CVS: `$Id: diary.tex,v 1.77 2003/12/07 18:18:26 david Exp $`

2001-12-15:001

Let $\mathscr{U}$ be a ultrafilter on $\mathbb{Z}$. Say that a subset A of $\mathbb{Z}$ is *green* (for lack of a better name!) relative to $\mathscr{U}$ iff for every $k \in A$ the translation $A - k = \{\ell \in \mathbb{Z} : \ell + k \in A\}$ belongs to $\mathscr{U}$. Evidently, $\varnothing$ and $\mathbb{Z}$ are green (relative to any ultrafilter on $\mathbb{Z}$); in fact, it is easy to see that the green subsets of $\mathbb{Z}$ (relative to a given ultrafilter on $\mathbb{Z}$) are the open sets of a certain topology (the "green topology") on $\mathbb{Z}$.

If $\mathscr{U}$ is principal, then green subsets of $\mathbb{Z}$ are easy to describe: for $a \in \mathbb{Z}$, let $\mathscr{U}_a$ be the set of all subsets of $\mathbb{Z}$ containing a—then every subset of $\mathbb{Z}$ is green relative to $\mathscr{U}_0$ (i.e. the green topology relative to $\mathscr{U}_0$ is the discrete topology on $\mathbb{Z}$), and, in general, green subsets of $\mathbb{Z}$ relative to $\mathscr{U}_a$ are arbitrary unions of sets of the form $\{k + an : n \in \mathbb{N}\}$ (i.e. these sets, $\mathbb{N}$-indexed arithmetic sequences of reason a, form a basis for the green topology relative to $\mathscr{U}_a$).

Say that a ultrafilter $\mathscr{U}$ on $\mathbb{Z}$ is *fenced* iff for every element $V \in \mathscr{U}$ there exists a green subset of V belonging to $\mathscr{U}$. Note that this is the same as demanding that for every $V \in \mathscr{U}$ containing 0 there exist a green subset of V containing 0 (indeed, for $\mathscr{U} = \mathscr{U}_0$, both conditions are satisfied; for $\mathscr{U} = \mathscr{U}_a$ with $a \neq 0$, neither condition is satisifed, and for $\mathscr{U}$ a non principal ultrafilter, both conditions are easily seen to be equivalent). Thus, a principal ultrafilter $\mathscr{U}_a$ is fenced iff $a = 0$.

To say that a ultrafilter $\mathscr{U}$ is fenced is precisely the same as to say that $\mathscr{U}$ is the set of unpointed neighborhoods of 0 for the green topology relative to $\mathscr{U}$.

Question: what about non principal ultrafilters? Are some of them fenced? Are all of them fenced? I have no idea on how to approach the question.

2001-12-15:002

If X is a set and, for every $x \in X$, we are given a filter $\mathscr{V}_x$ on X which is coarser than the principal ultrafilter of all subsets of X containing x (in other words, every element of $\mathscr{V}_x$ contains x), then we can define a topology on X by saying that a subset A of X is open iff for every $x \in A$ we have $A \in \mathscr{V}_x$. Unfortunately, it is *not true* in general that $\mathscr{V}_x$ is the set of neighborhoods of x for the topology in question. Stupid counterexample: let $X = \mathbb{N}$, let $\mathscr{V}_k$ be the trivial filter $\{\mathbb{N}\}$ except when $k = 0$ where it is the filter of all *infinite* subsets of $\mathbb{N}$ containing 0; then any non-empty subset of $\mathbb{N}$ which is open for the topology defined by the $\mathscr{V}_k$ must clearly be $\mathbb{N}$ itself, so the topology is indiscrete (aka coarse), and $\mathscr{V}_0$ is *not* the set of neighborhoods of 0...

Is there an easy criterion, or at least a useful sufficient condition, which enables one to conclude that $\mathscr{V}_x$ is indeed the set of neighborhoods of x for all $x \in X$? It seems that Steen and Seebach (*Counterexamples in Topology*) often define topology on various spaces by describing their filters of neighborhoods: how can one be sure that these are adequate (or should I say "fenced"?) in the above sense?

Note that the question in **2001-12-15:001** is to study the situation where $X = \mathbb{Z}$ and $\mathscr{V}_k$ is the translation by k of a certain ultrafilter $\mathscr{U}$ on $\mathbb{Z}$ (or, more precisely, of the filter of all elements of $\mathscr{U}$ containing 0, which is the same as the filter formed by adding 0 to every element of $\mathscr{U}$).

2001-12-15:003

A triviality: if G is a group of finite type (i.e. having a finite generating family) then each generating family has a finite generating subfamily. (Proof: express each element of a finite generating family in terms of the given generating family; then a finite number of elements of the latter will have been used, and they generate G.) In particular, if F is a free group with basis B, and F is of finite type, then B is finite. (Proof: B generates F (is this a tautology or simply a well-known fact?), so by the above a finite subset of B generates F; but then the other elements of B can be expressed in terms of these finite number of elements, and, since F is free, there are no other elements, so B is finite.)

Not a triviality: if G is a finitely presented group, then given any presentation of G with a finite number of generators, we can find a finite subset of the relations which form a presentation of G. This is proved in Rotman, *An*

Introduction to the Theory of Groups, lemma 11.84. In other words (using the above trivialities in the translation), the kernel of a surjective morphism from a free group of finite type to a finitely presented group, is of finite type. It would be tempting to combine the two facts and state that if G is a finitely presented group, then given *any* presentation of G we can find a finite subset of the generators and a finite subset of the relations (dealing only with the selected generators!) which form a presentation of G: is this true? (I doubt it.)

Update 2003-12-06: indeed, the assertion in question is false, as Yves de Cornulier points out to me. Take $\langle (x_i)_{i\in\mathbb{N}} | x_1 \cdot x_0^2 \cdot x_1^{-1} = 1\ ,\ x_{i+1} \cdot x_i \cdot x_{i+1}^{-1} = 1 \text{ for all } i \geq 1 \rangle$. Visibly this is a presentation of the cyclic group with two elements (and the latter is certainly of finite presentation), but any finite sub-presentation gives an infinite group (or the trivial group).

2001-12-15:004

If X is a, say, noetherian, scheme (over a base S), and $\mathscr{E}$ a locally free coherent sheaf on X, then we have an associated projective bundle $\mathbb{P}(\mathscr{E})$ (see Hartshorne, *Algebraic Geometry*, §7, and EGA, II, §4). Further, we have a "fundamental sheaf" $\mathscr{O}_{\mathbb{P}(\mathscr{E})}(1)$, which is a line bundle on $\mathbb{P}(\mathscr{E})$. Essentially, it is a way of "transforming" an arbitrary vector bundle $\mathscr{E}$ into a line bundle; in particular, if $\mathscr{L}$ is *already* a line bundle, then the canonical projection $\pi\colon \mathbb{P}(\mathscr{L}) \to X$ is an isomorphism, and $\pi^*\mathscr{L}$ is (canonically isomorphic to) $\mathscr{O}_{\mathbb{P}(\mathscr{L})}(1)$. (In particular, $\mathscr{O}_{\mathbb{P}(\mathscr{E})}(1)$ need not be ample!)

We can then transfer the terminology of line bundles to arbitrary vector bundles: say that $\mathscr{E}$ is ample on X iff $\mathscr{O}_{\mathbb{P}(\mathscr{E})}(1)$ is ample on $\mathbb{P}(\mathscr{E})$, for example. It also makes sense to talk about very ample vector bundles (when there exists an immersion i over S of $\mathbb{P}(\mathscr{E})$ in $\mathbb{P}(\mathscr{F})$ for $\mathscr{F}$ some vector bundle over S—say S is the spectrum of a field for simplicity—such that $\mathscr{O}_{\mathbb{P}(\mathscr{E})}(1) = i^*(\mathscr{O}_{\mathbb{P}(\mathscr{F})}(1))$). Question: does a very ample vector bundle somehow determine an immersion of X itself in a projective space? (In particular, if X is proper smooth over some field and has a very ample vector bundle, is it true that X is projective?)

This is very confused, and there are many questions floating around. EGA does things in "full generality" as usual, of course, and Hartshorne in a much more restricted context, and it is not even completely obvious how far the definitions coincide.

2001-12-15:005

Still concerning projective space (see also **2001-12-15:004** on this subject): if k is any ring, and E any k-module, then $\mathbb{P}(E)$ is (see EGA, II, theorem 4.2.4) the set of submodules F of E such that E/F is free of rank 1 (**2003-12-06**: no, this is *wrong*, it should read "locally free" or something; see **2003-12-06:064**). More precisely, $\mathbb{P}(E)$ is the functor which takes a k-algebra A to the set $\mathbb{P}(E)(A)$ of submodules F of $E \otimes_k A$ such that $(E \otimes_k A)/F$ is free of rank 1 (as an A-module); and which takes a morphism $A \to B$ of k-algebras to the map $\mathbb{P}(E)(A) \to \mathbb{P}(E)(B)$ which takes $F \subseteq E \otimes_k A$ to the image of $F \otimes_A B$ inside $E \otimes_k B$. In particular, $\mathbb{P}^1_k(A)$ is the set of submodules F of A^2 (the free A-module of rank 2) such that A^2/F is free of rank 1 (and $\mathbb{P}^1_k(A) \to \mathbb{P}^1_k(B)$ takes F to the image of $F \otimes_A B$ inside B^2); and the map $\mathbb{A}^1_k \to \mathbb{P}^1_k$ is given by the natural map $\mathbb{A}^1_k(A) \to \mathbb{P}^1_k(A)$ which takes $a \in A$ (viewed in $\mathbb{A}^1_k(A)$, which is precisely the underlying set to A) to the submodule of A^2 spanned by $(1, a)$. And more generally, it is clear how $\mathbb{A}^r_k$ maps to $\mathbb{P}^r_k$, in $r+1$ canonical ways.

2001-12-15:006

Let X be any set, and k any field. Consider the ring k^X of all k-valued functions on X, with pointwise addition and multiplication. If $\mathfrak{p}$ is a prime ideal of k^X, then the set $\mathscr{U} = \{A \subseteq X : 0_A \in \mathfrak{p}\}$ is a ultrafilter on X, where $0_A \in k^X$ is defined by $0_A(x) = 0$ if $x \in A$ and $0_A(x) = 1$ otherwise; furthermore, it is then clear that $\mathfrak{p}$ coincides precisely with the set of all $f \in k^X$ such that $\mathbf{Z}(f) = \{x \in X : f(x) = 0\}$ belongs to $\mathscr{U}$. But this clearly implies that $\mathfrak{p}$ is maximal. So all prime ideals of k^X are maximal: k^X is zero-dimensional. (Recall that a ring is artinian, i.e. satisfies the descending chain condition, iff it is noetherian, i.e. satisfies the ascending chain condition, and zero-dimensional, i.e. every prime ideal of it is maximal.) Thus, we have a natural identification (as topological spaces) $\beta X = \mathrm{Spec}(k^X) = \mathrm{Spm}(k^X)$, where β denotes Stone-Čech compactification (in the case of a discrete set X, this

is the set of ultrafilters of X), and $\mathrm{Spec}(k^X)$ is the set of prime ideals of k^X and $\mathrm{Spm}(k^X)$ the set of its maximal ideals. In particular, note that the Stone-Čech compactification of any discrete set is naturally a k-scheme for any field k ("naturally" in the sense that for any map of sets $X \to X'$ the morphism $\mathrm{Spec}(k^X) \to \mathrm{Spec}(k^{X'})$ deduced from the obvious morphism of rings $k^{X'} \to k^X$ coincides, as far as the underlying topological map goes, with the morphism $\beta X \to \beta X'$ of pushforward of ultrafilters obtained by functoriality of the Stone-Čech compactification). Also note that $\mathrm{Spec}(k^X)$ is Hausdorff. If $p \in \beta X$ corresponds to a ultrafilter $\mathscr{U}$, then the residue field $k(p)$ of $\mathrm{Spec}(k^X)$ at p is precisely the ultraproduct of X copies of k reduced by $\mathscr{U}$.

Note that if we considered instead the ring $k^{[X]}$ of k-valued functions on X with *finite image*, then we would also have the identification $\beta X = \mathrm{Spec}(k^{[X]}) = \mathrm{Spm}(k^{[X]})$, but this time with the residue field of $\mathrm{Spec}(k^{[X]})$ at $p \in \beta X$ being simply k.

2001-12-15:007

(This more or less continues **2001-12-15:006**.)

The obvious "next step" would be to consider X a topological space, and k^X the ring of *locally constant* k-valued functions on X (i.e. continuous functions from X to k, where k is given the discrete topology). Such a function takes each value on a clopen subset of X, and given a prime ideal $\mathfrak{p}$ of k^X we are led to consider $\mathscr{U}$ the set of clopen $A \subseteq X$ such that 0_A belongs to $\mathfrak{p}$. Then $\mathscr{U}$ is a ultrafilter in the boolean algebra of clopen subsets of X, and $\mathfrak{p}$ is precisely the set of all $f \in k^X$ such that $\mathbf{Z}(f)$ (which is clopen) belongs to $\mathscr{U}$. Again, every prime ideal of k^X is maximal: we have $\mathrm{Spec}(k^X) = \mathrm{Spm}(k^X)$, but it does not in general coincide with the Stone-Čech compactification of X.

Call ρX this set of ultrafilters on the boolean algebra of clopen subsets of X, and topologize ρX by declaring the $\{\mathscr{U} \in \rho X : A \in \mathscr{U}\}$ for A clopen in X to form a basis of closed sets; note that these sets are actually clopen in ρX. And we map X to ρX by sending $x \in X$ to the set $\mathscr{U}_x$ of clopen $A \subseteq X$ such that $x \in A$: this is evidently continuous and has a dense image; further, ρX is compact (Hausdorff). By the universal property of the Stone-Čech compactification, it follows that $X \to \rho X$ factors as $X \to \beta X \to \rho X$, and the latter map is surjective (since its image is dense and closed). In fact, it can be described precisely: if $p \in \beta X$ corresponds to a z-ultrafilter $\mathscr{U}$ (that is, a ultrafilter on the lattice of zero-sets of X), then the set of clopen $A \subseteq X$ which belong to $\mathscr{U}$ forms a ultrafilter on the boolean algebra of clopen subsets of X, and thus defines a point of ρX, which is precisely the image of p by the canonical map $\beta X \to \rho X$.

Now this construction is classical: ρX is the Stone space of the boolean algebra of clopen subsets of X. The space ρX is compact Hausdorff zero-dimensional (has a basis consisting of clopen sets), as we have seen; in fact, the map $X \to \rho X$ is the universal map from X to a compact Hausdorff zero-dimensional space (in particular, $\rho\rho X = \rho X$).

Note that applying functorially ρ to $X \to \beta X \to \rho X$ we see that $\rho\beta X$ is canonically isomorphic to ρX. In particular, it means that if βX is zero-dimensional, then it is equal to ρX.

Among other things, we have seen that any compact Hausdorff zero-dimensional space X is naturally a k-scheme for any field k, namely the spectrum of the ring k^X of locally constant k-valued functions on X. Appropriately, this scheme is zero-dimensional (this is the translation of the fact that any prime ideal of k^X is maximal).

Note that if we considered instead the ring $k^{[X]}$ of locally constant k-valued functions on X with *finite image* (for X an arbitrary topological space), then we would also have the identification $\rho X = \mathrm{Spec}(k^{[X]}) = \mathrm{Spm}(k^{[X]})$, but the residue field of $\mathrm{Spec}(k^{[X]})$ at $p \in \rho X$ is k whereas that of $\mathrm{Spec}(k^X)$ is (in general) larger. (Not always, though: if $X = \omega_1$ with the order topology, then $\rho\omega_1 = \beta\omega_1 = \omega_1 + 1 = \omega_1 \cup \{\omega_1\}$, and every locally constant function on ω_1 has finite image, so k^{ω_1} coincides with $k^{[\omega_1]}$ and in particular the residue field at the point "at infinity" (ω_1) is simply k.)

2001-12-15:008

Let k be a field. Call $k(\!(t)\!)$ the field of Laurent series in the variable t with coefficients in k: in other words, $k(\!(t)\!)$ is the quotient field of the ring $k[\![t]\!]$ of formal power series in the variable t with coefficients in k. We can then, of course, consider $k(\!(u)\!)(\!(v)\!)$: since this is a field containing $k[\![u]\!][\![v]\!] = k[\![u, v]\!]$, it also contains its quotient field which we denote by $k(\!(u, v)\!)$.

Now, an element of $k(\!(u)\!)(\!(v)\!)$ is a formal sum $\sum a_{ij}u^iv^j$, with i and j ranging over $\mathbb{Z}$, satisfying: (1) there exists $j_0 \in \mathbb{Z}$ such that $a_{ij} = 0$ if $j < j_0$ (for all i), and (2) for all $j \in \mathbb{Z}$, there exists $i_0 \in \mathbb{Z}$ such that $a_{ij} = 0$ if $i < i_0$. In other words, the set of pairs $(i, j) \in \mathbb{Z}^2$ such that $a_{ij} \neq 0$ is bounded at the bottom, and at the left on every horizontal line.

Given $f \in k[\![u, v]\!]$, we can write $f = v^{j_0}u^{i_0}(1 + vu^kh)g$, where $g \in [\![u, v]\!]$ is a *unit* (that is, its coefficient in u^0v^0 is non-zero), $i_0, j_0, k \in \mathbb{Z}$ and $h \in [\![u, v]\!]$. Now $(1 + vu^kh)^{-1} = 1 - vu^kh + v^2u^{2k}h^2 + \cdots$ in $k(\!(u)\!)(\!(v)\!)$: this has the property that there is a line with negative slope such that all non-zero coefficients are above that line; so the same thing holds for f^{-1}. Consequently, this property is true of any element of $k(\!(u, v)\!)$ when seen in $k(\!(u)\!)(\!(v)\!)$.

Conversely, if $f \in k(\!(u)\!)(\!(v)\!)$ is such that there is a line with negative slope such that all coefficients below that line are zero, is it true that $f \in k(\!(u, v)\!)$? Or else, how can we characterize elements of $k(\!(u, v)\!)$ when written in $k(\!(u)\!)(\!(v)\!)$? It seems, for example, that $\sum_{k=0}^{+\infty} c_k u^{-k} v^k$, is in $(\!(u, v)\!)$ iff $\sum c_k t^k$ is in $k(t)$. And what about the field of series $f \in k(\!(u)\!)(\!(v)\!)$ such that there is a line with negative slope such that all coefficients below that line are zero? Does it have any nice properties (or a geometric description)? More generally, it seems we can consider the field of formal sums $\sum a_{ij}u^iv^j$, with i and j ranging over $\mathbb{Z}$, where a_{ij} are all zero outside of some translate of a fixed (closed) angular sector of angle $< \pi$ and not containing the negative part of either coordinate axis.

2001-12-17:009

Consider a lattice Λ of equilateral triangles in the plane; pick some vertex and number it "0"; then number the six vertices surrounding it "1", "5", "4", "6", "2" and "3", in this order; and complete the numbering of all remaining vertices by imposing that three vertices that follow consecutively on any line are numbered in arithmetic progression in $\mathbb{Z}/7\mathbb{Z}$. This has some exceptionally nice properties, among which the following. Let Λ_0 be the lattice of points numbered 0: this is also a lattice of equilateral triangles, with edge length $\sqrt{7}$ times that of Λ. Then on the flat torus $\mathbb{C}/\Lambda_0$, the seven points corresponding to the points numbered "0", "1", "2", "3", "4", "5" and "6", are pairwise equidistant. And these can be written as the centers of seven regular hexagons, each adjacent and identical to the six other ones, which cover the torus. If we lift these hexagons to the plane, we obtain a partition of the plane in seven regions, with the property that no two points at a distance between $2a$ and $\sqrt{7}a$ (with a being the edge length of Λ) of one another can belong to the same region. (Recall that if we wish to partition the plane in k regions so that no two points at distance 1 from one another belong to the same region, then we need $k \geq 4$; and thos shows that it can be done for $k = 7$. As far as I know, the question of whether $k = 4$, $k = 5$ and $k = 6$ are possible is still open.)

2001-12-17:010

Let X be a proper noetherian scheme. The sum of two ample Cartier divisors on X is again ample: indeed, if D and D' are ample, and $\mathscr{F}$ is a coherent sheaf on X, there is some m_0 such that for $m \geq m_0$ the sheaf $\mathscr{F}(mD)$ is generated by its global sections and $\mathscr{O}(mD')$ similarly, and then $\mathscr{F}(m(D + D')) = \mathscr{F}(mD) \otimes \mathscr{O}(mD')$ is generated by its global sections. The sum of two very ample Cartier divisors on X is again very ample: this follows from the Segre embedding.

Question: what about the sum of an ample and a very ample Cartier divisor? Can it fail to be very ample (for a well-behaved X)?

2001-12-18:011

Let PA stand for a recursively axiomatizable first-order theory for doing arithmetic which embeds all primitive recursive functions (e.g. Peano's axioms). Then we can write in the language of PA the assertion G stating that "G is not a theorem of PA": this is because (a) Gödel's scheme allows one arithmetize deduction and speak about provability in PA (this uses the fact that PA is recursively axiomatizable, and embeds all primitive recursive functions), and (b) the fact that G speaks about G is not a problem, thank's to Quine's usual trick. Now assume $\mathrm{Consis(PA)}$ (i.e. the statement "$\perp$ is not a theorem of PA", arithmetized by Gödel's scheme and written in the language of PA); then, if G is a theorem of PA, then "G is a theorem of PA" is a theorem of PA (proofs can be upgraded to a proof of their existence), so "G

is not a theorem of PA" is not a theorem of PA (since we have assumed $\mathrm{Consis(PA)}$), which is exactly to say that G is not a theorem of PA; this shows that G cannot be a theorem of PA. So $\mathrm{Consis(PA)}$ implies that G is not a theorem of PA, in other words, G itself: we have $\mathrm{Consis(PA)} \Longrightarrow G$. And since G is not a theorem of PA provided PA is consistent (we have proved this), the same holds of $\mathrm{Consis(PA)}$. This is Gödel's incompleteness theorem.

Now in an ambient metamathematics (governed by, say, ZF, i.e. Zermelo-Fraenkel set theory), we have a model, viz. $\mathbb{N}$, of PA (actually, I skip a little here: in the preceding paragraph I did not require PA to be ω-consistent, merely to be "some" well-behaved formal system for doing arithmetic; here, I really have the true Peano's axioms in mind). Now $\mathrm{Consis(PA)}$ is *true* in $\mathbb{N}$ (and ZF proves it): indeed, if we assume $\neg\,\mathrm{Consis(PA)}$, then there is a proof of $\bot$ in PA, and since the axioms of PA are true in $\mathbb{N}$, then $\bot$ is true, and it is not. The key here is that in the language of ZF we can form a statement $T(n)$ which states that "the proposition labeled n in the chosen coding of arithmetic, is true (in $\mathbb{N}$)"; so ZF can speak about arithmetic truth, whereas PA can only speak about provability: it can encode the statement $P(n)$ which states that "the proposition labeled n in the chosen coding of arithmetic, is a theorem of PA" (e.g. $\mathrm{Consis(PA)}$ is $\neg P(\text{“}\bot\text{”})$); and we have $(\forall n)(P(n) \Longrightarrow T(n))$ (this is a theorem of ZF), and since evidently we have $\neg T(\text{“}\bot\text{”})$, we also have $\neg P(\text{“}\bot\text{”})$, i.e. $\mathrm{Consis}(PA)$.

So $\mathrm{Consis}(PA)$ is true (in $\mathbb{N}$, this being a theorem of ZF); but then the same reasoning shows that $\mathrm{Consis}(PA \wedge \mathrm{Consis}(PA))$ is true; and then that the theory obtained by adding *that* axiom to PA is still consistent; "and so on". The question is, where, exactly, to we stop?

If we let $\mathrm{PA}^0 = \mathrm{PA}$, and $\mathrm{PA}^{\alpha+1} = \mathrm{PA}^\alpha \wedge \mathrm{Consis}(\mathrm{PA}^\alpha)$, and $\mathrm{PA}^\delta = \bigwedge_{\alpha<\delta} \mathrm{PA}^\alpha$ if δ is limit, the question is, when does this stop making sense? At the smallest ordinal such that PA^α is no longer recursively axiomatizable: this is probably something like the smallest ordinal α such that there is no (primitive?) recursive well-order on $\mathbb{N}$ of order type α. Now what about the greatest system in question, call it PA^∞: it is no longer recursively axiomatizable—does Gödel's theorem still apply? What are its theorems (e.g. is every true statement in $\mathbb{N}$ a theorem of PA^∞, or am I just being utterly naïve)?

