THE L.E.J. BROUWER CENTENARY SYMPOSIUM
A.S. Troelstra and D. van Dalen (editors)
© North-Holland Publishing Company, 1982

PRIMALITY AND INVERTIBILITY OF POLYNOMIALS

Wim Ruitenburg*
Mathematisch Instituut
Budapestlaan 6
Utrecht, Netherlands

Abstract

Let K be a Heyting field, i.e. a field as defined in [He1]. Let $f \in K[X]$, $f \# 0$. It is well-known that there is a natural construction of a quotient ring $K[\alpha] = K[X]/(f)$ which is a ring with apartness. Then f is prime if and only if $K[\alpha]$ is an integral domain. $K[\alpha]$ is a field if f is prime and has invertible leading coefficient. If K satisfies some extra axioms, namely

$$\forall x,y(\exists z.xz = y \vee \exists z.yz = x)$$

and $$\forall x,y\exists n \in \mathbb{N}\,(\exists z.x^n z = y \rightarrow x \# 0 \vee y = 0),$$

then primality of f always implies $K[\alpha]$ is a field.

We shall also give some generalizations of these results. Furthermore, we present some illustrations in classical mathematics by using sheaf models, e.g. the sheaf of holomorphic functions from $\mathbb{C}$ to $\mathbb{C}$ which is a model of the extra axioms.

1. Basic properties

We start with a brief introduction to intuitionistic algebra in the presence of apartness. For a more detailed account, see [He1] or [Ru].

We also give some sheaf models and Kripke-models of field theory. If one is only interested in intuitionistic algebra one can skip the results about sheaf models. For those who are not familiar with sheaf models we refer to the literature ([Fo], [Go], [Jo], [Ma], [Ru], [Sm]).

The intuitionistic structures we consider are provided with an apartness relation $\#$, axiomatized by

(1) $\forall x.\ \neg x \# x$,

(2) $\forall x,y.x \# y \rightarrow y \# x$,

(3) $\forall x,y,z(x \# y \rightarrow x \# z \vee z \# y)$.

The apartness is tight if we have

(4) $\forall x,y.\ \neg x \# y \rightarrow x = y$.

From now on we assume that the apartness is tight, although many results remain valid in general.

Apartness behaves as a positive version of the inequality. Equality is the nega-

* The present research has been supported by the Netherlands Organization for the Advancement of Pure Research (Z.W.O)

tion of a tight apartness.

For functions f we have

$$\forall x_1,\dots,x_n,y_1,\dots,y_n(\bigwedge_{1\leqslant i\leqslant n} x_i = y_i \rightarrow f(x_1,\dots,x_n) = f(y_1,\dots,y_n)).$$

In the presence of apartness we can define a "positive inequality" version of this schema. We call f strongly extensional if it satisfies

$$\forall x_1,\dots,x_n,y_1,\dots,y_n(f(x_1,\dots,x_n)\#f(y_1,\dots,y_n) \rightarrow \bigvee_{1\leqslant i\leqslant n} x_i\# y_i).$$

With this notion there is a canonical way to axiomatize groups, rings and modules with apartness. The definitions can be paraphrased as

(1) The structure satisfies the well-known universal axioms.

(2) The domain is provided with an apartness such that the standard total functions on it are strongly extensional.

We restrict our attention to commutative rings.

1.1. Definition. An integral domain is a ring satisfying

(1) $1\#0$.

(2) $\forall x,y(x\#0 \wedge y\#0 \rightarrow xy\#0)$.

A field is a ring satisfying

(1) $1\#0$.

(2) $\forall x(x\#0 \rightarrow \exists y.xy = 1)$.

Examples: the Cauchy reals and the Dedekind reals are fields. A field is an integral domain and the quotient ring of an integral domain is a field. If R is an integral domain then the polynomial ring R[X] is also an integral domain. As apartness on R[X] we have $f\#g$ if and only if $f_i\#g_i$ for some $i\in\mathbb{N}$.

1.2 Examples of field models. For fields we have $x\#y \leftrightarrow \exists z.z(x-y) = 1$. So for the field models below we only need a description of their ring structures since the apartness is determined by invertibility.

(1) Let K be the following Kripke-model:

$$\begin{tikzcd}
\mathbb{Q} & & \mathbb{F}_2 \\
& \mathbb{Z}_{(2)} = S^{-1}\mathbb{Z} \text{ with } S = \mathbb{Z}\backslash(2). \arrow[ul] \arrow[ur] &
\end{tikzcd}$$

Then $\underline{K}\not\models 2 = 0 \vee \neg 2 = 0$.

(2) Let K be:

$$\begin{tikzcd}
K(X) & & K(Y) \text{ (K a field from classical mathematics)} \\
& S^{-1}K[X,Y]/(XY) \text{ with S the complement of } (X,Y). \arrow[ul, "Y\mapsto 0"'] \arrow[ur, "X\mapsto 0"] &
\end{tikzcd}$$

Then $\underline{K}\nvDash XY=0 \to X=0 \vee Y=0$.

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

$$[\![f\#g]\!] = \{\alpha \in U \mid f(\alpha) \neq g(\alpha)\} \text{ for } f,g \in \mathcal{C}(U,K).$$

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

Modules over a field are called <u>vector spaces</u>. Let M be a vector space over K, $x_1,\ldots,x_n \in M$. We define: $x_1,\ldots,x_n$ is <u>free</u> if

$$\forall \alpha_1,\ldots,\alpha_n \in K(\bigvee_{1\leqslant i\leqslant n} \alpha_i \# 0 \to \sum_{1\leqslant i\leqslant n} \alpha_i x_i \# 0).$$

In the presence of apartness the notion of freedom is more useful than the notion of independence. As an illustration we mention the Austauschsatz.

1.3. <u>Austauschsatz</u>. Let M be a vector space over K and $x_1,\ldots,x_m,y_1,\ldots,y_n \in M$ such that $x_1,\ldots,x_m$ is free and $x_1,\ldots,x_m$ depend on $y_1,\ldots,y_n$. Then there is a sequence $z_1,\ldots,z_n \in M$, made from $y_1,\ldots,y_n$ by replacing m vectors by $x_1,\ldots,x_m$ such that

(1) $z_1,\ldots,z_n$ is equivalent to $y_1,\ldots,y_n$, i.e. they depend on each other,

(2) $z_1,\ldots,z_n$ is free if and only if $y_1,\ldots,y_n$ is free,

(3) if $m=n$ then $x_1,\ldots,x_m$ is equivalent to $y_1,\ldots,y_m$ and $y_1,\ldots,y_m$ is free.

For a proof, see [He1] or [Ru].

Let $V \subset K^n$ be a sub vector space of K^n. Let V have a degree, i.e. assume that there is a sequence $v_1,\ldots,v_k$ of free generators of V. If $k=0$ then $V=\{0\}$. $v_1,\ldots,v_k$ is called a <u>basis</u> of V. Let $x \in K^n$. Then we define

$$x\#V \leftrightarrow \forall y \in V . x\#y.$$

Let φ be a formula not containing x free and let M be an m×n-matrix. Then we can prove:

1.4. <u>Theorem</u>.

$$\forall x \in K^n(x\#V \to (\varphi \vee Mx\#0)) \to \varphi \vee \forall x \in K^n(x\#V \to Mx\#0).$$

Proof: by induction on n. $n=1$ is trivial because then $V=K$ or $V=\{0\}$.

Induction step: take $n>1$. Assume that we have $\forall x\in K^n(x\#V \to (\varphi \vee Mx\#0))$. To prove: $\varphi \vee \forall x\in K^n(x\#V \to Mx\#0)$. By 1.3 there is a basis $e_1,\ldots,e_n$ of K^n such that $e_{n-k+1},\ldots,e_n$ is a basis of V. Then for all $x=\xi_1e_1+\ldots+\xi_ne_n$ we have

$$x\#V \leftrightarrow \mathop{\mathrm{W}}\limits_{i\leqslant n-k} \xi_i\#0.$$

Up to isomorphism $e_1,\ldots,e_n$ is the standard basis of K^n, i.e. $e_i=(0,.,0,1,0,.,0)$ with 1 on the i-th coordinate. Take e_1. Then we have $\varphi\vee Me_1\#0$. If φ holds, then we are done. So assume $Me_1\#0$. Then we have $\mathop{\mathrm{W}}\limits_{1\leqslant i\leqslant n}\alpha_{i1}\#0$, say $\alpha_{11}\#0$. ($M=(\alpha_{ij})$).

