LINEAR ALGEBRA AND PROJECTIVE GEOMETRY IN THE ZARISKI TOPOS

Anders Kock

The aim of this note is threefold: (i) logic, (ii) linear algebra, (iii) geometry. More precisely:

(i) We illustrate the technique of working with elements in a regular category (when dealing with 1^{st} order statements).

(ii) Using this we give a notion of field object in a regular category $\underline{E}$ such that the basic linear algebra is valid; the central basic theorem being that for any $m \times n$-matrix

row rank = column rank
= rank in terms of subdeterminants.

The example of such kind of field object (the axioms are given in (2.1) and (2.2) below) which we had in mind, is the affine line in the Zareski topos ("the universal local ring", according to Hakim [4], III §3).

(iii) Finally, assuming that $\underline{E}$ is an elementary topos equipped with a field object R of the kind defined by (2.1) - (2.2), one can construct the Grassmann manifolds $G(r,n)$ of "r-planes in n-space". For fixed n, these fit together to form a certain combinatorial structure, a "geometric lattice" or a "synthetic geometry". We prove this fact only for the case $n = 3$, in which case $G(1,3)$ and $G(2,3)$ should be thought of as the "set of points" and the "set of lines" in a "projective plane". We show that $G(1,3)$ and $G(2,3)$, with an obvious incidence relation, form a structure which satisfies the axioms for a projective plane ("through two different points, there is a unique line; two different lines intersect in a unique point". (Again "satisfying" some ordinary 1st order statements like these is meant in the sense of "working with elements in a regular category", or "Kripke-Joyal semantics".)

We do not here pursue the line further into higher dimensions. To do this in a coordinate free way would require consideration of exterior algebras. This should cause no difficulties, except that the exterior algebra on an R-module need not exist at all in $\underline{E}$, unless one assumes existence of a natural number object in $\underline{E}$. Of course, for R-modules locally isomorphic to R^n, the exterior algebra does exist and has locally a canonical basis. But then we are really just back working with matrices and determinants again.

We end up by a section (Section 4) where we use that the Zariski ringed topos satisfies our field axiom, together with the universal property which the Zariski ringed topos has among local ringed toposes (Hakim), to give a topos-theoretic framework to the Übertragungsprinzip of E. Study [13]: "to transfer statements about abstract spherical geometry to statements about the geometry of oriented lines in Euclidean 3-space" (by considering the ring of dual numbers).

Section 1 contains the logic by means of examples. It is roughly the content of a lecture [8] given at the Aarhus Category Open House, May 73. W. Mitchell, Osius, Mulvey and Benaon and his students have dealt more systematically and conceptually with language and interpretation for toposes. The conceptual way of formulation the above would be to pass to the topos sh($\underline{E}$) of sheaves on $\underline{E}$ (with respect to the "precanonical" topology, [10]). Instead of (informal) "statements" (as considered in Section 1 here), one would construct "conceptual" objects in sh($\underline{E}$). For formal computations (e.g. matrix-multiplication) I think, however, that it is an advantage not to conceptualize everything, but rather consider actual elements (or matrices of elements) in "external" rings (like hom(X,R)).

Section 2 contains the linear algebra. I have not been able to determine its exact relationship with Heyting's "intuitonistic linear algebra" [5], partly because Heyting's groundfield R is not assumed commutative, partly because he works with a separate "apartheid" relation ω, where we work just with negation of equality.

Section 3 constructs the Grassmannians, in particular the projective plane. For the special case of the Zariski topos, I think that the constructed objects are the same as those "classically" considered (in Demazure-Gabriel, say, [2] p. 9).

Sections 2-4 were the content of a lecture given at Giornate di Logica Categorical, Firenze, May 74.

1. Kripke-Joyal semantics.

We do not attempt to describe a formal language $L(\underline{E})$, and a complete interpretation of it. Rather we explain what are the principles behind the concrete interpretation of the concrete notions below (for more examples of this kind, see [9]).

Let B be an object in $\underline{E}$. Suppose that we have already interpreted a certain statement φ about arrows ending in $\underline{E}$; that is, for every $X \in |\underline{E}|$ and every $b: X \to B$, we assume that we know what we mean by saying that φ holds for b, denoted $\varphi(b)$. Then the statement $\neg\varphi$ is interpreted by saying that for X and $b: X \to B$ arbitrary

$(\neg\varphi)(b)$ iff for every arrow α which ends in X, if $\varphi(\alpha.b)$ holds, then the domain of α is the initial object.

In more succinct form: $\neg\varphi$ holds for b if it is <u>universally the case that</u> φ does not hold for b. Or:

Interpreting $\alpha: Y \to X$ as a passage from "time X" to the "later time Y", φ holds for b ("defined at time X", $b: X \to B$) iff for all later times Y, φ does not hold for b at time Y (unless $Y = \emptyset$).

This is Kripke's semantics for negation. Implication and universal quantification are interpreted the analogous way, i.e. by introducing a <u>universally</u> quantified parameter-shift α (or "passage to later time"). (See illustration below in connection with linear independence, or [9]).

In Kripke's original semantics, validity of conjunctions, disjunctions and existential quantifications are decided "at the spot", that is, no α is required. This was pointed out to be inadequate (for disjunction and existential qualification) for many mathematical purposes by Joyal (private communication). For instance in topology, existence of cross sections (in fiber bundles, or sheaves, say) is a rare thing compared to existence-locally of cross-sections. So the slogan was formed "existence means local existence". Similarly for disjunction. To be precise, suppose that we have already interpreted the statements φ_1 and φ_2, both being statements about arrows ending in B (as before). Then the statement $\varphi_1 \vee \varphi_2$ is interpreted by saying that for X and $b: X \to B$ arbitrary

$(\varphi_1 \vee \varphi_2)(b)$ iff there exists a jointly epic pair of maps ending in X, $(\beta_1: X_1 \to X, \beta_2: X_2 \to B)$ such that
φ_1 holds for $\beta_1 . b$ and
φ_2 holds for $\beta_2 . b$.

Similarly for n-fold disjunctions. (We also use the term cover for a finite jointly epic family). For an illustration of the analogous "local" interpretation of existential quantification, see the example below.

Such interpretations of statements φ are not very useful, unless they define subfunctors of representable functors; this means that if we have

$$Z \xrightarrow{\gamma} X \xrightarrow{b} B$$

and φ holds for b, then also φ holds for $\gamma . b$. So our interpretations of more composite statements should define subfunctors provided the constituent statements do.

This is automatically so for negation and universal quantification (provided the initial object is strict, and is preserved by pull-back). For existential quantification and disjunction, one has to require certain exactness properties of the category $\underline{E}$, for instance that jointly epi families are preserved by pull-back.

A final remark concerning the method of interpretation. For this, we have to assume that in $\underline{E}$ every epic is regular, that is, is coequalizer of its kernel pair (or, alternatively, that the interpretation of existential statements are changed by replacing localization by an arbitrary epic by localization by a regular epic). Under these conditions, we can augment the principle

Existence means local existence

by

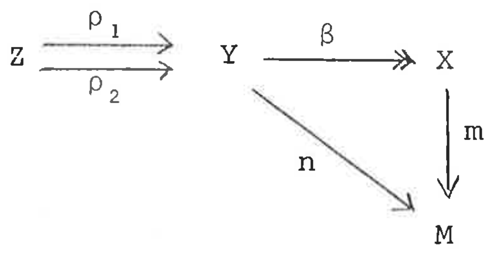
Unique existence implies global existence.

We illustrate this by an example.

Example. Let M be a ring-object in $\underline{E}$ (not necessarily commutative). Let $m: X \to M$ be a map in $\underline{E}$ (an "element of M defined over X"). Then by definition, m satisfies the existential statement: "there exists a right inverse for m" if there exists some epic $\beta: Y \to X$ and an element $n: Y \to M$ such that in the ring $hom_{\underline{E}}(Y,M)$

$$(\beta.m) \cdot n = e$$

where e is the neutral element in the ring $hom_{\underline{E}}(Y,M)$. So "locally" (namely "on" Y), m has a right inverse. Now, in a commutative ring, inverses are unique. So assume M is a commutative ring object. Let ρ_1, ρ_2 be the kernel pair of β. Consider the (non-commutative) diagram (m, β and n as above)



We shall prove that n factors across β. Since n is inverse to $\beta . m$ in hom(Y,M)

$$* \qquad \rho_i . n \text{ is inverse to } \rho_i . \beta . m \qquad i = 1,2$$

in hom(Z,M). Now $\rho_1 . \beta . m = \rho_2 . \beta . m$, since β coequalizes ρ_1, ρ_2. So $\rho_1 . n$ and $\rho_2 . n$ an inverse for the same element in the ring hom(Z,M). This ring was, however, commutative, whence $\rho_1 . n = \rho_2 . n$. So n factors across the coequalizer β

$$n = \beta . n'$$

where $n' : X \to M$. To prove that n' is an inverse for m in hom(X,M), it suffices (since β is epic) to see that $\beta . n'$ is inverse to $\beta . m$. But this is so. So m has a "global" inverse n'.

