

# INTUITIONISTIC ALGEBRA

## THEORY AND SHEAF MODELS

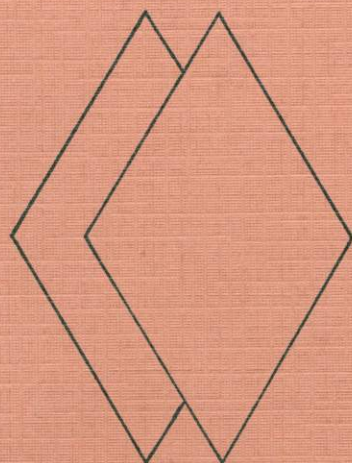
INTUITIONISTIC ALGEBRA

—

W.B.G. RUITENBURG

—

1982



W.B.G. RUITENBURG

**W.B.G. Ruitenburg**  
Huis de Vlietlaan 14, Utrecht

Receptie na afloop van de promotie in het Academieggebouw  
Domplein 29, Utrecht

## Stellingen

behorende bij het proefschrift INTUITIONISTIC ALGEBRA, THEORY AND SHEAF MODELS van Wim Ruitenburg.

1. Een intuïtionistisch lichaam zoals geïntroduceerd door Heyting is een (intuïtionistische) lokale ring waarvoor geldt:

$\forall x(\neg Ex^{-1} \rightarrow x = 0)$ . De theorie van intuïtionistische lichamen is conservatief over het meetkundige fragment van de theorie van de nilpotentvrije lokale ringen, d.w.z. lokale ringen waarvoor geldt  $\forall x(x^2 = 0 \rightarrow x = 0)$ .

(Dit proefschrift 2.6.2, 2.9.5)

2. Zij  $A$  een commutatieve ring in een topos  $\mathcal{E}$ , eventueel zonder verwijderingsrelatie. Beschouw de constructie van de lokale ring  $\text{Spec}(A)$  over de complete Heyting algebra  $\sqrt{A}$  van radikale idealen. Als  $A$  nilpotentvrij is dan is  $\text{Spec}(A)$  een lichaam met verwijderingsrelatie gedefinieerd door inverteerbaarheid:  $x \# y \leftrightarrow \exists E(x-y)^{-1}$ . Indien voor  $A$  axioma  $C_1$  of axioma  $C_2$  geldt dan voldoet ook  $\text{Spec}(A)$  daaraan. Indien  $A$  beslisbare gelijkheid heeft, d.w.z. als voor  $A$  geldt  $\forall x(x = 0 \vee \neg x = 0)$  dan heeft ook  $\text{Spec}(A)$  beslisbare gelijkheid.

([Fo 2], blz. 376)

3. Zij  $\sigma_1, \dots, \sigma_n$  een groep verwijderde automorfismen van  $L$  met vast lichaam  $K$ . Dan heeft  $(L/K)$  een normale basis  $\sigma_1(x), \dots, \sigma_n(x)$  voor een  $x \in L$ .

(Dit proefschrift 4.11.10)

4. De axioma's  $C_1$  en  $C_2$  blijven behouden onder deellichamen, in tegenstelling tot het axioma  $D$ .

(Dit proefschrift 5.2)

5. Zij A en B  $m \times n$ -matrices over een ring R. A en B heten equivalent als er een inverteerbare  $m \times m$ -matrix S is en een inverteerbare  $n \times n$ -matrix T zodat  $SA = BT$ .

Zij K een lichaam waarvoor axioma D geldt. Laat  $\bar{K}$  uit K verkregen worden door uitdelen naar de equivalentierelatie  $d \sim e \leftrightarrow d|e \wedge e|d$ . Voor iedere  $m \times n$ -matrix A met  $m \leq n$  is er een unieke rij objecten  $\bar{d}_1, \dots, \bar{d}_m$  uit  $\bar{K}$  zodat A equivalent is met de diagonaalmatrix  $\begin{pmatrix} \bar{d}_1 & & & \\ & \dots & & \\ & & \bar{d}_m & \\ & & & \ddots \end{pmatrix}$ , en zó dat  $d_i | d_{i+1}$ . Twee  $m \times n$ -matrices zijn equivalent dan en slechts dan als ze dezelfde rij  $\bar{d}_1, \dots, \bar{d}_m$  hebben.

(Dit proefschrift 5.2.2)

6. Zij R een klassieke unieke factorisatie domein waarvoor de volgende operaties berekenbaar zijn:

- (1) de ring operaties  $+, \cdot, -, =,$
  - (2) een operatie  $d: R \times R \rightarrow \text{RUIN}$  met voor alle  $x, y \in R$  óf  $d(x, y)$  is een getal zodat  $x$  ten hoogste  $d(x, y)$  maal deelbaar is op  $y$ , óf  $x^{-1}$  bestaat en  $d(x, y) = x^{-1}y$ , óf  $y = 0$  en  $d(x, y) = 0 \in R$ ,
  - (3) een operatie  $g: R \times R \rightarrow R^3$  die voor ieder paar  $x, y \in R$  een drietal  $g(x, y) = (h, x_1, y_1)$  levert met  $hx_1 = x$ ,  $hy_1 = y$  en  $h$  is de ggd van  $x, y$ .
- Als er een algoritme is voor het oplossen van lineaire vergelijkingen over R, dan is er ook een algoritme voor  $R[X]$ .

7. Zij  $\varphi(p)$  een propositielogische formule in  $p$ , mogelijk met extra parameters. Definieer  $\varphi^0(p) = p$  en  $\varphi^{n+1}(p) = \varphi(\varphi^n(p))$  voor alle  $n$ . Dan is er een  $m$  zodat

$$\vdash \varphi^m(p) \leftrightarrow \varphi^{m+2}(p).$$

8. Zij  $\Omega$  een complete Heyting algebra in een topos  $\mathcal{E}$  en zij  $J: \Omega \rightarrow \Omega$  een afbeelding in  $\mathcal{E}$  waarvoor geldt:  $J(p \wedge q) = Jp \wedge Jq$  en  $p \leq Jp$ . Dan is er een  $w: \Omega \rightarrow \Omega$  waarvoor geldt:

- (1)  $w$  is een nucleus ( $w(p \wedge q) = wp \wedge wq$ ,  $p \leq wp$ ,  $wp = wwp$ ),  
 (2)  $w$  is de "kleinste vaste punt" operator:  $Jwp = wp$  en voor alle  $q \geq p$  met  $Jq = q$  geldt  $q \geq wp$ .

Zij  $e: \Omega' \rightarrow \Omega$  de gelijkmaker van  $J$  en  $\text{id}: \Omega \rightarrow \Omega$ . Dan is

- (1)  $\Omega'$  is een complete Heyting algebra,  
 (2)  $w = e\pi$  voor een unieke  $\pi: \Omega \rightarrow \Omega'$ .

Voor het object  $\pi$  in de topos  $E/\Omega'$  geldt nu:

$\pi$  is een tralie zodat voor iedere bewoonde  $S \subseteq \pi$  een kleinste bovengrens bestaat en zo dat de volgende distributieve wet geldt:  
 $p \wedge \bigvee_{s \in S} s = \bigvee_{s \in S} p \wedge s$ . Op  $\pi$  kunnen we dan een implicatie definiëren, d.w.z. een afbeelding  $\rightarrow: \pi \times \pi \rightarrow \pi$  waarvoor geldt  $p \wedge q \leq r \Leftrightarrow p \leq q \rightarrow r$ .

Voor de geïnduceerde  $J: \pi \rightarrow \pi$  geldt nu:

$J$  is een Löb-operator op  $\pi$  ( $J(p \wedge q) = Jp \wedge Jq$ ,  $p \leq Jp$ ,  $Jp \rightarrow p \leq p$ ).

9. Zij  $K$  een priemlichaam  $\mathbb{F}_p$  of het klassieke lichaam der complexe getallen  $\mathbb{C}$ . Dan geldt het volgende schema van "totale inductie": voor iedere eerste-orde uitspraak  $\varphi(x)$  over  $K$  geldt:

$$\forall x(\varphi(x) \rightarrow \varphi(x+1)) \rightarrow (\exists x\varphi(x) \rightarrow \forall x\varphi(x)).$$

10. Bij het damspel met twintig schijven tegen één en bij het damspel met twintig schijven tegen twee met als doel het eerst de eigen schijven van het speelbord te krijgen is er een winnende strategie voor de speler met de twintig schijven.

8 juni 1982

(Dit proefschrift is afgegeven op 11.11.10)

4. De axioma's  $\Omega_1$  en  $\Omega_2$  blijven behouden onder deellichamen, in tegenstelling tot het axioma  $\Omega$ .

(Dit proefschrift is afgegeven op 11.11.10)

Acknowledgments

INTUITIONISTIC ALGEBRA

THEORY AND SHEAF MODELS

To my promotor, D. van Dalen, I am especially grateful for his stimulation and for his careful checking of the thesis. I thank him also for introducing me to the work of A. Heyting. I am also indebted to M. Beeson for checking a preliminary version of this manuscript. The following people have helped me by conversations or correspondence: K. Koymans, J. Lodder, L. Noordijk, B. Ruitenburg, A. Troelstra and A. Visser.

PROEFSCHRIFT

I thank Louis Verkerk for his careful reading of parts of this thesis.

ter verkrijging van de graad van doctor in de Wiskunde en Natuurwetenschappen aan de Rijksuniversiteit te Utrecht, op gezag van de Rector Magnificus Prof. Dr. M.A. Bouman, volgens besluit van het College van Decanen in het openbaar te verdedigen op dinsdag 8 juni 1982 des namiddags te 4.15 uur

door

WILLEM BASTIAAN GIJSBERTUS

RUITENBURG

geboren op 10 januari 1955

te Utrecht

*Promotor:* PROF. DR. D. VAN DALEN

### *Acknowledgements*

To my promotor, D. van Dalen, I am especially grateful for his stimulation and for his careful checking of the thesis. I thank him also for introducing me to the work of A. Heyting. I am also indebted to M. Beeson for checking a preliminary version of this manuscript.

The following people have helped me by conversations or correspondence: K. Koymans, J. Lodder, I. Moerdijk, B. Ruitenburg, A. Troelstra and A. Visser.

I thank Lenie Verkerk for her careful typing of parts of this thesis.

Ik bedank ook mijn ouders voor de wijze waarop zij hebben bijgedragen aan het tot stand komen van dit proefschrift.



## Contents

0. INTRODUCTION	1
1. PRELIMINARIES	5
1.1 <i>The presence of a natural number object</i>	5
1.2 <i>Apartness</i>	8
1.3 <i>Sheaf models</i>	11
1.4 <i>Kripke models</i>	18
2. ALGEBRAIC STRUCTURES	21
2.1 <i>Definitions</i>	21
2.2 <i>Groups</i>	23
2.3 <i>Rings</i>	25
2.4 <i>Integral domains</i>	26
2.5 <i>Fields</i>	30
2.6 <i>Local rings</i>	32
2.7 <i>Modules</i>	34
2.8 <i>Models of group theory</i>	36
2.9 <i>Models of ring theory</i>	38
2.10 <i>Models of module theory</i>	43
3. LINEAR ALGEBRA	45
3.1 <i>Local rings and fields</i>	45
3.2 <i>Dependence, independence and freedom</i>	47
3.3 <i>The Austauschsatz</i>	50
3.4 <i>Independence and freedom over AK-fields</i>	52
3.5 <i>Degree and dimension</i>	53
3.6 <i>The rank of a matrix</i>	54

3.7	<i>The determinant</i>	57
3.8	<i>Left and right inverses</i>	61
3.9	<i>The Generators Theorem</i>	63
3.10	$R^X$	68
4.	<b>GALOIS THEORY</b>	75
4.1	<i>Field extensions</i>	75
4.2	<i>The degree of a polynomial. Division algorithms</i>	76
4.3	<i>Coideals of polynomials and power series</i>	79
4.4	<i>Relative primality</i>	84
4.5	<i>Primality and minimality</i>	90
4.6	<i>Separable extensions</i>	96
4.7	<i>Morphisms and subfields</i>	101
4.8	<i>Characters</i>	104
4.9	<i>Degrees over a fixed field</i>	105
4.10	<i>Examples</i>	108
4.11	<i>Algebraic freedom and normal bases</i>	110
4.12	<i>Subfields generated by subobjects</i>	115
4.13	<i>Galois pairs</i>	117
5.	<b>PRIMALITY AND INVERTIBILITY</b>	122
5.1	<i>Extensions by one element</i>	122
5.2	$C_i D$ -fields	126
	<i>Index</i>	134
	<i>References</i>	137
	<i>Samenvatting</i>	141
	<i>Curriculum vitae</i>	143

## 0. INTRODUCTION

In some parts of constructive algebra there is a routine of providing new proofs of old results by carefully and almost literally constructivizing classical proofs. In this thesis we direct our attention to those parts where this does not hold. The following kinds of problems occur. In the first place we have to formulate an adequate theory which generalizes the classical version. A good intuitionistic theory must be sufficiently general such that it includes a fair number of interesting examples which are overlooked by the classical theory. On the other hand a good intuitionistic theory must be strong enough to enable us to derive the basic structural properties. In this thesis we only consider intuitionistic theorems that hold classically. So we are not concerned with the problem of handling essentially new principles (e.g. uniformity or continuity). Our task is to find new ways and means to circumvent the obstacles presented by the nature of non-classical logic. This includes that we have to work with more generalized notions such as relative primality modulo  $\varphi$  (4.4.2). In other cases we have to give detailed proofs for (parts of) theorems which classically follow from some general observations (like the existence of dimension, see 4.1.2). Peculiar to our intuitionistic algebra is the presence of an apartness relation. The additional structure we get provides us with a good intuitionistic theory in the above sense.

Intuitionistic algebra as presented here differs from versions like Seidenberg's, cf. [Se 1], in that it is more general and in that it allows for a considerably wider class of models. We do not use the traditionally constructive strong conditions on

fields like: for all  $x$   $x = 0$  or  $x$  is invertible. To put it in another way, intuitionistic algebra is not designed for discrete structures and phenomena as e.g. in recursive algebra but it also covers continuous algebra. A theorem usually remains true after small deformations of the input. This can be illustrated by the sheaf models. In short our algebra is more in the spirit of Brouwer than of Kronecker.

We interpret our intuitionistic statements in sheaf models over topological spaces. Sheaf models have the pleasant unifying virtue that they cover also the well-known topological models, Kripke-models and Beth-models. Topos theory provides even more general model notions, but we shall not have occasion to use them here. Interpretations of theorems of intuitionistic algebra in sheaves provide a connection with classical algebra via the stalk structures. Therefore it is convenient to have a class of formulas for which the interpretation is easy. Such a class is that of the geometric formulas. They are true in a sheaf model if and only if they hold under the classical interpretation in the stalk structures. We found it more convenient to work with the more general syntactic notion  $N$  plus  $P$  for formulas, although this class is logically equivalent to that of the geometric formulas.

The hard core of (intuitionistic) algebra is the solving of linear equations. It turns out that many proofs in constructive algebra basically use, at least partially, the reduction of problems to related problems in linear algebra. Most results in chapter 3, hence also those that can be reduced to questions in linear algebra, are finitistic in nature. Given some elementary properties of e.g. apartness we proceed almost entirely

finitistically, be it that the model theoretic considerations may be more general. In particular no higher-order non-classical principles are involved. We will, just as Heyting, use a good deal of determinant theory. The constructive aspects of determinant theory are more important in constructive algebra, because we do not have a powerful dimension theory as in classical linear algebra. Another aspect of determinant theory is that it enables us to reduce quantifier complexity, see 3.7. There is a striking resemblance between the linear algebra of fields and the linear algebra of local rings. This is not so surprising since local ring theory is geometric and many statements of linear algebra one is traditionally interested in are also geometric. Moreover, an intuitionistic field (with apartness) is a local ring with one extra axiom:  $\neg x \neq 0 \rightarrow x = 0$  (and - in the stalks of the field models - we find that there are no nilpotents in the local rings, cf. 2.9.5).

In the development of Galois theory the construction of field extensions is considerably more complicated than in classical field theory. We follow Scott in using coideals instead of ideals to define an apartness relation on extensions. Intuitionistic Galois theory not only differs from the classical one in method but also in form and content, e.g. for relative primality and for separability we have to introduce syntactically more complicated notions. One has to generalize relative primality beyond the classical framework to relative primality modulo  $\varphi$  (cf. 4.4.2). For our purpose the most suitable approach to Galois connections is via subfields and cogroups instead of subfields and subgroups. Our strengthened form of the fundamental theorem of Galois theory (4.13.3) required that the image

of an element  $\alpha$  of the field under an automorphism is apart from  $\alpha$  or is identical with  $\alpha$ .

In intuitionistic algebra the question of invertibility of elements in algebraic extensions  $K[\alpha]$  is considerably more complicated than in the classical case. There is a great variety of conditions that ensure invertibility. The conditions we give in chapter 5 are of a mixed logical and algebraic nature. They stress the importance of considering fields and local rings simultaneously.

The development of intuitionistic algebra in the presence of apartness was started by Heyting, cf. [He 1]. In his paper [He 2] Heyting has given the theory a firm basis. It is fair to say that we have continued in his tradition. In our notation and presentation we follow D. Scott, cf. [Sc 1] or [Sc 2].

There are parallels with the work of A. Kock ([Ko 1]). See also the papers by J. Kennison, C. Mulvey, G. Reyes and G. Wraith ([Ke 2], [Mu 1], [Re 1], [Wr 1]).

# 1. PRELIMINARIES

## 1.1 The presence of a natural number object

In this chapter we present some basic facts about intuitionistic logic and model theory. Although we shall not formalize all our intuitionistic statements, it is helpful to keep some formal system in mind. In this chapter as well as in the other chapters we shall use a higher order logic as presented in [Fo 1], p.1060 or [Sc 2], p.685. In many statements we use the presence of a natural number object  $\mathbb{N}$  ([Fo 1], p.1086, [Sc 2], p694), but we shall not mention that explicitly.

The formal system of [Fo 1] and [Sc 2] has several features and is more complicated than first-order intuitionistic logic. For first-order logic there is an axiomatization which is simpler to present. The quantifiers  $\forall$  and  $\exists$  range over a fixed domain  $A$ . The derivability relation  $\vdash$  will be defined as follows.

1.1.1. Definition. (1) A sequent is an expression of the form  $\phi \vdash \psi$  where  $\phi$  and  $\psi$  are first-order formulas.

(2) The set of derivable sequents is the smallest set of sequents, closed under all substitution instances of the following schemas (a single line means that if all sequents above the line are derivable, then so are the sequents below the line. A double line means the same as a single line, but in both directions).

$$\begin{array}{c}
 \phi \vdash \phi \\
 \hline
 \phi \vdash \psi \quad \psi \vdash \theta \\
 \hline
 \phi \vdash \theta
 \end{array}$$

$$\begin{array}{c}
 \phi \vdash \top \\
 \hline
 \phi \vdash \psi \quad \phi \vdash \theta \\
 \hline
 \phi \vdash \psi \wedge \theta
 \end{array}$$

$$\begin{array}{c}
 \perp \vdash \phi \\
 \hline
 \psi \vdash \phi \quad \theta \vdash \phi \\
 \hline
 \psi \vee \theta \vdash \phi
 \end{array}$$

$$\frac{\phi \wedge \psi \vdash \theta}{\phi \vdash \psi \rightarrow \theta}$$

$$\frac{\phi \vdash \psi(x)}{\phi \vdash \psi(t)} \quad x \text{ not free in } \phi, t \text{ contains no free variables bound by } \psi.$$

$$\frac{\phi \vdash \exists x \psi(x)}{\phi \vdash \forall x \psi(x)} \quad x \text{ not free in } \phi \qquad \frac{\exists x \psi(x) \vdash \phi}{\exists x \psi(x) \vdash \phi} \quad x \text{ not free in } \phi$$

$$\top \vdash x \equiv x$$

$$x \equiv y \vdash \phi(x) \rightarrow \phi(y)$$

The axiom system of 1.1.1 is motivated by the interpretation of Lawvere of the logical connectives as adjunctions. Observe that in 1.1.1 we use the equivalence  $\equiv$  instead of the strict equality  $=$ . We define  $x = y$  as  $\exists x \wedge \exists y \wedge x \equiv y$ . We also use partial functions. In the higher order case we prefer the equivalence  $\equiv$  in the presence of partial elements. There is an axiom system equivalent to that of [Fo 1] and [Sc 2] but which uses total and strict functions and relations (see definition 1.1.2 and [Bo 1]). Other sources for intuitionistic logic are [Du 1] and [Tr 1].

Instead of  $\top \vdash \phi$  we also write  $\vdash \phi$ . Let  $\Gamma$  be a set of sentences (i.e. formulas without free variables) and let  $\phi$  be a sentence. Then  $\phi$  follows from  $\Gamma$  if and only if there is a finite set  $\{\phi_1, \dots, \phi_n\} \subset \Gamma$  so that  $\phi_1 \wedge \dots \wedge \phi_n \vdash \phi$  is a derivable sequent. Thus for first-order statements we may use 1.1.1 to check provability.

The presence of a natural number object makes it possible to introduce the following kind of abbreviations, which have a straightforward interpretation. The definitions will not be made formal, because they do not play an essential role, but will merely be illustrated in examples. The description operator makes it possible to define new terms by "finitely iterated"



composition using  $\mathbb{N}$ -variables.

Let  $G$  be a group object with multiplication operator  $\cdot$ , then we may define for  $x$  of type  $G^{\mathbb{N}}$ :

$$x_1 \cdot \dots \cdot x_n \equiv \prod_{i=1}^n x_i \equiv \text{I}g \in G (\exists f \in G^{\mathbb{N}} (f(0) \equiv 1 \wedge f(n) \equiv g \wedge \wedge \forall m \in \mathbb{N} (m < n \rightarrow f(s(m)) \equiv x(s(m)) \cdot f(m))))).$$

Similarly we may do such things for "finite" quantification, e.g.

$\forall x_1 \dots x_n \in A \bigwedge_{1 \leq i < n} (\varphi(x_i) \rightarrow \psi(x_{i+1}))$  may be seen as abbreviation for

$$\forall x \in A^{\mathbb{N}} \exists i \in \mathbb{N} (1 \leq i \wedge i < n \wedge (\varphi(x(i)) \rightarrow \psi(x(s(i))))).$$

Or  $\exists x_1 \dots x_n \in A \bigwedge_{1 \leq i \leq n} \varphi(x_i)$  as abbreviation for

$$\exists x \in A^{\mathbb{N}} \forall i \in \mathbb{N} (1 \leq i \wedge i \leq n \rightarrow \varphi(x(i))).$$

When we substitute for  $n$  a standard natural number we get, up to provable equivalence, the common finitely iterated quantifications. The following definitions present examples of such abbreviations.

1.1.2. Definition. Let  $\varphi$  be an  $n$ -ary formula and  $\tau$  an  $n$ -ary term.

(1)  $\varphi$  is strict if we have

$$\varphi(x_1, \dots, x_n) \rightarrow Ex_1 \wedge \dots \wedge Ex_n.$$

(2)  $\tau$  is strict if we have

$$E\tau(x_1, \dots, x_n) \rightarrow Ex_1 \wedge \dots \wedge Ex_n.$$

(3)  $\tau$  is total if we have

$$Ex_1 \wedge \dots \wedge Ex_n \rightarrow E\tau(x_1, \dots, x_n).$$

It is an easy task to show the following preservations.

Strictness is preserved under substitution of strict terms.

Moreover, strictness of formulas is preserved under conjunction and - in the case the components have the same free variables - under disjunction of strict formulas. Finally, totality is preserved under composition.

## 1.2 Apartness

The structures that will be treated in more detail, are provided with an apartness relation.

1.2.1. Definition. An apartness relation on an object  $A$  is a binary relation  $\#$  satisfying

- (1)  $x\#y \rightarrow Ex \wedge Ey$ ,
- (2)  $\neg x\#x$ ,
- (3)  $x\#y \rightarrow y\#x$ ,
- (4)  $x\#z \wedge Ey \rightarrow x\#y \vee y\#z$ .

The apartness is tight if we have

- (5)  $\forall x, y (\neg x\#y \rightarrow x \equiv y)$ .

Originally an apartness relation was tight by definition ([He 1], [He 3]). In the definition above we follow [Sc 2]. We prefer the notation  $x\#y$  since notations like  $x \neq y$  and  $x \neq y$  are often used as abbreviations for  $\neg x = y$  and  $\neg x \equiv y$ .

An apartness relation gives rise to a strict equivalence relation  $\approx$  (do not confuse this with the relation  $\equiv$ ) defined by  $x \approx y \leftrightarrow \leftrightarrow Ex \wedge Ey \wedge \neg x\#y$ . The apartness  $\#$  is tight, just when  $\approx$  and  $=$  are the same.  $\approx$  satisfies the axioms, introduced in [Da 1]. That implies that  $\approx$  now is stable, i.e.  $\approx$  satisfies  $\forall x, y (\neg \neg x \approx y \rightarrow x \approx y)$ . The existence of an apartness on a structure often gives rise to a canonical apartness relation on another structure. Let  $A$  have a (tight) apartness relation and let  $X$  be an arbitrary object, then the following relation on  $A^X$  is a (tight) apartness:

$$f\#g \leftrightarrow Ef \wedge Eg \wedge \exists x \in X (f(x)\#g(x)).$$

Similarly, we can extend (tight) apartness of structures  $A$  and  $B$  to (tight) apartness on  $A \times B$ :

$$(a,b)\#(a',b') \leftrightarrow Ea \wedge Eb \wedge Ea' \wedge Eb' \wedge (a\#a' \vee b\#b').$$

There is an equivalence relation  $\approx$  so that we have

$$\forall x,y (\neg x\#y \leftrightarrow x \approx y).$$

In mathematics we are used to consider terms  $\tau$  and formulas  $\varphi$  preserving equivalence:  $x \approx y \rightarrow \tau(x) \approx \tau(y)$  and  $x \approx y \wedge \varphi(x) \rightarrow \varphi(y)$ .

So in the presence of apartness it is natural to look for complementary axiom schemas like  $\tau(x)\#\tau(y) \rightarrow x\#y$  and  $\varphi(y) \wedge Ex \rightarrow x\#y \vee \varphi(x)$ . Therefore we introduce the notion "strongly extensional".

1.2.2. Definition. A subobject  $X$  of an object  $A$  with apartness is said to be strongly extensional if we have

$$a \in X \wedge Eb \rightarrow a\#b \vee b \in X.$$

Let  $\varphi$  be a formula and let  $\tau$  be a term. Let  $\varphi$  and  $\tau$  be strict. Then  $\{x|\varphi(x)\}$  is a strongly extensional subobject of  $\{x|T\}$  if and only if the following formula holds:  $\varphi(y) \wedge Ex \rightarrow x\#y \vee \varphi(x)$ . And  $\{(x,z)|\tau(x)\#z\}$  is a strongly extensional subobject of  $\{(x,z)|T\}$  if and only if we have  $\tau(y)\#\tau(x) \rightarrow y\#x$ . This connects the definitions 1.2.2 and 1.2.3.

1.2.3. Definition. Let  $\varphi$  be an  $n$ -ary formula and  $\tau$  an  $n$ -ary term.

(1)  $\varphi$  is strongly extensional if we have

$$\varphi(y_1, \dots, y_n) \wedge Ex_1 \wedge \dots \wedge Ex_n \rightarrow y_1\#x_1 \vee \dots \vee y_n\#x_n \vee \varphi(x_1, \dots, x_n).$$

(2)  $\tau$  is strongly extensional if we have

$$\tau(y_1, \dots, y_n)\#\tau(x_1, \dots, x_n) \rightarrow y_1\#x_1 \vee \dots \vee y_n\#x_n.$$

Observe that the subcategory  $E^\#$  of a topos  $E$ , with as objects structures with (tight) apartness and with morphisms the strongly extensional ones, is a cartesian closed category which is more-

over separated: i.e., the composition on hom-sets is strongly extensional (due to Scott. See [Gr 1], p.15).

If we want to prove that a formula  $\varphi$  is strongly extensional, it is enough to show this coordinatewise. That means: change each variable separately and verify the statement.

1.2.4. Proposition. Let  $\varphi$  be an n-ary formula satisfying

$$\bigwedge_{1 \leq i \leq n} (\varphi(y_1, \dots, y_i, \dots, y_n) \wedge \text{Ex}_i \rightarrow y_i \# x_i \vee \varphi(y_1, \dots, x_i, \dots, y_n)).$$

Then  $\varphi$  is strongly extensional. If  $\varphi$  is strict, then the converse is also true.

For terms  $\tau$  the reduction to one variable cases does not work in full generality as it does for formulas. We have to add some assumptions.

1.2.5. Proposition. Let  $\tau$  be a total strict n-ary term, satisfying

$$\bigwedge_{1 \leq i \leq n} (\tau(y_1, \dots, y_i, \dots, y_n) \# \tau(y_1, \dots, x_i, \dots, y_n) \rightarrow y_i \# x_i).$$

Then  $\tau$  is strongly extensional.

Proof: by induction on  $m \equiv n-s$  we shall prove: if there is a subsequence  $y_{i_1}, \dots, y_{i_s}$  such that  $y_{i_j} \equiv x_{i_j}$  for all  $j \leq s$ , then from  $\tau(y_1, \dots, y_n) \# \tau(x_1, \dots, x_n)$  it follows that  $y_1 \# x_1 \vee \dots \vee y_n \# x_n$  holds. The case  $m \equiv 1$  has been given. Induction: without loss of generality we may assume that the property holds for the case  $m \equiv n-1$ . Now let  $\tau(y_1, \dots, y_n) \# \tau(x_1, \dots, x_n)$ . To prove:  $y_1 \# x_1 \vee \dots \vee y_n \# x_n$ .  $\tau$  and  $\#$  are strict, thus we have

$$\bigwedge_{1 \leq i \leq n} \text{Ey}_i \wedge \bigwedge_{1 \leq i \leq n} \text{Ex}_i.$$

$\tau$  is total, so  $\text{Et}(x_1, y_2, \dots, y_n)$ . Then we may apply (4) of the definition of  $\#$ : we get

$$\tau(y_1, \dots, y_n) \# \tau(x_1, y_2, \dots, y_n) \vee \tau(x_1, y_2, \dots, y_n) \# \tau(x_1, \dots, x_n).$$

$$y_1 \# x_1 \vee \tau(x_1, y_2, \dots, y_n) \# \tau(x_1, \dots, x_n).$$

Induction:  $y_1 \# x_1 \vee \dots \vee y_n \# x_n$ .

Using the above propositions it is simple to prove that  $\#$  and  $E$  are strongly extensional. Strong extensionality of a formula is preserved under conjunction, disjunction and existential quantification. Strong extensionality of a formula is also preserved under substitution of a total, strongly extensional term. Strong extensionality of terms is preserved under composition.

### 1.3 Sheaf models

We want to interpret our formal language in sheaves over a topological space, cf. [Go 1], p.359-p.374. We restrict ourselves to the interpretation of the first-order fragment of our language. There are two reasons for this restriction. The first reason is: the insiders in intuitionistic logic and model theory only need to know some conventions on notation and for that purpose the first-order part suffices. The second reason is: if one is not used to working with intuitionistic logic and model theory or if one is only interested in intuitionistic algebra, then the first-order fragment is adequate for understanding almost all aspects of the models that we shall give. For the remaining details we can refer to [Go 1] and [Fo 2]. For a more detailed account of sheaves, see [Te 1]. Some models we shall construct are in fact Kripke models ([Kr 1],[Sm 1]). Kripke models may be considered as special (pre)sheaves over a topological space ([Go 1],[Fo 2],p.310, p.345).

Let  $X$  be a topological space. Convention: we use  $U, V$  as symbols for open subsets of  $X$  and  $\alpha, \beta$  as symbols for elements of  $X$ . Let

$\text{Sh}(X)$  be the topos of sheaves over  $X$  and let  $\underline{S} \in \text{Sh}(X)$ . Following the notation of [Te 1] we write  $S(U)$  for the set of sections  $a \in \underline{S}$  with  $Ea = U$  and we write  $S_\alpha$  for the stalk in  $\alpha$ .

Let  $L$  be a first-order language. Without loss of generality we may assume that the atomic relations and functions are strict and total. Interpretations: as domain we take a sheaf  $\underline{S}$ . To an  $n$ -ary relation symbol  $r$  we assign a subsheaf  $\underline{R} \subseteq \underline{S}^n$  and to an  $n$ -ary function symbol  $f$  we assign a sheaf morphism  $F: \underline{S}^n \rightarrow \underline{S}$ . The equality symbol  $=$  will be assigned to the diagonal  $\Delta \subseteq \underline{S}^2$ , i.e. to the real equality on  $\underline{S}$  in the topos  $\text{Sh}(X)$ . The symbol  $E$  will be assigned to  $\underline{S}$  itself.

We extend our language to a new language  $L(\underline{S})$  by introducing constant symbols  $\dot{a}$  for all  $a \in \underline{S}$ . Then the interpretation of our terms is as follows: we define  $\llbracket \dot{a} \rrbracket = a$  for new constant symbols and  $\llbracket f \rrbracket = F: \underline{1} \rightarrow \underline{S}$  for 0-ary function symbols, i.e. constant symbols of  $L$ . Composed terms will be interpreted by  $\llbracket f(t_1, \dots, t_n) \rrbracket = F(\llbracket t_1 \rrbracket, \dots, \llbracket t_n \rrbracket)$ .

Let  $a \in \underline{S}$  be a section with  $Ea = U$ , i.e.  $a \in S(U)$  (observe that we use  $E$  for two different purposes. But see below). Let  $\alpha \in U$ . Then we write  $a_\alpha$  for the germ of  $a$  in  $S_\alpha$ . Now sentences of  $L(\underline{S})$  will be interpreted as follows. We interpret  $\llbracket T \rrbracket = X$  and  $\llbracket \perp \rrbracket = \emptyset$ . Let  $r$  be an  $n$ -ary relation symbol and let  $t_1, \dots, t_n$  be terms. Then

$$\llbracket r(t_1, \dots, t_n) \rrbracket = \{\alpha \in X \mid (\llbracket t_1 \rrbracket)_\alpha, \dots, \llbracket t_n \rrbracket_\alpha \in R_\alpha\}.$$

For the symbols  $=$  and  $E$  of  $L$  this implies

$$\llbracket \dot{a} = \dot{b} \rrbracket = \{\alpha \in X \mid \alpha \in Ea \cap Eb \text{ and } a_\alpha = b_\alpha\}$$

and  $\llbracket E\dot{a} \rrbracket = Ea$ .

These special cases relate the symbols  $=$  and  $E$  of the language  $L$  with the relations  $=$  and  $E$  of the sheaves. The interpretation

of connectives and quantifiers is given by

$$\llbracket \varphi \wedge \psi \rrbracket = \llbracket \varphi \rrbracket \cap \llbracket \psi \rrbracket,$$

$$\llbracket \varphi \vee \psi \rrbracket = \llbracket \varphi \rrbracket \cup \llbracket \psi \rrbracket,$$

$$\llbracket \varphi \rightarrow \psi \rrbracket = \text{Int}(\llbracket \varphi \rrbracket^c \cup \llbracket \psi \rrbracket), \text{ where } ^c \text{ and Int mean complement and interior,}$$

$$\llbracket \neg \varphi \rrbracket = \text{Int}(\llbracket \varphi \rrbracket^c) = (\text{Cl}\llbracket \varphi \rrbracket)^c \text{ where Cl means closure,}$$

$$\llbracket \exists x \varphi(x) \rrbracket = \bigcup_{a \in S} \llbracket E\dot{a} \wedge \varphi(\dot{a}) \rrbracket,$$

$$\llbracket \forall x \varphi(x) \rrbracket = \text{Int}(\bigcap_{a \in S} \llbracket E\dot{a} \rightarrow \varphi(\dot{a}) \rrbracket).$$

In the following chapters we shall work with the equivalence  $\equiv$  instead of with the equality  $=$ . The equivalence  $\equiv$  can be defined in terms of  $E$  and  $=$  as follows (see [Sc 2]):

$$x \equiv y \leftrightarrow (E x \vee E y \rightarrow x = y).$$

With the rules above this gives as interpretation for  $\equiv$ :

$$\llbracket \dot{a} \equiv \dot{b} \rrbracket = \text{Int}\{\alpha \in X \mid \text{if } \alpha \in E a \text{ or if } \alpha \in E b \text{ then } \alpha \in E a \cap E b \text{ and } a_\alpha = b_\alpha\}.$$

A sheaf  $\underline{S}$  together with morphisms  $F$  and relations  $R$  for all function symbols  $f$  and all relation symbols  $r$  is called a structure.

We usually write  $\underline{S}$  for the whole structure. We define  $\Gamma \vDash \varphi$  ( $\Gamma$  satisfies  $\varphi$ ) for sets of sentences  $\Gamma \cup \{\varphi\}$  as:

for all topological spaces  $X$  and for all structures  $\underline{S}$  we

$$\text{have } \bigcap_{\gamma \in \Gamma} \llbracket \gamma \rrbracket \subseteq \llbracket \varphi \rrbracket.$$

$\varphi$  is true in a structure  $\underline{S}$  if  $\llbracket \varphi \rrbracket = X$ , denoted by  $\underline{S} \vDash \varphi$ .

$\varphi$  is true if  $\varphi$  is true in all structures  $\underline{S}$ , i.e.  $\phi \vDash \varphi$ .

The completeness theorem for first-order intuitionistic logic states that

$$\Gamma \vdash \varphi \leftrightarrow \Gamma \vDash \varphi.$$

Remark: it is easy to generalize the first-order theory above to a many-sorted first-order version. Then we write  $(\underline{S}, \underline{S}', \dots)$  for structures over that language.

The interpretation  $\llbracket \varphi \rrbracket$  of a formula  $\varphi$  may become a complicated statement for the structure. But some formulas give easy interpretations. Example: let  $f, g, h, k$  be function symbols with interpretations  $F: \underline{S} \rightarrow \underline{S}$  and  $G, H, K: \underline{S}^2 \rightarrow \underline{S}$ . Let  $\varphi$  be the formula  $\forall x, y (g(f(x), f(y)) \equiv k(h(x, y), k(x, y)))$ . Then  $\underline{S} \models \varphi$  is equivalent to the commutativity of the following diagram.

$$\begin{array}{ccc}
 \underline{S} \times \underline{S} & \xrightarrow{F \times F} & \underline{S} \times \underline{S} \\
 \downarrow (H, K) & & \downarrow G \\
 \underline{S} \times \underline{S} & \xrightarrow{K} & \underline{S}
 \end{array}$$

Similar equivalences hold for other formulas  $\forall x. \varphi$  where  $\varphi$  is an equation.

Let  $\underline{S}$  be a structure with relations  $R \subseteq \underline{S}^n$  and morphisms  $F: \underline{S}^n \rightarrow \underline{S}$ . For each open  $U \subseteq X$  this gives us a set  $S(U)$  and relations  $R(U) \subseteq S(U)^n$  and functions  $F(U): S(U)^n \rightarrow S(U)$ . This is a structure with classical logic. We usually write  $S(U)$  for the whole structure. In the same way we get for each  $\alpha \in X$  a structure  $S_\alpha$  with relations  $R_\alpha \subseteq S_\alpha^n$  and functions  $F_\alpha: S_\alpha^n \rightarrow S_\alpha$ . Observe that  $\underline{S}$ ,  $S(U)$  and  $S_\alpha$  have the same similarity type, i.e. the language  $L$  has an interpretation in  $\underline{S}$ ,  $S(U)$  and  $S_\alpha$  simultaneously.  $\underline{S}$ ,  $S(U)$  and  $S_\alpha$  need not satisfy the same properties  $\varphi$  of the language  $L$ , e.g.  $S(U)$  and  $S_\alpha$  satisfy the excluded middle  $\varphi \vee \neg \varphi$  while for  $\underline{S}$  this need not be true. Therefore we search for formulas  $\varphi$  whose validity can be transported from the  $S_\alpha$  and the  $S(U)$  to  $\underline{S}$  and vice versa.

Let  $S(U) \models_c \varphi$  and  $S_\alpha \models_c \varphi$  mean  $S(U)$  satisfies  $\varphi$  under classical interpretation and  $S_\alpha$  satisfies  $\varphi$  under classical interpretation.