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

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

$$MS=\left(\begin{array}{c|c} \alpha_{11} & 0 \;\cdots\cdot\; 0 \\ \hline \alpha_{21} & \\ \vdots & B \\ \alpha_{m1} & \end{array}\right)$$

Then $\forall x\in K^n(x\#S^{-1}V \to (\varphi\vee MS\#0)$ holds. Let W be the image of $S^{-1}V$ under the morphism $p:(\alpha_1,\ldots,\alpha_n)\to(\alpha_2,\ldots,\alpha_n):K^n\to K^{n-1}$. Then we have

$$\forall x\in K^{n-1}(x\#W \to (\varphi\vee Bx\#0)).$$

Induction hypothesis: $\varphi\vee\forall x\in K^{n-1}(x\#W \to Bx\#0)$. So we have

$$\varphi\vee\forall x\in K^n(x\#S^{-1}V \to MS\#0),\text{ thus}$$

$$\varphi\vee\forall x\in K^n(x\#V \to Mx\#0).$$

2. *Algebraic extensions of fields*

From a ring R and an ideal I we can construct a quotient ring R/I. However, in the presence of apartness there is the extra complication of defining an apartness on R/I. Therefore we have to introduce a complementary notion of ideal in the same way as the apartness itself is a complementary notion of equality.

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

(1) $\neg 0\in C$,

(2) $x+y\in C \to x\in C\vee y\in C$,

(3) $xy\in C \to x\in C\wedge y\in C$.

C is non-trivial if $1\in C$.

It is simple to show that $I = (\neg C) = \{x \in R \mid \neg x \in C\}$ is a stable ideal. On the ring object R/I we take as apartness $x+I \# y+I \leftrightarrow x-y \in C$. Observe that there is some ambiguity in the notation R/I since it is possible to have different coideals C,D such that $(\neg C) = (\neg D) = I$. In this paper the required coideals will be clear from the context.

2.2. Definition. A coideal C is called prime if it satisfies

(1) $1 \in C$,

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

A coideal is called minimal if it satisfies

(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 $C \subset R$ we have

$$(C \text{ is prime}) \leftrightarrow (R/I \text{ is an integral domain}),$$

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

This implies that a minimal coideal is prime. The name "minimal" for a minimal coideal C can be explained by the property that each non-trivial coideal $D \subset C$ is equal to C.

Let $K[X]$ be a polynomial ring with $f \in K[X]$. We can construct the quotient ring $K[\alpha] = K[X]/(f)$. As mentioned above, the new aspect that we have to consider for that construction is the apartness relation on $K[\alpha]$. We have to construct a coideal.

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

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

We want to show that C_f is a coideal such that $(\neg C_f) = (f) = \{g \in K[X] \mid \exists h \in K[X] g=hf\}$.

2.4. Lemma. Let $f = f_0 + \ldots + f_m X^m \in K[X]$ such that $f_r \# 0$. Let M be the following $(m+n) \times n$-matrix:

$$M = \begin{pmatrix} f_0 & 0 & \ldots & 0 \\ f_1 & f_0 & & \vdots \\ \vdots & & \ddots & \\ & & & f_0 \\ f_m & & & \vdots \\ 0 & f_m & & \vdots \\ \vdots & & \ddots & \\ 0 & \ldots\ldots & & f_m \end{pmatrix}$$

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

$$B = \begin{pmatrix} f_s & \cdots & \cdots & \vdots \\ \vdots & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ \cdots & \cdots & \vdots & f_s \end{pmatrix}$$

such that B'is invertible and $f_s \# 0$.

Proof: by induction on $(m-r)$. $m-r=0$ is trivial.

Induction step: let $f_r \# 0$. Let C be the $n\times n$-submatrix with f_r on the diagonal. $f_r^n \# 0$, thus $f_r^n \# \det C \vee \det C \# 0$. If $\det C \# 0$ then we take $B = C$. Assume $f_r^n \# \det C$. Writing detC as the sum of n! products we get $\bigvee_{r<t} f_t \# 0$. Then apply induction.

2.5. <u>Lemma</u>. Let $P_n = \{g\in K[X] \mid g$ has degree at most $n\}$. Let $g \in P_n$. Then we have for all $f\in K[X]$:

$$g\in C_f \leftrightarrow \forall h\in P_n . g \# hf.$$

Proof: from left to right is trivial. From right to left: let $h\in K[X]$. To prove: $g\# hf$. Split $h = h_< + h_>$ where $h_< = h_0 + \ldots + h_n X^n$ and $h_> = h_{n+1}X^{n+1} + \ldots + h_m X^m$. Then $g \# h_< f$, thus $g\# hf \vee hf \# h_< f$. Assume $hf \# h_< f$. Then $h_> f \# 0$ and hf has degree at least n+1. Thus $g \# hf$.

The following lemma gives a sort of "best approximation" of g by elements of the ideal (f).

2.6. <u>Lemma</u>. Let P_n be as above, $f\in K[X]$, $f\#0$. Then there is a K-linear mapping $(.)^*_f : P_n \to P_n$ such that for all $g\in P_n$ we have

(1) $g\in C_f \leftrightarrow g \# g^*_f f$,

(2) $\exists h\in K[X] . g = hf \leftrightarrow g = g^*_f f$.

Proof: (1). $f\#0$, thus for some r we have: $f_r \# 0$. Then there is an $s \geqslant r$ and an $(n+1)\times(n+1)$-matrix B as in lemma 2.4,

$$B = \begin{pmatrix} f_s & \cdots & \cdots & \vdots \\ \vdots & \ddots & & \vdots \\ \vdots & & \ddots & \vdots \\ \cdots & \cdots & \vdots & f_s \end{pmatrix}$$

such that B is invertible and $f_s \# 0$. We identify polynomials $h = x_0 + \ldots + x_n X^n \in P_n$ with vectors $(x_0,\ldots,x_n) \in K^{n+1}$. Then we define:

$$h^*_f = B^{-1}\begin{pmatrix} x_s \\ x_{s+1} \\ \vdots \\ x_{s+n}\end{pmatrix} \quad \text{where } x_m = 0 \text{ if } m>n.$$

To keep the notation simple we shall write h^* instead of h^*_f. Let $k = h - h^*f =$

$=k_0+k_1X+k_2X^2+\ldots$. Then it easily follows from the definition above that

$$k_s=k_{s+1}=\ldots=k_{s+n}.$$

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 2.5. We have: $g\#hf \vee hf\#g^*f$. Assume $hf\#g^*f$. Then $h\#g^*$ and

$$Bh\#Bg^*.$$

Let $l=X^sBh$ (we use the identification of P_n and K^{n+1}). Then for some t, $s\leqslant t\leqslant s+n$, we have: $l_t\#g_t$ while $l^*=h$. Thus $g\#l^*f=hf$. This proves (1). (2) follows from (1) by using the tightness of the apartness relation.

2.7. <u>Theorem</u>. Let $f\in K[X]$, then C_f is a coideal.

Proof: we first consider the case $f\#0$. We check the axioms of 2.1.
$\neg 0\in C_f$ is trivial: take $h=0$.
Let $g_1g_2\in C_f$. To prove: $g_1\in C_f$. Let $h\in K[X]$, then $g_1g_2\#hg_2f$. Thus $g_1\#hf$.
Finally, let $g_1+g_2\in C_f$. There is an n such that $g_1,g_2\in P_n$. Let $(.)^*$ be a linear mapping according to 2.6 for this P_n. Then

$$g_1+g_2\#(g_1+g_2)^*f.$$
$$g_1-g_1^*f+g_2-g_2^*f\#0.$$
$$g_1\#g_1^*f \vee g_2\#g_2^*f.$$
$$g_1\in C_f \vee g_2\in C_f.$$

This proves that C_f is a coideal if $f\#0$.
Now consider the general situation. Again one easily verifies the axioms 2.1.(1) and 2.1.(3) for C_f. So let $g_1+g_2\in C_f$. To prove: $g_1\in C_f \vee g_2\in C_f$. $g_1+g_2\#0.f=0$, thus $g_1\#0$ or $g_2\#0$. We may assume that $g_1\#0$. Take an n such that $g_1\in P_n$. For all $h\in P_n$ we have $g_1\#hf \vee hf\#0$. This implies that the following formula holds:

$$\forall h\in P_n(f\#0 \vee g_1\#hf).$$

Let M be the following $(m+n+1)\times(n+2)$-matrix:

$$M=\begin{pmatrix} g_0 & f_0 & 0 & \ldots & 0\\ g_1 & f_1 & f_0 & & \vdots\\ \vdots & \vdots & & \ddots & f_0\\ \vdots & f_m & & & \vdots\\ g_n & 0 & f_m. & & \vdots\\ \vdots & \vdots & & & \\ 0 & 0 & \ldots & \ldots & f_m \end{pmatrix}$$

Let V be the subspace of K^{n+2}, generated by the sequence $e_2,\ldots,e_{n+2}$, where $e_i=(0,..,0,1,0,..,0)$ with 1 on the i-th coordinate. Then the formula above implies that we have

$$\forall x\in K^{n+2}(x\#V \rightarrow (f\#0 \vee Mx\#0)).$$

Apply 1.4. That gives us

$$f\#0 \vee \forall x\in K^{n+2}(x\#V \to Mx\#0).$$

$$f\#0 \vee \forall h\in P_n . g_1\#hf.$$

If $f\#0$ then C_f is a coideal and we have $g_1\in C_f \vee g_2\in C_f$. If $\forall h\in P_n . g_1\#hf$ holds then we apply 2.5: $g_1\in C_f$.