This means in particular that for a commutative ring object M in $\underline{E}$, one does not have to distinguish between the "Kripke-Joyal" interpretation of "m is invertible", and the "isolated" interpretation: "m is invertible in the ring hom(X,M)" ("Isolated", because here we ignore the rest of the category <u>E</u> when deciding the validity).

For non-commutative rings, this is not so; in particular, for the matrix rings we consider in the next paragraph.

2. Linear algebra

In the following two sections, $\underline{E}$ denotes a fixed elementary topos. (Actually, for Section 2, only the exactness properties are needed, and in fact the whole thing could be carried out in an arbitrary regular category with well-behaved coproducts and initial object, provided the word 'epic' is understood to mean 'regular epic'.)

Let R be a commutative ring object in $\underline{E}$. We say that it is a field object provided for each $n = 1,2,...$

$$(2.1) \qquad \neg\left(\bigwedge_{i=1}^{n} (a_i = 0)\right) \quad \text{implies} \quad \bigvee_{i=1}^{n} (a_i \text{ is invertible})$$

and

$$(2.2) \qquad \neg(1 = 0).$$

Note that (2.1), according to §1, means the following: Assume that $a_1,...,a_n$ are maps $X \to R$ (with same domain X), having the property that for all $\alpha: Y \to X$ (with $Y \neq \emptyset$), $\alpha.a_1,...,\alpha.a_n$ are not all 0; then there exists a jointly epic family

$$\beta_i: X_i \to X \qquad (i = 1,...,n)$$

such that, for each $i = 1,...,n$, $\beta_i . a_i$ is an invertible element in the ring $\hom(X_i,R)$.

Similarly, (2.2) means that the zero- and the one-element in the ring $\hom(X,R)$ are different for arbitrary $X \in \underline{E}$ $(X \neq \emptyset)$.

The axiom (2.1) for $n = 1$ is what Mulvey [11] calls a "ring of fractions". The effect of having the axiom for all n is to build a little boolean logic (one of de Morgan's laws) into R. The axioms (2.1) and (2.2) together imply that R is a local ring in the sense of Hakim [4] (cf. also Mulvey [11]).

If $\mathfrak{Z} \subseteq \mathcal{S}^{\mathcal{R}}$ is the Zariski topos ($\mathcal{R}$ the category of small commutative rings (models, [2]), then the forgetful functor $R: \mathcal{R} \to \mathcal{S}$ is in $\mathfrak{Z}$, and it is a commutative ring object canonically. It satisfies (2.1) and (2.2). This comes from the fact that <u>if</u> A is a commutative ring, and $a_1, \ldots, a_n$ are elements in A such that for every ring homomorphism $f: A \to B$, the a_i's are not all sent to 0 (unless B is the zero ring), <u>then</u> the a_i's generate the unit ideal in A (Proof: take $B = A/(a_1, \ldots, a_n)$). So the family $A \to A[a_i^{-1}]$ $(i = 1, \ldots, n)$ form a covering for the Zariski topology ([3], IV.6.3), and on $A[a_a^{-1}]$, a_i is invertible.)

Returning to the general situation, let $M \in |\underline{E}|$ be a module object over a commutative ring object R. An n-tuple of elements

$$\text{(2.3)} \qquad \underline{v}_i : X \to M \qquad i = 1, \ldots, n$$

(all having the same domain X) is said to form a <u>(linearly) Independent set</u> (note the capital I) provided they satisfy (in the sense of §1)

$$\forall (t_1, \ldots, t_n) : (\Sigma t_i \cdot \underline{v}_i = 0 \Rightarrow (t_1 = \ldots = t_n = 0)).$$

In elementary terms, this means: given arbitrary $\alpha: Y \to X$ and $t_i: Y \to R$ $(i = 1, \ldots, n)$, such that, in $\hom(Y, M)$

$$\Sigma t_i \cdot (\alpha . \underline{v}_i) = 0;$$

then $t_1 = \ldots = t_n = 0$. This condition is stronger than: "$\underline{v}_1,\ldots,\underline{v}_n$ form an independent set in the hom(X,R)-module hom(X,M)"; the extra strength is that for every $\alpha\colon Y \to X$, the $\alpha \cdot \underline{v}_i$ are independent in hom(Y,M). Or, in suggestive terms: $\underline{v}_1,\ldots,\underline{v}_n$ are Independent iff they are universally independent.

Let r be an integer, $0 \leq r \leq n$. We say that the n-tuple (2.3) has Rank $\geq r$, if there exists a jointly epic family $\beta_H\colon X_H \to X$ ($H \in \binom{n}{r}$, where $\binom{n}{r}$ is the set of subsets of $\{1,\ldots,n\}$ consisting of r elements) such that for each H, the family (consisting of r elements in $\hom(X_H,M)$)

$$\beta_H \cdot \underline{v}_k \qquad (k \in H)$$

is independent.

We do not talk about the Rank of (2.3) being <u>equal</u> to r unless r = n.

We are mainly going to be concerned with the R-modules $M = R^k$ (k an integer). An element $\underline{v}\colon X \to R^k$ can be identified with a k-tuple $v_i\colon X \to R$ ($i = 1,\ldots,k$) of elements in R. An element $\underline{\underline{A}}\colon X \to R^{nm}$ may be identified with an $m \times n$ matrix of elements $a_{ij}\colon X \to R$ (a matrix with elements from the ring hom(X,R)), and this in turn may be identified with an m-tuple $\underline{r}_i\colon X \to R^n$ ("the m-tuple of rows") or with an n-tuple: $\underline{s}_j\colon X \to R^m$ ("the n-tuple of columns").

Consider such a matrix $\underline{A}\colon X \to R^{nm}$. We say that its <u>determinant-Rank</u> is $\geq r$, provided there exists a jointly epic family

$$\{\beta_{HK}\colon X_{HK} \to X \mid H \in \tbinom{m}{r},\ \ K \in \tbinom{n}{r}\},$$

such that for each H,K, the $r \times r$ submatrix $\underline{\underline{A}}_{HK}$ picked out of $\underline{\underline{A}}$ by means of H and K has the property that $\beta_{HK} \cdot \underline{\underline{A}}_{HK}$ has invertible determinant (the determinant of the $r \times r$-matrix $\beta_{HK} \cdot \underline{\underline{A}}_{HK}$ over the ring $\hom(X_{HK}, R)$ is computed as usual).

The reader will easily see that this is precisely the interpretation according to §1 of the statement: "at least one of the $r \times r$ submatrices of $\underline{\underline{A}}$ has invertible determinant" (this being formally a disjunction with $\binom{m}{r} \times \binom{n}{r}$ terms). A similar remark holds for the other Rank-definition.

Remark. Note that both rank notions are local in the sense that if the domain X of the set $(\underline{v}_1, \ldots, \underline{v}_n)$ of elements in (2.3) (respectively the domain of the matrix $\underline{\underline{A}}: X \to R^{mn}$) can be covered by a finite family $\{\gamma_j : X_j \to X \mid j \in J\}$, such that, for each j, $(\gamma_j \cdot \underline{v}_1, \ldots, \gamma_j \cdot \underline{v}_n)$ has Rank $\geq r$ (respectively $\gamma_j \cdot \underline{\underline{A}}$ has determinant-Rank $\geq r$), then $(\underline{v}_1, \ldots, \underline{v}_n)$ (respectively $\underline{\underline{A}}$) has Rank (respectively determinant-Rank) $\geq r$.

We shall see now that the field axioms (2.1) and (2.2) are precisely what is needed to prove

Theorem 2.1. For any matrix $\underline{\underline{A}}: X \to R^{nm}$,

$$\text{row-Rank}(\underline{\underline{A}}) \geq r \Leftrightarrow \text{determinant-Rank}(\underline{\underline{A}}) \geq r \Leftrightarrow \text{column-Rank}(\underline{\underline{A}}) \geq r.$$

(Here of course row-Rank$(\underline{\underline{A}}) \geq r$ means that the m-tuple of rows $\underline{r}_i : X \to R^n$ $(i = 1, \ldots, m)$ has Rank $\geq r$; similarly for column Rank).

Proof. We sketch the proof of the first bi-implication; the second then follows by transposing. We start with the easy part (which does not use the axioms (2.1) - (2.2)).

