COMMUNICATIONS IN ALGEBRA, 3(6), 545-561 (1975)

LINEAR ALGEBRA IN A LOCAL RINGED SITE

Anders Kock

Aarhus Universitet
Aarhus, Denmark

Introduction

In this article, we develop so much standard linear and multilinear algebra over a commutative local ring object A which is needed for constructing the Grassmann manifolds and proving their basic combinatorial properties (in particular, for constructing "the projective plane" over A; this is a "global" form of classical "Ring-Geometrie", [2], [7]). We push this programme to the algebraic theorem which gives the duality between p-planes and (n-p)-planes in n-space (Corollary 3.3). The geometric motivation for having this theory is given in [8]; a version of [8], simplified by means of the present paper, is in preparation, [9].

When A is a field (in the category of sets), the linear and multilinear algebra given here is standard and can be found for instance in Bourbaki [3]. When A is a (commutative) local ring (in the category of sets), there seems to be no explicit reference; however, in that case it is standard technique to lift the results from the field case by means of the Nakayama lemma.

For the application we have in mind [9], the universal local ring in the Zariski topos, that technique does not work so well, mainly becase even linear algebra over a field object in a site or a non-boolean topos is not (yet) worked out. Such a linear algebra is in some sense equivalent to intuitionistic linear algebra, as developed by Heyting, [5], [6]. Furthermore, the Nakayama lemma does not seem to be there, which makes it natural to take the two steps at once, partly leaving the category of sets in favour of an arbitrary site, partly working over a local ring object instead of a field object.

In the present exposition, I have tried to do things in a direct ad hoc manner, thereby neglecting any attempt of showing how concepts introduced (like the concept of local ring object, or rank of a matrix) are canonical interpretations of certain 1st order logic expressions expressing the same concept in the category of sets. (One observes that all mathematical notions dealt with here (local ring, rank, ...) are formulated in that fragment of 1st order language which Joyal, Reyes and others have called geometric logic, [12].)

In §1, we give the preliminaries about tensor products, duality, and exterior powers, in a very general setting; §2 deals with module theory for an arbitrary commutative ring object in an arbitrary site with products; finally, the results of §3 give the main theorems (3.2 and 3.3), which further depends on the ring object being local (in the sense, slightly generalized, of Hakim [4]). Remark that the site structure (the notion of covering) is needed precisely where the mathematical notions come to involve existential quantifiers.

§1. Tensor products and duality for free module objects

Let $\underline{E}$ be a category with finite products, and A a commutative ring object in it, that is, A comes equipped with

$$A\times A \xrightarrow{+} A, \quad A \xrightarrow{-} A, \quad A\times A \xrightarrow{\cdot} A, \quad 1 \xrightarrow{0} A, \quad 1 \xrightarrow{1} A$$

satisfying associativity, distributivity, etc. (all of which can be expressed in terms of commutativity of certain diagrams in $\underline{E}$, as is well-known (see e.g. [10], Chapter III, §6)). We consider the category Mod(A) of A-module objects M, i.e. the category of abelian group objects M in $\underline{E}$ equipped with an A-action (associative etc.):

$$A \times M \to M;$$

morphisms in Mod(E) being maps $M \to M'$ compatible with the abelian group structures and the actions.

Then Mod(A) is an additive category (in the sense of [10], Ch.III, §2, say), with the biproduct $M_1 \oplus M_2$ being given as $M_1 \times M_2$ with suitable (obvious) A-action and abelian group structure. This means that we can describe maps in terms of matrices:

A map

$$\bigoplus_{j=1}^{n} X_j \xrightarrow{\alpha} \bigoplus_{i=1}^{m} Y_i$$

being given by the $m\times n$ matrix whose ij'th entry is $incl_j.\alpha.proj_i$ (see e.g. [10],VIII, §2).

We shall say that an A-module object M is free if it is isomorphic in $Mod(A)$ to an object of form

$$A^n = A \oplus \ldots \oplus A \qquad (n \text{ times}).$$

For each $X \in |\underline{E}|$ and each $M \in |Mod(A)|$, $hom_{\underline{E}}(X,M)$ carries a canonical structure of an (ordinary) module over $hom(X,A)$ (which canonically is a commutative ring). For each $\xi: X' \to X$, the induced map

$$hom(X,M) \to hom(X',M)$$

is a $hom(X,A)$-module homomorphism.