2.8. *Corollary*. Let $f\in K[X]$. If $f=0$ or $f\#0$ then C_f is a coideal such that

$$(f) = (\neg C_f).$$

Proof: the case $f=0$ is trivial. The case for $f\#0$ immediately follows from 2.6 and 2.7.

Observe that by 2.7 we can always construct the quotient ring $K[X]/(\neg C_f)$. If $f\#0$ or if $f=0$ then this is the same ring as $K[X]/(f)$. The restriction on f is essential as the following model shows.

$$\underline{K}\text{ is:}\quad \begin{tikzcd} K(T) & \text{(K a field from classical mathematics)} \\ K[T]_{(T)} \arrow[u] & \text{, the localization to the prime ideal (T).} \end{tikzcd}$$

Let $f=T^2\in \underline{K[X]}$ and $g=T$. So f and g are constants in the polynomial ring $\underline{K[X]}$. One easily verifies that we have $\underline{K[X]}\models \neg g\in C_f$ but also $\underline{K[X]}\not\models g\in(f)$.

Let $K[\alpha]=K[X]/(f)$ with $\alpha = X+(f)$, $f\#0$. Then $K[\alpha]$ is a ring with apartness. $K[\alpha]$ can be seen as a vector space over K, denoted by $(K[\alpha]/K)$. If f has an invertible leading coefficient, then f has a *degree*, denoted by $\deg(f)$. In that case $K[\alpha]$ is generated over K by the free sequence $1,\alpha,\ldots,\alpha^{n-1}$ with $n=\deg(f)$. We say that $K[\alpha]$ has *degree* n over K.

Now let $g\in K[X]$. If $\deg(f)=n$ exists and g has degree at most n-1 then

$$g\#0 \leftrightarrow g(\alpha)\#0.$$

However, in intuitionistic algebra $\deg(f)$ need not exist. Therefore we have a more elaborate statement.

2.9. *Proposition*. Let $f,g\in K[X]$, $f\#0$ and $K[\alpha]=K[X]/(f)$. Assume

$$\forall i\in \mathbb{N}\,(g_i\#0 \to \exists j>i . f_j\#0).$$

Then we have

$$g\#0 \leftrightarrow g(\alpha)\#0.$$

Proof: $g(\alpha)\#0$ immediately implies that $g\#0$. So assume $g\#0$. Then $g_i\#0$ for some i and $g\in P_n$ for some n. We complete the proof by induction on n-i. The case for $n-i=0$ is easy because then $f_j\#0$ for some $j>n$.

Induction step: $g\#0$. Let $(.)^*$ be a linear map of 2.6 for P_n. Then

$$g\#g^*f \vee g^*f\#0.$$

If $g \# g^*f$ then $g \in C_f$ and $g(\alpha) \# 0$. Assume $g^*f \# 0$. $f_j \# 0$ for some $j > i$ thus we have $g \# g^*f \vee (\exists k \geqslant j . g_k \# 0)$. If $g \# g^*f$ we are done and if g has a $k \geqslant j$ with $g_k \# 0$ we can apply induction.

2.10. Remark: Let $f, g \in K[X]$, $f \# 0$ and $K[\alpha] = K[X]/(f)$. Let $g \in P_n$ and let $(.)^*$ be a map of 2.6 for P_n. Then we can write

$$g - g^*f = (k_0 + \ldots + k_{s-1}X^{s-1}) + (k_{s+n+1}X^{s+n+1} + k_{s+n+2}X^{s+n+2} + \ldots).$$

Let $g - g^*f = l + h$ where $l = k_0 + \ldots + k_{s-1}X^{s-1}$. If $h \# 0$ then there is an $s' > s$ such that $f_{s'} \# 0$, because g and g^* have degree at most n. If $l \# 0$ then even $l(\alpha) \# 0$ as follows from 2.9.

Remark 2.10 plays a role in some induction proofs.

3. *Relative primality*

We first consider relatively prime pairs of polynomials before we consider prime polynomials. This looks somewhat unnatural, but there are reasons of economy for it. In particular we can avoid repetition of similar proofs.

There are several ways to define relative primality. We shall consider three of them.

3.1. Let $f, g \in K[X]$. Let φ be a formula in which h, k and l do not occur free. We shall consider the following notions of relative primality modulo φ.

(1) $(g \# 0 \wedge \forall h, k \in K[X](h \in C_g \rightarrow hf + kg \# 0 \vee \varphi)) \vee$
$\vee\ (f \# 0 \wedge \forall h, k \in K[X](k \in C_f \rightarrow hf + kg \# 0 \vee \varphi))$,

(2) $(f \# 0 \vee g \# 0) \wedge \forall h, k \in K[X](h \in C_g \vee k \in C_f \rightarrow hf + kg \# 0 \vee \varphi)$,

(3) $\forall h, k, l \in K[X](h \# h(0) \rightarrow hk \# f \vee hl \# g \vee \varphi)$.

We shall prove that 3.1.(1),(2) and (3) are equivalent. Our main interest concerns the case when φ is false. Then we can delete φ. However, the more general notions of 3.1 are needed for the proof of 3.6.

3.2. Lemma. Let $f, g, h, k \in K[X]$ be such that $f \# 0$, $g \# 0$ and $h \# h(0)$. Then we have:

(1) $f \# hk \vee k \in C_f$,

(2) $k \in C_f \rightarrow f \# f(0)$,

(3) $k \in C_f \rightarrow k \in C_g \vee f \# g$.

Proof: (1). From $f \# 0$ it follows that $f \# hk \vee hk \# 0$. Assume $hk \# 0$. Then $k \# 0$. If $k_i \# 0$ for some i then hk has degree at least $i+1$. Thus $f \# hk \vee \exists j > i . f_j \# 0$. Since k has degree at most n for some n we find

$$f \# hk \vee \forall i \in \mathbb{N}\, (k_i \# 0 \rightarrow \exists j > i . f_j \# 0).$$

$k \# 0$ thus by 2.9 we yield $f \# hk \vee k \in C_f$.

Concerning (2): $f \# f(0) \vee f(0) \# 0$. Therefore we may assume $f(0) \# 0$. From $k \in C_f$ now follows $k\#kf(0)^{-1}f$. Thus $f\#f(0)$.

(3). Assume $k\in C_f$. Let f,g have degree at most p. By induction on $m=(2p-m_1-m_2)$ we shall prove: $f_{m_1}\#0$ and $g_{m_2}\#0$ then $k\in C_g\vee f\#g$. The case for $m=0$ is contained in the induction step. Induction step: there is an n such that $k\in P_n$. Let $(.)^*_f$ and $(.)^*_g$ be maps for P_n according to 2.6. Then $k\#k^*_f f$. Thus $k\#k^*_g g\vee k^*_g g\#k^*_f f$, hence $k\in C_g\vee g\#f\vee k^*_g\#k^*_f$. We may assume $k^*_g\#k^*_f$. Then we easily find that

$$g\#f\vee\exists n_1>m_1.f_{n_1}\#0\vee\exists n_2>m_2.g_{n_2}\#0.$$

Applying induction we get $k\in C_g\vee f\#g$.

3.3. Lemma. The statements 3.1.(1) and (2) are equivalent.

Proof: one easily proves that (2) implies (1).
Assume (1). Let $g\#0$ and $\forall h,k\in K[X](h\in C_g\to hf+kg\#0\vee\varphi)$. Let $h,k\in K[X]$ be so that $k\in C_f$. It is sufficient to show $hf+kg\#0\vee\varphi$ for these assumptions. $h\in P_n$ for some n. Let $(.)^*_g$ be a map for P_n according to 2.6. Then $hf+kg=((h)^*_g g+d)f+kg=$ $=((h)^*_g f+k)g+df$ with $d=h-(h)^*_g g$. Since $g\#0$ and $k\in C_f$ we have that $((h)^*_g f+k)g\#0$. Thus $hf+kg\#0\vee df\#0$. Assume $df\#0$. Then $d\#0$ and $h\in C_g$. Apply the assumption:

$$hf+kg\#0\vee\varphi.$$

3.4. Lemma. 3.1.(2) implies 3.1.(3).

Proof: assume that 3.1.(2) holds. Let $k,l\in K[X]$ and let $h\in K[X]$ such that $h\#h(0)$. We have $f\#0\vee g\#0$ so by 3.2 we get $f\#hk\vee k\in C_f\vee g\#hl\vee l\in C_g$. Assumption 3.1.(2) implies $f\#hk\vee g\#hl\vee lf-kg\#0\vee\varphi$. Assume $lf\#kg$. Then $lf\#lhk\vee lhk\#kg$. Thus

$$f\#hk\vee g\#hl.$$

3.5. Lemma. Let $f,g,q,r\in K[X]$ such that $f=qg+r$. Then we have

(1) If f,g satisfies 3.1.(1) (or 3.1.(2)) then the same holds for g,r.