Assume det.-Rank$(\underline{\underline{A}}) \geq r$. So we have a jointly epic family $\{X_{HK} \xrightarrow{\beta_{HK}} X\}$ as above. We shall first prove that for each H,K, the r rows with index from H in the $m \times n$-matrix $\beta_{HK} \cdot \underline{\underline{A}}$ form an Independent set. So let $\alpha \colon Y \to X_{HK}$ and $t_1, \ldots, t_r \colon Y \to R$ be so that

$$\sum_{j_i \in H} t_i \cdot (\alpha . \beta_{HK} . \underline{r}_{j_i}) = 0$$

in $\hom(Y,R^n)$. Since the $r \times n$ matrix in $\hom(Y,X)$ consisting of the rows $\alpha \cdot \beta_{HK} \cdot \underline{r}_{j_i}$ $(j_i \in H)$ has an invertible $r \times r$ subdeterminant (the columns with index from K), we conclude, by standard linear algebra over a commutative ring (namely $\hom(Y,R)$), that the t_i's are all 0.

This proves that $\beta_{HK} \cdot \underline{\underline{A}}$ has row-rank $\geq r$; since this holds for arbitrary HK and the β_{HK} form a finite covering, we conclude by the remark above that $\underline{\underline{A}}$ has row-rank $\geq r$.

The converse implication uses (2.1) and (2.2) (in fact, even for $n = m = 1$, we need (2.2) for "$\{a_{11}\}$ Independent $\Rightarrow$ $\neg(a_{11} = 0)$" and (2.1) for "$\neg(a_{11} = 0) \Rightarrow a_{11}$ invertible"). So let us assume (2.1) and (2.2), and that the $m \times n$-matrix

$$\underline{\underline{A}} \colon X \to R^{nm}$$

(with ij'th entry denoted $a_{ij} \colon X \to R$) has row-Rank $\geq r$. So X can be covered by $\{\beta_H \colon X_H \to X \mid H \in \binom{m}{r}\}$ such that the $m \times n$-matrix $\beta_H \cdot \underline{\underline{A}}$ has the r rows with index from H Independent. By the remark above, it suffices to prove that for each H, the $m \times n$-matrix $\beta_H \cdot \underline{\underline{A}}$ has determinant-

Rank $\geq r$. For simplicity, let us prove this for $H = \{1,\ldots,r\} \subseteq \{1,\ldots,m\}$. For this H, the r first rows of $\beta_H \cdot \underline{\underline{A}}$ are linearly Independent. In particular the set consisting of the first row alone, $\beta_H \cdot \underline{r}_1$, is an independent set. Suppose that $\alpha: Y \to X_H$ is so that

$$(2.4) \qquad \alpha \cdot \beta_H \cdot a_{1j} = 0 \qquad \text{for } j = 1,\ldots,n$$

Consider the 1-element t in the ring $\hom(Y,R)$. Then

$$t \cdot \alpha \cdot \beta_H \cdot \underline{r}_1 = 0 \qquad \text{in } \hom(Y,R^n),$$

by (2.4), so by independence of $\{\alpha \cdot \beta_H \cdot \underline{r}_1\}$, $t = 0$. So in $\hom(Y,R)$, $1 = 0$, whence $Y = \emptyset$ by Axiom (2.2). This proves that the $\beta_H \cdot a_{11},\ldots,\beta_H \cdot a_{1n}$ satisfy the statement

$$\neg \left(\bigwedge_{j=1}^{n} \beta_H \cdot a_{1j} = 0\right)$$

(in the sense of §1). By Axiom (2.1), we therefore conclude that they also satisfy the statement

$$\bigvee_{j=1}^{n} (\beta_H \cdot a_{1j} \text{ is invertible})$$

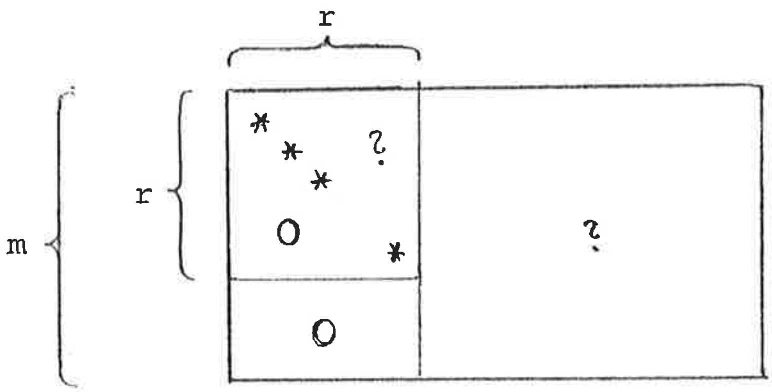
So X_H can be covered by $\{X_{Hj} \xrightarrow{\gamma_j} X_H \mid j = 1,\ldots,n\}$ such that $\gamma_j \cdot \beta_H \cdot a_{1j}$ is invertible, for each $j = 1,\ldots,n$. Again by the remark, it suffices to prove that, for each $j = 1,\ldots,n$ the matrix

$$\gamma_j \cdot \beta_H \cdot \underline{\underline{A}}$$

has determinant-Rank $\geq r$. For simplicity, let us do the case $j = 1$. By construction of the γ_j, the element

$$\gamma \cdot \beta_H \cdot a_{11}$$

is invertible in $\hom(X_{H1}, R)$. Now it is clear that performing admissible row-operations on a matrix does not change its subdeterminants (except for sign), and thus does not change the determinant-Rank, either. (Admissible row-operations: interchanging rows; adding a multiple of one row to another). Also, admissible row operations do not change row rank, because every admissible operation has an inverse admissible operation. So we can use admissible row operations on the matrix $\gamma_1 \cdot \beta_H \cdot \underline{\underline{A}}$ to sweep the first column by the invertible element $\gamma_1 \cdot \beta_H \cdot a_{11}$ to get 0's everywhere in this column except in the top. The considerations now start over again with the $(m-1) \times (n-1)$-matrix of row-rank $r-1$ which we get by deleting first row and first column in $\gamma_1 \cdot \beta_H \cdot \underline{\underline{A}}$. We continue this way $n-1$ times, each time passing to a finer covering. On each part β_ν of the ultimate covering, we have that the matrix $\beta_\nu \cdot \underline{\underline{A}}$ by suitable admissible row-operations (depending on ν) can be brought to a form where a certain $r \times r$ submatrix (depending on ν) is immediately seen to be invertible (for the "lexicographically first" of the ν's, $\beta_\nu \cdot \underline{\underline{A}}$ is transformed to the form



with invertible elements in the places marked *. The upper left $r \times r$ matrix here has invertible determinant (the product of the *-marked elements).)

By the remark, this implies that determinant-Rank($\underline{\underline{A}}$) $\geq$ r. This proves the theorem.

From now on, we of course say that the Rank of an $m \times n$-matrix $\underline{\underline{A}}: X \to R^{nm}$ is $\geq r$ if in one (and therefore in each) of the three Rank-concepts (row, column, determinant), the Rank is $\geq r$.

Many other statements of the character "Independent ⇒ invertible" can now be proved using Theorem 1 as well as standard determinant theory (Cramers rule). As an illustration (which we shall need), we prove (still assuming (2.1) and (2.2) for R):

Theorem 2.2. Let $\underline{\underline{A}}: X \to R^{nm}$ be an $m \times n$ matrix with Independent rows (respectively columns). Then, locally, $\underline{\underline{A}}$ has a right inverse (respectively left inverse).

Stated more elementary, there exists an epic map $\beta: Y \to X$ and an $n \times m$-matrix $\underline{\underline{B}}: Y \to R^{mn}$ such that $(\beta.\underline{\underline{A}}) \cdot \underline{\underline{B}}$ is the identity $m \times m$ matrix (respectively, such that $\underline{\underline{B}} \cdot (\beta.\underline{\underline{A}})$ is the identity $n \times n$ matrix).

Proof. Given $\underline{\underline{A}}$, an $m \times n$ matrix over the ring hom(X,R). To find $\underline{\underline{B}}$ such that

$$(2.5) \qquad \underline{\underline{A}} \cdot \underline{\underline{B}} = \underline{\underline{E}}_{mm} \qquad \text{(identity matrix)}$$

amounts to solving m^2 linear equations with nm unknowns (namely the entries b_{ji} of $\underline{\underline{B}}$). The coefficient matrix for this system is

$$(2.6) \qquad \begin{pmatrix} \underline{\underline{A}} & & & 0 \\ & \underline{\underline{A}} & & \\ & & \ddots & \\ 0 & & & \underline{\underline{A}} \end{pmatrix} \qquad (m \text{ copies of } \underline{\underline{A}}).$$

By Theorem 2.1, the determinant-Rank of $\underline{\underline{A}}$ is m, so X can be covered by a finite family $\beta_H: X_H \to X$ $(H \in \binom{n}{m})$ such that $\beta_H \cdot \underline{\underline{A}}$ has the $m \times m$ submatrix corresponding to H (that is, obtained by omitting the $n-m$ columns with index not in H), invertible (its determinant d_H being invertible). On a given of the X_H's, one obtains an $m^2 \times m^2$ submatrix of (2.6) by omitting the "same" $n-m$ columns from each of the $\underline{\underline{A}}$'s (strictly, from each of the $\beta_H \cdot \underline{\underline{A}}$); and this submatrix has invertible determinant, namely d_H^m. Therefore one obtains by Cramers rule <u>explicitly</u> a solution to the system (2.5) (with $\underline{\underline{A}}$ replaced by $\beta_H \cdot \underline{\underline{A}}$). Then

$$\beta: \coprod_{H \in \binom{n}{m}} X_H \twoheadrightarrow X$$

constructed out of the β_H's, and the solutions obtained on each X_H give the desired local solution. - The proof for the case of Independent columns is similar.