1.3.1. Definition. Let  $\varphi$  be a sentence. We define:



- $\varphi$  is pos if  $(S(U) \models_c \varphi \Rightarrow U \subseteq \llbracket \varphi \rrbracket)$ ,  
 $\varphi$  is neg if  $(U \subseteq \llbracket \varphi \rrbracket \Rightarrow S(U) \models_c \varphi)$ ,  
 $\varphi$  is p if  $(S_\alpha \models_c \varphi \Rightarrow \alpha \in \llbracket \varphi \rrbracket)$ ,  
 $\varphi$  is n if  $(\alpha \in \llbracket \varphi \rrbracket \Rightarrow S_\alpha \models_c \varphi)$ ,  
 $\varphi$  is P if  $(\text{for all } \alpha \ S_\alpha \models_c \varphi \Rightarrow X = \llbracket \varphi \rrbracket)$ ,  
 $\varphi$  is N if  $(X = \llbracket \varphi \rrbracket \Rightarrow \text{for all } \alpha \ S_\alpha \models_c \varphi)$ .

These definitions can be extended to formulas  $\varphi$  in a canonical way, although they become more lengthy. For instance,  $\varphi(x)$  is P means: [for all  $a \in \underline{S}$  and for all  $\alpha \in E a \ S_\alpha \models_c \varphi(\dot{a}) \Rightarrow \Rightarrow$  [for all  $a \in \underline{S} \ E a \subseteq \llbracket \varphi(\dot{a}) \rrbracket$ ]].

It is easy to check that (in abbreviated form):

$\text{pos} \wedge \text{pos} \subseteq \text{pos}$	$p \wedge p \subseteq p$
$\text{pos} \vee \text{pos} \subseteq \text{pos}$	$p \vee p \subseteq p$
$\exists x. \text{pos} \subseteq \text{pos}$	$\exists x. p \subseteq p$
$\text{neg} \wedge \text{neg} \subseteq \text{neg}$	$n \wedge n \subseteq n$
	$n \vee n \subseteq n$
$\neg \text{pos} \subseteq \text{neg}$	$\neg p \subseteq n$
$\text{pos} \rightarrow \text{neg} \subseteq \text{neg}$	$p \rightarrow n \subseteq n$
$\forall x. \text{neg} \subseteq \text{neg}$	$\forall x. n \subseteq n$
	$\exists x. n \subseteq n$
$n \rightarrow p \subseteq P$	$n \subseteq N$
$P \wedge P \subseteq P$	
$\forall x. P \subseteq P$	

Strict atomic sentences satisfy all conditions pos, neg, p, n, P and N. Thus T, 1, E and = satisfy these conditions.

Remark: formulas of both type N and type P are up to logical equivalence the well-known geometric formulas (cf. [Jo 2], [Ma 2]). We will return to that notion below. We use the name

"of type N and of type P" for our present purposes.

1.3.2. Example. We give the interpretation of the axioms of an apartness relation (see 1.2.1). By axiom (1)  $\#$  is strict and so it is assigned to a subsheaf  $\# \subseteq \underline{S}^2$ . Axiom (2) is of both type N and type P. Thus it is equivalent to the same condition in the stalk structures  $S_\alpha$ : for all  $x_\alpha \in S_\alpha$  we have that not  $x_\alpha \#_\alpha x_\alpha$  holds. Axioms (3) and (4) are also of form N as well as of form P. They are equivalent to the following conditions for the stalk structures  $S_\alpha$ .

(3)  $\#_\alpha$  is symmetric,

(4) for all  $x_\alpha, y_\alpha, z_\alpha$  if  $x_\alpha \#_\alpha z_\alpha$  then  $x_\alpha \#_\alpha y_\alpha$  or  $y_\alpha \#_\alpha z_\alpha$ .

The complement of the relation  $\#_\alpha$  in  $S_\alpha^2$  is called  $\approx_\alpha$ . Thus  $x_\alpha \approx_\alpha y_\alpha$  if and only if not  $x_\alpha \#_\alpha y_\alpha$ . Note that  $\approx_\alpha$  need not correspond to a subsheaf of  $\underline{S}^2$ . The axioms (2), (3) and (4) just tell us that  $\approx_\alpha$  is an equivalence relation on  $S_\alpha$ . Axiom (5) for a tight apartness is of type P and not of type N. Thus we do not get an equivalence as above. A direct interpretation gives:

for all  $a_\alpha, b_\alpha \in S_\alpha$  (with  $a, b \in S(U)$  for some  $U$ ) we have

$$(a_\alpha \approx_\alpha b_\alpha \text{ and } a_\alpha \#_\alpha b_\alpha) \Rightarrow \alpha \in \text{Cl}\{\beta \in U \mid a_\beta \#_\beta b_\beta\}.$$

Let  $f$  be a function symbol with interpretation  $F$ :  $f$  is total and strict. The axiom for strong extensionality is of type N and of type P. That implies that strong extensionality for  $f$  is equivalent to saying that  $F_\alpha$  preserves equivalence  $\approx_\alpha$  for all  $\alpha$ . In the same way one shows that strong extensionality of a strict relation  $\underline{R}$  is equivalent to saying that the  $R_\alpha$  are closed with respect to  $\approx_\alpha$ .

Let  $\vdash_c$  mean classical derivability. From definition 1.3.1 it

follows that

1.3.3. Proposition. Let  $\Gamma \cup \{\varphi\}$  be a set of first-order sentences. Let the sentences of  $\Gamma$  be of type N and let  $\varphi$  be of type P. Then we have  $\Gamma \vdash_{\mathcal{C}} \varphi \Rightarrow \Gamma \vdash \varphi$ .

Proof: straightforward.

This proposition often presents us with a convenient test for intuitionistic derivability. Nevertheless we prefer to give intuitionistic proofs for the sake of a uniform treatment of the theory.

We do not want to underestimate the value of geometric logic. Therefore we shall say a few things about it. Let  $E, F$  be topoi (see [Jo]). It may help to think of topoi as categories like  $\text{Sh}(X)$ ). A geometric morphism  $f: E \rightarrow F$  consists of an adjunction of functors  $f_*: E \rightarrow F$  and  $f^*: F \rightarrow E$  such that  $f^* \dashv f_*$  and  $f^*$  is left exact. The advantage of geometric formulas  $\varphi$  is that they are preserved by the functor  $f^*$ , the "inverse image functor" of the geometric morphism  $f$ : if a structure  $\underline{S}$  in  $F$  satisfies  $\varphi$  then so does  $f^*\underline{S}$ .

Example of a geometric morphism: let  $\text{Sh}(X)$  and  $\text{Sh}(Y)$  be sheaf categories,  $f: X \rightarrow Y$  a continuous function. Then we construct a geometric morphism, also denoted by  $f$ ,  $f: \text{Sh}(X) \rightarrow \text{Sh}(Y)$  such that for  $\underline{S} \in \text{Sh}(X)$  and open  $V \subseteq Y$   $(f_*(\underline{S}))(V) = \mathcal{S}(f^{-1}(V))$ . Let  $\underline{S} \in \text{Sh}(Y)$  correspond to the local homeomorphism  $s: G \rightarrow Y$ . Form the pullback

$$\begin{array}{ccc} H & \longrightarrow & G \\ \downarrow t & & \downarrow s \\ X & \xrightarrow{f} & Y \end{array}$$

Then  $f^*(\underline{S})$  is the sheaf corresponding to the local homeomorphism

$t: H \rightarrow X$ . Literature: [Jo 2], [Ma 2]. For an example of a study of a geometric theory, see [Wr 1].

#### 1.4 Kripke-models

The natural way, at least for us, to show that a formula  $\varphi$  is not derivable from some set of axioms is by constructing a countermodel: if  $\Gamma \not\vdash \varphi$  then  $\Gamma \not\models \varphi$ . It turns out that Kripke-models are convenient for that purpose.

Let  $\mathbb{P} = (P, \leq)$  be a partially ordered set (poset). Then we construct a topological space  $T\mathbb{P}$  on  $P$  by taking  $U \subseteq P$  open if and only if  $U$  is upward closed. These spaces  $T\mathbb{P}$  have some extra properties. The collection of open sets is closed under arbitrary intersection. Each point  $\alpha \in P$  has a smallest open neighbourhood  $U_\alpha$ . The sets  $U_\alpha$  form a basis and we have  $\alpha \leq \beta \Leftrightarrow \beta \in U_\alpha$ . If we want to describe a sheaf  $\underline{S}$  over  $T\mathbb{P}$  we only have to give the sets  $S(U_\alpha)$  and the restriction maps  $p_\beta^\alpha: S(U_\alpha) \rightarrow S(U_\beta)$  for  $\alpha \leq \beta$  (in fact we even have that  $S(U_\alpha) = S_\alpha$ ). This makes it possible to give an easy description of sheaves over  $T\mathbb{P}$ . They are related to Kripke-models. The definition of Kripke-model below differs from [Kr 1] and [Sm 1] in that the equality is interpreted as the real equality and that the restriction maps  $p_\beta^\alpha$  need not be injective. Moreover, the  $K_\alpha$ 's may be empty.

1.4.1. Definition. A Kripke-model  $\underline{K} = (K, \mathbb{P})$  over a poset  $\mathbb{P} = (P, \leq)$  consists of:

- (1) for each  $\alpha \in P$  a set  $K_\alpha$ ,
- (2) for each pair  $\alpha \leq \beta$  a function  $p_\beta^\alpha: K_\alpha \rightarrow K_\beta$  such that  $p_\alpha^\alpha = \text{id}$  and  $p_\gamma^\beta p_\beta^\alpha = p_\gamma^\alpha$ .

Let  $\underline{K}, \underline{L}$  be Kripke-models over  $\mathbb{P}$ , then a morphism  $F: \underline{K} \rightarrow \underline{L}$  of

Kripke-models consists of: for each  $\alpha \in P$  a function  $F_\alpha : K_\alpha \rightarrow L_\alpha$  such that for each pair  $\alpha \leq \beta$  the following diagram commutes:

$$\begin{array}{ccc} K_\alpha & \xrightarrow{F_\alpha} & L_\alpha \\ \downarrow p_\beta^\alpha & & \downarrow q_\beta^\alpha \\ K_\beta & \xrightarrow{F_\beta} & L_\beta \end{array}$$

The category of Kripke-models and morphisms over a poset  $\mathbb{P}$  is the same as the functor category  $\text{Set}^{\mathbb{P}}$ . One easily verifies that the categories  $\text{Sh}(\text{TIP})$  and  $\text{Set}^{\mathbb{P}}$  are equivalent.

Let  $\underline{K}$  be a Kripke-model. Then the product  $\underline{K}^n$  is given by for each  $\alpha \in P$  the set  $(K_\alpha^n)_\alpha = (K_\alpha)^n$  and for each pair  $\alpha \leq \beta$  the function  $q_\beta^\alpha = p_\beta^\alpha \times p_\beta^\alpha \times \dots \times p_\beta^\alpha$ . A relation  $\underline{R} \subseteq \underline{K}$  satisfies: for each  $\alpha \in P$  we have a subset  $R_\alpha \subseteq K_\alpha$  and we have restriction maps  $q_\beta^\alpha$  such that for all  $\alpha \leq \beta$  the following diagram commutes.

$$\begin{array}{ccc} R_\alpha & \xrightarrow{\quad} & K_\alpha \\ \downarrow q_\beta^\alpha & & \downarrow p_\beta^\alpha \\ R_\beta & \xrightarrow{\quad} & K_\beta \end{array}$$

A Kripke-model  $\underline{K}$  with morphisms  $F$  and relations  $\underline{R}$  for all function symbols  $f$  and all relation symbols  $r$  of the language  $L$  (see 1.3) is called a structure. We usually write  $\underline{K}$  for the whole structure. For each  $\alpha \in P$  we have a structure  $K_\alpha$  with morphisms  $F_\alpha$  and relations  $R_\alpha$ . Definition 1.3.1 also applies to this situation. Thus if  $\varphi$  is a  $P$  sentence and  $K_\alpha \models_c \varphi$  then  $\alpha \in \llbracket \varphi \rrbracket$ . And in the same way if  $\varphi$  is an  $N$  sentence and  $\alpha \in \llbracket \varphi \rrbracket$  then  $K_\alpha \models_c \varphi$ . Instead of  $\alpha \in \llbracket \varphi \rrbracket$  we usually write  $\alpha \Vdash \varphi$ . From the definition of  $\llbracket . \rrbracket$  we find:

$$\alpha \Vdash \varphi \wedge \psi \quad \Leftrightarrow \quad \alpha \Vdash \varphi \text{ and } \alpha \Vdash \psi,$$

$$\alpha \Vdash \varphi \vee \psi \Leftrightarrow \alpha \Vdash \varphi \text{ or } \alpha \Vdash \psi,$$

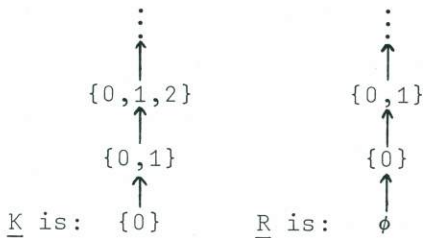
$$\alpha \Vdash \varphi \rightarrow \psi \Leftrightarrow \text{for all } \beta \geq \alpha: \beta \Vdash \varphi \Rightarrow \beta \Vdash \psi,$$

$$\alpha \Vdash \neg \varphi \Leftrightarrow \text{for all } \beta \geq \alpha: \beta \nVdash \varphi,$$

$$\alpha \Vdash \exists x \varphi(x) \Leftrightarrow \text{there is an } a \in K_\alpha \text{ such that } \alpha \Vdash \varphi(\dot{a}),$$

$$\alpha \Vdash \forall x \varphi(x) \Leftrightarrow \text{for all } \beta \geq \alpha \text{ and all } a \in K_\beta: \beta \Vdash \varphi(\dot{a}).$$

Example: let  $\mathbb{P} = (\mathbb{N}, \leq)$ , the set of natural numbers with standard ordering. Define  $\underline{K}$  by  $K_n = \{0, 1, \dots, n\}$ ,  $p_n^m$  the inclusions. As unary relation  $\underline{R}$  on  $\underline{K}$  we take  $R_n = \{0, 1, \dots, n-1\}$ .



One easily observes that the structure  $\underline{K}$  satisfies

$$\underline{K} \models \neg \forall x (r(x) \vee \neg r(x)).$$

Remark: our restriction to the class of Kripke-models for the construction of countermodels is not only motivated by their simplicity but also by the completeness theorem for Kripke-models. If there is a countermodel in the class of sheaves, then there is also a countermodel in the class of Kripke-models.

## 2. ALGEBRAIC STRUCTURES

### 2.1 Definitions

We shall straightforwardly adopt the classical notions of group, ring and module. All structures are equipped with a tight apartness relation, except if we explicitly specify otherwise. The standard operations and relations will be strongly extensional. The main sources we use are [He 2], [Ru 1] and [Sc 1]. Other definitions of algebraic structures can be found in [Ju 1],[Jo 1],[Ko 1] and [Mu 1].

2.1.1. Remark. In classical mathematics we can define monoids, groups, rings and modules by some elementary universal axioms like  $\forall x,y,z.(x+(y+z) = (x+y)+z)$ . Therefore we axiomatize them in a canonical way in intuitionistic mathematics as structures with tight apartness. The definitions can be paraphrased as:

- (1) The structure satisfies the well-known universal axioms.
- (2) The domain is provided with a tight apartness so that the standard total functions on it are strongly extensional.

We shall give two examples below. With respect to rings we shall restrict ourselves to the commutative one's with unity. The definition below can be generalized to the theory of all rings by deleting the commutativity axiom.

2.1.2. Definition. A (commutative) ring with tight apartness is a structure with  $\#, +, \cdot, -, 0, 1$  such that  $+, \cdot, -, 0$  and  $1$  are total and strict and

- (1) For  $+$ ,  $\cdot$ ,  $-$ ,  $0$  and  $1$  we have the well-known universal axioms of a commutative ring.
- (2)  $\#$  is a tight apartness relation such that  $+$ ,  $\cdot$ , and  $-$  are strongly extensional.

Let  $R$  be a ring and  $A$  an abelian group as defined above. The induced apartness relation on  $R \times A$  is (see chapter 1):

$$(r, a) \# (s, b) \leftrightarrow Er \wedge Ea \wedge Es \wedge Eb \wedge (r \# s \vee a \# b).$$

We use this tight apartness in the definition of scalar multiplication for modules.

**2.1.3. Definition.** An  $R$ -module  $A$  is a structure with a ring  $R$ , an abelian group  $A$  and a function  $\cdot : R \times A \rightarrow A$  such that  $\cdot$  is total and strict and

- (1) For  $\cdot$  we have the well-known universal axioms of a module.
- (2)  $\cdot$  is strongly extensional.

If  $R$  is a field (to be defined later) the structure is called an  $R$ -vector space  $A$ . The study of vector spaces is the main goal of the following chapter.

The definition of morphism (total and strict) for monoids, groups, rings and  $R$ -modules is straightforward. If a morphism is strongly extensional, then it will be called a strong morphism. It is not natural to restrict our attention to strong morphisms alone. It turns out that the inverse of a strong morphism, if it exists, need not be strongly extensional. The notion of surjectivity of a morphism is more or less canonical: a morphism  $\sigma : A \rightarrow B$  is surjective if it satisfies:

$$\forall b \in B \exists a \in A. \sigma(a) \equiv b.$$



The morphism is injective if

$$\forall a, a' \in A. (\sigma(a) \equiv \sigma(a') \rightarrow a \equiv a').$$

Now there is a reasonable alternative for injectivity:  $\sigma$  is an embedding if we have

$$\forall a, a' \in A. (a \neq a' \rightarrow \sigma(a) \neq \sigma(a')).$$

A morphism  $\sigma$  is bijective if it is surjective and injective.

Then the inverse morphism  $\sigma^{-1}$  exists and is also bijective. If  $\sigma$  is a strong bijection, then  $\sigma^{-1}$  is a bijective embedding. If  $\sigma$  is a bijective embedding, then  $\sigma^{-1}$  is a strong bijection.

Therefore we define:  $\sigma$  is an isomorphism if it is a strong bijective embedding. The inverse then is an isomorphism too.

A bijective morphism of a structure  $A$  to  $A$  itself is called a weak automorphism. An isomorphism of a structure  $A$  to  $A$  itself is called an automorphism.

Now we shall treat the structures in more detail.

## 2.2 Groups

We begin with some examples of groups, using the definitions above.

(1)  $\text{Aut}(A)$  is the group of weak automorphisms of a structure (monoid, group, ring, module)  $A$ . The apartness is induced by the apartness on  $A^A$ .

(2)  $\text{Aut}^{\#}(A)$  is the group of automorphisms with the apartness of  $A^A$ .  $\text{Aut}^{\#}(A)$  is a subgroup of  $\text{Aut}(A)$ .

(3) From a subobject  $X$  of a group  $G$  we can construct the subgroup  $H$  of  $G$ , generated by  $X$ , by using  $\mathbb{N}$ :

$$H = \{x \in G \mid \exists n \in \mathbb{N} \exists f \in G^{\mathbb{N}}. (x \equiv f_1 \cdot \dots \cdot f_n \wedge \forall m \leq n (f_m \in X \vee f_m^{-1} \in X))\}.$$

In classical mathematics we may construct from a group and a

normal subgroup a quotient group. Intuitionistically this may not work because we may lose apartness on the quotient object. Therefore we need a "complementary" version just as  $\#$  is in some sense "complementary" to equality.

2.2.1. Definition. A cogroup  $C$  of a group  $G$  is a subobject of  $G$  satisfying

- (1)  $\neg 1 \in C$ ,
- (2)  $xy \in C \rightarrow x \in C \vee y \in C$ ,
- (3)  $x^{-1} \in C \rightarrow x \in C$ .

$C$  is normal if it satisfies one of the following equivalent conditions:

- (4.a)  $\forall x, y (xy \in C \rightarrow yx \in C)$ ,
- (4.b)  $\forall x, y (x \in C \rightarrow yxy^{-1} \in C)$ ,
- (4.c)  $\forall x, y (yxy^{-1} \in C \rightarrow x \in C)$ .

The subobject  $(\neg C) \equiv \{x \in G \mid \neg x \in C\}$  is a subgroup. If  $C$  is normal, then  $(\neg C)$  is a normal subgroup of  $G$ , i.e. for all  $g \in G$   $g(\neg C)g^{-1} = (\neg C)$ .  $(\neg C)$  is stable: it satisfies  $\forall x \in G (\neg x \in C \rightarrow x \in C)$ . In the case  $C$  is normal, the quotient structure  $G/(\neg C)$  becomes a group with apartness (2.1.1) generated by  $x \cdot (\neg C) \# 1 \cdot (\neg C) \leftrightarrow x \in C$ . Remark: each group satisfies  $x \# y \leftrightarrow xy^{-1} \# 1$ .

2.2.2. A morphism  $\sigma : G \rightarrow H$  gives rise to a cogroup

$$C_\sigma \equiv \{x \in G \mid \sigma(x) \# 1\}.$$

$C_\sigma$  is a normal cogroup and we have a factorization diagram as in the classical case:

$$\begin{array}{ccc} G & \xrightarrow{\sigma} & H \\ & \searrow & \nearrow \sigma^* \\ & G/(\neg C_\sigma) & \end{array}$$

$\sigma^*$  is a strong embedding.

2.2.3. Remark. Names like cogroup (and coideal as we shall define later) have the advantage of being recognizably related to subgroup (and ideal). It should be natural to call  $C_\sigma$  above the "cokernel" of  $\sigma$ . Unfortunately the word "cokernel" has already a meaning in homology theory. For a name for  $C_\sigma$  we still have to look for an alternative.

### 2.3 Rings

From a ring  $R$  we can construct several group structures. Some of them play a role in the following chapters.

(1) The additive group of  $R$ . With respect to  $\#, +, -, 0$   $R$  is simply an abelian group, the additive group of  $R$ .

(2) The multiplicative group or the group of units of  $R$ . Let  $x^{-1}$  be the term  $1y$ . ( $xy = 1$ ). Then this group is

$R^* = \{x \in R \mid \exists x^{-1}\}$ , with  $\#, \cdot, ^{-1}, 1$  as for the ring  $R$ . The elements of  $R^*$  are the units.

The constructions of the power series ring  $R[[X]]$  and the polynomial ring  $R[X]$  over  $R$  play a role in studying extensions of a ring  $R$ , e.g. algebraic extensions if  $R$  is a field (cf. chapter 4).

2.3.1. Definition. The power series ring  $R[[X]]$  over  $R$  is the ring  $R[[X]] = R^{\mathbb{N}}$  with the canonical definitions of  $+, \cdot, -, 0, 1$  and with  $\#$  the canonical apartness relation of  $R^{\mathbb{N}}$ , i.e.

$$f \# g \leftrightarrow \exists f \wedge \exists g \wedge \exists n \in \mathbb{N} f(n) \# g(n).$$

2.3.2. Definition. The polynomial ring  $R[X]$  over  $R$  is the subring of  $R[[X]]$  with domain  $\{f \in R^{\mathbb{N}} \mid \exists n \in \mathbb{N} \forall m \in \mathbb{N} (m > n \rightarrow f(m) = 0)\}$ .

For convenience a term  $f \in R[[X]]$  will usually be written as

$$f \equiv f_0 + f_1 X + f_2 X^2 + \dots$$

or, if  $f$  is a polynomial, as

$$f \equiv f_0 + \dots + f_n X^n.$$

$R$  may be embedded in  $R[X]$  by the well-known strong embedding  $\sigma : R \rightarrow R[X]$  defined by

$$\sigma(a) \equiv \text{If } a \in R[X], (f(0) \equiv a \wedge \forall m \in \mathbb{N} (m > 0 \rightarrow f(m) \equiv 0)).$$

The inclusion  $R[X] \rightarrow R[[X]]$  clearly is a strong embedding.

As with cogroups (2.2.1) it is natural to define a complementary notion of ideal.

2.3.3. Definition. A coideal  $C$  of a ring  $R$  is a subobject of  $R$  satisfying

- (1)  $\neg 0 \in C$ ,
- (2)  $x+y \in C \rightarrow x \in C \vee y \in C$ ,
- (3)  $xy \in C \rightarrow x \in C \wedge y \in C$ .

$C$  is weakly non-trivial if  $\neg \neg 1 \in C$ .  $C$  is strongly non-trivial if  $1 \in C$ .

It is simple to show that  $(\neg C) \equiv \{x \in R \mid \neg x \in C\}$  is a stable ideal. The quotient object  $R/(\neg C)$  is defined straightforward.

2.3.4. A morphism  $\sigma : R \rightarrow S$  gives a coideal  $C_\sigma \equiv \{x \in R \mid \sigma(x) \neq 0\}$ .

There is a factorization as in the classical case:

$$\begin{array}{ccc} R & \xrightarrow{\sigma} & S \\ & \searrow & \nearrow \sigma^* \\ & R/(\neg C_\sigma) & \end{array}$$

$\sigma^*$  is a strong embedding.

## 2.4 Integral domains

When we want to define an intuitionistic notion of integral do-

main, there are several non-equivalent versions which generalize the classical notion. Here we choose a version, which is well-known in the literature ([He 2], [He 3]) and which has nice properties, see below. Moreover, we already had some rings in mind which we should like to be integral domains, and now they do.

An axiom like  $\forall x, y (xy \equiv 0 \rightarrow x \equiv 0 \vee y \equiv 0)$  is too restricted. The strength of it comes from the disjunction on the right hand side of the implication. An axiom like  $\neg 1 \equiv 0$  is less attractive because of its double negation nature in the presence of apartness ( $\neg 1 \equiv 0 \leftrightarrow \neg \neg 1 \neq 0$ ).

2.4.1. Definition. An integral domain is a ring satisfying

- (1)  $1 \neq 0$ ,
- (2)  $x \neq 0 \wedge y \neq 0 \rightarrow xy \neq 0$ .

Some simple properties of integral domains are:

$$xy \equiv 0 \wedge \neg x \equiv 0 \rightarrow y \equiv 0,$$

$$x \neq 0 \wedge \exists n \rightarrow x^n \neq 0, \text{ n an } \mathbb{N}\text{-variable,}$$

$$\left[ \bigwedge_{1 \leq i < j \leq n} (\neg x_i \equiv 0 \vee \neg x_j \equiv 0) \wedge x_1^{m_1} \cdot \dots \cdot x_n^{m_n} \equiv 0 \right] \rightarrow (x_1 \equiv 0 \vee \dots \vee x_n \equiv 0).$$

A property which is not derivable from the theory above is

$$xy \equiv 0 \rightarrow x \equiv 0 \vee y \equiv 0.$$

Nevertheless in some proofs of statements later on we need such splittings of products. It turns out that, with aid of the apartness relation, we sometimes can get such splittings. In the following example we illustrate how we get one.

Let  $p_1(X)$ ,  $p_2(X)$  and  $p(X, Y)$  be polynomials over an integral domain such that  $p_1(0) \equiv p_2(0) \equiv p(0, 0) \equiv 0$ . Without use of the apartness we only may expect splittings in the following way.

We have:

$$xy \equiv 0 \wedge (\neg p_1(x) \equiv 0 \vee \neg p_2(y) \equiv 0) \rightarrow x \equiv 0 \vee y \equiv 0.$$

On the left hand side as well as on the right hand side of the implication we have a disjunction. But with use of the apartness we can derive:

$$xy \equiv 0 \wedge p(x,y) \neq 0 \rightarrow x \equiv 0 \vee y \equiv 0.$$

Here we only have a disjunction on the right hand side of the implication. That makes the result more valuable.

Another application of apartness is: let  $p, q$  be distinct prime numbers. Then we have  $p \neq 0 \vee q \neq 0$ .

Proof: there are  $s, t \in \mathbb{R}$  such that  $sp + tq \equiv 1 \neq 0$ . Then  $sp \neq 0 \vee tq \neq 0$  and  $p \neq 0 \vee q \neq 0$ .

The result holds in each ring with  $1 \neq 0$ .

2.4.2. Definition. A coideal  $C$  is called prime if it satisfies the conditions

- (1)  $1 \in C$ ,
- (2)  $x \in C \wedge y \in C \rightarrow xy \in C$ .

We can use prime coideals to construct integral domains. From the definitions it easily follows that for all coideals  $C$  we have (" $C$  is prime")  $\leftrightarrow$  (" $R/(\neg C)$  is an integral domain").

The following theorem is due to Heyting, see [He 2].

2.4.3. Theorem. Let  $R$  be an integral domain. Then  $R[X]$  is an integral domain too.

Proof: easy. The essential step in the proof is based on the following lemma.

2.4.4. Lemma.  $R$  is an integral domain. Let  $b \equiv b_0 + \dots + b_p X^p$ ,  $c \equiv c_0 + \dots + c_q X^q$  and  $a \equiv bc \equiv a_0 + \dots + a_{p+q} X^{p+q}$ . Then for each pair

$i, j$  we have  $b_i c_j \neq 0 \rightarrow \exists k \in \mathbb{N} (i+j \leq k \leq p+q \wedge a_k \neq 0)$ .

Proof: induction on  $(p+q-i-j)$ . Step 0: trivial. Induction step:

assume  $b_i c_j \neq 0$ . Thus  $b_i c_j = a_{i+j} - \sum_{\substack{k+l=i+j \\ k \neq i}} b_k c_l \neq 0$ .

$$a_{i+j} \neq 0 \vee \bigvee_{\substack{k+l=i+j \\ k > i}} (b_k \neq 0) \vee \bigvee_{\substack{k+l=i+j \\ l > j}} (c_l \neq 0).$$

Now use the induction hypothesis ( $k+j > i+j$  or  $i+l > i+j$ ):

$$a_{i+j} \neq 0 \vee \bigvee_{i+j+1 \leq k \leq p+q} a_k \neq 0.$$

This lemma has more applications, for instance in the following theorem as Heyting observed [He 2].

2.4.5. Theorem.  $R$  is an integral domain. Let  $b = b_0 + \dots + b_p X^p$ ,  $c = c_0 + \dots + c_q X^q$  and  $a = bc = a_0 + \dots + a_n X^n$ . Let  $t \in \mathbb{N}$  such that  $p+q > n+t$  and  $a_{n-t} \neq 0$ . Then  $b_p = 0 \vee c_q = 0$ .

Proof:  $p+q > n+t$ , thus  $n-t > n+(n-p-q) = (n-p)+(n-q)$ . And  $a_{n-t} \neq 0$ ,

thus  $\bigvee_{i+j=n-t} b_i c_j \neq 0$ .

Assume some  $b_r c_s \neq 0$  from this disjunction. Thus  $r+s = n-t$ . Then

$$r > n-q \vee s > n-p.$$

Because of the symmetry we may choose in this disjunction.

Choose  $r > n-q$ . Then  $b_r \neq 0$  and we have  $c_q \neq 0 \rightarrow \exists m > n. a_m \neq 0$  by using lemma 2.4.4. Thus  $\neg c_q \neq 0$ , i.e.  $c_q = 0$ . Symmetry:

$$b_p = 0 \vee c_q = 0.$$

In the last theorem the case  $t = 0$  is of special interest. Applying the theorem repeatedly we can find  $p$  and  $q$  so that  $p+q = n$  and  $b_p \neq 0, c_q \neq 0$ .

The following lemma is closely related to 2.4.4 and it can be used to prove that  $R[[X]]$  is an integral domain if  $R$  is so.

2.4.6. Lemma.  $R$  is an integral domain and  $a, b, c \in R[[X]]$ . Let

$b \equiv b_0 + \dots + b_p X^p + \dots$ ,  $c \equiv c_0 + \dots + c_q X^q + \dots$  and  $a \equiv bc \equiv a_0 + \dots + a_n X^n + \dots$ .  
Then for each pair  $i, j$  we have  $b_i c_j \neq 0 \rightarrow \exists k \in \mathbb{N} (0 \leq k \leq i+j \wedge a_k \neq 0)$ .

Proof: by induction on  $(i+j)$ , analogous to the proof of 2.4.4.

From lemma 2.4.6 it immediately follows that

2.4.7. Theorem. If  $R$  is an integral domain then so is  $R[[X]]$ .

Since subrings of integral domains are also integral domains, theorem 2.4.7 gives an alternative proof of the theorem that if  $R$  is an integral domain then  $R[X]$  is an integral domain (2.4.3).

## 2.5 Fields

Of main interest is now the notion of field. The apartness makes it again possible to give an axiomatization without negation.

2.5.1. Definition. A field is a ring satisfying

- (1)  $1 \neq 0$ ,
- (2)  $x \neq 0 \rightarrow \exists x^{-1}$ ,

where  $x^{-1}$  is the term  $\text{Iy}.xy \equiv 1$  (cf. 2.3).

It is simple to prove that a field is an integral domain. Examples of fields are the rationals, the Cauchy reals and the Dedekind reals and its algebraic extension, the complex numbers ([Bu 1],[Da 2],[Ro 1],[Tr 3]).

As in the classical case it is possible to construct from an integral domain the so-called quotient field. In detail:

Let  $R$  be the integral domain and  $S = \{x \in R \mid x \neq 0\}$ . Then we define on  $R \times S$  the following equivalence relation:

$$(x, y) \sim (z, t) \leftrightarrow xt \equiv yz.$$



Let

$$Q(R) \equiv \{a \in P(R \times S) \mid \exists (x, y) \in R \times S \forall (z, t) \in R \times S [(z, t) \in a \leftrightarrow (x, y) \sim (z, t)]\}.$$

As tight apartness on  $Q(R)$  we have:

$$a \# b \leftrightarrow \exists (x, y) \in a \exists (z, t) \in b. xt \# yz.$$

With the well-known definitions of  $+$ ,  $\cdot$ ,  $-$ ,  $0$  and  $1$ ,  $Q(R)$  becomes a field. The standard inclusion  $\sigma : R \rightarrow Q(R)$ , defined by  $\sigma(x) \equiv \{a \in Q(R). (x, 1) \in a\}$  is a strong embedding.

For the following theorem we need a weak version of finiteness.

2.5.2. Definition. An object  $X$  is weakly finite if it satisfies

$$\forall a \in X^{\mathbb{N}} \exists i, j \in \mathbb{N} (i < j \wedge a(i) \equiv a(j)).$$

In classical algebra finite integral domains are fields. This property can be extended to the following intuitionistic version.

2.5.3. Theorem. Let  $R$  be a weakly finite integral domain. Then  $R$  is a field satisfying  $\forall x \in R (x \# 0 \vee x \equiv 0)$ .

Proof: let  $x \in R$ . Take  $a \equiv \{f \in R^{\mathbb{N}} (f(0) \equiv 1 \wedge \forall m \in \mathbb{N} (f(s(m)) \equiv x \cdot f(m))\}$ .

Thus  $a(m) \equiv x^m$ .  $R$  is weakly finite thus there are  $i, j \in \mathbb{N}$  with  $i < j$  and  $x^i \equiv x^j$ .  $x^i(1-x^{j-i}) \equiv 0$ . From  $1 \# 0$  we get

$$1 \# x^{j-i} \vee x^{j-i} \# 0.$$

$$1 - x^{j-i} \# 0 \vee x^i \# 0$$

$$x^i \equiv 0 \vee x^{j-i} \equiv 1$$

$$x \equiv 0 \vee (x \# 0 \wedge \exists x^{-1}).$$

This theorem shows that finiteness makes the theory of integral domains and fields considerably stronger.

2.5.4. Definition. A coideal  $C \subseteq R$  is called minimal if it satisfies the conditions

$$(1) 1 \in C,$$

$$(2) x \in C \rightarrow \exists y \in R. \neg xy - 1 \in C.$$

One easily verifies that for all coideals  $C \subseteq R$  we have

$$("C \text{ is minimal}") \leftrightarrow ("R/(\neg C) \text{ is a field}).$$

This implies that a minimal coideal is prime (see 2.4.2). The name "minimal" of a minimal coideal can be justified by the property: Let  $D, C$  be coideals,  $C$  minimal, and let  $1 \in D \subseteq C$ . Then  $D = C$ .

Proof: let  $x \in C$ . We must prove that  $x \in D$ . By definition there is a  $y \in R$  such that  $\neg xy - 1 \in C$ . Thus  $\neg xy - 1 \in D$ .  $D$  is strongly non-trivial, thus  $1 - xy \in D \vee xy \in D$ . So  $xy \in D$  and  $x \in D$ .

## 2.6 Local rings

We shall study local rings in a more general context than that of rings with a tight apartness. The theory of local rings is of special interest, e.g. see [Jo 2], [Mu 1], [Sc 2] or [Wr 1]. It can be axiomatized by geometric axioms ([Jo 2], [Ma 2]). This implies that - in the terminology of chapter 1 - it has a finite set of axioms of both the forms N and P as we shall see below. We will consider local rings because many results in chapter 3 and chapter 4 for fields can easily be generalized to local rings. Then these results are also applicable to other notions of fields ([Ko 1], [Re 1]).

2.6.1. Definition. A (commutative) local ring is a structure with  $+, \cdot, -, 0, 1$  such that

$$(1) +, \cdot, -, 0, \text{ and } 1 \text{ are total and strict,}$$

$$(2) \text{ for } +, \cdot, -, 0 \text{ and } 1 \text{ we have the well-known universal axioms of a commutative ring, with } \neg 0 = 1,$$

$$(3) \forall x (\exists x^{-1} \vee \exists (1-x)^{-1}).$$

When we replace axiom (3) by the equivalent axiom

$$\forall x. (\exists y. xy \equiv 1 \vee \exists y. (1-x)y \equiv 1)$$

we see that it is of type N and of type P. The relation  $\#$  on a local ring, defined by  $x\#y \leftrightarrow E(x-y)^{-1}$  is a (not necessarily tight) apartness. Now we can formulate the relation between local rings and fields as follows.

2.6.2. Proposition. Let R be a local ring. The following properties are equivalent:

- (1) R satisfies  $\forall x(\neg Ex^{-1} \rightarrow x \equiv 0)$ ,
- (2) the apartness  $\#$  on R is tight,
- (3) R is a field (2.5.1).

Proof: straightforward.

Most results of the sections 2.3, 2.4 and 2.5 can be generalized to rings whose apartness need not be tight. Here we shall list some differences. For the construction of a quotient ring we need more than only a coideal as in 2.3.3. We need a pair C, I where C is a coideal and I is an ideal such that  $I \subseteq (\neg C)$ . Then the quotient ring  $(R/I, C)$  has the following equality:  $x \equiv y \leftrightarrow x-y \in I$  and apartness  $x\#y \leftrightarrow x-y \in C$ . The prime coideals give integral domains, but with not necessarily tight apartness and the minimal coideals give local rings if they satisfy

$$x \in C \rightarrow \exists y. xy - 1 \in I.$$

Theorem 2.4.5 does not hold in general.

The construction of the quotient local ring  $Q(R)$  from an integral domain with generalized apartness still works although we have to define the equivalence relation  $\sim$  on  $R \times S$  in another way:  $(x, y) \sim (z, t) \leftrightarrow \exists s \in S. s(xt - yz) \equiv 0$  (see [La 1] p.67).

The real drawback is that the canonical morphism  $\sigma : R \rightarrow Q(R)$  need not be injective without an extra assumption.  $R$  must be balanced, i.e.  $R$  has to satisfy  $\forall x, y (x \neq 0 \wedge xy = 0 \rightarrow y = 0)$ .

2.6.3. Proposition. Let  $R$  be a local ring. Then  $R[X]$  is balanced.

Proof: let  $f, g \in R[X]$ ,  $f = f_0 + \dots + f_m X^m \neq 0$ ,  $g = g_0 + \dots + g_n X^n$  and  $fg = 0$ . The equation  $fg = 0$  can be translated into the following linear equation for the coefficients.

$$\begin{pmatrix} 0 \\ \vdots \\ \vdots \\ \vdots \\ 0 \end{pmatrix} = \begin{pmatrix} f_0 & 0 & \dots & 0 \\ f_1 & f_0 & & \vdots \\ \vdots & \vdots & \ddots & f_0 \\ f_m & & & \vdots \\ 0 & f_m & & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ 0 & \dots & \dots & f_m \end{pmatrix} \begin{pmatrix} g_0 \\ \vdots \\ \vdots \\ \vdots \\ g_n \end{pmatrix}$$

By 4.3.2 this implies  $(g_0, \dots, g_n) = 0$ . Thus  $g = 0$ .

The generalized version of theorem 2.5.3 is also somewhat different. Let  $R$  be a weakly finite integral domain with generalized apartness. If  $R$  is balanced then it is a local ring satisfying  $\forall x (x \neq 0 \vee \neg x \neq 0)$ . Moreover, if  $R$  has no nilpotents, i.e. if  $R$  satisfies  $\forall x (x^2 = 0 \rightarrow x = 0)$ , then  $R$  is a field according to 2.5.1.

## 2.7 Modules

We return to structures with a tight apartness. Let  $A$  be an  $R$ -module. We shall use Greek characters for  $R$  elements and Latin characters for  $A$  elements. A module over a field is called a vector space. Vector spaces have some additional properties, e.g.  $\alpha x \neq 0 \leftrightarrow \alpha \neq 0 \wedge x \neq 0$ . We shall present some constructions of modules below. They will be used in chapters 3 and 4.