(2) If f,g satisfies 3.1.(3) then the same holds for g,r.

Proof: (2) is easy.
(1): let f,g,q,r be as above and let f,g satisfy condition 3.1.(1). From $f\#0\vee g\#0$ it immediately follows that we have $g\#0\vee r\#0$. First consider the case $g\#0$. Let $K[\beta]=K[X]/(g)$. Since f,g satisfies 3.1.(1) and since $f(\beta)=r(\beta)$ we have: $\forall h(\beta)\in K[\beta](h(\beta)\#0\to h(\beta)r(\beta)\#0\vee\varphi)$. Thus g,r satisfies 3.1.(1). This solves the case when $g\#0$.
Now assume $r\#0$. Let $h,k\in K[X]$ such that $k\in C_r$. By 3.2 this implies $k\in C_f\vee f\#r$. If $f\#r$ then $g\#0$ and we are done by the proof above. If $k\in C_f$ then $hf+kg\#0\vee\varphi$. Thus $hr+kg\#0\vee\varphi\vee hqg\#0$, where $hqg\#0$ again implies $g\#0$.

3.6. Theorem. 3.1.(1), (2) and (3) are equivalent.

Proof: by 3.3 and 3.4 we only have to prove that 3.1.(3) implies 3.1.(1). By induction on $m_1 = n_1+n_2$ we shall show: for all f,g,φ if f,g satisfies 3.1.(3) modulo φ and if f has degree at most n_1 and g has degree at most n_2 then f,g satisfies 3.1.(1) modulo φ. The case for $m_1 = 1$ is trivial since $f \# 0 \vee g \# 0 \vee \varphi$ holds (take $k = l = 0$ in 3.1.(3)).

Induction step: let f,g be given, satisfying the conditions for the induction step. $f \# 0 \vee g \# 0 \vee \varphi$ holds, thus we may assume: $g \# 0$. Let $h,k \in K[X]$ such that $h \in C_g$. To prove: $hf+kg \# 0 \vee \varphi$. By 3.2 we have that $g \# g(0)$. Then the assumption 3.1.(3) implies $f \in C_g \vee \varphi$. We may assume that $f \in C_g$ holds. There are s_1,s_2 such that $f_{s_1} \# 0$ and $g_{s_2} \# 0$. 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 $\underline{f} = f_0 + \ldots + f_{s_1}X^{s_1}$ and $\underline{g} = g_0 + \ldots + g_{s_2}X^{s_2}$. We may assume that $s_1 \geqslant s_2$ without loss of generality. There are $q,r \in K[X]$ such that $\underline{f} = q\underline{g}+r$ and r has degree at most s_2-1. One easily verifies that for all $\underline{h},\underline{k},\underline{l} \in K[X]$ such that $\underline{h} \# \underline{h}(0)$ we have $\underline{hk} \# r \vee \underline{hl} \# \underline{g} \vee \underline{f} \# f \vee \underline{g} \# g \vee \varphi$. Let ψ be the formula $\underline{f} \# f \vee \underline{g} \# g \vee \varphi$. Then $r,\underline{g}$ satisfies 3.1.(3) modulo ψ. By the induction hypothesis on m_1, $r,\underline{g}$ satisfies 3.1.(1) modulo ψ. By 3.5 $\underline{f},\underline{g}$ satisfies 3.1.(1) modulo ψ. Thus since $h \in C_g$ implies $h \in C_{\underline{g}} \vee \underline{g} \# g$ we get $h\underline{f}+k\underline{g} \# 0 \vee \underline{f} \# f \vee \underline{g} \# g \vee \varphi$, and thus

$$hf+kg \# 0 \vee \varphi \vee \underline{f} \# f \vee \underline{g} \# g.$$

And if $\underline{f} \# f \vee \underline{g} \# g$ holds we apply the induction hypothesis on m_2.

3.7. Definition. Let $f,g \in K[X]$. f and g are relatively prime if they satisfy one of the statements in 3.1 with φ is false.

3.8. Definition. Let R be a ring, $b \in R$. b is zero divisor free if

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

The following proposition relates relative primality with zero divisor free elements.

3.9. Proposition. Let $f,g \in K[X]$, $f \# 0$ and $K[\alpha] = K[X]/(f)$. Then the following are equivalent:

(1) f and g are relatively prime,

(2) $g(\alpha)$ is zero divisor free.

Proof: immediate from the definitions and 3.6.

Now it is easy to show:

3.10. Proposition. Let $f,g_1,g_2 \in K[X]$ such that the pairs f,g_1 and f,g_2 are both relatively prime. Then f and g_1g_2 are relatively prime.

Proof: we have $f\#0 \vee (g_1\#0 \wedge g_2\#0)$. If $f\#0$ then we consider $K[\alpha]=K[X]/(f)$. Then $g_1(\alpha)$ and $g_2(\alpha)$ are zero divisor free if and only if $g_1(\alpha)g_2(\alpha)$ is zero divisor free. So by 3.9 we have that f and g_1g_2 are relatively prime.
Assume $g_1\#0$ and $g_2\#0$. Thus $g_1\#g_1(0) \vee g_2\#g_2(0) \vee (g_1(0)\#0 \wedge g_2(0)\#0)$. If $g_1\#g_1(0)$ or $g_2\#g_2(0)$ then $f\#0$ and we are done. Thus assume that $g_1(0)\#0$ and $g_2(0)\#0$. Let $h,k\in K[X]$ such that $h\in C_{g_1g_2}$. To prove: $hf+kg_1g_2\#0$. Since $h\in C_{g_2(0)g_1}$ if and only if $h\in C_{g_1}$ we have $h\in C_{g_1} \vee g_2\#g_2(0)$ (use 3.2.(3)). If $g_2\#g_2(0)$ then $f\#0$ and we are done. Assume $h\in C_{g_1}$. Then $hf+kg_1g_2\#0$.

4. *Primality and minimality*

Let $f\in K[X]$, $f\#0$. Let $K[\alpha]=K[X]/(f)$. We shall give conditions for f such that $K[\alpha]$ is an integral domain. In contrast to the classical case this does not yet imply that $K[\alpha]$ is a field. In section 5 we shall consider a special class of fields for which we have that $K[\alpha]$ is a field if and only if $K[\alpha]$ is an integral domain.

4.1. Definition. Let $f\in K[X]$. Then f is prime if $f\#f(0)$ and for all $g,h\in K[X]$ with $g\#g(0)$ and $h\#h(0)$ we have $f\#gh$.

4.2. Lemma. Let $f\in K[X]$, $f\#0$. Then the following are equivalent:

(1) f is prime,

(2) $f\#f(0)$ and for all $g\in C_f$ f and g are relatively prime.

Proof: assume (1). Let $g\in C_f$ and $h,k,l\in K[X]$ such that $h\#h(0)$. To prove: $hk\#f \vee hl\#g$. Since $f\#0$ we have $f\#hk \vee hk\#0$. So we may assume: $hk\#0$. Then $k\#k(0) \vee k(0)\#0$. If $k\#k(0)$ then $f\#hk$ because f is prime. Assume $k(0)\#0$. Let $K[\alpha]=K[X]/(f)$. $g\in C_f$ implies $g(\alpha)\#0$. Thus $g(\alpha)\#h(\alpha)l(\alpha) \vee h(\alpha)l(\alpha)\#0$. If $g(\alpha)\#h(\alpha)l(\alpha)$ then $g\#hl$. Assume $h(\alpha)l(\alpha)\#0$. Then $h(\alpha)\#0$, thus $h(\alpha)k(0)\#0$. Then we have $h(\alpha)k(\alpha)\#0 \vee h(\alpha)(k(\alpha)-k(0))\#0$. If $h(\alpha)k(\alpha)\#0$ then $hk\#f$. Assume $h(\alpha)(k(\alpha)-k(0))\#0$. Then $k\#k(0)$ in $K[X]$ thus $hk\#f$ because f is prime. This proves (2).
Assume (2). Let $g,h\in K[X]$ such that $g\#g(0)$ and $h\#h(0)$. By 3.2 this implies $f\#gh \vee g\in C_f$. Assume $g\in C_f$. Then f and g are relatively prime, thus $f\#gh \vee g\#g\cdot 1$. Thus $f\#gh$ and f is prime.

As in classical mathematics we can prove([He1]):

4.3. Theorem. Let $f\in K[X]$, $f\#0$, $K[\alpha]=K[X]/(f)$. Then the following are equivalent: (1) f is prime,

(2) $K[\alpha]$ is an integral domain.