2001-12-21:012

Each (infinite) countable ordinal α can be represented as a certain well-order on $\mathbb{N}$, thus as a certain subset of $\mathbb{N} \times \mathbb{N}$ (trivially not unique). Now given any countable family of subsets of $\mathbb{N} \times \mathbb{N}$ we can consider the smallest countable ordinal α which has *no* representation as one of these subsets. For example, taking the recursive subsets of $\mathbb{N} \times \mathbb{N}$, we consider the smallest countable ordinal which cannot be represented by some computable well-ordering on $\mathbb{N}$. Similarly, we can consider the smallest countable ordinal which cannot be represented by some well-ordering on $\mathbb{N}$ given by a primitive recursive function (resp. a function calculable in polynomial time by a Turing machine, resp...). How can we prove *strict* inequalities between these ordinals?

2001-12-21:013

("The Very Basic General Tao of the Universal Ring.")

Let k be any ring and let $\mathscr{R} = \mathrm{Spec}\, k[t]$ be the forgetful functor from k-algebras to sets. By flat descent, this is a sheaf on the category of affine k-schemes, for any "reasonable" topology. Moreover, it is an internal ring in the topos of sheaves of sets (for the "reasonable" topology in question), because each $\mathscr{R}(A)$ can trivially be endowed with a ring structure (in a natural fashion), by "unforgetting" what was forgotten. To say that a section x of $\mathscr{R}$ (in other words, an element x of some k-algebra $A = \mathscr{R}(A)$, where $\mathrm{Spec}\, A$ is the affine scheme on which the section is taken) is "not equal to zero", i.e. $\neg(x = 0)$ for the Kripke-Joyal sheaf semantics, means that for any morphism $A \to B$ of k-algebras (i.e. for any A-algebra B), if the image of x in B is 0 then B is covered by the empty family (this translates $\bot$), and the latter happens exactly when $B = 0$ because we have assumed a "reasonable" topology. In other words, $\{x \in \mathscr{R} : \neg(x = 0)\}$ is the functor $\mathscr{R}^\times$ which takes a k-algebra A to the set $\mathscr{R}^\times(A) = A^\times$ of its invertible elements (indeed, to say that every morphism $A \to B$ sends x to some non-zero element when $B \neq 0$ means that x is invertible); and this functor is a sheaf for any "reasonable" topology. Now this is also $\{x \in \mathscr{R} : (\exists y \in \mathscr{R})(xy = 1)\}$, the "set of invertible elements of $\mathscr{R}$", for pretty much obvious reasons. So we have $(\forall x \in \mathscr{R})((\neg(x = 0)) \Longleftrightarrow$

$((\exists y \in \mathscr{R})(xy = 1)))$ for the Kripke-Joyal semantics. It is in this sense that $\mathscr{R}$ is actually a "field". (Note, by the way, that we have $\neg(0 = 1)$ in $\mathscr{R}$, which means that a k-algebra in which $0 = 1$ is covered by the empty family.)

Furthermore, the sheaf $\{x \in \mathscr{R} : \neg\neg(x = 0)\}$ is easily seen to be the sheaf which takes a k-algebra A to its set of nilpotent elements (indeed, to say that every morphism $A \to B$ sends x to some non-invertible element when $B \neq 0$ means that x is nilpotent). It is an ideal of $\mathscr{R}$ (in intuitionistic set theory, if $\mathscr{A}$ is any ring, then $\{x \in \mathscr{A} : \neg\neg(x = 0)\}$ is an ideal of $\mathscr{A}$). In fact, it is exactly the ideal $\{x \in \mathscr{R} : (\exists n \in \mathbb{N})(x^n = 0)\}$ of nilpotent "elements" of $\mathscr{R}$: one direction is clear in view of the description we have given and the other follows because $\mathscr{R}$ is a "field" as seen above. So we have $(\forall x \in \mathscr{R})((\neg\neg(x = 0)) \iff ((\exists n \in \mathbb{N})(x^n = 0)))$.

In algebraic geometry, the additive group of $\mathscr{R}$ is written $\mathbb{G}_{\mathrm{a}}$, and the multiplicative group $\mathscr{R}^\times$ is written $\mathbb{G}_{\mathrm{m}}$. Both are (representable by) affine k-schemes, respectively $\mathbb{G}_{\mathrm{a}} = \operatorname{Spec} k[t]$ and $\mathbb{G}_{\mathrm{m}} = \operatorname{Spec} k[t, t^{-1}]$. However, $\{x \in \mathscr{R} : \neg\neg(x = 0)\}$ is not representable by a k-scheme (as soon as k is not the zero ring). We now prove this fact (I am indebted to Joël Bellaïche for showing me how to do it).

First, we can assume that k is an algebraically closed field. Indeed, let $k \to \Omega$ be the algebraic closure of the quotient of k by some maximal ideal. Suppose the functor $\mathscr{V} = \{x \in \mathscr{R} : \neg\neg(x = 0)\}$ taking a k-algebra to its set of nilpotents, is reprensentable by a k-scheme V; then the functor of points of the Ω-scheme $V \times_{\operatorname{Spec} k} \operatorname{Spec} \Omega$ is the functor taking an Ω-algebra A to its set of nilpotents (which is the same as an Ω-algebra or as a k-algebra). So if we have the statement for Ω, it also holds for k.

So consider k an algebraically closed field and suppose the functor $\mathscr{V}$ taking a k-algebra to its set of nilpotents, is representable by a k-scheme V. Now $\mathscr{V}(k)$ has a single element, corresponding to $0 \in k$, so V has a single closed point; moreover, if K is any extension field of k (i.e. any function field over k), then $\mathscr{V}(K)$ still has a single element, which comes from $\mathscr{V}(k)$, so that V has no other point than the closed point (here, a "point" means a point of the underlying topological space of the k-scheme V).

But this shows that V is affine, because there must exist some affine subscheme containing the unique point of V, and this must then be all of V. Let $V = \operatorname{Spec} \Delta$, where Δ is a k-algebra.

Since V has a single point, it is irreducible, so its reduced scheme V^{red} is integral, and it is $\operatorname{Spec}(\Delta/N)$ where N is the nilradical of Δ (i.e. the ideal of nilpotent elements of Δ). But then Δ/N is an integral domain with a unique prime ideal, (0), which is therefore also maximal, so that Δ/N is a field, and this field is k (since the closed point corresponding to (0) was already defined over k).

By now we know that every element of Δ not belonging to k must be nilpotent.

The natural transformation $\mathscr{V} \to \mathscr{R}$ (injecting canonically the set of nilpotent elements of a k-algebra A in the set of *all* elements of A) corresponds to a morphism of schemes $V \to \operatorname{Spec} k[t]$, or again to a morphism of k-algebras $k[t] \to \Delta$, or yet again to an element $\delta \in \Delta$. And δ does not come from k because $V \to \operatorname{Spec} k[t]$ is not constant. Therefore δ is nilpotent, say $\delta^n = 0$. But this means that *any* nilpotent element x of *any* k-algebra A satisfies $x^n = 0$, and this is certainly impossible.

This is the desired contradiction.

Even though $\mathscr{V} = \{x \in \mathscr{R} : \neg\neg(x = 0)\}$ somehow "looks like" the (formal) scheme $\operatorname{Spec} k[\![t]\!]$ (recall that $k[\![t]\!]$ is the projective limit of the $k[t]/(t^n)$ with n ranging over $\mathbb{N}$), yet is not equal. There is a map $\mathscr{V} \to \operatorname{Spec} k[\![t]\!]$ (because if $x \in A$ is nilpotent, we can form a morphism $k[\![t]\!] \to A$ which sends t to x), which is a monomorphism in the category (topos) of sheaves, but it is not surjective (a morphism $k[\![t]\!] \to A$ can exist without the image of t being nilpotent, witness the identity morphism on $k[\![t]\!]$). It is also true that morphisms $\mathscr{V} \to \mathscr{R}$ are precisely given by elements of $k[\![t]\!]$. Morality: the category of schemes does not have nice inductive limits (even filtered inductive limits when all arrows are monomorphisms are not nice).

2001-12-21:014

(This more or less continues **2001-12-21:013**.)

Let k be any ring and let $\mathscr{R}$ be the "universal ring", i.e. the forgetful functor from k-algebras to sets, endowed with its internal ring structure in the topos of sheaves of sets on the category of affine k-schemes for some "reasonable" topology. And let $\mathscr{N} = \{x \in \mathscr{R} : \neg\neg(x = 0)\}$ (written $\mathscr{V}$ in **2001-12-21:013**) be the ideal of nilpotent elements of

$\mathscr{R}$, the sheaf taking a k-algebra A to the set of its nilpotent elements. We want to try to understand $\mathscr{R}' = \mathscr{R}/\mathscr{N}$, the reduced ring of $\mathscr{R}$.

A section of $\mathscr{R}'$ on $\operatorname{Spec} A$ (with A a k-algebra) is a (descent) datum as follows: an A-algebra B which covers A for the given ("reasonable") topology (e.g. B a finitely presented faithfully flat A-algebra), and an element $x \in B$ such that the element $x \otimes 1 - 1 \otimes x \in B \otimes_A B$ is nilpotent; furthermore, we declare two such data (B_1, x_1) and (B_2, x_2) to be equivalent when the element $x_1 \otimes 1 - 1 \otimes x_2 \in B_1 \otimes_A B_2$ is nilpotent. And if $A \to A'$ is a morphism of k-algebras, it takes a datum (B, x) on A to the datum $(B \otimes_A A', x \otimes 1)$ on A'.

Fact: if Ω is an algebraically closed field (over k), then $\mathscr{R}'(\Omega) = \mathscr{R}(\Omega)$. Indeed, let B be a non-zero Ω-algebra (necessarily faithfully flat), and $x \in B$ be such that $x \otimes 1 - 1 \otimes x \in B \otimes_\Omega B$ is nilpotent. Let B' be the Ω-subalgebra of B generated by x, in other words the Ω-vector subspace of B generated by the powers of x: evidently, $B' \otimes_\Omega B'$ is an Ω-vector subspace of $B \otimes_\Omega B$. If B' is infinite dimensional, then it is isomorphic to the ring $\Omega[x]$ of polynomials in one variable with coefficients in Ω, and $x \otimes 1 - 1 \otimes x$ cannot be nilpotent. Otherwise, let x act (faithfully) on the finite-dimensional Ω-vector space B' by multiplication, and let λ_i be its eigenvalues, witnessed by the eigenvectors v_i, say $xv_i = \lambda_i v_i$, with $\lambda_i \in \Omega$. If there exist i and j such that $\lambda_i \neq \lambda_j$, then $(x \otimes 1 - 1 \otimes x)(v_i \otimes v_j) = (\lambda_i - \lambda_j)(v_i \otimes v_j)$ in $B' \otimes_\Omega B'$, so that $x \otimes 1 - 1 \otimes x$ cannot be nilpotent. Therefore all λ_i are equal to the same, say λ; but then $x - \lambda$ is nilpotent, and this shows that the class of the datum (B, x) in $\mathscr{R}'(\Omega)$ is the same as the class of (Ω, λ). On the other hand, the class of (Ω, λ) and the class of (Ω, λ') are evidently different, and we have indeed shown $\mathscr{R}'(\Omega) = \mathscr{R}(\Omega)$.

The same statement $\mathscr{R}'(K) = \mathscr{R}(K)$ therefore also holds for any field K (not necessarily algebraically closed) over k, simply by embedding it in its algebraic closure. (**Update:** this is *false*, cf. **2002-04-06:041**.)

Now if A is an integrally closed domain (over k), we again wish to show that $\mathscr{R}'(A) = \mathscr{R}(A)$. Let K be the field of fractions of A, and B a faithfully flat A-algebra. Since $A \rightarrowtail K$, it follows that $B \rightarrowtail B_K$ (where $B_K = B \otimes_A K$) by flatness. Now if $x \in B$ is such that $x \otimes 1 - 1 \otimes x \in B \otimes_A B$ is nilpotent, then it is also nilpotent in $B_K \otimes_K B_K$, so $x - \lambda$ is nilpotent in B_K for some (unique) $\lambda \in K$ as seen above. How do we conclude from there? It shouldn't be too hard, but I seem completely stuck.

2001-12-21:015

Let us try to contract the axis $x = 0$ in the affine plane. More precisely: let $\mathbb{A}^2_k = \operatorname{Spec} k[x, y]$ (over a field k), let $\mathbb{A}^1_k = \operatorname{Spec} k[x]$ and let A be the k-subalgebra of $k[x, y]$ generated by the xy^i for $i \in \mathbb{N}$. So A is the k-algebra of polynomials which have no term in y^i for $i > 0$, or, in other words, which are constant along the axis $x = 0$. The projection morphism $\mathbb{A}^2_k \to \mathbb{A}^1_k$ (determined by the inclusion $k[x] \rightarrowtail k[x, y]$) factors through $\operatorname{Spec} A$ in the obvious way. Note that A is a (faithfully) flat $k[x]$-algebra, because it is free as a $k[x]$-module (with basis $1, xy, xy^2, xy^3, \ldots$). The fiber of $\operatorname{Spec} A$ over a closed point of $\mathbb{A}^1_k$ other than the origin is isomorphic to $\operatorname{Spec} k[y]$, whereas the fiber over the origin is $\operatorname{Spec} k$.

Is the ring A noetherian? (**Update:** the answer is *no*, see **2001-12-23:017**.) Is it catenary? Is $k[x, y]$ flat over A? Numerous questions of this kind can be asked...

Similar techniques can be used to perform many other kinds of contractions (e.g. two points in the plane to one: this was used by Luc Illusie to provide me with an example of a non-placid scheme).

2001-12-22:016

Some facts about modules over commutative rings:

- A module over a local ring is projective iff it is free ("Kaplansky's theorem": cf. Matsumura, *Commutative Ring Theory*, theorem 2.5).
- A module of finite type over a local ring is flat iff it is free (cf. Matsumura, *op. cit.*, theorem 7.10).
- A module of finite presentation M over a ring A is projective iff its localization $M_\mathfrak{m}$ is free over $A_\mathfrak{m}$ for every maximal ideal $\mathfrak{m}$ of A (cf. Matsumura, *op. cit.*, theorem 7.12).
- A module M over a ring A is flat iff its localization $M_\mathfrak{m}$ is flat over $A_\mathfrak{m}$ for every maximal ideal $\mathfrak{m}$ of A (cf. EGA, **0**.6.3.3).
- A module of finite presentation is flat iff it is projective (this follows from the above).

- A module is flat iff it is a filtered inductive limit of free modules ("Govorov-Lazard theorem": cf. Eisenbud, *Commutative Algebra with a View Toward Algebraic Geometry*, theorem A.6.6).
- A module over a principal ideal domain is flat iff it is torsion free (cf. Eisenbud, *op. cit.*, corollary 6.3).
- A submodule of a free module over a principal ideal domain is free (cf. Hilton & Stammbach, *A Course in Homological Algebra*, theorem 5.1). In particular, every projective module over a principal ideal domain is free.
- A module of finite type over a noetherian integral domain is torsion free iff it is a submodule of a free module of finite type (Joël Bellaïche and Gaëtan Chenevier, personal communication).
  Question: can we find analogues of these statements over non necessarily commutative rings?

2001-12-23:017

(This answers a question of **2001-12-21:015**.)

The ring A of polynomials $f \in k[x,y]$ having zero coefficient in y^i for all $i > 0$, introduced in **2001-12-21:015** is not noetherian. Indeed, let I_n be the ideal of A generated by the xy^i with $0 \leq i \leq n$: thus, I_n consists of the $f \in A$ having no coefficient in xy^i for $i > n$. The I_n form a strictly ascending chain of ideals of A; and their union I_∞ is the ideal consisting of the $f \in A$ whose constant coefficient (the value on the axis $x = 0$) is zero: it is a maximal ideal.

The quotient A/I_∞ is isomorphic to k. On the other hand, the quotients A/I_n are all isomorphic to the extension of k by a countable infinity of infinitesimals, the product of any two of which (including two the same) is zero.

2001-12-23:018

Let k be any ring (this means "commutative", of course). We say that a k-algebra A is *connected* when there are exactly two idempotents, namely 0 and 1 (note that this implies $A \neq 0$, because the zero-ring has exactly one idempotent which is both 0 and 1). Since idempotents of A are the same as k-algebra homomorphisms $k^2 \to A$, this is again the same as saying that $\mathrm{Hom}_k(k^2, A)$ has exactly two elements.

Unfortunately, the tensor product of two connected k-algebras need not be connected, even when k is a field. For example, $\mathbb{C}$ is a connected étale $\mathbb{R}$-algebra, but its tensor product with itself is $\mathbb{C} \otimes_{\mathbb{R}} \mathbb{C} = \mathbb{C}^2$ and it is not connected. However, over an algebraically closed field Ω, the tensor product of two connected algebras is again connected. (...continued at **2001-12-30:021**...)

See also **2001-12-30:022**.

2001-12-26:019

If k is a field, and A a k-algebra (this means "commutative", of course) of finite type, then A is a *Jacobson ring*, in other words every prime ideal is an intersection of maximal ideals: this is the "advanced formulation" of the Nullstellensatz. (More generally, this holds for an algebra of finite type over a Jacobson ring.) In particular, the Jacobson radical (the intersection of the maximal ideals) of A coincides with the set of nilpotent elements (the intersection of the prime ideals) of A. Moreover, the residue fields of A (modulo some maximal ideal) are finite field extensions of k (more generally, of the corresponding residue field of the base ring, for a Jacobson base ring).

Now let Ω be an algebraically closed field, and A an Ω-algebra. If $x \in A$, to see whether x is nilpotent (resp. idempotent) in A, it suffices to see whether it is in the algebra $\Omega[x] \subseteq A$ generated by x over Ω, or in any other Ω-subalgebra A_0 of A of finite type. In particular (by the above), it means that x is nilpotent iff it belongs to all the maximal ideals of A_0, and the quotient field of any such ideal is Ω. Therefore, x is nilpotent iff every Ω-algebra homomorphism $\eta\colon A_0 \to \Omega$ takes x to 0. This can be used to show that the tensor product of two reduced Ω-algebras is reduced. Indeed, let A and A' be two reduced Ω-algebras, and $x \in A \otimes_\Omega A'$ nilpotent: we can find two Ω-subalgebras A_0 of A and A'_0 of A' of finite type such that x belongs to the subalgebra $A_0 \otimes_\Omega A'_0$ of $A \otimes_\Omega A'$ (e.g. write x as a finite linear combination of tensor product of elements of A and of A' and take the Ω-subalgebras generated by these elements). (...continued at **2001-12-30:020**...)

2001-12-30:020

(This continues **2001-12-26:019**.)

We wish to show that if Ω is an algebraically closed field, then the tensor product of two reduced Ω-algebras is again reduced. So let A and A' be two reduced Ω-algebras, and $x \in A \otimes_\Omega A'$ be nilpotent. Write $x = \sum_i a_i \otimes a'_i$, with $a_i \in A$ and $a'_i \in A'$; furthermore, we can assume that the a'_i are linearly independent (over Ω). Call A_0 the Ω-subalgebra of A (finitely!) generated by the a_i. Now for every maximal ideal $\mathfrak{m}$ of A_0, the class of x in $(A_0/\mathfrak{m}) \otimes_\Omega A'$ (which is canonically isomorphic to A' since $A_0/\mathfrak{m} = \Omega$ canonically because A_0 is an algebra of finite type over the algebraically closed field Ω) is nilpotent, so it is 0 since A' is reduced; and, since the a'_i are linearly independent, the a_i are all in $\mathfrak{m}$, so they are in every maximal ideal of A_0, hence in every prime ideal (A_0 is a Jacobson ring), so they are all zero (A_0 is reduced). So $x = 0$, QED.

This proof is extremely unsatisfactory because of the use of the linear independence of the a'_i, which simply doesn't seem to belong there. Geometrically, we consider x as an Ω-valued function on $\operatorname{Spm}(A_0 \otimes_\Omega A'_0) = \operatorname{Spm} A_0 \times \operatorname{Spm} A'_0$, which is zero everywhere, so it is zero on every line (corresponding to a maximal ideal $\mathfrak{m}$ of A_0), but exactly how we go from there to x being zero is obscure at best.

2001-12-30:021

(This continues **2001-12-30:020** *and* **2001-12-23:018**.)

We wish to show that if Ω is an algebraically closed field, then the tensor product of two connected Ω-algebras is again connected. So let A and A' be two reduced Ω-algebras, and $e \in A \otimes_\Omega A'$ be idempotent. Write $e = \sum_i a_i \otimes a'_i$, with $a_i \in A$ and $a'_i \in A'$. Call A_0 the Ω-subalgebra of A (finitely!) generated by the a_i and A'_0 that generated by the a'_i. Now if e is not 1, there exists a maximal ideal, of $A_0 \otimes_\Omega A'_0$, which we can write $A_0\mathfrak{m}' + \mathfrak{m}A'_0$ for maximal ideals $\mathfrak{m}$ of A_0 and $\mathfrak{m}'$ of A'_0, to which it belongs. The class of e in $(A_0/\mathfrak{m}) \otimes_\Omega A'_0$ (which is canonically isomorphic to A'_0 since $A_0/\mathfrak{m} = \Omega$ canonically because A_0 is an algebra of finite type over the algebraically closed field Ω) is idempotent, so it is 0 or 1 since A'_0 is connected, and since it belongs to $\mathfrak{m}'$, it is not 1, so we have in fact $e \in \mathfrak{m}A'_0$. Then the class of e in $A_0 \otimes_\Omega (A'_0/\mathfrak{m}'') = A_0$, for any maximal ideal $\mathfrak{m}''$ of A'_0, is an idempotent of A_0, hence 0 or 1, and it cannot be 1 because it is in $\mathfrak{m}$. So e belongs to every maximal ideal of $A_0 \otimes_\Omega A'_0$, so it is nilpotent, so it is 0, QED.

This proof absolutely sucks! Geometrically, we say first that an ring A is connected iff $\operatorname{Spm} A$ is connected: the "only if" part is evident, and for the "if" part, notice that if U and V are disjoint open sets which cover $\operatorname{Spm} A$, then there exist elements p_U and p_V of A which vanish exactly on U and V respectively, and then $p_U + p_V$ is invertible (because it belongs to no maximal ideal) whereas $p_U p_V = 0$, and then $(p_U + p_V)^{-1} p_U$ is idempotent. Furthermore, we have $\operatorname{Spm}(A_0 \otimes_\Omega A'_0) = \operatorname{Spm} A_0 \times \operatorname{Spm} A'_0$ (as sets!), and as far as the topology is concerned, we use the following easy topological lemma. Lemma: let X and Y be two connected topological spaces, and consider some topology on $X \times Y$ (not necessarily the product topology) such that the restriction to every $\{x\} \times Y$ is canonically homeomorphic to Y and the restriction to every $X \times \{y\}$ is canonically homeomorphic to X; then $X \times Y$ is connected. Evidently, the Zariski topology on $\operatorname{Spm}(A_0 \otimes_\Omega A'_0) = \operatorname{Spm} A_0 \times \operatorname{Spm} A'_0$ has this property. Still, the whole process, whether presented algebraically (as above) or geometrically (as we have just done) is horrendous.

2001-12-30:022

(This resumes **2001-12-23:018**.)

As we have seen, a (commutative) k-algebra A is connected iff $\operatorname{Hom}_k(k^2, A)$ has exactly two elements (notice that we don't consider the zero algebra to be connected). A more satisfactory notion is that of a relatively connected algebra: namely when the map $\operatorname{Hom}_k(k^2, k) \to \operatorname{Hom}_k(k^2, A)$, induced by the canonical morphism $k \to A$, is bijective (here the idea is that A has precisely as many "connected parts" (a deliberately vague term) as k); of course, if k is connected, this is just the same as saying that A is connected. And then we create a relative notion: an k-algebra A is universally relatively connected iff for every k-algebra B the B-algebra $A \otimes_k B$ is relatively connected ("relatively" as a B-algebra!). Evidently, a universally relatively connected k-algebra is relatively connected; a counter-example

is readily found: take $\mathbb{C}[x]$ as a $\mathbb{C}[y]$-algebra with $y = x^2$ (the parabola), which is (relatively) connected, but not universally relatively connected as can be seen by tensoring by the $\mathbb{C}[y]$-algebra $\mathbb{C}$ given by, say, $y \mapsto 1$.

We should, of course, mention that the set $\mathrm{Hom}_k(k^2, A)$ of idempotents of a k-algebra A can be ordered by letting $e \leq e'$ iff $ee' = e$. This makes it into a lattice with least element 0, greatest element 1, greatest lower bound given by $\inf(e, e') = ee'$, and least upper bound by $\sup(e, e') = e + e' - ee'$; better even: it is a boolean algebra with "negation" $e \mapsto 1 - e$. This can also be identified with the boolean algebra of clopen subsets of $\mathrm{Spec}\, A$ (compare with **2001-12-15:007**; see also **2002-03-18:038**).

If A is a noetherian algebra, e.g. an algebra of finite type over a field k, then the boolean algebra $\mathrm{Hom}_k(k^2, A)$ of idempotents of A is finite. This follows (for example) from the following lemma on boolean algebras: a boolean algebra in which every (strictly) decreasing (or, equivalently, increasing) sequence of elements is finite, is finite.