The maps $M_1 \to M_2$ in $Mod(A)$ are called A-linear maps. But we have also a notion of A-bilinear map.

$$M_1 \times M_2 \overset{\nu}{\to} M_3,$$

where the M_i's are A-module objects. This notion can be described by means of four commutative diagrams in $\underline{E}$, or, more economically, by saying that for each $X \in |\underline{E}|$, the composite

$$hom(X,M_1) \times hom(X,M_2) \cong hom(X,M_1 \times M_2) \xrightarrow{hom(X,\nu)} hom(X,M_3)$$

is $hom(X,A)$-bilinear.

A map ν as above which is A-bilinear, and is universal among A-bilinear maps out of $M_1 \times M_2$, is called a tensor-product of M_1 and M_2 and is denoted

$$M_1 \times M_2 \to M_1 \underset{A}{\otimes} M_2$$

(or just $M_1 \otimes M_2$ if it causes no confusion). It depends bifunctorially on those M_1, M_2 for which it exists. It always exists for a pair of free modules. It suffices to see that $A^n \otimes A^m$ exists. Here $A^{nm} = A^n \otimes A^m$ is going to work. The universal bilinear map ν is constructed by commutativity of the diagrams

$$\begin{array}{ccc} A^n \times A^m \xrightarrow{\ \nu\ } A^n \otimes A^m & = & A^{nm} \\ {\scriptstyle proj_i \times proj_j}\downarrow & & \downarrow{\scriptstyle proj_{<i,j>}} \\ A \times A & \xrightarrow{\quad \cdot \quad} & A \end{array}$$

for each $<i,j> \in n \times m$. Since $proj_i$ and $proj_j$ are linear, and $\cdot$ is bilinear, one easily gets that ν is bilinear. To see its universality: let $\varphi\colon A^n \times A^m \to M$ be bilinear. To construct $\bar{\varphi}\colon A^{nm} \to M$, take the unique $\bar{\varphi}$ which makes all the diagrams

$$\begin{array}{ccc} A & \xrightarrow{\ incl_{<i,j>}\ } & A^{nm} \\ {\scriptstyle <incl_i, incl_j>}\downarrow & & \downarrow{\scriptstyle \bar{\varphi}} \\ A^n \times A^m & \xrightarrow{\quad \varphi \quad} & M \end{array}$$

commute (using that A^{nm} is also a coproduct of its nm factors).

From the explicit construction of $A^n \otimes A^m$ and from the fact that it works in any category with $\times$, we conclude that for each pair of free A-module objects M_1 and M_2, $M_1 \otimes M_2$ exists and that for each $X \in |\underline{E}|$, the canonical

$$hom(X,M_1) \otimes hom(X,M_2) \to hom(X,M_1 \otimes M_2)$$

(derived from the universal property), is an isomorphism of hom(X,A)-modules.

By similar explicit constructions, we conclude that for M_2 and M_3 free module objects, we can form the A-module object $[M_2,M_3]$ with the property that

$$hom(M_1 \otimes M_2,M_3) \simeq hom(M_1,[M_2,M_3])$$

natural in M_1,M_2,M_3 (M_1 any A-module object), in particular, we can form the linear dual M^* of a free module object M; the duality is described in terms of a bilinear pairing

$$M \times M^* \xrightarrow{\ <-,->\ } A,$$

and again, $\hom(X,-)$ preserves formation of linear duals; M^* and the pairing is universal among all A-module objects N equipped with a bilinear $b: M\times N \to A$; given such b, there exists a unique A-linear $\bar{b}: N \to M^*$ with $id \times \bar{b}.\langle -,- \rangle = b$.

