT OF MATHEMATICS

BACHELOR THESIS

---

# Primes in Nonstandard Models of Open Induction

---

*Author:*  
Martijn DEN BESTEN

*Supervisor:*  
Dr. Jaap VAN OOSTEN

August, 2014

# Contents

<b>1</b>	<b>Introduction</b>	<b>2</b>
<b>2</b>	<b>Background, definitions and notation</b>	<b>4</b>
2.1	General definitions . . . . .	4
2.2	Irreducibles, primes and maximal elements . . . . .	5
<b>3</b>	<b>Shepherdson's theorem</b>	<b>8</b>
<b>4</b>	<b>The constructions</b>	<b>11</b>
4.1	Wilkie's construction . . . . .	11
4.1.1	Preserving properties . . . . .	12
4.2	The $\hat{\mathbb{Z}}$ -construction . . . . .	14
4.2.1	Preserving properties . . . . .	16
4.3	Adding a prime . . . . .	19
4.3.1	Preserving properties . . . . .	20
4.4	Eliminating a prime . . . . .	20
4.4.1	Preserving properties . . . . .	22
4.5	Extending to a model of open induction . . . . .	23
4.5.1	Preserving properties . . . . .	25
<b>5</b>	<b>The main theorems</b>	<b>27</b>

# Chapter 1

## Introduction

Many formal systems are studied with a particular interpretation in mind. For example, the formal theory of sets is intended to give rigor to our intuitive notion of grouping together objects that share a certain property. When a theory has such an intended interpretation, this interpretation is called the standard model. The system of first order Peano arithmetic is another case where there exists an intended interpretation. The language of Peano arithmetic consists of the symbols  $0, 1, +, \cdot$  and has the following axioms.

1.  $\forall x \neg(x + 1 = 0)$
2.  $\forall xy(x + 1 = y + 1 \rightarrow x = y)$
3.  $\forall x(x + 0 = x)$
4.  $\forall xy(x + (y + 1) = (x + y) + 1)$
5.  $\forall x(x \cdot 0 = 0)$
6.  $\forall xy(x \cdot (y + 1) = (x \cdot y) + x)$
7.  $\forall \vec{x}[(\varphi(0, \vec{x}) \wedge \forall y(\varphi(y, \vec{x}) \rightarrow \varphi(y + 1, \vec{x}))) \rightarrow \forall y\varphi(y, \vec{x})]$

The last line is not just a single axiom, but stands for an infinite number of axioms, known as the induction axioms. It is meant to be interpreted as representing an axiom for every possible formula  $\varphi$ . The standard model of Peano arithmetic is the set of natural numbers. A nonstandard model is an interpretation of a system that is not isomorphic to the intended model. In a series of papers from 1922 to 1934, Thoralf Skolem introduced nonstandard models of set theory and arithmetic. In the case of Peano arithmetic, Skolem viewed the existence of such nonstandard models as a failure of the formal system to fully capture the intended interpretation. Nonetheless, nonstandard models have been used for finding new results in other branches of mathematics, in addition to being interesting mathematical structures in their own right. This thesis is not concerned with the nonstandard models of Peano arithmetic, but with the nonstandard models of a fraction of Peano arithmetic, where certain limitations

have been put on the induction axioms. This slightly weaker system of arithmetic is called *open induction*. To be precise, we study rings whose nonnegative part satisfies the axioms of open induction. The language of open induction consists of the symbols  $0, 1, +, \cdot, <$ , but for convenience symbols as  $>, \leq, \geq$  will also be used. These are the axioms of open induction.

1.  $\forall xyz(x + (y + z) = (x + y) + z \wedge x \cdot (y \cdot z) = (x \cdot y) \cdot z)$
2.  $\forall xy(x + y = y + x \wedge x \cdot y = y \cdot x)$
3.  $\forall xyz(x \cdot (y + z) = (x \cdot y) + (x \cdot z))$
4.  $\forall x(x + 0 = x \wedge x \cdot 1 = x \wedge x \cdot 0 = 0)$
5.  $\forall xyz(x < y \wedge y < z \rightarrow x < z)$
6.  $\forall x \neg(x < x)$
7.  $\forall xy(x < y \wedge x = y \wedge y < x)$
8.  $\forall xyz(x < y \rightarrow x + z < y + z)$
9.  $\forall xyz(0 < z \wedge x < y \rightarrow x \cdot z < y \cdot z)$
10.  $\forall xy(x < y \rightarrow \exists z(x + z = y))$
11.  $\forall x(0 \leq x)$
12.  $\forall x(0 < x \leftrightarrow 1 \leq x)$
13.  $\forall \vec{x}[(\varphi(0, \vec{x}) \wedge \forall y(\varphi(y, \vec{x}) \rightarrow \varphi(y + 1, \vec{x}))) \rightarrow \forall y \varphi(y, \vec{x})]$  (For  $\varphi$  open.)

Again, the last line represents an infinite number of axioms, but this time only for those formulas  $\varphi$  which are open, meaning they are free of quantifiers. This of course explains the term open induction. The remaining axioms are known as  $PA^-$  and differ from those of Peano arithmetic only because they capture some essential properties of the natural numbers that can be proven using the axioms of Peano arithmetic, but need to be added manually to the axioms of open induction.

In this thesis the focus lies on the behavior of primes in models of open induction. A great portion of it is dedicated to developing techniques for constructing models in which primes display some of interesting properties. A significant part of this is based on the work of Macintyre and Marker [5], but much material has been added or altered to produce a more or less self-contained study of the subject.

## Chapter 2

# Background, definitions and notation

### 2.1 General definitions

In this chapter we will discuss the basic concepts and definitions that are needed in the upcoming chapters.

Most of the mathematical structures we will encounter are members of the class of discretely ordered rings.

**Definition 2.1.1.** *The class of discretely ordered rings,  $DOR$ , is the class of those rings whose nonnegative part satisfies the axioms of  $PA^-$ .*

Ordered rings obey the usual axioms for commutative rings and linear orders and in these rings the operations  $+$  and  $\cdot$  respect the order of the ring. An ordered ring is called discrete if 1 is the smallest element greater than 0 in this ring. A ring  $R \in DOR$  has a unique subring isomorphic to  $\mathbb{Z}$ , by identifying  $n \in \mathbb{Z}_{>0}$  with  $1 + 1 + \dots + 1 \in R$ , where the last expression has  $n$  summands. We denote this subring by  $\mathbb{Z}$  as well. The elements of  $\mathbb{Z} \subset R$  are called the finite or standard elements of  $R$  and the elements of  $R \setminus \mathbb{Z}$  are called infinite or nonstandard. We write  $F(R)$  for the ordered field of fractions of  $R \in DOR$  and  $C(R)$  for the real closure of  $F(R)$ .

**Definition 2.1.2.** *Let  $R \in DOR$ . The real closure of  $F(R)$  is the unique ordered field  $C(R)$ , such that  $C(R)$  is not algebraically closed, but the field extension  $C(R)(\sqrt{-1})$  is the algebraic closure of  $F(R)$ .*

The real closure is the nonstandard analog of the algebraic real numbers. We shall not attempt to prove the asserted uniqueness here.

A special subclass of the discretely ordered rings is formed by the so-called  $\mathbb{Z}$ -rings.

**Definition 2.1.3.** *The class of  $\mathbb{Z}$ -rings,  $ZR$ , is the class of those  $R \in DOR$  which satisfy the division-with-remainder property when dividing by an element*

$n \in \mathbb{Z}$ , with  $n > 0$ . So  $R \in ZR$  if

$$R \models \forall x \exists y r [x = ny + r \wedge 0 \leq r < n]$$

holds for each  $n > 0$  in  $\mathbb{Z}$ .

It will turn out that the  $\mathbb{Z}$ -rings play an important role in the construction of models of open induction. Which brings us to the last important class of rings.

**Definition 2.1.4.** *The class of models of open induction,  $OI$ , is the class of those  $R \in DOR$  such that the nonnegative part of  $R$  fulfills the induction axioms for all open formulas.*

Remember that a polynomial is monic if it is a polynomial in one variable, in which the leading coefficient is equal to 1.

**Definition 2.1.5.** *A ring  $R \in DOR$  is called normal if every root of a nonzero monic polynomial in  $R[X]$  that lies in  $F(R)$  automatically lies in  $R$ .*

It is a well known fact that the ring  $\mathbb{Z}$  is normal. However, not all models of open induction share this property. For example, Shepherdson [7] constructed a model of open induction in which there exists a solution to the equation

$$x^2 - 2y^2 = 0, xy \neq 0$$

Such a model cannot be normal, as the absolute value of the fraction  $\frac{x}{y}$  must be smaller than 1 and is consequently not an element of  $R$ . We will therefore put in extra effort to ensure that our models are normal, to preserve more of the arithmetic structure of  $\mathbb{Z}$ .

All of the constructions involving discretely ordered rings are meant to be taking place inside a certain large field  $L$ . Unfortunately, it is beyond the scope of this thesis to discuss  $L$ . There are, however, a few instances in which we make use of the properties of  $L$ . In these cases, the proof is omitted and the lemmas will be marked with a  $\blacklozenge$ . For each lemma or theorem where a proof or proof sketch is available from one of the sources, it is cited next to the word “**Proof.**”.

## 2.2 Irreducibles, primes and maximal elements

Since the the main theorems involve elements which are maximal, prime or irreducible, some more definitions are in order.

**Definition 2.2.1.** *Let  $R \in DOR$ . The element  $p \in R$  is irreducible if it is unequal to 0, 1 or  $-1$  and whenever  $p = rs$ , with  $r, s \in R$ , then  $r$  or  $s$  is a unit.*

The next definition will not play big role, but is needed for a later lemma and fits in naturally. Remember that an element is nilpotent if there exists a natural number such that the element raised to this natural number yields 0.

**Definition 2.2.2.** *Let  $R \in DOR$ . The element  $p \in R$  is semiprime if it is irreducible and  $R/pR$  has no nonzero nilpotents.*

Notice that  $R/pR$  having no nilpotent elements is equivalent to saying that for  $r \in R$  and  $n \in \mathbb{Z}_{>0}$ ,  $p \mid r^n$  implies that  $p \mid r$ .

**Definition 2.2.3.** *Let  $R \in DOR$ . The element  $p \in R$  is prime if it is unequal to  $0, 1$  or  $-1$  and  $R/pR$  is a domain.*

The statement that  $R/pR$  is a domain is equivalent to saying that for  $r, s \in R$ ,  $p \mid rs$  implies that  $p \mid r$  or  $p \mid s$ .

**Definition 2.2.4.** *Let  $R \in DOR$ . The element  $p \in R$  is maximal if it is unequal to  $0, 1$  or  $-1$  and  $R/pR$  is a field.*

Saying that  $R/pR$  is a field is equivalent to saying that whenever  $p \nmid r$ , with  $r \in R$ , there exist  $s, t \in R$  such that  $rs = 1 + pt$ .

There exists an obvious hierarchy between these types of elements. Since all fields are domains, maximality implies primality. Furthermore, if  $p, r, s \in R$  with  $p$  prime and  $p = rs$ , then  $p \mid rs$ , so that  $p \mid r$  or  $p \mid s$ . Suppose  $p \mid r$ , then  $s \frac{r}{p} = 1$ . Hence  $s$  is a unit and we see that primality implies irreducibility. These definitions turn out to be equivalent for models of Peano arithmetic, as we shall demonstrate.

In the next lemma we will be using the least number principle. The least number principle is equivalent to the principle of induction and states that every nonempty subset of the nonnegative elements of a ring  $R \in DOR$  has a least element. In models of open induction the least number principle applies to sets which can be defined by a quantifier free sentence.

**Lemma 2.2.5.** *Every model of open induction satisfies the division-with-remainder property.*

**Proof.** [5] Suppose  $R \in IO$ . Let  $x \in R$ , with  $x \geq 0$  and  $\alpha > 0$ . We want to find  $u, v \in R$ , such that  $x = u\alpha + v$ , with  $0 \leq v < \alpha$ . To this end we apply the least number principle to the set

$$A = \{y \in R : y \geq 0 \wedge \alpha y > x\}.$$

Notice that  $A$  is defined by a quantifier free sentence. Notice also that  $A$  is nonempty, since it contains the element  $x + 1$ . We conclude that it has a least element  $y_0$ . Let  $r = x - \alpha(y_0 - 1)$ . Then  $x = \alpha(y_0 - 1) + r$ . Furthermore  $r < \alpha$  because  $y_0 \in A$  and  $0 \leq r$ , because  $y_0$  is minimal. The proof for  $x < 0$  is similar.  $\square$

As the property of being a  $\mathbb{Z}$ -ring is a special case of the division-with-remainder property, we have the following corollary.

**Corollary 2.2.6.** *Every model of open induction is a  $\mathbb{Z}$ -ring.*

It turns out that every  $\mathbb{Z}$ -ring can be extended to a model of open induction, as we shall see later on. For now, we only need the following corollary, as it is used in the next two theorems.