> Let us prove the fact. Assume on the contrary that we have an infinite boolean algebra B in which every decreasing sequence of elements is finite (an infinite well-founded boolean algebra, that is). Recall that an element $u > \bot$ is called an *atom* iff there is no v such that $u > v > \bot$. Certainly B, being well-founded, has atoms: for example, start with $u_0 = \top$; now either this is an atom or there exists a u_1 such that $u_0 > u_1 > \bot$; so either u_1 is an atom or there exists a u_2 such that $u_0 > u_1 > u_2 > \bot$; and so on, and the process must stop with an atom since otherwise the (u_i) would form an infinite decreasing sequence, contrary to the hypothesis that B is well-founded.
>
> Now, if $u = u_0$ is an atom, every element v is either disjoint from u (in the sense that $u \sqcap v = \bot$), or it is greater or equal to u (which is equivalent to $u \sqcap v = u$); this is because $u \sqcap v \leq u$, so it can be only $\bot$ or u. And the boolean algebra $B_0 = B$ is the product of the two-element algebra $\{\bot, \top\}$ by the subalgebra B_1 consisting of elements disjoint from u (the term "subalgebra" is actually an abuse of language since $\top$ is not the same in B_1 as in B, but the meaning is clear anyway). Now B_1 verifies the same hypotheses as B. So we get an infinite sequence $u_0, u_1, \ldots$ of pairwise disjoint atoms. And then the sequence $u_0 < u_0 \sqcup u_1 < u_0 \sqcup u_1 \sqcup u_2 < \cdots$, forms an infinite increasing sequence of elements of B, and we deduce an infinite decreasing sequence, QED.

A noetherian k-algebra A is a direct product of finitely many connected k-algebras (note that the zero algebra is the empty product).

If Ω is an algebraically closed field, then any (relatively) connected Ω-algebra is, in fact, universally relatively connected. Indeed, we have to show that if B is an Ω-algebra and A a connected Ω-algebra, then the idempotents of $A \otimes_\Omega B$ are exactly those of B; now by standard arguments (see, e.g., **2001-12-26:019**), we can assume that A and B are noetherian, and furthermore that B is connected, and we have then to show that the tensor product of two connected Ω-algebras is again connected, which was done in **2001-12-30:021**.

If A is a universally relatively connected algebra over some ring k, then for every morphism $k \to \Omega$ to an algebraically closed field Ω, we have $A \otimes_k \Omega$ (relatively) connected. This follows immediately from the definition. We say that the algebra A has *connected geometric fibers*.

The converse seems to be true: if A is a k-algebra with connected geometric fibers, then A is universally relatively connected. But I don't have the patience to write it in full just now.

2002-01-03:023

If A is a noetherian, reduced, (commutative) ring and K_A is its total ring of fractions (i.e. the localization of A inverting the multiplicative set S of non-zerodivisors), the Olivier Wittenberg points out to me that K_A is an artinian ring (precisely, a finite product of fields).

If A is not reduced, this is no longer necessarily true. The simplest example seems to be $\mathbb{C}[\![x]\!][y]/(xy, y^2)$: every non zerodivisor of A is already invertible, but A is not artinian. However, this example is not really fascinating.

If A is not noetherian, even the conclusion that K_A is zero dimensional (recall that "artinian" is equivalent to "noetherian and zero-dimensional") is not necessarily true. Indeed, consider $A_n = \mathbb{C}[\![x_1, \ldots, x_n]\!]/((x_i x_j)_{i \neq j})$, i.e. the ring of formal series in n variables the product of any two (different) of which is zero, and let A be the

inductive limit of the A_n with the obvious (injective) arrows. Then every non-zerodivisor of A is already invertible, but A is not zero-dimensional.

This leaves us to challenge the idea of the total ring of fractions as an interesting construction. Still, it would be nice, given an arbitrary ring A, to find a zero-dimensional ring K_A and a morphism $A \to K_A$ that satisfies some universal property among such. Thus, $\operatorname{Spec} K_A \to \operatorname{Spec} A$ would form some kind of "zero-dimensional skeleton" (of generic points).

In the first case given above, $A = \mathbb{C}[\![x]\!][y]/(xy, y^2)$, we should have $K_A = \mathbb{C}(\!(x)\!) \times \mathbb{C}[y]/(y^2)$: note in particular that the prime ideals of K_A, viz. $((1,0))$ and $((0,y))$, do not correspond to the minimal prime ideals of A (there is only one such, namely (y))—here, we have something like an embedded component. In the second case, with A the inductive limit of the A_n defined above, K_A should be the subset of the direct product $\prod_{i=1}^{\infty} \mathbb{C}(\!(x_i)\!)$ of countably many copies of $\mathbb{C}(\!(x)\!)$ consisting of families $(f_1, f_2, \ldots)$ such that for some i_0 and some $c \in \mathbb{C}$ we have $f_i = c$ for $i > i_0$. (Perhaps it would be more reasonable to consider K_A as a pseudo-ring, i.e. not require the existence of a multiplicative unit, in which case we can just let $c = 0$.)

How can we compute K_A in general, and how can we check that the above assertions are correct?

2002-01-07:024

Is the following assertion true (it would be pleasant): a (commutative) ring A is reduced and zero-dimensional iff every element is the product of an idempotent by an invertible element? And can we find some analogous statement for possibly non-reduced rings?

If A has the property that every element is the product of an idempotent by a unit, then this also holds for every quotient of A, and in particular for the quotient of A by a prime ideal. But the quotient by a prime ideal is an integral domain, so its only idempotents are 0 and 1, so every element is either 0 or invertible, so the quotient is a field, so the prime ideal is maximal. So every prime ideal is maximal, and A is indeed zero-dimensional. And it is easy to see that it is reduced: if u is a unit and e is an idempotent, then for $n \geq 1$ we have $(ue)^n = u^n e$ and this can be zero only if e itself is zero. Therefore the "if" direction above is correct. (**Update:** the "only if" direction is also correct, see **2002-03-18:038**.)

2002-01-08:025

(This comes from an attempt to settle **2002-01-07:024**.)

Let A be a *reduced* (commutative) ring: this means that the intersection $\bigcap_{\mathfrak{p} \in \operatorname{Spec} A} \mathfrak{p}$ of all prime ideals of A is (0). If I is an ideal of A, the intersection $\bigcap_{I \subseteq \mathfrak{p} \in \operatorname{Spec} A} \mathfrak{p}$ of all prime ideals of A containing I is the radical $\sqrt{I}$ of I, which is I exactly when A/I is reduced (this does not require A reduced). Now is it true (for A reduced) that, for any ideal I of A, the intersection $I_0 = \bigcap_{\mathfrak{p} \in \operatorname{Spec} A} (\mathfrak{p} + I)$ of the sum of I with every prime ideal of A, is exactly I? Evidently I_0 contains I and is contained in the radical $\sqrt{I}$ of I. The statement is clear when I is radical (i.e. A/I is reduced), or in the case where A is an integral domain or more generally when I contains a prime ideal. But does it always hold? (**Update:** the answer is *no*, see **2002-01-09:026**.)

This would imply that A/I injects in $\prod_{\mathfrak{p} \in \operatorname{Spec} A} (A/(\mathfrak{p} + I))$, and, in particular, if all the $A/(\mathfrak{p} + I)$ are reduced (e.g. if A is zero-dimensional), so is A/I.

2002-01-09:026

(This answers **2002-01-08:025**.)

The answer to the question asked in **2002-01-08:025** is "no" (thanks to Hugues Randriambololona for providing me with a counter-example): take A the ring $\mathbb{C}[x,y]/(xy)$ and $I = (x - y)$ the ideal of the trace of the diagonal; then the two minimal primes of A are (x) and (y), so the intersection I_0 of the $\mathfrak{p} + I$ is $\sqrt{I} = (x, y)$ which is not I. And A/I is not reduced, whereas all the $A/(\mathfrak{p} + I)$ are. Ugh. This was utterly naïve.

2002-01-11:027

Let $A = C^*(\mathbb{N}, \mathbb{R})$ be the ring of bounded sequences of real numbers: this can be also seen as the ring $C(\beta\mathbb{N}, \mathbb{R})$ of continuous real-valued functions on the Stone-Čech compactification $\beta\mathbb{N}$ of the set of integers. If $p \in \beta\mathbb{N}$ is a point of said compactification, and $\mathscr{U}$ the ultrafilter on $\mathbb{N}$ to which it corresponds, there are two particularly important ideals of A which we can associate to p:

- The ideal $\mathbf{M}_p$ of all $f \in C(\beta\mathbb{N}, \mathbb{R})$ which vanish at p; in other words, $\mathbf{M}_p$ consists of those bounded sequences of real numbers which, when extended in the unique possible way to a continuous real-valued function on $\beta\mathbb{N}$, vanish at p. This is equivalent to saying that for every $\varepsilon > 0$ there exists $V \in \mathscr{U}$ such that $|f(n)| < \varepsilon$ for $n \in V$.
- The ideal $\mathbf{O}_p$ of all $f \in C(\beta\mathbb{N}, \mathbb{R})$ which vanish in the neighborhood of p; in other words, $\mathbf{O}_p$ consists of those bounded sequences of real numbers which, when extended in the unique possible way to a continuous real-valued function on $\beta\mathbb{N}$, vanish in some neighborhood of p. This is equivalent to saying that there exists $V \in \mathscr{U}$ such that $|f(n)| = 0$ for $n \in V$.

Facts: the $\mathbf{M}_p$ are exactly the maximal ideals of A; the $\mathbf{O}_p$ are prime ideal (which are not maximal except when $p \in \mathbb{N}$, i.e. when the ultrafilter $\mathscr{U}$ to which it corresponds is principal); every prime ideal $\mathfrak{p}$ of A satisfies $\mathbf{O}_p \subseteq \mathfrak{p} \subseteq \mathbf{M}_p$ for a unique $p \in \beta\mathbb{N}$ (and in particular, every prime ideal of A is contained in a unique maximal ideal, and the $\mathbf{O}_p$ are the minimal prime ideals of A). Among these facts, the only non-obvious statement is that every prime ideal is contained between $\mathbf{O}_p$ and $\mathbf{M}_p$ for a unique $p \in \beta\mathbb{N}$. To prove this, let $\mathfrak{p}$ be a prime ideal of A and $\mathbf{M}_p$ a prime ideal containing $\mathfrak{p}$ (we do not yet assert that $\mathbf{M}_p$ is unique). For every $f \in \mathbf{O}_p$ we can find $g \notin \mathbf{M}_p$ such that $fg = 0$ (e.g. let $g = 1_V$ where f cancels on $V \in \mathscr{U}$); then $g \notin \mathfrak{p}$ so we must have $f \in \mathfrak{p}$. This shows that $\mathbf{O}_p \subseteq \mathfrak{p}$, and it is then easy to see that $\mathbf{M}_p$ is the unique maximal ideal of A containing $\mathfrak{p}$.

Let I be the principal ideal of A generated by the sequence $(\frac{1}{n})$. In other words, I consists of those sequences f such that $g(n) = nf(n)$ is bounded. (Note: we simply forget about $0 \in \mathbb{N}$; this is unimportant.) Let $p \in \beta\mathbb{N} \setminus \mathbb{N}$ and $\mathscr{U}$ the corresponding non principal ultrafilter: then $f \in \mathbf{O}_p + I$ iff $g(n) = nf(n)$ is bounded on a certain $V \in \mathscr{U}$. So if $f \in \bigcap_{p \in \beta\mathbb{N}\setminus\mathbb{N}} (\mathbf{O}_p + I)$ then $g(n) = nf(n)$ is bounded on one some element of each ultrafilter $\mathscr{U}$ on $\mathbb{N}$. But then g is bounded on $\mathbb{N}$: otherwise, find an infinite subset $S \subseteq \mathbb{N}$ such that $g(n) \to +\infty$ on S (the case $g(n) \to -\infty$ is handled similarly) and consider a non principal ultrafilter concentrated on S—this gives a contradiction. Thus $I = \bigcap_{p \in \beta\mathbb{N}\setminus\mathbb{N}} (\mathbf{O}_p + I)$; and in particular, $I = \bigcap_{\mathfrak{p} \in \operatorname{Spec} A} (\mathfrak{p} + I)$. Thus in this case (rather surprisingly), the answer to the question asked in **2002-01-08:025** is "yes".

Note that I is *not* equal to $\bigcap_{\mathfrak{m} \in \operatorname{Spm} A} (\mathfrak{m} + I) = \bigcap_{p \in \beta\mathbb{N}} (\mathbf{M}_p + I)$: indeed, since $I \subseteq \mathbf{M}_p$ for every $p \in \beta\mathbb{N} \setminus \mathbb{N}$ and $\mathbf{M}_p + I = A$ for $p \in \mathbb{N}$, the intersection in question is $\bigcap_{p \in \beta\mathbb{N}\setminus\mathbb{N}} \mathbf{M}_p$, which is the set of sequences tending to 0 at infinity. In particular, A is certainly not of dimension 0 (anyway, we already know that $\mathbf{O}_p$ is prime but not maximal), a somewhat surprising fact since $\beta\mathbb{N}$ is a zero-dimensional topological space—and the ring of *all* real-valued sequences *is* zero-dimensional (see **2001-12-15:006**).

Thanks to Yves de Cornulier for this example. For a more general discussion of spaces $C(X, \mathbb{R})$, see Gillman & Jerison, *Rings of Continuous Functions* (Springer GTM 43).

2002-01-13:028

If E is a totally ordered set, we say that a pair (U, V) of subsets of E is a *Dedekind cut* of E iff $U = \{x \in E : (\exists y \notin V)(x < y)\}$ and $V = \{y \in E : (\exists x \notin U)(y > x)\}$. Evidently this means that whenever $x < y$, we have $y \in U \implies x \in U$ and $x \in V \implies y \in V$, and consequently $U \cap V = \varnothing$. The complement of $U \cup V$ is either empty or equal to a singleton $\{a\}$, in which case $U = \{x \in E : x < a\}$ and $V = \{y \in E : y > a\}$. In the latter case, we say that the Dedekind cut is *convergent* or *principal*, and a is its *limit* (note that it is uniquely determined, by definition). The set E^* of Dedekind cuts of E is totally ordered by letting $(U, V) \leq (U', V')$ iff $U \subseteq U'$, or, equivalently, $V' \subseteq V$; and E naturally embeds in E^* by sending each a to the principal cut with limit a. We say that a totally ordered set F is *Dedekind-complete* iff every subset of F has a least upper bound: this is equivalent to every subset having a greatest lower bound, or to F being compact for the order topology, or to every Dedekind cut being principal. The set E^* of Dedekind cuts of E as previously defined is Dedekind-complete for every E, and we call it the *Dedekind completion*

of E. It is, in a sense which we shall not bother to make precise, the smallest Dedekind-complete totally ordered set containing E.

Now suppose E is a totally ordered abelian group: this means that E has a structure as a totally ordered set and a structure as an abelian group and that the two are compatible in the sense that every translation is order-preserving. Then E^* does *not* have a totally ordered abelian group structure except if it is trivial — this is because it has a least element (as the least upper bound of the empty set) and no non trivial totally ordered abelian group has a least element. On the other hand, we can define a *Dedekind-Cauchy cut* of E as a Dedekind cut (U, V) with the additional property that for every $\varepsilon > 0$ of E there exists an $x \in U$ and an $y \notin U$ with $y - x = \varepsilon$ (or, equivalently, there exists $y \in V$ and $x \notin V$ with $y - x = \varepsilon$). For example, each principal Dedekind cut is a Dedekind-Cauchy cut. Conversely, if every Dedekind-Cauchy cut is principal, we say that E is *Dedekind-Cauchy-complete* (or simply *complete*). In general, the set E^+ of Dedekind-Cauchy cuts of E, with the order induced upon it by the set E^* of all Dedekind cuts, has a natural structure as a totally ordered abelian group, extending E (seen as the subset of principal cuts), which is Dedekind-Cauchy-complete. We call it the *Dedekind-Cauchy completion* of E. It is again, in a sense which we shall not bother to make precise, the smallest Dedekind-Cauchy-complete totally ordered abelian group containing E.

For example, the Dedekind-Cauchy completion of the set $\mathbb{Q}$ of rational numbers (with the usual order and the abelian group structure given by addition) is $\mathbb{R}$ (with the usual order and addition). There are only two Dedekind cuts of $\mathbb{Q}$ which are not Cauchy, namely $(\mathbb{Q}, \varnothing)$, which we write as $+\infty$, and $(\varnothing, \mathbb{Q})$, which we write as $-\infty$; so the Dedekind completion of $\mathbb{Q}$ is $\bar{\mathbb{R}} = \mathbb{R} \cup \{\pm\infty\}$.

If E is a totally ordered *field* (which means that it is a totally ordered abelian group for addition, and the product of two positive elements is positive), its Dedekind-Cauchy completion is again a totally ordered field. Recall that a totally ordered field E is *real-closed* iff for every polynomial $f \in E[t]$, whenever $f(x) < 0$ and $f(y) > 0$ there exists $x < a < y$ such that $f(a) = 0$ (there are various equivalent definitions of this); every totally ordered field E can be embedded in a unique smallest real-closed field containing E, called the *real closure* of E. Note that neither of the two notions of Dedekind-Cauchy completeness and real closedness implies the other (for example, the real closure of $\mathbb{Q}$, i.e. the set of real algebraic numbers, is real-closed but not Dedekind-Cauchy-complete; and on the other hand the field $\mathbb{Q}(\!(t)\!)$ of Laurent series with rational coefficients in the indeterminate t, totally ordered lexicographically on powers of t—thus making t^{-1} infinitely large with respect to $\mathbb{Q}$—is Dedekind-Cauchy-complete but not real-closed). On the other hand, the Dedekind-Cauchy completion of a real-closed field is again real-closed (at least I think so; perhaps I should check more carefully).

Now if E is a real-closed field and (U, V) is a Dedekind cut (not necessarily Cauchy) which does not converge (note that such cuts always exist: $(E, \varnothing)$ is an example), we can form a new real-closed field E' containing E and in which there exists t verifying $U < t < V$ (this means $x < t$ for all x in U and $y > t$ for all y in V; we do not assert that t is unique), as follows. First form the field $E(t)$ of rational functions with coefficients in E on the indeterminate t. If $f(t)$ is a non-zero element of $E(t)$, it changes sign a finite number of times, and, because E is real-closed, at elements of E (either zeroes or poles); therefore there exist $x \in U$ and $y \in V$ such that it has a constant sign on the interval $[x; y]$: we let $f(t) > 0$ or $f(t) < 0$ according as this sign is positive or negative. This defines a total order on $E(t)$ extending that on E. And we let E' be the real closure of $E(t)$ for this total order. Note that if (U, V) was a Dedekind-Cauchy cut, E' is contained in the Dedekind-Cauchy completion (and t is indeed unique, as the limit of (U, V) in the latter).

We can then attempt to repeat the previous operation several times (even transfinitely many times). For example, let E be a real-closed field, and define $E_0 = E$, and, for each ordinal α, if E_α has been defined and there exists a Dedekind cut (U, V) of E such that no t of E_α satisfies $U < t < V$, then let $E_{\alpha+1} = (E_\alpha)'$ for the unique Dedekind cut of E_α extending (U, V), and for δ a limit ordinal let $E_\delta = \bigcup_{\alpha<\delta} E_\alpha$ (which is really an inductive limit for the inductively defined natural embeddings). Evidently the process must stop at some point, and then we have obtained a field $E^\sharp$ which has "filled" every cut (U, V) of E. *Petitio principii*: the field $E^\sharp$ does not depend on the choices made. How do I prove this? Then we call $E^\sharp$ the Dedekind-Conway completion of E. Note that there is no such thing as a Dedekind-Conway-complete field (thus the term "completion" is inadequate), because $E^\sharp$ is *always* larger than E. *Petitio principii secunda*: iterating the operation $E \mapsto E^\sharp$ transfinitely on all ordinals, starting from the field of real

algebraic numbers, we obtain Conway's field of "Numbers". This needs to be carefully checked.

Another similar process we can go through is as follows. We say that a totally ordered set (and, in particular, a real-closed field) E is an η_γ-set iff for any two subsets A, B (possibly empty) of E of cardinal $< \aleph_\gamma$ such that $A < B$ (that is, $x < y$ for all $x \in A$ and $y \in B$) there exists $t \in E$ such that $A < t < B$. Now start with a real-closed field E, and let α be any ordinal. If E is not η_γ, there exist subsets A, B of E with cardinal $< \aleph_\gamma$ such that $A < B$ but there is no $t \in E$ with $A < t < B$; and then the subsets $U = \{x \in E : (\exists y \in A)(x \leq y)\}$ and $V = \{y \in E : (\exists x \in B)(y \geq x)\}$ form a Dedekind cut (U, V) of E, which is not convergent. By the operation described above, we can construct a larger real-closed field E' which adds an element t to E satisfying $U < t < V$ (and in particular $A < t < B$). Either E' is η_α, in which case we have finished, or it is not, in which case we continue, and we repeat the process transfinitely. Eventually this must come to a stop: at least this is clear if we first fill all the η_γ gaps in E and then in the extension thus created, and so on. Indeed, let $E_0 = E$ and for every α let $E_{\alpha+1}$ be real-closed field containing E_α and such that for all A end B of cardinal $< \aleph_\gamma$ in E_α there exists $t \in E_{\alpha+1}$ with $A < t < B$ and for δ a limit ordinal let $E_\delta = \bigcup_{\alpha<\delta} E_\alpha$; then, if κ has cofinality at least $\aleph_\gamma$, for any A and B of cardinal $< \aleph_\gamma$ in E_κ, these already belong to some E_α for $\alpha < \kappa$, and then there exists $t \in E_{\alpha+1} \subseteq E_\kappa$ such that $A < t < B$: so E_κ is a real-closed η_γ field. (Does the process always stop, no matter in what order the completions are carried out?)

2002-01-13:029

It is a well-known fact that we can calculate the integral (the antiderivative, actually) of any rational function in closed form: the result involves rational functions and logarithms—precisely, it is a linear combination of logarithms (of translations of the indeterminate) with coefficients being rational functions (we remain voluntarily very vague as to where the coefficients live; on the reals, for example, we would need to introduce the arctangent). This is done by writing the rational function in partial fractions, and integrating each separately: we have $\int \frac{dt}{(t-a)^k} = -\frac{1}{(k-1)(t-a)^{k-1}}$ for $k \neq 1$, and $\int \frac{dt}{t-a} = \log(t-a)$.

Every polynomial in logarithms (with coefficients being rational functions) can still be integrated in closed form: this is done by integrating by parts as many times as necessary. For example, $\int \frac{\log t}{(t-a)^2}\,dt = -\frac{\log t}{t-a} + \int \frac{dt}{t(t-a)} = -\frac{\log t}{t-a} - \frac{\log t}{a} + \frac{\log(t-a)}{a}$. There is one exception, however: to evaluate expressions such as $\int \frac{\log t}{t-a}\,dt$, we need to introduce the dilogarithm, given by $\operatorname{dilog}' t = -\frac{\log(1-t)}{t}$ (and $\operatorname{dilog} 0 = 0$). It would seem that the smallest ring (whatever that means) which contains rational functions and is closed under integration (antiderivatives) is the ring of polynomials (with coefficients being rational functions) over all polylogarithms of linear terms. This is already rather complicated.

If we introduce logarithms in the denominator, things get even worse. Notably, there appears the logarithm integral function, $\operatorname{li} t = \int \frac{dt}{\log t}$. Note that $\int \frac{t^k}{\log t}\,dt = \operatorname{li} t^{k+1}$ except, weirdly, when $k = -1$ and then $\int \frac{dt}{t \log t} = \log\log t$.

Question: what is the smallest field containing t (and hence all rational functions) and closed under integration? (Precondition: how to define it rigorously?) Do its elements have some canonical form? Is equality decidable (and with what complexity) in this field?

2002-01-20:030

Let A be a finite alphabet, and A^* the free monoid with base A (the set of words with letters in A). Define a partial order on A^* by letting $u \preceq v$ iff we can write $u = u_1 \cdots u_n$ and $v = v_0 \cdot u_1 \cdot v_1 \cdots v_{n-1} \cdot u_n \cdot v_n$, where $u_1, \ldots, u_n$ and $v_0, \ldots, v_n$ are elements of A^* (possibly equal to the unit element, i.e. the empty word). In other terms, $u \preceq v$ iff u can be obtained by removing certain letters (anywhere) from v; we say that u is a *subword* of v. *Higman's lemma* states that for any infinite subset S of A^* there must exist distinct $u, v \in S$ verifying $u \preceq v$. (**Update:** for a proof, and a probably better statement, see **2002-01-23:031**.)