A morphism in Mod(A)

$$M \xrightarrow{\varphi} E$$

where E further is equipped with the structure of a graded A-algebra object

$$E = \bigoplus_{i=0}^{k} E_i$$

is said to be an exterior algebra for M (in analogy with e.g. [11], XXI, §6) if φ is an isomorphism with degree 1 part E_1 of E, if the multiplication $E_1 \times E_1 \to E_2$ is the zero map, and if $M \overset{\varphi}{\to} E$ is universal with this property. For M a free module object, such exterior algebras exist; it suffices to construct them for A^n. We may take the p'th grading of E to be

$$E_p = A^{\binom{n}{p}}$$

and $E = E_0 \oplus \dots \oplus E_n$. Multiplication $\wedge$ in E is given "by the usual formulas":

$$\begin{array}{ccc} A^{\binom{n}{p}} \times A^{\binom{n}{q}} & \xrightarrow{\ \wedge\ } & A^{\binom{n}{p+q}} \\ \cup \downarrow & & \nearrow m \\ A^{\binom{n}{p}} \otimes A^{\binom{n}{q}} = A^{\binom{n}{p}\cdot\binom{n}{q}} & & \end{array}$$

where m is given by the

$$\binom{n}{p+q} \times \binom{n}{p}\cdot\binom{n}{q}$$

matrix, which in its $(L,(H,K))$'th place has 0 if $H \cup K$ is not L, and $+1$ or -1 if $H \cup K = L$ (depending on the parity of the permutation needed to reorder $H \cup K$ into L).

If an exterior algebra for a module object M exists, we denote it $\wedge M$ (and its p'th grade is denoted $\overset{p}{\wedge} M$). Choosing for each M, for which an exterior algebra exists, a definite one and denoting it $\wedge M$, it follows from the universal property of exterior algebras that $\wedge$ depends functorially on M. Furthermore, from the above explicit (and "absolute") description of $\wedge(A^n)$, it follows that for any $X \in |\underline{E}|$ the canonical map (derived from the universal property of $\wedge$)

$$\wedge \hom(X,A^n) \to \hom(X,\wedge A^n)$$

is an isomorphism of $\hom(X,A)$-algebras. This therefore also holds for any other free module object M in place of A^n. If M is a free module object, then we have that $\wedge M$ is a free module and its linear dual $(\wedge M)^*$ exists; in fact, we may use $\wedge(M^*)$ for this linear dual by means of a certain bilinear pairing

$$\wedge M \times \wedge(M^*) \to A$$

whose construction (in the set case and with $M = A^n$) involves determinants, see e.g. [11], Ch.XVI, §9, or [3], Ch.III, §8 No.3. Here we get it from the set case via the Yoneda Lemma and the identifications

$$\hom(X,\wedge M) \simeq \wedge \hom(X,M); \qquad \hom(X,\wedge M^*) \simeq \wedge(\hom(X,M))^*,$$

which are natural in X.

Finally, we can get an A-bilinear map

$$\overset{p}{\wedge} M \times \overset{q}{\wedge} M^* \longrightarrow \overset{q-p}{\wedge} M^* \qquad (q \geqq p)$$

with the property that, applying $\hom(X,-)$ and the various natural isomorphisms, the induced map

$$\overset{p}{\wedge} \hom(X,M) \times \overset{q}{\wedge} \hom(X,M)^* \xrightarrow{\lrcorner} \overset{q-p}{\wedge} \hom(X,M)^*$$

is that canonical hom(X,A)-bilinear map with this name, which is described in [3], Ch.III, §8 No.4.

§2. Basis, Prebasis, Span

In the rest of the article, we assume that $\underline{E}$ is a category with finite products and equipped with a notion of "covering family" (a pretopology, [1], Exposé II,Def.1.3), making it into a site. If Φ is a property of morphisms in $\underline{E}$ ending in $M \in |\underline{E}|$, then one says that Φ holds locally for $v: X \to M$ if there is a covering family of X

$$\{\beta_i : X_i \to X \mid i \in I\}$$

such that for each $i \in I$, Φ holds for $\beta_i . v$. The property Φ is called a local property if it holds for a v whenever it holds locally for v. (This use of the word 'local' has nothing to do with the other use it has here, namely in the phrase 'local ring'.)