**Corollary 2.2.7.** *Every model of Peano arithmetic satisfies the division-with-remainder property.*

**Theorem 2.2.8.** *Let  $R$  be a model of Peano arithmetic and let  $p \in R$  be prime. Then  $p$  is maximal.*

**Proof.** Let  $r \in R$ , with  $p \nmid r$ . For convenience, let  $r > 0$  and  $p > 0$ . The proof for the other cases is similar. We apply the least number principle to the set

$$A = \{x \in R : x > 0 \wedge \exists st(rs = x + pt \wedge p \nmid s)\}$$

The set  $A$  is nonempty, since  $r \in A$ , by setting  $s = p + 1$  and  $t = r$ . Therefore  $A$  has a least element  $x_0$  and there exist  $s_0, t_0 \in R$  satisfying  $rs_0 = x_0 + pt_0$  and  $p \nmid s_0$ . We use division with remainder to find  $u, v \in R$  such that  $p = ux_0 + v$ , with  $0 \leq v < x_0$ . Substituting  $x_0 = rs_0 - pt_0$  into this equation and rearranging gives

$$-us_0r = v - (ut_0 + 1)p$$

By minimality of  $x_0$ ,  $v$  must be 0. Hence  $p = ux_0$ . Since  $p$  is prime and therefore irreducible, either  $x_0 = p$  or  $x_0 = 1$ . Suppose that the former is the case. Then  $rs_0 = p + pt_0$ . But this is impossible as  $p$  is prime and both  $p \nmid r$  and  $p \nmid s_0$ . We conclude that  $x_0 = 1$ . Hence  $rs_0 = 1 + pt_0$ , and we are done.  $\square$

**Theorem 2.2.9.** *Let  $R$  be a model of Peano arithmetic and let  $p \in R$  be irreducible. Then  $p$  is prime.*

**Proof.** [6] Define the set

$$A = \{x \in R : x > 0 \wedge \exists st(x = st \wedge p \mid st \wedge p \nmid s \wedge p \nmid t)\}$$

If we can prove that  $A$  is empty, then we are done, because the case  $x < 0$  is similar and the case  $x = 0$  is trivial. Suppose that  $A$  is not empty. Then by the least number principle,  $A$  has a least element  $x_0$ . So let  $s_0, t_0 \in R$  satisfy  $x_0 = s_0t_0$ ,  $p \mid s_0t_0$ ,  $p \nmid s_0$  and  $p \nmid t_0$ . For convenience, we may assume  $s_0$  and  $t_0$  positive. Notice that  $s_0 < p$  must hold, because otherwise the pair  $s_0 - p$ ,  $t_0$  would generate the element  $(s_0 - p)t_0 \in A$ , strictly smaller than  $x_0$ . We use division with remainder to find  $u, v \in R$  such that  $p = us_0 + v$ , with  $0 \leq v < s_0$ . If  $v = 0$ , then by irreducibility of  $p$ ,  $s_0 = 1$  or  $s_0 = p$ , contradicting either  $p \nmid t_0$  or  $p \nmid s_0$ . If  $v > 0$  we have

$$vt_0 = (p - us_0)t_0 = pt_0 - us_0t_0$$

Therefore  $p \mid vt_0$ ,  $p \nmid t_0$  and  $p \nmid v$  since  $0 < v < s_0 < p$ . We also have that  $vt_0 < s_0t_0 = x_0$ , contradicting the minimality of  $x_0$ . We conclude that  $A$  is empty.  $\square$

For models of open induction this equivalence may not hold. In two of the three main theorems of this thesis, we shall demonstrate this fact by constructing models of open induction which have irreducible elements that are not prime and prime elements that are not maximal. In the third main theorem, a model of open induction is constructed in which every positive nonstandard even integer is the sum of two positive primes. This is a nonstandard variation of one of the most famous unsolved problems in number theory, known as *Goldbach's conjecture*. Goldbach's conjecture states that every positive even integer can be expressed as the sum of two positive primes. It is not difficult to see the resemblance between this theorem and Goldbach's conjecture.

## Chapter 3

# Shepherdson's theorem

In this chapter we shall discover an alternative way to characterize models of open induction. This characterization will provide a way to extend certain discretely ordered rings to models of open induction.

**Lemma 3.0.1.** *Let  $R \in \text{DOR}$ . Then  $R$  is a cofinal subset of  $C(R)$ . That is to say, for every  $\alpha \in C(R)$ ,  $\alpha \geq 0$  there exists  $r \in R$  such that  $\alpha < r$ .*

**Proof.** To prove this, we show that every element which is infinite with respect to  $R$  is transcendental over  $F(R)$ . This proves the lemma since every element of  $C(R)$  is the root of some polynomial with coefficients in  $R$ .

Let  $\alpha \in L$  with  $r < \alpha$  for all  $r \in R$ . Suppose that  $\alpha$  is the root of some polynomial with coefficients in  $R$ , say

$$b_n \alpha^n + b_{n-1} \alpha^{n-1} + \dots + b_1 \alpha + b_0 = 0$$

Rearranging gives

$$\alpha^n \left( b_n + \frac{b_{n-1}}{\alpha} + \dots + \frac{b_1}{\alpha^{n-1}} + \frac{b_0}{\alpha^n} \right) = 0$$

But since the absolute value of  $\frac{b_{n-1}}{\alpha} + \frac{b_{n-2}}{\alpha^2} + \dots + \frac{b_1}{\alpha^{n-1}} + \frac{b_0}{\alpha^n}$  is smaller than any positive integer, and we may take  $b_n \neq 0$ , both factors are nonzero. This is clearly impossible, so  $\alpha$  cannot be algebraic over  $F(R)$ .  $\square$

This next theorem is due to Shepherdson.

**Theorem 3.0.2.** *Let  $R \in \text{DOR}$ . Then  $R \in \text{OI}$  if and only if for each  $\alpha \in C(R)$  there exists  $r \in R$  such that  $r \leq \alpha < r + 1$ .*

**Proof.** [2] Let  $R \in \text{OI}$  and let  $\alpha \in C(R)$ . We must find  $r \in R$  such that  $r \leq \alpha < r + 1$ . First, we may take  $\alpha > 0$ , for if we can find a suitable  $r$  for all positive  $\alpha$ , then surely we can find these for negative  $\alpha$  as well. We also leave out the case  $0 \leq \alpha \leq 1$ , because here  $r = 0$  or  $r = 1$  will meet our requirement. So assume  $r > 1$ . Let  $r$  be a root of  $f(X) \in R[X] \setminus \{0\}$ . Define the formula  $\phi(y)$ , with variables in  $R$ , as  $\exists x[f(x) = 0 \wedge 0 < x < y]$ . Because  $C(R)$  is a real closed field,  $C(R)$  admits elimination of quantifiers. This was proven by Alfred Tarski

in 1951. This means that there exists an open formula  $\psi(y)$ , also with variables in  $R$ , such that  $C(R) \models \forall y[\phi(y) \leftrightarrow \psi(y)]$ . Since  $R$  is a substructure of  $C(R)$  and  $\psi(y)$  is quantifier free, we have that for  $y \in R$ ,  $R \models \psi(y) \Leftrightarrow C(R) \models \psi(y)$ . Combined with the fact that  $R$  is cofinal in  $C(R)$ , we see that  $R$  cannot satisfy  $\forall y \geq 0[\neg\psi(y)]$ . This would contradict the fact that  $f$  has a positive root in  $C(R)$ . On the grounds that  $R \models \neg\psi(0)$  and  $R$  is a model of open induction, there must exist  $r_0 \in R$  with  $R \models \neg\psi(r_0) \wedge \psi(r_0 + 1)$ . This means that for the smallest positive root of  $f$ ,  $\alpha_0$ , we have that  $r_0 \leq \alpha_0 < r_0 + 1$ .

Now suppose we have found  $r_i \in R$ , such that  $r_i \leq \alpha_i < r_i + 1$ , for  $\alpha_i$  the  $i$ -th positive root of  $f$ . Then for the next root,  $\alpha_{i+1}$ , we may either have  $r_i \leq \alpha_{i+1} \leq r_i + 1$  or  $r_i + 1 < \alpha_{i+1}$ . In the former case  $r_{i+1} = r_i$  or  $r_{i+1} = r_i + 1$  suffices. In the later case  $\alpha_{i+1}$  is the smallest positive root of the polynomial  $f(X + r_i + 1)$ , and we may apply the previous technique. Since  $f$  has finitely many roots, eventually we will treat  $\alpha$  and find  $r \in R$  such that  $r \leq \alpha < r + 1$ , as desired.

We now prove the converse. Suppose that for each  $\alpha \in C(R)$  there exists  $r \in R$  such that  $r \leq \alpha < r$ . We have to show that the induction axioms

$$\forall \vec{x}[(\phi(0, \vec{x}) \wedge \forall y \geq 0(\phi(y, \vec{x}) \rightarrow \phi(y + 1, \vec{x}))) \rightarrow \forall y \geq 0\phi(y, \vec{x})]$$

are satisfied for all open formulas  $\phi$ .

First let us prove that each open formula  $\phi(y)$  with constants in  $R$  is equivalent to a composition of formulas of the form  $0 < f(y)$  with elements from the set  $\{\wedge, \neg\}$ . Here  $f$  is a polynomial with coefficients in  $R$ . Since  $\rightarrow$  and  $\vee$  can be expressed using combinations of  $\wedge$  and  $\neg$ , we may restrict ourselves to use induction on the number of symbols from the set  $\{\wedge, \neg\}$  in the formulas. For atomic formulas, we have the equivalencies

$$\begin{aligned} f(y) < g(y) &\leftrightarrow 0 < g(y) - f(y) \\ f(y) = g(y) &\leftrightarrow \neg(0 < g(y) - f(y)) \wedge \neg(0 < f(y) - g(y)) \\ \perp &\leftrightarrow 0 < 0 \end{aligned}$$

with  $f(X), g(X) \in R[X]$ . So our claim is true for atomic formulas. The induction step is trivial.

Now, in  $C(R)$ , each formula of the form  $0 < f(y)$  is equivalent to a composition of formulas  $\alpha_i < y$  and  $y < \alpha_i$ , and the symbols  $\wedge$  and  $\neg$ , where the  $\alpha_i \in C(R)$  are roots of  $f$ . This is because  $C(R)$  is a real closed field and is therefore elementary equivalent to  $\mathbb{R}$ , as  $\mathbb{R}$  is also a real closed field. Consequently, since  $\mathbb{R}$  satisfies the intermediate value theorem,  $C(R)$  does too. The intermediate value theorem implies that the value of a polynomial  $f$ , not equal to the zero polynomial, always has a root between positive and negative values of  $f$ , and  $f$  is either always positive or always negative between consecutive roots.

By our hypothesis, there exist  $r_i \in R$  such that  $r_i \leq \alpha_i < r_i + 1$ . This means that for  $y \in R$  we have  $\alpha_i < y \Leftrightarrow r_i < y$ . For  $y < \alpha_i$ , we either have the equivalency  $y < \alpha_i \Leftrightarrow y < r_i + 1$  or  $y < \alpha_i \Leftrightarrow y < r_i$ , depending on whether  $r_i = \alpha_i$  or not.

Suppose that the formulas  $\psi(y)$  and  $\chi(y)$  both define a finite union of disjoint segments in  $R$  of the form  $\{y \in R : a < y\}$ ,  $\{y \in R : a < y < b\}$ ,  $\{y \in R : y < b\}$ ,

with  $a, b \in R$ , or simply define all of  $R$ . Then  $\neg\psi(y)$  and  $\psi(y) \wedge \chi(y)$  also define a finite union of this kind. So by induction on the number of occurrences of  $\neg$  and  $\wedge$ , we have that every open formula  $\phi(y)$  describes a set of this type. We choose the segments in such a way that there are always elements lying strictly between consecutive segments, by joining neighbouring segments when possible.

Let  $\phi(y)$  be an open formula and suppose that  $\forall y \geq 0 \phi(y)$  does not hold. In this case there must exist  $z \in R$  with  $z \geq 0$  and  $\neg\phi(z)$ . Because  $\neg\phi(y)$  is also an open formula,  $z$  is an element of the set defined by  $\neg\phi(y)$ , as described above. Suppose for example  $z \in \{y \in R : a < y\}$ . Then if  $a < 0$ ,  $\phi(0)$  fails, and if  $a \geq 0$ ,  $\phi(a) \rightarrow \phi(a+1)$  fails. The other cases are similar. We conclude that the induction axioms are satisfied for all open formulas  $\phi$ .  $\square$

# Chapter 4

## The constructions

### 4.1 Wilkie's construction

The next two lemmas are due to Wilkie and shed some light on why theorem 3.0.2 might be useful. In these lemmas the norm for an element  $a + \sqrt{-1}b \in C(R)(\sqrt{-1})$ , with  $a, b \in C(R)$ , is given by  $\sqrt{a^2 + b^2}$ , analogous to the complex numbers. With infinitesimal is meant that an element is smaller in absolute value than  $\frac{1}{n}$ , for any  $n \in \mathbb{Z}_{>0}$ .

**Lemma 4.1.1.** *Let  $R \in ZR$  and  $\alpha \in C(R)$ . Suppose that  $r \leq \alpha < r + 1$  does not hold for any  $r \in R$ . Then there exist  $\xi \in L$  such that that  $|\xi - \theta|$  is not infinitesimal for any  $\theta$  in  $C(R)(\sqrt{-1})$ , the algebraic closure of  $R$ .  $\blacklozenge$*

**Proof.** [5]

We can use the previous lemma to expand a  $\mathbb{Z}$ -ring  $R$  to  $R[\xi]$ . By adding "enough" elements in this way, we will be able to expand the original ring into a model of open induction. The general idea is to recursively expand an existing ring using several methods, including lemma 4.1.1. The final ring we will be the union of this family of rings. Theorem 3.0.2 and lemma 4.1.1 are used to ensure that the final ring will be a model of open induction. Along the way, we will use techniques from the upcoming sections to impart these rings with the necessary properties. It is therefore important that certain properties are preserved when expanding a ring. Some of these safeguards are set up after the following lemma.