Proof: assume (1). Then $1 \# 0$ in $K[\alpha]$ because $f \# f(0)$ in $K[X]$. Let $g_1(\alpha), g_2(\alpha) \in$ $\in K[\alpha]$ such that $g_1(\alpha) \# 0$ and $g_2(\alpha) \# 0$. By 4.2 the pair f, g_1 is relatively prime. Thus $g_1(\alpha)$ is zero divisor free and $g_1(\alpha)g_2(\alpha) \# 0$. Thus $K[\alpha]$ is an integral domain. Assume (2). $1 \# 0$ in $K[\alpha]$ thus $f \# f(0)$ in $K[X]$ by 3.2. Let $g \in C_f$. Then $g(\alpha) \# 0$. Since $K[\alpha]$ is an integral domain $g(\alpha)$ is zero divisor free. Thus f and g are relatively prime. Now use 4.2.

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.

4.4. Theorem. Let $f, g \in K[X]$ be relatively prime and let $\deg(f)$ exist, $\deg(f) = n$. Then there are unique $h, k \in K[X]$ such that k has degree at most n-1 and such that

$$hf + kg = 1.$$

Proof: the case for $f = f(0)$ is trivial. Assume that $\deg(f) > 0$. Let $x = x_0 + \ldots$ $\ldots + x_{n-1}X^{n-1}$ with $x_0, \ldots, x_{n-1}$ variables over K. As in classical mathematics we have the following division algorithm. Since f has invertible leading coefficient there are unique $q, r \in K(x_0, \ldots, x_{n-1})[X]$ such that $xg = qf + r$ and such that r has degree at most n-1. The division algorithm gives that the coefficients $r_0, \ldots, r_{n-1}$ of r are linear in the x_j, say:

$$r_i = \alpha_{i+1,1}x_0 + \ldots + \alpha_{i+1,n}x_{n-1}.$$

Let $K[\alpha] = K[X]/(f)$. $g(\alpha)$ is zero divisor free. If we substitute elements $\xi_0, \ldots$ $\ldots, \xi_{n-1} \in K$ for $x_0, \ldots, x_{n-1}$ and such that $\xi_i \# 0$ for some i, then $x(\alpha) \# 0$ by 2.9. Thus $x(\alpha)g(\alpha) \# 0$ and $r(\alpha) \# 0$. This implies that the matrix $(\alpha_{i,j})$ is invertible. Thus we find a unique $k = k_0 + \ldots + k_{n-1}X^{n-1}$ such that after substitution $x_1 \mapsto k_i$ we get $kg = -hf + 1$. Since $f \# 0$, h is unique too.

As a corollary we get ([He1]):

4.5. Theorem. Let $f \in K[X]$, $f \# 0$, $K[\alpha] = K[X]/(f)$. Let f be prime such that $\deg(f) =$ $= n$ exists. Then $K[\alpha]$ is a field such that the vector space $(K[\alpha]/K)$ has degree n.

The existence of the degree of f in theorem 4.5 is not always necessary to show that $K[\alpha]$ is a field, see section 5. On the other hand $K[\alpha]$ need not be a field if f has no degree, see the example below.

4.6. Example. Let $\underline{K}$ be the following field model.

$\underline{K}$ is:

$$\begin{tikzcd}
\mathbb{Q}(x,y) \\
S^{-1}\mathbb{Q}[x,y] \text{ with } S = (x,y)^{\text{compl.}} \arrow[u]
\end{tikzcd}$$

The elements x and y are transcendental over Φ. Let $f = xX^2+X+1$ and let $g = yX+1$ be polynomials over $\underline{K}$. One easily verifies that f is prime and that f and g are relatively prime in the model. Thus $\underline{K[\alpha]} = \underline{K[X]}/\underline{(f)}$ is an integral domain with $g(\alpha)\#0$. 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. 4.10. Over $\Phi(x,y)$ in the top node of the Kripke-model we find for all n unique $a_n, b_n \in \Phi(x,y)$ 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.

The traditional method of [Ar] fails in the intuitionistic case if f has no invertible leading coefficient. But by refining the traditional proof we can derive the following invertibility theorem for prime polynomials in general.

4.7. Theorem. Let $f = f_0 + \ldots + f_nX^n \in K[X]$ be prime, $f_m\#0$, $g\in K[X]$ such that $g(\alpha)\#0$ in $K[\alpha] = K[X]/(f)$. Then we can split $f = f^{\#}+f^{=}$ where $f^{\#} = f_0 + \ldots + f_sX^s$, $s\geq m$, $f_s\#0$ such that $g(\beta)$ is invertible in $K[\beta] = K[X]/(f^{\#})$. Moreover, we can find an inverse $b(\beta)$ such 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.

Induction step: start with $f^{\#} = f_0 + \ldots + f_mX^m$. $f^{=} = f-f^{\#}$. Let $\xi_0,\ldots,\xi_{m-1}$ be K-variables and $x = \xi_0 + \ldots + \xi_{m-1}X^{m-1}$. Then $gx = qf^{\#}+r$ by the division algorithm. $r = r_0 + \ldots + r_{m-1}X^{m-1}$ with the r_i linear in the ξ_j: $r_i = \alpha_{i+1,1}\xi_0 + \ldots + \alpha_{i+1,m}\xi_{m-1}$. Altogether we have $g\in C_f$, f prime, $f_m\#0$, $g(\alpha)$ zero divisor free in $K[\alpha]$ and $gx = qf+r-qf^{=}$. Thus $\forall\xi_0,\ldots,\xi_{m-1}(\bigvee_{0\leq i\leq m-1}\xi_i\#0 \to r-qf^{=}\#0)$.

$$\forall\xi_0,\ldots,\xi_{m-1}(\bigvee_{0\leq i\leq m-1}\xi_i\#0 \to r\#0 \vee qf^{=}\#0).$$

Using lemma 1.4 with $V = \{0\}$ we get $\det(\alpha_{ij})\#0 \vee qf^{=}\#0$. Assume $qf^{=}\#0$. Then $f^{=}\#0$, thus $f_{m'}\#0$ for some $m' > m$. Apply induction. Assume $\det(\alpha_{ij})\#0$. Then there are $\beta_0,\ldots,\beta_{m-1}\in K$ such that

$$(\alpha_{ij})\begin{pmatrix} \beta_0 \\ \vdots \\ \beta_{m-1} \end{pmatrix} = \begin{pmatrix} 1 \\ 0 \\ \vdots \\ 0 \end{pmatrix}$$

Let $b = \beta_0 + \ldots + \beta_{m-1}X^{m-1}$. Then $gb = qf^{\#} + 1$ (with β_i for the ξ_i). $g(\beta)$ is invertible in $K[\beta] = K[X]/(f^{\#})$.

Let $K \subset L$ be fields, $\alpha \in L$. Let $K(\alpha)$ be the smallest field containing K and α. α is <u>algebraic</u> over K if there is an $f \in K[X]$ such that $f \# 0$ and $f(\alpha) = 0$. The following theorem gives some conditions under which f is prime and $\deg(f)$ exists.

4.8. <u>Theorem</u>. Let $K \subset L$ be fields, $\alpha \in L$, $f \in K[X]$, $f \# 0$. Then are equivalent:

(1) f has degree at most n, $f(\alpha) = 0$ and $(K(\alpha)/K)$ has degree at least n,

(2) f is prime and $\deg(f) = n$ exists, $K[X]/(f) \cong K[\alpha] = K(\alpha)$ with the canonical morphism and $(K[\alpha]/K)$ has degree n.

Proof: from (2) to (1) is trivial.

Assume (1). There are $p_1, \ldots, p_n, q_1, \ldots, q_n \in K[X]$ such that $p_1(\alpha)q_1^{-1}(\alpha), \ldots$ $\ldots, p_n(\alpha)q_n^{-1}(\alpha)$ is free in $(K(\alpha)/K)$. Let $q = q_1 \cdot \ldots \cdot q_n$ and take $r_i = p_i q_i^{-1} q$, $1 \leqslant i \leqslant n$. Then $r_1(\alpha), \ldots, r_n(\alpha) \in K[\alpha]$. A simple calculation shows that $r_1(\alpha), \ldots, r_n(\alpha)$ is free in $(K[\alpha]/K)$. There is a $k \in \mathbb{N}$ such that $r_1(\alpha), \ldots, r_n(\alpha)$ depend on $1, \alpha, \ldots, \alpha^k$. Let $f = c_0 + \ldots + c_n X^n$ and $c_j \# 0$. Now we can prove by induction on $(n-j)$ that $c_n \# 0$. $(n-j) = 0$ is trivial.