Let A be a commutative ring object in $\underline{E}$, and let M be an A-module object. For each $X \in |\underline{E}|$, hom(X,M) is then a hom(X,A)-module, and therefore it makes sense to say that an n-tuple of elements $\underline{v}_1,\ldots,\underline{v}_n$ in hom(X,M),

$$\underline{v}_j : X \to M, \qquad j = 1,\ldots,n,$$

is a basis for hom(X,M) ([3], II,§1 No.11, Def.10), that is, establishes a bijective correspondence of hom(X,M) with $(\mathrm{hom}(X,A))^n$ $(\simeq \mathrm{hom}(X,A^n))$. If $\underline{v}_1,\ldots,\underline{v}_n$ is a basis for hom(X,M), and $\alpha: Y \to X$ is arbitrary, then the n-tuple

$$(\alpha . \underline{v}_j)_{j=1,\ldots,n}$$

of elements in hom(Y,M) is again a basis (for hom(Y,M) as a hom(Y,A)-module). (Note that if hom(Y,A) has only one element, it is the zero ring, and thus any p-tuple (for any p) is a basis for hom(Y,M); also note that hom(Y,A) is never empty.)

Let $\underline{v}_1,\ldots,\underline{v}_r$ be an r-tuple of elements in hom(X,M). It is called a Prebasis for M if "locally it can be extended to a basis", i.e. if there exists a covering $\{\beta_i : X_i \to X \mid i \in I\}$ such that for each $i \in I$, the n-tuple

$$\beta_i \cdot \underline{v}_1, \ldots, \beta_i \cdot \underline{v}_r$$

is part of a (finite) basis for $\hom(X_i, M)$.

Note that if $\underline{v}_1,\ldots,\underline{v}_r$, as above, is a Prebasis, then so is $\alpha\cdot\underline{v}_1,\ldots,\alpha\cdot\underline{v}_r$ for an arbitrary $\alpha : Y \to X$. The reason we use capital letter in spelling 'Prebasis' is that it is not a property which can be decided on basis of knowledge of the single module hom(X,M), but requires knowledge of the whole of $\underline{E}$ (including the $\hom(X_i, M)$). (There is a similar reason for spelling Rank, Span, and Decomposable with capital initial later on.)

Let again $\underline{v}_1,\ldots,\underline{v}_r$ be a set of elements in hom(X,M). By $\mathrm{span}(\underline{v}_1,\ldots,\underline{v}_r)$ we mean, as usual, the submodule of hom(X,M) consisting of linear combinations of the $\underline{v}_j$'s with coefficients from hom(X,A). We say that

$$\underline{u} \in \mathrm{Span}(\underline{v}_1,\ldots,\underline{v}_r)$$

if locally $\underline{u} \in \mathrm{span}(\underline{v}_1,\ldots,\underline{v}_r)$, that is, if there is a covering $\{\beta_i : X_i \to X \mid i \in I\}$ and for each $i \in I$ an r-tuple of scalars

$$t_j^{(i)} : X_i \to A, \qquad j = 1,\ldots,r,$$

such that

$$\sum_j t_j^{(i)} \cdot (\beta_i \cdot \underline{v}_j) = \beta_i \cdot \underline{u} .$$

Clearly $\mathrm{span}(\underline{v}_1,\ldots,\underline{v}_r) \subseteq \mathrm{Span}(\underline{v}_1,\ldots,\underline{v}_r)$. (The converse implication holds provided $\underline{v}_1,\ldots,\underline{v}_r$ is a Prebasis and provided "the topology of the site is less fine than the canonical", [1], Exposé II, 2.5; this is then an example of the "unique existence implies global existence" principle, compare [8].)

Now, assume that M is a free A-module, $M \simeq A^n$; an element

$$v: X \to \overset{p}{\wedge} M$$

is called a Decomposable p-vector provided it "locally is of form $\underline{v}_1 \wedge \ldots \wedge \underline{v}_p$ where $\underline{v}_1,\ldots,\underline{v}_p$ is a Prebasis", or, equivalently, provided there exists a covering $\{\beta_i: X_i \to X \mid i \in I\}$, and for each $i \in I$ a basis

$$\underline{v}_1^{(i)},\ldots,\underline{v}_n^{(i)}: \qquad X_i \to N$$

such that

$$\beta_i.v = \underline{v}_1^{(i)} \wedge \ldots \wedge \underline{v}_p^{(i)}$$

(under the identification $\hom(X_i,\wedge M) \simeq \wedge\hom(X_i,M)$).