**Lemma 4.1.2.** *Let  $R \in ZR$  and  $\xi \in L$ . Suppose that  $|\xi - \theta|$  is not infinitesimal for any  $\theta$  in  $C(R)(\sqrt{-1})$ , the algebraic closure of  $R$ . Then  $\xi$  is transcendental over  $F(R)$  and  $R[\xi] \in DOR$ .*

**Proof.** [8] Let  $\xi$  and  $R$  be as stated above. It suffices to show that if  $f(X) \in R[X]$  is nonconstant, then  $f(\xi)$  is infinite. We write  $f(X) = b_n(X - \theta_1)(X - \theta_2)\dots(X - \theta_n)$ , where  $b_n \in R$  and  $\theta_i \in C(R)(\sqrt{-1})$  are the roots of  $f$ . For convenience we take  $b_n$  positive. Then  $f(\xi) = b_n(\xi - \theta_1)(\xi - \theta_2)\dots(\xi - \theta_n)$ . Suppose that  $f(\xi)$  is not infinite. By our assumptions, none of the factors  $b_n$ ,  $(\xi - \theta_1)$ ,  $(\xi - \theta_2)$ ,  $\dots$ ,  $(\xi - \theta_n)$  are infinitesimal. Because their product is not

infinite, this means that all the factors must be finite. In particular,  $b_n \in \mathbb{Z}_{>0}$  and there exists  $N \in \mathbb{Z}_{>0}$  such that  $\sum_{i=1}^n |\xi - \theta_i| \leq N$ . Notice that  $b_n \sum_{i=1}^n \theta_i$  is equal to  $b_{n-1}$ , the coefficient of  $X^{n-1}$  in  $f(X)$ . We have the following inequality

$$\left| \xi - \frac{b_{n-1}}{nb_n} \right| = \left| \sum_{i=1}^n \frac{\xi - \theta_i}{n} \right| \leq \frac{1}{n} \sum_{i=1}^n |\xi - \theta_i| \leq \frac{N}{n}$$

Since  $R \in ZR$  and  $nb_0 \in \mathbb{Z}_{>0}$ , there exist  $y \in R$  and  $r \in \mathbb{Z}$  with  $0 \leq r < nb_0$  such that  $b_{n-1} = nb_0 y + r$ . But this implies that  $|\xi - y| \leq \frac{N}{n} + \frac{r}{nb_n}$ . So there must exist  $m \in \mathbb{Z}$ , with  $-\frac{N}{n} - \frac{r}{nb_n} - 1 \leq m \leq \frac{N}{n} + \frac{r}{nb_n}$  such that  $y + m \leq \xi < y + m + 1$ . This is contradicting the assumptions we made for  $\xi$ . We conclude that  $f(\xi)$  must be infinite.  $\square$

### 4.1.1 Preserving properties

#### Normality

**Lemma 4.1.3.** *If  $K$  is a field, then  $K[X]$  is normal.*

**Proof.** We shall prove that  $K[X]$  is a principal ideal domain. Then as a corollary we have that  $K[X]$  is a unique factorization domain. This proves the lemma, because all unique factorization domains are normal.

Let  $I$  be a nonzero ideal of  $K[X]$ . Take  $f(X) \in I \setminus \{0\}$ , so that the degree of  $f$  is minimal. We claim that  $I = (f)$ . Let  $g(X) \in I$ . Then, because  $K$  is a field, we can write  $g(X) = h(X)f(X) + r(X)$ , with  $h(X), r(X) \in K[X]$  and where  $r$  has a degree strictly smaller than the degree of  $f$ . But then  $r(X) = g(X) - h(X)f(X) \in I$ . So, by the minimal property of  $f$ , we must have that  $r(X) = 0$ . Hence  $g(X) = h(X)f(X) \in (f)$ . So  $I = (f)$  and we conclude that  $K[X]$  is a principal ideal domain.  $\square$

**Lemma 4.1.4.** *Let  $R \in DOR$  be normal. If  $f(X), g(X) \in F(R)[X]$  are monic and  $f(X)g(X) \in R[X]$ , then  $f(X), g(X) \in R[X]$ .*

**Proof.** [9] Suppose  $f, g$  and  $R$  satisfy the conditions stated above. Then  $f(X)g(X) \in R[X]$  is monic. So the roots of  $f(X)$  and  $g(X)$  are roots of the monic polynomial  $f(X)g(X)$  with coefficients in  $R$ . Now, the roots of all monic polynomials with coefficients in  $R$  form a ring; a fact that we shall not attempt to prove here. So the coefficients of  $f$  and  $g$  are also the roots of some monic polynomial with coefficients in  $R$ . Since the coefficients of  $f$  and  $g$  lie in  $F(R)$  and  $R$  is normal, the coefficients must be elements of  $R$ . Hence  $f(X), g(X) \in R[X]$ .  $\square$

**Lemma 4.1.5.** *If  $R \in DOR$  is normal, then  $R[X]$  is normal as well.*

**Proof.** [9] Suppose  $R \in DOR$  is normal. We have to show that if  $\alpha(X) \in R(X)$  satisfies the equation

$$\alpha(X)^n + b_{n-1}\alpha(X)^{n-1} + \dots + b_1\alpha(X) + b_0 = 0$$

where the coefficients  $b_i$  lie in  $R[X]$ , then  $\alpha(X) \in R[X]$ . First notice that  $\alpha(X) \in F(R)(X)$ , because  $F(R)(X) = R(X)$  and that  $b_{n-1}, b_{n-2}, \dots, b_1, b_0 \in$

$F(R)[X]$ , because  $R[X] \subset F(R)[X]$ . So, since  $F(R)$  is a field,  $F(R)$  is normal by lemma 4.1.3. Thus  $\alpha(X) \in F(R)[X]$ . We take  $m \in \mathbb{Z}$  strictly larger than the degree of  $\alpha$  and consider the following equation in the variable  $Y$

$$(Y - X^m)^n + b_{n-1}(Y - X^m)^{n-1} + \dots + b_1(Y - X^m) + b_0 = 0$$

This is a monic polynomial with coefficients in  $R[X]$ . Notice that it has  $\alpha(X) + X^m$  as a solution, which we shall denote by  $\beta(X)$ . So if we rewrite the equation as

$$Y^n + c_{n-1}Y^{n-1} + \dots + c_1Y + c_0 = 0$$

where the  $c_i$  are elements in  $R[X]$ , then we have that

$$\beta(X)^n + c_{n-1}\beta(X)^{n-1} + \dots + c_1\beta(X) + c_0 = 0$$

Rearranging this gives

$$\beta(X)(\beta(X)^{n-1} + c_{n-1}\beta(X)^{n-2} + \dots + c_1) = -c_0$$

So we have two monic polynomials in  $F(R)[X]$  whose product lies in  $R[X]$ . Lemma 4.1.4 implies that  $\beta(X)$  actually lies in  $R[X]$ . Thus  $\alpha(X) = \beta(X) - X^m \in R[X]$ , as asserted.  $\square$

### Irreducibility

**Lemma 4.1.6.** *Let  $R \in \text{DOR}$ . If  $q \in R$  is irreducible in  $R$ , then  $q$  is irreducible in  $R[X]$ .*

**Proof.** Let  $f(X), g(X) \in R[X]$  and suppose that  $q = f(X)g(X)$ . Then  $f$  and  $g$  must be constant. The lemma then follows from the fact that  $f(X), g(X) \in R$  and the assumption that  $q$  is irreducible in  $R$ .  $\square$

### Primality

**Lemma 4.1.7.** *Let  $R \in \text{DOR}$ . If  $p \in R$  is prime in  $R$ , then  $p$  is also prime in  $R[X]$ .*

**Proof.** Let  $f(X), g(X) \in R[X]$ . We give a proof by contraposition and show that if  $p \nmid f(X)$  and  $p \nmid g(X)$ , then  $p \nmid f(X)g(X)$ . Write

$$f(X) = b_nX^n + b_{n-1}X^{n-1} + \dots + b_1X + b_0$$

and

$$g(X) = c_mX^m + c_{m-1}X^{m-1} + \dots + c_1X + c_0$$

If  $p$  does not divide  $f$  and  $g$ , then there is a smallest index  $i$  and a smallest index  $j$ , such that  $p \nmid b_i$  and  $p \nmid c_j$ . The coefficient of  $X^{i+j}$  in  $f(X)g(X)$  is given by  $\sum_{k=0}^{i+j} b_k c_{i+j-k}$ . Notice that by minimality of  $i$  and  $j$  every term of the sum is divisible by  $p$ , except for  $b_i c_j$ . Therefore  $p \nmid \sum_{k=0}^{i+j} b_k c_{i+j-k}$  and we conclude that  $p \nmid f(X)g(X)$ , as was asserted.  $\square$

## Nonprimality

**Lemma 4.1.8.** *Let  $R \in DOR$ . If  $r, s \in R$  and for all  $n \in \mathbb{Z}_{>0}$ ,  $r \nmid ns$  in  $R$ , then for all  $n \in \mathbb{Z}_{>0}$ ,  $r \nmid ns$  in  $R[X]$ .*

**Proof.** Suppose that for all  $n \in \mathbb{Z}_{>0}$ ,  $r \nmid ns$  in  $R$  and suppose to the contrary that  $r \mid ms$  in  $R[X]$ , for a certain  $m \in \mathbb{Z}_{>0}$ . Then  $ms = rf(X)$ , with  $f(X) \in R[X]$ . We see that  $f$  must be constant. Therefore  $r \mid ms$  in  $R$ , which contradicts our assumption.  $\square$

## Nonmaximality

**Lemma 4.1.9.** *Let  $R \in DOR$ . Suppose that  $p, q \in R$  and assume that for all  $n \in \mathbb{Z}_{>0}$  there is no  $r \in R$  such that  $qr \equiv n \pmod{p}$  in  $R/pR$ . Then for all  $n \in \mathbb{Z}_{>0}$  there is no  $f(X) \in R[X]$  such that  $qf(X) \equiv n \pmod{p}$  in  $R[X]/(p)$ .*

**Proof.** Suppose to the contrary that there exists  $n \in \mathbb{Z}_{>0}$  and  $f(X) \in R[X]$  such that  $qf(X) \equiv n \pmod{p}$  in  $R[X]/(p)$ . Then  $qf(X) = n + pg(X)$ , for some  $g(X) \in R[X]$ . Corresponding powers of  $X$  must be equal on both sides of the equality. In particular, the constant terms must be equal, so that  $qa_0 = n + pb_0$ , where  $a_0$  and  $b_0$  are the constant terms of  $f$  and  $g$  respectively. But this contradicts the assumption that for all  $n \in \mathbb{Z}_{>0}$  there is no  $r \in R$  such that  $qr \equiv n \pmod{p}$  in  $R/pR$ .  $\square$

## 4.2 The $\hat{\mathbb{Z}}$ -construction

One of the prerequisites for applying lemma 4.1.1 to a ring  $R \in DOR$  is that  $R$  is a  $\mathbb{Z}$ -ring. It turns out that we can expand an arbitrary ring  $R \in DOR$  into a  $\mathbb{Z}$ -ring exactly when there exists a ring homomorphism from  $R$  to the ring  $\hat{\mathbb{Z}}$ .

**Definition 4.2.1.** *We define  $\hat{\mathbb{Z}}$  as the inverse limit of the rings  $\mathbb{Z}/n\mathbb{Z}$ , with  $n \in \mathbb{Z}_{>1}$ .*

We elaborate on what we mean by this. Let  $m, n \in \mathbb{Z}_{>1}$  with  $m \mid n$ . Then there exists a unique ring homomorphism  $\psi_{n,m} : \mathbb{Z}/n\mathbb{Z} \rightarrow \mathbb{Z}/m\mathbb{Z}$ . The homomorphism  $\psi_{n,m}$  acts on an element of  $\mathbb{Z}/n\mathbb{Z}$  by simply taking the remainder modulo  $m$ . The ring  $\hat{\mathbb{Z}}$  is the subring of  $\prod_{n>1} \mathbb{Z}/n\mathbb{Z}$  consisting of those elements  $(a_2, a_3, a_4, \dots) \in \prod_{n>1} \mathbb{Z}/n\mathbb{Z}$  for which  $\psi_{n,m}(a_n) = a_m$  holds, for all combinations of  $m$  and  $n$  for which  $\psi_{n,m}$  is defined.

**Definition 4.2.2.** *For every prime  $p \in \mathbb{Z}_{>0}$  we define the ring of  $p$ -adic integers,  $\mathbb{Z}_p$ , as the inverse limit of the rings  $\mathbb{Z}/p^n\mathbb{Z}$ , with  $n \in \mathbb{Z}_{>0}$ .*

What we mean by this is that  $\mathbb{Z}_p$  is the subring of  $\prod_{n>0} \mathbb{Z}/p^n\mathbb{Z}$  consisting of those elements  $(a_1, a_2, a_3, \dots) \in \prod_{n>0} \mathbb{Z}/p^n\mathbb{Z}$  for which  $\psi_{p^n, p^m}(a_n) = a_m$  holds, for all combinations of  $m$  and  $n$  for which  $\psi_{p^n, p^m}$  is defined.

**Lemma 4.2.3.** *The rings  $\hat{\mathbb{Z}}$  and  $\prod_p \mathbb{Z}_p$ , where the product is taken over all primes in  $\mathbb{Z}$ , are isomorphic.*

**Proof.** Notice that for  $(a_2, a_3, a_4, \dots) \in \hat{\mathbb{Z}}$  and  $m, n > 1$  relatively prime, the value of  $a_{mn}$  is fully determined by the values of  $a_m$  and  $a_n$ , according to the Chinese remainder theorem. We see that the factors in  $\prod_{n>1} \mathbb{Z}/n\mathbb{Z}$  for which  $n$  is not a prime power are therefore redundant. So, if we choose to ignore these factors we recognize that  $\hat{\mathbb{Z}} \cong \prod_p \mathbb{Z}_p$ , where the product is taken over all primes  $p \in \mathbb{Z}$ .  $\square$

**Lemma 4.2.4.** *For every  $R \in ZR$  there exists a ring homomorphism  $Rem : R \rightarrow \hat{\mathbb{Z}}$ .*

**Proof.** [5] Because  $R \in ZR$ , there exists a ring homomorphism  $Rem_n : R \rightarrow \mathbb{Z}/n\mathbb{Z}$  by sending an element  $x \in R$  to the remainder of  $x$  after division by  $n \in \mathbb{Z}_{>0}$ . We combine these homomorphisms to create the homomorphism  $Rem : R \rightarrow \prod_{n>1} \mathbb{Z}/n\mathbb{Z}$ , by defining  $Rem(x) = \prod_{n>1} Rem_n(x)$ , for all  $x$  in  $R$ .

We have to show that the image of  $Rem$  lies in  $\hat{\mathbb{Z}}$ . Let  $x \in R$  and  $m, n \in \mathbb{Z}_{>1}$  with  $m \mid n$ . We write  $x = my + r$  and  $x = ny' + r'$ , with  $y, y' \in R$  and  $r, r' \in \mathbb{Z}$ , such that  $0 \leq r < m$  and  $0 \leq r' < n$ . Now if  $Rem(x) = (a_2, a_3, a_4, \dots)$ , then the statement  $\psi_{n,m}(a_n) = a_m$  is equivalent to saying that  $r$  and  $r'$  are congruent modulo  $m$ . This is in fact the case, because  $r - r' = m(\frac{n}{m}y' - y)$ .  $\square$

If  $R \in OI$ , then  $R \in ZR$ , by corollary 2.2.6. By lemma 4.2.4 there exist a ring homomorphism  $Rem : R \rightarrow \hat{\mathbb{Z}}$ . Consequently, for a subring of a model of open induction there will also exist a homomorphism to  $\hat{\mathbb{Z}}$ . In the upcoming chapters we will show that the converse of this statement also holds. If  $R \in DOR$  and there exists a ring homomorphism  $\varphi : R \rightarrow \hat{\mathbb{Z}}$ , then  $R$  can be embedded into a model of open induction. The following theorem will be of help in establishing this.