(1) Let  $R^n = R^X$  where  $X = \{m \in \mathbb{N} \mid 1 \leq m \leq n\}$ . As apartness on  $R^n$  we

take the apartness of the exponent. With the well-known operations of  $R^X$ , it is an  $R$ -module. Elements of  $R^n$  are usually written as  $(\alpha_1, \dots, \alpha_n)$ . The apartness relation is in this notation

$$(\alpha_1, \dots, \alpha_n) \# (\beta_1, \dots, \beta_n) \leftrightarrow \bigwedge_{1 \leq i \leq n} (E\alpha_i \wedge E\beta_i) \wedge \bigvee_{1 \leq i \leq n} \alpha_i \# \beta_i.$$

(2) Let  $A$  be an  $S$ -module,  $B \subseteq A$  a subgroup and  $R \subseteq S$  a subring, such that  $\alpha \in R \wedge x \in B \rightarrow \alpha x \in B$ . Then  $B$  is an  $R$ -module.

A case of special importance: for each subring  $R$  of  $S$  we have:  $S$  is an  $R$ -module.

(3) This is a generalization of construction (1). From an  $R$ -module  $A$  and an object  $V$  we can construct the  $R$ -module over  $A^V$ , which is the function module with pointwise operations. For a subobject  $D \subseteq A^V$  we can construct the submodule generated by  $D$ . Define

$$M(D, R) = \{x \in A^V \mid \exists n \in \mathbb{N} \exists \alpha \in R^{\mathbb{N}} \exists a \in D^{\mathbb{N}} \forall v \in V (x(v) = \sum_{i=1}^n \alpha_i a_i(v))\}.$$

$M(D, R)$  is a module with the operations and the apartness from  $A^V$ . For elements of  $M(D, R)$  we usually write

$$x = \alpha_1 a_1 + \dots + \alpha_n a_n \text{ with the } a_i \in D \subseteq A^V.$$

2.7.1. Definition. A comodule  $C$  of a module  $A$  is a subobject of  $A$  satisfying

- (1)  $\neg 0 \in C$ ,
- (2)  $x + y \in C \rightarrow x \in C \vee y \in C$ ,
- (3)  $\alpha x \in C \rightarrow x \in C$ .

Let  $C \subseteq A$  be a comodule. Then  $(\neg C)$  is a stable submodule of  $A$ . The quotient module  $A/(\neg C)$  is defined straightforwardly. A morphism  $\sigma : A \rightarrow B$  of  $R$ -modules, also called an  $R$ -linear map, gives a comodule  $C_\sigma = \{x \in A \mid \sigma(x) \# 0\}$ . For  $C_\sigma$  we can derive the well-known theorems about quotient objects and factorization as in 2.2.2 and 2.3.4.

## 2.8 Models of group theory

With help of the remarks of chapter 1 we can characterize the sheaf models of groups, rings and modules. The classes will be treated successively. We start with groups.

Let  $\underline{G}$  be a model of the theory of groups,  $\underline{G} \in \text{Sh}(X)$ , the category of sheaves over the topological space  $X$ . The group operations give rise to functions on the sets  $G(U)$  and  $G_\alpha$  ( $U \subseteq X$ ,  $\alpha \in X$ ). The group axioms yield that the  $G(U)$  and  $G_\alpha$  are (classical) groups. In chapter 1 we found that  $\#_\alpha$ , the induced apartness relation on  $G_\alpha$ , is the complement of an equivalence relation  $\approx_\alpha$ . It is simple to show that strong extensionality of  $\cdot$  and  $^{-1}$  means that the corresponding group operations on  $G_\alpha$  preserve  $\approx_\alpha$ . Therefore, to characterize this equivalence relation it is enough to determine the structure of the equivalence class of the unit element  $1_\alpha$  in each stalk  $G_\alpha$ . Let the equivalence class of the unit element in stalk  $G_\alpha$  be  $N_\alpha$ . From the strong extensionality of  $\cdot$  and  $^{-1}$  we can prove the following intuitionistic statements.

$$xy \# 1 \rightarrow x \# 1 \vee y \# 1,$$

$$x^{-1} \# 1 \rightarrow x \# 1,$$

$$yxy^{-1} \# 1 \rightarrow x \# 1.$$

These are of type N and of type P, thus for the  $N_\alpha$  in the stalks we have

$$a_\alpha \in N_\alpha \text{ and } b_\alpha \in N_\alpha \Rightarrow a_\alpha b_\alpha \in N_\alpha,$$

$$a_\alpha \in N_\alpha \Rightarrow a_\alpha^{-1} \in N_\alpha,$$

$$a_\alpha \in N_\alpha \text{ and } b_\alpha \in G_\alpha \Rightarrow b_\alpha a_\alpha b_\alpha^{-1} \in N_\alpha.$$

Thus the  $N_\alpha$  are normal subgroups of the  $G_\alpha$ .

Conversely let  $\underline{G}$  be a sheaf of groups with a tight apartness.

Assume that in each stalk  $G_\alpha$  there is a normal subgroup  $N_\alpha$  so that for all  $a_\alpha, b_\alpha \in G_\alpha$  we have  $\alpha \in [\dot{a} \# \dot{b}]$  if and only if  $a_\alpha b_\alpha^{-1} \in N_\alpha$ . Then we easily see that this model satisfies the intuitionistic statement  $\forall z (x \# y \rightarrow xz \# yz \wedge zx \# zy)$ . With this property we can show that  $\cdot$  and  $^{-1}$  are strongly extensional. Thus  $\underline{G}$  is a group model.

Examples:

(1) Let  $M$  be a  $k$ -dimensional manifold in  $\mathbb{R}^n$  with smooth group operations. Take for the group model  $\underline{G}$  as underlying topological space  $X = \mathbb{R}^k$  with standard topology. For open  $U \subseteq \mathbb{R}^k$  we take

$$G(U) = \{f \in C^\infty(U, M) \mid f \text{ is a local immersion}\}.$$

For  $f, g \in G(U)$  we take as apartness

$$[\dot{f} \# \dot{g}] = \{x \in U \mid f(x) \neq g(x)\}.$$

With the group operations of  $M$  pointwise applied to the functions we get an intuitionistic group  $\underline{G}$ .

(2) Let  $G$  be a (classical) group with normal subgroup  $N$ . Then we can form the following simple Kripke-model.

$$\begin{array}{ccc} G_\alpha = G, N_\alpha = \{1\} & & G_\gamma = G/N, N_\gamma = \{1\} \\ & \swarrow & \searrow \\ & G_\beta = G, N_\beta = N & \end{array}$$

All morphisms are canonical. As apartness we have  $\alpha \Vdash \dot{x} \# \dot{y} \Leftrightarrow xy^{-1} \in N$ ,  $\beta \Vdash \dot{x} \# \dot{y} \Leftrightarrow x \neq y$  and  $\gamma \Vdash \dot{x} \# \dot{y} \Leftrightarrow x \neq y$ . In other words, the apartness is induced by the normal subgroups in the nodes (i.e. the stalks of the corresponding sheaf, see chapter 1) as described above. Observe that if  $\alpha \Vdash \neg \dot{x} \# \dot{y}$ , then  $\beta \Vdash \neg \dot{x} \# \dot{y}$ , thus  $x = y$ . From that it follows that the apartness of  $\underline{G}$  is tight and  $\underline{G}$  is a group model. This model serves as a prototype for all sorts of Kripke-models for group theory.

## 2.9 Models of ring theory

Analogous to the characterization of models of group theory we can characterize the models of ring theory.

2.9.1. Let  $\underline{R}$  be a sheaf of (commutative) rings with a tight apartness. Assume that in each stalk  $R_\alpha$  there is an ideal  $I_\alpha$  such that for all  $a_\alpha, b_\alpha \in R_\alpha$  we have  $\alpha \in \llbracket \dot{a} \# \dot{b} \rrbracket$  if and only if  $a_\alpha - b_\alpha \in I_\alpha$ . Then  $+$ ,  $\cdot$  and  $-$  are strongly extensional and  $\underline{R}$  is a ring model.

Examples:

(1) Let  $R$  be a (classical) ring,  $1 \neq 0$ . Consider the following Kripke-model  $\underline{R}$ .

$$\begin{array}{ccc}
 R_\beta = R, I_\beta = 0 & & R_\gamma = R[X]/(X^2), I_\gamma = 0 \\
 & \swarrow & \searrow \\
 & R_\alpha = R[X]/(X^2), I_\alpha = (X) &
 \end{array}$$

All morphisms are canonical. As apartness we have  $\alpha \Vdash \dot{x} \# \dot{y} \Leftrightarrow x - y \in I_\alpha$ ,  $\beta \Vdash \dot{x} \# \dot{y} \Leftrightarrow x \neq y$  and  $\gamma \Vdash \dot{x} \# \dot{y} \Leftrightarrow x \neq y$ . Thus the apartness is induced by the ideals in the nodes as described in 2.9.1.  $\underline{R}$  is a ring model. Observe that  $\underline{R} \models \dot{X}^2 \equiv 0$ , but also

$$\underline{R} \not\models \dot{X} \equiv 0 \vee \neg \dot{X} \equiv 0.$$

(2) Let  $S = C^0([0,1], \mathbb{R})$  be the (classical) ring of continuous functions with the topology induced by the supremum norm. Let  $X$  be an arbitrary topological space. Take as model the sheaf  $\underline{S}$  over  $X$  which is defined for each open  $U \subseteq X$  as follows:

$$S(U) = \{f : U \rightarrow S \mid f \text{ is continuous}\}.$$

As apartness we take for  $f, g \in S(U)$

$$\llbracket \dot{f} \# \dot{g} \rrbracket = \{\alpha \in U \mid f(\alpha) \neq g(\alpha)\}.$$

With the canonical ring operations  $\underline{S}$  is a ring model.



If a sheaf model  $\underline{R}$  is a model for the axioms of an integral domain, then by definition  $\underline{R}$  is a ring model too. Therefore, if we want to characterize integral domain sheaves we may restrict ourselves to ring models.

2.9.2. A ring model  $\underline{R}$  is an integral domain if for the stalk structures  $(R_\alpha, I_\alpha)$  as in 2.9.1 we have  $I_\alpha \neq R_\alpha$  and  $I_\alpha$  is a prime ideal. This easily follows from the axioms of 2.4.1 which are of type N as well as of type P (see chapter 1).

For group theory it is simple to prove, that for each pair  $(N, G)$  with  $N$  a normal subgroup of a classical group  $G$  there is a group model  $\underline{G}$  in which  $(N, G)$  occurs in some stalk as  $N = N_\alpha$  and  $G = G_\alpha$ . And for ring theory we have the same for each pair  $(I, R)$  with  $I$  an ideal of a classical ring  $R$ . The question arises: which pairs  $(I, R)$  occur as stalk in integral domain sheaves?

Let  $\underline{R}$  be a ring model which is an integral domain. Let  $(I_\alpha, R_\alpha)$  be a stalk structure as described in 2.9.1 and in 2.9.2. We shall derive some necessary conditions for  $(I_\alpha, R_\alpha)$ . We already know that  $I_\alpha \neq R_\alpha$  and that  $I_\alpha$  is a prime ideal.  $\underline{R}$  is an integral domain, thus for each natural number  $n$  we have  $\underline{R} \models x^n \equiv 0 \rightarrow x \equiv 0$ . The sentence  $x^n \equiv 0 \rightarrow x \equiv 0$  is of N-form, thus  $R_\alpha$  must be nilpotentfree. An element  $c \in R_\alpha$  is called a zero divisor if there exists a  $b \in R_\alpha$  such that  $cb = 0$  and  $b \neq 0$ . We can derive that  $\underline{R} \models xy \equiv 0 \wedge x \neq 0 \rightarrow y \equiv 0$ , which is of N-form, thus  $I_\alpha$  must contain all zero divisors.

Taken together: if a pair  $(I_\alpha, R_\alpha)$  occurs in a stalk of a sheaf model of integral domain theory, then  $R_\alpha$  is a nilpotentfree ring and  $I_\alpha$  is a prime ideal,  $I_\alpha \neq R_\alpha$ , such that  $I_\alpha$  contains all zero divisors.

The converse is also true: all such pairs occur in a stalk of a

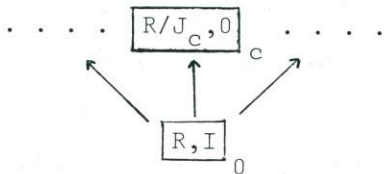
model:

Given a nilpotentfree ring  $R$  with prime ideal  $I \neq R$  containing all zero divisors, then there is a sheaf model of integral domain theory with  $(I, R)$  in a stalk in a way as described in 2.9.1. Before we construct our sheaf model we need the following lemma.

2.9.3. Lemma. Let  $R$  be a nilpotentfree ring with prime ideal  $I \neq R$  such that  $I$  contains all zero divisors. Let  $c \in R, c \neq 0$ . Then there is a prime ideal  $J_c \subseteq I$  such that  $c \notin J_c$ .

Proof: let  $S = R \setminus I$ .  $S$  is a multiplicative subset such that  $0 \notin S$ . Let  $S'$  be the least multiplicative subset containing  $S$  and  $\{c\}$ . Since  $S' = \{c^n s \mid n \geq 0 \text{ and } s \in S\}$  and  $c \neq 0$  nilpotentfree and  $s$  zero-divisorfree for each  $s \in S$ , we have  $0 \notin S'$ . Thus there is (use Zorn) a maximal multiplicative subset  $T \supseteq S'$  with  $0 \notin T$ . Let  $J_c = R \setminus T$ . Then  $J_c$  is a prime ideal with  $J_c \subseteq I$  and  $c \notin J_c$ .

Now we construct the integral domain sheaf  $\underline{R}$  in which the  $(I, R)$  as mentioned above occurs in some stalk. In fact we construct a Kripke-model such that  $\underline{R}$  is the corresponding sheaf model. As underlying partially ordered set we take as domain  $D = R$  and as ordering  $x \leq y \Leftrightarrow (x = y \text{ or } x = 0)$ . In  $x = 0$  we take as stalk structure  $I_0 = I, R_0 = R$ . For  $x \neq 0$  we take  $R_x = R/J_x$  and  $I_x = 0$  (we take the  $J_x$  from 2.9.3). In a picture



The apartness is defined as follows: let  $a, b \in R_x$ , then  $x \Vdash a \# b \Leftrightarrow a - b \notin I_x$ . We easily verify that this model is an integral domain. The only non-trivial point is the tightness of the apartness.

Assume that  $0 \Vdash \neg \dot{c} \neq 0$ . Then  $c \Vdash \neg \dot{c} \neq 0$ . If  $c \neq 0$  then  $c = 0$  in  $R/J_c$ . This contradicts 2.9.3. Thus  $c = 0$  in  $R$  and  $0 \Vdash \dot{c} \equiv 0$ . From this the tightness easily follows.

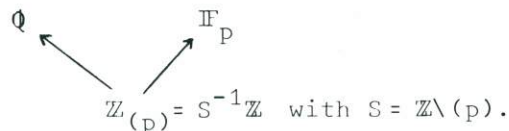
For the characterization of the sheaf models of the axioms of field theory we may restrict ourselves to ring models. From 2.9.1 and 2.5.1 we easily find the following characterization.

2.9.4. A ring model  $\underline{R}$  is a field if for the stalk structures  $(R_\alpha, I_\alpha)$  as in 2.9.1 we have  $I_\alpha \neq R_\alpha$  and  $I_\alpha$  is the unique maximal ideal of  $R_\alpha$ . The rings  $R_\alpha$  are local rings.

2.9.5. Let  $R$  be a ring,  $I \subseteq R$  an ideal. From 2.9.2 and 2.9.3 it easily follows that  $(R, I)$  occurs as stalk structure of a field model if and only if  $R$  is nilpotentfree and  $I$  is the unique maximal ideal of  $R$ . Therefore, to describe some stalk structure of a field model we only need to give a nilpotentfree local ring  $R$ .

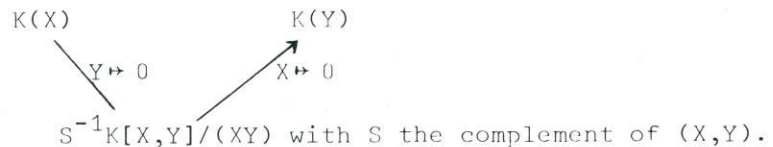
2.9.6. Examples. For the field models below, by 2.9.5, we only need a description of their ring structures.

(1) Let  $\underline{R}$  be:



Then  $\underline{R} \# \dot{p} \equiv 0 \vee \neg \dot{p} \equiv 0$ .

(2) Let  $\underline{R}$  be:



Then  $\underline{R} \# \dot{X}\dot{Y} \equiv 0 \rightarrow \dot{X} \equiv 0 \vee \dot{Y} \equiv 0$ .

(3) Let  $X$  be a topological space and  $F$  a (classical) field with

absolute value ([La 1], p.283). This absolute value induces a topology on  $F$ . Then the sheaf  $\mathcal{C}(X, F)$  of partial continuous functions with open domain and with the canonical operations from  $F$ , is a field model with apartness

$$\llbracket f \# g \rrbracket = \{\alpha \in U \mid f(\alpha) \neq g(\alpha)\} \text{ for } f, g \in \mathcal{C}(U, F).$$

(4) Let  $R$  be a nilpotentfree (classical) ring.  $\text{Spec}(R) = \{p \subseteq R \mid p \text{ is a prime ideal}\}$ . On  $\text{Spec}(R)$  we take the Zariski topology, which has as a basis the collection  $\mathcal{O}_d = \{p \in \text{Spec}(R) \mid d \notin p\}$ ,  $d \in R$ . Then we take on  $\text{Spec}(R)$  the sheaf with in each  $p \in \text{Spec}(R)$  as stalk the local ring  $R_p = S^{-1}R$ , with  $S = R \setminus p$ . As ring of sections  $R(\mathcal{O}_d)$  on the basic opens  $\mathcal{O}_d$  we get  $R(\mathcal{O}_d) = S^{-1}R$  with  $S$  the multiplicative subset, generated by  $d$ .

Finally we want to give a characterization of local ring models where local rings are defined as in 2.6.1. We cannot use the characterization of rings with apartness of 2.9.1 since the induced apartness of a local ring need not be tight. But the axioms for a local ring are of type N and of type P (see chapter 1). Hence we find the following characterization.

2.9.7. Let  $\underline{R}$  be a sheaf of rings. Then  $\underline{R}$  is a local ring model if and only if the stalks  $R_\alpha$  are local rings.

Since fields with apartness are local rings the models of 2.9.6 are examples of local ring models. However, local rings are more general. One easily verifies that for all (classical) rings  $R \neq 0$  the construction of 2.9.6(4) gives a local ring model. This implies that each non-trivial commutative ring  $R$  occurs as global sections ring of a local ring model.

## 2.10 Models of module theory

The characterization of the module models  $\underline{A}$  over a ring model  $\underline{R}$  easily follows from the characterization of the group models and of the ring models.

2.10.1. Let  $\underline{R}$  be a ring model and let  $\underline{A}$  be a group model so that  $\underline{A}$  is abelian. For all open  $U \subseteq X$  and for all  $\alpha \in X$  we have that  $A(U)$  and  $A_\alpha$  are abelian groups. We use an additive notation for the group operations on  $\underline{A}$ . By 2.8 there are subgroups  $N_\alpha \subseteq A_\alpha$  so that for all  $a_\alpha, b_\alpha \in A_\alpha$  we have  $\alpha \in [\dot{a} \neq \dot{b}] \Leftrightarrow a_\alpha - b_\alpha \notin N_\alpha$ . By 2.9.1 there are ideals  $I_\alpha \subseteq R_\alpha$  so that for all  $a_\alpha, b_\alpha \in R_\alpha$  we have  $\alpha \in [\dot{a} \neq \dot{b}] \Leftrightarrow a_\alpha - b_\alpha \notin I_\alpha$ . Let  $\underline{A}$  be an  $\underline{R}$ -module. By chapter 1 we easily find that 2.1.3(1) means that we have a morphism  $*$  :  $\underline{R} \times \underline{A} \rightarrow \underline{A}$  satisfying the well-known commutative diagrams for scalar multiplication, i.e. the equations  $\alpha(x+y) \equiv \alpha x + \alpha y$ ,  $(\alpha+\beta)x \equiv \alpha x + \beta x$ ,  $(\alpha\beta)x \equiv \alpha(\beta x)$  and  $1x \equiv x$  correspond with the following diagrams.

$$\begin{array}{ccccc}
 \underline{R} \times \underline{A} \times \underline{A} & \xrightarrow{\cong} & \underline{R} \times (\underline{A} \times \underline{A}) & \xrightarrow{\text{id} \times *} & \underline{R} \times \underline{A} \\
 \downarrow (\pi_1 \times \pi_2) \times (\pi_1 \times \pi_3) & & & & \downarrow * \\
 (\underline{R} \times \underline{A}) \times (\underline{R} \times \underline{A}) & & & & \\
 \downarrow * \times * & & & & \downarrow * \\
 \underline{A} \times \underline{A} & \xrightarrow{+} & & \xrightarrow{+} & \underline{A} \\
 \\
 \underline{R} \times \underline{R} \times \underline{A} & \xrightarrow{\cong} & (\underline{R} \times \underline{R}) \times \underline{A} & \xrightarrow{+ \times \text{id}} & \underline{R} \times \underline{A} \\
 \downarrow (\pi_1 \times \pi_3) \times (\pi_2 \times \pi_3) & & & & \downarrow * \\
 (\underline{R} \times \underline{A}) \times (\underline{R} \times \underline{A}) & & & & \\
 \downarrow * \times * & & & & \downarrow * \\
 \underline{A} \times \underline{A} & \xrightarrow{+} & & \xrightarrow{+} & \underline{A} \\
 \\
 (\underline{R} \times \underline{R}) \times \underline{A} & \xrightarrow{\cong} & \underline{R} \times (\underline{R} \times \underline{A}) & \xrightarrow{\text{id} \times *} & \underline{R} \times \underline{A} \\
 \downarrow \cdot \text{id} & & & & \downarrow * \\
 \underline{R} \times \underline{A} & \xrightarrow{*} & & \xrightarrow{*} & \underline{A}
 \end{array}$$

$$\begin{array}{ccc}
 \underline{1 \times A} & \xrightarrow{\cong} & \underline{A} \\
 \downarrow 1 \times \text{id} & & \downarrow \text{id} \\
 \underline{R \times A} & \xrightarrow{*} & \underline{A}
 \end{array}$$

For all open  $U \subseteq X$  and for all  $\alpha \in X$  we have  $R(U)$ -modules  $A(U)$  and  $R_\alpha$ -modules  $A_\alpha$ . The strong extensionality of the scalar multiplication is equivalent to the property  $\alpha x \neq 0 \rightarrow \alpha \neq 0 \wedge x \neq 0$ . This formula is of type N and of type P. So this property and hence 2.1.3(2) is equivalent to the assertion that for the scalar multiplication in the stalks we have  $I_\alpha \cdot A_\alpha \subseteq N_\alpha$  and  $R_\alpha \cdot N_\alpha \subseteq N_\alpha$ .

Example:

Let  $R$  be a (classical) ring,  $I \subseteq R$  an ideal. Let  $A$  be a module over  $R$  with submodule  $N \subseteq A$  so that  $I \cdot A \subseteq N$ . Then the following Kripke models  $\underline{R}$  and  $\underline{A}$  with canonical morphisms form a ring model  $\underline{R}$  and a module  $\underline{A}$  over  $\underline{R}$ . The ideals and submodules in the nodes are the  $I_\alpha$  and  $N_\alpha$  as mentioned above.

$$\begin{array}{ccc}
 \underline{R}: & R, 0 & R/I, 0 \\
 & \swarrow & \searrow \\
 & R, I & \\
 \underline{A}: & A, 0 & A/N, 0 \\
 & \swarrow & \searrow \\
 & A, N &
 \end{array}$$

Observe that  $A/N$  is the module over  $R/I$  with scalar multiplication  $\xi/I \cdot a/N = \xi a/N$ .

### 3. LINEAR ALGEBRA

#### 3.1 Local rings and fields

In the literature there exist several versions of intuitionistic field theory, all extending the notion of field in classical mathematics. For some of these theories, some statements have been derived, which are extensions of well-known properties in classical mathematics. As we shall do here with linear algebra, we of course have to reprove all of such statements, starting on an elementary level. However, it is not very attractive, if we have to do this for each of these field theories again. We cannot avoid this completely, because on a more advanced level the different theories will diverge, but on the level of linear algebra some theories are close enough so that we can give a uniform way to derive their basic properties ([He 2], [Ko 1], [Re 1], [Jo 1],[Ju 1]). Therefore we shall do linear algebra over local rings.

Further we shall consider the following sorts of field theory:

3.1.1. Definition. A W-field is a local ring satisfying

$$\forall \alpha. (\neg E\alpha^{-1} \rightarrow \neg \alpha \equiv 0).$$

An H-field is a local ring satisfying

$$\forall \alpha (\neg E\alpha^{-1} \rightarrow \alpha \equiv 0).$$

An AK-field is a local ring satisfying for all  $n$

$$\forall \alpha_1, \dots, \alpha_n \left( \neg \bigwedge_{1 \leq i \leq n} \alpha_i \equiv 0 \rightarrow \bigvee_{1 \leq i \leq n} E\alpha_i^{-1} \right)$$

As we observed before, an H-field is just a field in the sense of chapter 2. The relation  $E(x-y)^{-1}$  is an apartness relation on local rings making the operations strongly extensional. The extra axiom for H-fields makes this apartness tight. The axiom defining a W-field is fairly weak. It is possible to construct models for the theory of W-fields satisfying

$$\neg \forall \alpha (\neg E \alpha^{-1} \rightarrow \alpha \equiv 0)$$

or satisfying

$$\neg \forall \alpha (\neg \alpha \equiv 0 \rightarrow E \alpha^{-1}).$$

On the other hand both H-fields and AK-fields are W-fields. AK-fields are studied in [Ko 1] and [Re 1].

There is a little ambiguity in the definition of AK-fields: in the presence of a natural number object we have an object of finite sequences of field elements. Now we can interpret the definition so as to quantify over sequence objects. Another way of interpreting the definition is to read it as a scheme of axioms with  $n = 1, 2, \dots$ . Usually it is enough to work with the scheme, but for instance if we wish to work with matrices, whose size is indexed by a natural number internally, we need an AK-field with quantification over the sequence object.

By introducing modules over a local ring we have to distinguish modules which are provided with an apartness and modules without apartness.

3.1.2. Definition. An R-module without apartness (defined as usual) will be called a general module.



An R-module provided with apartness so that scalar multiplication is strongly extensional will be called a strong module. We tacitly assume that the apartness on such a module is tight if R is an H-field. The names introduced here are used in chapter 3 only.

From chapter 1 we get that each submodule of a module of the form  $R^X$  is, with canonical apartness, a strong module over R and also over subrings of R. Thus  $R^n$  is a strong R-module for local rings R, with canonical apartness:

$$(\alpha_1, \dots, \alpha_n) \# (\beta_1, \dots, \beta_n) \leftrightarrow \bigwedge_{1 \leq i \leq n} (E\alpha_i \wedge E\beta_i) \wedge \bigwedge_{1 \leq i \leq n} \alpha_i \# \beta_i.$$

### 3.2 Dependence, independence and freedom

With respect to notions like dependence, independence and freedom we shall restrict our attention to finite sequences of vector elements of the modules.

3.2.1. Definition. Let A be a general R-module and  $y, y_1, \dots, y_m, x_1, \dots, x_n \in A$ .

1.  $y_1, \dots, y_m$  depends on  $x_1, \dots, x_n$  if for all  $y_i$  we have

$$\exists \alpha_1, \dots, \alpha_n \in R \ y_i \equiv \alpha_1 x_1 + \dots + \alpha_n x_n.$$

2.  $y_1, \dots, y_m$  and  $x_1, \dots, x_n$  are equivalent if the two sequences depend on each other (i.e. if they generate the same submodule).

3.  $y$  is independent of  $x_1, \dots, x_n$  if we have

$$\forall \alpha_1, \dots, \alpha_n \in R \ \neg y \equiv \alpha_1 x_1 + \dots + \alpha_n x_n.$$

4. For strong modules we can define:

$y$  is free from  $x_1, \dots, x_n$  if we have

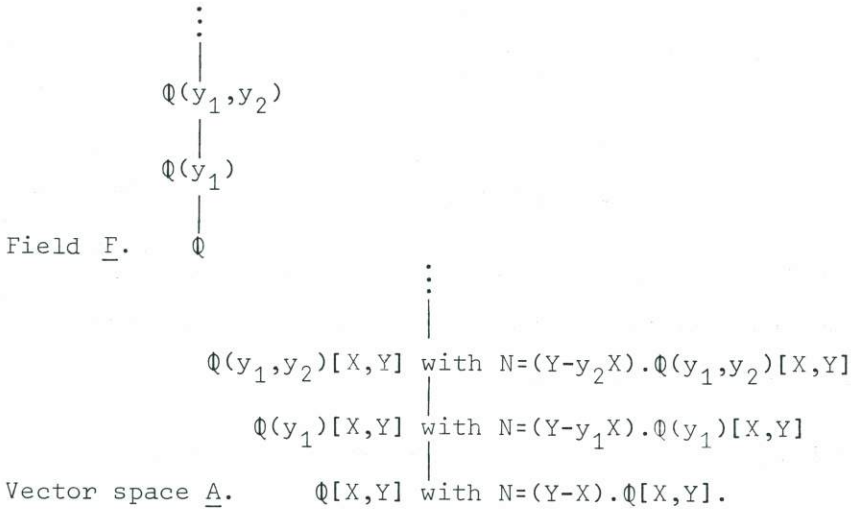
$$\forall \alpha_1, \dots, \alpha_n \in R \ y \# \alpha_1 x_1 + \dots + \alpha_n x_n.$$

Clearly we have:

$\neg$  "y depends on  $x_1, \dots, x_n$ "  $\leftrightarrow$  "y independent of  $x_1, \dots, x_n$ "  
 and "y is free from  $x_1, \dots, x_n$ "  $\rightarrow$  "y is independent of  $x_1, \dots, x_n$ ".

The expressions in quotes abbreviate certain formulas of the formal language. In classical mathematics the last implication could be replaced by a bi-implication if we should consider vector spaces over fields.

3.2.2. Example. The following vector space model over a field shows that in intuitionistic logic this is not so simple.



The N's in the definition of the node structures of  $\underline{A}$  are the  $N_\alpha$ 's of 2.10.1. In the definition of  $\underline{F}$  we need not specify the unique maximal ideals. In fact they are the 0-ideals of the fields in the nodes.  $\underline{F}$  is an H-field as well as an AK-field and  $\underline{A}$  is a (strong) module over  $\underline{F}$  with tight apartness. We have:

$$\underline{F} \models \forall \alpha (\alpha \neq 0 \vee \alpha \equiv 0)$$

and  $\underline{A} \models \forall x (\neg x \equiv 0 \vee x \equiv 0)$ , but nevertheless:

$(\underline{F}, \underline{A}) \models \dot{Y}$  is independent of  $\dot{X} \wedge \neg \dot{Y}$  is free from  $\dot{X}$ ".

3.2.3. Definition. Let  $x_1, \dots, x_n \in A$ , a general module.

1.  $x_1, \dots, x_n$  are weakly dependent if

$$\exists \alpha_1, \dots, \alpha_n \left( \bigwedge_{1 \leq i \leq n} \alpha_i \equiv 0 \wedge \alpha_1 x_1 + \dots + \alpha_n x_n \equiv 0 \right)$$

2. Over strong modules  $A$  we define:

$x_1, \dots, x_n$  are strongly dependent if

$$\exists \alpha_1, \dots, \alpha_n \left( \bigwedge_{1 \leq i \leq n} \alpha_i \neq 0 \wedge \alpha_1 x_1 + \dots + \alpha_n x_n \equiv 0 \right)$$

With respect to strong modules over AK-fields the notions are equivalent. Over W-fields the negations are equivalent. Over H-fields these negations are equivalent to the notion of independence, because of the stability of the equality (chapter 1).

3.2.4. Definition. Let  $A$  be a general module,  $x_1, \dots, x_n \in A$ .

1.  $x_1, \dots, x_n$  is independent if

$$\forall \alpha_1, \dots, \alpha_n \left( \alpha_1 x_1 + \dots + \alpha_n x_n \equiv 0 \rightarrow \bigwedge_{1 \leq i \leq n} \alpha_i \equiv 0 \right).$$

2. Over strong modules  $A$  we define:

$x_1, \dots, x_n$  is free if

$$\forall \alpha_1, \dots, \alpha_n \left( \bigwedge_{1 \leq i \leq n} \alpha_i \neq 0 \rightarrow \alpha_1 x_1 + \dots + \alpha_n x_n \neq 0 \right).$$

For the construction of free sequences we have the following

3.2.5. Lemma. Let  $A$  be a strong module and  $y, x_1, \dots, x_n \in A$ .

Let  $x_1, \dots, x_n$  be free and  $y$  free from  $x_1, \dots, x_n$ . Then  $y, x_1, \dots, x_n$  is free.

Proof: Let  $\alpha_0, \dots, \alpha_n \in R$  such that  $\bigwedge_{0 \leq i \leq n} \alpha_i \neq 0$ .

Let  $z \equiv \alpha_0 y + \alpha_1 x_1 + \dots + \alpha_n x_n$ . To prove:  $z \neq 0$ . We have

$\alpha_0 \neq 0 \vee \bigvee_{1 \leq i \leq n} \alpha_i \neq 0$ . From  $\alpha_0 \neq 0$  we get  $E\alpha_0^{-1}$  and

$$y \equiv \alpha_0^{-1} z - \alpha_0^{-1} (\alpha_1 x_1 + \dots + \alpha_n x_n).$$

$y$  free from  $x_1, \dots, x_n$  gives  $z \neq 0$ . From  $\bigvee_{1 \leq i \leq n} \alpha_i \neq 0$  we get

$$z - \alpha_0 y \neq 0, \text{ for } x_1, \dots, x_n \text{ is free.}$$

Thus  $z \neq 0 \vee \alpha_0 \neq 0$ . From  $\alpha_0 \neq 0$  we already derived  $z \neq 0$ . Thus  $z \neq 0$ .

### 3.3 The Austauschatz

As Heyting observed ([He 2]), the Austauschatz is a basic tool in many proofs. Before we present the theorem we give a lemma.

3.3.1. Lemma. Let  $A$  be a strong module,  $x, y_1, \dots, y_n \in A$  such that  $x \neq 0$  and  $x$  depends on  $y_1, \dots, y_n$ . Then there is an  $i$ ,  $1 \leq i \leq n$ , such that  $y_i \neq 0$  and  $y_1, \dots, y_{i-1}, x, y_{i+1}, \dots, y_n$  and  $y_1, \dots, y_n$  are equivalent. Moreover, if one of these sequences is free or independent, then so is the other sequence.

Proof: There are  $\alpha_1, \dots, \alpha_n$  such that

$$x \equiv \alpha_1 y_1 + \dots + \alpha_n y_n \neq 0, \text{ thus } \bigvee_{1 \leq i \leq n} \alpha_i y_i \neq 0.$$

Then there is an  $i$ ,  $1 \leq i \leq n$ , such that  $y_i \neq 0$  and  $\alpha_i \neq 0$  and

$$y_i \equiv \alpha_i^{-1} (-\alpha_1 y_1 - \dots - \alpha_{i-1} y_{i-1} + x - \alpha_{i+1} y_{i+1} - \dots - \alpha_n y_n).$$

Conclusion:  $y_1, \dots, y_{i-1}, x, y_{i+1}, \dots, y_n$  and  $y_1, \dots, y_n$  are equivalent. This transformation is invertible, because  $y_i \neq 0$  and  $y_i$  depends on  $y_1, \dots, y_{i-1}, x, y_{i+1}, \dots, y_n$  in the way described above. For the last claim it is enough, because of the invertibility,

to prove one direction : if  $y_1, \dots, y_n$  is free, then  $y_1, \dots, y_{i-1}, x, y_{i+1}, \dots, y_n$  is free. The same for independence. Assume  $y_1, \dots, y_n$  free and let  $\beta_1, \dots, \beta_n$  be given, satisfying  $\bigwedge_{1 \leq i \leq n} \beta_i \neq 0$ .

Let  $z \equiv \beta_1 y_1 + \dots + \beta_{i-1} y_{i-1} + \beta_i x_i + \beta_{i+1} y_{i+1} + \dots + \beta_n y_n$ . To prove:  $z \neq 0$ .

We have:

$$z \equiv (\beta_1 + \alpha_1 \beta_i) y_1 + \dots + (\beta_{i-1} + \alpha_{i-1} \beta_i) y_{i-1} + \alpha_i \beta_i y_i + (\beta_{i+1} + \alpha_{i+1} \beta_i) y_{i+1} + \dots$$

If  $\beta_i \neq 0$  then  $\alpha_i \beta_i \neq 0$  and thus  $z \neq 0$ , because  $y_1, \dots, y_n$  is free. If  $\beta_j \neq 0$  for  $\neg i \equiv j$  then

$\beta_j + \alpha_j \beta_i \neq 0 \vee \alpha_j \beta_i \neq 0$ . And this gives  $z \neq 0$ , because  $y_1, \dots, y_n$  is free and  $\alpha_i$  is invertible. The proof for independence is similar.

With the lemma we get (see [He 2]):

3.3.2. Theorem (Austauschsatz). Let  $A$  be a strong module and  $x_1, \dots, x_m, y_1, \dots, y_n \in A$  such that

$$x_1, \dots, x_m \text{ is free and } x_1, \dots, x_m \text{ depends on } y_1, \dots, y_n.$$

Then there is a sequence  $z_1, \dots, z_n \in A$ , made from  $y_1, \dots, y_n$  by replacing  $m$  vectors by  $x_1, \dots, x_m$ , such that

$$z_1, \dots, z_n \text{ is equivalent to } y_1, \dots, y_n.$$

Moreover, if one of these sequences is free or independent, then so is the other sequence.

Proof: We apply the proposition to the successive substitution of  $x_1, \dots, x_m$ . There is only one aspect that we have to check. If we have replaced say  $y_1, \dots, y_i$  by  $x_1, \dots, x_i$ , then we know

(induction) that  $x_1, \dots, x_i, y_{i+1}, \dots, y_n$  and  $y_1, \dots, y_n$  are equivalent. Now we must replace one of  $y_{i+1}, \dots, y_n$  by  $x_{i+1}$ . This is possible because there are  $\alpha_1, \dots, \alpha_n$  so that

$$x_{i+1} = \alpha_1 x_1 + \dots + \alpha_i x_i + \alpha_{i+1} y_{i+1} + \dots + \alpha_n y_n.$$

Now  $x_{i+1} - \alpha_1 x_1 - \dots - \alpha_i x_i \neq 0$  because  $x_1, \dots, x_{i+1}$  is free.

Thus  $\sum_{j \geq i+1} \alpha_j y_j \neq 0$ .

Then we apply the method of the lemma. The remaining details are routine.

3.3.3. Corollary. If in the premiss of the Austauschatz  $m = n$ , then  $x_1, \dots, x_n$  is equivalent to  $y_1, \dots, y_n$  and  $y_1, \dots, y_n$  is free.

### 3.4 Independence and freedom over AK-fields

With respect to vector spaces over H-fields freedom is the basic notion to work with. With respect to AK-fields one uses independence ([Ko 1], [Re 1]). So 3.3.2. seems to be less interesting for vector spaces over AK-fields.

Let  $R$  be an AK-field and consider the strong module  $R^m$  over  $R$ . It is simple to show that this vector space satisfies:

$$\forall x_1, \dots, x_n (\neg \bigwedge_{1 \leq i \leq n} x_i = 0 \rightarrow \bigvee_{1 \leq i \leq n} x_i \neq 0).$$

As a special case: for  $n = 1$  we have  $\forall x (\neg x = 0 \leftrightarrow x \neq 0)$ . Therefore we have for  $x_1, \dots, x_n \in R^m$ : if  $x_1, \dots, x_n$  is independent, then  $x_1, \dots, x_n$  is free. Now we shall present a result in the converse direction.

3.4.1. Lemma. Let  $R$  be a W-field. For  $x_1, \dots, x_n \in R^m$ , if  $x_1, \dots, x_n$  is free then  $x_1, \dots, x_n$  is independent.