Proposition 2.1. Let $\underline{v}_1,\ldots,\underline{v}_p: X \to M$ $(M \simeq A^n)$ be a Prebasis, and consider the Decomposable p-vector

$$v = \underline{v}_1 \wedge \ldots \wedge \underline{v}_p \in \hom(X,M)$$

If $\underline{z}: X \to M$ has the property $\underline{z} \wedge v = 0$, then $\underline{z}$ belongs to $\mathrm{Span}(\underline{v}_1,\ldots,\underline{v}_p)$. (The converse implication holds if the topology of $\underline{E}$ is less fine than the canonical.)

Proof. By assumption we can find a covering $\{\beta_i: X_i \to X \mid i \in I\}$, and for each $i \in I$, a basis of form

$$(2.1) \qquad \beta_i.\underline{v}_1,\ldots,\beta_i.\underline{v}_p,\ \underline{v}_{p+1}^{(i)},\ldots,\underline{v}_n^{(i)};$$

also $\beta_i.\underline{z}$ can uniquely be written as a linear combination of these elements in $\hom(X_i,M)$, with coefficients in $\hom(X_i,A)$;

denote these coefficients $t_1^{(i)},\dots,t_n^{(i)}$. By the assumption $\underline{z} \wedge v = 0$ (and thus $\beta_i.\underline{z} \wedge \beta_i.v = 0$), and because $\beta_i.\underline{v}_j \wedge \beta_i.v=0$ for $j = 1,\dots,p$, we conclude

$$\sum_{j=p+1}^{n} t_j^{(i)}.(\underline{v}_j \wedge \beta_i.v) = 0,$$

but the $\underline{v}_j \wedge (\beta_i.v) = \underline{v}_j \wedge \beta_i.\underline{v}_1 \wedge \dots \wedge \beta_i.\underline{v}_p$ for $j = p+1,\dots,n$, form (modulo sign changes) part of the basis for $\overset{p+1}{\wedge}\mathrm{hom}(X_i,M)$ derived from the basis (2.1) for $\mathrm{hom}(X_i,M)$. Therefore

$$t_{p+1}^{(i)} = \dots = t_n^{(i)} = 0,$$

whence $\beta_i.\underline{z} \in \mathrm{span}(\beta_i.\underline{v}_1,\dots,\beta_i.\underline{v}_p)$. This holds for each $i \in I$; Thus $z \in \mathrm{Span}(\underline{v}_1,\dots,\underline{v}_p)$.

We shall not prove the converse statement in the parenthesis, since we are not going to use it here.

Let $M \simeq A^n$, and let $e'\colon X \to \overset{n}{\wedge} M$ be a basis ($\overset{n}{\wedge} M$ being one-dimensional). Then we get an isomorphism

$$\varphi\colon \mathrm{hom}(X, \overset{p}{\wedge} M) \to \mathrm{hom}(X, \overset{n-p}{\wedge} M^*),$$

namely $\varphi(v) = v \lrcorner e'$ (modulo the identifications $\mathrm{hom}(X, \wedge M) = \wedge\,\mathrm{hom}(X,M)$, etc.). With this notation,

Proposition 2.2. If v is Decomposable, then so is $\varphi(v) = \varphi(v) = v \lrcorner e'$.