**Theorem 4.2.5.** *Let  $R \in DOR$  and suppose  $\varphi : R \rightarrow \hat{\mathbb{Z}}$  is a ring homomorphism. Then  $R$  can be embedded into a  $\mathbb{Z}$ -ring.*

**Proof.** [2] For each standard prime  $p$ , let  $\varphi_p : R \rightarrow \mathbb{Z}_p$  be the restriction of  $\varphi$  to the factor  $\mathbb{Z}_p$  of  $\prod_p \mathbb{Z}_p$ . We define the relation  $Div$  on the set  $\mathbb{Z}_{>0} \times R$  by

$$Div(n, r) \Leftrightarrow \text{for all primes } p : n \mid \varphi_p(r) \text{ in } \mathbb{Z}_p.$$

We form a new ring  $R_\varphi \subset F(R)$  by letting

$$R_\varphi = \left\{ \frac{r}{n} : r \in R, n \in \mathbb{Z}, n > 0, Div(n, r) \right\}$$

We extend  $\varphi$  to  $R_\varphi$  by letting  $\varphi\left(\frac{r}{n}\right) = \frac{\varphi(r)}{n}$  and  $\varphi_p$  extends in the same way.

We check that  $R_\varphi$  is closed under  $+$  and  $\cdot$ . Suppose  $\frac{r}{n}, \frac{r'}{n'} \in R_\varphi$ . Then  $\frac{r}{n} + \frac{r'}{n'} = \frac{rn' + r'n}{nn'}$ . In  $\mathbb{Z}_p$  we have  $nn' \mid \varphi_p(r)n'$ , because  $n \mid \varphi_p(r)$  by  $Div(n, r)$ . Similarly  $nn' \mid \varphi_p(r')n$ , because  $n' \mid \varphi_p(r')$  by  $Div(n', r')$ . Hence  $nn' \mid \varphi_p(rn' + r'n)$  in  $\mathbb{Z}_p$ . This is true for any prime  $p$ , so  $Div(nn', rn' + r'n)$  holds and  $\frac{rn' + r'n}{nn'} \in R_\varphi$ . For  $\frac{r}{n} \cdot \frac{r'}{n'} = \frac{rr'}{nn'}$  it is an immediate consequence of  $Div(n, r)$  and  $Div(n', r')$  that in  $\mathbb{Z}_p$ ,  $nn' \mid \varphi_p(r)\varphi_p(r')$ . Again, this is true for any prime  $p$ , so  $Div(nn', rr')$  holds and  $\frac{rr'}{nn'} \in R_\varphi$ .

Now we show that  $R_\varphi \in DOR$ . Suppose  $\frac{r}{n} \in R_\varphi$  and  $0 < \frac{r}{n} < 1$ . Then  $0 < r < n$ . Because of this inequality and because  $R \in DOR$ ,  $r$  must be standard.

Otherwise there would exist  $m \in \mathbb{Z}$ ,  $0 \leq m < n$  such that  $0 < r - m < 1$ . Consequently, there exists a prime power  $p^l \in \mathbb{Z}$  such that  $p^l \mid n$  but  $p^l \nmid r$ . Therefore  $\varphi_p(n) \in p^l \mathbb{Z}_p$  and if we write  $\varphi_p(n) = (a_1, a_2, a_3, \dots)$ ,  $a_l$  must be 0. Hence, every multiple of  $\varphi_p(n)$  has 0 on the  $l$ -th position. But since  $r$  has a non-zero remainder modulo  $p^l$ ,  $\varphi_p(r)$  is non-zero on the  $l$ -th position. So  $\varphi_p(r)$  cannot be a multiple of  $\varphi_p(n)$  in  $\mathbb{Z}_p$  and  $Div(r, n)$  does not hold. The assumption that  $0 < \frac{r}{n} < 1$  must have been false, so  $R \in DOR$ .

More importantly, we prove that  $R_\varphi \in ZR$ . Let  $\frac{r}{n} \in R_\varphi$  and let  $q^l \in \mathbb{Z}$  be a fixed prime power. First we show that  $\frac{r}{n}$  satisfies the division-with-remainder property when dividing by  $q^l$ . We write  $\varphi_q(\frac{r}{n}) = (a_1, a_2, a_3, \dots)$ . We pick  $k \in \mathbb{Z}$ ,  $0 \leq k < q^l$ , such that  $k$  is in the congruence class  $a_l$ . Then  $\varphi_q(k)$  has  $a_l$  on the  $l$ -th position, so that  $\varphi_q(\frac{r}{n} - k)$  has 0 on the  $l$ -th position. Thus  $\varphi_q(\frac{r-nk}{n}) \in q^l \mathbb{Z}_q$ . We see that  $nq^l \mid \varphi_q(r - nk)$  in  $\mathbb{Z}_q$ . For a prime  $p \neq q$  the condition  $nq^l \mid \varphi_p(r - nk)$  is also satisfied, because  $q^l$  is a unit in  $\mathbb{Z}_p$ . We conclude that  $Div(nq^l, r - nk)$  holds and therefore  $\frac{r-nk}{nq^l} \in R_\varphi$ . Consequently  $\frac{r}{n} = q^l \frac{r-nk}{nq^l} + k$ , as desired.

We generalize result to any positive integer  $m \in \mathbb{Z}_{>0}$ . Notice that the division-with-remainder property when dividing by  $m$  is equivalent to stating that  $R_\varphi/mR_\varphi \cong \mathbb{Z}/m\mathbb{Z}$ . We decompose  $m$  in its prime powers as follows,  $m = \prod_{i=0}^n p_i^{l_i}$ . Using the Chinese remainder theorem we see that

$$R_\varphi/mR_\varphi \cong \prod_{i=0}^n R_\varphi/p_i^{l_i} R_\varphi \cong \prod_{i=0}^n \mathbb{Z}/p_i^{l_i} \mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z}.$$

So indeed  $R_\varphi \in ZR$ . □

## 4.2.1 Preserving properties

### Normality

**Lemma 4.2.6.** *If  $S$  is normal and  $Y \subset S$  such that  $1 \in Y$ ,  $0 \notin Y$  and  $Y$  is closed under multiplication, then  $SY^{-1} = \{s/y : s \in S, y \in Y\}$  is normal.*

**Proof.** Let  $x \in F(SY^{-1})$  and suppose  $x$  satisfies the equation

$$x^n + \frac{s_{n-1}}{y_{n-1}} x^{n-1} + \dots + x \frac{s_1}{y_1} + \frac{s_0}{y_0} = 0$$

with  $s_i \in S$  and  $y_i \in Y$ . For  $SY^{-1}$  to be normal, we have to show that  $x \in SY^{-1}$ . First notice that  $F(SY^{-1}) = F(S)$ , making  $x \in F(S)$ . Now let  $y = y_{n-1}y_{n-2}\dots y_1y_0$ . Multiplying the equation by  $y^n$  gives

$$y^n x^n + \frac{y s_{n-1}}{y_{n-1}} y^{n-1} x^{n-1} + \dots + \frac{y^{n-1} s_1}{y_1} y x + \frac{y^n s_0}{y_0} = 0.$$

The coefficients  $\frac{y s_{n-1}}{y_{n-1}}, \frac{y^2 s_{n-2}}{y_{n-2}}, \dots, \frac{y^{n-1} s_1}{y_1}, \frac{y^n}{y_0}$  all lie in  $S$ , so because  $S$  is normal,  $yx \in S$ . And since  $y$  is an element of  $Y$ ,  $x = \frac{yx}{y}$  is an element of  $SY^{-1}$ . So  $SY^{-1}$  is normal. □

**Lemma 4.2.7.** *The ring  $\mathbb{Z}_p$  is normal.*

**Proof.** [1] We shall prove that  $\mathbb{Z}_p$  is a principal ideal domain, with as ideals  $\{0\}$  and  $p^n\mathbb{Z}_p$ , for  $n \in \mathbb{Z}_{\geq 0}$ . Then as a corollary we have that  $\mathbb{Z}_p$  is a unique factorization domain. This proves the lemma, because all unique factorization domains are normal.

Let  $I$  be nonzero ideal of  $\mathbb{Z}_p$ . Take  $(a_1, a_2, a_3, \dots) \in I$ , so that the number of zeros at the beginning of the sequence is minimal. Suppose that the first nonzero element sits at the  $n$ -th position. Then we can write  $(a_1, a_2, a_3, \dots) = p^n(b_1, b_2, b_3, \dots)$ , with  $b_1$  nonzero. This means that  $(b_1, b_2, b_3, \dots)$  is invertible, because the individual  $b_i$  are invertible in  $\mathbb{Z}/p^i\mathbb{Z}$ . Hence  $p^n \in I$  and  $p^n\mathbb{Z}_p \subset I$ .

Conversely, because of the minimal property of  $(a_1, a_2, a_3, \dots)$ , we can write any element in  $I$  as  $p^k(c_1, c_2, c_3, \dots)$ , with  $k \geq n$ . Then  $p^k(c_1, c_2, c_3, \dots) = p^n p^{k-n}(c_1, c_2, c_3, \dots) \in p^n\mathbb{Z}_p$ . This shows that  $I \subset p^n\mathbb{Z}_p$ .  $\square$

The next lemma is due to Van den Dries.

**Lemma 4.2.8.** *If  $R$  is normal, then  $R_\varphi$  is normal.*

**Proof.** [2] Suppose  $R$  is normal. Let  $x \in F(R_\varphi)$  and suppose  $x$  satisfies the equation

$$x^n + b_{n-1}x^{n-1} + \dots + b_1x + b_0 = 0$$

with  $b_i \in R_\varphi$ . For  $R_\varphi$  to be normal, we have to show that  $x \in R_\varphi$ . Because  $R_\varphi \subset R\mathbb{Z}_{>0}^{-1}$ , the coefficients  $b_i$  lie in  $R\mathbb{Z}_{>0}^{-1}$ . Since  $R$  is normal and  $\mathbb{Z}_{>0}$  is closed under multiplication,  $R\mathbb{Z}_{>0}^{-1}$  is normal by lemma 4.2.6. Therefore  $x \in R\mathbb{Z}_{>0}^{-1}$ . Say  $x = \frac{r}{m}$ , with  $r \in R$  and  $m \in \mathbb{Z}_{>0}$ . Hence

$$\frac{r^n}{m^n} + b_{n-1}\frac{r^{n-1}}{m^{n-1}} + \dots + b_1\frac{r}{m} + b_0 = 0$$

Multiplying by  $m^n$  gives

$$r^n + b_{n-1}mr^{n-1} + \dots + b_1m^{n-1}r + b_0m^n = 0$$

These elements lie in  $R_\varphi$ , so we can apply  $\varphi_p$  to the equation to get the following equation in  $\mathbb{Z}_p$

$$\varphi_p(r)^n + m\varphi_p(b_{n-1})\varphi_p(r)^{n-1} + \dots + m^{n-1}\varphi_p(b_1)\varphi_p(r) + m^n\varphi_p(b_0) = 0$$

Lastly we divide by  $m^n$  to get

$$\frac{\varphi_p(r)^n}{m^n} + \varphi_p(b_{n-1})\frac{\varphi_p(r)^{n-1}}{m^{n-1}} + \dots + \varphi_p(b_1)\frac{\varphi_p(r)}{m} + \varphi_p(b_0) = 0$$

The coefficients  $\varphi_p(b_{n-1}), \varphi_p(b_{n-2}), \dots, \varphi_p(b_1), \varphi_p(b_0)$  are elements of  $\mathbb{Z}_p$  and  $\frac{\varphi_p(r)}{m} \in F(\mathbb{Z}_p)$ , so because  $\mathbb{Z}_p$  is normal by lemma 4.2.7,  $\frac{\varphi_p(r)}{m}$  must lie in  $\mathbb{Z}_p$ . Hence  $m \mid \varphi_p(r)$  in  $\mathbb{Z}_p$ . Since this is true for every prime  $p$ ,  $Div(m, r)$  holds and  $\frac{r}{m} \in R_\varphi$ . So  $R_\varphi$  is normal.  $\square$

## Irreducibility

**Lemma 4.2.9.** *Let  $R \in \text{DOR}$ . Assume that the standard primes in  $\mathbb{Z}$  remain prime in  $R$ . If  $q \in R$  is irreducible in  $R$  and  $\varphi(q) \in U(\hat{\mathbb{Z}})$ , the group of units of  $\hat{\mathbb{Z}}$ , then  $q$  is also irreducible in  $R_\varphi$ .*

**Proof.** [5] First we take  $q$  positive and nonstandard. Suppose  $r, s \in R$  and  $n, m \in \mathbb{Z}$ , with  $r, s, n, m > 0$ , such that  $q = \frac{r}{n} \frac{s}{m}$  and  $\frac{r}{n}, \frac{s}{m} \in R_\varphi$ . We have to prove that either  $\frac{r}{n}$  or  $\frac{s}{m}$  is equal to 1.