We shall need the following standard fact about linear equations over a commutative ring A. It is probably well-known. For A a field, it is the familiar statement that an inhomogeneous system of linear equations has a solution if the rank of the total matrix of the system is no larger than the rank of the coefficient matrix.

<u>Proposition 2.3</u>. Let $\underline{\underline{B}}$ be an $p \times q$ matrix $(p \geq q)$ on A, and assume that B has an invertible $q \times q$ sub-

determinant. Let $\underline{b}$ be a $p \times 1$ matrix such that the $p \times (q+1)$ matrix $(\underline{\underline{B}},\underline{b}) = \tilde{\underline{\underline{B}}}$ has all its $(q+1) \times (q+1)$ subdeterminants equal to 0. Then $\underline{b}$ can be written as a linear combination of the columns $\underline{b}_1,\ldots,\underline{b}_q$ of $\underline{\underline{B}}$.

Proof. Assume for instance that the first q rows of $\underline{\underline{B}}$ have invertible determinant $d \in A$. We may think of $\underline{\underline{B}}$ as the coefficient matrix and $\tilde{\underline{\underline{B}}}$ as the total matrix of a system of p linear equations with q unknowns. The first q equations have a unique solution $(t_1,\ldots,t_q)$ given by Cramers rule:

$$(2.7) \qquad d \cdot t_j = |\underline{b}_1',\underline{b}_2',\ldots,\underline{b}',\ldots,\underline{b}_q'|,$$

the $\underline{b}'$ being put on the j'th place instead of $\underline{b}_j'$. (We denote by $\underline{b}'$ the part of $\underline{b}$ consisting of first q entries; similarly for $\underline{b}_j$). We have to check that these t_i also satisfy the remaining $p-q$ equations. Consider for instance the r'th equation

$$(2.8) \qquad t_1 \cdot b_{r1} + t_2 \cdot b_{r2} + \ldots + t_q \cdot b_{rq} = b_r$$

(where $\underline{b}_r = (b_{r1},b_{r2},\ldots,b_{rq})$, $\underline{b} = (b_1,\ldots,b_q)$). To see that (2.8) holds, replace t_j by the expression for it obtained from (2.7); we then get that (2.8) is equivalent to

$$(2.9) \qquad \sum_{j=1}^{q} |\underline{b}_1',\underline{b}_2',\ldots,\underbrace{\underline{b}'}_{\uparrow \text{ j'th place}},\ldots,\underline{b}_q'| \cdot b_{rj} - d \cdot b_r = 0$$

The left hand side here can be examined: it is the expansion of a certain $(q+1) \times (q+1)$ subdeterminant of $\tilde{\underline{\underline{B}}}$, along its last row hence is 0 by assumption. So the equation (2.9) and thus (2.8) holds.

If $\underline{v}_1,\ldots,\underline{v}_m$ are elements $X \to M$, where M is an R-module (here R can be any commutative ring object), we say that an element $\underline{w}$: $X \to M$ belongs to $\mathrm{Span}(v_1,\ldots,\underline{v}_m)$, provided there exists an epic β: $X' \twoheadrightarrow X$ and an m-tuple t_i: $X' \to R$ $(i = 1,\ldots,m)$, such that, in $\hom(X',M)$

$$\Sigma t_i \cdot (\beta.\underline{v}_i) = \beta.\underline{w}.$$

In general, $\mathrm{Span}(\underline{v}_1,\ldots,\underline{v}_m)$ will be larger than the $\hom(X,R)$-submodule $\mathrm{span}(\underline{v}_1,\ldots,\underline{v}_m)$ of $\hom(X,M)$ generated by the $\underline{v}_i$. (If the set $\underline{v}_1,\ldots,\underline{v}_m$ is Independent, it will not be larger, because of the principle "unique existence implies global existence".)

We now apply this for the case $M = R^n$. Let

$$\underline{\underline{A}}: X \to (R^n)^p$$

and

$$\underline{\underline{B}}: X \to (R^n)^q$$

be two matrices with same domain X, of size $p \times n$ and $q \times n$, respectively. We say $\underline{\underline{B}} \leq \underline{\underline{A}}$ if each row of the $\underline{\underline{B}}$-matrix belongs to the Span of the set of rows of the matrix $\underline{\underline{A}}$. This defines a preorder-relation $\leq$ on the set of matrices with n columns having X as domain. If α: $Y \to X$ is arbitrary and $\underline{\underline{B}} \leq \underline{\underline{A}}$, then also $\alpha.\underline{\underline{B}} \leq \alpha.\underline{\underline{A}}$. If $\underline{\underline{A}}$ has a $p \times p$ submatrix $X \to R^{pp}$ which has invertible determinant, and $\underline{\underline{B}} \leq \underline{\underline{A}}$, then the coefficients t_{jk} used to display the rows of $\underline{\underline{B}}$ as linear combinations of the rows of $\underline{\underline{A}}$ are unique, hence globally defined, t_{jk}: $X \to R$, by "unique implies global". Using this principle once more, we see that it is even enough to assume that $\underline{\underline{A}}$ has determinant-Rank p to get the coefficients t_{jk} globally defined, $t_{jk}: X \to R$.

Combining this observation with Proposition 2.3 (transposed), we get (by considering the ring hom(X,R)):

Proposition 2.4. Let $\underline{\underline{A}}: X \to (R^n)^p$ be a $p \times n$ matrix of determinant-Rank p. If $\underline{\underline{B}}: X \to (R^n)^q$ is a $q \times n$-matrix such that all $(p+1) \times (p+1)$ subdeterminants of the $(p+q) \times n$ matrix $\{\frac{\underline{\underline{A}}}{\underline{\underline{B}}}\}$ are zero, then each of the rows of $\underline{\underline{B}}$ is a linear combination of the rows in $\underline{\underline{A}}$ (with coefficients from hom(X,R)), and, in particular, $\underline{\underline{B}} \leq \underline{\underline{A}}$.

If both $\underline{\underline{A}}$ and $\underline{\underline{B}}$ in the above Propostiton are $p \times n$-matrices of determinant-Rank p, then the coefficients used to write the rows of $\underline{\underline{B}}$ as linear combinations of the rows of $\underline{\underline{A}}$ form a $p \times p$ matrix $\underline{\underline{C}}$ over hom(X,R) with $\underline{\underline{B}} = \underline{\underline{C}} \cdot \underline{\underline{A}}$. The determinant of $\underline{\underline{C}}$, by product rule for determinants, is necessarily invertible, so that $\underline{\underline{C}}$ itself is invertible. So for such matrices $\underline{\underline{A}}$ and $\underline{\underline{B}}$, $\underline{\underline{B}} \leq \underline{\underline{A}}$ is equivalent to $\underline{\underline{A}}$ and $\underline{\underline{B}}$ being congruent modulo the general linear group GL(p) over hom(X,R).

Returning now to the case where R satisfies (2.1) and (2.2), we have

Proposition 2.5. Let $\underline{\underline{A}}$ and $\underline{\underline{B}}$ be matrices $X \to R^{np}$ of size $p \times n$, and both having Rank p. If

$$\neg\ (\underline{\underline{A}} \equiv \underline{\underline{B}} \quad \mathrm{mod} \quad GL(p)),$$

then the $2p \times n$ matrix $\{\frac{\underline{\underline{A}}}{\underline{\underline{B}}}\}$ has Rank $\geq p+1$.

Proof. The conclusion says that the statement

$$\bigvee_{\underline{\underline{H}}} \{\underline{\underline{H}} \text{ has invertible determinant}\}$$

holds, where H runs over the set of $(p+1) \times (p+1)$ submatrices of $\{\frac{\underline{\underline{A}}}{\underline{\underline{B}}}\}$. To prove this conclusion, by (2.1) it is enough to see

(2.10) $$\neg\,(\bigwedge_{\underline{\underline{H}}} \{\det(\underline{\underline{H}}) = 0\})$$

with $\underline{\underline{H}}$ as before. So let $\alpha: Y \to X$ be such that $\det(\alpha.\underline{\underline{H}}) = 0$ for all $\underline{\underline{H}}$. This implies, by Proposition 2.4 that $\alpha.\underline{\underline{B}} \leq \alpha.\underline{\underline{A}}$, and, by the remarks after this Proposition, it even implies that

$$\alpha.\underline{\underline{A}} \equiv \alpha.B \qquad \text{mod} \quad GL(p)$$

in hom(Y,R). Since $\neg(\underline{\underline{A}} \equiv \underline{\underline{B}}$ mod GL(p)) was assumed, we conclude $Y = \emptyset$. This proves (2.10)

3. The Grassmannians.

So far, definitions and theorems have been valid in any regular category $\underline{E}$ with well-behaved coproducts, because we have been dealing with properties of elements (elements in the various hom-sets). This was the algebraic, or formal, side. To get the geometric objects, we need more about the topos structure of $\underline{E}$, namely "representability of first order predicates".