Induction step: $(n-j) > 0$, thus $j < n$. Take the sequence S consisting of

$$\begin{array}{llll}
1, \alpha, \alpha^2, \ldots, \alpha^{j-1}, & & & \\
c_{j+1}\alpha^{j+1}, & c_{j+1}\alpha^{j+2}, & \ldots, & c_{j+1}\alpha^{k+n-j}, \\
c_{j+2}\alpha^{j+1}, & c_{j+2}\alpha^{j+2}, & \ldots, & c_{j+2}\alpha^{k+n-j}, \\
\vdots & \vdots & & \vdots \\
c_n\alpha^{j+1}, & c_n\alpha^{j+2}, & \ldots, & c_n\alpha^{k+n-j}.
\end{array}$$

Then, by induction on l we can prove that α^l $(0 \leqslant l \leqslant k)$ depends on S, because if $l \geqslant j$ then $\alpha^l = -c_j^{-1}(c_0\alpha^{l-j} + c_1\alpha^{l-j+1} + \ldots + c_{j-1}\alpha^{l-1} + c_{j+1}\alpha^{l+1} + \ldots + c_n\alpha^{l+n-j})$. $1, \alpha, \ldots, \alpha^k$ depends on S, thus also $r_1(\alpha), \ldots, r_n(\alpha)$ depends on S. $r_1(\alpha), \ldots$ $\ldots, r_n(\alpha)$ is free, thus $c_s\alpha^t \# 0$ for some $s > j$ and $t > j$. Thus $c_s \# 0$ for some $s > j$. Replace c_j by c_s. Using induction on $(n-j)$ we can conclude: $c_n \# 0$. Thus $\deg(f) = n$ exists.

From this follows immediately: $1, \alpha, \ldots, \alpha^k$ is equivalent to $1, \alpha, \ldots, \alpha^{n-1}$ and $r_1(\alpha), \ldots, r_n(\alpha)$ depends on $1, \alpha, \ldots, \alpha^{n-1}$. Thus $1, \alpha, \ldots, \alpha^{n-1}$ is free (1.3). Take the canonical morphism $\varphi : K[X] \to K[\alpha]$ sending X to α. Let $g \in K[X]$. f has invertible leading coefficient, thus $g = qf + r$ by the division algorithm. So $\varphi(g) = r(\alpha)$. Now it is simple to see that $C_f = \{g \in K[X] \mid \varphi(g) \# 0\}$ and that φ is surjective. That means $\varphi^* : K[X]/(f) \to K[\alpha]$ is an isomorphism. $K[\alpha]$ is an integral domain, thus C_f is prime. Thus f is prime and $\deg(f) = n$ exists. Thus $K[\alpha]$ is a field. Thus $K[\alpha] = K(\alpha)$ and $(K[\alpha]/K)$ has degree n.

We may not assume that a prime polynomial f has an invertible leading coefficient. On the other hand we may assume that the bottom coefficient is invertible, see 4.10.

4.9. Lemma. Let f be prime and $a,b \in K$ such that $a \# b$. Then $f(a) \# 0$ or $f(b) \# 0$.

Proof: we may assume $a = 1$ and $b = 0$. $f \# f(0)$ thus $1 \in C_f$. That implies $1-X \in C_f \vee X \in C_f$. If $1-X \in C_f$ we substitute $Y = 1-X$, thus reducing case $1-X \in C_f$ to case $X \in C_f$. Therefore we may assume that $X \in C_f$. To prove: $f(0) \# 0$.
$f = a_0 + \ldots + a_n X^n \# f(0)$ thus $a_i \# 0$ for some $i \geqslant 1$. We have two cases to consider.
Case 1. $a_1 \# 0$ for some $i \geqslant 2$. Then $f = pX + f(0)$ with $p \# p(0)$. f is prime, thus $f(0) \# 0$.
Case 2. $a_1 \# 0$. Then $a_1 X \in C_f$ and $a_1 X - f \in C_f$. Thus $f(0) \# 0$ or $a_i \# 0$ for some $i \geqslant 2$.

4.10. Remarks. Let $f = f_0 + \ldots + f_n X^n$ be prime, $K[\alpha] = K[X]/(f)$. Take $a = 1$ and $b = 0$ in lemma 4.9. Then $f(1) \# 0 \vee f(0) \# 0$. If $f(1) \# 0$ then we substitute $(1-X)$ for X. This gives an isomorphism $K[X] \cong K[X]$. So up to isomorphism we may assume $f_0 \# 0$ or even $f_0 = 1$. Then α is invertible and $\alpha^{-1} = -f_1 - \ldots - f_n \alpha^{n-1}$.
Let $g(\alpha) = g_0 + \ldots + g_m \alpha^m$, then $g(\alpha) = \alpha(g_1 + \ldots + g_m \alpha^{m-1} - g_0 f_1 - \ldots - g_0 f_n \alpha^{n-1})$.
Iterating this procedure we find $x_0, \ldots, x_{n-1} \in K$ such that

$$g(\alpha) = \alpha^m (x_0 + \ldots + x_{n-1} \alpha^{n-1})$$

and such that for all i

$$x_i \# 0 \rightarrow \exists j > i.\, f_j \# 0.$$

By 2.9 this implies:

$$\exists i.\, x_i \# 0 \leftrightarrow g(\alpha) \# 0.$$

4.11. Some useful properties. Let $K[\alpha] = K[X]/(f)$ with $f = f_0 + \ldots + f_n X^n$ prime, $f_m \# 0$. 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. Instead of integral domains $K[\alpha]$ as above we consider rings $K[\alpha]$ with some $g(\alpha)$ which is 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. We may assume $f \in C_X$. Then $f(0) \# 0$. Let $f = a_0 + \ldots + a_n X^n$, $a_m \# 0$. We may assume that $a_0 = 1$. Let $K[\alpha] = K[X]/(f)$. Then $g(\alpha)$ is zero divisor free, i.e. we have

(1) $\forall h(\alpha).(h(\alpha) \# 0 \rightarrow g(\alpha)h(\alpha) \# 0)$, (cf. 3.9).

There are $h,k \in K[X]$ such that $hf + kg = 1$ if and only if $g(\alpha)$ is invertible (with inverse $k(\alpha)$). Thus if we want to find h,k such that $hf + kg = 1$ 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 4.6, but we have some approximate results. We can show: there is an $s \geqslant m$ such that

$a_s \# 0$ and for $f^{\#} = a_0 + \ldots + a_s X^s$ there are $h, q \in K[X]$ such that $gh = qf^{\#} + 1$. Proof: analogous to 4.7. Write $gh = qf + 1 - r$ with $r = q(f - f^{\#})$. This gives:

(2) There are $h, r \in K[X]$ such that we have $r \# 0 \to \exists m' > m . a_{m'} \# 0$ and
$g(\alpha)h(\alpha) = 1 - r(\alpha)$.

As in 4.10 we can write $g(\alpha) = \alpha^p k(\alpha)$ for some $p \in \mathbb{N}$ and some $k = k_0 + \ldots + k_{n-1} X^{n-1} \in K[X]$ satisfying $k_i \# 0 \to \exists j > i . a_j \# 0$. Then for $k(\alpha), \alpha^{-1} k(\alpha), \ldots, \alpha^{-n+1} k(\alpha)$ there are polynomials $k^{(1)}, \ldots, k^{(n)} \in K[X]$ each of degree at most n-1 such that $\alpha^{-i+1} k(\alpha) = k^{(i)}(\alpha)$. Let A be the matrix $A = (k^{(1)}, \ldots, k^{(n)})$ using the coefficients of the polynomials as column vectors, $\det A = \xi$. Then by Cramer's rule there exists a vector $v \in K^n$ such that $Av = (\xi, 0, \ldots, 0)$. Let $c = v_0 + \ldots + v_{n-1} X^{n-1}$. Then $c(\alpha)k(\alpha)\alpha^{-n+1} = = \xi$. Thus for some $l \in K[X]$ with $l(\alpha) = c(\alpha)\alpha^{-p-n+1}$ we have $g(\alpha)l(\alpha) = \xi$. Assume $a_n \# 0$. Since $k(\alpha)$ is zero divisor free we find $\forall w \in K^n (w \# 0 \to Aw \# 0)$. Thus A is invertible and $\xi \# 0$. Conclusion:

(3) There is an $l \in K[X]$ and a $\xi \in K$ such that we have $a_n \# 0 \to \xi \# 0$ and
$g(\alpha)l(\alpha) = \xi$.

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 $\xi t(\alpha) = r(\alpha)^{2^{n'}}$ for some $t \in K[X]$. Then we have

$$g(\alpha)\underline{h}(\alpha) = g(\alpha)h(\alpha)(1+r(\alpha))(1+r(\alpha)^2) \cdot \ldots \cdot (1+r(\alpha)^{2^{n'-1}}) = 1 - r(\alpha)^{2^{n'}}$$

and $g(\alpha)(\underline{h}(\alpha) + l(\alpha)t(\alpha)) = 1$. Thus $g(\alpha)$ is invertible.