Proof: let  $x_1, \dots, x_n \in R^m$  be free.  $x_1, \dots, x_n$  depends on the basis  $e_1, \dots, e_m \in R^m$ . Using the Austauschatz we can extend our sequence to length  $m$ . It is enough to prove that this new sequence  $x_1, \dots, x_m$ , which is free, also is independent. Let the vectors  $x_1, \dots, x_m$  form the columns of an  $m \times m$ -matrix  $M$  with  $\det M \neq 0$ , i.e.  $M$  has an inverse  $M^{-1}$  (by 3.7.2). Now assume  $\alpha_1 x_1 + \dots + \alpha_m x_m = 0$  and let  $a = (\alpha_1, \dots, \alpha_m)$ . We must show that  $a = 0$ . We know that  $Ma = 0$ , thus:

$$a = M^{-1} M a = M^{-1} 0 = 0.$$

AK-fields are W-fields. Thus if  $R$  is an AK-field and  $x_1, \dots, x_n \in R^m$  then we have

$$"x_1, \dots, x_n \text{ is independent}" \leftrightarrow "x_1, \dots, x_n \text{ is free}."$$

### 3.5 Degree and dimension

A basic notion in linear algebra is dimension. We shall use more than one intuitionistic version of that notion in classical mathematics.

3.5.1. Definition. Let  $x_1, \dots, x_n \in A$ .

1. If  $x_1, \dots, x_n$  generates  $A$  we say that  $A$  has degree at most  $n$ .
2. If  $x_1, \dots, x_n$  is free ( $A$  is strong) we say that  $A$  has degree at least  $n$ .
3. If  $x_1, \dots, x_n$  generates  $A$  freely ( $A$  strong), we say that  $A$  has degree  $n$  or is of degree  $n$ .
4. If  $x_1, \dots, x_n$  generates  $A$  independently, we say that  $A$  is  $n$ -dimensional.

Notations:  $\deg(A) \leq n$ ,  $\deg(A) \geq n$ ,  $\deg(A) = n$ ,  $\dim(A) = n$ .

It is a simple task to extend the list of definitions with

properties, related to names like  $\dim(A) \leq n$  and  $\dim(A) \geq n$ .

From the Austauschatz we can derive some corollaries concerning degrees.

3.5.2. Remark. 1. If the degree of a strong module exists, then it is unique. Thus  $\deg(A)$  is a partial map.

2. Let  $A$  be a strong module so that  $\deg(A)$  exists. Let  $x_1, \dots, x_m \in A$ . If  $x_1, \dots, x_m$  generates  $A$ , then  $\deg(A) \leq m$ . If  $x_1, \dots, x_m$  is free, then  $\deg(A) \geq m$ .

The same sort of statements can be made for dimension, but then we need the Generators Theorem, so we postpone their treatment. Degree and dimension are not equivalent, even if we restrict ourselves to the very special vector space-model of 3.2.2:

Take the sub vector space of  $\underline{A}$  over  $\underline{F}$ , generated by  $X$  and  $Y$ , say  $\underline{B}$ . Then  $(\underline{F}, \underline{B}) \models \text{"}\underline{B} \text{ has dimension } 2\text{"} \wedge \neg \text{"}\underline{B} \text{ has a degree"}$ .

From this we conclude, that the vector space  $\underline{B}$  is not embeddable in any vector space of the form  $\underline{F}^n$ , because we can derive:

3.5.3. Proposition. Let  $A$  be a vector space over a  $W$ -field with  $\deg(A) = n$ . Let  $B$  be a finitely generated subspace.

Then we have:

$$\neg \neg \text{"}B \text{ has a degree"}$$

We shall give a proof in 3.7.4.

### 3.6 The rank of a matrix

Now we shall study  $R$ -modules of the form  $R^n$  in more detail. As we already observed (3.1.2), this is a strong module and it has degree  $n$ . Morphisms  $\varphi: R^n \rightarrow R^m$  can be expressed by  $m \times n$ -matrices



$$M \equiv \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{m1} & \cdots & \alpha_{mn} \end{pmatrix} \text{ with } \alpha_{ij} \in R.$$

Matrices will play an important role in most proofs below.

3.6.1. Definition. Let  $A$  be a strong module and  $x_1, \dots, x_n \in A$ .

We say that this sequence has rank  $r$  if the submodule generated by it has degree  $r$ . In other words: there exists a sequence  $y_1, \dots, y_r \in A$  such that

1.  $x_1, \dots, x_n$  and  $y_1, \dots, y_r$  are equivalent
2.  $y_1, \dots, y_r$  is free.

Let  $M$  be an  $m \times n$ -matrix. Then the  $n$  columns may be seen as a sequence of vectors out of  $R^m$  and the  $m$  rows may be seen as a sequence of vectors of  $R^n$ . The ranks of these sequences are called column rank and row rank respectively. We want to prove that they are equal. Therefore we need a lemma.

3.6.2. Lemma. If the column rank (or the row rank) of a matrix exists, then it is invariant under the following manipulations:

1. Permutation of columns, multiplication of a column by a factor  $\alpha \neq 0$  and addition to a column of a linear combination of the other columns.
2. As 1., but for rows.

Proof: straightforward.

One easily verifies that there are analogous invariance properties for weak and strong dependence and also for something like independence rank for rows and columns.

3.6.3. Theorem. If the column rank or the row rank of a matrix exists, then they both exist and are equal.

Proof: by induction on the size of the matrix.

Given a matrix  $\begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{m1} & \cdots & \alpha_{mn} \end{pmatrix}$  with, say, column rank  $r > 0$ .

Then  $\alpha_{i,j} \neq 0$  for some  $i, j$ . Applying row and column permutations (allowed by the lemma) we may assume  $\alpha_{11} \neq 0$ .

With the manipulations of the lemma we can make a new matrix with the same column rank and - if it exists - the same row rank: using the invertibility of  $\alpha_{11}$  we can get:

$$\begin{pmatrix} \alpha_{11} & 0 & \cdots & 0 \\ 0 & \beta_{22} & \cdots & \beta_{1n} \\ \vdots & \vdots & & \vdots \\ 0 & \beta_{m2} & \cdots & \beta_{mn} \end{pmatrix}$$

We apply induction on the lower right  $(m-1) \times (n-1)$ -matrix: it has column rank  $(r-1)$ . Thus also row rank  $(r-1)$ . But then the row rank of the total matrix is  $r$ .

We define the rank of a matrix as the column rank. We cannot generalize this theorem to independence rank without extra assumptions. Namely, the problem is to find the invertible  $\alpha_{ij}$ . It turns out that we just need the extra axioms for an AK-field. Thus over AK-fields independence rank exists.

Assume, that the matrix  $\begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{m1} & \cdots & \alpha_{mn} \end{pmatrix}$  has among the

columns a subsequence, say the first  $r$  columns

$\begin{pmatrix} \alpha_{11} \\ \vdots \\ \alpha_{m1} \end{pmatrix}, \dots, \begin{pmatrix} \alpha_{1r} \\ \vdots \\ \alpha_{mr} \end{pmatrix}$ , of  $r$  free vectors.

Then the same holds for the rows.

Take the submatrix  $N \equiv \begin{pmatrix} \alpha_{11} & \dots & \alpha_{1r} \\ \vdots & & \vdots \\ \alpha_{m1} & \dots & \alpha_{mr} \end{pmatrix}$ .

Then  $\text{rank}(N) = r$ . Thus there are  $r$  rows free. The extension to the original matrix preserves freedom. The same method works for independent sequences over AK-fields.

### 3.7 The determinant

In intuitionistic mathematics the theory of determinants is of more importance than in classical mathematics because of its "constructive" character. For example let  $x_1, \dots, x_n \in R^m$  be free. Let  $x_{n+1} \in R^m$ . If we want to know whether  $x_{n+1}$  depends on  $x_1, \dots, x_n$  we have to go through all linear combinations  $\alpha_1 x_1 + \dots + \alpha_n x_n$  to find out whether this is equal to  $x_{n+1}$  or not: i.e. we have to show:  $\exists \alpha_1, \dots, \alpha_n \in R. (\alpha_1 x_1 + \dots + \alpha_n x_n \equiv x_{n+1})$ . This precisely requires the computation of a finite number of determinants:

$$\bigwedge_{1 \leq i \leq p} \det M_i \equiv 0$$

where the  $M_i$  range over a finite collection of  $(n+1) \times (n+1)$  matrices. The point in favour of the use of determinants

is that it allows us to reduce logical complexity. Let  $R$  be an H-field. Then  $x_1, \dots, x_n, x_{n+1}$  is free if  $\forall \alpha_1, \dots, \alpha_n, \alpha_{n+1} \in R. (\bigvee \alpha_i \neq 0 \rightarrow \sum \alpha_i x_i \neq 0)$ . This is equivalent to

$$\bigwedge_{1 \leq i \leq p} \det M_i \neq 0.$$

where the  $M_i$  range over the same collection of  $(n+1) \times (n+1)$  matrices as above. In both cases we have eliminated quantifiers. Especially in constructive mathematics the quantifier free formulation can be used to show for H-fields  $R$ : if  $x_1, \dots, x_n, x_{n+1} \in R^m$  so that  $x_1, \dots, x_n$  is free then

$$\neg "x_1, \dots, x_n, x_{n+1} \text{ is free}" \leftrightarrow "x_{n+1} \text{ depends on } x_1, \dots, x_n".$$

3.7.1. Definition. Let  $M$  be an  $n \times n$ -matrix. Then  $\det(M)$  is the well-known polynomial in the  $n^2$  entries.

From Cramer's rule it follows that for every  $n \times n$ -matrix  $M$  there is an  $n \times n$ -matrix  $N$  such that

$$MN = NM = \det(M) \cdot I_n \text{ with } I_n \text{ the } n \times n\text{-identity matrix.}$$

This even works for  $n \times n$ -matrices over a ring. The coefficients of  $N$  are polynomials in the coefficients of  $M$ .

With this property one can verify:

3.7.2. Proposition. Let  $M$  be an  $n \times n$ -matrix with coefficients  $\in R$ . Then:

1.  $\forall x \in R^n (x \neq 0 \rightarrow Mx \neq 0) \leftrightarrow \det M \neq 0$ .
2. " $M$  invertible"  $\leftrightarrow \det M \neq 0$ .

For arbitrary formulas  $\varphi$  and  $\psi(x)$ , with  $x$  not free in  $\varphi$ , the following formula is not generally valid:

$$\forall x (\varphi \vee \psi(x)) \rightarrow \varphi \vee \forall x \psi(x).$$

Nevertheless we have the following

3.7.3. Lemma. Let  $M$  be an  $n \times n$ -matrix. Then we have

$$\forall x \in R^n (x \neq 0 \rightarrow (\varphi \vee Mx \neq 0)) \rightarrow \varphi \vee \det M \neq 0.$$

Proof: By induction on  $n$ .  $n=1$  is trivial, thus we consider  $n>1$ . Given the  $n \times n$ -matrix  $M$  and given the induction hypothesis, take the first vector  $e_1$  of the standard basis (basis = free generators)  $e_1, \dots, e_n$ .  $e_1 \neq 0$ , then we have  $\varphi \vee Me_1 \neq 0$ . To prove:  $\varphi \vee \det M \neq 0$ . If  $\varphi$ , then we are done. If  $Me_1 \neq 0$ , then we have  $\bigvee_{1 \leq i \leq n} \alpha_{i1} \neq 0$ , say  $\alpha_{11} \neq 0$ . (Here  $M = (\alpha_{ij})$ ).

$$\text{Let } S \equiv \begin{pmatrix} 1 - \frac{\alpha_{12}}{\alpha_{11}} - \frac{\alpha_{13}}{\alpha_{11}} \dots - \frac{\alpha_{1n}}{\alpha_{11}} \\ 0 & 1 & 0 & \dots & 0 \\ 0 & 0 & 1 & & \cdot \\ \vdots & \vdots & & & \vdots \\ 0 & 0 & 0 \dots 0 & & 1 \end{pmatrix}$$

Now  $\det S = 1$ , thus  $S$  is invertible and

$$MS \equiv \begin{pmatrix} \alpha_{11} & 0 & \dots & 0 \\ \alpha_{21} & \boxed{\phantom{B}} \\ \vdots & & & \\ \alpha_{n1} & & & \end{pmatrix}$$

Using transposition and the same arguments we see that there is an invertible  $n \times n$ -matrix  $T$  such that  $\det T = 1$  and

$$TMS \equiv \begin{pmatrix} \alpha_{11} & 0 & \dots & 0 \\ 0 & \boxed{\phantom{C}} \\ \vdots & & & \\ 0 & & & \end{pmatrix} \quad . \text{ Thus } \det M = \alpha_{11} \cdot \det C.$$

Induction:  $\forall x \in \mathbb{R}^{n-1} (x \neq 0 \rightarrow (\varphi \vee Cx \neq 0)) \rightarrow \varphi \vee \det C \neq 0$ .

The left hand side of this implication is derivable from the assumption about  $M$ , thus:

$$\varphi \vee \det C \neq 0, \text{ and hence } \varphi \vee \det M \neq 0.$$

Matrices need not have a rank. But over W-fields we have for each matrix M:

$\neg \neg$  "M has a rank".

Proof: use the determinants of the square submatrices and apply double negations. With this fact we can prove proposition 3.5.3.:

3.7.4. Proposition. Let A be a vector space over a W-field with  $\text{deg}(A) \equiv n$ . Let B be a finitely generated subspace. Then we have:

$\neg \neg$  "B has a degree".

Proof: Write the generators  $y_i$  of B as

$$y_i \equiv \alpha_{1i}x_1 + \dots + \alpha_{ni}x_n, \quad x_1, \dots, x_n \text{ a basis of A.}$$

For the matrix  $M \equiv \begin{pmatrix} \alpha_{11} & \dots & \alpha_{1r} \\ \vdots & & \vdots \\ \alpha_{n1} & \dots & \alpha_{nr} \end{pmatrix}$  we have:  $\neg \neg$  "M has a rank".

And from that it follows:  $\neg \neg$  "B has a degree".

Another application of the result above is: let A be a vector space over an H-field with  $\text{deg}(A) \equiv n$ . Let  $y_1, \dots, y_r \in A$ . Then we have

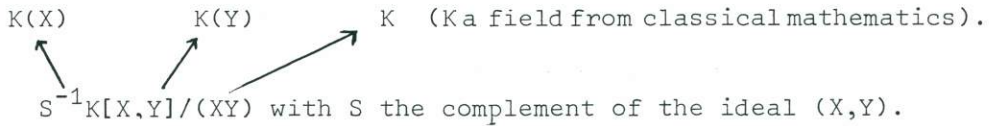
" $y_1, \dots, y_r$  is independent"  $\leftrightarrow \neg \neg$  " $y_1, \dots, y_r$  is free"

(see 3.5.2.).

Given a matrix M with an  $r \times r$ -invertible submatrix and so that each  $(r+1) \times (r+1)$ -submatrix has determinant 0. By using lemma 3.6.2 it is simple to show  $\text{rank}(M) \equiv r$  (see 3.10.7).

But if we have a square matrix  $M$  with  $\det(M) \equiv 0$ , then the columns or rows need not be dependent: even not over a field. Take the following model:

$\underline{F}$  is:



$\underline{F}$  is an H-field as well as an AK-field. For the matrix  $M \equiv \begin{pmatrix} X & 0 \\ 0 & Y \end{pmatrix}$  we have  $\det(M) \equiv 0$ , but the columns are not even weakly dependent.

There may be other notions of dependence for the columns of the matrix  $M$  above. We shall list some of them

1. Strongly dependent.
2. Weakly dependent.
3. Not independent.
4. Not free.

It is simple to verify that we have (for strong modules)

$$(1 \rightarrow 2) \vee (2 \rightarrow 3).$$

Further we have for vector spaces over H-fields  $(3 \rightarrow 4)$  and

$$\neg 1 \leftrightarrow \neg 2 \leftrightarrow \neg 3. \text{ But none of } 1, 2, 3 \text{ and } 4 \text{ are equivalent.}$$

There is even a model of  $\neg 3 \wedge 4$  (3.5.2).

Returning to the square matrix  $M$  over  $\underline{F}$ :

If  $\det(M) \equiv 0$  then

$$\neg \text{"the columns are independent"}, \text{ thus version 3 holds.}$$

### 3.8 Left and right inverses

We shall give some properties which can simply be derived

from previous results. Here we study the possibility to simplify the structure of a matrix by multiplication on the left hand side or on the right hand side.

3.8.1. Theorem. Let  $M$  be an  $m \times n$ -matrix over  $R$  and  $r \in \mathbb{N}$ .

Then the following assertions are equivalent:

1.  $M$  has  $r$  columns free.
2.  $M$  has  $r$  rows free.
3. There is an  $n \times m$ -matrix  $N$  and an  $n \times n$ -permutation matrix  $S$  such that

$$NM \equiv S \cdot \begin{pmatrix} 1 & 0 & \dots & 0 & \boxed{\phantom{*}} \\ 0 & 1 & & & \\ \vdots & & \ddots & & \\ 0 & \dots & & 0 & \\ \vdots & & & & \\ 0 & \dots & & 1 & \\ \vdots & & & & \\ 0 & \dots & & & 0 \\ \vdots & & & & \\ 0 & \dots & & & 0 \end{pmatrix} \cdot S^{-1}, \text{ with } r \text{ times } 1 \text{ on the diagonal.}$$

4. There is an  $n \times m$ -matrix  $N$  and an  $m \times m$ -permutation matrix  $S$  such that

$$MN \equiv S \cdot \begin{pmatrix} 1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 1 & & & \vdots & & \vdots \\ \vdots & & & & 0 & & \vdots \\ 0 & \dots & & 0 & 1 & & \vdots \\ \vdots & & & & & & \vdots \\ \boxed{*} & & & & & & 0 \dots 0 \end{pmatrix} \cdot S^{-1}, \text{ with } r \text{ times } 1 \text{ on the diagonal.}$$

From this we get

3.8.2. Corollary. 1. Let  $M$  be an  $m \times n$ -matrix with  $m \geq n$ . Then we have:  $M$  has rank  $n$  if and only if there is an  $n \times m$ -matrix  $N$ , such that  $NM \equiv I_n$ .

2. Let  $M$  be an  $m \times n$ -matrix with  $n \geq m$ . Then we have:  $M$  has rank  $m$  if and only if there is an  $n \times m$ -matrix  $N$ , such that



$$MN \equiv I_m.$$

The corollary remains valid if we replace the identities  $I_n$  and  $I_m$  by invertible matrices of the same size. In both cases  $M$  and  $N$  have the maximal rank.

### 3.9 The Generators Theorem

In the Generators Theorem we need notions like sum and direct sum.

3.9.1. Definition. Let  $A$  be a strong module, and  $B$  and  $C$  subspaces. Then we define

$A \equiv B \oplus C$  if and only if

1.  $A \equiv B + C$ , that means  $\forall a \in A \exists b \in B \exists c \in C \quad a \equiv b + c$
- and 2.  $\forall b \in B \forall c \in C (b \neq 0 \vee c \neq 0 \rightarrow b + c \neq 0)$

In the same way we define over general modules:

$A \equiv B \oplus_w C$  if and only if

1.  $A \equiv B + C$
- and 2.  $\forall b \in B \forall c \in C (b + c \equiv 0 \rightarrow b \equiv 0 \wedge c \equiv 0)$ , or:  $B \cap C \equiv \{0\}$ .

Let  $A, B$  be general modules, then we can construct  $A \oplus_w B$  as in the traditional case. The same is true when we construct  $A \oplus B$  out of two strong modules  $A$  and  $B$ .

Let  $f: A \rightarrow B$  be a morphism of  $R$ -modules. Define kernel  $\text{Ker } f$  and image  $\text{Im } f$  as usual. Then we see: if  $A$  and  $B$  are general modules then

$$A \cong \text{Ker } f \oplus_w \text{Im } f$$

if we have a morphism  $\varphi: \text{Im } f \rightarrow A$  so that  $f \cdot \varphi = \text{id}$ . As bijective

morphism we can use the map  $\psi_1: A \rightarrow \text{Ker } f \oplus_w \text{Im } f$  defined by

$$\psi_1: x \mapsto (x - \varphi(f(x)), f(x)).$$

If we have a morphism  $\theta: A \rightarrow \text{Ker } f$  so that  $\theta \cdot i = \text{id}$  ( $i$  the inclusion map) then we also have a bijective morphism, namely:

$$\psi_2: x \mapsto (\theta(x), f(x)).$$

Let  $A$  and  $B$  be strong modules and let  $f$  be strongly extensional. When do we have isomorphisms  $A \cong \text{Ker } f \oplus_w \text{Im } f$ ? If  $\varphi$  is strongly extensional then  $\psi_1$  is an isomorphism. If for  $\theta$  we have:

$$\theta(x) \neq x \rightarrow f(x) \neq 0$$

then  $\psi_2$  is an isomorphism.

3.9.2. Theorem (Generators Theorem). Let  $x_1, \dots, x_m, y_1, \dots, y_n \in A$ ;  $n \leq m$ . Let  $B \subseteq A$  be the subspace generated by  $y_1, \dots, y_n$ . Let  $Z \subseteq A$  be the subspace generated by  $x_1, \dots, x_m$ . Let  $C \subseteq A$  be a subspace such that

$$A \cong B + C \text{ and}$$

$$A \cong Z + C.$$

Then we have:

1. There is a subspace  $X \subseteq A$  generated by a subsequence  $x_{i_1}, \dots, x_{i_n}$  so that  $A \cong X + C$  and so that:
2. If  $A \cong B \oplus_w C$  and  $y_1, \dots, y_n$  is independent, then  $x_{i_1}, \dots, x_{i_n}$  is independent and  $A \cong X \oplus_w C$ .
3. If  $A$  is strong,  $A \cong B \oplus C$  and  $y_1, \dots, y_n$  is free, then  $x_{i_1}, \dots, x_{i_n}$  is free and  $A \cong X \oplus C$ .

Proof: by induction on the number of generators  $n$  of  $B$ , we show the existence of  $x_{i_1}, \dots, x_{i_n}$ . We restrict ourselves to the induction step.

There are matrices

$$K \equiv \begin{pmatrix} \alpha_{11} & \cdots & \alpha_{1n} \\ \vdots & & \vdots \\ \alpha_{m1} & \cdots & \alpha_{mn} \end{pmatrix} \quad \text{and} \quad L \equiv \begin{pmatrix} \beta_{11} & \cdots & \beta_{1m} \\ \vdots & & \vdots \\ \beta_{n1} & \cdots & \beta_{nm} \end{pmatrix} \quad \text{such that}$$

$y_i \equiv \alpha_{1i}x_1 + \cdots + \alpha_{mi}x_m + d_i$  and  $x_i \equiv \beta_{1i}y_1 + \cdots + \beta_{ni}y_n + c_i$   
with  $c_i, d_i \in C$ .

$$\text{Let } LK \equiv \begin{pmatrix} \gamma_{11} & \cdots & \gamma_{1n} \\ \vdots & & \vdots \\ \gamma_{n1} & \cdots & \gamma_{nn} \end{pmatrix}$$

Then  $y_i \equiv \gamma_{1i}y_1 + \cdots + \gamma_{ni}y_n + \alpha_{1i}c_1 + \cdots + \alpha_{mi}c_m + d_i$ .

Now we apply the fact that

$$\det(LK) \neq 1 \vee \det(LK) \neq 0.$$

Consider  $\det(LK) \neq 0$ . Then the rank of  $L$  exists and is  $n$ .

Let the columns of  $L$ , numbered by  $i_1, \dots, i_n$ , be free. It is simple to prove that  $x_{i_1}, \dots, x_{i_n}$  generates an  $X$  with the right properties. Consider  $\det(LK) \neq 1$ . Writing  $\det(LK)$  as the well-known sum of  $n!$  products we find:

$$\gamma_{11} \cdots \gamma_{nn} \neq 1 \vee \left( \prod_{i \neq j} \gamma_{ij} \neq 0 \right).$$

For some  $i$  we must have  $\gamma_{ii} \neq 1$  or  $\gamma_{ij} \neq 0$  for some  $j \neq i$ . Then  $y_i$  depends on the  $y_k$  with  $k \neq i$  and on  $C$ . Thus

$$A \equiv B' + C$$

where  $B' \subseteq A$  is the subspace generated by  $y_1, \dots, y_{i-1}, y_{i+1}, \dots, y_n$ .

Now apply induction. This proves part one of the theorem.

Now assume that  $B \cap C \equiv \{0\}$  and  $y_1, \dots, y_n$  is independent. Then

in the induction process we find  $\alpha_{1i}c_1 + \cdots + \alpha_{mi}c_m + d_i \equiv 0$

for all  $i$ , thus

$$y_i \equiv \gamma_{1i}y_1 + \dots + \gamma_{ni}y_n.$$

The independence of  $y_1, \dots, y_n$  makes that

$$LK \equiv I_n.$$

So we find the subsequence, say  $x_1, \dots, x_n$ , such that

$$x_i \equiv \beta_{1i}y_1 + \dots + \beta_{ni}y_n + c_i \text{ and } \begin{pmatrix} \beta_{11} & \dots & \beta_{1n} \\ \vdots & & \vdots \\ \beta_{n1} & \dots & \beta_{nn} \end{pmatrix} \text{ invertible.}$$

To prove the independences:

$$\text{Assume } \delta_1x_1 + \dots + \delta_nx_n + c \equiv 0.$$

Then there is a sequence  $\epsilon_1, \dots, \epsilon_n$  such that

$$\begin{pmatrix} \epsilon_1 \\ \vdots \\ \epsilon_n \end{pmatrix} \equiv \begin{pmatrix} \beta_{11} & \dots & \beta_{1n} \\ \vdots & & \vdots \\ \beta_{n1} & \dots & \beta_{nn} \end{pmatrix} \begin{pmatrix} \delta_1 \\ \vdots \\ \delta_n \end{pmatrix} \quad \text{and}$$

$$\epsilon_1y_1 + \dots + \epsilon_ny_n + \delta_1c_1 + \dots + \delta_nc_n + c \equiv 0.$$

$B \cap C \equiv \{0\}$ , thus

$$\epsilon_1y_1 + \dots + \epsilon_ny_n \equiv 0. \quad y_1, \dots, y_n \text{ is independent:}$$

$$\epsilon_1 \equiv \dots \equiv \epsilon_n \equiv 0.$$

Thus  $\delta_1 \equiv \dots \equiv \delta_n \equiv 0$  and thus  $c \equiv 0$ .

Conclusion:  $x_1, \dots, x_n$  is independent and  $A \equiv X \oplus_w C$ .

This proves part 2. The proof of part 3 is analogous.

Assume  $A$  strong,  $A \equiv B \oplus C$  and  $y_1, \dots, y_n$  free. By going through the proof of part 1 we again find that  $\det(LK) \neq 0$  because if  $\det(LK) = 1$  then some  $y_i$  depends strongly on the other  $y_j$  and on  $C$ . That contradicts the assumptions. Thus we get the same invertible matrix  $(\beta_{ij})$  as in the proof of part 2.

3.9.3. Corollary. Let  $x_1, \dots, x_m$  and  $y_1, \dots, y_r$  be two sequences of generators. Let  $n \in \mathbb{N}$ , so that  $n \leq m, r$ . Then there is a subsequence  $x_{i_1}, \dots, x_{i_n}$  such that

$x_{i_1}, \dots, x_{i_n}, y_{n+1}, \dots, y_r$  is a sequence of generators.

A special case of this is:

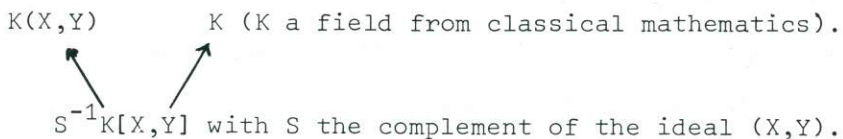
3.9.4. Corollary. Let  $y_1, \dots, y_n, x_1, \dots, x_m \in A$  such that  $y_1, \dots, y_n$  and  $x_1, \dots, x_m$  both generate  $A$ , and let  $n \leq m$ . Then there is a subsequence  $x_{i_1}, \dots, x_{i_n}$  generating  $A$ .

Using the Generators Theorem we can extend some properties about degree as in 3.5.2 to properties about dimension.

3.9.5. Theorem. (Dimension theorem). If  $A$  has a (finite) dimension then it is unique.

Proof: apply the Generators Theorem to two sequences of independent vectors, with  $C = \{0\}$ .

Given sequences  $y_1, \dots, y_n$  and  $x_1, \dots, x_m$  over  $A$  with  $n \leq m$ ; let  $y_1, \dots, y_n$  generate  $A$ . Does there exist a subsequence  $x_{i_1}, \dots, x_{i_n}$  equivalent to  $x_1, \dots, x_m$ ? The answer is yes if  $x_1, \dots, x_m$  generates  $A$  (3.9.4), but without that extra assumption it need not be true as the following model shows:  $\underline{F}$  is



$\underline{A}$  is  $\underline{F}$  itself.

$\underline{F}$  is an H-field as well as an AK-field and  $\underline{A}$  is a strong module with tight apartness and of degree 1.


Take  $y_1 := 1$  and  $x_1 := X, x_2 := Y$ .

Then  $x_1, x_2$  is not even weakly dependent:

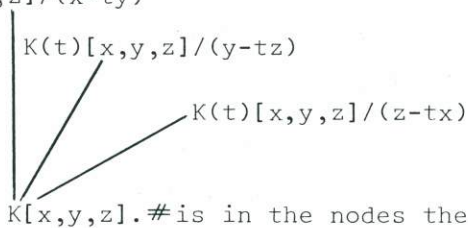
$$\underline{F} \neq \exists \alpha, \beta (\neg(\alpha \equiv 0 \wedge \beta \equiv 0) \wedge \alpha \dot{X} + \beta \dot{Y} \equiv 0).$$

3.10  $R^X$ 

Let  $A$  be a strong module,  $y_1, \dots, y_n$  free and let this sequence depend on  $x_1, \dots, x_m$ .  $n < m$ . The Austauschatz suggests that there is a free subsequence  $x_{i_1}, \dots, x_{i_n}$ . The Generators Theorem gives a condition (the existence of  $C$ ) for the validity of the above statement. In some modules we can construct a  $C$  for the Generators Theorem. But it is not true in general, as the following model shows.

3.10.1. Example.  $\underline{F}$  is:  $K(t) \quad K(t) \quad K(t)$   $K$  a field in classical  
 mathematics

and  $\underline{A}$  is:  $K(t)[x, y, z]/(x-ty)$



Take  $y_1, y_2 := x, y + z$ . Take  $x_1, x_2, x_3 := x, y, z$ . Then  $y_1, y_2$  is free and depends on  $x_1, x_2, x_3$ . But we cannot give the requested subsequence of  $x_1, x_2, x_3$ .

As we observed in 3.1.2  $R^X$  is a strong module over  $R$  for all objects  $X$  and with apartness

$$f \# g \leftrightarrow \exists \xi \in X. f(\xi) \wedge g(\xi) \wedge \xi \in X. f(\xi) \# g(\xi).$$

All submodules  $A$  with the induced apartness are strong over  $R$  too.

3.10.2. Lemma. Let  $y_1, \dots, y_n \in R^X$  be free. Then there exist  $\xi_1, \dots, \xi_n \in X$  and  $z_1, \dots, z_n \in R^X$  so that

1.  $y_1, \dots, y_n$  is equivalent to  $z_1, \dots, z_n$  and
2.  $z_i(\xi_j) \equiv \delta_{ij}$  for all  $i, j$ ,  $1 \leq i, j \leq n$ .

Proof: by induction on  $n$ .

$n = 1$ :  $y_1 \neq 0$ , so there is a  $\xi_1 \in X$  so that  $y_1(\xi_1) \neq 0$ .

Take  $z_1 \equiv y_1(\xi_1)^{-1} \cdot y_1$ .

Induction step: assume  $y_1, \dots, y_{n-1}$  equivalent to  $z_1, \dots, z_{n-1}$ .

Let  $y_n^* \equiv y_n - y_n(\xi_1) \cdot z_1 - \dots - y_n(\xi_{n-1}) \cdot z_{n-1}$ .

$y_1, \dots, y_n$  is free, thus  $y_n^* \neq 0$ . There is a  $\xi_n \in X$  so that  $y_n^*(\xi_n) \neq 0$ .

Take  $z_n \equiv y_n^*(\xi_n)^{-1} \cdot y_n^*$  and  $z_i' \equiv z_i - z_i(\xi_n) \cdot z_n$  for  $i < n$ .

3.10.3. Theorem. Let  $y_1, \dots, y_n \in A \subseteq R^X$  and let  $y_1, \dots, y_n$  be free. Let  $B \subseteq A$  be the subspace generated by  $y_1, \dots, y_n$ . Then there is a submodule  $C \subseteq A$  so that

$$A \equiv B \oplus C$$

Proof: by lemma 3.10.2 there are  $\xi_1, \dots, \xi_n \in X$  and  $z_1, \dots, z_n \in A$  satisfying the properties mentioned above. Let

$$C \equiv \{f \in A \mid f(\xi_i) \equiv 0 \text{ for } 1 \leq i \leq n\}.$$

Let  $a \in A$ . Then

$$a \equiv (a - a(\xi_1) \cdot z_1 - \dots - a(\xi_n) \cdot z_n) + (a(\xi_1) \cdot z_1 + \dots + a(\xi_n) \cdot z_n).$$

Thus  $a \in B + C$ .

$$A \equiv B + C.$$

On the other hand, let  $z \in B$  and  $c \in C$ . If  $z \neq 0$ , then  $z(\xi_i) \neq 0$  for some  $i$ , while  $c(\xi_i) \equiv 0$ . Thus  $z+c \neq 0$ . If  $c \neq 0$ , then  $z+c \neq 0$  or  $z \neq 0$ . Thus again  $z+c \neq 0$ . So  $A \equiv B \oplus C$ .

Application (see 3.10.1):

3.10.4. Proposition. Let  $A$  be a submodule of  $R^X$ . Let  $y_1, \dots, y_n$  and  $x_1, \dots, x_m$  be sequences of vectors such that  $y_1, \dots, y_n$  is free and depends on  $x_1, \dots, x_m$ . Then there is a subsequence  $x_{i_1}, \dots, x_{i_n}$  of free vectors.

Proof: immediate from 3.9.2 and 3.10.3.

Another application concerns the extension of free sequences.

3.10.5. Theorem. Let  $A$  be a submodule of  $R^X$ . Let  $y_1, \dots, y_n$  and  $x_1, \dots, x_m$  be two sequences of free vectors,  $n < m$ . Then there is a subsequence  $x_{i_1}, \dots, x_{i_{(m-n)}}$  such that  $y_1, \dots, y_n, x_{i_1}, \dots, x_{i_{(m-n)}}$  is free.

Proof: It suffices to prove the theorem for  $m \equiv n+1$ . Let  $B$  be the subspace generated by  $y_1, \dots, y_n$ . Then  $\text{deg}(B) \equiv n$  and by 3.10.3 there is a submodule  $C \subset A$  so that

$$A \equiv B \oplus C.$$

We can write for all  $i$ ,  $1 \leq i \leq m$ :

$$x_i \equiv \alpha_{1i}y_1 + \dots + \alpha_{ni}y_n + c_i.$$

Since  $x_1, \dots, x_m$  is free and the matrix

$$\begin{pmatrix} \alpha_{11} & \dots & \alpha_{1m} \\ \vdots & & \vdots \\ \alpha_{n1} & \dots & \alpha_{nm} \end{pmatrix}$$

can at most have rank  $n < m$ , we have:

$$c_i \neq 0 \text{ for some } i.$$

Thus  $y_1, \dots, y_n, x_i$  is free.

3.10.6. Corollary. Let  $M$  be a matrix with at least  $r$  columns free. Then every  $i \times i$ -invertible submatrix with  $i \leq r$  is extendable



to an  $r \times r$ -invertible submatrix.

A converse of the corollary is the theorem below, giving a bound on the size of invertible submatrices.

3.10.7. Theorem. Let  $M$  be a matrix with an  $r \times r$ -invertible submatrix. Let  $\det(N) = 0$  for each  $(r+1) \times (r+1)$ -submatrix  $N$ . Then  $M$  has rank  $r$ .

Proof: Using the existence of the  $r \times r$ -invertible submatrix and 3.6.2 we may assume  $M$  has the following form

$$\left( \begin{array}{cccccc} 1 & 0 & \dots & 0 & 0 & \dots & 0 \\ 0 & 1 & & & & & \\ \vdots & & & & & & \\ \vdots & & & & & & \\ \vdots & & & 1 & 0 & & \\ 0 & \dots & 0 & 1 & 0 & \dots & 0 \\ 0 & \dots & \dots & 0 & & & \\ \vdots & & & & & & \\ \vdots & & & & & & \\ \vdots & & & & & & \\ 0 & \dots & \dots & 0 & & & \end{array} \right) \left. \vphantom{\begin{array}{c} \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \\ \end{array}} \right\} r \text{ times}$$

C
---

Now we can prove that each coefficient occurring in  $C$  is 0. Let  $\alpha$  occur in  $C$ . Using 3.6.2 we may assume that  $\alpha$  is the top left most coefficient of  $C$ . Then the determinant of the top left most  $(r+1) \times (r+1)$  matrix is  $\alpha$  and is 0. Thus  $\alpha = 0$ .

This theorem is of extra interest for solving linear equations:

3.10.8. Corollary. Let  $M$  be an  $m \times n$ -matrix with rank  $r$  and let  $b \in \mathbb{R}^m$ . Let  $\det(N) = 0$  for each  $(r+1) \times (r+1)$ -submatrix  $N$  of the  $m \times (n+1)$ -matrix  $(M, b)$ . Then there is an  $x \in \mathbb{R}^n$  so that

$$Mx = b.$$

As opposed to 3.2.2 we have the following propositions:

3.10.9. Proposition. Let  $x_1, \dots, x_n \in A \subseteq R^X$ . Then we have:

" $x_1, \dots, x_n$  is free"  $\rightarrow$  " $x_1, \dots, x_n$  is independent".

Proof: There are  $\xi_1, \dots, \xi_n \in X$  as in 3.10.2 so that

$$\begin{pmatrix} x_1(\xi_1) & \dots & x_n(\xi_1) \\ \vdots & & \vdots \\ x_1(\xi_n) & \dots & x_n(\xi_n) \end{pmatrix}$$

is invertible. But that immediately implies that  $x_1, \dots, x_n$  is independent.

3.10.10. Proposition. Let  $R$  be a  $W$ -field. Let  $x_1, \dots, x_n \in A \subseteq R^X$ .

Then we have:

" $x_1, \dots, x_n$  is independent"  $\rightarrow \neg\neg$ " $x_1, \dots, x_n$  is free".

Proof: by 3.1.1 and 3.10.2 we can show, up to double negations, that there exist  $\xi_1, \dots, \xi_n \in X$  so that

$$\begin{pmatrix} x_1(\xi_1) & \dots & x_n(\xi_1) \\ \vdots & & \vdots \\ x_1(\xi_n) & \dots & x_n(\xi_n) \end{pmatrix}$$

has determinant  $\delta$ ,  $\neg\delta = 0$ . That means:  $\neg\neg\delta \neq 0$  over the  $W$ -field  $R$ . If  $\delta \neq 0$  then  $x_1, \dots, x_n$  is free. Thus we have derived:

$\neg\neg$  " $x_1, \dots, x_n$  is free".

Conclusion: The model of 3.5.2 is not a submodule of any  $R^X$ .

Let  $L$  be a module over  $R$ . Then  $M \equiv L^m$  also is a module over  $R$  and  $M$  is strong if  $L$  is.

3.10.11. Theorem. Let  $L$  be strong. Then the following are equivalent.

a.  $M \cong L^m$  has a degree.

b.  $\text{deg}(L)$  exists.

If a or b holds then  $m \cdot \text{deg}(L) \cong \text{deg}(M)$ .

Proof: write  $l^k$  for  $\langle 0, \dots, 0, 1, 0, \dots, 0 \rangle \in L^m$  with 1 on the  $k$ -th coordinate. Assume b. Let  $e_1, \dots, e_k$  be a basis for  $L$ . Then one easily verifies that the following sequence is a basis of  $M$ :

$$e_1^1, \dots, e_k^1, e_1^2, \dots, e_k^2, \dots, e_k^m.$$

This proves a. Assume a. Let  $z_1, \dots, z_n$  be a basis of  $M$ . We shall only prove:

If we have a sequence  $x_1, \dots, x_i$  free in  $L$  so that

$\text{im} < n$  then there is a vector  $x_{i+1} \in L$  free from  $x_1, \dots, x_i$ .

The rest of the proof is routine.