It is standard knowledge that, in an elementary topos, any first order statement φ about elements $X \to B$ in an object B can be represented by a sub-object $B' \rightarrowtail B$ (this means, $X \to B$ factors through B' if and only if it satisfies φ). (See e.g. Mulvey [11] or, for a very precise form, Coste [1]). We call B' the extension of φ.

To get the Grassmannians, however, we need more than "carving out subobjects by means of statements"; we also need the formation of quotients under equivalence relations. The construction which follows, is step for step identical to the usual one for $\underline{E} = \mathcal{S}$.

Let R be a commutative ring object in $\underline{E}$. We let $Y(m,n) \rightarrowtail (R^n)^m$ denote the extension of the statement "$\underline{\underline{A}}$ is an $m \times n$-matrix of determinant-Rank m". In other words, a map

$$\underline{\underline{A}}: X \to (R^n)^m$$

factors through $Y(m,n)$ if and only if the $m \times n$ matrix $\underline{\underline{A}}$ (with entries from $\hom(X,R)$) has determinant-Rank m. The object $Y(m,m) \rightarrowtail R^{mm}$ is denoted $GL(m)$. It is a group object under matrix multiplication, and it acts on $Y(m,n)$ on the left, again by matrix multiplication:

$$\text{act:} \qquad GL(m) \times Y(m,n) \to Y(m,n).$$

Out of this action is constructed a relation

$$(3.1) \qquad GL(m) \times Y(m,n) \xrightarrow{\langle act, proj_2 \rangle} Y(m,n) \times Y(m,n)$$

The fact that this map is monic is seen as follows. If

$$(3.2) \qquad \langle \underline{\underline{C}}_i, \underline{\underline{A}} \rangle : X \to GL(m) \times Y(m,n) \qquad i = 1,2$$

is given, then X can be covered by $\binom{n}{m}$ pieces X_H such that on the piece X_H, the matrix $X_H \xrightarrow{\beta_H} X \xrightarrow{\underline{\underline{A}}} Y(m,n)$ has the $m \times m$ submatrix indexed by H invertible. From this easily follows that, over the ring $hom(X_H, R)$, $\beta_H \underline{\underline{C}}_1 \cdot \beta_H \underline{\underline{A}} = \beta_H \underline{\underline{C}}_2 \cdot \beta_H \underline{\underline{A}}$ implies $\beta_H \cdot \underline{\underline{C}}_1 = \beta_H \cdot \underline{\underline{C}}_2$. Since the β_H's are joint epic, we conclude that $\underline{\underline{C}}_1 \cdot \underline{\underline{A}} = \underline{\underline{C}}_2 \cdot \underline{\underline{A}}$ implies $\underline{\underline{C}}_1 = \underline{\underline{C}}_2$.

Since $GL(m)$ is a group object and (3.1) is monic, (3.1) actually describes an equivalence-relation on the object $Y(m,n)$. (It is in fact the extension of the previously discussed relation "congruence $\mathrm{mod}\, GL(m)$", as it appears in Proposition 2.5.)

We can also represent the relation $\leq$ between matrices with same number of columns, as it appears in Proposition 2.4. This gives a subobject

$$\textcircled{\leq} \rightarrowtail (R^n)^q \times (R^n)^p$$

having the property that $\langle \underline{\underline{B}}, \underline{\underline{A}} \rangle : X \to R^{nq} \times R^{np}$ factors through $\textcircled{\leq}$ if and only if each of the rows in $\underline{\underline{B}}$ belongs to Span of the set of rows of $\underline{\underline{A}}$. We consider the intersection of this $\textcircled{\leq}$ with $Y(q,n) \times Y(p,n)$. This gives a subobject

(3.3) $$\textcircled{\le} \rightarrowtail Y(q,n) \times Y(p,n).$$

It equals $\emptyset$ if $q > p$. If $q = p = m$, it equals the equivalence relation (3.1). Finally, we remark that the relation (3.3) is saturated under the action of $GL(q)$ and $GL(p)$. More precisely, we have that if

$$\underline{\underline{B}}: X \to Y(q,n), \qquad \underline{\underline{A}}: X \to Y(p,n)$$

and

$$\underline{\underline{C}}: X \to GL(q)\ , \qquad \underline{\underline{D}}: X \to GL(p),$$

then

$$\underline{\underline{B}} \le \underline{\underline{A}} \qquad \text{iff} \qquad \underline{\underline{C}} \cdot \underline{\underline{B}} \le \underline{\underline{D}} \cdot \underline{\underline{A}}\ .$$

We can now describe the objects of our main concern here, the Grassmannians. We denote by $G(m,n)$ the quotient object of $Y(m,n)$ under the equivalence relation (3.1) (congruence mod $GL(m)$). Because of the stability which we just noted, the relation $\textcircled{\le}$ gives rise to a relation

(3.5) $$\textcircled{\le} \rightarrowtail G(q,n) \times G(p,n).$$

It has the property that $\langle a,a' \rangle : X \to G(q,n) \times G(p,n)$ factors through $\textcircled{\le}$ if and only if for some (or equivalently, for every) commutative diagram of the form

$$\begin{array}{ccc} X' & \xrightarrow{\langle \underline{\underline{A}},\underline{\underline{A}}' \rangle} & Y(q,n) \times Y(p,n) \\ \big\downarrow & & \big\downarrow \\ X & \xrightarrow[\langle a,a' \rangle]{} & G(q,n) \times G(p,n) \end{array}$$

$\langle \underline{\underline{A}}, \underline{\underline{A}}' \rangle$ factors through $(\leq) \rightarrowtail Y(q,n) \times Y(p,n)$.

The objects $G(q,n)$ (for fixed n) together with the relations $(\leq)$ form a certain combinatorial structure in the topos $\underline{E}$, "projective $(n-1)$-space of the ringed topos $\underline{E}, R$". I believe that, without further assumptions on R, not much of synthetic or combinatorial projective geometry holds for this (unless you introduce a separate "apartheid relation" ω). However, in case R satisfies the axioms (2.1) and (2.2), then some synthetic geometry does work. We illustrate this by considering the projective plane $G(1,3)$, $G(2,3)$. We assume throughout from now that R satisfies (2.1) and (2.2). We denote $G(1,3)$ by $\mathbb{P}$ ("the object of points), $G(2,3)$ by $\mathbb{L}$ ("the object of lines"), and the relation $(\leq) \rightarrowtail G(1,3) \times G(2,3)$ is of course called 'incidence' (or 'lies on', or 'passes through').

Theorem 3.1. Through two different points passes a unique line.

Proof. We must prove that if two elements $a_1, a_2 : X \to \mathbb{P}$ satisfy the statement

$$\neg (a_1 = a_2),$$

then also

(3.6) $$\exists ! \ell : a_1 \leq \ell \wedge a_2 \leq \ell \qquad (\ell \text{ in } \mathbb{L})$$

is satisfied.

We first construct (for instance by pull-back) a commutative diagram

$$\begin{array}{ccc} X' & \xrightarrow{\langle \underline{a}_1,\underline{a}_2\rangle} & Y(1,3)\times Y(1,3) \subseteq R^{31}\times R^{31} = (R^3)^2 \\ \beta\Big\downarrow & & \Big\downarrow \\ X & \xrightarrow[\langle a_1,a_2\rangle]{} & G(1,3)\times G(1,3) \quad . \end{array}$$

Since $\neg(a_1 = a_2)$ holds, we conclude that

$$\neg(\underline{a}_1 \equiv \underline{a}_2 \mod GL(1)).$$

By Proposition 2.5, the 2×3 matrix

$$X' \xrightarrow{\{\underline{a}_1 \atop \underline{a}_2\}} (R^3)^2$$

has Rank ≥ 2, hence has Rank 2, thus defines

$$X' \xrightarrow{\ell'} Y(2,3).$$

Clearly $(\underline{a}_1 \leq \ell')\wedge(\underline{a}_2 \leq \ell')$ holds, which proves the conclusion (3.6) in so far as existence is concerned. Uniqueness is seen as follows. If $\alpha\colon Y \to X$, $\ell\colon Y \to G(2,3)$

$$a_1 \leq \ell \qquad a_2 \leq \ell,$$

then, on $Y' = Y \underset{X}{\times} X'$, one has (omitting some greek letters)

$$\ell' = \{\underline{a}_1 \atop \underline{a}_2\} \leq \ell$$

with both ℓ and ℓ' elements of $Y(2,3)$. But we remarked that $\textcircled{\leq} \rightarrowtail Y(2,3) \times Y(2,3)$ was the same relation as congruence mod $GL(2)$.