This leads us to consider the following game: two players take turns in selecting an element of A^* subject to the condition that no subword of it have already been played, and the first player who cannot play loses. Evidently, this

game is not really fascinating (because any player who can play can win in a single move by playing the empty word), and it is more interesting to consider the *"misère"* version of it, where the empty word is forbidden (or, equivalently, the first player who cannot play *wins*, the usual meaning of the word "misère" in combinatorial game theory). Call these two games respectively the *normal Higman game* and the *misère Higman game*. (**Update:** see also **2002-12-01:047** and **2002-12-01:048**.)

For S a subset of A^*, we define inductively the *length* and the *Grundy function*, written $\lg(S)$ and $\mathrm{Gy}(S)$ respectively, for the normal and misère versions of the Higman game (we write $\lg_N(S)$ and $\mathrm{Gy}_N(S)$ for the normal versions and $\lg_M(S)$ and $\mathrm{Gy}_M(S)$ for the misère versions), as follows:

- $\lg(S)$ is the smallest ordinal (strictly) greater than $\lg(S')$ for every $S' = S \cup \{w\}$ with w a word no subword of which belongs to S, and moreover with the constraint that w is not the empty word in the misère case (in other words, S' is a legal move in the game from the position S, that is, the position where S is the set of words that have been played).
- $\mathrm{Gy}(S)$ is the smallest ordinal different from $\mathrm{Gy}(S')$ for every $S' = S \cup \{w\}$ as above.

Higman's lemma assures that this inductive definition makes sense (i.e. terminates). Of course, the value of $\lg(S)$ or $\mathrm{Gy}(S)$ depends heavily on the chosen alphabet A: for more clarity, we might write, e.g. $\lg(A, S)$ to emphasize on the choice of A, or even $\lg(n, S)$ where $n = \operatorname{card} A$ (because only the size of A really matters).

We have $\lg(S) = 0$ iff every word (non-empty in the misère version) has an element of S as subword; in other words, iff the player who just played (the "second player") won. Of course, $\lg_N(S) = 0$ iff $\epsilon \in S$ where ϵ is the empty word; and $\lg_N(S) = 1$ iff $\epsilon \notin S$ and $\lg_M(S) = 0$; and more generally, when $\epsilon \notin S$, we have $\lg_N(S) = 1 + \lg_M(S)$ (proved inductively). Concerning the Grundy function, we have $\mathrm{Gy}(S) = 0$ iff the second player has a winning strategy, which consists of continuously playing so that $\mathrm{Gy}(S) = 0$ after the play: these configurations form the "kernel" of the game. Of course, $\mathrm{Gy}_N(S) = 0$ iff $\epsilon \in S$ (as previously mentioned, if the game is not immediately over, the first player wins by playing the empty word); and for any S such that $\epsilon \notin S$, we have $\mathrm{Gy}_N(S) = 1 + \mathrm{Gy}_M(S)$ (proved just as the corresponding statement for lg). So we can now concentrate on the normal version of the game, which is more elegant than the misère version (even though the normal game itself is vacuous, its Grundy function is of interest).

For $A = \varnothing$ (and consequently $A^* = \{\epsilon\}$), all is trivial: $\lg_N(0, \{\epsilon\}) = \mathrm{Gy}_N(0, \{\epsilon\}) = 0$, and consequently, $\lg_N(0, \varnothing) = \mathrm{Gy}_N(0, \varnothing) = 1$, or in other words $\lg_M(0, \varnothing) = \mathrm{Gy}_M(0, \varnothing) = 0$. For $A = \{a\}$ (so that A^* is isomorphic as a monoid to that of the natural numbers, written multiplicatively as powers of a), we have $\lg_N(1, \{a^k\}) = \mathrm{Gy}_N(1, \{a^k\}) = n$ (by induction on n), so that $\lg_N(1, \varnothing) = \mathrm{Gy}_N(1, \varnothing) = \omega$ (or in other words $\lg_M(1, \varnothing) = \mathrm{Gy}_M(1, \varnothing) = \omega$). For $\operatorname{card} A = n > 1$, things are already vastly complicated. We can notice however that if $a \notin A$ then for any $S \subseteq A^*$ we have $\lg(A \cup \{a\}, S \cup \{a\}) = \lg(A, S)$, and similarly $\mathrm{Gy}(A \cup \{a\}, S \cup \{a\}) = \mathrm{Gy}(A, S)$. In particular, for $A = \{a, b\}$ we have $\lg_N(2, \{a\}) = \mathrm{Gy}_N(2, \{a\}) = \omega$. Note also that if $\mathrm{Gy}_M(n, \varnothing) = 0$ then $\mathrm{Gy}_M(n+1, \varnothing) > 0$ because $\mathrm{Gy}_M(n+1, \varnothing) \neq \mathrm{Gy}_M(n+1, \{a\}) = \mathrm{Gy}_M(n, \varnothing)$ by definition; so in at least one half of all possible alphabet lengths the first player has a winning strategy in the misère version of the game from the canonical initial position.

Vincent Nesme observes that the Higman game with alphabet $A = \{a, b\}$, in the situation where the word ba has already been played can be identified with Conway's "poisoned wafer" game: start with the quarter integer plane $\mathbb{N}^2$ (where $(k, \ell) \in \mathbb{N}^2$ is identified with the word $a^k b^\ell$) and each player in turn chooses a remaining (k_0, ℓ_0) and removes $\{(k, \ell) : k \geq k_0 \wedge \ell \geq \ell_0\}$ from the plane until one cannot play (and then wins in the normal version and loses in the misère version). Calculating the Grundy function for this game is very difficult; but the length can be determined without too much trouble. Namely, when there remain r full lines or columns and s points not in a full line or column, the length is $\omega \cdot r + s$; and so for the full plane it is ω^2. That is, $\lg_N(2, \{ba\}) = \omega^2$ (and of course $\lg_M(2, \{ba\}) = \omega^2$).

(**Updated 2002-01-23**.) It would seem that $\lg(2, \{a^2\}) = \omega^2$ (as a variant of the poisoned wafer represented by the words $b^k a b^\ell$ and b^m). It then seems plausible to conjecture that $\lg(2, \{w\} = \omega^{l(w)}$ where $l(w)$ is the length of w (the number of letters in w), so $\lg(2, \varnothing) = \omega^\omega$. Do we perhaps have $\lg_N(n+1, \varnothing) = \omega^{\lg_N(n, \varnothing)}$ for every $n \in \mathbb{N}$?

2002-01-23:031

Here is an understandable (but non constructive) proof of Higman's lemma (used as the starting point of **2002-01-20:030**). This is based ("instanciated" would be a better word) from a proof that Alain Frisch provided.

Recall the following definitions from **2002-01-20:030**: Let A be a finite alphabet, and A^* the free monoid with base A (the set of words with letters in A). Define a partial order on A^* by letting $u \preceq v$ iff we can write $u = u_1 \cdots u_n$ and $v = v_0 \cdot u_1 \cdot v_1 \cdots v_{n-1} \cdot u_n \cdot v_n$, where $u_1, \ldots, u_n$ and $v_0, \ldots, v_n$ are elements of A^* (possibly equal to the unit element, i.e. the empty word). In other terms, $u \preceq v$ iff u can be obtained by removing certain letters (anywhere) from v; we say that u is a *subword* of v.

We say that a sequence $(w_i) = (w_0, w_1, w_2, \ldots)$ of elements of A^* is *miraculous* iff there do not exist integers $i < i'$ such that $w_i \preceq w_{i'}$, in other words, if no word in the sequence is a subword of some ulterior word. Higman's lemma states that there is no miraculous sequence, and our goal is to prove this.

(A side note: in **2002-01-20:030**, we made the weaker statement that if $S \subseteq A^*$ is infinite then there exist $u, v \in S$ distinct such that $u \preceq v$. This turns out to be equivalent: indeed, if we assume the latter, and (w_i) is a miraculous sequence of elements of A^*, by removing from the sequence every word that has some subword later in the sequence, we clearly obtain a still infinite and still miraculous sequence, about which a contradiction can be found by applying the assumed statement. In fact, we have tacitly used the stronger form in **2002-01-20:030**, and the proof was more or less contained in our description of the game...)

Now, assume there exists a miraculous sequence, that starts, say, with $w_0 \in A^*$. Remove the first letter from w_0, and see whether it still starts some miraculous sequence: and keep doing so until we find a w_0 which starts a miraculous sequence but such that after removing its first letter it no longer does. Since any word reduces to the empty word after removal of a finite number of initial letters, and since the empty word ϵ cannot be part of a miraculous sequence, we certainly can find such w_0.

Now there exists a miraculous sequence that starts with, say, (w_0, w_1) (where w_0 has been found above). Removing again the first letter from w_1 as much as possible, we can assume that (w_0, w_1) starts a miraculous sequence, but no longer does so after removal of the first letter from w_1. And we continue in this way to form a miraculous sequence $(w_i) = (w_0, w_1, w_2, \ldots)$ which satisfies the following minimality condition. If (v_i) is a sequence obtained by removing the initial letter from some term of (w_i) and altering the subsequent terms in any way whatsoever (i.e. $v_i = w_i$ for $i < i_0$, v_{i_0} is obtained by removing the first letter of w_{i_0}, and v_i for $i > i_0$ are arbitrary), then (v_i) is *not* miraculous.

Having obtained this minimal miraculous sequence $(w_i) = (w_0, w_1, w_2, \ldots)$, we observe that an infinite number of terms thereof must start with the same letter, say $a \in A$ (because A is finite). Say $\varphi\colon \mathbb{N} \to \mathbb{N}$ is an increasing function such that $w_{\varphi(j)}$ starts with the letter a.

We then construct (v_i) as follows: remove the initial "a" from this sequence of words, keep all words before the initial one unchanged, and delete all others. That is, $v_i = w_i$ for $i < i_0$ where $i_0 = \varphi(0)$, and v_{i_0+j} is obtained by removing the initial "a" from $w_{\varphi(j)}$.

Then by minimality of (w_i) the sequence (v_i) is *not* miraculous, that is, there exist $j < j'$ such that $v_j \preceq v_{j'}$. But by adding possibly an initial "a" to $v_{j'}$ (precisely if $j' \geq i_0$), and, *only if so* (precisely if $j \geq i_0$), possibly also an initial "a" to v_j, we construct two terms w_i and $w_{i'}$ of the sequence (w_i) with $i < i'$ (viz. $i = j$ if $j < i_0$ and $i = \varphi(j - i_0)$ otherwise; and similarly for i') such that $w_i \preceq w_{i'}$. This contradicts the miraculousness of (w_i).

This contradiction proves Higman's lemma.

Note that this proof is non constructive and does not seem to give a bound on the ordinal length of the Higman game (defined in **2002-01-20:030**)—though perhaps a closer study will reveal more information.

2002-02-07:032

(I am grateful to Alain Frisch for teaching me about the following concepts.)

A totally ordered set E is well-ordered iff there exist no (strictly) decreasing sequence $u_0 > u_1 > u_2 > \cdots$ of elements of E (this uses the axiom of dependent choice, but no matter: we always work with the full axiom of choice); alternatively, iff for every sequence (u_i) of elements of E there are $i < j$ such that $u_i \leq u_j$ (a mere restatement of the same fact).

When we translate these conditions to partially ordered sets, we get two different notions. Precisely, a partially ordered set E is called *well-founded* iff there exist no (strictly) decreasing sequence $u_0 > u_1 > u_2 > \cdots$ of elements of E. And a partially ordered set E is called *fairly ordered* iff for every sequence (u_i) of elements of E there are $i < j$ such that $u_i \leq u_j$. Evidently, a fairly ordered set is well-founded, but the converse is not true (consider an infinite set any two distinct elements of which are incomparable).

To say that E (a partially ordered set) is well-founded is equivalent to saying that if $S \subseteq E$ satisfies the condition that "if $x \in E$ is such that every $y \in E$ with $y < x$ belongs to S, then x itself belongs to S" then $S = E$. Indeed, if E is a partially ordered set containing a decreasing sequence $u_0 > u_1 > u_2 > \cdots$, consider the set $S = \{x \in E : \neg\exists n(x \geq u_n)\}$ of elements of E which are not greater than some term of the sequence: a moment's thought suffices to check that it satisfies the stated induction condition, and yet $u_0 \notin S$ so $S \neq E$. Conversely, if E is a partially ordered, and $S \neq E$ satisfies the stated induction condition, then there exists $u_0 \in E \subseteq S$ (because $S \neq E$) and then—by the condition in question—there exists $u_1 < u_0$ in E with $u_1 \notin S$, and so on, forming a strictly decreasing sequence of elements of E.)

Equivalently, a partially ordered set is well-founded iff every non-empty subset $S \subseteq E$ contains a minimal element (in the sense that it is an element of S for which there is no element of S that is strictly smaller). This is easy to see.

There are several equivalent conditions to being fairly ordered. One is this: a partially ordered set E is fairly ordered iff every non-empty subset S of E has a finite (strictly) positive number of minimal elements. Indeed, that it has minimal elements follows by the above, since "fairly ordered" is stronger than "well-founded"; and if there were an infinite number of such, then we could form a sequence of pairwise incomparable elements of E, a contradiction. In fact, we can also use this reasonging to see that being fairly ordered is equivalent to the (seemingly weaker) condition of being well-founded and having no infinite antichain. Indeed, if E is well-founded and has no infinite antichain and (u_i) is a sequence of elements of E, the reasoning shows that there is a minimal element of the sequence, say u_k, with greatest index k. Now x_{k+1} is not minimal, so by well-foundedness it is greater than a minimal element, u_ℓ, with $\ell \leq k$, and we then have $u_\ell \leq u_{k+1}$ with $\ell < k + 1$, as was to be shown.

Yet another equivalent condition can be described as follows. If E is a partially ordered set, let E^* be the set of finite (possibly empty) subsets of E no two elements of which are comparable. Partially order E^* by letting $\{u_1, \ldots, u_m\} \leq \{v_1, \ldots, v_n\}$ iff for every $j \in \{1, \ldots, n\}$ there exists $i \in \{1, \ldots, m\}$ with $u_i \leq v_j$. For commodity, we write the elements of E^* as follows: the empty set will be written $\top$ and the finite set $\{u_1, \ldots, u_m\}$ will be written $u_1 \wedge \cdots \wedge u_m$, with each $u \in E$ being implicitly identified with its singleton in E^* (this identifies E as an ordered set and a subset of E^* with the induced order). We extend $\wedge$ to make it into an associative and commutative binary operation on E^* by declaring that if $u \leq v$ are elements of E then $u \wedge v = u$ (this suffices, given a finite set of elements of E, to reduce it to a subset no two elements of which are comparable, thus giving an element of E^*). Clearly, if u and v are elements of E^* then $u \wedge v$ is the greatest lower bound of u and v in E^*; notice however that even if u and v belong to E and their greatest lower bound already exists in E, it may not coincide with $u \wedge v$ in E^* (if does coincide exactly when u and v are comparable). The property is then that E is fairly ordered iff E^* is well-founded. Indeed, if E has a strictly decreasing sequence, it is also strictly decreasing in E^*; and if E has an infinite antichain (u_i) then the sequence $\top, u_0, u_0 \wedge u_1, u_0 \wedge u_1 \wedge u_2, \ldots$ is a strictly decreasing sequence in E^*; this proves that if E^* is well-founded then E is fairly ordered; conversely, if E is fairly ordered and $\top > u_0 > u_1 > u_2 > \cdots$ is a strictly decreasing sequence in E^*, choose for each $j \in \mathbb{N}$ a v_j in u_j such which is not in any u_i for $i < j$, then we cannot have $v_i \leq v_j$ for $i < j$. This formulation means that we can also rewrite the condition of being "fairly ordered" as an induction principle, only this time not on E but on E^*.

TODO: ranks, heights, lengths and so forth; extending orders by total orders and relation with ranks, heights, lengths and so forth; lengths of games; products of fairly ordered sets are fairly ordered and explicit bounds on this; applications to Higman's lemma (see **2002-01-23:031**): obtaining explicit ordinal bounds.

See also **2002-05-21:043** for some further questions on E^*.

2002-03-11:033

("Tao of Topoi.")

An (elementary) *topos* is a category which admits finite limits (in particular it has a terminal object $\top$ and a binary product $\times$; in fact, it suffices to suppose the existence of these), an internal Hom functor (this means that there exists a functor $(A, B) \mapsto A^B$ together with a natural isomorphism $\mathrm{Hom}(C, A^B) \cong \mathrm{Hom}(B \times C, A)$) and a subobject classifier (this means that there exists an object Ω and an arrow $true\colon \top \to \Omega$ such that every monomorphism $B \to A$ is the pullback of $true$ by a unique morphism $\chi\colon A \to \Omega$ called the characteristic morphism of B in A).

These properties already suffice to construct arbitrary finite colimits. For example, to construct $\bot$ (the initial object), using the key idea that "$\bot = \forall_{(p:\Omega)} p$", we consider the identity morphism $\Omega \to \Omega$ and the $true$ morphism $\Omega \to \Omega$ (actually the composite $\Omega \to \top \stackrel{true}{\to} \Omega$), and we form their product, giving a morphism $\Omega \to \Omega^2$, or, if we prefer, $\top \to \Omega^{2\times\Omega}$. Now we have a diagonal morphism $\Omega^\Omega \to \Omega^{2\times\Omega}$ which is a monomorphism, so it has a characteristic morphism $\Omega^{2\times\Omega} \to \Omega$, so the composition of the two morphisms we have defined gives a $false\colon \top \to \Omega$ which is the characteristic morphism of $\bot \to \top$. Similarly, the motto "$p \vee q = \forall_{(r:\Omega)}((p \Rightarrow r) \wedge (q \Rightarrow r)) \Rightarrow r$" allows one to construct the binary coproduct.

If $\mathbf{C}$ is a category, we have a topos of presheaves of sets on $\mathbf{C}$, i.e. contravariant functors from $\mathbf{C}$ to $\mathbf{Sets}$. Limits and colimits are computed pointwise. The internal Hom takes two presheaves A and B on $\mathbf{C}$ to the presheaf A^B whose sections $(A^B)(U)$ on an object U of $\mathbf{C}$ are natural transformations from $\mathrm{Hom}(-, U) \times B$ to A. And the subobject classifier Ω is the presheaf whose sections $\Omega(U)$ on an object U of $\mathbf{C}$ are sieves on U (i.e. sets of arrows with target U closed under composition on the right when meaningful). If further J is a Grothendieck topology on $\mathbf{C}$ (i.e. a data giving, for every object U of $\mathbf{C}$ a set of sieves $J(U)$ on U, called covering sieves, such that (i) the full sieve with target U belongs to $J(U)$, (ii) if S belongs to $J(U)$ and $h\colon V \to U$ is any arrow then $h^*S = \{f | hf \in S\}$ is in $J(V)$, and (iii) if S is in $J(U)$ and R is a sieve on U such that for every $h \in S$ the sieve h^*R is covering, then S is covering), then we have a topos of sheaves of sets on $(\mathbf{C}, J)$, i.e. the full subcategory of that of presheaves consisting of those presheaves A for which, for every $S \in J(U)$, sections of A on U coincide exactly with matching families of sections of A on S. The internal Hom is the same as for presheaves. And the subobject classifier Ω is the sheaf whose sections $\Omega(U)$ on an object U of $\mathbf{C}$ are J-closed sieves on U (i.e. sieves S with target U having the property that if S covers $h\colon V \to U$, that is, $h^*S \in J(V)$, then h is already in S; the converse is automatic). The inclusion functor of the category of sheaves in the category of presheaves has a left adjoint, the "associated sheaf functor", which is itself left exact.

More generally, in a topos $\mathcal{T}$, we say that a *Lawvere-Tierney topology* is a morphism $j\colon \Omega \to \Omega$ such that (i) $j \circ true = true$, (ii) $j \circ j = j$ and (iii) $j \circ and = and \circ (j \times j)$, where $and\colon \Omega^2 \to \Omega$ is the characteristic function of $(true, true)\colon \top \to \Omega^2$. In other words, for the internal logic of the topos, j is an idempotent modalizer which preserves finite conjunctions. A monomorphism $C \to B$ is called j-closed (resp. j-covering, sometimes called "j-dense") iff its characteristic function $\chi\colon B \to \Omega$ factors through j (in the sense that $j \circ \chi = \chi$; resp. satisfies $j \circ \chi = true$); every monomorphism $C \to B$ factors as $C \to C' \to B$ where $C' \to B$ is j-closed and $C \to C'$ is j-covering. We say that an object A (of $\mathcal{T}$) is a *sheaf* (for j) iff for every j-covering monomorphism $C \to C'$ the associated map $\mathrm{Hom}(C', A) \to \mathrm{Hom}(C, A)$ is bijective. Then the subcategory $\mathrm{Sh}_j(\mathcal{T})$ of $\mathcal{T}$ consisting of j-sheaves is again a topos. The inclusion functor $\mathrm{Sh}_j(\mathcal{T}) \to \mathcal{T}$ of the category of j-sheaves in the original topos has a left adjoint, the "associated sheaf functor", which is itself left exact. The internal Hom functor of $\mathrm{Sh}_j(\mathcal{T})$ is the same as that of $\mathcal{T}$; and the subobject classifier Ω_j of $\mathrm{Sh}_j(\mathcal{T})$ is the equalizer of $j\colon \Omega \to \Omega$ and $true\colon \top \to \Omega$.

Lawvere-Tierney topologies generalize Grothendieck topologies: if J is a Grothendieck topology on a category $\mathbf{C}$, the morphism $j\colon \Omega \to \Omega$ in the topos $\mathbf{Sets}^{\mathbf{C}^{\mathrm{op}}}$ of presheaves on $\mathbf{C}$, which takes a sieve S on U (an object of $\mathbf{C}$) to the smallest J-closed sieve $j(S)$ containing S (that is, $j(S)$ is the set of all arrows h with target U such that h^*S is covering), defines a Lawvere-Tierney topology. Furthermore, sheaves for j and sheaves for J coincide, and so do the associated sheaf functors. And every Lawvere-Tierney topology on a presheaf topos comes from a Grothendieck topology in this sense.

TODO: examples of Lawvere-Tierney topologies (the $\neg\neg$ topology, the skyscraper topology); construction of topoi of coalgebras on a comonad (see **2002-03-12:035**); factorization of geometric morphisms; examples in algebraic

geometry. (See also **2002-12-05:051** and **2002-12-21:053**.)

2002-03-12:034

("Mental exercises in abstract nonsense.")

Let G be a group. Consider on the one hand the category $\mathbf{Sets}$ of sets and on the other hand the category $G\,\mathbf{Sets}$ of G-sets (sets together with an action of G, morphisms being maps preserving the action of G); both are topô. We can define several functors between these categories:

- $\phi_!\colon G\,\mathbf{Sets} \to \mathbf{Sets},\ X \mapsto X/G$ takes a G-set X to its set of orbits.
- $\phi^*\colon \mathbf{Sets} \to G\,\mathbf{Sets},\ X \mapsto X$ takes a set X to the G-set whose underlying set is X, with trivial action of G.
- $\phi_*\colon G\,\mathbf{Sets} \to \mathbf{Sets},\ X \mapsto X^G$ takes a G-set X to its set of points fixed under the action of G.
- $\psi_!\colon \mathbf{Sets} \to G\,\mathbf{Sets},\ X \mapsto G \times X$ takes a set X to the "free G-set with basis X", that is, the G-set whose underlying set is $G \times X$ with trivial action on the X component and (left) translation action on G.
- $\psi^*\colon G\,\mathbf{Sets} \to \mathbf{Sets},\ X \mapsto X$ takes a G-set X to the underlying set.
- $\psi_*\colon \mathbf{Sets} \to G\,\mathbf{Sets},\ X \mapsto \mathrm{Hom}(G, X)$ takes a set X to the ("cofree") G-set whose underlying set is that of maps (of sets) from G to X and whose G-action is given by $(g \cdot \delta)\colon h \mapsto \delta(hg)$ for $g \in G$ and $\delta \in \mathrm{Hom}(G, X)$.

We have some adjunction relations between these functors: namely, $\phi_! \dashv \phi^* \dashv \phi_*$ and $\psi_! \dashv \psi^* \dashv \psi_*$; of course, composing them, we get some further adjunctions $\phi^*\phi_! \dashv \phi^*\phi_*$ and $\psi_!\phi_! \dashv \phi^*\psi^*$ and $\psi_!\psi^* \dashv \psi_*\psi^*$ (plus the trivial adjunction on the identity functor on $\mathbf{Sets}$, and the usual $G \times \text{—} \dashv \mathrm{Hom}(G, \text{—})$ in $\mathbf{Sets}$).