(4) If $\xi | r(\alpha)^{m'}$ for some m' then $g(\alpha)$ is invertible.

4.12. Example. Let f,g be as in example 4.6, $\underline{K[\alpha]} = \underline{K[X]}/\underline{(f)}$. When we apply 4.11 to $g(\alpha) = y\alpha + 1$ we find that

$$\frac{1}{1-y}(y\alpha+1) = 1 - \frac{xy}{1-y}\alpha^2$$

and

$$(-xy\alpha + x - y)(y\alpha + 1) = x + y^2 - y.$$

Thus $r(\alpha) = \frac{xy}{1-y}\alpha^2$ and $\xi = x + y^2 - y$. Observe that in the bottom node of the Kripke-model $\underline{K}$ we do not have $\xi | r(\alpha)^{m'}$ for any m'.

5. $C_i D$-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 $x_1, \ldots, x_n$ of elements of K. Another consequence of D is:

5.1. Proposition. If a field K satisfies D then it also satisfies $xy = 0 \to x = 0 \vee y = 0$.

With help of D we can diagonalize matrices in the following sense. We call a matrix $B = (\beta_{ij})$ a half matrix if $\beta_{ij} = 0$ for all pairs $i > j$ or if $\beta_{ij} = 0$ for all pairs $i < j$. B is a diagonal matrix if $\beta_{ij} = 0$ for all pairs $i \neq j$.

5.2. Proposition. Let K satisfy D and let A be an $m\times n$-matrix over K. Then there is an $m\times n$-half matrix B_1 and an $n\times n$-matrix B_2 with $\det B_2 = 1$ such that $A = B_1B_2$.

Proof: use that each row $\alpha_{i1},\dots,\alpha_{in}$ contains a gcd.

5.3. 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, an $m\times m$-matrix B_1 and an $n\times n$-matrix B_2 with $\det B_1 = \det B_2 = 1$ such that $A = B_1BB_2$.

Proof: as for 5.2.

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 $hf+kg = 1$. This implies that for prime $f\in K[X]$ $K[\alpha] = K[X]/(f)$ is a field. The main lemma for this result is:

5.4. Lemma. Let K satisfy D, let $f,g\in K[X]$ be relatively prime with $f = a_0 + \dots$ $\dots + a_nX^n$, $a_m \# 0$ and $K[\alpha] = K[X]/(f)$. Then there are $\xi,\eta\in K$ such that

$$(\eta\#0 \vee \xi = 0) \to .(\exists s>m.a_s\#0 \vee a_n = 0) \text{ and}$$
$$\forall i\in\mathbb{N}\,(\xi|\eta^i \to \text{"}g(\alpha)\text{ is invertible"}).$$

Proof: from 4.11 we get: there are $h,r,l\in K[X]$ and $\xi\in K$ such that $g(\alpha)h(\alpha) = 1-r(\alpha)$ and $g(\alpha)l(\alpha) = \xi$ and if $r\#0$ then $a_s\#0$ for some $s>m$ and if $\xi = 0$ then $a_n = 0$. Moreover, if $\xi|r(\alpha)^i$ for some i then $g(\alpha)$ is invertible. Let η be the gcd of the coefficients of $r\in K[X]$. Then $r = \eta\underline{r}$ with $\underline{r}\#0$. If $\eta\#0$ then $r\#0$ thus we have

$$(\eta\#0 \vee \xi = 0) \to (\exists s>m.a_s\#0 \vee a_n = 0).$$

Let $i\in\mathbb{N}$. If $\xi|\eta^i$ then $\xi|r(\alpha)^i$ and $g(\alpha)$ is invertible by 4.11.(4). Thus we have proved: $\forall i\in\mathbb{N}\,(\xi|\eta^i \to \text{"}g(\alpha)\text{ is invertible"})$.

5.5. Consider the following principles.

C_1: $\forall y,x\exists n\in\mathbb{N}\,(x^n|y \to x\#0 \vee y = 0)$,

C_2: $\forall y\exists n\in\mathbb{N}\,\forall x\,(x^n|y \to x\#0 \vee y = 0)$.

We call fields that satisfy C_i and D C_iD-fields.

One easily verifies that C_2 implies C_1.

5.6. Theorem. Let K be a C_1D-field. Let $f,g\in K[X]$ be relatively prime. Then there are $h,k\in K[X]$ such that $hf+kg = 1$.

Proof: we have $f\in C_X \vee g\in C_X$. By symmetry we may assume $f\in C_X$. Then $f(0)\#0$ and thus we may assume $f(0) = 1$. Write f as $f = a_0 + \dots + a_nX^n$ and let $K[\alpha] = K[X]/(f)$. By induction on $(n-m)$ we show: if $a_m\#0$ then $g(\alpha)$ is invertible in $K[\alpha]$. The case for $n-m = 0$ follows from theorem 4.4.

Induction step: let $a_m \# 0$. By lemma 5.4 there are $\xi, \eta \in K$ such that $\eta \# 0 \vee \xi = 0$ implies $\exists s > m. a_s \# 0 \vee a_n = 0$ 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 $\eta \# 0 \vee \xi = 0$. 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 $\eta \# 0 \vee \xi = 0$ holds. Then we have $\exists s > m. a_s \# 0 \vee a_n = 0$ and we apply induction: $g(\alpha)$ is invertible.

5.7. Corollary. Let K be a C_1D-field, $f \in K[X]$, $f \# 0$, $K[\alpha] = K[X]/(f)$. Then we have:

$$f \text{ is prime} \leftrightarrow K[\alpha] \text{ is a field.}$$

Proof: from right to left is trivial. So assume that f is prime and let $g \in K[X]$. By 3.9 we have $g(\alpha) \# 0$ if and only if f and g are relatively prime. Now apply 5.6.

One thing that is missing in 5.6 compared to 4.4 is that we do not have a bound on the degrees of h and k, see example 5.11.(1). Another difference between 5.6 and 4.4 is that we do not have a uniqueness condition on h and k. But we have a weak uniqueness in the following sense.

5.8. Proposition. Let K be an arbitrary field. Let $f, g \in K[X]$ be relatively prime, $f = a_0 + \ldots + a_n X^n$, $f(0) \# 0$. Let $m \in \mathbb{N}$. Then there is at most one pair $h, k \in K[X]$ such that $k = X^m k^{(1)}$ where $k^{(1)}$ satisfies $\forall i \in \mathbb{N}\, (k_i^{(1)} \# 0 \rightarrow \exists j > i. a_j \# 0)$ and such that $hf + kg = 1$.

Proof: we only have to show the existence of at most one k. Let $K[\alpha] = K[X]/(f)$. Let $k = X^m k^{(1)}$ and $l = X^m l^{(1)}$ be so that $g(\alpha)\alpha^m k^{(1)}(\alpha) = g(\alpha)\alpha^m l^{(1)}(\alpha) = 1$. Then $k^{(1)}(\alpha) = l^{(1)}(\alpha)$ and $k^{(1)} - l^{(1)} \in (f)$. Assume $k^{(1)} \# l^{(1)}$. Then $k_i^{(1)} \# l_i^{(1)}$ for some i and thus $k_i^{(1)} \# 0 \vee l_i^{(1)} \# 0$ holds. Thus $a_j \# 0$ for some $j > i$. This implies that we have $\forall i \in \mathbb{N}\, ((k^{(1)} - l^{(1)})_i \# 0 \rightarrow \exists j > i. a_j \# 0)$. So by 2.9 $k^{(1)} - l^{(1)} \in C_f$. Contradiction. $k^{(1)} = l^{(1)}$.

Observe that from 5.6 and 4.10 it follows that if K is a C_1D-field then for some $m \in \mathbb{N}$ there is a solution h,k where $k = X^m k^{(1)}$ is as described in 5.8.
If for some m we have a $k = X^m k^{(1)}$ as in 5.8 such that $g(\alpha)\alpha^m k^{(1)}(\alpha) = 1$, then there is a $k^{(2)} \in K[X]$ such that $k^{(2)}(\alpha) = \alpha^{-1} k^{(1)}(\alpha)$ and $X^{m+1} k^{(2)}$ satisfies the conditions of 5.8. 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 $m' \geqslant m$.

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.

5.9. 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 $f/g \in K(X)$ can be written as $f = \eta h$ with $\eta \in K$ and $h \# 0$. The rest is trivial.

5.10. Theorem. Let K be a C_iD-field, $f \in K[X]$, f prime and $K[\alpha] = K[X]/(f)$. Then $K[\alpha]$ is also a C_iD-field.

Proof: from 5.7 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 $r(\alpha) \# 0$.

The remaining details concerning $D \wedge C_i$ then follow easily from the property $D \wedge C_i$ for K.