Notation. If $a_1, a_2 \colon X \to \mathbb{P}$ satisfy $\neg(a_1 = a_2)$, then the theorem guarantees the existence of a unique element $\ell \colon X \to \mathbb{L}$ with $a_1 \leq \ell$ and $a_2 \leq \ell$. We denote this ℓ by $[a_1 a_2]$.

Theorem 3.2. Two different lines pass through a unique point.

Proof. We must prove that if two elements $\ell_1, \ell_2 \colon X \to \mathbb{L}$ satisfy the statement

$$\neg(\ell_1 = \ell_2),$$

then also

$$\exists ! a\colon a \leq \ell_1 \wedge a \leq \ell_2 \qquad (a \text{ in } \mathbb{P}). \tag{3.7}$$

We first construct (for instance by pull-back) a commutative diagram

$$\begin{array}{ccc}
X' & \xrightarrow{\langle \underline{\underline{A}}_1, \underline{\underline{A}}_2 \rangle} & Y(2,3) \times Y(2,3) \subseteq (R^3)^2 \times (R^3)^2 \\
\downarrow & & \downarrow \\
X & \xrightarrow[\langle \ell_1, \ell_2 \rangle]{} & G(2,3) \times G(2,3)
\end{array}$$

Since $\neg(\ell_1 = \ell_2)$ holds, we conclude

$$\neg(\underline{\underline{A}}_1 \equiv \underline{\underline{A}}_2 \quad \text{mod } GL(2)).$$

By Proposition 2.5, the 4×3 matrix

$$\underline{\underline{A}} = \{{\underline{\underline{A}}_1 \atop \underline{\underline{A}}_2}\}$$

has Rank ≥ 3, hence Rank 3. Consider the element $\underline{t}$

$$\underline{t} = (t_1, t_2, t_3, t_4) : X' \to R^4$$

where t_i is $(-1)^i$ times the 3×3 subdeterminant of $\underline{\underline{A}}$ obtained by omitting the i'th row. Then

$$\underline{t} \cdot \underline{\underline{A}} = 0 \tag{3.7}$$

as (1×3)-matrices in $\hom(X', R)$ (the fact that the k'th entry, $k = 1,\ldots,3$, is 0 in this matrix, is seen by adding the k'th column of $\underline{\underline{A}}$ to the right of $\underline{\underline{A}}$ to obtain 4×4 matrix with 0 determinant; expanding this determinant along its last column gives (3.7)). Also, since the determinant-Rank of $\underline{\underline{A}}$ is 3, the 1×4 matrix $\underline{t}$ has Rank 1. By (3.7), we have

$$(t_1, t_2) \cdot \underline{\underline{A}}_1 = -(t_3 \cdot t_4) \cdot \underline{\underline{A}}_2 . \tag{3.8}$$

Since $\mathrm{Rank}(\underline{t}) = 1$, we have that X' is covered by two pieces X_1' and X_2', such that on X_1', (t_1, t_2) has Rank 1 and on X_2' (t_3, t_4) has Rank 1. $\underline{\underline{A}}_1$ locally has a right inverse $\underline{\underline{B}}$, by Theorem 2.2; multiplying (3.8) on the right by $\underline{\underline{B}}$ we get that on X_1', (t_1, t_2) is locally of form $-(t_3, t_4) \cdot \underline{\underline{A}}_2 \cdot \underline{\underline{B}}$, so that also (t_3, t_4) has Rank 1 on X_1'. So we conclude that (t_1, t_2) (as well as (t_3, t_4)) has Rank 1 (on the whole of X'). The point to be constructed "on the intersection of the two lines" can now be taken to be represented by the 1×3-matrix $\underline{a} = (t_1,t_2) \cdot \underline{\underline{A}}_1$ which has Rank 1 because (t_1,t_2) has Rank 1, and $\underline{\underline{A}}_1$ Rank 2). Clearly $\underline{a} \leq \underline{\underline{A}}_1$, and, by (3.8), $\underline{a} \leq \underline{\underline{A}}_2$. This proves the existence. To prove uniqueness amounts to proving that any two Rank 1-solutions $\underline{t}'$ and $\underline{t}''$ to (3.7) must be congruent mod GL(1). Consider a $\beta\colon X'' \to X'$ such that the top 3×3 submatrix has invertible determinant. On this X'', the bottom row $\underline{r}_4$ of $\underline{\underline{A}}$ can be written as a linear combination of the three first rows $\underline{r}_1,\underline{r}_2,\underline{r}_3$ (essentially by Cramers rule);

$$(3.8_1) \qquad \sum_{i=1}^{3} t_i'\underline{r}_i + \underline{r}_4 = 0$$

Suppose we have $(t_1,\ldots,t_4)$ satisfying (3.7). This means

$$(3.9) \qquad \sum_{i=1}^{4} t_i\underline{r}_i = 0$$

Multiply (3.8_1) by t_4 and subtract it from (3.9). This yields

$$\sum_{i=1}^{3} (t_i - t_4 t_i') \cdot \underline{r}_i .$$

Since the $\underline{r}_1,\underline{r}_2,\underline{r}_3$ are Independent on X'', this implies that

$$(3.10) \qquad t_i = t_4 \cdot t_i' \qquad i = 1,2,3$$

Thus, on X'', the solution $(t_1,\ldots,t_4)$ is proportional to $(t_1',t_2',t_3',1)$ with t_4 as factor. If $(t_1,\ldots,t_4)$ has Rank 1, it follows from (3.10) that t_4 is invertible, (and unique). So X can be covered by (four) pieces X'' on each of which Rank 1 solutions to (3.7) are proportional. The uniqueness statement in the theorem now follows, since the relation $\leq$ between 1×4 matrices of Rank 1 is equivalent to '$\equiv$ mod GL(1)', as we have observed. - Note that the simpler argument "if there were two distinct intersection points, the two lines ℓ_1 and ℓ_2 would be equal by Theorem 3.1" does not work, since we may well have points a_1, a_2 which are distinct, but not "universally distinct: $\neg(a_1 = a_2)$.

Notation. If $\ell_1, \ell_2 : X \to \mathbb{L}$ satisfy $\neg(\ell_1 = \ell_2)$, then the theorem guarantees the existence of a unique element $a: X \to \mathbb{P}$ with $a \leq \ell_1$ and $a \leq \ell_2$. We denote this a by $\ell_1 \cap \ell_2$.

The following theorem shows that the relation $\neg(a = b)$ satisfies Heytings Axiom II e [6] for the apartheid relation ω; for projective geometry over a field in the category of sets, the statement is empty (belongs to logic). For the more general situation here, this is not so.

Theorem 3.3. Let a and $b: X \to \mathbb{P}$ be given, and assume $\neg(a = b)$. For any $c: X \to \mathbb{P}$,

$$\neg(a = c) \vee \neg(b = c)$$

holds.

Proof. Let a be represented by

$$\begin{array}{ccc} X' & \xrightarrow{\quad \underline{a} \quad} & Y(1,3) \subseteq R^3 \\ {\scriptstyle \beta}\downarrow & & \downarrow \\ X & \xrightarrow[\quad a \quad]{} & \mathbb{P} \end{array}$$

with $\underline{a} = (a_1, a_2, a_3)$, and similarly for $\underline{b}$ and $\underline{c}$ (we may choose the same X'). The conclusion to be proved is now equivalent to proving a certain statement about the matrix

$$\underline{\underline{D}} = \begin{Bmatrix} a_1 & a_2 & a_3 \\ b_1 & b_2 & b_3 \\ c_1 & c_2 & c_3 \end{Bmatrix}$$

namely

(3.11) $$\bigvee_H (\det(H) \text{ is invertible})$$

where H runs over the set of those 2×2 submatrices of D which contain two elements from the $\underline{c}$-row. Now $\underline{c}: X' \to R^3$ has rank 1, so X' can be covered by three pieces X'_i $i = 1,2,3$, such that on X'_i, c_i is invertible. It is clearly enough to prove the conclusion (3.11) on each of the three pieces. Let us consider the first, where c_i is invertible. By (2.1), it is enough to prove

(3.12) $$\neg \left(\bigwedge_H \det(H) = 0\right)$$

where H runs over the same set of six 2×2 submatrices as in (3.11). If $\alpha: Y \to X_1'$ is so that these six determinants are 0 in hom(Y,R), we have here