Note that:

- $\phi_!$ is neither full nor faithful. It preserves all colimits because it has a right adjoint (in particular, it is right exact, that is, it preserves finite colimits). However, $\phi_!$ does not preserve limits: in fact, it does not even preserve binary products.
- ϕ^* is full and faithful. It preserves all limits and colimits because it has both left and right adjoints.
- ϕ_* is neither full nor faithful (note that it superficially *seems* to be full, but in fact $\mathrm{Hom}_{G\,\mathbf{Sets}}(G, \varnothing)$ is empty whereas $\mathrm{Hom}_{\mathbf{Sets}}(\phi_*G, \phi_*\varnothing) = \mathrm{Hom}_{\mathbf{Sets}(\varnothing,\varnothing)}$ is not, if G has the action by (left) translation on itself). It preserves all limits because it has a left adjoint (in particular, it is left exact, that is, it preserves finite limits). Further, ϕ_* does preserve coproducts; however, it does not preserve (even finite) coequalizers (hence not all finite limits).
- $\psi_!$ is faithful but not full. It preserves all colimits because it has a right adjoint (in particular, it is right exact, that is, it preserves finite colimits). However, $\psi_!$ does not preserve limits: in fact, it does not even preserve binary products.
- ψ^* is full and faithful. It preserves all limits and colimits because it has both left and right adjoints.
- ψ_* is faithful but not full. It preserves all limits because it has a left adjoint (in particular, it is left exact, that is, it preserves finite limits). However, ϕ_* does preserve colimits: in fact, it does not even preserve binary coproducts.

(In the language of topoi, the pairs (ϕ^*, ϕ_*) and (ψ^*, ψ_*) (of adjoint functors, where the left one is left exact) mean that we have two *geometric morphisms*, $\phi\colon G\,\mathbf{Sets} \to \mathbf{Sets}$ and $\psi\colon \mathbf{Sets} \to G\,\mathbf{Sets}$, both of which are *surjections*, which means that the inverse image functors (ϕ^*, ψ^*) are faithful.)

Concerning the non trivial units and coünits of the adjunctions, we have:

- $\eta'_\phi\colon 1_{G\,\mathbf{Sets}} \to \phi^*\phi_!$, the unit of $\phi_! \dashv \phi^*$, maps a G-set X to its set of orbits X/G with trivial action of G through the canonical surjection.
- $\epsilon_\phi\colon \phi^*\phi_* \to 1_{G\,\mathbf{Sets}}$, the coünit of $\phi^* \dashv \phi_*$, includes the set of fixed points of a G-set X in X.
- $\eta'_\psi\colon 1_{\mathbf{Sets}} \to \psi^*\psi_!$, the unit of $\psi_! \dashv \psi^*$, maps a set X to the set $G \times X$ by sending x to $(1, x)$.
- $\epsilon_\psi\colon \psi^*\psi_* \to 1_{\mathbf{Sets}}$, the coünit of $\psi^* \dashv \psi_*$, sends $\mathrm{Hom}(G, X)$ to X by applying on $1 \in G$.

We now pause for a moment to speak of monads and comonads in the next note.

2002-03-12:035

"Recall" that a *monad* on a category $\mathbf{C}$ is a triple (T, η, μ), where $T\colon \mathbf{C} \to \mathbf{C}$ is an endofunctor, and $\eta\colon 1 \to T$ and $\mu\colon T^2 \to T$ are natural transformations satisfying (i) $\mu \circ \eta_T = 1_T = \mu \circ (T\eta)$ and (ii) $\mu \circ \mu_T = \mu \circ (T\mu)$.

Dually, a *comonad* is a triple (V, ϵ, ν), where $V\colon \mathbf{C} \to \mathbf{C}$ is an endofunctor, and $\epsilon\colon V \to 1$ and $\nu\colon V \to V^2$ are natural transformations satisfying (i) $\epsilon_V \circ \nu = 1_V = (V\epsilon) \circ \nu$ and (ii) $\nu_V \circ \nu = (V\nu) \circ \nu$.

Every pair of adjoint functors $F \dashv U$ (with, say, $F\colon \mathbf{A} \to \mathbf{B}$ and $U\colon \mathbf{B} \to \mathbf{A}$), determines a monad (UF, η, μ) on $\mathbf{A}$, where $\eta\colon 1_{\mathbf{A}} \to UF$ is the unit of the adjunction, and $\mu\colon UFUF \to UF$ is given by $U\epsilon_F$ (where ϵ is the coünit). Dually, the same pair $F \dashv U$ determines a comonad (FU, ϵ, ν) on $\mathbf{B}$, where $\epsilon\colon FU \to 1_{\mathbf{B}}$ is the coünit of the adjunction, and $\nu\colon FU \to FUFU$ is $F\eta_U$.

"Recall" further that an *algebra* on a monad (T, η, μ) (on a category $\mathbf{C}$) is a morphism $\lambda\colon TA \to A$, with A an object of $\mathbf{C}$, such that (i) $\lambda \circ \eta_A = 1_A$ and (ii) $\lambda \circ \mu_A = \lambda \circ (T\lambda)$. Algebras on a monad (T, η, μ) form a category where morphisms from $\lambda\colon TA \to A$ to $\lambda'\colon TA' \to A'$ are morphisms $\alpha\colon A \to A'$ (in $\mathbf{C}$) such that $\lambda' \circ (T\alpha) = \alpha \circ \lambda$: this category is called the *Eilenberg-Moore category* of the monad, $\mathbf{C}^T$.

Given a monad (T, η, μ) on a category $\mathbf{C}$, and $\mathbf{C}^T$ its Eilenberg-Moore category, we have two important functors: $U\colon \mathbf{C}^T \to \mathbf{C}$ which takes an algebra $\lambda\colon TA \to A$ to the object A of $\mathbf{C}$, and $F\colon \mathbf{C} \to \mathbf{C}^T$ which takes an object A of $\mathbf{C}$ to the "free algebra" $\mu_A\colon T^2A \to A$; these functors are adjoint $F \dashv U$ and we have $UF = T$ with unit η and with $\mu = U\epsilon_F$ where ϵ is the coünit. (But note that if T is given from a functor adjunction, we may not find the functors we started with: the Eilenberg-Moore category of a monad is only one possible resolution of the monad as a pair of adjoint functors, universal in a certain sense, whereas the Kleisli category is coüniversal. A functor U of the form—up to an equivalence of categories— of the forgetful functor from an Eilenberg-Moore category is said to be *monadic*; this implies that it has a left adjoint.)

Dually, given a comonad (V, ϵ, ν), we have the notion of a *coälgebra*, which is a morphism $\gamma\colon A \to VA$ such that (i) $\epsilon_A \circ \gamma = 1_A$ and (ii) $\nu_A \circ \gamma = (V\gamma) \circ \gamma$. Coälgebras on a comonad (V, ϵ, ν) also form a category with the obvious morphisms, the Eilenberg-Moore category $\mathbf{C}^V$ of the comonad. And again, the forgetful functor $U\colon \mathbf{C}^V \to \mathbf{C}$ and the "cofree coälgebra" functor $H\colon \mathbf{C} \to \mathbf{C}^V$ are adjoint in the sense $U \dashv H$, with $UH = V$, with coünit ϵ and with $\nu = U\eta_H$ where η is the unit.

If (T, η, μ) is a monad (on a category $\mathbf{C}$), and the functor T has a right adjoint V, then the natural transformations $\epsilon\colon V \to 1$ and $\nu\colon V \to V^2$ deduced from $\eta\colon 1 \to T$ and $\mu\colon T^2 \to T$ by adjunction (and Yoneda — this could use some more explaining) make (V, ϵ, ν) into a comonad. Furthermore, the (Eilenberg-Moore) categories of T-algebras and V-coälgebras are isomorphic, in a way that commutes with the forgetful functor, by sending a T-algebra $\lambda\colon TA \to A$ to the coälgebra $\gamma\colon A \to VA$ deduced by adjunction. And the forgetful functor $U\colon \mathbf{C}^T \cong \mathbf{C}^V \to \mathbf{C}$ has a both a left adjoint (the "free (co)algebra" functor $F\colon \mathbf{C} \to \mathbf{C}^T$) and a right adjoint (the "cofree (co)algebra" functor $H\colon \mathbf{C} \to \mathbf{C}^V$).

Some examples: if U is the forgetful functor from the category of groups to the category of sets, it has a left adjoint F (the free group functor), and the monad $T = UF$ takes a set to the set of elements of the free group with that basis, whereas η selects the basis elements, and μ performs a "removing of quotes"; a (T, η, μ)-algebra is simply a group, that is, the forgetful functor U we started with is monadic. (Indeed, in sufficiently abstract terms, an "algebraic structure" is a monadic functor from a category to the category of sets...)

We can also take U to be the inclusion functor from the category of abelian groups to the category of groups: it has a left adjoint F, which takes a group G to its abelianization G/DG (where DG is the derived group, i.e. the (normal) subgroup generated by commutators) seen as an abelian group. Then the monad $T = UF$ takes G to G/DG (this time seen as a not necessarily abelian group which happens to be abelian), the unit η is the canonical surjection $G \twoheadrightarrow G/DG$ and μ is the identity. A (T, η, μ)-algebra is a group G together with a morphism $G/DG \to G$ which, when composed *on the right* with the canonical surjection gives the identity on G: but there is no other way for that than for G to be abelian. So U again is monadic.

The example of G-sets (see **2002-03-12:034**) illustrates the situation where we have an adjoint monad and comonad: the forgetful functor ψ^* taking a G-set to its underlying set has both a left adjoint, the "free G-set functor" $\psi_!$ which takes a set X to $G \times X$ and a right adjoint, the "cofree G-set functor" ψ_* which takes a set X to $\mathrm{Hom}(G, X)$. So the monad $\psi^*\psi_!$ is left adjoint to the comonad $\psi^*\psi_*$, and $\psi^*\psi_!$-algebras are the same thing as $\psi^*\psi_!$-coälgebras; and it turns out that both are the same thing as G-sets, so ψ^* is both monadic and comonadic.

If X is a topological space, let Δ be the functor taking a set to the sheaf of locally constant functions in that

set, and let Γ be the functor taking a sheaf on X to its set of global sections: we have an adjunction $\Delta \dashv \Gamma$. The coünit ϵ on a sheaf $\mathcal{F}$ is the map of sheaves $\Delta\Gamma\mathcal{F} \to \mathcal{F}$ which embeds locally constant sections in all sections, and $\nu\colon \Delta\Gamma\mathcal{F} \to \Delta\Gamma\Delta\Gamma\mathcal{F}$ is the identity. A coälgebra is a sheaf $\mathcal{F}$ on X together with a map $\gamma\colon \mathcal{F} \to \Delta\Gamma\mathcal{F}$ which composed (on the *left*) with $\varepsilon_{\mathcal{F}}\colon \Delta\Gamma\mathcal{F} \to \mathcal{F}$ gives the identity, in other words it is (isomorphic to) a constant sheaf (a sheaf in the image of Δ). So the functor Δ is comonadic.

Slogan: monads are important, because many interesting categories can be realized as Eilenberg-Moore categories of monads; comonads are important because, if $\mathcal{T}$ is a topos, and (V, ϵ, ν) is a comonad on $\mathcal{T}$ such that V is left-exact (which is the case in particular when V has a right adjoint, which is then a monad as we have seen) then the Eilenberg-Moore category of coälgebras on V is itself a topos (and, furthermore, this construction and that of sheaves on a Lawvere-Tierney topology, see **2002-03-11:033** and **2002-12-05:051**, are "essentially the only possible constructions of topoi", in the intriguing sense that every geometric morphism factors essentially uniquely and up to isomorphism as a composition of the two).

2002-03-16:036

(**Updated 2002-03-17**, to reformulate over an arbitrary base ring k, and to add the word "reduced" here or there. Thanks to Joël Riou and Olivier Wittenberg for various remarks and explanations.)

In notes **2002-01-03:023** through **2002-01-11:027** I considerered the question of constructing, for a given ring A, a (reduced?) zero-dimensional ring K_A (i.e. every prime ideal of K_A is maximal) that would serve as a "zero-dimensional skeleton" of A (probably the universal morphism from A to a (reduced?) zero-dimensional ring) or something of the kind.

Let k be a (commutative) ring and $\mathbf{AffScm}_k$ be the category of affine k-schemes (opposite to the category of (commutative) k-algebras). Define a topology on $\mathbf{AffScm}_k$ by declaring a family of arrows $\operatorname{Spec} B_i \to \operatorname{Spec} A$ to be covering iff every prime ideal $\mathfrak{p} \in \operatorname{Spec} A$ of A is the (inverse) image of some prime ideal $\mathfrak{q} \in \operatorname{Spec} B_i$ of some B_i (by the arrow $\operatorname{Spec} B_i \to \operatorname{Spec} A$, i.e. $A \to B_i$). (Sanity check: does this, indeed, constitute a Grothendieck topology—see, e.g., **2002-03-11:033** for a definition?)

It *appears* that this topology coincides with the $\neg\neg$ topology (topology in the sense of Lawvere & Tierney) on the Zariski topos. Is this correct?

Clearly, not every representable presheaf on $\mathbf{AffScm}_k$ is a sheaf for the topology we have defined. E.g., $\operatorname{Spec} k[t]$ is not a sheaf, for the morphism $\operatorname{Spec} k \uplus \operatorname{Spec} k[u^{\pm 1}] \to \operatorname{Spec} k[u]$ (where $\operatorname{Spec} k$ maps to the origin of $\operatorname{Spec} k[u]$ and $\operatorname{Spec} k[u^{\pm 1}]$ maps as the complement of the origin) is covering, but it does not descend sections of $\operatorname{Spec} k[t]$. Is this topology indeed *strictly finer* (i.e. having strictly more covers than) the canonical topology on $\mathbf{AffScm}_k$?

It vaguely seems that (the presheaf represented by) an affine scheme $\operatorname{Spec} A$ is a sheaf (for the topology in question) iff the k-algebra A is reduced and zero-dimensional: is this true (at least if k is an algebraically closed field, or giving some definition of zero-dimension like "having zero-dimensional geometrical fibers")? (Incidentally, is it true that if $A \to B$ is a morphism of (commutative) k-algebras, with A reduced and zero-dimensional, not necessarily noetherian, then it (the morphism) is flat?) If so, is it true that the associated sheaf (sheafification) of a representable presheaf is again representable? In that case we can write it $\operatorname{Spec} K_A$ and call it the zero-dimensional skeleton of $\operatorname{Spec} A$.

2002-03-17:037

(This expands **2002-03-16:036**.)

Let k be a (commutative) ring, and $\mathbf{AffScm}_k$ the category of affine k-schemes (opposite to the category of (commutative) k-algebras). Recall that a morphism $\operatorname{Spec} B \to \operatorname{Spec} A$ is said to be *surjective* iff for every prime ideal $\mathfrak{p}$ of A there exists a prime ideal $\mathfrak{q}$ of B such that $\mathfrak{p}$ is the inverse image of $\mathfrak{q}$ by the map of rings $A \to B$; equivalently, it means that for every field K and every morphism $\operatorname{Spec} K \to \operatorname{Spec} A$ there exists a field extension L of K and a morphism $\operatorname{Spec} L \to \operatorname{Spec} B$ so that the obvious diagram commutes (EGA, I.3.5.3); surjective morphisms are stable under base change (*id*, I.3.5.2). Say that a family $\operatorname{Spec} B_i \to \operatorname{Spec} A$ of morphisms (in $\mathbf{AffScm}_k$) is surjective iff $\operatorname{Spec} \prod_i B_i \to \operatorname{Spec} A$ is surjective (note: this is equivalent to the map of schemes $\biguplus_i \operatorname{Spec} B_i \to \operatorname{Spec} A$ being

surjective—making use, of course, of the fact that the target $\mathrm{Spec}\, A$ is affine). We can define a topology on $\mathbf{AffScm}_k$ by saying that $S \in J(\mathrm{Spec}\, A)$ (a sieve S covers its target $\mathrm{Spec}\, A$) iff the family S of morphisms (with target $\mathrm{Spec}\, A$) is surjective: call this the surjective topology on $\mathbf{AffScm}_k$. Joël Riou notes that it might be of use to add some hypothesis such as "(locally?) of finite presentation", but let us try to do without (the essential idea being that a morphism $\mathrm{Spec}\, B \to \mathrm{Spec}\, A$ between affine k-schemes is, in any case, affine, and therefore quasi-compact).

We wonder for which k-algebras T the representable presheaf $\mathrm{Spec}\, T\colon \mathbf{AffScm}_k \to \mathbf{Sets},\ \mathrm{Spec}\, A \mapsto \mathrm{Hom}(T, A)$ is a sheaf for the surjective topology.

Suppose that A is such a k-algebra, that (the presheaf represented by) $\mathrm{Spec}\, A$ is a sheaf, and let $x \in A$. We consider $B = A \otimes_k A$ and the two morphisms $\varphi_1, \varphi_2\colon A \rightrightarrows B$ such that $\varphi_1(t) = t \otimes 1$ and $\varphi_2(t) = 1 \otimes t$. We let $B_1 = B/(x \otimes 1)$ be the quotient of B by the ideal generated by $x \otimes 1 = \varphi_1(x)$, and we let $B_2 = B_{(x\otimes 1)} = A_{(x)} \otimes_k A$ be the quotient ring making $x \otimes 1$ invertible in B; call $\iota\colon B \times B_1 \times B_2$ the canonical map (canonical surjection ι_1 on one component, canonical map ι_2 on the other). It is easy to see that $\mathrm{Spec}\, B_1 \uplus \mathrm{Spec}\, B_2 \to \mathrm{Spec}\, B$ (the map of affine schemes associated to ι) is surjective. By the hypothesis on A (and because $B_1 \otimes_B B_2 = 0$), every map $A \to B_1 \times B_2$ must factor through ι. Consider in particular the map $\psi\colon A \to B_1 \times B_2$ given by $\psi(t) = (\iota_1(\varphi_1(t)), \iota_2(\varphi_2(t)))$: there must exist $\tilde{\psi}\colon A \to B$ such that $\psi = \iota \circ \tilde{\psi}$. Now $\psi(x) = (0, 1 \otimes x)$. So $\tilde{\psi}(x)$ must be in the ideal generated by $x \otimes 1$, say $\tilde{\psi}(x) = z(x \otimes 1)$ with $z \in B$, and we have $z(x \otimes 1) = 1 \otimes x$ in $B_2 = B_{(x\otimes 1)}$. Therefore, there exists $z \in B = A \otimes_k A$ which goes to $x^{-1} \otimes x \in B_{(x\otimes 1)} = A_{(x)} \otimes_k A$.

So, question: what does it tell us on an element x of a k-algebra A that $x^{-1} \otimes x \in A_{(x)} \otimes_k A$ belongs to the image of $A \otimes_k A$? What does it tell us on a k-algebra A that every element x satisfies that property?

A simpler question: what does it tell us on an element x of a k-algebra A that $x^{-1} \in A_{(x)}$ belongs to the image of A? What does it tell us an a k-algebra A that every element satisfies that property? Here we can probably answer that: the image of A in $A_{(x)}$ contains x^{-1} iff it contains everything, i.e. iff the map $A \to A_{(x)}$ is surjective, which means that the open set $\mathrm{Spec}\, A_{(x)} \rightarrowtail \mathrm{Spec}\, A$ is closed, and then A is the product of two rings and x is equal to a nilpotent plus the product of an invertible element by an idempotent; and conversely. And very probably if this is true of every x then A is zero-dimensional (compare **2002-01-07:024**).

At least if k is a field and A an integral domain, we can probably answer the more complicated question: for $A \otimes_k A$ injects in $A_{(x)} \otimes_k A$ (as soon as x is not zero) by the canonical map, and the condition implies that x is invertible; so if it holds for every x, we see that A is a field.

2002-03-18:038

We resolve the question asked in **2002-01-07:024**.

For any ring A, we have mentioned in **2001-12-30:022** that the boolean algebra $\mathrm{Hom}(\mathbb{Z}^2, A)$ of idempotents of A is isomorphic by $e \mapsto D(e)$ to the boolean algebra of clopen subsets of $\mathrm{Spec}\, A$. Indeed, it is quite clear that if e is idempotent then $D(e)$ is clopen; on the other hand, if U is a clopen subset of $\mathrm{Spec}\, A$, then (i) its structure as an open subscheme is the same as its (thickest!) structure as a closed subscheme, and (ii) it is therefore an affine open subscheme and so is its complement, at which point it is easy to see that A is the product of two rings and gives rise to two complementary idempotents, etc.

On the other hand, if A is a reduced zero-dimensional ring, then for any prime ideal $\mathfrak{m} \in \mathrm{Spec}\, A$ of A ($\mathfrak{m}$ is maximal, by hypothesis), the localization $A_\mathfrak{m}$ of A at $\mathfrak{m}$ is a reduced zero-dimensional local ring, *thus* a field (because it has a unique prime ideal, which is necessarily 0 because the ring is reduced). So the canonical map $A_\mathfrak{m} \to A/\mathfrak{m}$ is an isomorphism. In particular, if $f \in \mathfrak{m}$, it goes to 0 in $A_\mathfrak{m}$, so there exists an element, say, $g \notin \mathfrak{m}$, such that $fg = 0$; and then $\mathfrak{m} \in D(g) \subseteq V(f)$. This shows that $V(f) \subseteq \mathrm{Spec}\, A$ is open for any $f \in A$ (and it is also closed by the very definition of being closed).

The two preceding paragraphs mean that if A is a reduced zero-dimensional ring, for any $f \in A$ we can define an idempotent e with $D(e) = V(f)$; and then $f + e$ is invertible in A (because it belongs to no maximal ideal) and $fe = 0$; so $f = (f + e)(1 - e)$ is the product of an invertible $f + e$ by an idempotent $1 - e$.

Together with what was already proven in **2002-01-07:024**, we can therefore state that a ring is reduced zero-dimensional *iff* every element is the product of an invertible by an idempotent.

2002-03-24:039

("Tao of Topoi in Algebraic Geometry.")

Let k be any (commutative) ring. Let $\mathbf{AffScm}_k$ be the category of affine k-schemes (opposite to the category of (commutative) k-algebras). We can define several important Grothendieck topologies on $\mathbf{AffScm}_k$:

- The Zariski topology. We say that a k-algebra A is covered by localizations $A_{(f_1)}, \ldots, A_{(f_n)}$ of A (where $A_{(f_i)}$ is obtained by inverting f_i in A) iff the elements $f_1, \ldots, f_n$ of A generate the unit ideal. More generally, we say that A is covered by an A-algebra B for the Zariski topology iff there exist elements f_i of A generating the unit ideal and such that the sum $A \to \bigoplus_i A_{(f_i)}$ of the localization maps factors as $A \to B \to \bigoplus_i A_{(f_i)}$ where $A \to B$ is the given map; and we say that A is covered by A-algebras $(B_j)_{j \in J}$ (not necessarily in finite number, although a finite subset will always suffice) for the Zariski topology iff it is covered by $\bigoplus_j B_j$.
- The étale topology. We say that an A-algebra B is faithfully étale iff the map $A \to B$ is finitely presented (that is, B is the quotient of some $A[t_1, \ldots, t_n]$ by a finitely generated ideal of it), formally étale (that is, for any A-algebra C and ideal I of C such that $I^2 = 0$, the canonical map from $\mathrm{Hom}_A(B, C)$ to $\mathrm{Hom}_A(B, C/I)$ is bijective) and faithfully flat ("flat" is automatic by étaleness, so we are just stating that for any non-zero A-module M, the B-module $M \otimes_A B$ is non-zero; and actually it suffices to check this if M is an integral domain quotient of A). And we say that a k-algebra A is covered by an A-algebra B (resp. by A-algebras $(B_j)_{j \in J}$, where, again, a finite number will actually suffice) for the étale topology iff there exists $B \to B'$ such that the composite $A \to B \to B'$ is faithfully étale (resp. iff A is covered by $\bigoplus_j B_j$ in that sense).
- The fppf (faithfully flat and finitely presented) topology. We say that a an A-algebra B is fppf iff B is finitely presented and faithfully flat over A (i.e. for every injective homomorphism of A-modules $M' \to M$ the homomorphism $M' \otimes_A B \to M \otimes_A B$ obtained by tensoring with B over A is still injective). And we say that a k-algebra A is covered by an A-algebra B (resp. by A-algebras $(B_j)_{j \in J}$, where, again, a finite number will actually suffice) for the fppf topology iff there exists $B \to B'$ such that the composite $A \to B \to B'$ is fppf (resp. iff A is covered by $\bigoplus_j B_j$ in that sense).
- The fp[qc] (faithfully flat [and quasi-compact—but in the case of affine schemes the latter is automatic]). We say that a k-algebra A is covered by an A-algebra B (resp. by A-algebras $(B_j)_{j \in J}$, where, again, a finite number will actually suffice) for the fp[qc] topology iff B is ("fp[qc]") faithfully flat as an A-algebra (resp. iff A is covered by $\bigoplus_j B_j$ in that sense).

(Of course, the above is formulated with k-algebras by abuse of language and we should reverse all arrows to get definitions on $\mathbf{AffScm}_k$.)

For example, the map from $\mathbb{A}^2_k = \mathrm{Spec}\, k[x, y]$ to $\mathbb{A}^1_k = \mathrm{Spec}\, k[x]$ obtained by injecting $k[x]$ in $k[x, y]$, is faithfully flat and finitely presented, so it is covering for the fpqc and fppf topologies. It is certainly not étale, but it is still covering for the étale topology (the whole point of this example, indeed) because it has a section; indeed, the fact that it has a section shows that it is covering for *any* Grothendieck topology.