Proof of the claim: Given  $x_1, \dots, x_i$  as in the assumption, the sequence of all  $x_j^k$  is free in  $M$  and has length  $\text{im}$ . Using the Austauschsatz we may assume that in the basis  $z_1, \dots, z_n$  the first  $\text{im}$  vectors  $z_1, \dots, z_{\text{im}}$  are  $x_1^1, \dots, x_i^1, x_1^2, \dots, x_i^2, \dots, x_i^m$ . Each  $z_j$  can be written as

$$z_j \cong \langle a_{1j}, \dots, a_{mj} \rangle.$$

This gives an  $m \times n$ -matrix with  $L$ -elements on the coordinates:

$$\begin{pmatrix} x_1 & x_2 & \dots & x_i & 0 & \dots & \dots & 0 & a_{1,\text{im}+1} & \dots & a_{1,n} \\ 0 & \dots & \dots & 0 & x_1 \dots x_i & 0 & \dots & \vdots & \vdots & \dots & \vdots \\ \vdots & \dots & \dots & \dots & 0 & \dots & \dots & \vdots & \vdots & \dots & \vdots \\ \vdots & \dots & \dots & \dots & \dots & \dots & \dots & \vdots & \vdots & \dots & \vdots \\ 0 & \dots & \dots & \dots & 0 & \dots & 0 & \dots & 0 & a_{m,\text{im}+1} & \dots & a_{m,n} \\ & & & & & & x_1 & \dots & x_i & & & \end{pmatrix}$$

The columns of this matrix are free in  $L^m$ . Let  $c_j \cong a_{j,n}^j$  for  $j = 1, \dots, m$ . Then

$$z_n \equiv \langle a_{1,n}, \dots, a_{m,n} \rangle \equiv c_1 + \dots + c_m.$$

$z_1, \dots, z_n$  is a basis of  $M$  thus there are  $\beta_{j,k} \in K$  such that

$$\begin{aligned} c_1 &\equiv \beta_{1,1}z_1 + \dots + \beta_{n,1}z_n \\ &\vdots \\ c_m &\equiv \beta_{1,m}z_1 + \dots + \beta_{n,m}z_n. \end{aligned}$$

Addition of both sides of the equations gives  $z_n$  on the left hand side. The sequence  $z_1, \dots, z_n$  is free over  $K$ , thus

$$\begin{aligned} \beta_{n,1} + \dots + \beta_{n,m} &\neq 0. \\ \bigvee_{1 \leq j \leq m} \beta_{n,j} &\neq 0. \end{aligned}$$

Let us assume that  $\beta_{n,j} \neq 0$ . Then  $z_1, \dots, z_{n-1}, c_j$  is a basis of  $M$ . Take  $x_{i+1} \equiv a_{j,n}$ . We showed that  $x_1^j, \dots, x_i^j, a_{j,n}^j$  is free. Thus  $x_1, \dots, x_i, x_{i+1}$  is free.

## 4. GALOIS THEORY

In this section we consider extensions of H-fields, that means fields as defined in chapter 2. Thus by "field" we mean "H-field", i.e. a local ring with tight apartness. Many results of this chapter can be generalized from fields to local rings. Therefore we shall explicitly mention the cases where we essentially needed the tightness of the apartness relation.

### 4.1 Field extensions

4.1.1. Definition. Let  $K, L$  be fields such that  $K \subseteq L$ . Then  $(L/K)$  is the  $K$  vector space  $L$ .

$[L:K]_i$  is the dimension of  $(L/K)$ .

$[L:K]$  is the degree of  $(L/K)$ .

Given a tower of fields  $K \subseteq L \subseteq M$ , such that  $[M:L]_i$  and  $[L:K]_i$  exist. Then  $[M:K]_i$  exists and

$$[M:K]_i = [M:L]_i [L:K]_i.$$

The proof of this fact is the same as in the classical case: Take sequences  $x_1, \dots, x_m$  and  $y_1, \dots, y_n$  of independent generators of  $(L/K)$  and  $(M/L)$  respectively. The products  $x_i y_j$  form a sequence of independent generators of length  $mn$ . If we replace independence by freedom we get more.

4.1.2. Theorem. Let  $K \subseteq L \subseteq M$  be a tower of fields. If two of the three terms  $[M:K]$ ,  $[M:L]$  and  $[L:K]$  exist, then the third also exists, and

$$[M:K] = [M:L][L:K].$$

Proof: The main problem is the construction of a basis. There are three cases that we have to consider.

a. Assume that  $[M:L]$  and  $[L:K]$  exist. Then the same simple proof as in the independence case works.

b. Assume that  $[M:K]$  and  $[L:K]$  exist and let

$$[M:K] = n \text{ and } [L:K] = \ell.$$

Then we can prove:

If we have a sequence  $x_1, \dots, x_i \in M$  so that it is free in  $(M/L)$  and so that  $i\ell < n$ , then there is a vector

$x_{i+1} \in M$  so that  $x_1, \dots, x_i, x_{i+1}$  is free in  $(M/L)$ .

With that result the existence of  $[M:L]$  (and the proof of the equation above) follows simply by an induction argument.

Proof of the claim: Given  $x_1, \dots, x_i$  with  $i\ell < n$  and a basis  $y_1, \dots, y_\ell$  of  $(L/K)$ , the sequence of products  $x_j y_k$  is free in  $(M/K)$  and has length  $i\ell < n$ . Using the Austauschatz (3.3.2) we find a  $z$  in  $(M/K)$  free from them. Now take  $x_{i+1} = z$ .  $x_{i+1}$  is free from  $x_1, \dots, x_i$  in  $(M/L)$ , thus  $x_1, \dots, x_i, x_{i+1}$  is free.

c. Assume that  $[M:K]$  and  $[M:L]$  exist. Let  $[M:L] = m$ .

Then  $M \cong L^m$  as  $K$  vector spaces. Apply 3.10.11:  $\deg(L) = [L:K]$  exists and

$$[M:K] = [M:L] \cdot [L:K].$$

#### 4.2 The degree of a polynomial. Division algorithms

Let  $K$  be a field. One can make field extensions of  $K$  as follows. Take the polynomial ring  $K[X]$ .  $K[X]$  is an integral domain, so the quotient field exists. For the quotient field

of  $K[X]$  we write:  $K(X)$ . However, there is no finite degree or dimension for  $(K(X)/K)$ . Another construction uses minimal coideals  $C$  in  $K[X]$ . Then take the quotient structure  $K[X]/(\cap C)$ . Later on we shall discuss in more detail how to get minimal coideals. Some extensions are related with roots of polynomials. First some definitions.

4.2.1. Definition. Let  $R$  be a ring and  $f \in R[X]$ ,  $f \equiv a_0 + \dots + a_n X^n$ , then we say  $f$  has degree at most  $n$ . If for some  $r$   $a_r \neq 0$ , we say  $f$  has degree at least  $r'$  for  $r' \leq r$ .  $f$  is regular if there is an  $m$  such that  $f$  has degree  $m$ ; i.e. degree at most  $m$  and degree at least  $m$ . If the degree exists, it is unique and we write  $\deg(f) \equiv m$ .

From these definitions and the results in chapter 2 one easily deduces

4.2.2. Proposition. Let  $R$  be an integral domain and  $f, g, h \in R[X]$  such that  $f \equiv gh$ . Then the following are equivalent:

- a.  $g$  and  $h$  are regular.
- b.  $f$  is regular.

Moreover, if  $f$  is regular, then

$$\deg(f) \equiv \deg(g) + \deg(h).$$

Proof: for the implication  $\underline{b} \rightarrow \underline{a}$  we use the fact that the apartness is tight.

Now we shall consider the division algorithm.

4.2.3. Proposition. Let  $R$  be a ring and  $f, g \in R[X]$ .

$$f \equiv a_0 + \dots + a_n X^n$$

$$g \equiv b_0 + \dots + b_m X^m \text{ with } n \geq m.$$

Then there are  $q, r \in R[X]$  with  $r$  degree at most  $(m-1)$  such that

$$b_m^{n-m+1} f \equiv qg + r.$$

Proof: as in the classical case by induction on  $(n-m)$ .

Sketch of the induction step: Given  $f, g$  as above, let  $f^* \equiv b_m f - a_n X^{n-m} g$ . Then  $f^*$  has degree at most  $(n-1)$  and we apply induction:

$$b_m^{n-m} f^* \equiv qg + r \text{ for some } q \text{ and } r \text{ satisfying the conditions.}$$

$$\text{Thus } b_m^{n-m+1} f \equiv (q + b_m^{n-m} a_n X^{n-m})g + r.$$

For the extra conditions necessary for the uniqueness of  $q$  and  $r$  we need new notions.

4.2.4. Definition. Let  $R$  be a ring,  $b \in R$ .

$b$  is weakly zero divisor free if

$$\forall x \in R (xb \equiv 0 \rightarrow x \equiv 0).$$

$b$  is strongly zero divisor free if

$$\forall x \in R (x \neq 0 \rightarrow xb \neq 0).$$

Now we can strengthen proposition 4.2.3:

4.2.5. Proposition. If moreover  $b_m$  in 4.2.3 is weakly zero divisor free then  $q$  and  $r$  are unique. Thus if in that proposition  $R$  is an integral domain and  $\neg b_m \equiv 0$ , then  $q$  and  $r$  are unique.

This extra proposition requires the apartness to be tight.

If  $b_m$  is invertible we can eliminate the power  $b_m^{n-m+1}$ , in particular:

4.2.6. Corollary. If in the proposition  $R$  is a field and  $b_m \neq 0$ , then there are unique  $q, r \in R[X]$  with  $r$  degree at most



(m-1), such that  $f \equiv qg + r$ .

### 4.3 Coideals of polynomials and power series

Now we shall construct from a power series  $f \in K[[X]]$  a coideal in  $K[X]$ . In classical mathematics for power series that are not polynomials the following holds:  $K[X]/(f) \cong K[X]$ . This fact yields no useful information. But in intuitionistic mathematics polynomials are closer to power series. For instance, consider a power series  $f \equiv f_0 + f_1X + \dots$  satisfying  $\neg \exists n \forall m > n \ f_m \equiv 0$ . See also 4.4.11.

4.3.1. Definition. Let  $K$  be a field and let  $f \in K[[X]]$ . Then

$$C_f \equiv \{g \in K[X] \mid \forall h \in K[X]. g \equiv hf\}.$$

When is  $C_f$  a coideal? Certainly if  $f \equiv 0$ . This is a trivial case. For the case  $f \neq 0$  we need some lemmas.

4.3.2. Lemma. Let  $f \equiv f_0 + f_1X + f_2X^2 + \dots$ ,  $f \in K[[X]]$ , so that  $f_r \neq 0$ . Let  $M$  be the following  $(r+n) \times n$ -matrix:

$$M \equiv \begin{pmatrix} f_0 & 0 & \dots & 0 \\ f_1 & f_0 & \dots & \vdots \\ \vdots & \vdots & \ddots & \vdots \\ \vdots & \vdots & \vdots & 0 \\ f_r & \vdots & \vdots & f_0 \\ \vdots & \vdots & \vdots & \vdots \\ \vdots & \vdots & \vdots & \vdots \\ f_{r+n-1} & \dots & \dots & f_r \end{pmatrix}$$

Then there is an  $s \leq r$  and an  $n \times n$ -submatrix  $B$  of  $M$  of the form

$$B \equiv \begin{pmatrix} f_s & \dots & \dots \\ \vdots & \ddots & \vdots \\ \vdots & \vdots & f_s \end{pmatrix}$$

so that  $B$  is invertible and  $f_s \neq 0$ .

Proof: by induction on  $r$ .  $r=0$  is trivial.

Induction step: let  $f_r \neq 0$ . Let  $C$  be the submatrix with the  $f_r$  on the diagonal.

$$f_r^n \neq 0, \text{ thus}$$

$$f_r^n \neq \det C \vee \det C \neq 0.$$

If  $\det C \neq 0$  then we take  $B \equiv C$ . The case  $f_r^n \neq \det C$ . Writing  $\det C$  as the sum of  $n!$  products we get

$$\bigwedge_{t < r} f_t \neq 0.$$

Then apply induction.

4.3.3. Lemma. Let  $f \equiv f_0 + \dots + f_m X^m \in K[X]$  so that  $f_r \neq 0$ . Let  $M$  be the following  $(m+n) \times n$ -matrix:

$$M \equiv \begin{pmatrix} f_0 & 0 & \dots & 0 \\ f_1 & f_0 & \dots & \vdots \\ \vdots & \vdots & \ddots & 0 \\ f_m & \dots & \dots & f_0 \\ 0 & \dots & \dots & \vdots \\ \vdots & \dots & \dots & \vdots \\ 0 & \dots & 0 & f_m \end{pmatrix}$$

Then there is an  $s \geq r$  and an  $n \times n$ -submatrix  $B$  of  $M$  of the form

$$B \equiv \begin{pmatrix} f_s & \dots & \dots \\ \vdots & \ddots & \vdots \\ \vdots & \dots & f_s \end{pmatrix}$$

so that  $B$  is invertible and  $f_s \neq 0$ .

Proof: by induction on  $(m-r)$ , analogous to the proof of 4.3.2.

4.3.4. Lemma. Let  $P_n \equiv \{g \in K[X] \mid g \text{ has degree at most } n\}$ . Let

$g \in P_n$ . Then we have for all  $f \in K[[X]]$ :

$$g \in C_f \leftrightarrow \forall h \in P_n. g \neq hf.$$

Proof: From left to right is trivial. From right to left:

let  $h \in K[X]$ . To prove:  $g \neq hf$ .

Split  $h \equiv h_{<} + h_{>}$  where  $h_{<} \equiv h_0 + \dots + h_n X^n$  and  $h_{>} \equiv h_{n+1} X^{n+1} + \dots + h_m X^m$ .

Then  $g \neq h_{<} f$ , thus  $g \neq hf \vee hf \neq h_{<} f$ . Assume  $hf \neq h_{<} f$ . Then

$h_{>} f \neq 0$ . Then  $hf$  has degree at least  $n+1$ . Thus  $g \neq hf$ .

4.3.5. Remark. One easily shows that for  $f, g$  and  $P_n$  as above we have

$$\exists h \in K[X]. g \equiv hf \leftrightarrow \exists h \in P_n. g \equiv hf.$$

Take the proof of 4.3.4 and use that the apartness is tight.

4.3.6. Lemma. Let  $P_n$  be as above,  $f \in K[[X]]$ ,  $f \neq 0$ . Then there is a  $K$  linear mapping  $(\cdot)_f^*: P_n \rightarrow P_n$  so that for all  $g \in P_n$

$$a. g \in C_f \leftrightarrow g \neq g_f^* f$$

and b.  $\exists h \in K[X]. g \equiv hf \leftrightarrow g \equiv g_f^* f$ .

Proof: a.  $f \neq 0$  thus for some  $r$  we have:  $f_r \neq 0$ . Then there is an  $s \leq r$  and an  $(n+1) \times (n+1)$  matrix  $B$  as in lemma 4.3.2,

$$B \equiv \begin{pmatrix} f_s & \dots & \dots & \dots \\ \vdots & \ddots & \ddots & \vdots \\ \vdots & \dots & f_s & \dots \\ \vdots & \dots & \dots & f_s \end{pmatrix}$$

so that  $B$  is invertible. (If  $f$  is a polynomial we can get

an  $s$  so that  $s \geq r$  by 4.3.3). If we write polynomials

$h \equiv x_0 + \dots + x_n X^n \in P_n$  as vectors  $(x_0, \dots, x_n) \in K^{n+1}$  then we

define:

$$h_f^* \equiv B^{-1} \begin{pmatrix} x_s \\ x_{s+1} \\ \vdots \\ x_{s+n} \end{pmatrix} \quad \text{where } x_m \equiv 0 \text{ if } m > n.$$

To keep the notation easy we shall write  $h^*$  instead of  $h_f^*$ . Let  $k \equiv h - h^*f \equiv k_0 + k_1X + k_2X^2 + \dots$ . Then it easily follows from the definition above that

$$k_s \equiv k_{s+1} \equiv \dots \equiv k_{s+n} \equiv 0.$$

Now consider  $g \in P_n$ . If  $g \in C_f$  then we immediately can conclude that  $g \# g^*f$ . So assume  $g \# g^*f$  and let  $h \in P_n$ . To prove:  $g \# hf$ . Then we are done by 4.3.4. We have:  $g \# hf \vee hf \# g^*f$ . Assume  $hf \# g^*f$ . Then  $h \# g^*$  and

$$Bh \# Bg^*$$

Let  $l \equiv X^s \cdot Bh$  (we use the identification of  $P_n$  and  $K^{n+1}$ ). Then for some  $t$ ,  $s \leq t \leq s+n$ , we have:  $l_t \# g_t$  while  $l^* \equiv h$ . Thus  $g \# l^*f \equiv hf$ . This proves a. b. follows from a by using the tightness of the apartness relation.

4.3.7. Theorem. Let  $f \in K[[X]]$ ,  $f \# 0$ , then  $C_f$  is a coideal.

Proof: We check the axioms of chapter 2.

$$\neg 0 \in C_f \text{ is trivial: take } h \equiv 0.$$

Let  $g_1g_2 \in C_f$ . To prove:  $g_1 \in C_f$ . Let  $h \in K[X]$ , then

$$g_1g_2 \# hg_2f. \text{ Thus } g_1 \# hf.$$

Finally let  $g_1 + g_2 \in C_f$ . There is an  $n$  so that  $g_1, g_2 \in P_n$ . Let  $(\cdot)^*$  be the linear mapping of 4.3.6 for this  $P_n$ . Then

$$\begin{aligned}
 g_1 + g_2 &\neq (g_1 + g_2)^*f. \\
 g_1 - g_1^*f + g_2 - g_2^*f &\neq 0. \\
 g_1 &\neq g_1^*f \vee g_2 \neq g_2^*f. \\
 g_1 &\in C_f \vee g_2 \in C_f.
 \end{aligned}$$

In 4.3.6 and 4.3.7 we essentially use that  $x \neq 0$  implies  $Ex^{-1}$ .

This is necessary, as the following model shows:

$\underline{R}$  is:

$$\begin{array}{ccc}
 \underline{\mathbb{Z}}_2 & & \underline{\mathbb{Z}}_3 \\
 & \searrow & / \\
 & \underline{\mathbb{Z}} &
 \end{array}$$

where  $\underline{\mathbb{Z}}_n = S^{-1}\mathbb{Z}$  with  $S = \{1, n, n^2, \dots\}$ .

$\neq$  is in the nodes the inequality.

Let  $f = 6X$ . Then  $\underline{R} \models 5X \in C_f$ . But  $\underline{R} \not\models 2X \in C_f \vee 3X \in C_f$ .

In this model  $\underline{R}$  is an integral domain satisfying  $\forall x(x \neq 0 \vee x = 0)$ .

4.3.8. Remarks. a. We can write  $K[\alpha]$  for  $K[X]/(\neg C_f)$  where  $\alpha \equiv \varphi(X)$ ,  $\varphi$  the canonical morphism

$$\varphi: K[X] \rightarrow K[X]/(\neg C_f).$$

If  $f$  is a polynomial then  $f(\alpha) \equiv 0$ .  $K[\alpha]$  is a vector space over  $K$ . If  $f$  is regular with  $\deg(f) \equiv n$ , then  $(K[\alpha]/K)$  has degree  $n$ . The sequence  $1, \alpha, \dots, \alpha^{n-1}$  forms a basis.

b. There also is a construction of  $K[\alpha]$  for local rings  $K$ . The only difference is that we have to define the equality by an ideal:  $K[\alpha] \equiv K[X]/(f)$ , where

$$(f) \equiv \{g \in K[X] \mid \exists h \in K[X]. g \equiv hf\}.$$

If the apartness is tight then  $(f) = \neg C_f$  (4.3.6).

c. Let  $r \in K[X]$ . If  $\deg(f)$  exists and  $r$  has degree at most  $\deg(f)-1$  then

$$r \neq 0 \leftrightarrow r(\alpha) \neq 0$$

However, in intuitionistic algebra  $\deg(f)$  need not exist.

Therefore we have a more elaborate statement: if  
 $\forall i \in \mathbb{N}. (r_i \neq 0 \rightarrow \exists j > i. f_j \neq 0)$  then

$$r \neq 0 \leftrightarrow r(\alpha) \neq 0.$$

Proof:  $r(\alpha) \neq 0$  immediately implies that  $r \neq 0$ . So assume  $r \neq 0$ .  
 Then  $r_i \neq 0$  for some  $i$  and  $r \in P_n$  for some  $n$ . We complete  
 the proof by induction on  $n-i$ . The case  $n-i \equiv 0$  is easy because  
 $f_j \neq 0$  for some  $j > n$ .

Induction step:  $r \neq 0$ . Let  $(\cdot)^*$  be the linear map of 4.3.6  
 for  $P_n$ . Then

$$r \neq r^*f \vee r^*f \neq 0.$$

If  $r \neq r^*f$  then  $r \in C_f$  and  $r(\alpha) \neq 0$ . Assume  $r^*f \neq 0$ .  $f_j \neq 0$  for  
 some  $j > i$  thus  $r \neq r^*f$  or  $r$  has degree at least  $j$ . If  $r \neq r^*f$   
 we are done and if  $r$  has degree at least  $j$  we can apply induction.

d. Let  $g \in P_n$  and let  $(\cdot)^*$  be the map of 4.3.6 for  $P_n$ . Then  
 we can write

$$k \equiv g - g^*f \equiv (k_0 + \dots + k_{s-1}X^{s-1}) + (k_{s+n+1}X^{s+n+1} + k_{s+n+2}X^{s+n+2} + \dots)$$

Let  $k = l+h$  where  $l \equiv k_0 + \dots + k_{s-1}X^{s-1}$ . If  $h \neq 0$  then there  
 is an  $s' > s$  so that  $f_{s'} \neq 0$ , because  $g$  has degree at most  $n$ .  
 If  $l \neq 0$  then even  $l(\alpha) \neq 0$  as follows from 4.3.8c. Remark  
 4.3.8d plays a role in some induction proofs.

#### 4.4 Relative primality

We first consider relatively prime pairs of polynomials before  
 we consider prime polynomials. This looks somewhat unnatural,  
 but there are economical reasons for it. In particular we can  
 avoid repetition of similar proofs.

4.4.1. There are several ways to define relative primality. Let  $f, g \in K[[X]]$ . Let  $\varphi$  be a formula in which  $h, k$  and  $l$  do not occur free. We shall consider the following notions of relative primality modulo  $\varphi$ :

- (a)  $(g \neq 0 \wedge \forall h, k \in K[X]. (h \in C_g \rightarrow hf + kg \neq 0 \vee \varphi)) \vee$   
 $\vee (f \neq 0 \wedge \forall h, k \in K[X]. (k \in C_f \rightarrow hf + kg \neq 0 \vee \varphi)),$
- (b)  $(f \neq 0 \vee g \neq 0) \wedge \forall h, k \in K[X]. (h \in C_g \vee k \in C_f \rightarrow hf + kg \neq 0 \vee \varphi),$
- (c)  $\forall h \in K[[X]]. (h \neq h(0) \rightarrow f \in C_h \vee g \in C_h \vee \varphi),$
- (d)  $\forall h \in K[[X]] \forall k, l \in K[X]. (h \neq h(0) \rightarrow hk \neq f \vee hl \neq g \vee \varphi).$

4.4.2. Remark. We want to prove that under special circumstances (a), (b), (c) and (d) are equivalent. Our main interest concerns the case when  $\varphi$  is false. Then we can delete  $\varphi$ . However, the more general notions of 4.4.1 are needed for the proof of 4.4.7.

4.4.3. Lemma. Let  $k \in K[X]$  and let  $f, g, h \in K[[X]]$  be so that  $f \neq 0$ ,  $g \neq 0$  and  $h \neq h(0)$ .

- Then: (1)  $f \neq hk \vee k \in C_f,$   
 (2)  $k \in C_f \rightarrow f \neq f(0),$   
 (3)  $k \in C_f \rightarrow k \in C_g \vee f \neq g.$

Proof: (1). From  $f \neq 0$  it follows that  $f \neq hk \vee hk \neq 0$ . Assume  $hk \neq 0$ . Then  $k \neq 0$ . If  $k_i \neq 0$  for some  $i$  then  $hk$  has degree at least  $i+1$ . Thus  $f \neq hk \vee \exists j > i. f_j \neq 0$ . Since  $k$  has degree at most  $n$  for some  $n$  we find

$$f \neq hk \vee \forall i \in \mathbb{N}. (k_i \neq 0 \rightarrow \exists j > i. f_j \neq 0)$$

$k \neq 0$  thus by 4.3.8c  $f \neq hk \vee k \in C_f$ .

Concerning (2):  $f \neq f(0) \vee f(0) \neq 0$ . Therefore we may assume  $f(0) \neq 0$ . From  $k \in C_f$  now follows that  $k \neq kf(0)^{-1}f$ . Thus  $f \neq f(0)$ .

(3). Assume  $k \in C_f$ . By induction on  $r \equiv r_1 + r_2$  we shall prove: if  $f_{r_1} \neq 0$  and  $g_{r_2} \neq 0$  then  $k \in C_g \vee f \neq g$ . The case for  $r \equiv 0$  is contained in the induction step.

Induction step: there is an  $n$  so that  $k \in P_n$ . Let  $(\cdot)_f^*$  and  $(\cdot)_g^*$  be maps for  $P_n$  according to 4.3.6. Then  $k \neq k_f^* f$ . Thus  $k \neq k_g^* g \vee k_g^* g \neq k_f^* f$ , hence  $k \in C_g \vee g \neq f \vee k_g^* \neq k_f^*$ . We may assume  $k_g^* \neq k_f^*$ . Then we easily find that

$$g \neq f \vee \exists s_1 < r_1 \cdot f_{s_1} \neq 0 \vee \exists s_2 < r_2 \cdot g_{s_2} \neq 0.$$

Applying induction we get  $k \in C_g \vee g \neq f$ .

4.4.4. Proposition. The statements 4.4.1(a) and 4.4.1(b) are equivalent.

Proof: one easily proves that (b) implies (a).

Assume (a). Let  $g \neq 0$  and  $\forall h, k \in K[X] \cdot (h \in C_g \rightarrow hf + kg \neq 0 \vee \varphi)$ .

Let  $h, k \in K[X]$  be so that  $k \in C_f$ . It is sufficient to show that  $hf + kg \neq 0 \vee \varphi$  for these assumptions.  $h \in P_n$  for some  $n$ .

Let  $(\cdot)_g^*$  be a map for  $P_n$  according to 4.3.6. Then

$$hf + kg \equiv ((h)_g^* g + d)f + kg \equiv ((h)_g^* f + k)g + df \text{ with } d \equiv h - (h)_g^* g.$$

Since  $g \neq 0$  and  $k \in C_f$  we have that  $((h)_g^* f + k)g \neq 0$ . Thus

$$hf + kg \neq 0 \vee df \neq 0.$$

Assume  $df \neq 0$ . Then  $d \neq 0$  and  $h \in C_g$ . Apply the assumption:

$$hf + kg \neq 0 \vee \varphi.$$

4.4.5. Lemma. Let (b), (c) and (d) be the statements of 4.4.1.

Then (b)  $\Rightarrow$  (d) and (c)  $\Rightarrow$  (d) holds.

Proof: (c) trivially implies (d).

Assume (b). Let  $k, l \in K[X]$  and let  $h \in K[[X]]$  so that  $h \neq h(0)$ .

We have  $f \neq 0 \vee g \neq 0$  so by 4.4.3 we get



$$f \neq hk \vee k \in C_f \vee g \neq hl \vee l \in C_g.$$

Assumption (b) implies  $f \neq hk \vee g \neq hl \vee lf - kg \neq 0 \vee \varphi$ . Assume  $lf \neq kg$ . Then  $lf \neq lhk \vee lhk \neq kg$ . Thus  $f \neq hk \vee g \neq hl$ .

4.4.6. Proposition. Let  $f, g, r \in K[[X]]$ ,  $q \in K[X]$  and  $f \equiv qg + r$ .

Then we have:

- (1) If  $f, g$  satisfies condition 4.4.1(d) then the same holds for  $g, r$ .
- (2) If  $f, g$  satisfies condition 4.4.1(a) or condition 4.4.1(b) then the same holds for  $g, r$ .

Proof: (1) is easy.

(2): let  $f, g, q, r$  be as above and let  $f, g$  satisfy condition 4.4.1(a). To show:  $g, r$  satisfies 4.4.1(a) (or 4.4.1(b) by proposition 4.4.4). If  $g \neq 0$  then the proof is easy. So assume  $f \neq 0$ . Then  $g \neq 0 \vee r \neq 0$ . We may assume  $r \neq 0$ . Let  $h, k \in K[X]$  so that  $k \in C_r$ . By 4.4.3 this implies  $k \in C_f \vee f \neq r$ . To show:  $hr + kg \neq 0 \vee \varphi$ . If  $f \neq r$  then  $g \neq 0$  and we are done because of the remark above. If  $k \in C_f$  then  $hf + kg \neq 0 \vee \varphi$ . Thus  $hr + kg \neq 0 \vee \varphi \vee hqg \neq 0$ , where  $hqg \neq 0$  again implies  $g \neq 0$ .

4.4.7. Lemma. Let  $f, g \in K[X]$  satisfy 4.4.1(d). Then  $f, g$  satisfies 4.4.1(a).

Proof: by induction on  $m_1 \equiv n_1 + n_2$  we shall show: for all  $f, g, \varphi$  if  $f, g$  satisfies 4.4.1(d) modulo  $\varphi$  and if  $f$  has degree at most  $n_1$  and  $g$  has degree at most  $n_2$  then  $f, g$  satisfies 4.4.1(a) modulo  $\varphi$ . The case  $m_1 = 1$  is trivial since  $f \neq 0 \vee g \neq 0 \vee \varphi$  holds (take  $k \equiv l \equiv 0$  in 4.4.1(d)).

Induction step: let  $f, g$  be given, satisfying the conditions for the induction step.  $f \neq 0 \vee g \neq 0 \vee \varphi$  holds,

thus we may assume:  $g \neq 0$ . Let  $h, k \in K[X]$  so that  $h \in C_g$ . To prove:  $hf + kg \neq 0 \vee \varphi$ . By 4.4.3 we have that  $g \neq g(0)$ . Then the assumption 4.4.1(d) implies  $f \in C_g \vee \varphi$ . We may assume that  $f \in C_g$  holds. There are  $s_1, s_2$  so that  $f_{s_1} \neq 0$  and  $g_{s_2} \neq 0$ . We complete the proof of the induction step by induction on  $m_2 = n_1 + n_2 - s_1 - s_2$ . The case for  $m_2 = 0$  is contained in the induction step for  $m_2$ . Induction step for  $m_2$ : let  $\underline{f} = f_0 + \dots + f_{s_1} X^{s_1}$  and  $\underline{g} = g_0 + \dots + g_{s_2} X^{s_2}$ . We may assume that  $s_1 \geq s_2$ . There are  $q, r \in K[X]$  so that  $\underline{f} = q\underline{g} + r$  and  $r$  has degree at most  $s_2 - 1$ . One easily verifies that for all  $\underline{h} \in K[[X]]$  and  $\underline{k}, \underline{l} \in K[X]$  so that  $\underline{h} \neq \underline{h}(0)$  we have

$$\underline{h}\underline{k} \neq \underline{r} \vee \underline{h}\underline{l} \neq \underline{g} \vee \underline{f} \neq \underline{f} \vee \underline{g} \neq \underline{g} \vee \varphi.$$

Let  $\psi$  be the formula  $\underline{f} \neq \underline{f} \vee \underline{g} \neq \underline{g} \vee \varphi$ . Then  $r, \underline{g}$  satisfies 4.4.1(d) modulo  $\psi$ . By the induction hypothesis on  $m_1$   $r, \underline{g}$  satisfies 4.4.1(a) modulo  $\psi$ . By 4.4.6  $\underline{f}, \underline{g}$  satisfies 4.4.1(a) modulo  $\psi$ . Thus since  $h \in C_g$  implies  $h \in C_{\underline{g}} \vee \underline{g} \neq \underline{g}$  we get

$$hf + kg \neq 0 \vee \underline{f} \neq \underline{f} \vee \underline{g} \neq \underline{g} \vee \varphi, \text{ i.e.}$$

$$hf + kg \neq 0 \vee \varphi \vee \underline{f} \neq \underline{f} \vee \underline{g} \neq \underline{g}.$$

And if  $\underline{f} \neq \underline{f} \vee \underline{g} \neq \underline{g}$  holds we apply the induction hypothesis on  $m_2$ .

As a corollary we get:

4.4.8. Theorem. Let  $f, g \in K[X]$ . Then the statements 4.4.1(a), (b), (c) and (d) are equivalent.

Proof: for polynomials  $f$  and  $g$  one easily shows that 4.4.1(d) implies 4.4.1(c) by using 4.3.6. The other implications between the statements follow from 4.4.4, 4.4.5 and 4.4.7.

4.4.9. Definition. Let  $f, g \in K[X]$ .  $f$  and  $g$  are called relatively prime if they satisfy one of the statements in 4.4.1 with  $\varphi$

is false.

Let  $f, g \in K[X]$ ,  $f \neq 0$ ,  $K[\alpha] \equiv K[X]/(\neg C_f)$ . Then  $f$  and  $g$  are relatively prime if and only if for all  $h(\alpha) \in K[\alpha]$   $h(\alpha) \neq 0$  implies  $g(\alpha)h(\alpha) \neq 0$ .

In other words:  $f$  and  $g$  are relatively prime if and only if  $g(\alpha)$  is strongly zero divisor free in  $K[\alpha]$  (cf. 4.2.4).

Now it is easy to show:

4.4.10. Proposition. Let  $f, g_1, g_2 \in K[X]$  so that the pairs  $f, g_1$  and  $f, g_2$  are both relatively prime. Then  $f$  and  $g_1 g_2$  are relatively prime.

Proof: we have  $f \neq 0 \vee (g_1 \neq 0 \wedge g_2 \neq 0)$ . Assume  $f \neq 0$ . Then  $g_1(\alpha)$  and  $g_2(\alpha)$  are strongly zero divisor free in  $K[\alpha] \equiv K[X]/(\neg C_f)$ . But then the same holds for  $g_1(\alpha)g_2(\alpha)$ . Thus  $f$  and  $g_1 g_2$  are relatively prime. Assume  $g_1 \neq 0$  and  $g_2 \neq 0$ . Thus  $(g_1 \neq g_1(0) \vee g_2 \neq g_2(0)) \vee (g_1(0) \neq 0 \wedge g_2(0) \neq 0)$ . If  $g_1 \neq g_1(0)$  or  $g_2 \neq g_2(0)$  then  $f \neq 0$  and we are done. Thus assume that  $g_1(0) \neq 0$  and  $g_2(0) \neq 0$ .

Let  $h, k \in K[X]$  so that  $h \in C_{g_1 g_2}$ . To prove:  $hf + kg_1 g_2 \neq 0$ . Since  $h \in C_{g_2(0)g_1} \vee h \in C_{g_1}$  we have that  $h \in C_{g_1} \vee g_2 \neq g_2(0)$ . If  $g_2 \neq g_2(0)$  then  $f \neq 0$  and we are done. Assume  $h \in C_{g_1}$ . Then  $hf + kg_1 g_2(0) \neq 0$ . Thus  $hf + kg_1 g_2 \neq 0 \vee g_2 \neq g_2(0)$ .

4.4.11. Remark. The theory as presented here makes it possible to generalize results over relative primality for polynomials to result over other kinds of power series. We especially think of power series which strongly resemble polynomials. Our main interest in this chapter concerns polynomials. Therefore we shall restrict ourselves to one example;  
A power series  $f$  is called a pseudo polynomial if it satisfies

$\exists m \in \mathbb{N}. ((\exists i > m. f_i \neq 0) \rightarrow f \in K[X]).$

A pseudo polynomial need not be a polynomial. It is easy to show that for pseudo polynomials lemma 4.3.2 holds with  $s \geq r$  by a method as used for 4.3.3. 4.4.7 also holds for pseudo polynomials, this follows after modifying the proofs of 4.4.5 and 4.4.7. Then we have shown:

For pseudo polynomials  $f$  and  $g$  the statements 4.4.1(a), (b) and (d) are equivalent. The study of power series seems rather promising for future research.

#### 4.5 Primality and minimality

Let  $f \in K[X]$ ,  $f \neq 0$ . Then  $C_f$  is a coideal in  $K[X]$ . We shall give conditions for  $f$  so that  $C_f$  is prime or minimal (cf. chapter 2).

4.5.1. Definition. Let  $f \in K[X]$ . Then  $f$  is prime if  $f \neq f(0)$  and for all  $g, h \in K[X]$  with  $g \neq g(0)$  and  $h \neq h(0)$  we have  $f \neq gh$ .

4.5.2. Lemma. Let  $f \in K[X]$ ,  $f \neq 0$ . Then the following are equivalent:

- (a)  $f$  is prime
- (b)  $f \neq f(0)$  and for all  $g \in C_f$   $f$  and  $g$  are relatively prime.

Proof: Assume (a). Let  $g \in C_f$  and  $h, k, l \in K[X]$  so that  $h \neq h(0)$ .

To prove:  $hk \neq f \vee hl \neq g$  (the generalization to power series  $h$  is trivial). Since  $f \neq 0$  we have  $f \neq hk \vee hk \neq 0$ . So we may assume:  $hk \neq 0$ . Then  $k \neq k(0) \vee k(0) \neq 0$ . If  $k \neq k(0)$  then  $f \neq hk$  because  $f$  is prime. Assume  $k(0) \neq 0$ . Let  $K[\alpha] \equiv K[X]/(\neg C_f)$ .  $g \in C_f$  implies  $g(\alpha) \neq 0$ . Thus

$$g(\alpha) \neq h(\alpha)l(\alpha) \vee h(\alpha)l(\alpha) \neq 0.$$

If  $g(\alpha) \neq h(\alpha)l(\alpha)$  then  $g \neq hl$ .

Assume  $h(\alpha)k(\alpha) \neq 0$ . Then  $h(\alpha) \neq 0$ , thus  $h(\alpha)k(0) \neq 0$  because  $f \neq f(0)$  in  $K[X]$ . Then is  $h(\alpha)k(\alpha) \neq 0 \vee h(\alpha)(k(\alpha) - (k(0))) \neq 0$ . If  $h(\alpha)k(\alpha) \neq 0$  then  $hk \neq f$ .

Assume  $h(\alpha)(k(\alpha) - k(0)) \neq 0$ . Then  $k \neq k(0)$  in  $K[X]$  thus  $hk \neq f$  because  $f$  is prime. This proves (b).

Assume (b). Let  $g, h \in K[X]$  so that  $g \neq g(0)$  and  $h \neq h(0)$ . By 4.4.3 this implies

$$f \neq gh \vee g \in C_f.$$

Assume  $g \in C_f$ . Then  $f$  and  $g$  are relatively prime, thus  $f \neq gh \vee g \neq g \cdot 1$ . Thus  $f \neq gh$ . Thus  $f$  is prime.

As in traditional mathematics we can prove ([He 2]):

4.5.3. Theorem. Let  $f \in K[X]$ ,  $f \neq 0$ ,  $K[\alpha] \equiv K[X]/(\neg C_f)$ . Then the following are equivalent:

- (a)  $f$  is prime
- (b)  $K[\alpha]$  is an integral domain.

Proof: Assume (a). Then  $1 \neq 0$  in  $K[\alpha]$  because  $f \neq f(0)$  in  $K[X]$ .

Let  $g_1(\alpha), g_2(\alpha) \in K[\alpha]$  so that  $g_1(\alpha) \neq 0$  and  $g_2(\alpha) \neq 0$ .

Then by 4.5.2 the pair  $f, g_1$  is relatively prime. Thus  $g_1(\alpha)$  is strongly zero divisor free and  $g_1(\alpha)g_2(\alpha) \neq 0$ . Thus  $K[\alpha]$  is an integral domain.

Assume (b).  $1 \neq 0$  in  $K[\alpha]$  thus  $f \neq f(0)$  in  $K[X]$  by 4.4.3.

Let  $g \in C_f$ . Then  $g(\alpha) \neq 0$ . Since  $K[\alpha]$  is an integral domain  $g(\alpha)$  is strongly zero divisor free. Thus  $f$  and  $g$  are relatively prime. Now use 4.5.2.

In classical mathematics we have that if  $f$  is prime then  $K[\alpha]$  is a field. But in intuitionistic mathematics this matter is more complicated. A special case can be derived from the theorem below.