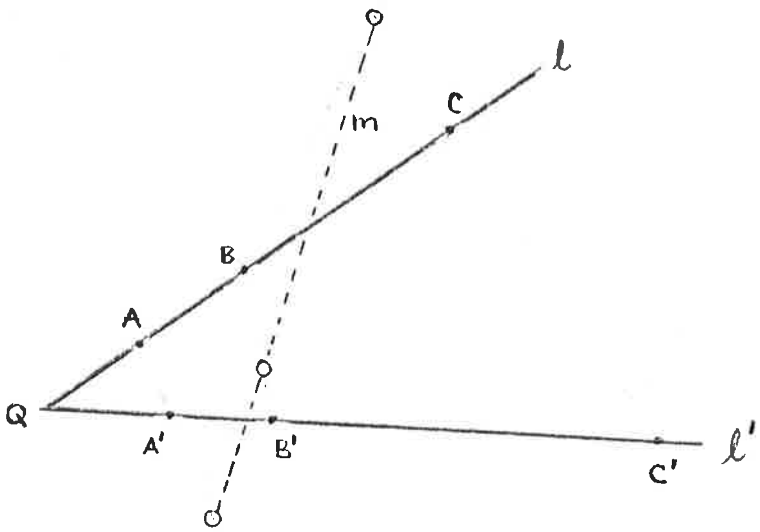
$$a_1c_2 = c_1a_2 \qquad a_1c_3 = c_1a_3$$
$$b_1c_2 = c_1b_2 \qquad b_1c_3 = c_1b_3$$

From this follows that the two last columns in the 2×3 matrix $\{\frac{\underline{a}}{\underline{b}}\}$ are proportional to the first (with factors $c_2 \cdot c_1^{-1}$ and $c_3 \cdot c_1^{-1}$, respectively. Since $\neg(\underline{a} \equiv \underline{b}$ mod GL(1)) was assumed, we conclude that $Y = \emptyset$. This proves (3.12) and thus the theorem.

We can now prove

Theorem 3.4. (Pappos' Theorem) Let ℓ and ℓ' be lines such that $\neg(\ell_1 = \ell_2)$. Let A,B,C be points on ℓ, and A',B',C' points on ℓ'. Assume that for U and V any two of these six points we have $\neg(U = V)$. Then $\neg([AA'] = [B'C])$, $\neg([A'B] = [CC'])$ and $\neg([BB'] = [C'A])$, and there is a unique line m such that

$$[AA'] \cap [B'C] \leq m$$
$$[A'B] \cap [CC'] \leq m$$
$$[BB'] \cap [C'A] \leq m$$



Proof. Some preparations are necessary before the problem is reduced to linear algebra. Let $Q = \ell \cap \ell'$ denote the point $Q: X \to \mathbb{P}$ where ℓ and ℓ' intersect (X being the common domain of $A,B,C,A',B',C': X \to \mathbb{P}$ and $\ell,\ell': X \to \mathbb{L}$). Denote by a the statement $\neg(Q = A)$, by b the statement $\neg(Q = B),\ldots,$ by c' the statement $\neg(Q = C')$. Since $\neg(A = B)$ we have by Theorem 3.3 that

$$a \vee b.$$

Similarly, we get the other factors in the conjunction

$$(3.13) \qquad (a \vee b) \wedge (a \vee c) \wedge (b \vee c) \wedge (a' \vee b') \wedge (a' \vee c') \wedge (b' \vee c').$$

Now $\wedge$ distributes over $\vee$ in intuitionistic logic; so it is easy to see that (3.13) implies

$$(a \wedge a') \vee (b \wedge b') \vee (c \wedge c').$$

So the domain X can be covered by three pieces X_i, so that, on the first, for instance, $a \wedge a'$ holds. Let us consider this piece and prove the theorem there. This is enough since the conclusion is of local nature. So we can assume $\neg(Q = A) \wedge \neg(Q = A')$. Let $\underline{q},\underline{a}$ and $\underline{a}'$ be 1×3-matrices representing Q,A and A', respectively, all with domain X'. The matrix

$$(3.14) \qquad \begin{Bmatrix} q_1 & q_2 & q_3 \\ a_1 & a_2 & a_3 \\ a'_1 & a'_2 & a'_3 \end{Bmatrix}$$

has Rank 3. To see this, note first that $\neg(Q = A)$ implies that the two first row form a 2×3 matrix of Rank 2, thus is a representative in $Y(2,3)$ of ℓ. Similarly, the first and third row yield a representative of ℓ'. Since $\neg(\ell = \ell')$ these two 2×3 matrices of Rank 2 are (universally) non-congruent mod GL(2). Thus, placing them on top of each other yields a 4×3-matrix of Rank 3, by Proposition 2.5. This 4×3 matrix is just (3.14) with the q row repeated. Therefore (most easily using row-Rank), (3.14) has Rank 3.

Since now this matrix is invertible, we can express all elements in $\hom(X',R^3)$ uniquely as linear combinations of the three rows in (3.14). These new coordinates are, respectively:

$$\begin{aligned} Q &: (1,0,0) \\ A &: (0,1,0) \\ A' &: (0,0,1) \\ B &: (\beta_1,\beta_2,0) \end{aligned}$$

Since $\neg(A = B)$, the Rank of

$$\begin{Bmatrix} 0 & 1 & 0 \\ \beta_1 & \beta_2 & 0 \end{Bmatrix}$$

is 2, by Proposition 2.5, and therefore β_1 is invertible. Thus we may replace the representative $(\beta_1,\beta_2,0)$ of B by the simpler $\{1,\beta,0\}$ for suitable β. Similarly for B',C and C'

$$\begin{aligned} B &: (1,\beta,0) \\ B' &: (1,0,\beta') \\ C &: (1,\gamma,0) \\ C' &: (1,0,\gamma') \end{aligned}$$

To see that $\neg([AA'] = [B'C])$ it suffices (by the easy converse of Proposition 2.5) to see that the matrix

$$\begin{Bmatrix} 0 & 1 & 0 \\ 0 & 0 & 1 \\ 1 & 0 & \beta' \\ 1 & \gamma & 0 \end{Bmatrix}$$

has Rank 3, which is obvious. The other non-equalities in the statement of the theorem are proved similarly. The three intersection points mentioned in the theorem can now each be found by a procedure similar to the solution of (3.7). The three solutions thus found are written into the rows of the matrix

$$\begin{Bmatrix} 0 & -\gamma & \beta' \\ -\gamma & -\beta\gamma & \beta\gamma'-\gamma\gamma' \\ \beta' & \beta\beta'-\beta\gamma' & \beta'\gamma' \end{Bmatrix} \tag{3.15}$$

The line m is uniquely determined by the rows of this matrix; to see this, we have to verify that the determinant is 0 and that the Rank is ≥ 2. It is easy to compute the determinant. To verify the Rank-condition, we use Theorem 3.3 to conclude

$$\neg(C = Q) \vee \neg(B' = Q)$$

Covering X' by two pieces as usual, we get on the piece where $\neg(C = Q)$ that γ is invertible; the upper left 2×2 matrix has determinant $-\gamma^2$, which is invertible on this piece. On the piece where $\neg(B' = Q)$, β' is invertible. The matrix obtained by omitting middle row and middle column has determinant $-\beta'^2$, which is invertible on this piece. So the Rank of (3.15) is ≥ 2.

4. On a transfer principle in geometry.

E. Study [13] found around 1900 a remarkable principle for transferring statements about spherical geometry into statements about the 4-dimensional manifold of lines in Euclidean 3-space. It rests on a change-of-rings from the reals $\mathbb{R}$ to the ring of dual numbers $\mathbb{R}[\varepsilon]$ over $\mathbb{R}$ $(\varepsilon^2 = 0)$: a point on the "unit sphere" relative to $\mathbb{R}[\varepsilon]$ may be interpreted as an oriented line as follows: If $\underline{a} + \varepsilon\underline{b}$ has norm 1 (with $\underline{a}$ and $\underline{b}$ in $\mathbb{R}^3$), then $||\underline{a}|| = 1$ and $\underline{a} \cdot \underline{b} = 0$; to this vector in $(\mathbb{R}[\varepsilon])^3$ is associated the oriented line whose direction is $\underline{a}$ and whose momentum around the origin is $\underline{b}$. If one takes the projective plane instead of the unit sphere, the correspondence is between $\mathbb{R}[\varepsilon]$-points in the projective plane, and unoriented lines in space. What corresponds to lines in the projective plane are then <u>line-stacks</u> in the space-of-lines: a line stack being the set of all those lines which intersect a given line (the <u>axis</u> of the stack) at right angles.

As an example of how statements of spherical geometry transfers to statements about line-geometry, Klein [7] gives the example how the theorem: "The altitudes of a spherical triangle intersect" interpreted over $\mathbb{R}[\varepsilon]$ by the Study principle yields the theorem: "If all angles of a hexagon in space are right, then the three lines which occur as common perpendiculars (or orthogonal transversals) for the three pairs of opposite sides of the hexagon, have a common orthogonal transversal". (This, however, involves a metric on the sphere. Below we give an example which does not).