A *presheaf* (of sets on the category of affine schemes) $\mathcal{F}$ is a contravariant functor from $\mathbf{AffScm}_k$ to $\mathbf{Sets}$ (which can be, equivalently, considered as a covariant functor from k-algebras to sets); it is a *sheaf* for one of the above-defined topologies iff for every covering of a k-algebra A by A-algebras $(B_j)_{j \in J}$ (for the topology in question) the diagram of sets $\mathcal{F}(A) \to \prod_j \mathcal{F}(B_j) \rightrightarrows \prod_{j,j'} \mathcal{F}(B_j \otimes_A B_{j'})$, with the obvious maps, is exact (i.e. the first arrow is injective and its image is the set of points where the two latter coincide).

(...to be continued...)

2002-03-31:040

(Many thanks to Joël Bellaïche and Yves de Cornulier for various results in this note.)

Let X be any set. If A is a (commutative) ring, we write $A^{(X)} = \bigoplus_{x \in X} A$ the sum of $\mathrm{card}(X)$ copies of A *as an A-module*, and $A^X = \prod_{x \in X} A$ the product of $\mathrm{card}(X)$ copies of A (ditto), which contains $A^{(X)}$ and is also its dual $(A^{(X)})^*$. We have a short exact sequence $0 \to A^{(X)} \to A^X \to A^X/A^{(X)} \to 0$ of A-modules. This gives us a sequence $0 \to (A^X/A^{(X)})^* \to (A^X)^* \to A^X \to \mathrm{Ext}^1(A^X/A^{(X)}, A) \to \mathrm{Ext}^1(A^X, A) \to 0$ (the next term would be $\mathrm{Ext}^1(A^{(X)}, A)$, but this vanishes as $A^{(X)}$ is free by definition). Further note that the duality $A^{(X)} \times (A^{(X)})^* \to A$,

which is nondegenerate on the left, when read as $A^{(X)} \times A^X \to A$, implies that $A^{(X)}$ injects in $(A^X)^*$ in a way that is right inverse to the arrow $(A^X)^* \to A^X$ defined above; so the image of $(A^X)^*$ in A^X by the latter arrow contains, at least, $A^{(X)}$.

Fact: if $A = \mathbb{Z}$ is the ring of integers, then the image of $(\mathbb{Z}^X)^* \to \mathbb{Z}^X$ is precisely $\mathbb{Z}^{(X)}$, which we have just seen it must contain. In other words, and expliciting the arrow $(\mathbb{Z}^X)^* \to \mathbb{Z}^X$, we must prove that if ℓ is a linear form on $\mathbb{Z}^X$, and δ_x (for $x \in X$) the element of $\mathbb{Z}^X$ defined by $\delta_x(x) = 1$ and $\delta_x(y) = 0$ if $y \neq x$, then there are only finitely many $x \in X$ such that $\ell(\delta_x) \neq 0$. Assume on the contrary that there are infinitely many such x. Then we might as well assume that $X = \mathbb{N}$ and that $c_i \neq 0$ for each $i \in \mathbb{N}$, where $c_i = \ell(\delta_i)$; in fact, we might as well assume that $c_i > 0$ for each i. Now, for each $i \in \mathbb{N}$, let $b_i \in \mathbb{N}$ be such that $2^{b_i} > 2c_i$, and consider the element $u \in \mathbb{Z}^{\mathbb{N}}$ given by the sequence $(1, 2^{b_0}, 2^{b_0+b_1}, 2^{b_0+b_1+b_2}, \ldots)$. Now since $u - \delta_0$ is divisible by 2^{b_0}, the integer $\ell(u) - c_0$ must also be divisble by 2^{b_0}, or, in other terms, $\ell(u)$ has the same b_0 low-order bits as c_0. Similarly, $\ell(u) - (c_0 + c_1 2^{b_0})$ is divisible by $2^{b_0+b_1}$, so the next b_1 low-order bits of $\ell(u)$ are the b_1 low-order bits of c_1. And so on. If $\ell(u) \geq 0$, we have finished, because all bits are 0 after a certain rank, so all c_i are zero for i sufficiently large. If $\ell(u) < 0$ then all bits are 1 after a certain rank, so $c_i \geq 2^{b_i - 1}$ for i sufficiently large—but we have assumed the contrary, viz. $2^{b_i} > 2c_i$. This completes the proof.

The same statement definitely does *not* hold over an arbitrary ring A. In fact, if $A = k$ is a field, then the map $(k^X)^* \to k^X$ is clearly always surjective. The proof appears to work with the following hypothesis on A: there exists an element $p \in A$ (namely 2 in the above proof) such that multiplication by p is injective (i.e. p is "regular") and such that $\bigcap_{b \in \mathbb{N}} p^b A = 0$; the arguments with inequalities are probably red herrings, but this requires a little more thought.

If there exists a non principal $\mathrm{card}(A)^+$-complete ultrafilter $\mathscr{U}$ on X, in other words if there exists a measurable cardinal κ such that $\mathrm{card}(A) < \kappa \leq \mathrm{card}(X)$, then $(A^X/A^{(X)})^*$ is not zero. Indeed, if $u \in A^X$, since the union of all the $u^{-1}(a)$, for a ranging over A, is X (and therefore belongs to $\mathscr{U}$), by $\mathrm{card}(A)^+$-completeness, there exists $a \in A$ such that $u^{-1}(a) \in \mathscr{U}$, and this a is necessarily unique since for $a \neq a'$ the sets $u^{-1}(a)$ and $u^{-1}(a')$ are disjoint (so they cannot both be in the ultrafilter): call such a the *limit* of u along $\mathscr{U}$. Taking the limit is manifestly an A-linear map, and, since $\mathscr{U}$ is non principal, depends only on the class of u in $A^X/A^{(X)}$. So $\mathscr{U}$ defines a non-zero element of $(A^X/A^{(X)})^*$ (non-zero because the diagonal map $A \to A^X/A^{(X)}$ is a section of it: that is, the limit of a constant function is that constant value).

Fact: if $A = \mathbb{Z}$ is the ring of integers, then $(\mathbb{Z}^{\mathbb{N}}/\mathbb{Z}^{(\mathbb{N})})^* = 0$. Indeed, assume on the contrary that there exists a linear form ℓ on $\mathbb{Z}^{\mathbb{N}}$ that vanishes on $\mathbb{Z}^{(\mathbb{N})}$. Say that an element u of $\mathbb{Z}^{\mathbb{N}}$ is 2^N-*divisible* iff $2^n | u(n)$ for every $n \in \mathbb{N}$; we then have $\ell(u) = 0$ because the value of ℓ on u is the same as that on the sequence obtained by replacing the first values N of u by zeroes (for any N), which must then be divisible by 2^N—for any N—and this is possible only if $\ell(u) = 0$. But similarly, $\ell(u) = 0$ if u is 3^N-divisible, with the obvious meaning. However, any element of $\mathbb{Z}^{\mathbb{N}}$ can be written as the sum of a 2^N-divisible element and a 3^N-divisible one, using a Bézout relation between 2^n and 3^n. So $\ell(u) = 0$ for any $u \in \mathbb{Z}^{\mathbb{N}}$, which was to be proven.

Again, the statement definitely does *not* generalize to an arbitrary ring A, because if $A = k$ is a field the vector space $k^{\mathbb{N}}/k^{(\mathbb{N})}$ is non trivial, so its dual also is. The proof appears to work with the following hypothesis on A: there exists an element $p \in A$ (namely 2 in the above proof) such that multiplication by p is injective (i.e. p is "regular") and such that $\bigcap_{b \in \mathbb{N}} p^b A = 0$, and an element $q \in A$ (namely 3 in the above proof) verifying the same hypotheses, and such that p and q generate the unit ideal of A.

If the ring A satisfies the hypothesis that $(A^{\mathbb{N}})^* = A^{(\mathbb{N})}$ (that is, the image of $(A^{\mathbb{N}})^*$ in $A^{\mathbb{N}}$ is inside $A^{(\mathbb{N})}$ *and* $(A^{\mathbb{N}}/A^{(\mathbb{N})})^* = 0$), then it satisfies $(A^X/A^{(X)})^* = 0$ for any set X of cardinality less than the first measurable cardinal (resp. any set if measurable cardinals do not exist). Indeed, assume ℓ is a linear form on A^X that vanishes on $A^{(X)}$. Consider the set $\mathscr{U}$ of subsets $U \subseteq X$ of X such that ℓ is identically zero on $A^{X \setminus U}$ (considered as a subset of A^X by extending with zeroes on U). It is clear that $\mathscr{U}$ is a filter on X. It is not always true that it is a ultrafilter (think $\ell = \lim_{\mathscr{U}_1} + \lim_{\mathscr{U}_2}$ with $\mathscr{U}_1, \mathscr{U}_2$ two σ-complete non principal ultrafilters on X), but it is always true that there exists $Y \subseteq X$, with $(X \setminus Y) \notin \mathscr{U}$, such that the restriction $\mathscr{U}|_Y$ of $\mathscr{U}$ to Y is a ultrafilter, where the "restriction" in question is as follows: it is the set of $U \subseteq Y$ such that $U \cup (X \setminus Y) \in \mathscr{U}$ (things are much more natural in terms of ideals than in terms of filters, but tradition demands filters). For if it were otherwise, we could write $X = U_0 \cup U_0'$ with

$U_0, U_0' \notin \mathscr{U}$ and $U_0 \cap U_0' = \varnothing$, and then considering $\mathscr{U}|_{U_0'}$ we could write $U_0' = U_1 \cup U_1'$ with $U_1, U_1' \notin \mathscr{U}|_{U_0'}$ and $U_1 \cap U_1' = \varnothing$, and so on. This implies that there are elements $u_0, u_1, u_2, \dots$ of A^X with come from $A^{U_0}, A^{U_1}, A^{U_2}, \dots$ respectively, and which satisfy $\ell(u_i) \neq 0$ for all i. But these can easily be used to construct an element of $(A^{\mathbb{N}})^*$ which does not come from $A^{(\mathbb{N})}$, something we assumed does not exist. So we can find Y as explained, and we might as well assume that $Y = X$ and therefore that $\mathscr{U}$ is a ultrafilter on X. It is non principal because ℓ vanishes on $A^{(X)}$. And it is σ-complete because otherwise we can find elements $u_0, u_1, u_2, \dots$ of A^X which come from $A^{F_0}, A^{F_1}, A^{F_2}, \dots$ with $F_0, F_1, F_2, \dots$ disjoint, such that $\ell(u_i) = 0$ for all i but the function u extending u_i on each F_i and 0 elsewhere satisfies $\ell(u) \neq 0$; and these data can be used to construct a non-zero element of $(A^{\mathbb{N}}/A^{(\mathbb{N})})^*$, something we assumed does not exist. So finally we have a σ-complete non principal ultrafilter $\mathscr{U}$ on X, and $\mathrm{card}(X) \geq \kappa$ for κ the smallest measurable cardinal.

There is much mystery in this whole matter. Note that we have two different conditions (on a ring A and a set X): first, that the image of $(A^X)^* \to A^X$ falls inside $A^{(X)}$ (call this the "finiteness writing condition"), in other words given $\ell \in (A^X)^*$, only finitely many of the $c_x = \ell(\delta_x)$ are non-zero; and second, that the map $(A^X)^* \to A^X$ in question is injective (call this the "uniqueness writing condition"), in other words the c_x above suffice to determine ℓ. The "uniqueness writing condition" can fail in the presence of measurable cardinals; the "finiteness writing condition" on the other hand requires very little on the ring A (and nothing at all on X). But, strangely, to prove that the "uniqueness writing condition" holds for small enough X we apparently need not only the condition in question for $X = \mathbb{N}$ (and for the given ring A) but also the "finiteness writing condition" for $X = \mathbb{N}$. We can wonder, for example, whether there actually exists a ring A such that the uniqueness writing condition holds for $X = \mathbb{N}$ but not for some larger X still smaller than the first measurable cardinal, or whether this apparent problem is just a weird artifact of our proof technique.

2002-04-06:041

The claim made in **2001-12-21:014** that, if K is any field and B a faithfully flat (i.e. non-zero) K-algebra, an element x of B such that $x \otimes 1 - 1 \otimes x \in B \otimes_K B$ is nilpotent necessarily comes from K, is *false*. Indeed, if K is a non perfect field, say of characteristic p, and $K^{p^{-\infty}}$ its perfect closure, then $K^{p^{-\infty}}$ is faithfully flat as a K-algebra, and for *every* $x \in K^{p^{-\infty}}$ the element $x \otimes 1 - 1 \otimes x \in K^{p^{-\infty}} \otimes_K K^{p^{-\infty}}$ is nilpotent. (And this is not a problem of the perfect closure being not of finite type over K, because a similar statement holds at finite levels.)

What is true, however, is that the elements obtained in this way are precisely the elements of the perfect closure of K; that is, if K is any field and B a faithfully flat K-algebra, an element x of B is such that $x \otimes 1 - 1 \otimes x \in B \otimes_K B$ is nilpotent iff x belongs to some purely inseparable algebraic extension field of K included in B. Indeed, the statement over algebraically closed fields was (it seems correctly) proved in **2001-12-21:014**, and the more general statement hold by Galois descent. I will try to give a clear and irreproachable proof later on.

But it certainly seems that the hopes of **2001-12-21:014** were hasty, and the question demandes more thought.

2002-05-02:042

Let $\Delta_s = \{(x_0, \dots, x_s) \in \mathbb{R}^{s+1} : x_0 \geq 0, \dots, x_s \geq 0, x_0 + \cdots + x_s = 1\}$ be the simplex of dimension s, and let μ be the measure on Δ_s given by $d\mu = s!\, dx_1 \wedge \cdots \wedge dx_s$. Then we have

$$\int_{\Delta_s} x_0^{k_0} \cdots x_s^{k_s}\, d\mu = \frac{k_0! \cdots k_s!\, s!}{(k_0 + \cdots + k_s + s)!}$$

In particular, $\mu(\Delta_s) = 1$ (we say that μ is the uniform probability measure on the simplex Δ_s).

Here is a sample application of this formula. Given $x = (x_0, \dots, x_s) \in \Delta_s$, we consider $\boldsymbol{\theta}$ a uniformly distributed random variable in $[0; 1]$ and we let $\boldsymbol{i}$ be the index such that $x_0 + \cdots + x_{\boldsymbol{i}-1} < \boldsymbol{\theta} < x_0 + \cdots + x_{\boldsymbol{i}}$ (for almost every value of $\boldsymbol{\theta}$ this is well-defined); in other words, $\boldsymbol{i} = 0$ with probability x_0, $\boldsymbol{i} = 1$ with probability x_1 and so on. We actually consider N independent variables $\boldsymbol{\theta}_1, \dots, \boldsymbol{\theta}_N$ and we let $\boldsymbol{M}_0, \dots, \boldsymbol{M}_s$ (with $\boldsymbol{M}_0 + \cdots + \boldsymbol{M}_s = N$) be the count of the corresponding $\boldsymbol{i}_1, \dots, \boldsymbol{i}_N$ which are equal to $0, \dots, s$ respectively. Let $\boldsymbol{y} = (\boldsymbol{y}_0, \dots, \boldsymbol{y}_s)$ be defined

as $(\boldsymbol{M}_0/N, \ldots, \boldsymbol{M}_s/N)$: for a given N, the random variable $\boldsymbol{y}$ is distributed over the grid of points of denominator (dividing) N in Δ_s with a probability law that follows the multinomial distribution, namely

$$\Pr\big((\boldsymbol{y}_0, \ldots, \boldsymbol{y}_s) = (M_0/N, \ldots, M_s/N)\big) = \frac{N!}{M_0! \cdots M_s!} x_0^{M_0} \cdots x_s^{M_s}$$

Note that $\mathsf{E}(\boldsymbol{y}) = x$ (expectation of $\boldsymbol{y}$), and $\mathsf{V}(\boldsymbol{y}_i) = x_i(1-x_i)/\sqrt{N}$ (variance of $\boldsymbol{y}_i$: each $\boldsymbol{y}_i$ is a binomial variable) and $\mathsf{Cov}(\boldsymbol{y}_i, \boldsymbol{y}_j) = -x_i x_j/\sqrt{N}$ (covariance of $\boldsymbol{y}_i$ and $\boldsymbol{y}_j$ for $i \neq j$).

Now let $\boldsymbol{x}$ be uniformly distributed on Δ_s (according to the law μ we have defined above), and define $\boldsymbol{y}$ in the same way as previously, for variables $\boldsymbol{\theta}_1, \ldots, \boldsymbol{\theta}_N$ independent of $\boldsymbol{x}$. In Bayesian way, fix $\boldsymbol{y} = (M_0/N, \ldots, M_s/N)$ and consider $\boldsymbol{x}$ as a random variable for this new conditioning: we have

$$\Pr\big((\boldsymbol{x}_0, \ldots, \boldsymbol{x}_s) = (x_0, \ldots, x_s)\big) = \frac{(N+s)!}{M_0! \cdots M_s!\, s!} x_0^{M_0} \cdots x_s^{M_s}$$

We then have, according to the integration formula given at the start, that $\mathsf{E}(\boldsymbol{x}_i) = (M_i+1)/(N+s+1)$ (add a fictitious 1 to every measure), and $\mathsf{V}(\boldsymbol{x}_i) = ((M_i+1)(N-M_i+s))/((N+s+1)^2(N+s+2))$ and $\mathsf{Cov}(\boldsymbol{x}_i, \boldsymbol{x}_j) = -((M_i+1)(M_j+1))/((N+s+1)^2(N+s+2))$.

2002-05-21:043

(This pursues some ideas from **2002-02-07:032**.)

If E is a partially ordered set, we let E^* be the set of finite antichains of E, i.e. finite subsets of E no two elements of which are comparable, and we partially order E^* by letting $\{u_1, \ldots, u_m\} \leq \{v_1, \ldots, v_n\}$ iff for every $j \in \{1, \ldots, n\}$ there exists $i \in \{1, \ldots, m\}$ with $u_i \leq v_j$. We embed E (as a partially ordered set) in E^* by sending u to $\{u\}$, and we shall identify E with its image *via* this embedding. The operation sending a finite tuple $(u_1, \ldots, u_m)$ of elements of E to its set of minimal elements, seen as an element of E^*, defines a map $E^m \to E^*$, which factors through the action of the symmetric group $\mathfrak{S}_m$ on E^m and for $m = 1$ gives the previously mentioned embedding $E \to E^*$; we write $u_1 \wedge \cdots \wedge u_m$ for the image of $(u_1, \ldots, u_m)$ by this map, and $\top$ for the image of the empty tuple (in other words, the empty set, seen as an element of E^*). Thus, every element of E^* can be written $u_1 \wedge \cdots \wedge u_m$ for some $u_1, \ldots, u_m \in E$, and this expression is unique if we impose the u_i to be pairwise incomparable, and we can always reduce to this form by removing non-minimal elements. Further, the $\wedge$ operation extends uniquely to a commutative and associative operation on E^*, having $\top$ as neutral element, which is simply taking the greatest lower bound of a finite set.

We pointed out in **2002-02-07:032** that E is fairly ordered (i.e. well-founded and without infinite antichains) iff E^* is well-founded. (Being well-founded means satsfying the DCC: every descending chain of elements is stationary.)

The surprise is that it is not always true in this case that E^* is fairly ordered: it may have infinite antichains. I thank Larry Hammick for raising the question and for pointing out that my initial reaction was wrong; the following counterexample can be found in Diane Maclagan, « Antichains of Monomial Ideals are Finite », *Proceedings of the AMS*, **129** (2001), no. 6, 1609–1615, also `math.CO/9909168` (see example 4.1), and was initially published in D. Duffus, M. Pouzet & I. Rival, « Complete ordered sets with no infinite antichains », *Discrete Math*, **35** (1981), 39–52.

Consider $E = \{(i,j) \in \mathbb{N}^2 : i < j\}$, and let define a partial order on E by $(i,j) \leq (i',j')$ iff either $i = i'$ and $j \leq j'$, or else $j < i'$; in other words, $(i,j) \leq (i',j')$ iff $j \leq j'$ and either $i = i'$ or $j < i'$; and $(i,j) < (i',j')$ iff $j < j'$ and either $i = i'$ or $j < i'$. Now E is well-founded, because in any strictly decreasing sequence of elements of E, the j coordinate must strictly decrease, which is impossible unless the sequence is finite. Furthermore, E has no infinite antichain, because if (i_0, j_0) belongs to an antichain, then every other element (i,j) of that antichain must satisfy $i \leq j_0$; but each of the finitely many possible values of i can be used by at most one element of the antichain (because two elements of E with the same i coordinate are comparable); so the antichain has at most $j_0 + 1$ elements. On the other hand, for $k > 0$, consider the elements $S_k = (0,k) \wedge \cdots \wedge (k-1,k)$ of E^* (note that the elements $(0,k)$

through $(k-1,k)$ of E are pairwise incomparable). If $k<\ell$ the we cannot have $S_k \leq S_\ell$ because (k,ℓ) is in S_ℓ but is not greater or equal to any element of S_k; and conversely, we cannot have $S_\ell \leq S_k$ because $(0,k)$ (or indeed any element of S_k) is in S_k but is not greater or equal to any element of S_ℓ. So the S_k for $k>0$ form an infinite antichain in E^*.

We therefore have an example of a partially ordered set E such that E^* is well-founded (i.e. E is fairly ordered) but E^{**} is not (i.e. E^* is not fairly ordered). This leads us to consider the following notions. Define $E^{*\alpha}$, where α ranges over the ordinals, as follows: let $E^{*0}=E$, and for $\alpha+1$ a successor, $E^{*(\alpha+1)}=(E^{*\alpha})^*$ (with the embedding of $E^{*\alpha}$ in it), and for δ a limit ordinal let $E^{*\delta}$ be the inductive limit of the $E^{*\alpha}$ for $\alpha<\delta$ with the embeddings we have defined. Define the *well-foundedness generation* of E to be the smallest γ such that $E^{*\gamma}$ is *not* well-founded, and ∞ if $E^{*\gamma}$ is well-founded for all ordinal γ. (**Updated 2002-05-22**, to allow for ordinal generations.)

The well-foundedness generation of a partially ordered set E is >0 (of course, $\infty>0$) iff E is well-founded. When E is a well-ordered (this implies "totally ordered") set, manifestly, E^* is isomorphic to $E\cup\{\top\}$, where $\top$ is a greatest element, so it is again well-ordered; this means that the well-foundedness generation of any well-ordered set is always ∞. So partially ordered sets E whose well-foundedness generation is 0 (i.e. E is not well-founded), 1 (i.e. E is well-founded but not fairly ordered) or ∞ (e.g. E is well-ordered) are easy to construct, and we have given an example of a partially ordered set whose well-foundedness generation is 2. The obvious stupid question is then: what well-foundedness generations are possible among partially ordered sets?

2002-07-07:044

TODO on future notes in this diary:

- Divisions of the simplex according to proportional electoral system: is it of equal measure?
- "Eclectic" subsets of an algebraically closed field. (See **2002-07-13:045** and **2002-07-13:046**.)
- Describe a necessary and condition sufficient for a morphism of schemes (or more generally sheaves of sets on affine schemes for the flat topology) to be finite, where the condition is sought in the internal language of the topos (as far as possible).
- Associating a dimension 0 ring (spectrum of connected components) to a given ring as the associated sheaf functor for the $\neg\neg$ Lawvere-Tierney topology: how can we describe it concretely? Can we do something for irreducible components?
- If $X\subseteq\mathbb{P}^N$ is a smooth projective variety defined by known equations, and $f\colon\mathbb{P}^1\to X$ a rational curve, how to compute the ℓ_i such that $f^*T_X\cong\bigoplus_i\mathscr{O}(\ell_i)$: describe the actual algorithm, give examples.
- A composition law on deformation classes of morphisms $f\colon\mathbb{P}^1\to X$ (for X a smooth projective variety). Concrete computation in the case where X is the blowup of $\mathbb{P}^2$ at the origin.
- Describe the arithmetic operation on ordinals $\alpha\dot{+}\beta$ being the largest possible order-type of a well-order on the disjoint union $\alpha\uplus\beta$ extending the sum order; similarly, $\alpha\dot{\cdot}\beta$ being the largest possible order-type of a well-order on the cartesian product extending the product order. Show that these are Conway's operations.
- Seek a nice sum and product operation on polarized games (with a finer equivalence relation than that Conway uses, so products of games can be taken).
- Differentially closed fields and how they formalize symbolic computation.
- Iterated Gödelization cannot provide completeness. (See **2003-10-18:055**.)
- ("Recall"...) Construction of $\mathbb{C}_p$ and the completion of the algebraic closure of $\mathbb{F}_p[\![t]\!]$ inside Mal'cev-Neumann rings.