4.5.4. Theorem. Let  $f, g \in K[X]$  be relatively prime and let  $\deg(f)$  exist,  $\deg(f) = n$ . Then there are unique  $h, k \in K[X]$  so that  $k$  has degree at most  $n-1$  and so that

$$hf + kg = 1.$$

Proof: the case  $f = f(0)$  is trivial. Assume that  $\deg(f) > 0$ . Let  $x = x_0 + \dots + x_{n-1}X^{n-1}$  with  $x_0, \dots, x_{n-1}$  variables over  $K$ . Compute the remainder in  $K(x_0, \dots, x_{n-1})[X]$  of  $xg$  over  $f$  (4.2.6):

$$xg = qf + r.$$

The division algorithm gives that the coefficients  $r_0, \dots, r_{n-1}$  of  $r$  are linear in the  $x_j$ , say:

$$r_i = \alpha_{i+1,1}x_0 + \dots + \alpha_{i+1,n}x_{n-1}.$$

Let  $K[\alpha] = K[X]/(\neg C_f)$ .  $g(\alpha)$  is strongly zero divisor free.

If we substitute elements  $\xi_0, \dots, \xi_{n-1} \in K$  for  $x_0, \dots, x_{n-1}$  and so that  $\xi_i \neq 0$  for some  $i$ , then  $x(\alpha) \neq 0$  by 4.3.8c.

Thus  $x(\alpha)g(\alpha) \neq 0$  and  $r(\alpha) \neq 0$ . This implies that the matrix  $(\alpha_{i,j})$  is invertible. Thus we find a unique  $k = k_0 + \dots + k_{n-1}X^{n-1}$  so that after substitution  $x_i \mapsto k_i$  we get

$$kg = -hf + 1.$$

Since  $f \neq 0$ ,  $h$  is unique too.

Observe that we did not use the tightness of the apartness in the proof above. From 4.3.8a and 4.5.4 it immediately follows ([He 2]):

4.5.5. Theorem. Let  $f \in K[X]$ ,  $f \neq 0$ ,  $K[\alpha] = K[X]/(\neg C_f)$ . Let  $f$

be prime and regular with  $\deg(f) = n$ . Then  $K[\alpha]$  is a field so that

$$[K[\alpha] : K] = n.$$

4.5.6. Remark. It is a simple task to find a model showing that primality alone is not enough for  $f$ , to prove that  $C_f$  is minimal (cf. chapter 2). On the other hand regularity is not necessary, as follows from the model below:

$$\begin{array}{l} \underline{K} \text{ is: } \mathbb{F}_2 \quad \mathbb{Q} \\ \quad \quad \quad \diagdown \quad \diagup \\ \quad \quad \quad \mathbb{Z}_{(2)} \end{array} \quad \begin{array}{l} f = 2X^2 + X + 1. \\ \\ = S^{-1}\mathbb{Z} \text{ with } S = (2)^{\text{compl.}}. \end{array}$$

Then  $\underline{K} \models "f \text{ is prime}" \wedge "K[\alpha] \text{ is a field}"$ , but

$\underline{K} \not\models "f \text{ is regular}"$  (see [Ru 2] or 5.2.10(1)).

The traditional method of [Ar 1] fails in the intuitionistic case if  $f$  is not regular. But by refining the traditional proof we can derive the following invertibility theorem for prime polynomials in general:

4.5.7. Theorem. Let  $f = c_0 + \dots + c_n X^n \in K[X]$  be prime,  $c_m \neq 0$ ,  $g \in K[X]$  so that  $g(\alpha) \neq 0$  in  $K[\alpha] = K[X]/(\neg C_f)$ . Then we can split  $f = f^\# + f^\equiv$  where  $f^\# = c_0 + \dots + c_s X^s$ ,  $s \geq m$ ,  $c_s \neq 0$  so that  $g(\beta)$  is invertible in  $K[\beta] = K[X]/(\neg C_{f^\#})$ .

Moreover, we can find an inverse  $b(\beta)$  so that  $b$  has degree at most  $(s-1)$ .

Proof: We prove the statement above by induction on  $(n-m)$ .

The case for  $n-m = 0$  immediately follows from 4.5.5.

Induction step: Start with  $f^\# = c_0 + \dots + c_m X^m$ .  $f^\equiv = f - f^\#$ .

Let  $\xi_0, \dots, \xi_{m-1}$  be  $K$ -variables and

$$x = \xi_0 + \dots + \xi_{m-1} X^{m-1}.$$

Then  $gx = qf^\# + r$  by the division algorithm.

$r \equiv r_0 + \dots + r_{m-1} X^{m-1}$  with the  $r_i$  linear in the  $\xi_j$ :

$$r_i \equiv \alpha_{i+1,1} \xi_0 + \dots + \alpha_{i+1,m} \xi_{m-1}.$$

Altogether we have  $g \in C_f$ ,  $f$  prime,  $c_m \neq 0$  and

$$gx \equiv qf + r - qf^{\equiv}.$$

Thus  $\forall \xi_0, \dots, \xi_{m-1} \left( \bigwedge_{0 \leq i \leq m-1} \xi_i \neq 0 \rightarrow r - qf^{\equiv} \neq 0 \right)$

$$\forall \xi_0, \dots, \xi_{m-1} \left( \bigwedge_{0 \leq i \leq m-1} \xi_i \neq 0 \rightarrow r \neq 0 \vee qf^{\equiv} \neq 0 \right).$$

Using lemma 3.7.3 we get

$$\det(\alpha_{ij}) \neq 0 \vee qf^{\equiv} \neq 0.$$

Assume  $qf^{\equiv} \neq 0$ . Then  $f^{\equiv} \neq 0$ , thus  $c_{m'} \neq 0$  for some  $m' > m$ . Apply induction. Assume  $\det(\alpha_{ij}) \neq 0$ . Then there are  $\beta_0, \dots, \beta_{m-1} \in K$  so that

$$(\alpha_{ij}) \begin{pmatrix} \beta_0 \\ \vdots \\ \beta_{m-1} \end{pmatrix} \equiv \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Let  $b \equiv \beta_0 + \dots + \beta_{m-1} X^{m-1}$ . Then  $gb \equiv qf^{\equiv} + 1$  (with  $\beta_i$  for the  $\xi_i$ ).  $g(\beta)$  is invertible in  $K[\beta] \equiv K[X] / (\neg C_f \neq)$ .

Let  $K \subseteq L$  be fields,  $\alpha \in L$ . Let  $K(\alpha)$  be the smallest field containing  $K$  and  $\alpha$ .  $\alpha$  is algebraic over  $K$  if there is an  $f \in K[X]$  so that  $f \neq 0$  and  $f(\alpha) \equiv 0$ . The following theorem gives some conditions under which  $f$  is prime and regular.

4.5.8. Theorem. Let  $K \subseteq L$  be fields,  $\alpha \in L$ ,  $f \in K[X]$ ,  $f \neq 0$ .

Then are equivalent:

(a)  $f$  has degree at most  $n$ ,  $f(\alpha) \equiv 0$  and  $(K(\alpha)/K)$  has degree at least  $n$ .

(b)  $f$  is prime and regular with  $\deg(f) \equiv n$ ,

$K[X] / (\neg C_f) \cong K[\alpha] \equiv K(\alpha)$  with the canonical morphism and  $[K[\alpha] : K] \equiv n$ .

Proof: From (b) to (a) is trivial.



Assume (a).

There are  $p_1, \dots, p_n, q_1, \dots, q_n \in K[X]$  so that

$$p_1(\alpha)q_1^{-1}(\alpha), \dots, p_n(\alpha)q_n^{-1}(\alpha) \text{ is free in } (K(\alpha)/K).$$

Let  $q \equiv q_1(\alpha) \cdot \dots \cdot q_n(\alpha)$  and take

$$r_i \equiv p_i q_i^{-1} q, \quad 1 \leq i \leq n. \text{ Then } r_1(\alpha), \dots, r_n(\alpha) \in K[\alpha].$$

A simple calculation shows that  $r_1(\alpha), \dots, r_n(\alpha)$  is free in  $(K[\alpha]/K)$ . There is an  $m \in \mathbb{N}$  so that  $r_1(\alpha), \dots, r_n(\alpha)$  depend on  $1, \alpha, \dots, \alpha^m$ . Now let  $f \equiv c_0 + \dots + c_n X^n$  and  $c_j \neq 0$ . Now we can prove by induction on  $m \equiv (n-j)$  that

$$c_n \neq 0.$$

$m = 0$ : trivial.

Induction step:  $m > 0$ , thus  $j < n$ . Take the sequence  $S$  consisting

$$\begin{array}{l} \text{of } 1, \alpha, \alpha^2, \dots, \alpha^{j-1}, \\ c_{j+1} \alpha^{j+1}, c_{j+1} \alpha^{j+2}, \dots, c_{j+1} \alpha^{m+n-j}, \\ c_{j+2} \alpha^{j+1}, c_{j+2} \alpha^{j+2}, \dots, c_{j+2} \alpha^{m+n-j}, \\ \vdots \\ c_n \alpha^{j+1}, c_n \alpha^{j+2}, \dots, c_n \alpha^{m+n-j}. \end{array}$$

Then, by induction on  $k$  we can prove that  $\alpha^k$  ( $0 \leq k \leq m$ ) depends on  $S$ , because if  $k \geq j$

$$\alpha^k \equiv -c_j^{-1} (c_0 \alpha^{k-j} + c_1 \alpha^{k-j+1} + \dots + c_{j-1} \alpha^{k-1} + c_{j+1} \alpha^{k+1} + \dots + c_n \alpha^{k+n-j}).$$

Then  $1, \alpha, \dots, \alpha^m$  depends on  $S$ , thus also

$$r_1(\alpha), \dots, r_n(\alpha) \text{ depends on } S.$$

From the procedure of the Austauschatz (3.3.2) it easily follows that  $c_s \alpha^t \neq 0$  for some  $s > j$  and  $t > j$ . Thus  $c_s \neq 0$  for some  $s > j$ . Replace  $c_j$  by  $c_s$ . Using induction on  $m$  we can conclude:  $c_n \neq 0$ . Thus

$$f \text{ is regular and } \deg(f) \equiv n.$$

From this follows immediately:

$1, \alpha, \dots, \alpha^m$  is equivalent to  $1, \alpha, \dots, \alpha^{n-1}$   
and  $r_1(\alpha), \dots, r_n(\alpha)$  depends on  $1, \alpha, \dots, \alpha^{n-1}$ .

Thus  $1, \alpha, \dots, \alpha^{n-1}$  is free (3.3.3). Take the canonical morphism  $\varphi: K[X] \rightarrow K[\alpha]$  sending  $X$  to  $\alpha$ . Let  $g \in K[X]$ .  $f$  is regular, thus  $g \equiv qf + r$  by the division algorithm. So  $\varphi(g) \equiv r(\alpha)$ .

Now it is simple to see that the cokernel is  $C_f$  and that  $\varphi$  is surjective. That means  $\varphi^*: K[X]/(\neg C_f) \rightarrow K[\alpha]$  is an isomorphism.  $K[\alpha]$  is an integral domain, thus  $C_f$  is prime. Thus  $f$  is prime and regular. Thus  $K[\alpha]$  is a field. Thus  $K[\alpha] \equiv K(\alpha)$  and  $[K[\alpha]:K] \equiv \deg(f) \equiv n$ .

#### 4.6 Separable extensions

The construction of normal and separable extensions of fields for a polynomial  $f$  is complicated. It only works under special circumstances (see [Ke 1], [Ri 1] or 4.10). However, it is possible to prove some general facts about separability.

4.6.1. Definition. The derivative is the  $K$  linear map  $D: K[X] \rightarrow K[X]$  so that  $D(X) \equiv 1$  and  $D(fg) \equiv fD(g) + gD(f)$ .  $D(f)$  is the derivative of  $f$ . We also write  $Df$  or  $f'$  for the derivative of  $f$ .  $f$  is separable if  $f$  is prime and  $Df \neq 0$ .

By 4.3.8c we have for all  $f \in K[X]$ : if  $Df \neq 0$  then  $Df \in C_f$ .

4.6.2. Remark. We introduce the following notations. Let  $n \in \mathbb{N}$ . Then we write  $\bar{n}$  for the corresponding integer in  $K$ . By doing so we can avoid some confusion in the theorems below.  $\mathbb{P}$  is the

subobject of prime numbers of  $\mathbb{N}$ .

4.6.3. Proposition. Let  $f \in K[X]$  be prime. Then are equivalent:

- (a)  $f$  is separable,
- (b)  $\forall g \in K[X]. \forall p \in \mathbb{P}. (\bar{p} \# \bar{0} \vee f(X) \# g(X^p))$ .

Proof: Let  $f \equiv a_0 + \dots + a_n X^n$ .

Assume (a). Then  $Df \# \bar{0}$ , thus  $\bar{m} a_m \# \bar{0}$  for some  $\bar{m}$ . Let  $p \in \mathbb{P}$ .

If  $p$  divides  $m$  then  $\bar{p} \# \bar{0}$ . If  $p$  does not divide  $m$  then  $f(X) \# g(X^p)$  for all  $g \in K[X]$ . This proves (b).

Assume (b).  $f \# f(\bar{0})$  thus  $a_m \# \bar{0}$  for some  $m > 0$ . Let  $p \in \mathbb{P}$  be a prime number so that  $p$  divides  $m$ . Let  $g \equiv a_0 + a_p X + a_{2p} X^2 + \dots$ . Then  $\bar{p} \# \bar{0} \vee g(X^p) \# f$ . We can choose  $p$  so that for all other prime  $q \leq n$  we have  $\bar{q} \# \bar{0}$ .

Assume  $\bar{p} \# \bar{0}$ . Then  $\bar{m} \# \bar{0}$  and  $Df \# \bar{0}$ .

Assume  $g(X^p) \# f$ . Then there is an  $m' \leq n$  so that  $p$  does not divide  $m'$  and  $a_{m'} \# \bar{0}$ . Thus  $\bar{m}' a_{m'} \# \bar{0}$  and  $Df \# \bar{0}$ .

4.6.4. Proposition. Let  $f \in K[X]$  be prime. Then are equivalent:

- (a)  $\neg$  "f is separable",
- (b)  $\exists g \in K[X]. \exists p \in \mathbb{P}, (\bar{p} \equiv \bar{0} \wedge f(X) \equiv g(X^p))$ .

Proof: Immediate from the definition. Use the tightness of the apartness relation.

4.6.5. Lemma. Let  $f$  be prime and  $a, b \in K$  so that  $a \# b$ . Then  $f(a) \# \bar{0}$  or  $f(b) \# \bar{0}$ .

Proof: We may assume  $a \equiv \bar{1}$  and  $b \equiv \bar{0}$ .  $f \# f(\bar{0})$  thus  $\bar{1} \in C_f$ . That implies  $\bar{1} - X \in C_f \vee X \in C_f$ . If  $\bar{1} - X \in C_f$  we substitute  $Y \equiv \bar{1} - X$ , thus reducing case one to case two. Therefore we may assume  $X \in C_f$ . To prove:  $f(\bar{0}) \# \bar{0}$ .

$f \equiv a_0 + \dots + a_n X^n \not\equiv f(\bar{0})$  thus  $a_i \not\equiv \bar{0}$  for some  $i \geq 1$ . We have two cases to consider.

Case 1.  $a_i \not\equiv \bar{0}$  for  $i \geq 2$ . Then  $f \equiv pX + f(\bar{0})$  with  $p \not\equiv p(\bar{0})$ .  $f$  is prime, thus  $f(\bar{0}) \not\equiv \bar{0}$ .

Case 2.  $a_1 \not\equiv \bar{0}$ . Then  $a_1 X \in C_f$  and  $a_1 X - f \in C_f$ . Thus  $f(\bar{0}) \not\equiv \bar{0}$  or  $a_i \not\equiv \bar{0}$  for some  $i \geq 2$ .

4.6.6. Remark. Let  $f \equiv a_0 + \dots + a_n X^n$  be prime,  $K[\alpha] \equiv K[X] / (\neg C_f)$ . By 4.6.5 we may assume that  $a_0 \equiv \bar{1}$ . Then  $\alpha$  is invertible and

$$\alpha^{-1} \equiv -a_n \alpha^{n-1} - \dots - a_1.$$

Let  $g(\alpha) \equiv g_0 + \dots + g_m \alpha^m$ , then

$$g(\alpha) \equiv \alpha(g_1 + \dots + g_m \alpha^{m-1} - g_0 a_1 - \dots - g_0 a_n \alpha^{n-1}).$$

Iterating this procedure we find  $x_0, \dots, x_{n-1} \in K$  so that

$$g(\alpha) \equiv \alpha^m (x_0 + \dots + x_{n-1} \alpha^{n-1}) \text{ and so that for all } i \\ x_i \not\equiv \bar{0} \rightarrow \exists j > i. a_j \not\equiv \bar{0}.$$

By 4.3.8c this implies:  $\exists i. x_i \not\equiv \bar{0} \leftrightarrow g(\alpha) \not\equiv \bar{0}$ .

4.6.7. Lemma. Let  $f \equiv a_0 + \dots + a_n X^n \in K[X]$ ,  $a_r \not\equiv \bar{0}$  for some  $r > 0$ ,  $K[\alpha] \equiv K[X] / (\neg C_f)$ . Let  $y_1, \dots, y_r \in (K[\alpha] / K)$  and let  $\varphi$  be a formula in which  $x_1, \dots, x_r$  do not occur free. Assume that  $\forall x_1, \dots, x_r \in K. (\bigwedge_i x_i \not\equiv \bar{0} \rightarrow \bigvee_i x_i y_i \not\equiv \bar{0} \vee \varphi)$  holds. Then we have (" $y_1, \dots, y_r$  is free")  $\vee \exists r' > r. a_{r'} \not\equiv \bar{0} \vee \varphi$ .

Proof: there is an  $n$  and there are  $g_1, \dots, g_r \in P_n$  so that for all  $i$   $g_i(\alpha) \equiv y_i$ . Let  $(\cdot)^* \equiv (\cdot)_f^*$  be a map for  $P_n$  according to 4.3.6. By 4.3.8d there are  $k_1, \dots, k_r$  so that for all  $i$   $k_i \equiv g_i - g_i^* f \equiv k_{i,0} + k_{i,1} X + \dots + k_{i,s-1} X^{s-1} + h_i$ . By careful reading the proof of 4.3.6 we see that we may assume  $s \geq r$  and  $a_s \not\equiv \bar{0}$ . If  $s > r$  then  $\exists r' > r. a_{r'} \not\equiv \bar{0}$  holds. So we may assume

$r \equiv s$ . Then  $(k_{i,j})$  is an  $r \times r$ -matrix. The assumption of the lemma can be translated into

$$\forall z \in K^r. (z \neq \bar{0} \rightarrow (k_{i,j})z \neq \bar{0} \vee \exists i. h_i \neq \bar{0} \vee \varphi).$$

By 3.7.3 and 4.3.8d this implies  $(\text{"}(k_{i,j}) \text{ is invertible"} \vee \exists r' > r. a_{r'} \neq \bar{0} \vee \varphi)$ , where  $(\text{"}(k_{i,j}) \text{ is invertible"} \text{ gives } \text{"}y_1, \dots, y_r \text{ is free"} \text{"}$ .

The following theorem relates separability to a notion which can be used to define separability for field extensions  $L \supseteq K$  in general.

4.6.8. Theorem. Let  $f$  be prime,  $K[\alpha] \equiv K[X]/(\neg C_f)$ . Then we have:  $f$  is separable if and only if the following formula holds:

$$\begin{aligned} & \forall m \forall y_1, \dots, y_m \in K[\alpha] \forall p \in \mathbb{P} \\ & ((\text{"}y_1, \dots, y_m \text{ is free over } K\text{"}) \rightarrow \bar{p} \neq \bar{0} \vee (\text{"}y_1^p, \dots, y_m^p \text{ is free over } K\text{"})). \end{aligned}$$

Proof: Assume that the formula holds. Let  $p \in \mathbb{P}$  and  $g(X) \in K[X]$ .

It suffices to show:  $\bar{p} \neq \bar{0} \vee f(X) \neq g(X^p)$ . Then we can apply

4.6.3.  $f \neq \bar{0}$  thus  $f \neq g(X^p) \vee g(X^p) \neq \bar{0}$ . We may assume:

$g(X^p) \neq \bar{0}$ . Let  $g \equiv g_0 + \dots + g_m X^m$ . Then we shall prove by induction on  $(m-i)$ : if  $g_i \neq \bar{0}$  then  $\bar{p} \neq \bar{0}$  or  $f(X) \neq g(X^p)$ . The case for  $m-i \equiv 0$  is contained in the induction step.

Induction step: let  $g_i \neq \bar{0}$ . Then  $f \neq g(X^p) \vee$  ("f has degree at least  $i+1$ "). We may assume that  $f$  has degree at least  $i+1$ .

Then  $1, \alpha, \dots, \alpha^i$  is free thus  $1, \alpha^p, \dots, \alpha^{ip}$  is free or  $\bar{p} \neq \bar{0}$ .

We may assume that  $1, \alpha^p, \dots, \alpha^{ip}$  is free. Then is

$$g_0 + g_1 \alpha^p + \dots + g_i \alpha^{ip} \neq \bar{0}, \text{ thus } g(\alpha^p) \neq \bar{0} \vee \exists j > i. g_j \neq \bar{0}.$$

If  $g(\alpha^p) \neq \bar{0}$  then  $f(X) \neq g(X^p)$ . If  $g_j \neq \bar{0}$  for some  $j > i$  then

we apply induction. This proves that  $f$  is separable. Assume that  $f$  is separable. Let  $f = a_0 + \dots + a_n X^n \neq \bar{0}$ . Take  $p \in \mathbb{P}$  and  $y_1, \dots, y_m \in K[\alpha]$  so that  $y_1, \dots, y_m$  is free. To prove:  $\bar{p} \neq \bar{0} \vee ("y_1^D, \dots, y_m^D$  is free"). By 4.6.6 we can write  $y_i = \alpha^s (x_{i,0} + x_{i,1} \alpha + \dots + x_{i,n-1} \alpha^{n-1})$  so that  $x_{i,j} \neq \bar{0}$  implies that  $a_k \neq \bar{0}$  for some  $k > j$ . By induction on  $(n-r)$  we shall prove: if  $a_r \neq \bar{0}$  then  $\bar{p} \neq \bar{0}$  or  $y_1^D, \dots, y_m^D$  is free. The case for  $n-r = 0$  is contained in the induction step.

Induction step: let  $a_r \neq \bar{0}$ .  $y_1, \dots, y_m$  is free thus the  $m \times n$ -matrix  $(x_{i,j})$  has rank  $m$ . If  $m > r$  then  $a_{r'} \neq \bar{0}$  for some  $r' > r$  and we can apply induction. Assume  $m \leq r$ . The sequence  $\alpha^s, \alpha^{s+1}, \dots, \alpha^{s+r-1}$  is free. Therefore, by 3.10.5, we can extend the sequence  $y_1, \dots, y_m$  to a longer sequence  $y_1, \dots, y_r$  so that the corresponding  $r \times n$ -matrix  $(x_{i,j})$  has rank  $r$  and so that  $x_{i,j} = \bar{0}$  if  $i > m$  and  $j \geq r$ . This does not yet imply that  $y_1, \dots, y_r$  is free. However, we have  $\forall z_1, \dots, z_r \in K. (\bigvee_i z_i \neq \bar{0} \rightarrow \sum_i z_i y_i \neq \bar{0} \vee \exists r' > r. a_{r'} \neq \bar{0})$  and by 4.6.7 this gives us  $("y_1, \dots, y_r$  is free")  $\vee \exists r' > r. a_{r'} \neq \bar{0}$ . We may assume that  $y_1, \dots, y_r$  is free. Let  $M$  be the following  $r \times r$ -matrix:

$$M = \begin{pmatrix} x_{1,0} & \cdots & x_{1,r-1} \\ \vdots & & \vdots \\ x_{r,0} & \cdots & x_{r,r-1} \end{pmatrix}$$

Since  $y_1, \dots, y_r$  is free we have  $\det M \neq \bar{0} \vee \exists r' > r. a_{r'} \neq \bar{0}$ .

We may assume that  $\det M \neq \bar{0}$ . Let  $M_p$  be the  $r \times r$ -matrix  $(x_{i,j}^D)$ .

Then  $\det M_p \neq \bar{0} \vee \det M_p \neq \det M^D$ . If  $\det M_p \neq \det M^D$  then  $\bar{p} \neq \bar{0}$ .

Therefore we may assume that  $\det M_p = \bar{0}$ . We can write

$y_i^D = \alpha^{sp} (x_{i,0}^D + x_{i,1}^D \alpha^D + \dots + x_{i,r-1}^D \alpha^{(r-1)p}) + h_i$  where  $h_i \neq \bar{0}$

implies that  $\bar{p} \neq \bar{0} \vee \exists r' > r. a_{r'} \neq \bar{0}$ . Then we have

$\forall z_1, \dots, z_r \in K. (\bigvee_i z_i \neq \bar{0} \rightarrow \sum_i z_i y_i^D \neq \bar{0} \vee \bar{p} \neq \bar{0} \vee \exists r' > r. a_{r'} \neq \bar{0})$ .

By 4.6.7 we get

("y<sub>1</sub><sup>P</sup>, ..., y<sub>r</sub><sup>P</sup> is free")  $\vee \bar{p} \neq \bar{0} \vee \exists r' > r. a_{r'} \neq \bar{0}$

If y<sub>1</sub><sup>P</sup>, ..., y<sub>r</sub><sup>P</sup> is free then y<sub>1</sub><sup>P</sup>, ..., y<sub>m</sub><sup>P</sup> is free too. And if  $\exists r' > r. a_{r'} \neq \bar{0}$  holds then we can apply induction.

#### 4.7 Morphisms and subfields

Up to now we have constructed some extensions of fields. Now we shall start to do the converse: constructing subfields from an (extension-) field. The main tools are morphisms.

4.7.1. Theorem. Let  $\sigma: K \rightarrow R$  be a morphism with  $K$  a field and  $R$  a ring with  $1 \neq 0$ . Then  $\sigma$  is an embedding, i.e.

$$\forall \alpha \in K (\alpha \neq 0 \rightarrow \sigma(\alpha) \neq 0)$$

Moreover, if  $\sigma$  is surjective and  $R$  a field, then  $\sigma$  is an isomorphism.

Proof: Let  $\alpha \in K$ ,  $\alpha \neq 0$ . Then  $\alpha^{-1}$  exists and

$$\sigma(\alpha) \cdot \sigma(\alpha^{-1}) = \sigma(\alpha \cdot \alpha^{-1}) = \sigma(1) = 1 \neq 0.$$

Thus  $\sigma(\alpha) \neq 0$ .  $\sigma$  is an embedding. If, moreover,  $\sigma$  is surjective, then it is a bijective embedding. It remains to prove that  $\sigma$  is strongly extensional if  $R$  is a field. Let  $\sigma(\alpha) \neq 0$ . Then there is a  $\sigma(\beta) \in R$  ( $\sigma$  is surjective) so that

$$\sigma(\alpha)\sigma(\beta) = 1$$

$$\sigma(\alpha\beta) = 1; \alpha\beta \neq 0. \text{ And so } \alpha \neq 0.$$

The extra assumption for  $R$  in 4.7.1 that  $\alpha \neq 0$  implies  $\exists \alpha^{-1}$  is needed to prove that  $\sigma$  is isomorphic, as the following model shows:

$\underline{K}$  is:  $\mathbb{Q}$   
 $\downarrow$   
 $\mathbb{Z}_{(p)}$  with  $x \neq 0$  in  
the nodes if  
 $x$  is invertible.

$\underline{R}$  is:  $\mathbb{Q}$   
 $\downarrow$   
 $\mathbb{Z}_{(p)}$  with  $\neq$  in the  
nodes the inequality.

$\underline{K}$  is a field,  $\underline{R}$  is an integral domain. Let  $\underline{\sigma}$  be the identity.  
Then  $(\underline{K}, \underline{R}) \not\models \sigma$  is strongly extensional".

4.7.2. Corollary. Let  $K$  be a field,  $\sigma: K \rightarrow K$  a surjective morphism.  
Then  $\sigma$  is an automorphism.

How can we construct subfields by morphisms?

4.7.3. Remark. The presence of apartness makes it natural to  
consider cofields analogous to coideals. A cofield of a field  
 $L$  is a subobject  $C \subseteq L$  so that

- (1)  $\neg 0 \in C \wedge \neg 1 \in C$
- (2)  $x - y \in C \rightarrow x \in C \vee y \in C$
- (3)  $xy \in C \rightarrow x \in C \vee y \in C$
- (4)  $x^{-1} \in C \rightarrow x \in C$

A cofield defines a subfield

$(\neg C)_L \equiv \{\alpha \in L \mid \neg \alpha \in C\}$ . We write  $(\neg C)$  if no confusion  
is possible.

Let  $H$  be a collection of morphisms from  $L$  to  $M$ . Then  $H$  defines  
a cofield as follows:

$$C \equiv \{\alpha \in L \mid \exists \sigma, \tau \in H. \sigma(\alpha) \neq \tau(\alpha)\}.$$

$(\neg C)$  is called the fixed field of  $H$ : using the tightness of  
the apartness we find  $(\neg C) \equiv \{\alpha \in L \mid \forall \sigma, \tau \in H. \sigma(\alpha) \equiv \tau(\alpha)\}$ .



Unfortunately we get only stable subfields in this way. To cover more general subfields we use a generalization.

4.7.4. Definition. Let  $S \subseteq G$  be two collections of morphisms from  $L$  to  $M$ . Then

$$\varphi_G(S) \equiv \{\alpha \in L \mid \forall \sigma, \tau \in G (\sigma(\alpha) \neq \tau(\alpha) \rightarrow \sigma \in S \vee \tau \in S)\}.$$

We write  $\varphi(S)$  if no confusion is possible. The reader may think of  $G$  as a group of automorphisms and of  $S$  as a cogroup of  $G$ . It is a simple task to show that  $\varphi(S)$  is a subfield and that for  $(\neg C)$  above  $(\neg C) \equiv \varphi_H(\phi)$ .

In case  $G$  is a group of automorphisms of  $L$  we can do the converse, i.e. we can construct cogroups out of subobjects of  $L$ .

4.7.5. Definition. Let  $G$  be a group of automorphisms of  $L$ . Then for each subobject  $D$  of  $L$  we define

$$\gamma(D) \equiv \{\sigma \in G \mid \exists \alpha \in D. \sigma(\alpha) \neq \alpha\}.$$

4.7.6. Remark.  $\gamma(D)$  is a cogroup. A sketch of the proof is given below.  $(\neg\gamma(D))$  is called the fixed group of  $D$  and its morphisms  $D$ -automorphisms. The least trivial step in the proof that  $\gamma(D)$  is a cogroup is the verification of the axiom

$$\sigma\tau \in \gamma(D) \rightarrow \sigma \in \gamma(D) \vee \tau \in \gamma(D).$$

Assume  $\sigma\tau \in \gamma(D)$ . There is an  $\alpha \in D$  so that

$$\begin{aligned} \sigma\tau(\alpha) &\neq \alpha \\ \tau(\alpha) &\neq \sigma^{-1}(\alpha) \\ \tau(\alpha) &\neq \alpha \vee \alpha \neq \sigma^{-1}(\alpha) \\ \tau \in \gamma(D) &\vee \sigma \in \gamma(D). \end{aligned}$$

There is a standard procedure to construct from a collection

of automorphisms of  $L$  an automorphism group.

Namely: take all finite sequences of automorphisms and their inverses and take their compositions. Of course we need the natural number object for this construction. The group carries the apartness relation from  $L^L$ :

$$\sigma \# \tau \leftrightarrow \exists \alpha \in L. \sigma(\alpha) \# \tau(\alpha).$$

#### 4.8 Characters

4.8.1. Definition. Let  $S$  be a monoid and let  $L$  be a field.

A character is a morphism from  $S$  to the multiplicative monoid of  $L$  (i.e.  $L$  with restriction to  $\#, \cdot, 1$ ).

Example: a ring morphism  $\sigma: L \rightarrow M$  from a field  $L$  to a field  $M$  defines a character  $\sigma^*: L^* \rightarrow M^* \subseteq M$  ( $L^*$  and  $M^*$  are the multiplicative groups as in chapter 2).

We call a sequence  $x_1, \dots, x_n \in X$  apart if the  $x_i$ 's are pairwise apart.

4.8.2. Theorem. Let  $\sigma_1, \dots, \sigma_n \in L^S$  be an apart sequence of characters;  $S$  a monoid. Then  $\sigma_1, \dots, \sigma_n$  is free in the vector space  $L^S$  over  $L$ .

Proof: induction on  $n$ .  $n = 1$ : let  $\alpha \in L$  with  $\alpha \neq 0$ . Then  $\alpha\sigma_1(1) = \alpha \neq 0$ , thus  $\alpha\sigma_1 \neq 0$  in  $L^S$ .

Induction step: Let  $\alpha_1, \dots, \alpha_n \in L$  with  $\bigwedge_{1 \leq i \leq n} \alpha_i \neq 0$ . It is no restriction to suppose  $\alpha_1 \neq 0$ .

Define  $\tau = \alpha_1\sigma_1 + \dots + \alpha_n\sigma_n$ ,  $\tau \in L^S$ . To prove:  $\tau \neq 0$ .

There is an  $\alpha \in S$  such that  $\sigma_1(\alpha) \neq \sigma_n(\alpha)$ .

Define  $\tau_\alpha \equiv \alpha_1 \sigma_1(\alpha) \sigma_1 + \dots + \alpha_n \sigma_n(\alpha) \sigma_n$  and

$\sigma_n(\alpha) \tau \equiv \alpha_1 \sigma_n(\alpha) \sigma_1 + \dots + \alpha_n \sigma_n(\alpha) \sigma_n$ . Subtract:

$$\tau_\alpha - \sigma_n(\alpha) \tau \equiv \alpha_1 (\sigma_1(\alpha) - \sigma_n(\alpha)) \sigma_1 + \dots + \alpha_{n-1} (\sigma_{n-1}(\alpha) - \sigma_n(\alpha)) \sigma_{n-1}.$$

Since  $\alpha_1 (\sigma_1(\alpha) - \sigma_n(\alpha)) \neq 0$ , we can apply induction: there is a  $\beta \in S$  such that

$$\tau_\alpha(\beta) - \sigma_n(\alpha) \tau(\beta) \neq 0.$$

Thus  $\tau(\alpha\beta) \neq \sigma_n(\alpha) \tau(\beta)$ , i.e.

$$\tau(\alpha\beta) \neq 0 \vee \tau(\beta) \neq 0 \text{ and}$$

$$\tau \neq 0.$$

Let  $L, M$  be fields and  $\sigma_1, \dots, \sigma_n \in M^L$  ring morphisms. They define characters  $\sigma_1^*, \dots, \sigma_n^* \in M^{L^*}$ .

Then " $\sigma_1, \dots, \sigma_n$  is apart"  $\leftrightarrow$  " $\sigma_1^*, \dots, \sigma_n^*$  is apart".

For, let  $\sigma_i \neq \sigma_j$ . Then there is an  $\alpha \in L$  so that

$$\sigma_i(\alpha) \neq \sigma_j(\alpha).$$

Furthermore  $\alpha \neq 0 \vee 1-\alpha \neq 0$ . Assume  $\alpha \neq 0$ , then we are done:

$\sigma_i^* \neq \sigma_j^*$ . Assume  $1-\alpha \neq 0$ .

Now  $1-\sigma_i(\alpha) \neq 1-\sigma_j(\alpha)$

$$\sigma_i(1-\alpha) \neq \sigma_j(1-\alpha). \text{ Thus again } \sigma_i^* \neq \sigma_j^*.$$

Thus we have  $\sigma_i \neq \sigma_j \rightarrow \sigma_i^* \neq \sigma_j^*$ . The converse is trivial.

From 4.8.2 and the remarks above it easily follows that:

4.8.3. Corollary. Let  $\sigma_1, \dots, \sigma_n$  be ring morphisms from the field  $L$  to the field  $M$  and let them be apart. Then  $\sigma_1^*, \dots, \sigma_n^*$  is free in the vector space  $M^{L^*}$  over  $M$ .

#### 4.9 Degrees over a fixed field

Let the fixed field  $K$  of a sequence  $\sigma_1, \dots, \sigma_n$  of morphisms  $\in M^L$  be the field  $K \equiv \phi_H(\phi)$  as defined in 4.7.4, for  $H \equiv \{\sigma_1, \dots, \sigma_n\}$ .

4.9.1. Theorem. Let  $\sigma_1, \dots, \sigma_n$  be an apart sequence of morphisms  $\in M^L$  with fixed field  $K \subseteq L$ . Let the  $\sigma_i$  be strongly extensional. Then  $(L/K)$  has degree at least  $n$ .

Proof: we shall prove by induction on  $r$ , that for  $r \leq n$  there is a sequence of vectors  $\omega_1, \dots, \omega_r \in (L/K)$ , which is free and so that

$$A_r \equiv \begin{pmatrix} \sigma_1(\omega_1) & \dots & \sigma_r(\omega_1) \\ \vdots & & \vdots \\ \sigma_1(\omega_r) & \dots & \sigma_r(\omega_r) \end{pmatrix} \quad \text{is invertible over } M.$$

$r = 1$ : take  $\omega_1 \equiv 1$ . Then  $A_1 \equiv (1)$  is invertible.

Induction step: Let  $r < n$ ,  $\omega_1, \dots, \omega_r$  be free in  $(L/K)$  and  $A_r$  invertible. Then there are  $\xi_1, \dots, \xi_r \in M$  so that

$$A_r \begin{pmatrix} \xi_1 \\ \vdots \\ \xi_r \end{pmatrix} \equiv \begin{pmatrix} \sigma_{r+1}(\omega_1) \\ \vdots \\ \sigma_{r+1}(\omega_r) \end{pmatrix}$$

$\sigma_1, \dots, \sigma_{r+1}$  is free; thus there is an  $\omega_{r+1} \in L$  so that  $\omega_{r+1} \neq 0$  and

$$\xi_1 \sigma_1(\omega_{r+1}) + \dots + \xi_r \sigma_r(\omega_{r+1}) \neq \sigma_{r+1}(\omega_{r+1}).$$

First we shall prove that  $\omega_{r+1}$  is free from  $\omega_1, \dots, \omega_r$  in  $(L/K)$ .

Let  $\alpha_1, \dots, \alpha_r \in K$  and

$$v \equiv \alpha_1 \omega_1 + \dots + \alpha_r \omega_r. \quad \text{To prove: } \omega_{r+1} \neq v.$$

We have  $\xi_1 \sigma_1(\omega_{r+1}) + \dots + \xi_r \sigma_r(\omega_{r+1}) \neq \sigma_{r+1}(\omega_{r+1})$  and

$$\xi_1 \sigma_1(v) + \dots + \xi_r \sigma_r(v) \equiv \sigma_{r+1}(v), \quad \text{because for all}$$

$$i, j, k \quad \sigma_j(\alpha_i) \equiv \sigma_k(\alpha_i).$$

Thus  $\xi_1 \sigma_1(\omega_{r+1} - v) + \dots + \xi_r \sigma_r(\omega_{r+1} - v) \neq \sigma_{r+1}(\omega_{r+1} - v)$ .

For some  $i \leq r+1$  we have  $\sigma_i(\omega_{r+1} - v) \neq 0$ .  $\sigma_i$  is strongly extensional, so

$$\omega_{r+1} \neq v.$$

$\omega_1, \dots, \omega_{r+1}$  is free.

Then we must prove  $A_{r+1} \equiv \begin{pmatrix} \begin{pmatrix} & & \\ & A_r & \\ & & \end{pmatrix} & \begin{matrix} \sigma_{r+1}(\omega_1) \\ \vdots \\ \sigma_{r+1}(\omega_r) \end{matrix} \\ \sigma_1(\omega_{r+1}) \cdots \sigma_r(\omega_{r+1}) & \sigma_{r+1}(\omega_{r+1}) \end{pmatrix}$

is invertible.

Let the columns be  $v_1, \dots, v_{r+1}$ . Then  $v_1, \dots, v_r$  is free. To prove:  $v_{r+1}$  is free from them. We know that  $v_{r+1} \neq \xi_1 v_1 + \dots + \xi_r v_r$  because of the bottom row. Let  $\alpha_1, \dots, \alpha_r \in M$  and

$$w \equiv \alpha_1 v_1 + \dots + \alpha_r v_r. \text{ To prove } v_{r+1} \neq w.$$

$$v_{r+1} \neq w \vee w \neq \xi_1 v_1 + \dots + \xi_r v_r.$$

If  $v_{r+1} \neq w$ , we are done. Suppose  $w \neq \xi_1 v_1 + \dots + \xi_r v_r$ .