It seems natural to seek the "generic" true statements of, say, spherical geometry (that is, statements which hold for "the sphere" over every commutative ring), in the topos $\mathbb{S}^{\mathcal{R}}$ of functors from the category of commutative rings $\mathcal{R}$ (with some size limination)* into the category $\mathbb{S}$ of sets. The "sphere" object here is the functor which associates to a ring A the set of $(a_1,a_2,a_3) \in A^3$ with $\Sigma a_i^2 = 1$. However, the geometric objects become better when one passes to the Zariski-topos $\mathfrak{Z} \subseteq \mathbb{S}^{\mathcal{R}}$. This topos (denoted $\mathcal{S}_1$ in Hakim [4], $\widetilde{ME}$ in [2]) has a ring-object R which satisfies (2.1) and (2.2). Further, Hakim proved that R is a local ring-object: for every $a: X \to R$, the statement

$$(a \text{ is invertible}) \vee (1-a \text{ is invertible})$$

holds, and further, that $(\mathfrak{Z}, R)$ is universal with this property: given any local-ringed topos $(\mathfrak{X}, A)$, there is a unique (up to isomorphism) geometric morphism

$$f: \mathfrak{X} \to \mathfrak{Z}$$

such that $f^*(R) \cong A$. (See [4], III.(3.10)). In particular, every statement, which holds for R in $\mathfrak{Z}$, and whose syntactic form is so that its validity is preserved by inverse-image functors of geometric morphisms, hold for any local-ringed topos. These 'transferable' statements φ can be described as follows (let us assume they are statements in the language of the theory of commutative rings). First, we describe the "strongly transferable statements". These are built from equations by means of conjunction, disjunction and existential quantification. If $\varphi(X_1,\dots,X_n)$ and $\psi(X_1,\dots,X_n)$ are such strongly transferable statements, then

$$(\varphi(X_1,\dots,X_n) \Rightarrow \psi(X_1,\dots,X_n))$$

* see footnote p. 42.

is a transferable statement (predicate)**. For instance, the property of being a local ring is transferable, because A being a local ring is expressed by

$$(\exists b:\ a\cdot b = 1 \quad \vee \quad \exists b:(1-a)\cdot b = 1).$$

The properties (2.1) and (2.2) are not transferable, because they in $\mathfrak{S}$ describe the notion of field; if these statements were transferable, it would follow from the universal property of $(\mathfrak{Z}, R)$ that every local ring was a field. Likewise, Theorem 3.1, 3.2 and 3.3 are not transferable because they have the form

$$(4.1) \qquad \neg(a=b) \Rightarrow (\exists \ell:\ a \leq \ell \wedge b \leq \ell)$$

Nevertheless, we would like to transfer them, in particular (to get the Study-type examples), to transfer them along the inverse image part of that

$$(3.2) \qquad f:\ \mathfrak{S} \to \mathfrak{Z},$$

where $f^*(R) = \mathbb{R}[\varepsilon]$ ($\mathbb{R}[\varepsilon]$ being a local ring). This is achieved, essentially, by introduction of a transferable $a\omega b$ (a is apart from b) to replace the antecedent $\neg(a=b)$ in (4.1). More precisely, if R is any commutative ring object, we may, for given

$$X \xrightarrow{a} G(1,3) \qquad X \xrightarrow{b} G(1,3)$$

write $a\omega b$ to mean that for some (or equivalently, for any)

** more precise description can be found in the work of Reyes [12], and Lawvere [10].

matrix representatives $\underline{a}$ and $\underline{b}$ of a and b

$$X' \xrightarrow{\underline{a}} Y(1,3) \qquad X' \xrightarrow{\underline{b}} Y(1,3),$$

the determinant-Rank of the 2×3 matrix $\{\frac{\underline{a}}{\underline{b}}\}$ is 2. If R satisfies (2.1) and (2.2), this is, by Proposition 2.5, equivalent to $\neg(\underline{a} \equiv \underline{b} \mod GL(1))$, so $a\,\omega\,b \Leftrightarrow \neg(a = b)$, in this case. - Similarly for lines: $\ell\,\omega\,\ell'$ if two representing 2×3 matrices $\underline{\underline{A}}$ and $\underline{\underline{A}}'$ when put on top of each other yields a 4×3 matrix of determinant-Rank 3. Again, if (2.1) and (2.2) holds, $\ell\,\omega\,\ell' \Leftrightarrow \neg(\ell = \ell')$. In particular, Pappos' Theorem 3.4 may be rewritten, writing $x\,\omega\,y$ everywhere instead of $\neg(x = y)$. Then it is transferable. More precisely, let

$$f\colon \mathcal{X} \to \mathcal{Y}$$

be any geometric morphism between elementary toposes, and let R be a commutative ring object in $\mathcal{Y}$. Because of the exactness of the functor $f^*\colon \mathcal{Y} \to \mathcal{X}$, the whole construction of $G(p,n)$ and $\textcircled{\le}$ commutes with f^*, i.e. if $G(p,n)_R$ denotes the Grassmannian constructed out of R in $\mathcal{Y}$, and $G(p,n)_{f^*(R)}$ the Grassmannian constructed out of $f^*(R)$ in $\mathcal{X}$ (in both cases using the recipe of Section 3), then

$$f^*(G(p,n)_R) \cong G(p,n)_{f^*(R)}.$$

Also the incidence relation $\textcircled{\le} \to G(q,n) \times G(p,n)$ as well as the apartheid-relation $\omega \to G(p,n) \times G(p,n)$ (described above for the case $p = 1,2$, $n = 3$), are preserved in the same sense.

In the local-ringed topos $(\mathcal{S}, \mathbb{R}[\varepsilon])$, if $G(1,3)$ is interpreted as the set of lines in Euclidean 3-space, the relation $\omega \rightarrowtail G(1,3) \times G(1,3)$ is interpreted as "pairs of non-parallel lines"; the relation $G(2,3) \times G(2,3)$ is interpreted as "pairs of line stacks with non-parallel axes". Finally, incidence $\leq$ between lines and line-stacks is interpreted just as the relation of a line belonging to a line stack. This is the "Study interpretation".

We can now transfer Pappos' Theorem to a theorem about line geometry, by applying the $f: \mathcal{S} \to \mathcal{Z}$ with $f^*(R) = \mathbb{R}[\varepsilon]$, and the Study interpretation. (Of course, this application of the transfer principle is no different or deeper than the ones known to Study; the difference in viewpoint is that here it is actually a theorem <u>about</u> something (projective plane in $\mathcal{Z}$) which is transferred). To state it in manageable form, by the <u>transversal</u> of two non-parallel lines, we mean the unique line intersecting both of them at right angles.

<u>Theorem 4.1</u>. Let two line stacks* L and L' be given with non-parallel axes. Let a,b,c be lines of L, and a'b'c' lines of L'. All these six lines are assumed to be mutually non-parallel. Then the transversal of a,a' is not parallel to the transversal of b',c; let the transversal of these two transversals be denoted ℓ_1. Similarly ℓ_2 is constructed out of (a',b;c,c') and ℓ_3 out of (b,b';c',a). Then there is a unique line m intersecting ℓ_1, ℓ_2 and ℓ_3 at right angles.

---

* Recall that a <u>line stack</u> with axis m (m a line) was defined as the set of lines intersecting m at right angles.

BIBLIOGRAPHY

1. Seminaire Benabou 1973/74, Exposé de M. Coste, Logique du 1er ordre dans les topos elementaires

2. Demazure and Gabriel, Groupes Algebraiques, North-Holland 1970.

3. Demazure, Grothendieck et al., Schémas en Groupes I (SGA 3), Springer Lecture Notes Vol. 151 (1970).

4. Hakim, Topos anneles et Schémas relatifs, Springer Verlag 1972.

5. Heyting, Die Theorie der linearen Gleichungen in einer Zahlenspezies mit nichtkommutativer Multiplikation, Math. Annalen 98 (1928), 465-490.

6. Heyting, Zur intuitionistischen Axiomatik der projektiven Geometrie, Math. Annalen 98 (1928), 491-538.

7. Klein, Höhere Geometrie, Springer Verlag 1926.

8. Kock, Kripke-Joyal semantics, mimeographed manuscript, Aarhus, May 1973.

9. Kock, Lecouturier and Mikkelsen, Some topos-theoretic concepts of finiteness, Aarhus Universitet, Preprint Series 1973/74, No. 29.

10. Lawvere, Continuously variable sets: Algebraic geometry = Geometric logic, Preprint Perugia 1973 (to appear in Proc. of the Logic Coll., Bristol 1973).

11. Mulvey, Non-standard Algebra and Representations of Rings, Preprint, U. of Sussex 1973.

12. Reyes , From sheaves to logic, mimeographed, U. de Montreal, 1972.

13. Study, Geometrie der Dynamen, Leipzig 1903.

- oOo -

Footnote to p. 38:

The size limitation occurring in [4] is: $\mathcal{R}$ is the category of finitely presentable rings. In [2], it is a much larger category. It is $\mathcal{R}$ = category of finitely presented rings which gives $\mathfrak{Z}$ the universal property described.

- oOo -

Aarhus Universitet
June 1974
/ELL