Proof of the claim: let $f = a_0 + \ldots + a_n X^n$. We may assume that $f(0) = 1$. By induction on $(n-m)$ we shall prove: if $a_m \# 0$ then the claim holds. The case for $n-m = 0$ is easy. We continue with the induction step. Let $a_m \# 0$ and $g(\alpha) \in K[\alpha]$. η is the gcd of $a_{m+1}, \ldots, a_n$. By induction on p we show

$(g(\alpha) = \mu z(\alpha)$ with $z(\alpha) \# 0$, $\mu \in K) \vee (g(\alpha) = \eta^p u(\alpha)$ for some $u(\alpha))$.

The case for $p = 0$ is trivial. Induction step: we may assume that $g(\alpha) = \eta^p u(\alpha)$ holds, otherwise there is nothing to prove. We can write $g(\alpha) = \eta^p \alpha^{m'} x(\alpha)$ for some m' and $x = x_0 + .. + x_{n-1}X^{n-1}$. Let $(.)^* = (.)^*_f : P_n \to P_n$ be a map according to 2.6 and with corresponding invertible submatrix B with $a_s = f_s \# 0$ on the diagonal such that $s \geqslant m$. Then we can write $x = (x)^*f + y$ with $y = \underline{y} + \overline{y}$ according to 2.10. Let γ be the gcd of the coefficients of y. Then $y = \gamma z$ with $z \# 0$. $\underline{y} = \gamma \underline{z}$ and $\overline{y} = \gamma \overline{z}$. From $z \# 0$ we derive $\underline{z} \# 0 \vee \overline{z} \# 0$. Assume $\underline{z} \# 0$. Then $z(\alpha) \# 0 \vee \overline{z} \# 0$. If $z(\alpha) \# 0$ then $x(\alpha) = y(\alpha) =$ $= \gamma z(\alpha)$ and $g(\alpha) = \eta^p \gamma \alpha^{m'} z(\alpha)$ with $\alpha^{m'} z(\alpha) \# 0$. So assume $\overline{z} \# 0$. The coefficients of $\overline{y}$ are divisible by η thus we get $\eta | \gamma$. Conclusion: $x(\alpha) = \eta v(\alpha)$ for some $v \in K[X]$. So $g(\alpha) = \eta^{p+1} \alpha^{m'} v(\alpha)$. This completes the induction on p.

By 4.11.(3) there is an $l \in K[X]$ and a $\xi \in K$ such that $\xi = 0$ implies $a_n = 0$ and $g(\alpha) l(\alpha) = \xi$. By axiom C_i there is a $p \in \mathbb{N}$ such that $\eta^p | \xi$ implies $\eta \# 0 \vee \xi = 0$. Now we may assume that $g(\alpha) = \eta^p u(\alpha)$ for some $u \in K[X]$. Thus $\eta^p u(\alpha) l(\alpha) = \xi$. There is a $q \in K[X]$ such that $\eta^p ul + qf = \xi$. Let ε be the gcd of the coefficients of q: $q = \varepsilon \underline{q}$ with $\underline{q} \# 0$. From the fact that $\underline{q} f \# \underline{q}(0) f(0)$ it follows that $\eta^p | \varepsilon$. Thus also $\eta^p | \xi$ and $\eta \# 0 \vee \xi = 0$. Then we have $\exists s > m . a_s \# 0 \vee a_n = 0$ and we can apply induction on n-m.

5.11. Examples.

(1) Let $\underline{K}$ be the following field model.

$$\begin{tikzcd} \mathbb{F}_2 & & \mathbb{Q} \\ & \mathbb{Z}_{(2)} \arrow[ul] \arrow[ur] & \end{tikzcd}$$

$\mathbb{Z}_{(2)}$, the localization to the prime ideal (2).

Then one easily verifies that $\underline{K}$ satisfies the axioms D and C_2. Let $f = 2X^2 + X + 1$. Then f is prime and $\underline{K[\alpha]} = \underline{K[X]/(f)}$ is a field. For instance we have $6\alpha + 1 \# 0$ and $-\alpha^4(6\alpha + 1) = 1$. In fact there is no $f \in \mathbb{Z}_{(2)}[X]$ with degree at most 3 such that

$f(\alpha)(6\alpha+1)=1$.

(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 $X=\{(p)\subset R \mid p \text{ is prime}\}$ with the cofinite sets as open sets. For open $U\subset X$, $U=X\setminus\{(p_1),\ldots,(p_n)\}$, we take as ring of sections above U: $R(U)=S^{-1}R$ with S the multiplicative set generated by $p_1\cdot\ldots\cdot p_n$. Call this sheaf model $\underline{R}$. Then $\underline{R}$ is a local ring model satisfying D 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 $y=d/e$ where $d,e\in R$ and d has a prime number decomposition $d=p_1^{n_1}\ldots p_m^{n_m}$. Let $n=\max(n_1,\ldots,n_m)$. Then one easily verifies that for all $x\in R(V)$, $V\subset U$, we have $[\![x^{n+1}\mid y\rightarrow x\#0 \vee y=0]\!]\supset V$. Thus $\underline{R}$ satisfies C_2. Finally, let $\alpha=(p)\in[\![\neg y\#0]\!]$ for $y=d/e\in R(U)$, $\alpha\in U$. Thus $p\mid d$. Then $[\![\neg y\#0]\!]$ 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 $\alpha\in[\![y=0]\!]$. Conclusion: $\underline{R}$ is a field model satisfying D and C_2. Observe that this model satisfies more extra properties. Since each open subset $U\subset X$ of the infinite set X is cofinite or empty we find that for each formula φ $\underline{R}$ satisfies $\neg\varphi\vee\neg\neg\varphi$, e.g. in $\underline{R}$ $\forall x(x=0\vee\neg x=0)$ 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 ζ can be written as power series $a(\xi)=a_m(\xi-\zeta)^m+a_{m+1}(\xi-\zeta)^{m+1}+\ldots$ and $b(\xi)=b_n(\xi-\zeta)^n+b_{n+1}(\xi-\zeta)^{n+1}+\ldots$ 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 5.6 to derive a property of rings, using the sheaf construction of 5.11.(2). This property is chosen for its illustrative nature.

5.12. 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 $M\subset R$ we have $\gcd(\overline{f},\overline{g})=\overline{1}$ 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 5.11.(2). From the conditions on f and g it follows that $\underline{R}\models$ (f and g are relatively prime). Thus we have

$$\underline{R}\models\exists h,k\in K[X].hf+kg=1.$$

From the interpretation of the existential quantifier $\exists$ 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 $U,V\subset X$ such that $U\cup V=X$ and $[\![f(0)\#0]\!]=U$ and $[\![g(0)\#0]\!]=V$. Here $X\setminus U=\{(p)\subset R\mid p \text{ is prime and } p\mid f(0)\}$ and $X\setminus V=\{(p)\subset R\mid p \text{ is prime and } p\mid g(0)\}$. Then by 5.8 we have a cover $\{U_m | m \in \mathbb{N}\}$ of U such that we find unique h,k with $k = X^m k^{(1)}$ above U_m, where $X^m k^{(1)}$ is as described in 5.8. 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 $k = X^m k^{(1)}$ 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 ot 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 $(f(0), g(0)) \subset R$ is not contained in any maximal ideal $M \subset R$. 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

$$hf + kg = 1.$$

References

[Ar] E. Artin; *Galois theory*; Notre Dame, Indiana, 1948 (2nd edition)

[Fo] M.P. Fourman, D.S. Scott; *Sheaves and logic*; in: [FMS] , p.302-401

[FMS] M. Fourman, C. Mulvey, D.S. Scott (editors); *Applications of sheaves*; Springer, 1979 (Lecture Notes in Mathematics 753)

[Go] R. Goldblatt; *Topoi*; North-Holland, 1979 (Studies in Logic, vol. 98)

[He1] A. Heyting; *Untersuchungen über intuitionistische Algebra*; Verhandelingen der Nederlandsche Akademie van Wetenschappen, afd. Natuurkunde, 1^{e} sectie, dl. 18, no. 2, 1941 (36 p.)

[He2] A. Heyting; *Intuitionism, an introduction*; North-Holland, 1956

[Jo] P.T. Johnstone; *Topos theory*; Academic Press, 1977

[La] S. Lang; *Algebra*; Addison Wesley, 1965

[Ma] M. Makkai, G. Reyes; *First-order categorical logic*; Springer, 1977 (Lecture Notes in Mathematics 611)

[Ru] W. Ruitenburg; *Intuitionistic algebra*; Thesis, Utrecht, 1982

[Sc] D.S. Scott; *Identity and existence in intuitionistic logic*; in: [FMS], p.660-696

[Sm] C. Smoriński; *Applications of Kripke models*; in: [Tr], p.324-391

[Tr] A.S. Troelstra (editor); *Metamathematical investigation of intuitionistic arithmetic and analysis*; Springer, 1973 (Lecture Notes in Mathematics 344)