2002-07-13:045

Let E be a subset of an algebraically closed field k. We say that E is *eclectic* when it satisfies the following equivalent conditions:

- For any natural number n, if Z is an irreducible component of the Zariski closure of a subset of $E^n\subseteq k^n$, then there exists a finite set Λ and a partition $(N_\lambda)_{\lambda\in\Lambda}$ of $\{1,\ldots,n\}$ such that $Z=\prod_{\lambda\in\Lambda}Z_\lambda$ where, for each $\lambda\in\Lambda$,

either Z_λ is the diagonal of k^{N_λ} (that is, the subset of constant maps $N_\lambda \to k$), *or* N_λ is a singleton $\{i\}$ and Z_λ is the singleton of an element $c_i \in E$.

- For any natural number n, if U is a Zariski open set of a (closed) algebraic subvariety X of k^n, and if $U \cap E^n$ is infinite, then there exists a straight line L whose parametric equation in function of a parameter t can be given by n equations (for i ranging from 1 through n), each of the form $x_i = c_i$ where $c_i \in E$, or $x_i = t$, with at least one equation of the latter form, such that $L \subseteq X$ and L meets U.

We will show that these two conditions are, indeed, equivalent, but before we set out to do so, we introduce a bit of terminology. For any subset A of k, we call a (closed) subvariety Z of k^n "A-multidiagonal" iff there exists a finite set Λ and a partition $(N_\lambda)_{\lambda\in\Lambda}$ of $\{1,\dots,n\}$ such that $Z = \prod_{\lambda\in\Lambda} Z_\lambda$ where, for each $\lambda \in \Lambda$, *either* Z_λ is the diagonal of k^{N_λ}, *or* N_λ is a singleton $\{i\}$ and Z_λ is the singleton of an element $c_i \in A$. Thus, the first condition above states that E is eclectic iff any irreducible component of the Zariski closure of any subset of E^n is E-multidiagonal. Note that E-multidiagonal subvarieties of dimension 0 of k^n are just singletons of points of E^n. Futher, E-multidiagonal subvarieties of dimension 1 of k^n are precisely the straight lines L whose parametric equation in function of a parameter t can be given by n equations (for i ranging from 1 through n), each of the form $x_i = c_i$ where $c_i \in E$, or $x_i = t$, with at least one equation of the latter form (this is the sort of lines given by the second condition above).

We also define the *type* of an A-multidiagonal subvariety Z of k^n to be the set of N_λ of the first kind (Z_λ is a diagonal): more rigorously, the type of Z is the datum consisting of the finite set T that is the union of the N_λ for which Z_λ is not a singleton, endowed with the equivalence relation whose equivalence classes are the N_λ in question (note that the number of equivalence classes in the type is the dimension of the multidiagonal variety); we abusively tend to omit the mention of the equivalence relation on T when speaking of a type. An A-multidiagonal subvariety of k^n is determined uniquely by its type T and its projections, each one being a singleton $\{c_i\}$, on the coordinates $i \notin T$: it is then the product of $\{c\} \in A^{T'}$ (where $T' = \{1,\dots,n\} \setminus T$) by Δ_T, where Δ_T is the unique ("model") multidiagonal subvariety of k^T having type T.

Let us show now that the two conditions are, indeed, equivalent. Suppose E satisfies the first, and let X and U be respectively a closed algebraic variety of k^n (for some $n \in \mathbb{N}$) and a Zariski open set of X such that $U \cap E^n$ is infinite. Call F the latter set. The Zariski closure of F cannot be just a finite number of points (as F is infinite), so it must contain an irreducible component Z of dimension ≥ 1. Obviously, $Z \subseteq X$ (because X is Zariski closed), and $Z \cap U \neq \varnothing$ (otherwise Z would be disjoint from F and the union of all other components would be a smaller Zariski closed set containing F). Now by the first condition above (which we have assumed), Z is E-multidiagonal. Either Z is of dimension 1, in which case it is precisely the L we seek. Else Z is of dimension ≥ 2. Choose an $i \in \{1,\dots,n\}$ such that the projection of Z onto the i-th coordinate is not constant (and hence, by irreducibility, is all of k): such an i exists because Z is not a point. Of the infinitely many hypersurfaces of Z defined by the equations $x_i = c$ for c in E (notice that E is infinite since $U \cap E^n$ is), not all can be contained in $Z \setminus U$, so there exists $c \in E$ with the property that the intersection Z' of Z and the hyperplane $x_i = c$ meets U. Then $Z' \subseteq X$ and $Z' \cap U \neq \varnothing$, and we also note that Z' is E-multidiagonal (its type is obtained by removing one equivalence class from the type of Z). So proceed with Z' as we have with Z: again, if its dimension is 1 we have finished, otherwise there is a hypersurface Z'' in Z' with the same properties, and so on until the dimension is 1, which gives us the desired L.

Conversely, suppose E satisfies the second property above, and we must show that it satisfies the first. So let Z be an irreducible component of the Zariski closure of a subset F of E^n, and we must show that it has the structure detailed above. Replacing F by $F \cap Z$, we may assume that Z is the Zariski closure of F. Now consider all possible types $T \neq \varnothing$ of multidiagonal subvarieties of dimension > 0 of k^n: for each such T, writing T' for the complement $\{1,\dots,n\} \setminus T$, consider the set H_T of $c \in k^{T'}$ for which the (unique) k-multidiagonal subvariety of k^n of type T having projection c_i on each $i \in T'$, is contained in Z. This H_T is a Zariski closed subset of $k^{T'}$ (being the complement of a projection of the complement of Z); and $H_T \times \Delta_T \subseteq Z$, where Δ_T is the unique ("model") multidiagonal subvariety of k^T having type T (indeed, H_T is precisely the largest possible satisfying this condition). Either Z is contained in the union Y of all the $H_T \times \Delta_T$ or it is not. If it is, then it is contained in one of them (by irreducibility), and then by projecting the whole situation on $k^{T'}$, we are done by an easy induction on the dimension

of Z (the coordinates in T play no role at all in the problem). If it is not, then write U for the complement in Z of the union Y in question. Since Z is the Zariski closure of F, the latter cannot be contained in Y plus a finite number of points. So $U \cap F$, and in particular $U \cap E^n$, is infinite, and by the second condition above (which we have assumed), Z must contain an E-multidiagonal line L which meets U. But this is impossible since L must be contained in Y by construction of the latter.

(Whew! That was a excruciatingly tedious. We continue in **2002-07-13:046**.)

2002-07-13:046

(This continues **2002-07-13:045**.)

In **2002-07-13:045** we have given the definition of an eclectic subset E of an algebraically closed field k as one which satisfies the following two equivalent conditions (reworded to be slightly more understandable, if less precise):

- For any natural number n, any irreducible component of the Zariski closure of a subset of $E^n \subseteq k^n$ is multidiagonal, that is, is the product of diagonals and singletons.
- For any natural number n, if U is a Zariski open set of a (closed) algebraic subvariety X of k^n, and if $U \cap E^n$ is infinite, then there exists a straight line $L \subseteq X$ which meets U and is the product of a diagonal by a singleton in some power of E.

Evidently any finite subset of k is eclectic, and k itself is not eclectic. We can actually define the notion of being n_0-eclectic, where n_0 is a natural number: just replace "for any natural number n" in the definitions by "for any natural number $n \leq n_0$"; and the proof we have given in **2002-07-13:045** that the two conditions are equivalent applies equally well to n_0-eclecticism. It is obvious that any subset E of k is 1-eclectic. Trivially, n-eclectic implies n'-eclectic for $n' \leq n$, and eclectic means n-eclectic for any n.

Here are a few natural questions:

- Is it (by any chance) true that if a subset E of an algebraically closed field k is 2-eclectic then it is eclectic?
- If E is an eclectic subset of an algebraically closed field k and k' is an algebraically closed field containing k, is E necessarily eclectic in k'?
- If E is a set of algebraically independent elements (over the prime field) in a field k, is E eclectic?
- Is it true that for any algebraically field k there always exists an infinite eclectic subset E (better even: having the same cardinality as k)?

I tend to think that the answer to all of these is "yes" (but with a great doubt as to the first).

Here is a construction which should give an infinite eclectic subset of $\bar{\mathbb{Q}}$: start by enumerating all (closed) algebraic subvarieties of $\bar{\mathbb{Q}}^n$ (for variable n) in a sequence $(V_\iota)_{\iota \in \mathbb{N}}$. Construct a sequence $(x_\mu)_{\mu \in \mathbb{N}}$ of elements of $\bar{\mathbb{Q}}$ by induction on μ as follows. Assume all x_ν for $\nu < \mu$ have already been constructed. Consider all lines L in some $\bar{\mathbb{Q}}^n$ whose parametric equation in function of a parameter t can be given by n equations (for i ranging from 1 through n), each of the form $x_i = x_{\nu_i}$ for some $\nu_i < \mu$, or $x_i = t$, with at least one equation of the latter form. And for each such L and V_ι for $\iota \leq \mu$ living in $\bar{\mathbb{Q}}^n$ for the same n, *if* L is not completely contained in V_ι, consider all values of the parameter t for which the corresponding point in L happens to be in V_ι. Since there is only a finite number of $\iota \leq \mu$ and a finite number of L (omitting all those which play no role because they live in a $\bar{\mathbb{Q}}^n$ with n greater than any of the V_ι do), *all* of these t are only finite in number. Now choose some x_μ that is not among them nor equal to x_ν for any $\nu < \mu$. This defines a sequence $(x_\mu)_{\mu \in \mathbb{N}}$ of elements of $\bar{\mathbb{Q}}$ which is injective, and whose range should be an infinite eclectic subset of $\bar{\mathbb{Q}}$. The same applies, in fact, to any countable algebraically closed set k.

I also conjecture the following: a subset E of an algebraically closed field k is eclectic iff for any natural number n, if X is an algebraic (closed) hypersurface of k^n, and if $X \cap E^n$ is infinite, then there exists a straight line L whose parametric equation in function of a parameter t can be given by n equations (for i ranging from 1 through n), each of the form $x_i = c_i$, or $x_i = t$, with at least one equation of the latter form, such that $L \subseteq X$. This is obviously necessary, but it is (apparently) weaker than the (second form of the) definition in three counts: first, U is taken to be all of X; second, X is taken to be of codimension 1; and third, the c_i are not required to be in E. I believe that despite these three weakenings, we still get a condition equivalent to being eclectic; but I can't prove that any of these three weakenings (with or without the others) still gives an equivalent condition.

(Thanks to Joël Riou for discussions on this subject.)

2002-12-01:047

This adds to **2002-01-20:030**, and remarks on "Higman's game" defined there.

Péter Horvai points out to me that Higman's game has a trivial winning strategy (by this I mean the misère Higman's game: because the normal Higman's game has an even more trivial winning strategy, which consists of simply playing the empty word immediately). Namely, if the alphabet A has an odd number of letters, the first player plays a single-letter word and wins by reducing to being second player on an even alphabet; if the alphabet A has an even number of letters, the second player wins by choosing an involution $h\colon A \to A$ without fixed points, and, whenever the first player plays a word w, responding by playing $h^*(w)$, where $h^*\colon A^* \to A^*$ is defined by applying h to every letter. Manifestely, $h^*(w)$ is not a subword of w (since it has the same length and is not equal); nor is it a subword of any other previously played $u \in A^*$, for if it were then w would be subword of $h^*(u)$, and $h^*(u)$ has been played already (either just before, or just after u) if the second player has stuck to the same strategy—so the second player can always play, and therefore wins.

2002-12-01:048

This adds to **2002-01-20:030** and generalizes "Higman's game" defined there.

If M is any monoid (= set with an associative multiplication having a unit element), we can define a relation $\preceq$ on M by letting $x \preceq y$ iff we can write $x = x_1 \cdots x_n$ and $y = y_0 \cdot x_1 \cdot y_1 \cdots y_{n-1} \cdot x_n \cdot y_n$, where $x_1, \ldots, x_n$ and $y_0, \ldots, y_n$ are elements of M. In general, this is not an order relation: for example, if $M = G$ is a group, then $x \preceq y$ holds for any x and y. However, it is reflexive and transitive (i.e., it is a preorder relation). In fact, $\preceq$ is the smallest preorder on M that is invariant by left- and right-translation and such that $1 \preceq x$ for any x. If M is such that $\preceq$ is an order, we say that M is *cancellation-free* (note: there may be several different definitions for this, and I'm not sure as to how they relate).

Note that the relation $\equiv$ defined by $x \equiv y$ iff $x \preceq y$ and $y \preceq x$, is an equivalence relation, and it is compatible with the monoid structure so that the quotient $M/\equiv$ has a natural monoid structure, and is cancellation-free.

Higman's game on M can then be defined in the straightforward way: two players take turns in selecting an element $x \in M$ such that x does not satisfy $z \preceq x$ for any z that has been previously played, and the first one who cannot play looses (in the normal version) or wins (in the misère version). Of course, we might as well play the game in the cancellation-free monoid $M/\equiv$ defined above. Now Higman's lemma (proved in **2002-01-23:031**) assures that for a monoid of finite type (that is, having a finite set of generators), the game always terminates in a finite number of steps (no matter what the players choose), so that some player has a winning strategy.

We can of course defined the length $\lg_N(M)$ (and the Grundy function as well, $\mathrm{Gy}_N(M)$, if needed) of the monoid M as the length and Grundy function respectively of this game. For example, $\lg_N(\mathbb{N}) = \omega$ and $\lg_N(\mathbb{N}^2) = \omega^2$ (the Higman game on $\mathbb{N}^2$ is Conway's poisoned wafer game) and more generally $\lg_N(\mathbb{N}^r) = \omega^r$.

2002-12-01:049

Recall a few facts about closed unbounded subsets of a regular uncountable cardinal. If κ is a regular uncountable cardinal (seen, of course, as the set of ordinals $\alpha < \kappa$), we say that a subset $C \subseteq \kappa$ is *closed unbounded* iff C is closed but not compact for the order topology on κ (and the topology it induces on C, which incidentally has then good taste of being the order topology on C); in a more natural way, $C \subseteq \kappa$ is closed unbounded iff $\sup C = \kappa$ and $\sup C' \in C \cup \{\kappa\}$ for all $C' \subseteq C$. For any such C, there is a unique (strictly) increasing $f\colon \kappa \to \kappa$ whose image is C, and f is continuous; and conversely, any increasing continuous $f\colon \kappa \to \kappa$ has a closed unbounded image: an increasing continuous function $\kappa \to \kappa$ is sometimes called *normal*—then normal functions on κ and closed unbounded subsets of κ can be identified; evidently, if f is normal then $f(\alpha) \geq \alpha$ for all $\alpha < \kappa$.

(Vincent Nesme tells me that closed unbounded subsets of κ are also called *clubs* in κ, where "club" stands for "CLosed UnBounded". A rather smart terminology when the term is often mentioned.)

The intersection of two closed unbounded subsets of κ is closed unbounded. More generally, the intersection of less than κ closed unbounded subsets of κ is closed unbounded. The set of limit points (accumulation points) of a closed unbounded subset of κ is closed unbounded. The image of a closed unbounded subset by a normal function is closed unbounded. The set of fixed points of a normal function is closed unbounded.

Another important property is the following. If $(C_\alpha)_{\alpha<\kappa}$ is a collection of (otherwise arbitrary) closed unbounded subsets of κ, we define their *diagonal intersection* $\triangle_{\alpha<\kappa}C_\alpha$ as $\{\xi < \kappa : \xi \in \bigcap_{\alpha\leq\xi} C_\xi\}$ or equivalently as $\bigcap_{\alpha<\kappa}(C_\alpha \cup \alpha)$ (note that this definition is ever-so-slighty different from that found in Jech, but the difference is, of course, completely inconsequential). Note that the diagonal intersection does not change if we replace C_α by $C_\alpha \setminus \alpha$ (we remove the elements $\xi < \alpha$ from C_α). More importantly, note that the diagonal intersection does not change if we replace C_α by $\bigcap_{\beta\leq\alpha} C_\beta$, so that (C_α) is decreasing (in the broad sense), and then the diagonal intersection is $\{\xi < \kappa : \xi \in C_\xi\}$. The important property, of course, is that the diagonal intersection is again closed unbounded.

Suppose $f\colon\kappa \to \kappa$ is normal (i.e. continuous and (strictly) increasing). Put $C_0 = \kappa$, let $C_1 = f(\kappa)$ be the image of f, and $C_2 = f(C_1)$ image of its image (which is the image of $f^{\circ 2}$), $C_3 = f(C_2)$ and so on, more generally $C_{\alpha+1} = f(C_\alpha)$ for $\alpha < \kappa$ together with $C_\delta = \bigcap_{\beta<\delta} C_\beta$ for $\delta < \kappa$ limit. Note incidentally that this permits to define in a natural way the β-th iterate of f with itself (namely, $f^{\circ\beta}$ is the normal function which enumerates C_β). Unfortunately, I do not see a natural and elegant way to relate the diagonal intersection of the C_α to the set of fixed points of f (there should be a relation—or a common generalization at least); though naturally every fixed point of f is in the diagonal intersection (since it is in the plain intersection).

If F is a function taking closed unbounded sets of κ to closed unbounded sets of κ, such that $F(C) \subseteq C$ for all C closed unbounded, we define another operation G of the same type by letting $G(C)$ be the diagonal intersection of the $F^{\circ\alpha}(C)$ for $\alpha < \kappa$, where $F^{\circ\alpha}(C)$ is defined as one would think: $F^{\circ 0}(C) = C$, $F^{\circ(\alpha+1)}(C) = F(F^{\circ\alpha}(C))$ for all $\alpha < \kappa$, and $F^{\circ\delta}(C) = \bigcap_{\beta<\delta} F^{\circ\beta}(C)$ for $\delta < \kappa$ limit. Then, of course, we can let $G_0 = F$, $G_1 = G$, G_2 obtained as G previously if we take $F = G_1$, and so on, $G_{\alpha+1}$ obtained as G above by taking $F = G_\alpha$, and $G_\delta(C) = \bigcap_{\beta<\alpha} G_\beta(C)$ for $\delta < \kappa$ limit. And then we can define $H(C)$ to be the diagonal intersection of the $G_\alpha(C)$ for $\alpha < \kappa$. Similarly, we can let $H_0 = F$, $H_1 = H$, and iterate the process used to construct H from F to create H_α for alla $\alpha < \kappa$, all taking closed unbounded subsets to closed unbounded subsets. This naturall leads us to define $\mathscr{F}_0 = F$ and $\mathscr{F}_1 = G$ and $\mathscr{F}_2 = H$, and for all α we can define $\mathscr{F}_\alpha$, and we can again take a diagonal intersection to define $\mathscr{G}$... The picture should be clear by then.

In particular, these constructions can be used to define many denumerable ordinals.

2002-12-01:050

(Compare with **2002-01-13:028**.) This is an attempt to found "semialgebraic" geometry.

Recall that if K is a field, a necessary and sufficient condition for there to exist a total order on K such that (i) $x \leq y$ implies $x + z \leq y + z$ for all $x, y, z \in K$, and (ii) $0 \leq x$ and $0 \leq y$ imply $0 \leq xy$ for all $x, y \in K$, is that -1 is not a sum of squares in K. When this is the case, we say that K is *orderable*; furthermore, when there exists a *unique* order satisfying (i) and (ii), we say that K is *uniquely orderable*. The latter condition is weaker than being real-closed: a real-closed field is certainly uniquely orderable (since every element is either a square or the opposite of a square) but $\mathbb{Q}$ (or $\mathbb{Q}(\sqrt[3]{2})$) is uniquely orderable without being real-closed; on the other hand, $\mathbb{Q}(\sqrt{2})$ is orderable but not uniquely orderable.

We now say that a (commutative) ring A is orderable (an admittedly rather dubious terminology) iff, for every prime ideal $\mathfrak{p}$ of A, the field of fractions $\mathrm{Frac}(A/\mathfrak{p})$ of the quotient integral domain $A/\mathfrak{p}$ is orderable in the previous sense. It would be eminently desirable to obtain a simple necessary and sufficient condition (not involving quantification over prime ideals) for a ring to be orderable.

Note that any orderable field is of characteristic 0 for obvious reasons. It follows that if A is an orderable ring then it must contain $\mathbb{Q}$ (for if there were an integer $n \in \mathbb{N}^*$ not invertible in A then it would be contained in a prime ideal, contradicting the previous statement). In particular, we can evaluate any element of $\mathbb{Q}[t]$ (the ring of polynomials with coefficients in $\mathbb{Q}$ over the indeterminate t) at any element of A; an element f of $\mathbb{Q}[t]$ which is positive (in the broad sense, i.e. $f(x) \geq 0$) on every rational value x, or, equivalently, on every real x, will simply be called "positive"

(everywhere here, "positive" is meant in the broad sense). Note that if $f \in \mathbb{Q}[t]$ is positive then $f(x) \geq 0$ for any x in *any* real-closed field K, and, hence, in *any* orderable field K for any order on K. If now $f \in \mathbb{Q}[t]$ is such that $f(x) > 0$ for all real x (this time it is not sufficient to assume this for all rational x—however, it suffices to assume it for x in the real-closure of $\mathbb{Q}$), or, equivalently, if there exists $r > 0$ rational such that $f(x) = r + g(x)$ with g positive in the broad sense—and we summarize these conditions by saying that f is "strictly positive"—then $f(x)$ cannot be zero for any x in any orderable field K, so that $f(x)$ cannot belong to any prime ideal if x is an element of an orderable ring A. For example, for any orderable ring A, and any $x \in A$, the element $x^2 + 1 \in A$ must be invertible in A.

To put it differently, let $\mathbb{Q}\lfloor t \rfloor$ be the ring of rational functions $f \in \mathbb{Q}(t)$ that have no real poles. Then $\mathbb{Q}\lfloor t \rfloor$ is an orderable ring (this is easy), and for $f \in \mathbb{Q}\lfloor t \rfloor$ and $x \in A$ with A an orderable ring, the element $f(x) \in A$ is well-defined in the obvious manner. Abstract nonsense: the orderable ring $\mathbb{Q}\lfloor t \rfloor$ represents the forgetful functor from the category of orderable rings to the category of sets (much as $\mathbb{Z}[t]$ represents the forgetful functor from the category of rings to the category of sets).

Any quotient of an orderable ring is orderable: this is an easy consequence of the definition.

For any ring A there is a morphism $A \to A_r$ to an orderable ring A_r that is universal in the sense that any morphism $A \to B$ from A to an orderable ring B factors through B. Indeed, A_r can be constructed by inverting in A every element which does not belong to any prime ideal $\mathfrak{p}$ for which $\mathrm{Frac}(A/\mathfrak{p})$ is orderable. This construction takes any field which is not orderable to 0, of course; it takes $\mathbb{Z}$ to $\mathbb{Q}$ and $\mathbb{Q}[t]$ to $\mathbb{Q}\lfloor t \rfloor$.

If A is an orderable ring, we can define its *realspectrum* as follows. It is the set $\mathrm{RSpec}\, A$ of data consisting of a prime ideal $\mathfrak{p}$ of A together with a total order on the field $\mathrm{Frac}(A/\mathfrak{p})$. Actually we can translate such data in a different way: collect the set $\mathfrak{P}$ of elements x of A such that the class of x in $A/\mathfrak{p}$ is positive (in the broad sense); then $\mathfrak{p}$ can be reconstructed as the set of x of A such that $x \in \mathfrak{P}$ and $-x \in \mathfrak{P}$, and the order on $A/\mathfrak{p}$ in the obvious way; it turns out that $\mathfrak{P}$ satisfies the following conditions: (i) if $x, y \in \mathfrak{P}$ then $x + y \in \mathfrak{P}$, (ii) if $x \in A$ then $x^2 \in \mathfrak{P}$, (iii) if $x, y \in A$ are such that $xy \in \mathfrak{P}$ then either $x, y \in \mathfrak{P}$ or $-x, -y \in \mathfrak{P}$, and (iv) $-1 \notin \mathfrak{P}$; and any set satisfying (i), (ii), (iii) and (iv) comes from a point of $\mathrm{RSpec}\, A$ (and defines such a point) as explained. (Compare with the following definition of a prime ideal $\mathfrak{p}$ of A: (i) if $x, y \in \mathfrak{p}$ then $x + y \in \mathfrak{p}$, (ii) $0 \in \mathfrak{p}$ and if $x \in A$ and $y \in \mathfrak{p}$ then $xy \in \mathfrak{p}$, (iii) if $x, y \in A$ are such that $xy \in \mathfrak{p}$ then $x \in \mathfrak{p}$ or $y \in \mathfrak{p}$, and (iv) $1 \notin \mathfrak{p}$.)

The condition that A is orderable in defining the realspectrum is innocent: we can always replace A by its universal orderable algebra A_r as defined earlier, and then define $\mathrm{RSpec}\, A$ as $\mathrm{RSpec}\, A_r$, which is, anyway, exactly the definition we have given. But "morally", semialgebraic geometry only "sees" orderable rings.