Proof. The conclusion is local, so we may assume that v is of the form $\underline{v}_1 \wedge \dots \wedge \underline{v}_p$, where $\underline{v}_1,\dots,\underline{v}_n$ is a basis for $\mathrm{hom}(X,M)$. Let $f_1,\dots,f_n$ be the dual basis for $\mathrm{hom}(X,M)^* = \mathrm{hom}(X,M^*)$. Then $e'' = f_1 \wedge \dots \wedge f_n$ is a basis for $\overset{n}{\wedge}\mathrm{hom}(X,M^*) = \mathrm{hom}(X, \overset{n}{\wedge} M^*)$, and, by [3], III §8, formula (24), we have

$$v \lrcorner e'' = f_{p+1} \wedge \dots \wedge f_n.$$

But e' and e" differ by an invertible scalar t in hom(X,A), and $\lrcorner$ is hom(X,A)-bilinear. Thus

$$v \lrcorner e' = (t \cdot f_{p+1}) \wedge f_{p+2} \wedge \dots \wedge f_n,$$

and thus is Decomposable.

We conclude this section with some matrix theoretic notions which make sense in the setting of a commutative ring object A in a site $\underline{E}$ with finite products. Since we, for arbitrary $X \in |\underline{E}|$, may identify $hom(X,A^{mn})$ with $hom(X,A)^{mn}$, a map

$$\underline{\underline{B}}: X \to A^{mn}$$

may be identified with an m×n matrix over the ring hom(X,A). Given such a matrix $\underline{\underline{B}} = \{b_{ij}\}$ where $b_{ij} \in hom(X,A)$, we say that $Rank(\underline{\underline{B}}) \geq r$ if "locally there is an invertible r×r subdeterminant in $\underline{\underline{B}}$", that is, if there exists a covering $\{\beta_i: X_i \to X \mid i \in I\}$, and for each $i \in I$, an r×r submatrix of $\beta_i . \underline{\underline{B}}$ with invertible determinant. Note that $Rank(\underline{\underline{B}}) \geq r$ is a local property and that, for any $\alpha: Y \to X$, $Rank(\underline{\underline{B}}) \geq r$ implies $Rank(\alpha . \underline{\underline{B}}) \geq r$.

If one views $\underline{\underline{B}}$ as an n-tuple of elements in $hom(X,A^m)$ (the n-tuple of columns), and $Rank(\underline{\underline{B}}) \geq n$, then that n-tuple is a Prebasis. This is easy to see. The converse is not true in general, but will be true provided A is a local ring object in the sense of the next section.

§3. The Steinitz exchange theorem over a local ring object

In this section, A will denote a commutative ring object in a site $\underline{E}$ with finite products; furthermore, A will be assumed to be a <u>local</u> ring object in the sense of Hakim [4], that is, for each $X \in |\underline{E}|$, if $a_j: X \to A$ $(j = 1,\dots,n)$ is an n-tuple of elements such that

$$a_1 + a_2 + \ldots + a_n = 1$$

(= the multiplicative unit of the ring $\hom(X,A)$), then there is a covering $\{\beta_i\colon X_i \to X \mid i \in I\}$ such that for each $i \in I$, at least one of the elements

$$\beta_i \cdot a_1, \ldots, \beta_i \cdot a_n$$

is an invertible element in the ring $\hom(X_i, A)$.

Note that A being a local ring object does not imply that $\hom(X,A)$ is a local ring (not even "locally").

Proposition 3.1. Let $\underline{\underline{B}}\colon X \to A^{mn}$ be an $m\times n$ matrix whose n columns $X \to A^m$ is a Prebasis. Then $\mathrm{Rank}(\underline{\underline{B}}) \geq n$ (and conversely).

Proof. The conclusion being local, we may assume that the columns $\underline{b}_1, \ldots, \underline{b}_n\colon X \to A^m$ of $\underline{\underline{B}}$ are part of a basis $\underline{b}_1, \ldots, \underline{b}_n, \ldots, \underline{b}_m$ of $\hom(X, A^m)$, so that we have an invertible $m\times m$ matrix $\tilde{\underline{\underline{B}}}$ whose first n columns form $\underline{\underline{B}}$. We now take the Laplace expansion ([3],III §6 No.4) of the determinant of $\tilde{\underline{\underline{B}}}$ along its first n columns, and get

$$\det(\tilde{\underline{\underline{B}}}) = \sum_{\underline{\underline{K}}} \pm \det(\underline{\underline{K}}) \cdot \det(\hat{\underline{\underline{K}}})$$