We have  $nmq = rs$ . Since we assumed that the standard primes remain prime in  $R$ , any prime factor of  $n$  or  $m$  divides  $r$  or  $s$ . So we can take these factors out of  $r$  and  $s$  and find  $n', m' \in \mathbb{Z}_{>0}$  such that  $nm = n'm'$ ,  $s = n's'$  and  $r = m'r'$ . But then  $nmq = rs = n'r'm's' = nmr's'$ , so  $q = r's'$ . Because  $q$  is irreducible in  $R$ , we must have that either  $r' = 1$  or  $s' = 1$ . So suppose  $r' = 1$  and  $s' = q$ . Then  $s = m'q$  and  $r = n'$ . Since  $\frac{n'}{n} = \frac{r}{n} \in R_\varphi$  and  $R_\varphi$  is discretely ordered, we must have that  $n \mid n'$  in  $\mathbb{Z}$ . We rename  $\frac{n'}{n} = k$ . Because  $\frac{s}{m} \in R_\varphi$ , we have for any standard prime  $p$ , that  $m \mid \varphi_p(s)$  in  $\mathbb{Z}_p$ , by definition of  $R_\varphi$ . But  $s = m'q$  and as  $\varphi(q)$  is a unit in  $\hat{\mathbb{Z}}$ ,  $\varphi_p(q)$  is a unit in  $\mathbb{Z}_p$ . Therefore  $m \mid m'$  in each  $\mathbb{Z}_p$ , so that  $\frac{m'}{m} \in R_\varphi$ . By the same argument as before,  $m \mid m'$  in  $\mathbb{Z}$ . We rename  $\frac{m'}{m} = l$ . Plugging all of this in, we get that

$$klq = kr'ls' = \frac{n'r'}{n} \frac{m's'}{m} = \frac{r}{n} \frac{s}{m} = q$$

Thus,  $k$  and  $l$  are both equal to 1. So  $\frac{r}{n} = 1$  and  $\frac{s}{m} = q$ , as we wanted.

If  $q$  is a standard irreducible element of  $R$ , the irreducibility of  $q$  in  $R_\varphi$  follows from the fact that any factors of a standard element must be standard. Clearly then, the factorization of standard elements is the same in every discretely ordered ring. So if  $q$  is irreducible in  $R$ , then it is irreducible in  $R_\varphi$ .  $\square$

### Primality

**Lemma 4.2.10.** *Let  $R \in \text{DOR}$ . If  $q \in R$  is prime in  $R$  and  $\varphi(q) \in U(\hat{\mathbb{Z}})$ , then  $q$  is also prime in  $R_\varphi$ .*

**Proof.** [5] First suppose that  $q$  is nonstandard. Let  $r, s, t \in R$  and  $l, m, n \in \mathbb{Z}$ , such that  $\frac{r}{l}q = \frac{s}{m} \frac{t}{n}$  and  $\frac{r}{l}, \frac{s}{m}, \frac{t}{n} \in R_\varphi$ . We have to prove that either  $q \mid \frac{s}{m}$  or  $q \mid \frac{t}{n}$ .

We have  $mnrq = lst$ . Since  $q$  is nonstandard, we cannot have  $q \mid l$ . So, as  $q$  is prime in  $R$ , either  $q \mid s$  or  $q \mid t$  must hold. Suppose  $q \mid s$ , so that  $s = qs'$  for a certain  $s' \in R$ . For any standard prime  $p$ ,  $m \mid \varphi_p(s)$  in  $\mathbb{Z}_p$ . Since  $\varphi_p(q)$  is a unit, we also have that  $m \mid \varphi_p(s')$ . Thus  $\frac{s'}{m} \in R_\varphi$ . Since  $\frac{s}{m} = q \frac{s'}{m}$ , we conclude that  $q \mid \frac{s}{m}$ .

Now suppose that  $q$  is standard. Because  $R_\varphi \in \text{ZR}$ , we have that  $R_\varphi/qR_\varphi \cong \mathbb{Z}/q\mathbb{Z}$ . So,  $R_\varphi/qR_\varphi$  is a domain, as  $\mathbb{Z}/q\mathbb{Z}$  is a domain. Hence  $q$  is prime in  $R_\varphi$ .  $\square$

### Nonprimality

**Lemma 4.2.11.** *Let  $R \in \text{DOR}$ . If  $r, s \in R$  and for all  $n \in \mathbb{Z}_{>0}$ ,  $r \nmid ns$  in  $R$ , then for all  $n \in \mathbb{Z}_{>0}$ ,  $r \nmid ns$  in  $R_\varphi$ .*

**Proof.** Suppose that for all  $n \in \mathbb{Z}_{>0}$ ,  $r \nmid ns$  in  $R$  and suppose to the contrary that  $r \mid ns$  in  $R_\varphi$ , for a certain  $m \in \mathbb{Z}_{>0}$ . Then  $\frac{ms}{r} \in R_\varphi$ , so that  $\frac{ms}{r} = \frac{t}{n}$ ,

with  $t \in R$  and  $n \in \mathbb{Z}_{>0}$ . Thus  $nms = rt$  and  $r \mid nms$  in  $R$ . This contradicts our assumption, since  $nm \in \mathbb{Z}_{>0}$ .  $\square$

### Nonmaximality

**Lemma 4.2.12.** *Let  $R \in DOR$ . Suppose that  $p, q \in R$  and assume that for all  $n \in \mathbb{Z}_{>0}$  there is no  $r \in R$  such that  $qr \equiv n \pmod{p}$  in  $R/pR$ . Then for all  $n \in \mathbb{Z}_{>0}$  there is no  $\frac{t}{m} \in R_\varphi$  such that  $q\frac{t}{m} \equiv n \pmod{p}$  in  $R_\varphi/pR_\varphi$ .*

**Proof.** [5] Suppose to the contrary that there exists  $k \in \mathbb{Z}_{>0}$  and  $\frac{t}{m} \in R_\varphi$  such that  $q\frac{t}{m} \equiv k \pmod{p}$  in  $R_\varphi/pR_\varphi$ . Then  $q\frac{t}{m} = k + p\frac{s}{l}$ , for some  $\frac{s}{l} \in R_\varphi$ . Multiplying by  $lm$  gives  $qtl = psm + klm$ . This is contrary to the assumption that for all  $n \in \mathbb{Z}_{>0}$  there is no  $r \in R$  such that  $qr \equiv n \pmod{p}$  in  $R/pR$ , as  $tl \in R$  and  $klm \in \mathbb{Z}_{>0}$ .  $\square$

## 4.3 Adding a prime

**Definition 4.3.1.** *Let  $R \in DOR$ . A cut of  $R$  is a set  $C \subset R$  which is nonempty, such that  $x \in C$  implies  $x+1 \in C$ , and furthermore if  $y \in R$ ,  $z \in C$  with  $y < z$ , then  $y \in C$ .*

**Lemma 4.3.2.** *Let  $R \in DOR$  and assume that there exists a ring homomorphism  $\varphi : R \rightarrow \hat{\mathbb{Z}}$ . Suppose that  $C$  is a cut of  $R$ . Then there exists  $\alpha \in L$  such that for all  $c \in C$  we have that  $c < \alpha$  and for all  $d \in R \setminus C$  we have that  $\alpha < d$  and moreover  $\alpha$  is transcendental over  $F(R)$ .  $\blacklozenge$*

**Proof.** [5]

We can use the previous lemma to add new primes to an existing ring  $R$  by extending  $R$  to  $R[\alpha]$ . This follows from the next lemma, as  $\alpha$  is transcendental.

**Lemma 4.3.3.** *Let  $R \in DOR$  and  $r \in R$ , then  $X+r$  is prime in  $R[X]$ .*

**Proof.** Let  $f(X), g(X), h(X) \in R[X]$  be such that  $(X+r)f(X) = g(X)h(X)$ . We want to show that either  $(X+r) \mid g(X)$  or  $(X+r) \mid h(X)$ . This is equivalent to showing that either  $X \mid g(X-r)$  or  $X \mid h(X-r)$ . Suppose this is not the case. Then both  $f(X-r)$  and  $g(X-r)$  must have a constant term and so does their product. Since  $Xf(X-r)$  has no constant term, the polynomial  $Xf(X-r)$  is unequal to the polynomial  $g(X-r)h(X-r)$ . But this contradicts  $(X+r)f(X) = g(X)h(X)$ . So either  $(X+r) \mid g(X)$  or  $(X+r) \mid h(X)$  must hold.  $\square$

**Lemma 4.3.4.**  *$R[\alpha]$  is discretely ordered.*

**Proof.** [5] First let  $C = R$ . Then  $\alpha$  is infinite with respect to  $R$ . Suppose that  $f(X) \in R[X]$  such that  $0 < f(\alpha) < 1$ , say

$$0 < b_n\alpha^n + b_{n-1}\alpha^{n-1} + \dots + b_1\alpha + b_0 < 1$$

Where the  $b_i \in R$  are the coefficients of  $f(X)$  and we take  $b_n \neq 0$ . Notice that  $f(X)$  cannot be constant, since  $R \in DOR$ . We rearrange this and take the

absolute value

$$0 < |b_n \alpha^n| < |1 - b_{n-1} \alpha^{n-1} - \dots - b_1 \alpha - b_0|$$

Dividing by  $|b_n \alpha^n|$  gives

$$1 < \left| \frac{1}{b_n \alpha^n} - \frac{b_{n-1}}{b_n \alpha} - \dots - \frac{b_1}{b_n \alpha^{n-1}} - \frac{b_0}{b_n \alpha^n} \right|$$

This is impossible, since the righthand side is smaller than any positive element of  $R$ .

Now let  $C \neq R$ . Again, suppose that  $f(X) \in R[X]$  such that  $0 < f(\alpha) < 1$ . Now, because  $C(R)$  satisfies the intermediate value theorem, we can find  $s_1, \dots, s_m, t_1, \dots, t_m$  such that the following holds

$$C(R) \models \forall x [0 < f(x) < 1 \leftrightarrow (s_1 < x < t_1 \vee \dots \vee s_m < x < t_m)]$$

The  $s_i$  and  $t_i$  could be chosen as the roots of the polynomials  $f(X)$  and  $f(X) - 1$  for example. The fields  $C(R)$  and  $C(L)$  are both models of the theory of real closed fields, which admits elimination of quantifiers. Therefore  $C(R)$  is an elementary substructure of  $C(L)$ , from which we conclude that

$$C(L) \models \forall x [0 < f(x) < 1 \leftrightarrow (s_1 < x < t_1 \vee \dots \vee s_m < x < t_m)]$$

Combining this with the assumption that  $0 < f(\alpha) < 1$ , we see that for at least one pair  $s_j, t_j$ , holds that  $s_j < \alpha < t_j$ . Since  $R$  is a model of open induction, we can find  $r \in R$  such that  $r \leq s_j < r + 1$ . Notice that  $r < \alpha$ , so that  $r \in C$ . By the properties of the cut  $C$ ,  $r + 1$  must also lie in  $C$ . Hence  $r + 1 < \alpha$ , from which follows that  $s_j < r + 1 < t_j$ . But then  $0 < f(r + 1) < 1$ , which is a contradiction with  $f(r + 1) \in R$  and  $R \in \text{DOR}$ . We conclude that  $R[\alpha]$  must be discretely ordered.  $\square$

### 4.3.1 Preserving properties

The preservation of the necessary properties when a ring is expanded by adding a single transcendental element to it is already proven in section 4.1.1.

## 4.4 Eliminating a prime

**Lemma 4.4.1.** *Let  $R \in \text{DOR}$ . There exist  $\alpha, \beta \in L$  such that for all  $r \in R$ ,  $r < \alpha$  and for all  $f(X) \in R[X]$ ,  $f(\alpha) < \beta$ .  $\blacklozenge$*

**Proof.** [5]

Let  $p$  be a nonstandard prime in  $R$ . We use can use lemma 4.1.1 to extend  $R$  to  $R[\alpha, \beta, \frac{\alpha\beta}{p}]$ .

**Lemma 4.4.2.** *For all  $n \in \mathbb{Z}_{>0}$ ,  $p \nmid n\alpha$  and  $p \nmid n\beta$  in  $R[\alpha, \beta, \frac{\alpha\beta}{p}]$ .*

**Proof.** Let  $n \in \mathbb{Z}_{>0}$ . We show that  $p \nmid n\alpha$ . First notice that since  $\alpha$  is infinite with respect to  $R$ ,  $\alpha$  is transcendental over  $F(R)$  and since  $\beta$  is infinite with respect to  $R[\alpha]$ ,  $\beta$  is transcendental over  $F(R[\alpha])$ . Suppose that  $p \mid n\alpha$ . Then  $n\alpha = pf(\alpha, \beta, \frac{\alpha\beta}{p})$  for a certain  $f(X, Y, Z) \in R[X, Y, Z]$ . Therefore, by algebraic independence of  $\alpha$  and  $\beta$ , we must have  $f(X, Y, \frac{XY}{p}) = \frac{nX}{p}$ . Substituting  $X = 1, Y = p$ , gives  $f(1, p, 1) = \frac{n}{p}$ . But we must also have  $f(1, p, 1) \in R$ . This is a contradiction since  $R \in DOR$ , but  $0 < |\frac{n}{p}| < 1$ , because  $p$  is nonstandard. The same reasoning for  $\beta$  prevents that  $p \mid n\beta$ .  $\square$

Notice that  $p$  is not a prime element of  $R[\alpha, \beta, \frac{\alpha\beta}{p}]$ , because  $p \mid \alpha\beta$ , since  $\alpha\beta = p\frac{\alpha\beta}{p}$ , but  $p \nmid \alpha$  and  $p \nmid \beta$ .