Then  $A_r \begin{pmatrix} \alpha_1 \\ \vdots \\ \alpha_r \end{pmatrix} \neq \begin{pmatrix} \sigma_{r+1}(\omega_1) \\ \vdots \\ \sigma_{r+1}(\omega_r) \end{pmatrix}$

Thus  $v_{r+1} \neq w$ .

Conclusion:  $\omega_1, \dots, \omega_{r+1}$  is free and  $A_{r+1}$  is invertible.

4.9.2. Corollary. Let  $\sigma_1, \dots, \sigma_n$  be an apart sequence of automorphisms of a field  $L$  with fixed field  $K$  in  $L$ . Then  $(L/K)$  has degree at least  $n$ .

The automorphisms leaving the subfield  $K$  invariant are closed under composition and inversion. So we can only expect that  $[L:K] \equiv n$  if  $\sigma_1, \dots, \sigma_n$  forms a group. That assumption actually is enough.

4.9.3. Theorem. Let  $\sigma_1, \dots, \sigma_n$  form a group of apart automorphisms of  $L$  with fixed field  $K$  in  $L$ . Then  $[L:K] \equiv n$ .

Proof: by 4.9.1 there are  $\omega_1, \dots, \omega_n \in L$  free over  $K$  so that

$$A_n = \begin{pmatrix} \sigma_1(\omega_1) & \dots & \sigma_n(\omega_1) \\ \vdots & & \vdots \\ \sigma_1(\omega_n) & \dots & \sigma_n(\omega_n) \end{pmatrix} \text{ is invertible.}$$

Thus the transposed matrix  $A_n^T$  is invertible. We must prove that  $\omega_1, \dots, \omega_n$  generates  $(L/K)$ . Let  $\omega \in L$ . Then there are  $\xi_1, \dots, \xi_n \in L$  so that

$$\xi_1 \sigma_1(\omega_1) + \dots + \xi_n \sigma_n(\omega_n) = \sigma_i(\omega) \text{ for } 1 \leq i \leq n. \quad (1)$$

Let  $\sigma_k$  be one of the automorphisms. Then  $\sigma_k \sigma_1, \dots, \sigma_k \sigma_n$  is a permutation of  $\sigma_1, \dots, \sigma_n$ . Applying  $\sigma_k$  to the system (1) and reordering the rows we get

$$\sigma_k(\xi_1) \sigma_i(\omega_1) + \dots + \sigma_k(\xi_n) \sigma_i(\omega_n) = \sigma_i(\omega) \text{ for } 1 \leq i \leq n.$$

Subtracting from (1) we have

$$[\xi_1 - \sigma_k(\xi_1)] \sigma_i(\omega_1) + \dots + [\xi_n - \sigma_k(\xi_n)] \sigma_i(\omega_n) = 0 \text{ for } 1 \leq i \leq n.$$

The rank of  $A_n^T$  is  $n$ , thus

$$\sigma_k(\xi_i) = \xi_i \text{ for } 1 \leq i \leq n, 1 \leq k \leq n.$$

Thus  $\xi_1, \dots, \xi_n \in K$ .

Moreover,  $\text{id}_L$  is among the  $\sigma_i$ , thus

$$\xi_1 \omega_1 + \dots + \xi_n \omega_n = \omega.$$

$\omega_1, \dots, \omega_n$  generates  $(L/K)$ .

#### 4.10 Examples

Example 1. Let  $L, M$  be fields:  $M = L(X)$ . Let  $\sigma, \tau$  be automorphisms

of  $M$  such that

$$\sigma_{\mathbb{N}_L} \equiv \tau_{\mathbb{N}_L} \equiv \text{id}_L,$$

$$\sigma(X) \equiv \frac{1}{X} \text{ and}$$

$$\tau(X) \equiv 1 - X.$$

$\sigma$  and  $\tau$  are automorphisms with  $\sigma^2 \equiv \tau^2 \equiv \text{id}_M$ .  $\sigma$  and  $\tau$  generate a group of 6 apart automorphisms, sending  $X$  to

$$X, 1 - X, \frac{1}{X}, \frac{X-1}{X}, \frac{1}{1-X} \text{ and } \frac{X}{X-1} \text{ respectively. We can determine}$$

the fixed field  $K$  of this group.

$$\text{Let } I \equiv \frac{(X^2 - X + 1)^3}{X^2(X-1)^2}. \sigma(I) \equiv \tau(I) \equiv I, \text{ thus } I \in K.$$

$K \supseteq L(I)$  and  $[M:K] \equiv 6$ , thus  $(M/L(I))$  has degree at least 6 and  $M \equiv L(I)(X)$ . Now  $X$  is root of the polynomial

$$f \equiv (Y^2 - Y + 1)^3 - IY^2(Y-1)^2 \in L(I)[Y].$$

With theorem 4.5.8 we may conclude:  $f$  is prime, regular and  $[M:L(I)] \equiv 6$ . Thus by 4.1.2  $K \equiv L(I)$ .

Example 2. Let  $L, M$  be fields:  $M \equiv L(X_1, \dots, X_n)$ .

Let  $S_n$  be the collection of permutations of  $1, \dots, n$ . For each  $\pi \in S_n$  we take an automorphism  $\sigma_\pi$  defined by

$$\sigma_{\pi \mathbb{N}_L} \equiv \text{id}_{\mathbb{N}_L} \text{ and } \sigma_\pi(X_i) \equiv X_{\pi(i)}.$$

This is a sequence of  $n!$  apart automorphisms. The sequence forms a group. Again we shall determine the fixed field  $K$ . Extend the automorphisms  $\sigma_\pi$  of  $M$  to automorphisms of  $M[Y]$  by defining

$$\sigma_\pi(Y) \equiv Y.$$

Let  $f \equiv (Y+X_1) \cdot \dots \cdot (Y+X_n) \equiv Y^n + a_1 Y^{n-1} + \dots + a_n$ .

$a_1, \dots, a_n$  are the elementary symmetric functions.

$\sigma_\pi(f) \equiv f$ , thus

$\sigma_\pi(a_i) \equiv a_i$ , for  $\pi \in S_n$ ,  $1 \leq i \leq n$ .

$K \supseteq L(a_1, \dots, a_n)$ .

Thus  $(M/L(a_1, \dots, a_n))$  has degree at least  $n!$  for the same reason as in example 1. We construct a tower of rings  $R_n \subseteq R_{n-1} \subseteq \dots \subseteq R_1 \subseteq R_0$  where

$R_n \equiv L(a_1, \dots, a_n)$  and

$R_j \equiv R_{j+1}[X_{j+1}]$ . So  $M \equiv Q(R_0)$ , the quotient field of  $R_0$ .

By the division algorithm we find that  $f_{j+1} \equiv (Y+X_1) \cdot \dots \cdot (Y+X_{j+1}) \in R_{j+1}[Y]$  and  $(-X_{j+1})$  is a root of  $f_{j+1}$ . By an induction argument this gives

$(R_j/R_n)$  has degree at most  $n(n-1) \cdot \dots \cdot (j+1)$ ,  $j \leq n-1$ . Thus  $(R_0/R_n)$  has degree at most  $n!$ , while  $(Q(R_0)/R_n)$  has degree at least  $n!$ .

So  $[R_0:R_n] \equiv n!$ . By 4.5.8 we have  $M \equiv Q(R_0) \equiv R_0$  and  $[M:R_n] \equiv n!$ .

$[M:L(a_1, \dots, a_n)] \equiv n!$  and  $K \equiv L(a_1, \dots, a_n)$ .

From this follows that  $R_n, R_{n-1}, \dots, R_0$  are fields (theorem 4.5.8) with  $[R_j:R_{j+1}] \equiv j+1$ .

Especially  $R_0 \equiv M$ . It turns out that the set of monomials  $X_1^{m_1} \cdot \dots \cdot X_n^{m_n}$  with  $m_j \leq j-1$  is free in  $(M/R_n)$ . There are  $n!$  of them. Thus they form a basis of  $(M/L(a_1, \dots, a_n))$ .

#### 4.11 Algebraic freedom and normal bases

4.11.1. Definition. Let  $f \in K[X_1, \dots, X_n]$  be a polynomial in  $n$  variables.  $f$  has degree at most  $m$  if  $f$  has degree at most  $m$  in each of its variables separately.



4.11.2. Let  $L$  and  $M$  be fields and let  $\sigma_1, \dots, \sigma_n$  be a sequence of morphisms  $\in M^L$  so that the  $\sigma_i$  are strongly extensional. Since  $\sigma_1(L)$  is isomorphic to  $L$  we shall assume that  $L \subseteq M$  and that  $\sigma_1 \equiv \text{id}_L$ .

Let  $\sigma_1, \dots, \sigma_n, L \subseteq M$  be as mentioned above,  $f$  a polynomial of  $L[X_1, \dots, X_n]$ . We want to consider the problem whether there is an  $x \in L$  such that

$$f(\sigma_1(x), \dots, \sigma_n(x)) \neq 0.$$

4.11.3. Lemma. Let  $f \in K[X_1, \dots, X_n]$ ,  $f \neq 0$ , be a polynomial in  $n$  variables with degree at most  $m$ . Let  $x_0, \dots, x_m$  be an apart sequence of  $m+1$  elements of  $K$ . Then there is a sequence  $x_{i_1}, \dots, x_{i_n}$  such that  $f(x_{i_1}, \dots, x_{i_n}) \neq 0$ .

Proof: by induction on  $n$ .

$n=1$ : then we can give a proof by induction on  $m$ . But there is also a direct proof (see [Gr 1]). Let  $f \equiv f_0 + \dots + f_m X^m$ . Consider the Vandermonde matrix

$$M \equiv \begin{pmatrix} 1 & x_0 & \dots & x_0^m \\ 1 & x_1 & \dots & x_1^m \\ \vdots & & & \vdots \\ 1 & x_m & \dots & x_m^m \end{pmatrix} \quad \text{with } \det M \equiv \prod_{i < j} (x_j - x_i) \neq 0.$$

Then for the vector  $v \equiv (f_0, \dots, f_m) \neq 0$  we have  $Mv \neq 0$ . Thus  $f(x_i) \neq 0$  for some  $i$ .

Induction step: we can write  $f$  as follows:

$$f \equiv g_0(X_2, \dots, X_n) + X_1 g_1(X_2, \dots, X_n) + \dots + X_1^m g_m(X_2, \dots, X_n) \neq 0.$$

By induction there is a  $j$  and there is a sequence  $x_{i_2}, \dots, x_{i_n}$

so that  $g_j(x_{i_2}, \dots, x_{i_n}) \neq 0$ .

Thus  $f(X_1, x_{i_2}, \dots, x_{i_n}) = a_0 + X_1 a_1 + \dots + X_1^m a_m \neq 0$ . So there is an  $x_{i_1}$  so that  $f(x_{i_1}, \dots, x_{i_n}) \neq 0$ .

In the presence of apartness the notion "algebraically free" is more natural than the notion "algebraically independent".

4.11.4. Definition. Let  $\sigma_1, \dots, \sigma_n$ ,  $L \subseteq M$  be as in 4.11.2.  $\sigma_1, \dots, \sigma_n$  is algebraically free if for all  $f \in L[X_1, \dots, X_n]$  with  $f \neq 0$  there is an  $x \in L$  so that  $f(\sigma_1(x), \dots, \sigma_n(x)) \neq 0$ .

4.11.5. Lemma. Let  $\sigma_1, \dots, \sigma_n$ ,  $L \subseteq M$  be as in 4.11.2 and so that  $\sigma_1, \dots, \sigma_n$  is apart. Let  $K$  be the fixed field of  $\sigma_1, \dots, \sigma_n$ . Let  $x_0, \dots, x_m$  be an apart sequence of elements of  $K$ . Then for all  $f \in L[X_1, \dots, X_n]$  so that  $f \neq 0$  and so that  $f$  has degree at most  $m$  we have an  $x \in L$  with  $f(\sigma_1(x), \dots, \sigma_n(x)) \neq 0$ .

Proof: by 4.9.1 there is a sequence  $\omega_1, \dots, \omega_n \in (L/K)$  which is free and so that the  $n \times n$ -matrix  $(\sigma_i(\omega_j))$  is invertible.

Let  $\varphi: L[X_1, \dots, X_n] \rightarrow M[Y_1, \dots, Y_n]$  be the following strongly extensional embedding: for  $1 \in L$  we have  $\varphi(1) = 1$  and for  $1 \leq i \leq n$  we have  $\varphi(X_i) = \sigma_i(\omega_1)Y_1 + \dots + \sigma_i(\omega_n)Y_n$ .

Let  $g(Y_1, \dots, Y_n) = \varphi(f(X_1, \dots, X_n))$ . If  $f$  has degree at most  $m$  then  $g$  has degree at most  $m$ . For all  $x = \xi_1 \omega_1 + \dots + \xi_n \omega_n$

with  $\xi_1, \dots, \xi_n \in K$  the following equation holds (use that  $\sigma_1 = \text{id}_L$ ):

$g(\xi_1, \dots, \xi_n) = f(\sigma_1(x), \dots, \sigma_n(x))$ . By 4.11.3 we may conclude:

for all  $f \neq 0$  with degree at most  $m$  there is an  $x = \xi_1 \omega_1 + \dots + \xi_n \omega_n \in L$  such that  $f(\sigma_1(x), \dots, \sigma_n(x)) = g(\xi_1, \dots, \xi_n) \neq 0$ .

4.11.6. Definition. An object  $Y$  with apartness is strongly infinite if for all  $m$  there is an apart sequence  $y_1, \dots, y_m$  of elements of  $Y$ .

4.11.7. Theorem. Let  $\sigma_1, \dots, \sigma_n$ ,  $L \subseteq M$  be as in 4.11.2 and so that  $\sigma_1, \dots, \sigma_n$  is apart. Let the fixed field  $K$  of  $\sigma_1, \dots, \sigma_n$  be strongly infinite. Then  $\sigma_1, \dots, \sigma_n$  is algebraically free.

Proof: immediate.

Another application of lemma 4.11.5 concerns the construction of normal sequences and normal bases.

4.11.8. Definition. Let  $\sigma_1, \dots, \sigma_n$ ,  $L \subseteq M$  be as in 4.11.2. Let  $K$  be the fixed field of  $\sigma_1, \dots, \sigma_n$ . A normal sequence of  $(M/K)$  is a free sequence of  $(M/K)$  of the form  $\sigma_1(x), \dots, \sigma_n(x)$ ,  $x \in L$ . A normal basis of  $(M/K)$  is a basis of  $(M/K)$  of the form  $\sigma_1(x), \dots, \sigma_n(x)$ .

4.11.9. Theorem. Let  $\sigma_1, \dots, \sigma_n$  be a sequence of automorphisms of  $L$  with fixed field  $K$ . Let  $\sigma_1, \dots, \sigma_n$  be apart and let  $K$  have an apart sequence of  $n+1$  elements. Then  $(L/K)$  has a normal sequence  $\sigma_1(x), \dots, \sigma_n(x)$ .

Proof: let  $\tau_1, \dots, \tau_{n^2}$  be the sequence of all compositions  $\sigma_i \sigma_j$ . There is a bijective map  $u$  from pairs of numbers  $i, j$  with  $1 \leq i, j \leq n$  to numbers  $k$  with  $1 \leq k \leq n^2$  so that  $\tau_{u(i,j)} = \sigma_i \sigma_j$ . By induction on  $m \equiv n^2 - s$  we shall show: if there is an apart subsequence  $\tau_{i_1}, \dots, \tau_{i_s}$ , then there is a normal sequence  $\sigma_1(x), \dots, \sigma_n(x)$  of  $(L/K)$ . The case for  $m \equiv 0$  is contained in the induction step.

Induction step: we may assume that  $\tau_1, \dots, \tau_s$  is apart. For each  $t \leq n^2$  there is a number  $v(t) \leq s$  such that for all  $s' \leq s$  with  $s' \neq v(t)$  we have  $\tau_{s'} \neq \tau_t$ . Consider the  $n \times n$ -matrix  $(X_{v(u(i,j))})$ . Let  $f(X_1, \dots, X_s) = \det(X_{v(u(i,j))})$ .

For all  $i, j, k$  with  $j \neq k$  we have  $\sigma_i \sigma_j \neq \sigma_i \sigma_k$ . That implies: if  $j \neq k$  and

$v(u(i,j)) \equiv v(u(i,k))$  then  $\sigma_i \sigma_j \neq \tau_{v(u(i,j))} \vee \sigma_i \sigma_k \neq \tau_{v(u(i,k))}$ .  
 If  $\sigma_i \sigma_j \neq \tau_{v(u(i,j))}$  (or equivalently if  $\sigma_i \sigma_k \neq \tau_{v(u(i,k))}$ ) then  
 the sequence  $\tau_1, \dots, \tau_s, \tau_{u(i,j)}$  is apart. From this it easily  
 follows that

$$\forall i, j, k \leq n. (j \neq k \rightarrow v(u(i,j)) \neq v(u(i,k))) \vee \\ \vee \exists s' > s. (" \tau_1, \dots, \tau_s, \tau_{s'} \text{ is apart} ").$$

Thus  $f(X_1, \dots, X_s) \neq 0 \vee \exists s' > s. (" \tau_1, \dots, \tau_s, \tau_{s'} \text{ is apart} ")$ .

If there is an  $s' > s$  so that  $\tau_1, \dots, \tau_s, \tau_{s'}$  is apart then we  
 can apply induction on  $m$ . Assume that  $f(X_1, \dots, X_s) \neq 0$ .  $f$  has  
 degree at most  $n$ . By lemma 4.11.5 there is an  $x \in L$  so that  
 $f(\tau_1(x), \dots, \tau_s(x)) \neq 0$ . Thus for the  $n \times n$ -matrix  $(\sigma_i \sigma_j(x))$  we  
 get  $f(\tau_1(x), \dots, \tau_s(x)) \neq \det(\sigma_i \sigma_j(x)) \vee \det(\sigma_i \sigma_j(x)) \neq 0$ .  
 If  $f(\tau_1(x), \dots, \tau_s(x)) \neq \det(\sigma_i \sigma_j(x))$  then there is an  $s' > s$   
 so that  $\tau_1, \dots, \tau_s, \tau_{s'}$  is apart and we can apply induction on  $m$ .  
 Therefore we may assume that  $\det(\sigma_i \sigma_j(x)) \neq 0$ . Now we shall  
 prove that  $\sigma_1(x), \dots, \sigma_n(x)$  is a normal sequence. Let  
 $\xi_1, \dots, \xi_n \in K$  be so that  $\xi_k \neq 0$  for some  $k$ . To prove:  
 $\xi_1 \sigma_1(x) + \dots + \xi_n \sigma_n(x) \neq 0$ . But this easily follows from the  
 fact that  $\sigma_1(\xi_1) \sigma_i \sigma_1(x) + \dots + \sigma_1(\xi_n) \sigma_i \sigma_n(x) \neq 0$  for some  $i$ .  
 As a corollary we get:

4.11.10. Theorem. Let  $\sigma_1, \dots, \sigma_n$  form a group of apart automorphisms  
 of  $L$  with fixed field  $K$ . Let  $K$  have an apart sequence of  $n+1$   
 elements. Then  $(L/K)$  has a normal basis  $\sigma_1(x), \dots, \sigma_n(x)$ .

Observe that in 4.11.10 the polynomial  $f = (X - \sigma_1(x)) \cdot \dots \cdot (X - \sigma_n(x))$   
 is prime and regular over  $K$  with  $\deg(f) = n$ . Moreover,  $f$  is  
 separable and  $L \cong K[\sigma_1(x)] \cong K[X]/(\neg C_f)$ .

#### 4.12 Subfields generated by subobjects

Let  $M$  be a field and  $G$  a group of automorphisms of  $M$  with fixed field  $K$ . Let  $D \subseteq M$  and  $\sigma_1, \dots, \sigma_n \in G$  so that  $\sigma_1, \dots, \sigma_n$  is apart on  $D$  and

$$\forall \tau \in G \left( \bigwedge_{1 \leq i \leq n} \tau \sigma_i \neq \sigma_i \right)$$

The cogroup  $\gamma(D) = \{\tau \in G \mid \tau|_D \neq \text{id}_D\}$  defines a field

$$L \equiv \varphi_G(\gamma(D)) \equiv \{\alpha \in M \mid \forall \tau \in G (\tau(\alpha) \neq \alpha \rightarrow \tau|_D \neq \text{id}_D)\}.$$

Let  $H \equiv (\neg \gamma(D))$ .  $H$  is a subgroup of  $G$ .

The tightness of the apartness relation and the apartness of  $\sigma_1, \dots, \sigma_n$  on  $D$  give that  $H \equiv \{\tau \in G \mid \tau|_D \equiv \text{id}_D\}$  and  $L \equiv \{\alpha \in M \mid \forall \tau \in H, \tau(\alpha) \equiv \alpha\}$ . Hence,  $D \subseteq L$ .  $\sigma_1, \dots, \sigma_n$  are representatives of the left cosets of  $H$  in  $G$ .  $K$  and  $M$  can also be defined by  $\varphi$  (see 4.7.4):

$$K \equiv \varphi_G(\phi) \text{ and } M \equiv \varphi_G(G^*) \text{ where } G^* \equiv \{\tau \in G \mid \tau \neq \text{id}\}.$$

Now we have the following inclusions:

$G$	$\{\text{id}\}$	$M$
$\cup$	$\cap$	$\cup$
$\gamma(D)$	$H$	$L \supseteq D$
$\cup$	$\cap$	$\cup$
$\phi$	$G$	$K$

Now we can prove:

4.12.1. Theorem. Let  $D, K, L, M, G, H$  and  $\sigma_1, \dots, \sigma_n$  be as mentioned above. Then we have:  $L$  is the smallest subfield of  $M$  containing  $D$ . Moreover,  $L$  satisfies:

1.  $[L:K] \equiv n$ .
2.  $L \equiv K[D]$ , the polynomial ring in  $D$ -elements over  $K$ .

Proof: if we take  $\sigma_1 \mathbb{N}, \dots, \sigma_n \mathbb{N} \in M^L$  and apply 4.9.1 we find at once that  $(L/K)$  has degree at least  $n$ . But we need slightly more. Therefore we shall consider the proof of theorem 4.9.1 in more detail.

Let  $D^*$  be the multiplicative monoid generated by  $D$  (use  $\mathbb{N}$  to define  $D^*$ ). We can find the sequence  $\omega_1, \dots, \omega_n$  in  $D^*$ , by following the proof of 4.9.1 step by step.

First:  $\omega_1 \equiv 1 \in D^*$ . Now the induction step of 4.9.1. We use theorem 4.8.2 in this case:

$$\sigma_1 \mathbb{N}^*, \dots, \sigma_n \mathbb{N}^* \in M^{D^*} \text{ are apart, thus free over } M.$$

Given  $\tau \equiv \xi_1 \sigma_1 + \dots + \xi_r \sigma_r$  there is an  $\omega_{r+1} \in D^*$  so that

$$\tau(\omega_{r+1}) \equiv \xi_1 \sigma_1(\omega_{r+1}) + \dots + \xi_r \sigma_r(\omega_{r+1}) \neq \sigma_{r+1}(\omega_{r+1}).$$

So  $\omega_1, \dots, \omega_n \in D^*$  and  $L \supseteq D^*$ , thus  $(L/K)$  has degree at least  $n$ .

It remains to prove that  $\omega_1, \dots, \omega_n$  generates  $(L/K)$ . Then it follows automatically that  $L$  is the smallest subfield containing  $D$  and that  $[L:K] \equiv n$ . Therefore we modify the proof of theorem 4.9.3.

The relevant point of that proof is: Let  $\tau \in G$ . Then  $\tau\sigma_1, \dots, \tau\sigma_n$  need not be a permutation of  $\sigma_1, \dots, \sigma_n$  anymore. But we do not need that in full. Apply  $\tau$  to  $A_n$ . Because of the facts

- i)  $A_n$  is invertible and
- ii)  $\forall \tau \in G \left( \sum_{1 \leq i \leq n} \tau \mathbb{N}^* \equiv \sigma_i \mathbb{N}^* \right)$

we have that the columns of the matrix

$$\tau A_n \equiv \begin{pmatrix} \tau\sigma_1(\omega_1) & \dots & \tau\sigma_n(\omega_1) \\ \vdots & & \vdots \\ \tau\sigma_1(\omega_n) & \dots & \tau\sigma_n(\omega_n) \end{pmatrix}$$

are a permutation of the columns of  $A_n$ .

With this modification, the proof of theorem 4.9.3 applies in the present situation. The generators  $\omega_1, \dots, \omega_n$  are in  $D^*$ , so we have  $L \equiv K[D]$ .

The automorphisms  $\sigma_1 \mathbb{N}_L, \dots, \sigma_n \mathbb{N}_L$  of the theorem above represent all possible morphisms  $\tau \mathbb{N}_L$  from  $L$  to  $M$  leaving  $K$  fixed, but with the restriction  $\tau \in G$ . We want to extend this result to all strongly extensional  $\tau: L \rightarrow M$  leaving  $K$  fixed.

4.12.2. Proposition. Let  $K, L, M$  be as above,  $\tau: L \rightarrow M$  a strongly extensional morphism leaving  $K$  fixed. Then we have  $\tau \equiv \sigma_i \mathbb{N}_L$ .

Proof: by induction on  $r$ , we can prove that there is an  $i \leq r$  so that  $\tau \equiv \sigma_i \mathbb{N}_L$ . From this follows, that at most  $\sigma_i$  may be equal to  $\tau$ . Therefore, assume  $\tau \not\equiv \sigma_i \mathbb{N}_L$ .

Then  $\sigma_1 \mathbb{N}_L, \dots, \sigma_n \mathbb{N}_L$ ,  $\tau$  is a sequence of strongly extensional apart morphisms  $\in M^L$ , leaving  $K$  fixed. Then  $(L/K)$  has degree at least  $n+1$  (theorem 4.9.1). Contradiction:  $\tau \not\equiv \sigma_i \mathbb{N}_L$ .

Thus  $\tau \equiv \sigma_i \mathbb{N}_L$  by the tightness of the apartness relation.

#### 4.13 Galois pairs

A Galois pair is a pair  $(M, G)$  with  $M$  a field and  $G$  an automorphism group. For the fixed field of  $G$  we usually write  $K$ .

Let  $\underline{M/K}$  be the collection of subfields  $L$  such that  $K \subseteq L \subseteq M$ .

Let  $\underline{G}$  be the collection of cogroups of  $G$ .

We take  $\gamma: \underline{M/K} \rightarrow \underline{G}$  and  $\varphi: \underline{G} \rightarrow \underline{M/K}$  as follows (see 4.7.4, 4.7.5):

$$\gamma(L) \equiv \{\sigma \in G \mid \exists \alpha \in L. \sigma(\alpha) \neq \alpha\}$$

$$\varphi(C) \equiv \{\alpha \in M \mid \forall \sigma \in G (\sigma(\alpha) \neq \alpha \rightarrow \sigma \in C)\}.$$

We give a connection between intermediate fields and cogroups rather than between intermediate fields and subgroups. The reason for that is the following. Think of groups and fields as Kripke models  $\underline{G}$  and  $\underline{K}$  over some partially ordered set  $\mathbb{P}$ .

For  $\alpha \leq \beta$  we have a morphism  $\sigma: G_\alpha \rightarrow G_\beta$ .  $G_\beta$  can be seen as an extension of  $G_\alpha$  since we have:  $\alpha \Vdash \dot{x} \neq 1 \Rightarrow \beta \Vdash \sigma(x) \neq 1$ . Thus if we go upwards in the poset  $\mathbb{IP}$  then the  $G_\alpha$  may increase.

The same holds for the  $K_\alpha$  of a field model  $\underline{K}$ .

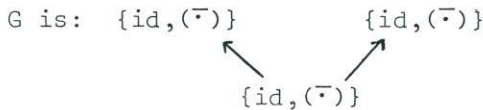
But the fixed field of a subgroup which should have to decrease if the subgroup increases, must be stable. In fact, fixed fields of subgroups are of the form  $(\neg C)$  with  $C$  a cofield, see 4.7.3. Therefore it is less probable to get a bijective correspondence between subgroups and subfields.

The following models show why cogroups give better connections.

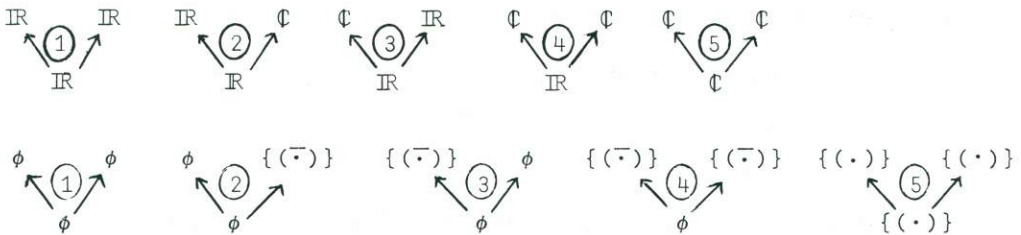
The models are constructed over the Kripke tree .



$K$  is the fixed field of the following automorphism group, where  $(\bar{\cdot})$  is complex conjugation:



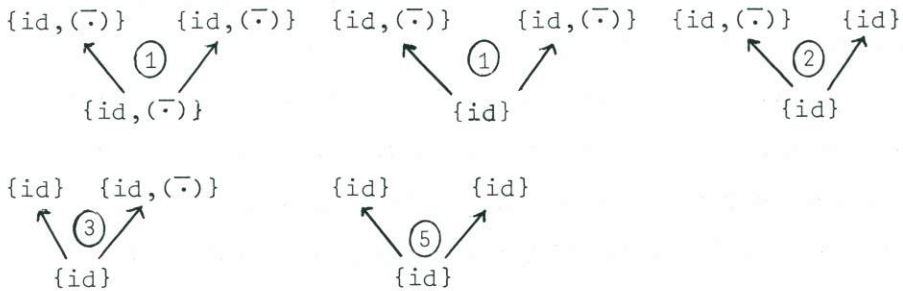
Then we can list the subfields of  $\underline{L/K}$  and the cogroups of  $\underline{G}$  over the bottom node of the Kripke tree (the other nodes are easy):



When we also make a list of the subgroups we see that we do not have a one one correspondence with the subfields (see the



numbers ①, ..., ⑤ ).



In this special case  $\varphi$  and  $\gamma$  are bijective and  $\varphi\gamma \equiv \text{id}$  and  $\gamma\varphi \equiv \text{id}$ . But in general this does not hold either. The only thing we have is that  $\varphi$  and  $\gamma$  form a so-called Galois connection (see [Ma 1]).

4.13.1. Proposition.  $\gamma \equiv \gamma\varphi\gamma$  and  $\varphi \equiv \varphi\gamma\varphi$ .

Proof: at least we have

$$L \subseteq \varphi\gamma(L) \quad \text{and} \quad \gamma\varphi(C) \subseteq C.$$

$\varphi$  and  $\gamma$  are inclusion order preserving, that means:

$$\forall L_1, L_2 \in \underline{M/K} (L_1 \subseteq L_2 \rightarrow \gamma(L_1) \subseteq \gamma(L_2)) \quad \text{and}$$

$$\forall C_1, C_2 \in \underline{G} (C_1 \subseteq C_2 \rightarrow \varphi(C_1) \subseteq \varphi(C_2)).$$

Thus  $\gamma(L) \subseteq \gamma\varphi\gamma(L)$  and  $\varphi\gamma\varphi(C) \subseteq \varphi(C)$ .

The inverse inclusions are also true. This completes the proof.

By definition of  $\varphi$  and  $\gamma$  we have

$$L \equiv \varphi\gamma(L) \leftrightarrow \forall \alpha \in M [\forall \sigma \in G (\sigma(\alpha) \neq \alpha \rightarrow \exists \beta \in L. \sigma(\beta) \neq \beta) \rightarrow \alpha \in L]$$

$$C \equiv \gamma\varphi(C) \leftrightarrow \forall \sigma \in G [\sigma \in C \rightarrow \exists \alpha \in M (\sigma(\alpha) \neq \alpha \wedge \forall \tau \in G (\tau(\alpha) \neq \alpha \rightarrow \tau \in C))]$$

The identities hold if and only if  $L$  is in the image of  $\varphi$  and  $C$  is in the image of  $\gamma$ .  $M$  and  $K$  are in the image of  $\varphi$  and  $G^* \equiv \{\sigma \in G \mid \sigma \neq \text{id}\}$  and  $\phi$  are in the image of  $\gamma$ .

For,  $\gamma(M) \equiv G^*$  and  $\varphi(G^*) \equiv M$   
and also  $\gamma(K) \equiv \phi$  and  $\varphi(\phi) \equiv K$ .

We want to extend these results to other intermediate fields. Therefore we have to add extra assumptions. It turns out that the following statement suffices to show that for stable subfields  $L$  we have  $\varphi\gamma(L) \equiv L$ . We have inserted double negations because it adds some extra generality that allows more models and it does not increase the technical difficulties. A Galois pair  $(M, G)$  is said to be of finite degree if  $G$  satisfies:

$$\exists n \in \mathbb{N} \forall \sigma_0, \dots, \sigma_n \in G (\neg \neg \bigwedge_{0 \leq i < j \leq n} \sigma_i \equiv \sigma_j).$$

4.13.2. Theorem. Let  $(M/G)$  be a Galois pair of finite degree. Let  $L \in \underline{M/K}$  be a stable subfield, i.e.  $L$  satisfies  $\forall \alpha \in M. (\neg \neg \alpha \in L \rightarrow \alpha \in L)$ . Then  $\varphi\gamma(L) \equiv L$ .

Proof: let  $\alpha \in M$  so that  $\forall \sigma \in G. (\sigma(\alpha) \neq \alpha \rightarrow \exists \beta \in L. \sigma(\beta) \neq \beta)$ .

To prove:  $\neg \neg \alpha \in L$ . There exists an  $n$  so that

$$\forall \sigma_0, \dots, \sigma_n \in G (\neg \neg \bigwedge_{0 \leq i < j \leq n} \sigma_i \equiv \sigma_j).$$

Now we can prove by induction on  $n-m$ :

$$\neg \neg \exists \sigma_1, \dots, \sigma_m (\bigwedge_{1 \leq i < j \leq m} \sigma_i \neq \sigma_j) \rightarrow \neg \neg \alpha \in L.$$

For  $n-m \equiv 0$  assume  $\neg \neg$  ("  $\sigma_1, \dots, \sigma_n$  is apart") Then we have

$\neg \neg$  ("  $\sigma_1, \dots, \sigma_n$  forms a group of apart automorphisms with fixed field  $K$ ")

and  $\neg \neg [ \bigwedge_{1 \leq i \leq n} (\sigma_i(\alpha) \neq \alpha \vee \sigma_i(\alpha) \equiv \alpha) \wedge \bigwedge_{1 \leq i \leq n} \sigma_i \upharpoonright L \neq \text{id} \upharpoonright L \vee \sigma \upharpoonright L \equiv \text{id} \upharpoonright L ]$

by the tightness of the apartness relation.

From this it easily follows, that  $\neg \neg$  (" $K[\alpha] \subseteq L$ ") thus  $\neg \neg \alpha \in L$ .

Induction step: Let  $m < n$  and assume that  $\neg \neg \exists \sigma_1, \dots, \sigma_m (\bigwedge_{1 \leq i < j \leq m} \sigma_i \neq \sigma_j)$  holds.

Then  $\sigma_1, \dots, \sigma_m$  generates a subgroup  $H \subseteq G$  with fixed field  $K^+$  and we have  $\neg(\sigma_1, \dots, \sigma_m \text{ is a group}) \vee$  "there is an automorphism  $\sigma_{m+1}$  so that  $\sigma_1, \dots, \sigma_{m+1}$  is apart". If  $\sigma_{m+1}$  exists such that  $\sigma_1, \dots, \sigma_{m+1}$  is apart then we apply induction. So we may assume  $\neg(\sigma_1, \dots, \sigma_m \text{ forms a group of apart automorphisms with fixed field } K^+)$ . By using the same method as above we have  $\neg(K^+[\alpha] \subseteq L^+)$  where  $L^+$  is the smallest field containing  $K^+$  and  $L$ . Assume  $\neg\alpha \in L$ . Then  $\neg\exists\beta \in K^+, \beta \in K$ . That implies that  $\neg(\text{there is an } \sigma_{m+1} \text{ so that } \sigma_1, \dots, \sigma_{m+1} \text{ is apart})$  holds. Applying induction we get  $\neg\alpha \in L$ . This contradicts the assumption  $\neg\alpha \in L$ . Thus  $\neg\alpha \in L$ . This completes the induction. Now take  $m = 1$ .

For a generalization of the result of 4.13.2 to all subfields, i.e. for having  $\varphi\gamma = \text{id}$ , we need still stronger conditions. The conditions that we give below suffice, but we expect that there exist many other conditions as well which imply that  $\varphi\gamma = \text{id}$ .

4.13.3. Theorem. Let  $(M, G)$  be a Galois pair,  $G = \{\tau_1, \dots, \tau_m\}$  and  $\forall\alpha \in M. \forall\sigma \in G. (\sigma(\alpha) \neq \alpha \vee \sigma(\alpha) = \alpha)$ . Then  $\varphi\gamma = \text{id}$ .

Proof: let  $\alpha \in M$  and  $L \in \underline{M/K}$  and

$$\forall\sigma \in G. (\sigma(\alpha) \neq \alpha \rightarrow \exists\beta \in L. \sigma(\beta) \neq \beta), \text{ i.e. } \alpha \in \varphi\gamma(L).$$

To prove:  $\alpha \in L$ .

Let  $\sigma_1, \dots, \sigma_n \in G$  be the automorphisms so that  $\sigma_i(\alpha) \neq \alpha$ . For each  $\sigma_i$  there is a  $\beta_i \in L$  so that  $\sigma_i(\beta_i) \neq \beta_i$ .

By 4.12.1 we find that  $\varphi\gamma(K[\alpha]) = K[\alpha]$  and

$\varphi\gamma(K(\beta_1, \dots, \beta_n)) = K(\beta_1, \dots, \beta_n)$ . Since  $\gamma(K[\alpha]) \subseteq \gamma(K(\beta_1, \dots, \beta_n))$

we have  $K[\alpha] \subseteq K(\beta_1, \dots, \beta_n) \subseteq L$ ; Thus  $\alpha \in L$ .

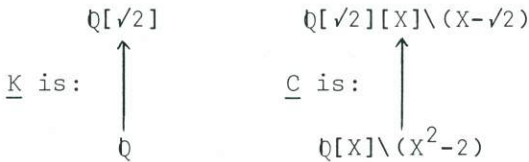
## 5. PRIMALITY AND INVERTIBILITY

In this chapter we consider invertibility problems in extensions  $K[\alpha]$  of a field  $K$ .

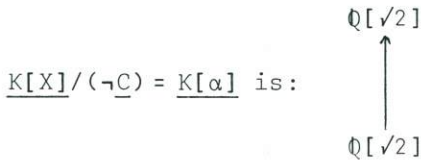
### 5.1 Extensions by one element

If  $K[\alpha]$  is a field then there is a minimal coideal  $C \subseteq K[X]$  such that  $K[\alpha] \cong K[X]/(\neg C)$ . Is  $C$  of the form  $C_f$  for some  $f \in K[X]$ ? The only theorem in that direction is 4.5.8. Unfortunately we cannot expect much more without strong extra assumptions as follows from the countermodel below.

5.1.1. Example. Let  $\underline{K}$  and  $\underline{C}$  be the following field model and coideal in  $K[X]$ :

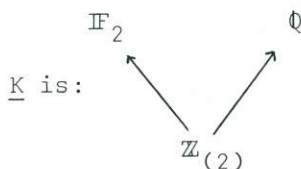


In this example  $\underline{C}$  is equal to the intersection  $\bigcap \{C_f \mid f \in K[X], f(\alpha) = 0\}$  but  $\underline{C}$  is not equal to any  $C_f$  separately. Observe that  $\underline{K}$  satisfies  $\forall x (x \neq 0 \vee x = 0)$  and that



Another problem is: let  $K(\beta)$  be a field,  $\beta \neq 0$ , and assume that there is an  $f \in K[X]$  such that  $f$  has invertible leading coefficient and such that  $f(\beta) = 0$ . Is  $K[\beta]$  a field? The answer is no. And again there is an easy countermodel.

5.1.2. Example. Let  $\underline{K}$  be the field model of 4.5.6.

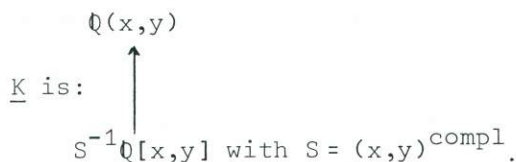


$\underline{K}[\alpha] = \underline{K}[X]/(\neg C_f)$  with  $f = 2X^2 + X + 1$ .  $\underline{K}[\alpha]$  is a field (see 5.2.10(1)).