where $\underline{\underline{K}}$ runs over the set of $n\times n$ submatrices of the first n columns of $\tilde{\underline{\underline{B}}}$, and $\hat{\underline{\underline{K}}}$ denotes the "complementary $(m-n)\times(m-n)$ submatrix of the last $(m-n)$ columns of $\tilde{\underline{\underline{B}}}$. Since A was assumed to be a local ring object, we conclude that there exists a covering $\{\beta_i\colon X_i \to X \mid i \in I\}$ such that, for each $i \in I$, at least one of the

$$\beta_i \cdot \det(\underline{\underline{K}}) = \det(\beta_i \cdot \underline{\underline{K}})$$

is invertible. So this covering is a witness that $\underline{\underline{B}}$ (= the first n columns of $\tilde{\underline{\underline{B}}}$) has $\mathrm{Rank} \geq n$.

The converse implication is easy (does not use that A is a local ring object). We omit the proof.

Theorem 3.2 ("Steinitz Exchange"). Let M be a free module over the local ring object A. Let u be a Decomposable q-vector and v a Decomposable p-vector over M. If u locally divides v, then there exists a Decomposable (p-q)-vector w such that

$$u \wedge w = v.$$

The conclusion being local, we may assume

$$v = \underline{v}_1 \wedge \dots \wedge \underline{v}_p$$

where

$$\underline{v}_1, \dots, \underline{v}_p, \dots, \underline{v}_n$$

is a basis for $\hom(X,M)$, and that

$$u = \underline{u}_1 \wedge \dots \wedge \underline{u}_q$$

where

$$\underline{u}_1, \dots, \underline{u}_q, \dots, \underline{u}_n$$

is also a basis for $\hom(X,M)$, and that, finally, there is a $z \in \overset{p-q}{\wedge} \hom(X,M)$ so that $u \wedge z = v$. We consider the invertible $n \times n$ matrix $\underline{\underline{U}}$ whose i'th column contain the coordinates of $\underline{u}_i$ with respect to $\underline{v}_1, \dots, \underline{v}_n$. We claim that the matrix has locally the form

$$\underline{\underline{U}} = \begin{array}{r} p \left\{ \right. \\ n-p \left\{ \right. \end{array} \overset{\overbrace{\quad}^{q}}{\left(\begin{array}{c|c} \underline{\underline{C}} & \\ \hline \underline{\underline{O}} & \underline{\underline{D}} \end{array} \right)} \left. \right\} n$$

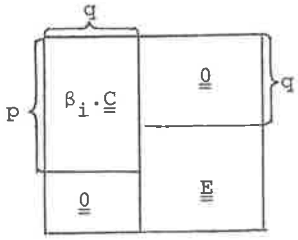
that is, that

(3.1) $$\underline{u}_i \in \mathrm{Span}(\underline{v}_1, \dots, \underline{v}_p) \quad \text{for} \quad i = 1, \dots, q.$$

For, since $\underline{u}_i \wedge u = 0$ for $i = 1,\ldots,q$, and u divides v, we conlude that $\underline{u}_i \wedge v = 0$ and thus, by Proposition 2.2, that (3.1) holds, thus $\underline{\underline{U}}$ has locally the form indicated. By Proposition 3.1, the $n\times q$ matrix

$$\begin{bmatrix} \underline{\underline{C}} \\ \underline{\underline{0}} \end{bmatrix}$$

has Rank $\geq q$. We can thus find a covering $\{\beta_i : X_i \to X \mid i \in I\}$ such that for each $i \in I$, some $q\times q$ subdeterminant of $\underline{\underline{C}}$ is invertible. Consider a fixed $i \in I$, for simplicity, one for which the top $q\times q$ subdeterminant of $\beta_i \cdot \underline{\underline{C}}$ is invertible, $= d$, say. The matrix



then has invertible determinant $(= d)$ (where $\underline{\underline{E}}$ is the unit $(n-q)\times(n-q)$ matrix). Since the top left $p\times p$ determinant of this matrix is likewise invertible $(= d)$, we conclude (by computing in