**Lemma 4.4.3.** *The ring  $R[\alpha, \beta, \frac{\alpha\beta}{p}]$  is discretely ordered.*

**Proof.** Let  $f(X, Y, Z) \in R[X, Y, Z]$  and suppose that  $0 < f(\alpha, \beta, \frac{\alpha\beta}{p}) < 1$ . By multiplying with an appropriate factor  $|p^m|$  we can ensure that  $|p^m|f(\alpha, \beta, \frac{\alpha\beta}{p}) = g(\beta)$  for a certain polynomial  $g(Y) \in R[\alpha][Y]$ . We write  $g(\beta)$  explicitly and get

$$0 < b_n\beta^n + b_{n-1}\beta^{n-1} + \dots + b_1\beta + b_0 < |p^m|$$

Where the  $b_i \in R[\alpha]$  are the coefficients of  $g(Y)$  and we take  $b_n \neq 0$ . First we consider the case where  $g(Y)$  is not constant. We rearrange the equation and take the absolute values.

$$0 < |b_n\beta^n| < ||p^m| - b_{n-1}\beta^{n-1} - \dots - b_1\beta - b_0|$$

Dividing by  $|b_n\beta^n|$  gives

$$1 < \left| \frac{|p^m|}{b_n\beta^n} - \frac{b_{n-1}}{b_n\beta} - \dots - \frac{b_1}{b_n\beta^{n-1}} - \frac{b_0}{b_n\beta^n} \right|$$

This is impossible, because the righthand side is smaller than any positive element of  $R[\alpha]$ . The situation where  $g(Y)$  is constant is nearly identical. We can now write  $|p^m|f(\alpha, \beta, \frac{\alpha\beta}{p}) = h(\alpha)$  for a certain polynomial  $h(X) \in R[X]$ . We write out  $h(\alpha)$  explicitly to get

$$0 < c_l\alpha^l + c_{l-1}\alpha^{l-1} + \dots + c_1\alpha + c_0 < |p^m|$$

Where the  $c_i \in R$  are the coefficients of  $h(X)$  and we take  $c_l \neq 0$ . Notice that  $h(X)$  cannot be constant, since  $R \in DOR$ . Like before, we rearrange, take the absolute value and divide by  $|c_l\alpha^l|$ . This gives us

$$1 < \left| \frac{|p^m|}{c_l\alpha^l} - \frac{c_{l-1}}{c_l\alpha} - \dots - \frac{c_1}{c_l\alpha^{l-1}} - \frac{c_0}{c_l\alpha^l} \right|$$

This is also impossible, since the righthand side is smaller than any positive element of  $R$ . The assumption that  $0 < f(\alpha, \beta, \frac{\alpha\beta}{p}) < 1$  must have been false and we conclude that  $R[\alpha, \beta, \frac{\alpha\beta}{p}] \in DOR$ .  $\square$

### 4.4.1 Preserving properties

#### Normality

**Lemma 4.4.4.** *If  $S$  is normal and  $v$  is semiprime in  $S[\frac{w}{v}]$ , with  $v, w \in S$ , then  $S[\frac{w}{v}]$  is normal.*

**Proof.** [5] Let  $S, v$  and  $w$  be as stated above and suppose that  $x \in F(S[\frac{w}{v}])$  satisfies

$$x^n + b_{n-1}x^{n-1} + \dots + b_1x + b_0 = 0$$

with  $b_i \in S[\frac{w}{v}]$ . We have to show that  $x \in S[\frac{w}{v}]$ . Define  $V = \{v^n : n \in \mathbb{Z}_{\geq 0}\}$ . Then  $S[\frac{w}{v}] \subset SV^{-1}$ , so the coefficients  $b_i$  lie in  $SV^{-1}$ . Notice that  $V$  meets the conditions of lemma 4.2.6. So  $SV^{-1}$  is normal, as  $S$  is normal. Hence  $x \in SV^{-1}$ . Suppose that  $x \notin S[\frac{w}{v}]$ . Then there exists an  $a \in S[\frac{w}{v}]$  such that  $x = \frac{a}{v^m}$  and  $\frac{a}{v} \notin S[\frac{w}{v}]$ . So

$$\left(\frac{a}{v^m}\right)^n + b_{n-1}\left(\frac{a}{v^m}\right)^{n-1} + \dots + b_1\frac{a}{v^m} + b_0 = 0$$

We multiply by  $v^{nm}$  to get

$$a^n + b_{n-1}v^m a^{n-1} + \dots + b_1v^{(n-1)m}a + b_0v^{nm} = 0$$

From this we infer that  $v \mid a^n$  in  $S[\frac{w}{v}]$ . Then, because  $v$  is a semiprime in  $S[\frac{w}{v}]$ ,  $v \mid a$ . But this a contradiction with  $\frac{a}{v} \notin S[\frac{w}{v}]$ . We must conclude that  $x$  lies in  $S[\frac{w}{v}]$ . So  $S[\frac{w}{v}]$  is normal.  $\square$

**Lemma 4.4.5.** *The element  $\alpha$  is semiprime in  $R[\alpha, \beta, \frac{\alpha\beta}{p}]$ .*

**Proof.** [5] We use a series of isomorphisms to show that  $R[\alpha, \beta, \frac{\alpha\beta}{p}]/(\alpha)$  has no nilpotent elements. We view  $R[\alpha, \beta, \frac{\alpha\beta}{p}]$  as  $R[\alpha, \beta, X]/(\alpha\beta - pX)$ . Then we have

$$\begin{aligned} R[\alpha, \beta, \frac{\alpha\beta}{p}]/(\alpha) &\cong (R[\alpha, \beta, X]/(\alpha\beta - pX))/(\alpha) \\ &\cong R[\beta, X]/(pX) \cong (R[X]/(pX))[\beta] \end{aligned}$$

Strictly speaking,  $\alpha$  is not an element of  $R[\alpha, \beta, X]/(\alpha\beta - pX)$ , so  $(R[\alpha, \beta, X]/(\alpha\beta - pX))/(\alpha)$  is not defined. We should actually write  $(R[\alpha, \beta, X]/(\alpha\beta - pX))/(\bar{\alpha})$ , where  $\bar{\alpha} = \alpha \pmod{\alpha\beta - pX}$ , but as this leads to cumbersome notation, we assume this is understood here and in similar situations as well.

To show that  $(R[X]/(pX))[\beta]$  has no nilpotent elements, it is sufficient to show that  $R[X]/(pX)$  has no nilpotent elements. If  $pX \mid a^l$ , where  $a \in R[X]$  and  $l \in \mathbb{Z}_{>0}$ , then  $pX \mid a$ , since  $p$  and  $X$  are prime in  $R[X]$  by lemma 4.1.7 and lemma 4.3.3 respectively. Therefore  $R[X]/(pX)$  has no nilpotent elements. We conclude that  $\alpha$  is semiprime in  $R[\alpha, \beta, \frac{\alpha\beta}{p}]$ .  $\square$

**Lemma 4.4.6.** *If  $R \in \text{DOR}$  is normal, then  $R[\alpha, \beta, \frac{\alpha\beta}{p}]$  is normal as well.*

**Proof.** [5] We view  $R[\alpha, \beta, \frac{\alpha\beta}{p}]$  as  $R[\alpha, \frac{\alpha\beta}{p}, \frac{\alpha\beta}{\alpha}]$ . First of all  $R[\alpha]$  is normal by lemma 4.1.5, since  $\alpha$  is transcendental over  $F(R)$ , by its infinitude with

respect to  $R$ . Furthermore  $R[\alpha, \frac{\alpha\beta}{p}]$  is also normal by lemma 4.1.5, since  $\frac{\alpha\beta}{p}$  is transcendental over  $R(\alpha)$ , because  $\frac{\alpha\beta}{p} > \beta$  and by the fact that  $\beta$  is infinite with respect to  $R[\alpha]$ . Lastly then  $R[\alpha, \frac{\alpha\beta}{p}, \frac{\alpha\beta}{\alpha}]$  is normal by applying lemma 4.4.4 for  $v = \alpha$  and  $w = \alpha\beta$ .  $\square$

### Irreducibility

**Lemma 4.4.7.** *If  $q$  is irreducible in  $R$ , then  $q$  is also irreducible in  $R[\alpha, \beta, \frac{\alpha\beta}{p}]$ .*

**Proof.** [5] Let  $f(X, Y, Z), g(X, Y, Z) \in R[X, Y, Z]$  and suppose that  $f(\alpha, \beta, \frac{\alpha\beta}{p})g(\alpha, \beta, \frac{\alpha\beta}{p}) = q$ . Since  $f(X, Y, \frac{XY}{p})g(X, Y, \frac{XY}{p}) - q$  is zero for  $X = \alpha, Y = \beta$ , it must be identically zero, by algebraic independence of  $\alpha$  and  $\beta$ , as it is a polynomial with coefficients in  $F(R)$ . This means that both  $f$  and  $g$  are constant. The lemma then follows from the fact that  $f(\alpha, \beta, \frac{\alpha\beta}{p}), g(\alpha, \beta, \frac{\alpha\beta}{p}) \in R$  and the assumption that  $q$  is irreducible in  $R$ .  $\square$

### Primality

**Lemma 4.4.8.** *If  $q$  is prime in  $R$  and  $q \neq \pm p$ , then  $q$  is also prime in  $R[\alpha, \beta, \frac{\alpha\beta}{p}]$ .*

**Proof.** [5] We use a series of isomorphisms to show that  $R[\alpha, \beta, \frac{\alpha\beta}{p}]/(q)$  is a domain.

$$\begin{aligned} R[\alpha, \beta, \frac{\alpha\beta}{p}]/(q) &\cong (R[\alpha, \beta, X]/(\alpha\beta - pX))/(q) \\ &\cong ((R/(q))[\alpha, \beta, X]/(\alpha\beta - pX)) \cong (R/(q))[\alpha, \beta, \frac{\alpha\beta}{p}] \end{aligned}$$

Since  $q$  is prime in  $R$ ,  $R/(q)$  is a domain, which implies that  $(R/(q))[\alpha, \beta, \frac{\alpha\beta}{p}]$  is a domain.  $\square$

## 4.5 Extending to a model of open induction

In the next theorem, we assume  $R \in DOR$  to be countable. One may notice however, that no countability arguments are used. It is indeed the case that the theorem is easily generalized for rings of arbitrary cardinality. The only reason for not doing so, is that it makes the argument slightly clearer and the weaker version of the theorem is sufficient for our needs.

**Theorem 4.5.1.** *If  $R \in DOR$  is countable and there exists a ring homomorphism  $\varphi : R \rightarrow \hat{\mathbb{Z}}$ , then it is possible to extend  $R$  to  $S \in OI$ .*

**Proof.** [5] Using transfinite recursion on the class of ordinal numbers, we will construct a linearly ordered set of rings  $\{R_\sigma : \sigma < \omega_1\}$ , ordered by inclusion. Here  $\omega_1$  denotes the smallest uncountable ordinal. The indices agree with this order, that is to say  $R_\mu \subset R_\sigma \Leftrightarrow \mu < \sigma$ . For each  $R_\sigma$  there will exist a ring homomorphism  $\varphi_\sigma : R_\sigma \rightarrow \hat{\mathbb{Z}}$ . For these homomorphisms will hold that

if  $R_\mu \subset R_\sigma$ , then  $\varphi_\sigma$  is an extension of  $\varphi_\mu$ . The following steps are used to construct  $\{R_\sigma : \sigma < \omega_1\}$ .

1. Set  $R_0 = R$  and  $\varphi_0 = \varphi$ .
2. Suppose that  $\sigma$  is a limit ordinal and  $\sigma \neq 0$ .

Then we define  $R_\sigma = \bigcup_{\mu < \sigma} R_\mu$  and  $\varphi_\sigma = \bigcup_{\mu < \sigma} \varphi_\mu$ . It is easy to check that  $R_\sigma \in DOR$  and that  $\varphi_\sigma$  in fact defines the desired homomorphism. Notice that if for all  $\mu < \sigma$ ,  $R_\mu$  is countable, then  $R_\sigma$  is countable, as  $\sigma < \omega_1$ .

3. Suppose that  $\sigma$  is of the form  $\lambda + 2 \cdot n + 1$ , where  $\lambda$  is a limit ordinal and  $n \in \omega$ . Let  $\mu + 1 = \sigma$ .

We apply the construction from theorem 4.2.5 to extend  $R_\mu$  to a  $\mathbb{Z}$ -ring. Let  $R_\sigma$  be this  $\mathbb{Z}$ -ring. We also extend  $\varphi_\mu$  to  $\varphi_\sigma$  as described in theorem 4.2.5. Notice that using this construction,  $R_\sigma$  is countable if  $R_\mu$  is countable.

4. Suppose that  $\sigma$  is not a limit ordinal and  $\sigma$  is of the form  $\lambda + 2 \cdot n$ , where  $\lambda$  is a limit ordinal and  $n \in \omega$ . Let  $\mu + 1 = \sigma$ .

As will become clear, this recursion step also preserves the countability of the ring. So by transfinite induction we have that for each  $\tau < \omega_1$ ,  $R_\tau$  is countable and consequently  $C(R_\tau)$  is countable. Therefore there exists a bijection  $\Gamma_\tau : \omega \rightarrow C(R_\tau)$ . Notice that if  $\tau < \mu$ , then  $C(R_\tau) \subset C(R_\mu)$ . This allows us to form the surjection  $H_\mu : \omega \cdot \sigma \rightarrow C(R_\mu)$ , which we define by  $(n, \tau) \mapsto \Gamma_\tau(n)$ , when  $\omega \cdot \sigma$  is viewed as the Cartesian product  $\omega \times \sigma$ , ordered lexicographically, with the least significant position first. Now, if possible, select the smallest  $\delta \in \omega \cdot \sigma$  such that  $r \leq H_\mu(\delta) < r + 1$  does not hold for any  $r \in R_\mu$ . When no such  $\delta$  exists, let  $R_\sigma = R_\mu$ . When such a  $\delta$  does exist, we apply lemma 4.1.1 to the ring  $R_\mu$  with respect to the element  $H_\mu(\delta) \in C(R_\mu)$ . Let  $R_\sigma$  be the resulting ring. We extend  $\varphi_\mu$  to  $\varphi_\sigma$  by setting  $\varphi_\sigma(\xi) = 0$ , for the new element  $\xi$ . We are free to do so, as  $\xi$  is transcendental over  $F(R_\mu)$ . Notice that using this construction  $R_\sigma$  is indeed countable if  $R_\mu$  is countable.