Let  $\beta = \alpha^{-1}$ . Then  $\underline{K}(\beta) = \underline{K}[\alpha]$  and  $\beta^2 + \beta + 2 = 0$  holds. But  $\underline{K}[\beta]$  is not a field because we do not have that  $\alpha \in \underline{K}[\beta]$  (observe that all elements of  $\underline{K}[\beta]$  can be written as  $a\beta + b$  with  $a, b \in \underline{K}$ ).

We shall restrict ourselves to integral domains  $\underline{K}[\alpha] = \underline{K}[X]/(\neg C_f)$ ,  $f$  prime. In contrast to the situation in classical mathematics  $\underline{K}[\alpha]$  need not be a field if  $f$  is not regular.

5.1.3. Example. Let  $\underline{K}$  be the following field model.



The elements  $x$  and  $y$  are transcendental over  $\mathbb{Q}$ . Let  $f = xX^2 + X + 1$  and  $g = yX + 1$  be polynomials over  $\underline{K}$ . One easily verifies that  $f$  is prime and that  $f$  and  $g$  are relatively prime in the model. Thus  $\underline{K}[\alpha] = \underline{K}[X]/(\neg C_f)$  is an integral domain with  $g(\alpha) \neq 0$ . But  $\underline{K}[\alpha]$  is not a field because we do not have an inverse element for  $g(\alpha) = y\alpha + 1$ . For, if  $g(\alpha)$  is invertible in  $\underline{K}[\alpha]$  we may assume that  $g(\alpha)^{-1}$  is of the form  $\alpha^m(a\alpha + b)$  with  $a, b \in \underline{K}$ , cf. 4.6.6. Over  $\mathbb{Q}(x,y)$  in the top node of the Kripke-model we find for all  $n$  unique  $a_n, b_n \in \mathbb{Q}(x,y)$  such that  $\alpha^n(a_n\alpha + b_n)(y\alpha + 1) = 1$ .  $a_n$  and  $b_n$  satisfy the equation

$$\begin{pmatrix} a_n \\ b_n \end{pmatrix} = \begin{pmatrix} 0 & -x \\ 1 & -1 \end{pmatrix}^n \begin{pmatrix} (-xy)/(x+y^2-y) \\ (x-y)/(x+y^2-y) \end{pmatrix}$$

Since  $x+y^2-y$  essentially occurs in the denominator of

$\det \begin{pmatrix} a_1 & a_0 \\ b_1 & b_0 \end{pmatrix}$  and since  $\det \begin{pmatrix} 0 & -x \\ 1 & -1 \end{pmatrix} = x$  it follows that  $x+y^2-y$  essentially occurs in the denominator of  $a_n$  or  $b_n$  for all  $n$ . Thus also in the denominator of  $a$  or  $b$ . But  $x+y^2-y$  is not invertible in the bottom node of  $\underline{K}$ . Contradiction.  $g(\alpha)$  is not invertible.

Let  $K[\alpha] \equiv K[X]/(\neg C_f)$  with  $f \equiv a_0 + \dots + a_n X^n$  prime,  $a_m \neq 0$ . If  $m < n$  then  $K[\alpha]$  need not be a field. But it is very much like a field. As illustration of that statement we shall list some properties of  $K[\alpha]$  below.

5.1.4. Some useful properties. Instead of integral domains  $K[\alpha]$  as above we consider rings  $K[\alpha]$  with some  $g(\alpha)$  which is strongly zero divisor free. This adds some generality to the results and it does not increase the length of the proofs. Let  $f, g \in K[X]$  be relatively prime. Then  $f \in C_X \vee g \in C_X$  holds. Because of symmetry we may assume  $f \in C_X$ . Then  $f(0) \neq 0$ . Let  $f \equiv a_0 + \dots + a_n X^n$ ,  $a_m \neq 0$ . We may assume that  $a_0 \equiv 1$ . Let  $K[\alpha] \equiv K[X]/(\neg C_f)$ . Then  $g(\alpha)$  is strongly zero divisor free, i.e. we have

(1)  $\forall h(\alpha). (h(\alpha) \neq 0 \rightarrow g(\alpha)h(\alpha) \neq 0)$ , (cf. remark following 4.4.9).

There are  $h, k \in K[X]$  such that  $hf + kg \equiv 1$  if and only if  $g(\alpha)$  is invertible (with inverse  $k(\alpha)$ ). Thus if we want to find  $h, k$  such that  $hf + kg \equiv 1$  as in classical algebra, then it is enough to find an inverse element for  $g(\alpha)$ . So we come to the invertibility problem for  $g(\alpha)$ .  $g(\alpha)$  need not be invertible as follows from 5.1.3 but we have some approximate results.

We can show: there is an  $s \geq m$  such that  $a_s \neq 0$  and for  $f^{\#} \equiv a_0 + \dots + a_s X^s$  there are  $h, q \in K[X]$  such that  $gh \equiv qf^{\#} + 1$ .

Proof: analogous to 4.5.7.

Write  $gh \equiv qf + 1 - r$  with  $r \equiv q(f - f^{\#})$ . This gives:

(2) There are  $h, r \in K[X]$  such that we have  $r \neq 0 \rightarrow \exists m' > m. a_{m'} \neq 0$

and  $g(\alpha)h(\alpha) \equiv 1-r(\alpha)$ .

As in 4.6.6 we can write  $g(\alpha) \equiv \alpha^p k(\alpha)$  for some  $p \in \mathbb{N}$  and some  $k \equiv k_0 + \dots + k_{n-1} X^{n-1} \in K[X]$  satisfying  $k_i \neq 0 \rightarrow \exists j > i, a_j \neq 0$ . Then for  $k(\alpha), \alpha^{-1}k(\alpha), \dots, \alpha^{-n+1}k(\alpha)$  there are polynomials  $k^{(1)}, \dots, k^{(n)} \in K[X]$  each of degree at most  $n-1$  such that  $\alpha^{-i+1}k(\alpha) \equiv k^{(i)}(\alpha)$ . Let  $A$  be the matrix  $A \equiv (k^{(1)}, \dots, k^{(n)})$  using the coefficients of the polynomials as column vectors,  $\det A \equiv \xi$ . Then by Cramer's rule there exists a vector  $v \in K^n$  such that  $Av \equiv (\xi, 0, \dots, 0)$ . Let  $c \equiv v_0 + \dots + v_{n-1} X^{n-1}$ . Then  $c(\alpha)k(\alpha)\alpha^{-n+1} \equiv \xi$ . Thus for some  $l \in K[X]$  with  $l(\alpha) \equiv c(\alpha)\alpha^{-p-n+1}$  we have  $g(\alpha)l(\alpha) \equiv \xi$ . Assume  $a_n \neq 0$ . Since  $k(\alpha)$  is strongly zero divisor free we find  $\forall w \in K^n (w \neq 0 \rightarrow Aw \neq 0)$ . Thus  $A$  is invertible and  $\xi \neq 0$ . Conclusion:

(3) There is an  $l \in K[X]$  and a  $\xi \in K$  such that we have  $a_n \neq 0 \rightarrow \xi \neq 0$  and  $g(\alpha)l(\alpha) \equiv \xi$ .

Assume that there is an  $m' \in \mathbb{N}$  such that  $\xi | r(\alpha)^{m'}$ . Then  $m' \leq 2^{n'}$  for some  $n' > 0$  and  $\xi t(\alpha) \equiv r(\alpha)^{2^{n'}}$  for some  $t \in K[X]$ . Then we have  $g(\alpha)\underline{h}(\alpha) \equiv g(\alpha)h(\alpha)(1+r(\alpha))(1+r(\alpha)^2) \dots (1+r(\alpha)^{2^{n'-1}}) \equiv 1-r(\alpha)^{2^{n'}}$  and  $g(\alpha)(\underline{h}(\alpha)+l(\alpha)t(\alpha)) \equiv 1$ . Thus  $g(\alpha)$  is invertible.

(4) If  $\xi | r(\alpha)^{m'}$  for some  $m'$  then  $g(\alpha)$  is invertible.

Example: Let  $f, g$  be as in example 5.1.3,  $\underline{K}[\alpha] = \underline{K}[X]/(\neg C_f)$ . When we apply 5.1.4 to  $g(\alpha) \equiv y\alpha+1$  we find that

$$\frac{1}{1-y}(y\alpha+1) \equiv 1 - \frac{xy}{1-y}\alpha^2$$

and

$$(-xy\alpha+x-y)(y\alpha+1) \equiv x+y^2-y.$$

Thus  $r(\alpha) \equiv \frac{xy}{1-y}\alpha^2$  and  $\xi \equiv x+y^2-y$ . Observe that in the bottom node of the Kripke-model  $\underline{K}$  we do not have  $\xi | r(\alpha)^{m'}$  for any  $m'$ .

5.2  $C_i$ -fields

In this section we consider fields satisfying the extra axiom

$$D: \forall x, y. x|y \vee y|x.$$

Using D we can find the greatest common divisor (gcd) of finite sequences  $x_1, \dots, x_n$  of elements of  $K$ . Another consequence of D is:

5.2.1. Proposition. If a field  $K$  satisfies D then it also satisfies  $xy \equiv 0 \rightarrow x \equiv 0 \vee y \equiv 0$ .

With help of D we can diagonalize matrices in the following sense. We call a matrix  $B \equiv (\beta_{i,j})$  a diagonal matrix if  $\beta_{i,j} \equiv 0$  for all pairs  $i \neq j$ .

5.2.2. Proposition. Let  $K$  satisfy D and let  $A$  be an  $m \times n$ -matrix over  $K$ . Then there is an  $m \times n$ -diagonal matrix  $B_1$  and an  $n \times n$ -matrix  $B_2$  with  $\det B_2 \equiv 1$  such that  $A \equiv B_1 B_2$ .

Proof: use that each row  $\alpha_{i,1}, \dots, \alpha_{i,n}$  contains a gcd.

With axiom D and some extra axioms we shall show that for all  $f, g \in K[X]$  we have  $f$  and  $g$  relatively prime if and only if there are  $h, k \in K[X]$  such that  $hf + kg \equiv 1$ . This implies that for prime  $f \in K[X]$   $K[\alpha] \equiv K[X]/(\neg C_f)$  is a field. The main lemma for this result is:

5.2.3. Lemma. Let  $K$  satisfy D, let  $f, g \in K[X]$  be relatively prime with  $f \equiv a_0 + \dots + a_n X^n$ ,  $a_m \neq 0$  and  $K[\alpha] \equiv K[X]/(\neg C_f)$ . Then there are  $\xi, \eta \in K$  such that  $(\eta \neq 0 \vee \xi \equiv 0) \rightarrow (\exists s > m. a_s \neq 0 \vee a_n \equiv 0)$  and  $\forall i \in \mathbb{N} (\xi | \eta^i \rightarrow "g(\alpha) \text{ is invertible}").$

Proof: From 5.1.4 we get: there are  $h, r, l \in K[X]$  and  $\xi \in K$  such



that  $g(\alpha)h(\alpha) \equiv 1 - r(\alpha)$ ,  $g(\alpha)l(\alpha) \equiv \xi$  and if  $r \neq 0$  then  $a_s \neq 0$  for some  $s > m$  and if  $\xi \equiv 0$  then  $a_n \equiv 0$ . Moreover, if  $\xi | r(\alpha)^i$  for some  $i$  then  $g(\alpha)$  is invertible.

Let  $\eta$  be the gcd of the coefficients of  $r \in K[X]$ . Then  $r \equiv \eta \underline{r}$  with  $\underline{r} \neq 0$ . If  $\eta \neq 0$  then  $r \neq 0$  thus we have  $(\eta \neq 0 \vee \xi \equiv 0) \rightarrow (\exists s > m. a_s \neq 0 \vee a_n \equiv 0)$ . Let  $i \in \mathbb{N}$ . If  $\xi | \eta^i$  then  $\xi | r(\alpha)^i$  and  $g(\alpha)$  is invertible by 5.1.4(4). Thus we have proved  $\forall i \in \mathbb{N} (\xi | \eta^i \rightarrow "g(\alpha) \text{ is invertible}").$

5.2.4. Consider the following principles.

$$C_1 \quad \forall y, x \exists n \in \mathbb{N} (x^n | y \rightarrow x \neq 0 \vee y \equiv 0),$$

$$C_2 \quad \forall y \exists n \in \mathbb{N} \forall x (x^n | y \rightarrow x \neq 0 \vee y \equiv 0).$$

We call fields that satisfy  $C_1$  and  $D$   $C_1$ - $D$ -fields.

One easily verifies that  $C_2$  implies  $C_1$ .

5.2.5. Theorem. Let  $K$  be a  $C_1$ - $D$ -field. Let  $f, g \in K[X]$  be relatively prime. Then there are  $h, k \in K[X]$  such that  $hf + kg \equiv 1$ .

Proof: we have  $f \in C_X \vee g \in C_X$ . By symmetry we may assume  $f \in C_X$ . Then  $f(0) \neq 0$  and thus we may assume  $f(0) \equiv 1$ . Write  $f$  as  $f \equiv a_0 + \dots + a_n X^n$  and let  $K[\alpha] \equiv K[X] / (\neg C_f)$ . By induction on  $(n-m)$  we show: if  $a_m \neq 0$  then  $g(\alpha)$  is invertible in  $K[\alpha]$ .

The case  $n-m \equiv 0$  follows from theorem 4.5.4.

Induction step: let  $a_m \neq 0$ . By lemma 5.2.3 there are  $\xi, \eta \in K$  such that  $\eta \neq 0 \vee \xi \equiv 0$  implies  $\exists s > m. a_s \neq 0 \vee a_n \equiv 0$  and if  $\xi | \eta^i$  for some  $i$  then  $g(\alpha)$  is invertible.

By axiom  $C_1$  there is a number  $p$  such that  $\eta^p | \xi$  implies  $\eta \neq 0 \vee \xi \equiv 0$ . By axiom  $D$  we have  $\eta^p | \xi \vee \xi | \eta^p$ . If  $\xi | \eta^p$  then  $g(\alpha)$  is invertible. If  $\eta^p | \xi$  then  $\eta \neq 0 \vee \xi \equiv 0$  holds. Thus we have  $\exists s > m. a_s \neq 0 \vee a_n \equiv 0$  and we apply induction:  $g(\alpha)$  is invertible.

5.2.6. Corollary. Let  $K$  be a  $C_1D$ -field,  $f \in K[X]$ ,  $f \neq 0$ ,  $K[\alpha] \cong K[X]/(\neg C_f)$ . Then we have:

$f$  is prime  $\Leftrightarrow K[\alpha]$  is a field.

Proof: let  $g \in K[X]$ . By 4.4.9 we have  $g(\alpha) \neq 0$  if and only if  $f$  and  $g$  are relatively prime. Now apply 5.2.5.

One thing that is missing in 5.2.5 compared to 4.5.4 is that we do not have a bound on the degrees of  $h$  and  $k$ , see example 5.2.10(1). Another difference between 5.2.5 and 4.5.4 is that we do not have a uniqueness condition on  $h$  and  $k$ . But we have a weak uniqueness in the following sense.

5.2.7. Proposition. Let  $K$  be an arbitrary field. Let  $f, g \in K[X]$  be relatively prime,  $f \equiv a_0 + \dots + a_n X^n$ ,  $f(0) \neq 0$ . Let  $m \in \mathbb{N}$ . Then there is at most one pair  $h, k \in K[X]$  such that  $k \equiv X^m k^{(1)}$  where  $k^{(1)}$  satisfies  $\forall i \in \mathbb{N} (k_i^{(1)} \neq 0 \rightarrow \exists j > i. a_j \neq 0)$  and such that  $hf + kg \equiv 1$ .

Proof: we only have to show the existence of at most one  $k$ . Let  $K[\alpha] \cong K[X]/(\neg C_f)$ . Let  $k \equiv X^m k^{(1)}$  and  $l \equiv X^m l^{(1)}$  be so that  $g(\alpha) \alpha^m k^{(1)}(\alpha) \equiv g(\alpha) \alpha^m l^{(1)}(\alpha) \equiv 1$ . Then  $k^{(1)}(\alpha) \equiv l^{(1)}(\alpha)$  and  $k^{(1)} - l^{(1)} \in (\neg C_f)$ . Assume  $k^{(1)} \neq l^{(1)}$ . Then  $k_i^{(1)} \neq l_i^{(1)}$  for some  $i$  and thus  $k_i^{(1)} \neq 0 \vee l_i^{(1)} \neq 0$  holds. Thus  $a_j \neq 0$  for some  $j > i$ . This implies that we have  $\forall i \in \mathbb{N} ((k^{(1)} - l^{(1)})_i \neq 0 \rightarrow \exists j > i. a_j \neq 0)$ . So by 4.3.8(c)  $k^{(1)} - l^{(1)} \in C_f$ . Contradiction.  $k^{(1)} \equiv l^{(1)}$ .

Observe that from 5.2.5 and 4.6.6 it follows that if  $K$  is a  $C_1D$ -field then for some  $m \in \mathbb{N}$  there is a solution  $h, k$  where  $k \equiv X^m k^{(1)}$  is as described in 5.2.7.

If for some  $m$  we have a  $k \equiv X^m k^{(1)}$  as in 5.2.7 such that

$g(\alpha)\alpha^{m_k(1)}(\alpha) \equiv 1$ , then there is a  $k^{(2)} \in K[X]$  such that  $k^{(2)}(\alpha) \equiv \alpha^{-1}k^{(1)}(\alpha)$  and  $X^{m+1}k^{(2)}$  satisfies the conditions of 5.2.7.

Iterating this procedure we find that if we have a special solution  $X^{m_k(1)}$  for some  $m$  then we have a special solution for all  $m' \geq m$ .

We have some constructions of new fields from old ones. We shall show that they preserve combinations of the axioms  $D$ ,  $C_1$  and  $C_2$ .

5.2.8. Theorem. Let  $K$  be a field and  $K(X)$  the field of rational functions over  $K$ . If  $K$  satisfies one of the axioms  $D$ ,  $D \wedge C_1$  or  $D \wedge C_2$  then  $K(X)$  does so too.

Proof: for  $D$ , use the fact that the numerator  $f$  of an element  $\frac{f}{g} \in K(X)$  can be written as  $f \equiv \eta h$  with  $\eta \in K$  and  $h \neq 0$ . The rest is trivial.

5.2.9. Theorem. Let  $K$  be a  $C_1D$ -field,  $f \in K[X]$ ,  $f$  prime and  $K[\alpha] \equiv K[X]/(\neg C_f)$ . Then  $K[\alpha]$  is also a  $C_1D$ -field.

Proof: from 5.2.6 it follows that  $K[\alpha]$  is a field. Now we shall prove the following claim:

each  $g(\alpha) \in K[\alpha]$  can be written as  $\zeta r(\alpha)$  with  $\zeta \in K$  and  $r(\alpha) \neq 0$ .

The remaining details concerning  $D \wedge C_1$  then follow easily from the property  $D \wedge C_1$  for  $K$ .

Proof of the claim: let  $f \equiv a_0 + \dots + a_n X^n$ . We may assume that  $f(0) \equiv 1$ . By induction on  $(n-m)$  we shall prove: if  $a_m \neq 0$  then the claim holds. The case  $n-m \equiv 0$  is easy. We continue with the induction step. Let  $a_m \neq 0$  and  $g(\alpha) \in K[\alpha]$ .  $\eta$  is the gcd of  $a_{m+1}, \dots, a_n$ . By induction on  $p$  we show

("g(α) ≡ μz(α) with z(α) ≠ 0, μ ∈ K") ∨ ("g(α) ≡ η<sup>p</sup>u(α) for some u(α)").

The case p = 0 is trivial. Induction step: we may assume that

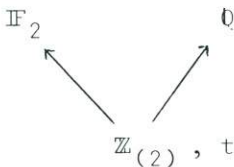
g(α) ≡ η<sup>p</sup>u(α) holds, otherwise there is nothing to prove. We can write g(α) ≡ η<sup>p</sup>α<sup>m'</sup>x(α) for some m' and x ≡ x<sub>0</sub> + ... + x<sub>n-1</sub>X<sup>n-1</sup>.

Let (.)<sub>f</sub>\* ≡ (.)<sub>f</sub>\*: P<sub>n</sub> → P<sub>n</sub> be a map according to 4.3.6 and with corresponding invertible submatrix B with a<sub>s</sub> ≡ f<sub>s</sub> ≠ 0 on the diagonal such that s ≥ m. Then we can write x ≡ (x)\*f + y with y ≡ y + ȳ according to 4.3.8(d). Let γ be the gcd of the coefficients of y. Then y ≡ γz with z ≠ 0. ȳ ≡ γz̄ and ȳ ≡ γz̄. From z ≠ 0 we derive z̄ ≠ 0 ∨ z̄ ≠ 0. Assume z̄ ≠ 0. Then z(α) ≠ 0 ∨ z̄(α) ≠ 0. If z(α) ≠ 0 then x(α) ≡ y(α) ≡ γz(α) and g(α) ≡ η<sup>p</sup>γα<sup>m'</sup>z(α) with α<sup>m'</sup>z(α) ≠ 0. So assume z̄ ≠ 0. The coefficients of ȳ are divisible by η thus we get η | γ. Conclusion: x(α) ≡ ηu(α) for some u ∈ K[X]. So g(α) ≡ η<sup>p+1</sup>α<sup>m'</sup>u(α). This completes the induction on p.

By 5.1.4(3) there is an l ∈ K[X] and a ξ ∈ K such that ξ ≡ 0 implies a<sub>n</sub> ≡ 0 and g(α)l(α) ≡ ξ. By axiom C<sub>1</sub> there is a p ∈ ℕ such that η<sup>p</sup> | ξ implies η ≠ 0 ∨ ξ ≡ 0. Now we may assume that g(α) ≡ η<sup>p</sup>u(α) for some u ∈ K[X]. Thus η<sup>p</sup>u(α)l(α) ≡ ξ. There is a q ∈ K[X] such that η<sup>p</sup>ul + qf ≡ ξ. Let ε be the gcd of the coefficients of q: q ≡ εq̄ with q̄ ≠ 0. From the fact that q̄f ≠ q̄(0)f(0) it follows that η<sup>p</sup> | ε. Thus also η<sup>p</sup> | ξ and η ≠ 0 ∨ ξ ≡ 0. Then we have ∃ s > m. a<sub>s</sub> ≠ 0 ∨ a<sub>n</sub> ≡ 0 and we can apply induction on n-m.

### 5.2.10. Examples.

(1) Let K be the following field model.



$\mathbb{Z}_{(2)}$ , the localization to the prime ideal (2).

Then one easily verifies that K satisfies the axioms D and C<sub>2</sub>.

Let  $f \equiv 2X^2 + X + 1$ . Then  $f$  is prime and  $\underline{K}[\alpha] = \underline{K}[X]/(\neg C_f)$  is a field. For instance we have  $6\alpha + 1 \neq 0$  and  $-\alpha^4(6\alpha + 1) \equiv 1$ . In fact there is no  $f \in \mathbb{Z}_{(2)}[X]$  with degree at most 3 such that  $f(\alpha)(6\alpha + 1) \equiv 1$ .

(2) Let  $R$  be a unique factorization domain from classical algebra. Let  $R$  have infinitely many prime numbers. Then we construct the following sheaf model. As topological space we have  $X = \{(p) \subseteq R \mid p \text{ is prime}\}$  with the cofinite sets as open sets. For open  $U \subseteq X$ ,  $U = X \setminus \{(p_1), \dots, (p_n)\}$ , we take as ring of sections above  $U$ :  $R(U) = S^{-1}R$  with  $S$  the multiplicative set generated by  $p_1 \cdot \dots \cdot p_n$ . Call this sheaf model  $\underline{R}$ . Then  $\underline{R}$  is a local ring model satisfying  $D$  (observe that these axioms are of type  $P$  as defined in 1.3.1) since as stalk structures in the points  $\alpha = (p)$  we have the local rings  $R_{(p)}$ . Each  $y \in R(U)$  with  $y \neq 0$  can be written as  $y = \frac{d}{e}$  where  $d, e \in R$  and  $d$  has a prime number decomposition  $d = p_1^{n_1} \cdot \dots \cdot p_m^{n_m}$ . Let  $n = \max(n_1, \dots, n_m)$ . Then one easily verifies that for all  $x \in R(V)$ ,  $V \subseteq U$ , we have

$$\|x^{n+1} \mid y \neq 0 \vee y \equiv 0\| \supseteq V.$$

Thus  $\underline{R}$  satisfies  $C_2$ . Finally, let  $\alpha = (p) \in \|\neg y \neq 0\|$  for  $y = \frac{d}{e} \in R(U)$ ,  $\alpha \in U$ . Thus  $p \mid d$ . Then  $\|\neg y \neq 0\|$  is an inhabited open set, thus cofinite in  $X$ . So there are infinitely many prime ideals  $(p)$  such that  $p \mid d$ . Thus  $d = 0$  and  $y = 0$ . This implies  $\alpha \in \|y \equiv 0\|$ . Conclusion:  $\underline{R}$  is a field model satisfying  $D$  and  $C_2$ . Observe that this model satisfies more extra properties. Since each open subset  $U \subseteq X$  of the infinite set  $X$  is cofinite or empty we find that for each formula  $\varphi$   $\underline{R}$  satisfies  $\neg \varphi \vee \neg \neg \varphi$ , e.g. in  $\underline{R}$   $\forall x (x \equiv 0 \vee \neg x \equiv 0)$  holds.

(3) Let  $\underline{C} = C(\mathbb{C}, \mathbb{C})$  be the sheaf of holomorphic functions. Then  $\underline{C}$  is a field model. Since sections  $a, b$  in a neighbourhood of some  $\zeta$  can be written as power series  $a(\xi) = a_m(\xi - \zeta)^m + a_{m+1}(\xi - \zeta)^{m+1} +$

$+a_{m+2}(\xi-\zeta)^{m+2}+\dots$  and  $b(\xi) = b_n(\xi-\zeta)^n + b_{n+1}(\xi-\zeta)^{n+1} + b_{n+2}(\xi-\zeta)^{n+2} + \dots$   
 we see that  $\underline{C}$  satisfies  $D \wedge C_2$ .

By interpreting intuitionistic theorems in their sheaf models we have an alternative method for deriving results concerning classical structures. As an illustration of such a procedure we shall use theorem 5.2.5 to derive a property of rings, using the sheaf construction of 5.2.10(2). This property is chosen for its illustrative nature.

5.2.11. Example. Let  $R$  be a unique factorization domain from classical algebra. Assume that  $R$  has infinitely many primes. Let  $f, g \in R[X]$  such that for each maximal ideal  $M \subseteq R$  we have  $\gcd(\bar{f}, \bar{g}) = \bar{1}$  in  $(R/M)[X]$ . Then there are  $h, k \in R[X]$  such that

$$hf + kg = 1.$$

Proof: let  $\underline{R}$  be the sheaf model of 5.2.10(2). From the conditions on  $f$  and  $g$  it follows that  $\underline{R} \models "f \text{ and } g \text{ are relatively prime}"$ . Thus we have  $\underline{R} \models \exists h, k \in K[X]. hf + kg \equiv 1$ . From the interpretation of the existential quantifier  $\exists$  (see 1.3) it follows that we get the  $h$  and  $k$  only as a collection of local sections. The problem to find global  $h, k$  (and thus  $h, k \in R[X]$ ) essentially makes the proof more complicated.

There are open  $U, V \subseteq X$  such that  $U \cup V = X$  and  $\llbracket f(0) \neq 0 \rrbracket = U$  and  $\llbracket g(0) \neq 0 \rrbracket = V$ . Here  $X \setminus U = \{(p) \subseteq R \mid p \text{ is prime and } p \mid f(0)\}$  and  $X \setminus V = \{(p) \subseteq R \mid p \text{ is prime and } p \mid g(0)\}$ . Then by 5.2.7 we have a cover  $\{U_m \mid m \in \mathbb{N}\}$  of  $U$  such that we find unique  $h, k$  with  $k \equiv X^m k^{(1)}$  above  $U_m$ , where  $X^m k^{(1)}$  is as described in 5.2.7. By the compactness of  $U$  we can find a fixed  $m$  such that we can choose  $U_m = U$ . By the sheaf property we can glue the local - unique -  $h, k$  with  $k \equiv X^m k^{(1)}$  to  $h_U, k_U \in R(U)[X]$ . So  $h_U f + k_U g = 1$  where we

allow divisors of  $f(0)$  in the denominators of the coefficients of  $h_U$  and  $k_U$ . So there is an  $a_U \in R$  and an  $n \in \mathbb{N}$  such that  $a_U h_U \in R[X]$ ,  $a_U k_U \in R[X]$  and  $a_U h_U f + a_U k_U g = f(0)^n$ . In the same way we get an equation  $a_V h_V f + a_V k_V g = g(0)^m$ . From the conditions on  $f$  and  $g$  it follows that the ideal  $(f(0), g(0)) \subseteq R$  is not contained in any maximal ideal  $M \subseteq R$ . Thus  $(f(0), g(0)) = R$  and so  $(f(0)^n, g(0)^m) = R$ . There are  $s, t \in R$  such that  $sf(0)^n + tg(0)^m = 1$ . Now take  $h = sa_U h_U + ta_V h_V$  and  $k = sa_U k_U + ta_V k_V$ . Then  $h, k \in R[X]$  and  $hf + kg = 1$ .

5.2.12. Remark. Theorem 5.2.5 can be generalized to local rings  $R$  satisfying

$$D \quad \forall x, y (x \mid y \vee y \mid x),$$

$$C_1^- \quad \forall y \exists n \in \mathbb{N} \forall x (x^n \mid y \rightarrow x \neq 0 \vee \neg y \neq 0),$$

$$\text{Nil} \quad \forall x (\neg x \neq 0 \rightarrow \exists n \in \mathbb{N} x^n = 0).$$

For, if  $f, g \in R[X]$  are relatively prime, then there are  $h, k \in R[X]$  such that  $\neg hf + kg = 1$ . Let  $d \equiv 1 - hf - kg$ . If  $R$  satisfies Nil then  $R[X]$  satisfies Nil. Thus since  $\neg d = 0$  we have an  $n$  such that  $d^{2^n} = 0$ . Let  $\underline{h} \equiv h(1+d)(1+d^2) \cdots (1+d^{2^{n-1}})$  and  $\underline{k} \equiv k(1+d)(1+d^2) \cdots (1+d^{2^{n-1}})$ . Then we have  $\underline{h}f + \underline{k}g = 1$ .

*Index*

AK-field	45
apartness	8
apart sequence	104
Austauschsatz	51
automorphism	23
balanced	34
bijective	23
$C_f$	79
character	104
cofield	102
cogroup	24
coideal	26
comodule	35
degree (module)	53
degree (polynomial)	77
depend on	47
derivative	96
determinant	57
dimension	53
embedding	23
equivalent (sequences of vectors)	47
fixed field	102
fixed field of a sequence	105
fixed group	103
free	49
free from	47
general module	46



Generators Theorem	64
geometric	15,17
group of units	25
H-field	45
independent	49
independent of	47
injective	23
isomorphism	23
Kripke-model	18
minimal coideal	31
module	22,46,47
morphism	22
N	15
normal basis	113
normal cogroup	24
P	15
polynomial ring	25
power series ring	25
prime coideal	28
prime (polynomial)	90
$Q(R)$	31
quotient field	30
rank	55
regular	77
separable	96
stalk	12
strict	7
strongly dependent	49
strongly extensional	9

strongly non-trivial (coideal)	26
strong module	47
strong morphism	22
structure	13,19
surjective	22
tight	8
total	7
weakly dependent	49
W-field	45
zero divisor free	78
$\neq$	8
$[[\varphi]]$	13
$\vDash$	13
$\approx_{\alpha}$	16
$\oplus$	63
$\oplus_w$	63
$[L:K]$	75

## References

- [Ar 1] E. Artin; *Galois theory*; Notre Dame, Indiana, 1948 (2nd edition)
- [Ba 1] J. Barwise (ed.); *Handbook of mathematical logic*; North-Holland, 1977 (Studies in Logic, vol. 90)
- [Bo 1] A. Boileau, A. Joyal; *La logique des topos*; J. Symb. Log., vol. 46, nr. 1, 1981, p.6-16
- [Bu 1] C.W. Burden, C.J. Mulvey; *Banach spaces in categories of sheaves*; in: [Fo 3], p.169-196
- [Cr 1] J.N. Crossley, M. Dummett (eds.); *Formal systems and recursive functions*; North-Holland, 1965
- [Da 1] D. van Dalen, R Statman; *Equality in the presence of apartness*; in: [Hi 1], p.95-116
- [Da 2] D. van Dalen; *Singleton reals*; in: [Da 3]
- [Da 3] D. van Dalen, D. Lascar, T.J. Smiley (eds.); *Logic '80*; North-Holland (to appear)
- [Du 1] M. Dummett; *Elements of intuitionism*; Clarendon Press, 1977
- [Fo 1] M.P. Fourman; *The logic of topoi*; in: [Ba 1], p.1053-1090
- [Fo 2] M.P. Fourman, D.S. Scott; *Sheaves and logic*; in: [Fo 3], p.302-401
- [Fo 3] M.P. Fourman, C.J. Mulvey, D.S. Scott (eds.); *Applications of sheaves*; Springer, 1979 (Lecture Notes in Mathematics 753)
- [Go 1] R. Goldblatt; *Topoi*; North-Holland, 1979 (Studies in Logic, vol. 98)
- [Gr 1] R.J. Grayson; *Intuitionistic set theory*; Ph.D. Thesis, 1978

- [He 1] A. Heyting; *Intuitionistische axiomatiek der projectieve meetkunde*; Thesis, P. Noordhoff, 1925
- [He 2] A. Heyting; *Untersuchungen über intuitionistische Algebra*; Verhandelingen der Nederlandsche Akademie van Wetenschappen, afd. Naturkunde, 1<sup>e</sup> sectie, dl. 18, no. 2, 1941 (36 p.)
- [He 3] A. Heyting; *Intuitionism, an introduction*; North-Holland, 1956
- [Hi 1] J. Hintikka, I. Niiniluoto, E. Saarinen (eds.); *Essays on mathematical and philosophical logic*; Reidel, Dordrecht, 1978
- [Jo 1] P.T. Johnstone; *Rings, fields, and spectra*; J. Algebra, vol. 49, nr. 1, 1977, p.238-260
- [Jo 2] P.T. Johnstone; *Topos theory*; Academic Press, 1977
- [Ju 1] W. Julian, R. Mines, F. Richman; *Algebraic numbers, a constructive development*; Pac. J. Math. 74, 1978, p.91-102
- [Ke 1] J.F. Kennison; *Galois theory and theaters of action in a topos*; J. Pure Appl. Alg. 18, 1980, p.149-164
- [Ke 2] J.F. Kennison; *Separable algebraic closure in a topos*; J. Pure Appl. Alg. 24, 1982, p.7-24
- [Ko 1] A. Kock; *Universal projective geometry via topos theory*; J. Pure Appl. Alg. 9, 1976, p.1-24
- [Kr 1] S.A. Kripke; *Semantical analysis of intuitionistic logic I*; in: [Cr 1], p.92-129
- [La 1] S. Lang; *Algebra*; Addison Wesley, 1965
- [Ma 1] S. MacLane; *Categories for the working mathematician*; Springer, 1971
- [Ma 2] M. Makkai, G. Reyes; *First-order categorical logic*;

- Springer, 1977 (Lecture Notes in Mathematics 611)
- [Mu 1] C.J. Mulvey; *Intuitionistic algebra and representations of rings*; Mem. Amer. Math. Soc. 148, 1974, p.3-57
- [Re 1] G.E. Reyes; *Cramer's rule in the Zariski topos*; in: [Fo 3], p.586-594
- [Ri 1] F. Richman; *Seidenberg's condition P*; in: [Ri 2], p.1-11
- [Ri 2] F. Richman (ed.); *Constructive mathematics*; Springer, 1981 (Lecture Notes in Mathematics 873)
- [Ro 1] C. Rousseau; *Topos theory and complex analysis*; in: [Fo 3], p.623-659
- [Ru 1] W. Ruitenburg; *Intuitionistic algebra in the presence of apartness*; Utrecht, Dep. of Math., Preprint series no. 183, 1981
- [Ru 2] W. Ruitenburg; *Primality and invertibility of polynomials*; (to appear)
- [Sc 1] D.S. Scott; *Identity and existence in intuitionistic logic*; preliminary draft, E.T.H. Zürich, 1975
- [Sc 2] D.S. Scott; *Identity and existence in intuitionistic logic*; in: [Fo 3], p.660-696
- [Se 1] A. Seidenberg; *Constructions in algebra*; Trans. Amer. Math. Soc. 197, 1974, p.273-313
- [Sm 1] C. Smoryński; *Applications of Kripke models*; in: [Tr 2], p.324-391
- [Te 1] B.R. Tennison; *Sheaf theory*; Cambridge University Press, 1975
- [Tr 1] A.S. Troelstra; *Principles of intuitionism*; Springer, 1969 (Lecture Notes in Mathematics 95)

- [Tr 2] A.S. Troelstra (ed.); *Metamathematical investigation of intuitionistic arithmetic and analysis*; Springer, 1973 (Lecture Notes in Mathematics 344)
- [Tr 3] A.S Troelstra; *Intuitionistic extensions of the reals*; Nieuw Archief voor Wiskunde 3, 28, 1980, p.63-113
- [Wr 1] G.C. Wraith; *Generic Galois theory of local rings*; in: [Fo 3], p.739-767

*Samenvatting*

Wiskundigen hebben altijd geweten dat constructieve bewijzen in bepaalde zin uitgaan boven niet-constructieve bewijzen. In de loop van deze eeuw ontstond er echter een trend om constructieve bewijzen door algemenere bewijzen te vervangen (bijvoorbeeld de introductie van idealen in de algebra). Dit leidde tot abstractie en generalisatie. Deze abstractie culmineerde in de ontwikkeling van categorieën theorie. Bij de grotere abstractie gingen meestal de constructieve aspecten verloren. Intuitionistische algebra zoals gepresenteerd in dit proefschrift is op te vatten als een terugkeer naar constructieve procedures. Vergeleken bij de constructieve algebra in de traditie van Kronecker is onze benadering, in de navolging van Heyting, algemener doordat wij bijvoorbeeld structuren met onbeslisbare gelijkheid toelaten. We nemen bijvoorbeeld niet aan dat ieder element uit een lichaam inverteerbaar is of gelijk aan nul is.

De prijs die we daarvoor moeten betalen is dat we bepaalde stellingen niet kunnen afleiden die in de klassieke algebra wel afleidbaar zijn. Zo krijgen we niet altijd lichaamsuitbreidingen via priempolynomen. Ook werkt de gangbare constructie van normale en separabele lichaamsuitbreidingen niet. Maar er is ook een voordeel. Intuitionistische stellingen kunnen geïnterpreteerd worden in schoven over een topologische ruimte en zelfs nog algemener: in topoi. Daarmee leveren die stellingen direct resultaten in de klassieke wiskunde. Als een voorbeeld: zie 5.2.11. In concreto bestaat de inhoud van dit proefschrift uit

lineaire algebra, lichaamsuitbreidingen, Galois theorie en enkele modeltheoretische beschouwingen daarover.

Algemene topos theorie sluit nauw aan op algemene categorieën theorie. Daar juist topoi de modellen vormen voor hogere orde intuitionistische logica kunnen we zeggen dat de ontwikkelingen van enerzijds verdere generalisatie en abstractie en anderzijds van de constructieve wiskunde - in dit geval de intuitionistische algebra - zich weer verenigen via de topos theorie.



*Curriculum vitae*

De schrijver van dit proefschrift is geboren op 10 januari 1955 te Utrecht. Van 1967 tot 1973 bezocht hij het St. Bonifatius College te Utrecht waar hij in 1973 het diploma hogereburger-school B behaalde en in datzelfde jaar ging hij wiskunde studeren aan de Rijksuniversiteit te Utrecht. In 1975 legde hij het kandidaats examen wiskunde af met bijvak natuurkunde en in 1977 volgde het doctoraal examen wiskunde met als hoofd-richting grondslagen van de wiskunde en met bijvak computer-kunde. Van 1978 tot 1980 werkte hij voor de Nederlandse Organisatie voor Zuiver-Wetenschappelijk Onderzoek aan een project over intuitionistische algebra en schoven theorie. Vanaf 1981 is hij medewerker in tijdelijke dienst bij de subfaculteit Wiskunde te Utrecht.