$$\wedge\mathrm{span}(\beta_i \cdot \underline{v}_1, \ldots, \beta_i \cdot \underline{v}_p))$$

that

$$\beta_i \cdot (\underline{u}_1 \wedge \ldots \wedge \underline{u}_q \wedge \underline{v}_{q+1} \wedge \ldots \wedge \underline{v}_p) = d \cdot \beta_i \cdot (\underline{v}_1 \wedge \ldots \wedge \underline{v}_p),$$

so in $\hom(X_i, \wedge M)$, the desired Decomposable $(p-q)$-vector w is

$$\frac{1}{d}(\beta_i \cdot \underline{v}_{q+1} \wedge \ldots \wedge \beta_i \cdot \underline{v}_p).$$

(In case the topology of $\underline{\underline{E}}$ is less fine than the canonical one, not only has $\underline{\underline{U}}$ locally the form indicated, but has this form "globally".)

A corollary of this form of Steinitz Exchange Theorem is the following, whose geometric interpretation is the self-duality of the Grassmannians viewed as combinatorial structures. Recall the isomorphism

$$\hom(X, \overset{p}{\wedge} M) \overset{\varphi}{\to} \hom(X, \overset{n-p}{\wedge} M^*)$$

considered in Proposition 2.2.

Corollary 3.3. If A is a local ring object, then the duality isomorphism φ inverts the order of local divisibility among Decomposable elements.

Proof. Let u and v be Decomposable elements $X \to \wedge M$ of degree q and p respectively, $q \leq p$, and assume that u divides v locally. We must prove that $\varphi(v)$ locally divides $\varphi(u)$. This conclusion being of local nature, we may, by Theorem 3.2, assume that we have a basis

(3.2) $$\underline{u}_1, \ldots, \underline{u}_q, \underline{v}_{q+1}, \ldots, \underline{v}_p, \underline{v}_{p+1}, \ldots, \underline{v}_n$$

with

$$u = \underline{u}_1 \wedge \ldots \wedge \underline{u}_q$$

and

$$v = \underline{u}_1 \wedge \ldots \wedge \underline{u}_q \wedge \underline{v}_{q+1} \wedge \ldots \wedge \underline{v}_p.$$

Let $f_1, \ldots, f_n$ be the dual basis to (3.2) for the module $\hom(X, M^*)$. Then as in Proposition 2.2,

$$\varphi(u) = t \cdot (f_{q+1} \wedge \ldots \wedge f_n)$$

$$\varphi(v) = t \cdot (f_{p+1} \wedge \ldots \wedge f_n)$$

for some invertible t. Then $f_{q+1} \wedge \ldots \wedge f_p$ witnesses the divisibility of $\varphi(u)$ by $\varphi(v)$.

REFERENCES

1. M. Artin, A. Grothendieck and J.L.Verdier, Théorie des Topos et Cohomologie Etale des Schémas (SGA 4), Vol. 1, Lecture Notes in Math. Vol. 269, Springer Verlag, Berlin 1972

2. W. Benz, Vorlesungen über Geometrie der Algebren, Springer Verlag, Berlin 1973

3. N. Bourbaki, Élements de mathématiques, Algèbre, Hermann, Paris, 1958

4. M. Hakim, Topos annelées et schémas relatifs, Ergebnisse der Mathematik Vol. 64, Springer Verlag, Berlin 1972

5. A. Heyting, Die Theorie der linearen Gleichungen ..., Math. Analen 98 (1928), 465 - 490

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

7. W. Klingenberg, Projektive und affine Ebenen mit Nachbarelementen, Math. Zeitschrift 60 (1954), 384 - 406

8. A. Kock, Linear Algebra and projective geometry, Aarhus Universitet, Preprint Series 1974/75 No. 4

9. A. Kock, Universal projective geometry, in preparation

10. S. Mac Lane, Categories for the working mathematician, Graduate Texts in Mathematics 5, Springer Verlag, New York 1971

11. S. Mac Lane and Birkhoff, Algebra, MacMillan, New York, 1967

12. G. Reyes (with Joyal), From sheaves to logic, Preprint, University of Montreal, 1972

Received: January 1975