We take  $S = \bigcup_{\sigma < \omega_1} R_\sigma$ . It is easily checked that  $S \in DOR$ . We use theorem 3.0.2 to prove the assertion that  $S \in OI$ . Let  $\alpha \in C(S)$ . Then  $\alpha$  is the root of some polynomial  $f(X) \in S[X]$ . Since  $S = \bigcup_{\sigma < \omega_1} R_\sigma$  and the set  $\{R_\sigma : \sigma < \omega_1\}$  is ordered by inclusion, we must have that  $f(X) \in R_\mu[X]$  for some  $\mu < \omega_1$ . From this we conclude that  $\alpha \in C(R_\mu)$ . Therefore there exists some  $\delta \in \omega \cdot \sigma$  such that  $\alpha = H_\mu(\delta)$ , where  $\sigma = \mu + 1$ . By construction, the ordinal  $\delta$  is treated in step 4 before reaching stage  $(1 + 2 \cdot \omega) \cdot \sigma = \omega \cdot \sigma$ , since steps 3 and 4 are alternated after applying step 1 or 2. It follows that there exists  $r \in R_{\omega \cdot \sigma} \subset S$  such that  $r \leq H_\mu(\delta) < r + 1$ . This leads us to conclude that  $S \in OI$ , as was to be proven.  $\square$

## 4.5.1 Preserving properties

### Normality

**Lemma 4.5.2.** *If  $R$  is normal, then  $S$  is normal.*

**Proof.** We show that steps 2 through 4 of theorem 4.5.1 preserve the normality of the ring. For step 2, let  $R_\sigma = \bigcup_{\mu < \sigma} R_\mu$ , with  $R_\mu$  normal for  $\mu < \sigma$ . Let  $f(X) \in R_\sigma$  be a monic polynomial. Since the rings are ordered by inclusion, there exists  $\mu < \sigma$  such that  $f(X) \in R_\mu[X]$ . Since we assumed that  $R_\mu$  is normal, the roots of  $f$  lie in  $F(R_\mu)$  and consequently in  $F(R_\sigma)$ . So  $R_\sigma$  is normal. Step 3 and 4 preserve normality by lemma 4.2.8 and lemma 4.1.5 respectively. Then, by transfinite induction, the rings  $R_\mu$  are normal for  $\mu < \omega_1$ . Using the same argument as we used for step 2, we see that the union  $S = \bigcup_{\sigma < \omega_1} R_\sigma$  is also normal, as asserted.  $\square$

### Primality

**Lemma 4.5.3.** *If  $p \in R$  is prime in  $R$  and  $\varphi(p) \in U(\hat{\mathbb{Z}})$ , then  $p$  is also prime in  $S$  as well as in the intermediate stages  $R_\mu$ , with  $\mu < \sigma$ .*

**Proof.** We show that steps 2 through 4 of theorem 4.5.1 preserve the primality of  $p$ . For step 2, let  $R_\sigma = \bigcup_{\mu < \sigma} R_\mu$ , with  $p$  prime in  $R_\mu$  for  $\mu < \sigma$ . Let  $r, s \in R_\sigma$  and suppose that  $p \mid rs$  in  $R_\sigma$ . Then  $pt = rs$ , with  $t \in R_\sigma$ . We must have that  $r, s, t \in R_\mu$ , for some  $\mu < \sigma$ . Therefore  $p \mid rs$  in  $R_\mu$ . Because  $p$  remains prime in  $R_\mu$ , either  $p \mid r$  or  $p \mid s$ . So suppose  $p \mid r$ . Then  $pu = r$ , with  $u \in R_\mu$ . Therefore  $u \in R_\sigma$ , so  $p \mid r$  holds in  $R_\sigma$  as well. We conclude that  $p$  is prime in  $R_\sigma$ . Step 3 and 4 preserve the primality of  $p$  by lemma 4.2.10 and lemma 4.1.7 respectively. Then, by transfinite induction,  $p$  is prime in the rings  $R_\mu$  for  $\mu < \omega_1$ . With the same argument as used for step 2,  $p$  is also prime in the union  $S = \bigcup_{\sigma < \omega_1} R_\sigma$ , which was to be proven.  $\square$

### Irreducibility

**Lemma 4.5.4.** *Suppose that the standard primes remain prime in  $R$ . If  $q \in R$  is irreducible in  $R$  and  $\varphi(q) \in U(\hat{\mathbb{Z}})$ , then  $q$  is irreducible in  $S$ .*

**Proof.** We show that steps 2 through 4 of theorem 4.5.1 preserve the irreducibility of  $q$ . For step 2, let  $R_\sigma = \bigcup_{\mu < \sigma} R_\mu$ , with  $q$  irreducible in  $R_\mu$  for  $\mu < \sigma$ . Let  $r, s \in R_\sigma$  and suppose that  $q \mid rs$  in  $R_\sigma$ . Then  $qt = rs$ , with  $t \in R_\sigma$ . We must have that  $r, s, t \in R_\mu$ , for some  $\mu < \sigma$ . Therefore  $q \mid rs$  in  $R_\mu$ . Because  $q$  is irreducible in  $R_\mu$ , either  $r$  or  $s$  is a unit in  $R_\mu$ . So, either  $r$  or  $s$  is a unit in  $R_\sigma$  and  $q$  is indeed irreducible in  $R_\sigma$ . For step 3, notice that by lemma 4.5.3 the standard primes remain prime at every stage. Therefore we may use lemma 4.2.9 to conclude that this step also preserves the irreducibility of  $q$ . Step 4 preserves the irreducibility of  $q$  by lemma 4.1.6. Then, by transfinite induction,  $q$  is irreducible in the rings  $R_\mu$  for  $\mu < \omega_1$ . With the same argument as used in step 2,  $q$  is also irreducible in the union  $S = \bigcup_{\sigma < \omega_1} R_\sigma$ .  $\square$

## Nonprimality

**Lemma 4.5.5.** *If  $r, s \in R$  and for all  $n \in \mathbb{Z}_{>0}$ ,  $r \nmid ns$  in  $R$ , then for all  $n \in \mathbb{Z}_{>0}$ ,  $r \nmid ns$  in  $S$ .*

**Proof.** We show that steps 2 through 4 of theorem 4.5.1 preserve the property that for all  $n \in \mathbb{Z}_{>0}$ ,  $r \nmid ns$ . For step 2, let  $R_\sigma = \bigcup_{\mu < \sigma} R_\mu$ , where  $R_\mu$  satisfies this property for  $\mu < \sigma$ . Suppose to the contrary that there exists  $m \in \mathbb{Z}_{>0}$ , such that  $r \mid ms$  in  $R_\sigma$ . Then  $rt = ms$ , with  $t \in R_\sigma$ . We must have that  $t \in R_\mu$ , for some  $\mu < \sigma$ . But then  $r \mid ms$  in  $R_\mu$ , contradicting our assumption. Step 23 and 4 preserve this property by lemma 4.2.11 and lemma 4.1.8 respectively. Then, by transfinite induction, the rings  $R_\mu$  have this property for  $\mu < \omega_1$ . Using the same argument as we used for step 2, we see that for the union  $S = \bigcup_{\sigma < \omega_1} R_\sigma$  also holds that for all  $n \in \mathbb{Z}_{>0}$ ,  $r \nmid ns$ , as asserted.  $\square$

## Nonmaximality

**Lemma 4.5.6.** *Suppose that  $p, q \in R$  and assume that for all  $n \in \mathbb{Z}_{>0}$  there is no  $r \in R$  such that  $qr \equiv n \pmod{p}$  in  $R/pR$ . Then for all  $n \in \mathbb{Z}_{>0}$  there is no  $r \in S$  such that  $qr \equiv n \pmod{p}$  in  $S/pS$ .*

**Proof.** We show that steps 2 through 4 preserve the property that for all  $n \in \mathbb{Z}_{>0}$  there is no  $r$  in that ring such that  $qr \equiv n \pmod{p}$ . For step 2, let  $R_\sigma = \bigcup_{\mu < \sigma} R_\mu$ , where  $R_\mu$  satisfies this property for  $\mu < \sigma$ . Suppose to the contrary that there exists  $n \in \mathbb{Z}$  and  $r \in R_\sigma$  such that  $qr \equiv n \pmod{p}$  in  $R_\sigma/pR_\sigma$ . Then  $qr = n + pt$ , for some  $t \in R_\sigma$ . There must exist some  $\mu < \sigma$  such that  $r, t \in R_\mu$ . Therefore  $qr \equiv n \pmod{p}$  in  $R_\mu$  contradicting our assumption. The property is also preserved in step 3 and 4 by lemma 4.2.12 and lemma 4.1.9 respectively. Then, by transfinite induction, the rings  $R_\mu$  have this property for  $\mu < \omega_1$ . With the same argument as used in step 2, the union  $S = \bigcup_{\sigma < \omega_1} R_\sigma$  also has the property that there is no  $r \in S$  such that  $qr \equiv n \pmod{p}$  in  $S/pS$ .  $\square$

## Chapter 5

# The main theorems

**Theorem 5.0.1.** *There is a normal model of open induction with an irreducible element which is not prime.*

**Proof.** [5] We start by adding a prime  $\pi$  to the ring  $\mathbb{Z} \in OI$  by applying lemma 4.3.2. According to lemma 4.3.4  $\mathbb{Z}[\pi] \in DOR$ . Next, we use lemma 4.4.1 to eliminate the prime  $\pi$  from the ring  $\mathbb{Z}[\pi]$ , by constructing the ring  $\mathbb{Z}[\pi][\alpha, \beta, \frac{\alpha\beta}{\pi}]$ . According to lemma 4.4.3,  $\mathbb{Z}[\pi][\alpha, \beta, \frac{\alpha\beta}{\pi}] \in DOR$ . We extend the ring homomorphism  $\varphi : \mathbb{Z} \rightarrow \hat{\mathbb{Z}}$  by putting  $\varphi(\pi) = \varphi(\alpha) = \varphi(\beta) = 1$ . We are free to make this choice since  $\pi, \alpha$  and  $\beta$  are algebraically independent over  $\mathbb{Q}$ . Since  $\mathbb{Z}[\pi][\alpha, \beta, \frac{\alpha\beta}{\pi}]$  is countable, the conditions of theorem 4.5.1 are met. We extend  $\mathbb{Z}[\pi][\alpha, \beta, \frac{\alpha\beta}{\pi}]$  to  $S \in OI$  using this theorem. Notice that  $\mathbb{Z}[\pi]$  is normal by lemma 4.1.5 and by the fact that  $\mathbb{Z}$  is normal. Therefore  $\mathbb{Z}[\pi][\alpha, \beta, \frac{\alpha\beta}{\pi}]$  is normal by lemma 4.4.6 and lastly  $S$  is normal by lemma 4.5.2.

Now we show that  $\pi$  is irreducible in  $S$ . By lemma 4.1.7 and lemma 4.4.8 the standard primes remain prime in  $\mathbb{Z}[\pi][\alpha, \beta, \frac{\alpha\beta}{\pi}]$ . Since  $\pi$  is prime, and therefore irreducible in  $\mathbb{Z}[\pi]$  by lemma 4.3.3,  $\pi$  is also irreducible in  $\mathbb{Z}[\pi][\alpha, \beta, \frac{\alpha\beta}{\pi}]$  by lemma 4.4.7. This means we can use lemma 4.5.4 to conclude that  $\pi$  is also irreducible in  $S$ .

Lastly we show that  $\pi$  is not a prime in  $S$ . By lemma 4.4.2  $\pi \nmid n\alpha$  and  $\pi \nmid n\beta$  in  $\mathbb{Z}[\pi][\alpha, \beta, \frac{\alpha\beta}{\pi}]$  for all  $n \in \mathbb{Z}_{>0}$ . By lemma 4.5.5 the ring  $S$  also has this property. We conclude that  $\pi$  is not a prime in  $S$ , as  $\pi \mid \alpha\beta$ , since  $\alpha\beta = \pi \frac{\alpha\beta}{\pi}$ , but  $\pi \nmid \alpha$  and  $\pi \nmid \beta$ .  $\square$

**Theorem 5.0.2.** *There is a normal model of open induction with a prime element which is not maximal.*

**Proof.** We begin by adding two primes  $\alpha$  and  $\beta$  to the ring  $\mathbb{Z} \in OI$  by applying lemma 4.1.1 twice. The ring  $\mathbb{Z}[\alpha][\beta]$  is discretely ordered by applying lemma 4.1.2 twice. We extend the ring homomorphism  $\varphi : \mathbb{Z} \rightarrow \hat{\mathbb{Z}}$  by putting  $\varphi(\alpha) = \varphi(\beta) = 1$ . Since  $\mathbb{Z}[\alpha][\beta]$  is countable, the conditions of theorem 4.5.1 are met. We extend  $\mathbb{Z}[\alpha][\beta]$  to  $S \in OI$  according to this theorem. Notice that  $\mathbb{Z}[\alpha][\beta]$  is normal by using lemma 4.1.5 twice and using the fact that  $\mathbb{Z}$  is normal. Hence  $S$  is normal by applying lemma 4.5.2.

Furthermore, the element  $\beta$  is prime in  $\mathbb{Z}[\alpha][\beta]$  by lemma 4.3.3 and the element  $\alpha$  is prime in  $\mathbb{Z}[\alpha][\beta]$  by lemma 4.3.3 and lemma 4.1.7. Therefore, by lemma 4.5.4  $\beta$  and  $\alpha$  are also prime in  $S$ .

Lastly we show that  $\beta$  is not a maximal element in  $S$ . We see that for all  $n \in \mathbb{Z}_{>0}$  there are no  $f(X, Y), g(X, Y) \in \mathbb{Z}[X][Y]$  such that  $\alpha f(\alpha, \beta) = n + \beta g(\alpha, \beta)$ , because  $\alpha$  and  $\beta$  are algebraically independent over  $\mathbb{Q}$ . Thus  $\alpha f(\alpha, \beta) \not\equiv n \pmod{\beta}$  in  $\mathbb{Z}[\alpha][\beta]/(\beta)$ . We use lemma 4.5.6 to conclude that for all  $n \in \mathbb{Z}_{>0}$  there is no  $r \in S$  such that  $\alpha r \equiv n \pmod{\beta}$  in  $S/\beta S$ . In particular  $\alpha r \not\equiv 1 \pmod{\beta}$ . Because  $\alpha$  is prime in  $S$  and unequal to  $\pm\beta$ ,  $\beta \nmid \alpha$ , so that  $\alpha \not\equiv 0 \pmod{\beta}$  in  $S/\beta S$ . We conclude that  $S/\beta S$  has a nonzero element which is not invertible and is therefore not a field. Thus  $\beta$  is not a maximal element of  $S$ .  $\square$

**Theorem 5.0.3.** *There is a normal nonstandard model of open induction in which every positive nonstandard even integer is the sum of two positive primes.*

**Proof.** [5] In theorem 5.0.1 and theorem 5.0.2 we have seen that there exist normal models of open induction which are nonstandard. Take a normal nonstandard model of open induction  $R$  and denote its cardinality as  $\aleph_\gamma$ . Analogous to theorem 4.5.1 we will construct a linearly ordered set of rings  $\{R_\sigma : \sigma < \omega_{\gamma+1}\}$ , ordered by inclusion. Here  $\omega_{\gamma+1}$  stands for the smallest ordinal with cardinality  $\aleph_{\gamma+1}$ . Again, the indices agree with this order and for each  $R_\sigma$  there will exist a ring homomorphism  $\varphi_\sigma : R_\sigma \rightarrow \hat{\mathbb{Z}}$ . For the homomorphisms will hold that if  $R_\mu \subset R_\sigma$ , then  $\varphi_\sigma$  is an extension of  $\varphi_\mu$ . We use the following steps to construct  $\{R_\sigma : \sigma < \omega_{\gamma+1}\}$ .

1. Set  $R_0 = R$ . Since  $R \in OI$ , we have that  $R \in ZR$  by corollary 2.2.6. Thus by lemma 4.2.4 there exists a ring homomorphism  $Rem : R \rightarrow \hat{\mathbb{Z}}$ . Set  $\varphi = Rem$ .
2. Suppose that  $\sigma$  is a limit ordinal and  $\sigma \neq 0$ .  
Then we define  $R_\sigma = \bigcup_{\mu < \sigma} R_\mu$  and  $\varphi_\sigma = \bigcup_{\mu < \sigma} \varphi_\mu$ . It is easy to check that  $R_\sigma \in DOR$  and that  $\varphi_\sigma$  in fact defines the desired homomorphism. Notice that if for all  $\mu < \sigma$ ,  $|R_\mu| = \aleph_\gamma$ , then  $|R_\sigma| = \aleph_\gamma$ , as  $\sigma < \omega_{\gamma+1}$ .
3. Suppose that  $\sigma$  is of the form  $\lambda + 3 \cdot n + 1$ , where  $\lambda$  is a limit ordinal and  $n \in \omega$ . Let  $\mu + 1 = \sigma$ .  
We apply the construction from theorem 4.2.5 to extend  $R_\mu$  to a  $\mathbb{Z}$ -ring. Let  $R_\sigma$  be this  $\mathbb{Z}$ -ring. We also extend  $\varphi_\mu$  to  $\varphi_\sigma$  as described in theorem 4.2.5. Notice that using this construction,  $|R_\sigma| = \aleph_\gamma$  if  $|R_\mu| = \aleph_\gamma$ .
4. Suppose that  $\sigma$  is not a limit ordinal and  $\sigma$  is of the form  $\lambda + 3 \cdot n + 2$ , where  $\lambda$  is a limit ordinal and  $n \in \omega$ . Let  $\mu + 1 = \sigma$ .

As will become clear, each recursion step preserves the cardinality of the ring. So by transfinite induction we have that for each  $\tau < \omega_{\gamma+1}$ ,  $|R_\tau| = \aleph_\gamma$  and consequently  $|C(R_\tau)| = \aleph_\gamma$ . Therefore there exists a bijection  $\Gamma_\tau : \omega_\gamma \rightarrow C(R_\tau)$ . We form the surjection  $H_\mu : \omega_\gamma \cdot \sigma \rightarrow C(R_\mu)$ , which we define by  $(\nu, \tau) \mapsto \Gamma_\tau(\nu)$ , when  $\omega_\gamma \cdot \sigma$  is viewed as the Cartesian product  $\omega_\gamma \times \sigma$ , ordered lexicographically, with the least significant position first. Now, if possible, select the smallest  $\delta \in \omega_\gamma \cdot \sigma$  such that  $r \leq H_\mu(\delta) < r + 1$  does not hold for any  $r \in R_\mu$ . When no such  $\delta$  exists, let  $R_\sigma = R_\mu$ . When

such a  $\delta$  does exist, we apply theorem 4.1.1 to the ring  $R_\mu$  with respect to the element  $H_\mu(\delta) \in C(R_\mu)$ . Let  $R_\sigma$  be the resulting ring. We extend  $\varphi_\mu$  to  $\varphi_\sigma$  by setting  $\varphi_\sigma(\xi) = 0$ , for the new element  $\xi$ . Notice that using this construction  $|R_\sigma| = \aleph_\gamma$  if  $|R_\mu| = \aleph_\gamma$ .

5. Suppose that  $\sigma$  is not a limit ordinal and  $\sigma$  is of the form  $\lambda + 3 \cdot n$ , where  $\lambda$  is a limit ordinal and  $n \in \omega$ . Let  $\mu + 1 = \sigma$ .

Since for each  $\tau < \omega_{\gamma+1}$ ,  $|R_\tau| = \aleph_\gamma$ , there exists a bijection  $\Lambda_\tau : \omega_\gamma \rightarrow R_\tau$ . We form the surjection  $G_\mu : \omega_\gamma \cdot \sigma \rightarrow R_\mu$ , which we define by  $(\nu, \tau) \mapsto \Lambda_\tau(\nu)$ , when  $\omega_\gamma \cdot \sigma$  is viewed as the Cartesian product  $\omega_\gamma \times \sigma$ , ordered lexicographically, with the least significant position first. If possible, select the smallest  $\delta \in \omega_\gamma \cdot \sigma$  such that  $G_\mu(\delta)$  is a positive even nonstandard integer which is not the sum of two primes. When no such  $\delta$  exists, let  $R_\sigma = R_\mu$ . When such a  $\delta$  does exist, we use lemma 4.1.1 to add a new prime  $\alpha$  to  $R_\mu$  and set  $R_\sigma = R_\mu[\alpha]$ . When applying the lemma, we choose the cut  $C$  to be the set  $\{r \in R_\mu : \exists n \in \mathbb{Z}(r < n)\}$ . This ensures that  $\alpha$  is positive, but smaller than any positive nonstandard element of  $R_\mu$ . In particular,  $G_\mu(\delta) - \alpha$  is positive. We expand  $\varphi_\mu$  in such a way that  $\varphi_\sigma(\alpha)$  and  $\varphi_\sigma(G_\mu(\delta) - \alpha)$  are both in  $U(\hat{\mathbb{Z}})$ . To see that this is in fact possible, we define  $\varphi_{\sigma,p} : R_\sigma \rightarrow \mathbb{Z}_p$  as the restriction of  $\varphi_\sigma$  to the factor  $\mathbb{Z}_p$  of  $\prod_p \mathbb{Z}_p$  and write  $\varphi_{\sigma,p}(G_\mu(\delta)) = (a_1, a_2, a_3, \dots)$ . Now, if  $a_1 \equiv 0 \pmod{p}$ , choose  $\varphi_{\sigma,p}(\alpha) = \varphi_{\sigma,p}(1)$ . Then both  $\varphi_{\sigma,p}(\alpha)$  and  $\varphi_{\sigma,p}(G_\mu(\delta) - \alpha) = \varphi_{\sigma,p}(G_\mu(\delta)) - \varphi_{\sigma,p}(1)$  are invertible, since the first element of their sequence is nonzero. If  $a_1 \not\equiv 0 \pmod{p}$ , choose  $\varphi_{\sigma,p}(\alpha) = -\varphi_{\sigma,p}(G_\mu(\delta))$ . Again, this is to arrange that  $\varphi_{\sigma,p}(\alpha)$  and  $\varphi_{\sigma,p}(G_\mu(\delta) - \alpha) = 2\varphi_{\sigma,p}(G_\mu(\delta))$  are invertible, by forcing the first element of their sequence to be nonzero. For this step it is crucial that  $G_\mu(\delta)$  is even, otherwise we run into trouble for  $p = 2$ . In this way we define the value of  $\varphi_\sigma(\alpha)$  by defining the value of each of its factors  $\varphi_{\sigma,p}(\alpha)$ . Both  $\varphi_\sigma(\alpha)$  and  $\varphi_\sigma(G_\mu(\delta) - \alpha)$  are now invertible, since all their factors  $\varphi_{\sigma,p}(\alpha)$  and  $\varphi_{\sigma,p}(G_\mu(\delta) - \alpha)$  are. Notice that using this construction  $|R_\sigma| = \aleph_\gamma$  if  $|R_\mu| = \aleph_\gamma$ .

We take  $S = \bigcup_{\sigma < \omega_{\gamma+1}} R_\sigma$ . It is easily checked that  $S \in \text{DOR}$ . We use theorem 3.0.2 to prove that  $S$  is a model of open induction. Let  $\alpha \in C(S)$ . Then  $\alpha$  is the root of some polynomial  $f(X) \in S[X]$ . We must have that  $f(X) \in R_\mu[X]$  for some  $\mu < \omega_{\gamma+1}$ . From this we conclude that  $\alpha \in C(R_\mu)$ . Therefore there exists some  $\delta \in \omega_\gamma \cdot \sigma$  such that  $\alpha = H_\mu(\delta)$ , where  $\sigma = \mu + 1$ . By construction, the ordinal  $\delta$  is treated in step 4 before reaching stage  $(1 + 3 \cdot \omega_\gamma) \cdot \sigma = \omega_\gamma \cdot \sigma$ , since steps 3, 4 and 5 are followed in turn after applying step 1 or 2. It follows that there exists  $r \in R_{\omega_\gamma \cdot \sigma} \subset S$  such that  $r \leq H_\mu(\delta) < r + 1$  and therefore  $S$  is a model of open induction.

To prove that  $S$  is normal, we show that steps 2 to 5 preserve the normality of the ring, analogous to lemma 4.5.2. For step 2, let  $R_\sigma = \bigcup_{\mu < \sigma} R_\mu$ , with  $R_\mu$  normal for  $\mu < \sigma$  and let  $f(X) \in R_\sigma$  be monic. There exists  $\mu < \sigma$  such that  $f(X) \in R_\mu[X]$ . Since we assumed that  $R_\mu$  is normal, the roots of  $f$  lie in  $F(R_\mu)$  and consequently in  $F(R_\sigma)$ . So  $R_\sigma$  is normal. Step 3 preserves normality by lemma 4.2.8. Step 4 and 5 preserve normality by lemma 4.1.5. Thus, by transfinite induction, the rings  $R_\mu$  are normal for  $\mu < \omega_{\gamma+1}$ . By the same argument as used for step 2, the union  $S = \bigcup_{\sigma < \omega_{\gamma+1}} R_\sigma$  is normal.

To show that every every positive nonstandard even integer is the sum of two primes, we first prove that if  $\alpha \in R_\mu$  is prime in  $R_\mu$  and  $\varphi_\mu(\alpha) \in U(\hat{\mathbb{Z}})$ , then  $\alpha$  is prime in  $R_\sigma$ , for  $\mu < \sigma < \omega_{\gamma+1}$  and in  $S$  as well, analogous to lemma 4.5.3. We show that steps 2 through 5 preserve the primality of  $\alpha$ . For step 2, let  $R_\sigma = \bigcup_{\mu < \sigma} R_\mu$ , with  $\alpha$  prime in  $R_\mu$  for  $\mu < \sigma$ . Let  $r, s \in R_\sigma$  and suppose that  $\alpha \mid rs$  in  $R_\sigma$ . We must have that  $\alpha \mid rs$  in  $R_\mu$ , for some  $\mu < \sigma$ . Because  $\alpha$  remains prime in  $R_\mu$ , either  $\alpha \mid r$  or  $\alpha \mid s$  in  $R_\mu$ . Therefore  $\alpha \mid r$  or  $\alpha \mid s$  in  $R_\sigma$  as well. We conclude that  $\alpha$  is prime in  $R_\sigma$ . Step 3 preserves the primality of  $\alpha$  by lemma 4.2.10. Step 4 and 5 preserve the primality of  $\alpha$  by lemma 4.1.7. Then, by transfinite induction,  $\alpha$  is prime in  $R_\sigma$  for  $\mu < \sigma < \omega_{\gamma+1}$ . With the same argument as used for step 2,  $\alpha$  is also prime in  $S = \bigcup_{\sigma < \omega_{\gamma+1}} R_\sigma$ .

Now suppose that  $\beta \in S$  is a positive nonstandard even integer. Then  $\beta \in R_\mu$  for some  $\mu < \omega_{\gamma+1}$ . Therefore there exists some  $\delta \in \omega_\gamma \cdot \sigma$  such that  $\beta = G_\mu(\delta)$ , where  $\sigma = \mu + 1$ . By construction, the ordinal  $\delta$  is treated in step 5 before reaching stage  $(1 + 3 \cdot \omega_\gamma) \cdot \sigma = \omega_\gamma \cdot \sigma$ , since steps 3, 4 and 5 are followed in turn after applying step 1 or 2. Hence there exists an element  $\alpha \in R_{\omega_\gamma \cdot \sigma} \subset S$  such that both  $\alpha$  and  $\beta - \alpha$  are positive primes in  $S$ .  $\square$

# Bibliography

- [1] Robert M. Alain. *A course in p-adic analysis*. Graduate texts in mathematics, Springer, 2000.
- [2] Lou van den Dries. *Some model theory and number theory for models of weak systems of arithmetic*. Model theory of algebra and arithmetic, 346-362, 1980.
- [3] Haim Gaifman. *Non-standard models in a broader perspective*. Nonstandard models of arithmetic and set theory, 1-22, Contemporary mathematics 361, 2004.
- [4] Richard Kaye. *Models of Peano arithmetic*. Oxford logic guides 15, 1991.
- [5] Angus Macintyre and David Marker. *Primes and their residue rings in models of open induction*. Annals of Pure and Applied Logic 43, 57-77, Lecture notes in mathematics 834, 1989.
- [6] Jaap van Oosten. *Introduction to Peano arithmetic*. 1999.
- [7] J. C. Shepherdson. *A non-standard model for a free variable fragment of number theory*. Journal of symbolic logic 30, 389-390, 1965.
- [8] A.J. Wilkie. *Some results and problems on weak systems of arithmetic*. Logic colloquium 77, 285-296, Studies in logic and the foundations of mathematics 96, 1978.
- [9] [http://www.math.columbia.edu/~nava/Exercise\\_2.pdf](http://www.math.columbia.edu/~nava/Exercise_2.pdf)