We further put a topology on $\mathrm{RSpec}\, A$ by as follows: if $x \in A$, we define $H(x)$ as the set of $\mathfrak{P} \in \mathrm{RSpec}\, A$ such that $-x \notin \mathfrak{P}$, or, in other words, prime ideals $\mathfrak{p}$ endowed with an order on $\mathrm{Frac}(A/\mathfrak{p})$ such that the image of x is strictly positive in $\mathrm{Frac}(A/\mathfrak{p})$. These are the subbasis for a topology on $\mathrm{RSpec}\, A$, that is, finite intersections of such $H(x)$ are the basis of a topology on $\mathrm{RSpec}\, A$ with which we endow the later.

We now put a sheaf or rings $\mathscr{O}$ on $\mathrm{RSpec}\, A$ as follows: define $\mathscr{O}(H(x_1) \cap \cdots \cap H(x_s))$ as the localization of A which inverts every $y \in A$ that satisfies $y \notin \mathfrak{p}$ for every $\mathfrak{p}$ for which some corresponding $\mathfrak{P}$ is in $H(x_1) \cap \cdots \cap H(x_s)$. We also put on $\mathrm{RSpec}\, A$ a subsheaf $\mathscr{P}$ of $\mathscr{O}$ as follows: define $\mathscr{P}(H(x_1) \cap \cdots \cap H(x_s))$ as the set of elements h of $\mathscr{O}(H(x_1) \cap \cdots \cap H(x_s))$ such that for every $\mathfrak{P}$ of $H(x_1) \cap \cdots \cap H(x_s)$ the image of h in $\mathrm{Frac}(A/\mathfrak{p})$ is positive in the broad sense (where $\mathfrak{p}$ and the order on $\mathrm{Frac}(A/\mathfrak{p})$ are defined by the datum $\mathfrak{P}$): note that the image of h in $\mathrm{Frac}(A/\mathfrak{p})$ is meaningful precisely because elements of $\mathfrak{p}$ have not been inverted in constructing $\mathscr{O}(H(x_1) \cap \cdots \cap H(x_s))$, by definition of the latter.

The datum consisting of the topological space $\mathrm{RSpec}\, A$ (for some orderable ring A) together with the sheaves $\mathscr{O}$ and $\mathscr{P}$ will be called an *affine realscheme*.

By definition, a *realscheme* will be a topological space X endowed with a sheaf of rings $\mathscr{O}$ and a subsheaf $\mathscr{P}$ of the latter such that X can be covered by open sets U such that the topological space U together with the sheaf of rings $\mathscr{O}|_U$ and the subsheaf $\mathscr{P}|_U$ of the latter is isomorphic to an open subset of an affine realscheme.

This definition is unpleasant because of the words "an open subset of" at the end. The problem, of course, is that an open subset of an affine realscheme may not be covered by affine realschemes: this is so for very stupid reasons, for example the open set $H(t)$ (the open positive half-line) of $\mathrm{RSpec}(\mathbb{Q}\lfloor t \rfloor)$ (the affine line) cannot be covered. To

make the definition less unpleasant, we introduce *realaffine* realschemes.

Specifically, we associate to a "principal" open subset $U = H(x_1) \cap \cdots \cap H(x_s)$ of $\mathrm{RSpec}\, A$ the ring $A' = \mathscr{O}(H(x_1) \cap \cdots \cap H(x_s))$ which we have already defined, together with the subset $P' = \mathscr{P}(H(x_1) \cap \cdots \cap H(x_s))$ of "positive" functions on $H(x_1) \cap \cdots \cap H(x_s)$. We can supposedly reconstruct the realscheme $(U, \mathscr{O}|_U, \mathscr{P}|_U)$ as follows. The set U is the set of data consisting of a prime ideal $\mathfrak{p}$ of A' together with a total order on $\mathrm{Frac}(A'/\mathfrak{p})$ such that all elements of P' have a positive image; the topology on U and the sheaves $\mathscr{O}' = \mathscr{O}|_U$ and $\mathscr{P}' = \mathscr{P}|_U$ can the be defined just as previously, taking into account the extra datum P'. We call this $\mathrm{RSpec}(A', P')$ and define a *realaffine* realscheme to be (isomorphic to) a realscheme of this form.

This definition is terribly nasty, because, just as I don't know a straightforward definition of an orderable ring, I also don't know what simple conditions P' must satisfy for (A', P') to be of the form $(\mathscr{O}(H(x_1) \cap \cdots \cap H(x_s))\ , \mathscr{P}(H(x_1) \cap \cdots \cap H(x_s)))$ (for some affine realscheme $\mathrm{RSpec}\, A$ and some $x_i \in A$), which then lets $\mathrm{RSpec}(A', P')$ be defined and be a realaffine realscheme. If I had elegant criteria on (A', P') ("rings with positivity conditions"), I would start by defining a realaffine realschemes from these data, and proceed from then on.

In the mean time, it remains to define morphisms. These are what you'd think: a morphism between realschemes is a morphism between locally ringed spaces which preserves positivity in the sense that it restricts to a morphism from the $\mathscr{P}$ ("positivity") sheaf of one to that of the other. If the world makes any sense, morphisms from $\mathrm{RSpec}\, A'$ to $\mathrm{RSpec}\, A$ are simply morphisms of rings from A to A'—here, of course, it is essential for A' to be orderable (and possibly A also); and more generally, morphisms from $\mathrm{RSpec}(A', P')$ to $\mathrm{RSpec}(A, P)$ should be morphisms of rings from A to A' which send P to a subset of P'.

Whew! That was rather tedious. And, of course, I didn't do any work here—I just charted the territory: it remains to check that things, in fact, do work as they should and that this whole semialgebraic (realalgebraic?) geometry does make sense.

The dream would be to end up with various nice topoi, analogous to the Zariski, étale and flat topoi of usual algebraic geometry. But whereas the sheaf represented by $\mathrm{Spec}\, \mathbb{Z}[t]$ (that is, the forgetful functor from rings to sets) is, in algebraic geometry, an algebraically closed field (for the appropriate, intuitionist, definition of "algebraically closed field") in the flat topos, in semialgebraic geometry, in the realflat topos, the sheaf represented by the affine realscheme $\mathrm{RSpec}\, \mathbb{Q}\lfloor t \rfloor$ should be, for a suitable definition, a realclosed field.

2002-12-05:051

Recall (compare **2002-03-11:033**) that on a topos $\mathcal{T}$ with subobject classifier Ω, a *Lawvere-Tierney topology* is a morphism $j\colon \Omega \to \Omega$ such that (i) $j \circ true = true$, (ii) $j \circ j = j$ and (iii) $j \circ and = and \circ (j \times j)$. Note that it follows that $j \geq \mathrm{id}_\Omega$ (for the natural order on Ω). (Proof: if X is any object of $\mathcal{T}$ we need to prove that the inequality holds in $\Omega(X) = \mathrm{Hom}(X, \Omega)$, the poset of subobjects of X. Now if U is a subobject of X and $\chi_U\colon X \to \Omega$ its characteristic morphism—so that $U \rightarrowtail X$ is the pullback of $true\colon \top \to \Omega$ by χ_U—then χ_U is $true$ when pulled back to U, so $j\chi_U$ also is: this proves that the subobject $j_X(U)$ of X whose characteristic morphim is $j\chi_U$, factors U, which is what we wanted. Hum, this last part would be better if it were a bit clearer.) In fact, it is a remarkable property of the complete Heyting algebra Ω that any (internal!) map $j\colon \Omega \to \Omega$ satisfying (i), (ii) and (iii) above automatically verifies $j \geq \mathrm{id}_\Omega$. In general, given a Heyting algebra $\mathbf{H}$, we define a Lawvere-Tierney topology on $\mathbf{H}$ to be a map $j\colon \mathbf{H} \to \mathbf{H}$ which satisfies (i) $j(u) \geq u$ for all $u \in \mathbf{H}$, (ii) $j(j(u)) = j(u)$ for all $u \in \mathbf{H}$ and (iii) $j(u \sqcap v) = j(u) \sqcap j(v)$ for all $u, v \in \mathbf{H}$ where $\sqcap$ is the meet operation in $\mathbf{H}$.

In particular, if $\mathcal{T}$ is the topos of sheaves on a topological space X, a Lawvere-Tierney topology on $\mathcal{T}$ (or, for short, on X) is precisely a Lawvere-Tierney topology on the Heyting algebra $\mathcal{O}(X)$ of open sets of X, i.e. a map $j\colon \mathcal{O}(X) \to \mathcal{O}(X)$ which satisfies (i) $j(U) \supseteq U$ for all U open in X, (ii) $j(j(U)) = j(U)$ for all U open in X and (iii) $j(U \cap V) = j(U) \cap j(V)$ for all U and V open in X. One particular example is given as follows: if Y is any subset of X (endowed with the induced topology), define, for U open in X, the set $j_Y(U)$ to be the largest open set $W \subseteq X$ such that $W \cap Y = U \cap Y$; equivalently, it is the union of all $W \subseteq X$ such that $W \cap Y = U \cap Y$, or equivalently the union of all $W \subseteq X$ such that $W \cap Y \subseteq U \cap Y$; or again, $j_Y(U)$ is the set of all points $x \in X$ such that x has a neighborhood W for which $W \cap Y = W \cap U \cap Y$, that is, the set of all points $x \in X$ in a neighborhood of

which U contains all the points of Y. For $Y \subseteq X$ closed, $j_Y(U)$ is simply the union $U \cup (X \setminus Y)$ of U and the (open) complement of Y: we have $j_Y : U \mapsto U \cup V$ where $V = j_Y(\varnothing) = X \setminus Y$. For $Y \subseteq X$ open, $j_Y(U)$ is simply $Y \Rightarrow U$ (as given by the Heyting algebra structure). Note that Y is dense iff $j_Y(\varnothing) = \varnothing$: more generally we will say that a Lawvere-Tierney topology on X is *dense* iff $j(\varnothing) = \varnothing$, or on any topos $\mathcal{T}$ iff $j \circ \mathit{false} = \mathit{false}$, or on any Heyting algebra $\mathbf{H}$ iff $j(\bot) = \bot$. Note that the $\neg\neg$ topology $j = \neg\neg$, on any topological space (j then sends an open set U to the regular open set which is the interior of the closure of U), on any topos or on any Heyting algebra, is (trivially) dense in the sense just defined.

A folkloric theorem on topoi states that every geometric morphism between topoi (a geometric morphism $f : \mathcal{T} \to \mathcal{T}'$ is a pair of functors: $f_* : \mathcal{T} \to \mathcal{T}'$ called the direct image part, and $f^* : \mathcal{T}' \to \mathcal{T}$ called the inverse image part, such that $f^* \dashv f_*$, i.e. f^* is left adjoint to f_*, and f^* is left exact, i.e. preserves finite limits) which is an embedding (meaning that the direct image part f_* is fully faithful) can be written, up to equivalence of categories, as the canonical embedding $\mathrm{Sh}_j(\mathcal{T}) \to \mathcal{T}$ (see **2002-03-11:033** for the definition of $\mathrm{Sh}_j(\mathcal{T})$; here, the direct image part $\mathrm{Sh}_j(\mathcal{T}) \to \mathcal{T}$ is the forgetful functor, and the inverse image part $\mathcal{T} \to \mathrm{Sh}_j(\mathcal{T})$ is the sheafification functor) from the topos of j-sheaves for some uniquely defined Lawvere-Tierney topology j on $\mathcal{T}$. We can then call a geometric morphism of topoi which is an embedding, according as its associated Lawvere-Tierney j is: dense iff j is dense (in the sense defined above), closed iff j is closed (that is, $j = \mathit{and}(\mathrm{id}_\Omega, j(\mathit{false}))$), and so on. It would also seem (**update:** this is in fact slightly dubious) that a geometric morphism is called *open* iff the inverse image part f^* admits a *left* adjoint (then written $f_!$ and called the "extension by zero/empty" functor): we can then call a Lawvere-Tierney topology j open iff the associated embedding of topoi is open—and if the world makes any sense, such j will be given exactly by some global section H of Ω by $j(U) = H \Rightarrow U$ (internalized) (this needs to be checked). We can further call an embedding of topoi (or, equivalently, a Lawvere-Tierney topology j) locally closed iff it is open after factorization by the "closure" which is the Lawvere-Tierney topology defined by $\mathit{and}(\mathrm{id}_\Omega, j(\mathit{false}))$.

Many details on this need to be checked, but there do not seem to be any major difficulties.

2002-12-12:052

Important note (2002-12-13): Much of what follows is *wrong* if not downright *nonsense*; and it is incomplete anyway. I am leaving it anyway, since some of it is of interest (if only to illustrate what nonsense can be spoken when enough care is not paid), and I will try to correct errors, but I might miss some.

(The following situation was suggested to me by Fabrice Orgogozo.)

Let $f : \mathcal{X} \to \mathcal{S}$ be a geometric morphism of topoi: in other words, we are given two functors $f^* : \mathcal{S} \to \mathcal{X}$ (the inverse image part) and $f_* : \mathcal{X} \to \mathcal{S}$ (the direct image part) with f^* left adjoint to f_* and f^* left exact (which means it preserves finite limits).

We define a topos $\mathcal{Z} = \mathcal{X} \overleftarrow{\times}_{\mathcal{S}} \mathcal{S}$ (**correction:** the topos $\mathcal{Z}$ defined here is *not* what should be called $\mathcal{X} \overleftarrow{\times}_{\mathcal{S}} \mathcal{S}$: see further corrections below) as follows: the objects of $\mathcal{Z}$ are triples (F, G, α) where (i) F is an object of $\mathcal{X}$, (ii) G is an object of $\mathcal{S}$, and (iii) α is an arrow $G \to f_*F$ in $\mathcal{S}$ (by adjunction, this is equivalent to giving the arbitrary arrow $\varepsilon f^* \alpha : f^*G \to F$ in $\mathcal{X}$); and its arrows $(F', G', \alpha') \to (F, G, \alpha)$ are pairs (φ, ψ) where $\varphi : F' \to F$ and $\psi : G' \to G$ are such that $\alpha\psi = (f_*\varphi)\alpha'$ (which is equivalent to demanding that $\varepsilon(f^*\alpha)(f^*\psi) = \varphi\varepsilon(f^*\alpha')$).

We define a geometric morphism $\pi : \mathcal{Z} \to \mathcal{X}$ as follows: the direct image part π_* is given by $\pi_*(F, G, \alpha) = F$ on objects and $\pi_*(\varphi, \psi) = \varphi$ on morphisms, and the inverse image part π^* by $\pi^*F = (F, 0, 0)$ (where 0 is first the initial object of $\mathcal{S}$ and then the unique arrow from it to F) and $\pi^*\varphi = (\varphi, 0)$ (**correction:** this π^* is *not* left exact since it does not send the terminal object to the terminal object; so we do *not* have a geometric morphism π as suggested). We also define a geometric morphism $\varpi : \mathcal{Z} \to \mathcal{S}$ by letting $\varpi_*(F, G, \alpha) = G$ and $\varpi_*(\varphi, \psi) = \psi$ and $\varpi^*G = (f^*G, G, \eta)$ (where η is the unit of the adjunction $f^* \dashv f_*$) and $\varpi^*\psi = (f^*\psi, \psi)$. Finally, we define a 2-morphism $\delta : \varpi \to f\pi$ by letting $\delta_* : \varpi_* \to f_*\pi_*$ be given as $\delta_*(F, G, \alpha) = \alpha : \varpi_*(F, G, \alpha) = G \to f_*F = f_*\pi_*(F, G, \alpha)$, or, equivalently, by defining $\delta^* : \pi^*f^* \to \varpi^*$ by $\delta^*G = (\mathrm{id}_{f^*G}, 0) : \pi^*f^*G = (f^*G, 0, 0) \to (f^*G, G, \eta) = \varpi^*G$.

So the topos $\mathcal{Z} = \mathcal{X} \overleftarrow{\times}_{\mathcal{S}} \mathcal{S}$ is equipped with the following data: a geometric morphism $\pi : \mathcal{Z} \to \mathcal{X}$, a geometric morphism $\varpi : \mathcal{Z} \to \mathcal{S}$, and a 2-morphism $\delta : \varpi \to f\pi$ (**correction:** as explained in the corrections above, this is plain *wrong*; if it is anything, the topos $\mathcal{Z}$ is equipped with morphisms *from* $\mathcal{X}$ and $\mathcal{S}$ and not *to* them; and if anything, it

is *coüniversal* not universal as claimed in the following sentence). It is, furthermore, *universal* for these data, in the sense that, if $\mathcal{T}$ is any topos, and we are given geometric morphisms $h\colon \mathcal{T} \to \mathcal{X}$ and $k\colon \mathcal{T} \to \mathcal{S}$ and a 2-morphism $d\colon k \to fh$, then there is a unique geometric morphism $\rho\colon \mathcal{T} \to \mathcal{Z}$ such that $h = \pi\rho$ and $k = \varpi\rho$ and $d = \delta * \rho$. In fact, ρ is constructed easily enough: if H is an object of $\mathcal{T}$, put $\rho(H) = (h(H), k(H), d(H))$ and if $\lambda\colon H' \to H$ is a morphism, put $\rho(\lambda) = (h(\lambda), k(\lambda))$.

Now besides the geometric morphisms $\pi\colon \mathcal{Z} \to \mathcal{X}$ and $\varpi\colon \mathcal{Z} \to \mathcal{S}$ we can also define a $\Psi\colon \mathcal{X} \to \mathcal{Z}$ by letting $\Psi_* F = (F, f_* F, \mathrm{id}_{f_* F})$ and $\Psi_* \varphi = (\varphi, f_* \varphi)$, and $\Psi^*(F, G, \alpha) = F$ and $\Psi^*(\varphi, \psi) = \varphi$: we trivially note that $\Psi^* = \pi_*$, so that Ψ^* not only has the right adjoint Ψ_* but also a left adjoint $\Psi_! = \pi^*$. In the language of geometric morphisms, this means that Ψ is an open (Ψ^* has a left adjoint (**correction:** this is dubious and needs to be checked)) embedding (Ψ_* is fully faithful). So Ψ identifies $\mathcal{X}$ with an open subtopos of $\mathcal{Z}$, namely the slice category of objects of sheaves over $\Psi_! 1 = (1, 0, 0)$, that is, objects of the form $(F, 0, 0)$ (recall that, in a topos, any arrow $G \to 0$ is an isomorphism).

Note incidentally that a morphism (φ, ψ) in $\mathcal{Z}$ is a monomorphism iff φ (in $\mathcal{X}$) and ψ (in $\mathcal{S}$) both are: the "if" direction is obvious; for the "only if", suppose $(\varphi, \psi)\colon (F', G', \alpha') \to (F, G, \alpha)$ are is a monomorphism: then if $\gamma_1, \gamma_2\colon G'' \to G'$ are such that $\psi\gamma_1 = \psi\gamma_2$, construct the object $\varpi^* G'' = (f^* G'', G'', \eta)$ and send it to (F', G', α') by the two morphisms deduced from γ_1 and γ_2 using the adjunction $\varpi^* \dashv \varpi_*$, namely $(\varepsilon(f^*\alpha')(f^*\gamma_i), \gamma_i)$, and note that after composition with (φ, ψ) they become equal, so since the latter is a monomorphism, $\gamma_1 = \gamma_2$ and this shows that ψ is a monomorphism; similarly, if $\varsigma_1, \varsigma_2\colon F'' \to F'$ are such that $\varphi\varsigma_1 = \varphi\varsigma_2$, construct the object $\pi^* F'' = (F'', 0, 0)$ and send it to (F', G', α') by the two morphisms deduced from ς_1 and ς_2 using the adjunction $\pi^* \dashv \pi_*$, namely $(\varsigma_i, 0)$, and note that after composition with (φ, ψ) they become equal, so since the latter is a monomorphism, $\varsigma_1 = \varsigma_2$ and this shows that φ is a monomorphism.

We now describe this in terms of the general theory summarized in **2002-12-05:051**: the embedding Ψ is associated to a Lawvere-Tierney topology j_Ψ on $\mathcal{Z}$ in the sense that $\mathcal{X}$ is equivalent to the category of j_Ψ-sheaves in such a way that Ψ_* becomes the forgetful functor and Ψ^* the sheafification functor. Now j_Ψ is easy enough to describe. First we describe $\Omega_\mathcal{Z}$ the subobject classifier of $\mathcal{Z}$. Since a morphism (φ, ψ) of $\mathcal{Z}$ is a monomorphism iff φ and ψ both are, we see that a subobject (F', G', α') of an object (F, G, α) of $\mathcal{Z}$ is determined by the subobjects F' of F and G' of G (in other words, α' is determined by α: this is because $\varepsilon_{F'}(f^*\alpha)(f^*\psi) = \varphi\varepsilon_F(f^*\alpha')$, as we have already noted, and the right-hand term imposes α' since φ is a monomorphism — here, ε is the coünit of the adjunction). A moment's reflection then suffices to see that $\Omega_\mathcal{Z}$ is a subobject of $(\Omega_\mathcal{X}, f_*\Omega_\mathcal{X} \times \Omega_\mathcal{S}, p)$, where p is the projection on the first factor. In fact, more specifically, $\Omega_\mathcal{Z}$ is exactly $(\Omega_\mathcal{X}, \Lambda, p)$ where Λ is the object of $\mathcal{S}$, subobject of $f_*\Omega_\mathcal{X} \times \Omega_\mathcal{S}$, that classifies data consisting of a subobject G' of G (a given object) and a subobject F' of f^*G with f^*G' included in F' (note that subobjects G' of G are classified by $\Omega_\mathcal{S}$ by definition, and subobjects F' of f^*G by $f_*\Omega_\mathcal{X}$ by adjunction). Or, to say things slightly informally but perhaps more comprehensibly, Λ is the subobject of $f_*\Omega_\mathcal{X} \times \Omega_\mathcal{S}$ consisting of those (μ, ν) such that $o^*(\nu) \leq \mu$, or equivalently $\nu \leq o_*(\mu)$, where $o^*\colon \Omega_\mathcal{S} \to \mathbf{H}$ (here with $\mathbf{H} = f_*\Omega_\mathcal{X}$) is the arrow that exists for any $\mathcal{S}$-internal complete Heyting algebra taking a truth value ν to the least upper bound of the set containing $\top$ with truth value ν and nothing else, and $o^*\colon \mathbf{H} \to \Omega_\mathcal{S}$ is its left adjoint, which takes an element μ of $\mathbf{H}$ to the truth value of $\mu = \top$. We can then state that $j_\Psi\colon \Omega_\mathcal{Z} \to \Omega_\mathcal{Z}$ is $(\mathrm{id}_{\Omega_\mathcal{X}}, j_\Lambda)$, where j_Λ takes (μ, ν) in Λ to $(\mu, o_*(\mu))$ where $o_*\colon f_*\Omega_\mathcal{X} \to \Omega_\mathcal{S}$ has been described. Note that $j_\Psi(\mathit{false}) = \mathit{false}$, which means that the (open) embedding Ψ is *dense*. Of course, the open Ψ can also be described by $\Psi_!(1) = (1, 0, 0)$, a subobject of the terminal object $(1, 1, \mathrm{id}_1)$ of $\mathcal{Z}$ (or, equivalently, a global section $(1, 1, \mathrm{id}_1) \to \Omega_\mathcal{Z}$ given by $(\mathit{true}, (\mathit{true}, \mathit{false}))$, which is the smallest such that $j_\Psi(s) = \mathit{true}$).

The Lawvere-Tierney topology corresponding to the closed complement Φ of the open embedding Ψ is then easy enough to describe: $j_\Phi\colon \Omega_\mathcal{Z} \to \Omega_\mathcal{Z}$ is given by $j_\Phi = (\mathit{true}, (\mathit{true}, 1_{\Omega_\mathcal{S}}))$. **(Interrupted...)**

2002-12-21:053

Contrary to what I naïvely believed in **2002-12-12:052**, the fiber product of topoi is not so easy to define (as a matter of fact, if we take the definition of elementary topoi by Lawvere, Tierney, MacLane, Moerdijk &al, which only demands the existence of finite limits and not arbitrary small limits, it is not even clear that the fiber product exists,

because certainly arbitrary finite limits do not exist, as there is no terminal topos: the topos of sets or that of finite sets come just short of satisfying the conditions).

Suppose $f\colon \mathcal{X} \to \mathcal{S}$ and $g\colon \mathcal{Y} \to \mathcal{S}$ are geometric morphisms. The (two-)fiber product $\mathcal{X} \times_{\mathcal{S}} \mathcal{Y}$ will certainly not have as objects things like pairs consisting of an object of $\mathcal{X}$ and one of $\mathcal{Y}$: this kind of construction might succeed in defining a (braided?) coproduct, but not a (fiber) product. Rather, the intuition we must follows is similar to this: f more or less defines $\mathcal{X}$ as as internal topos in $\mathcal{S}$, and we must mirror this construction within $\mathcal{Y}$.

Here is one case when things are simple enough: assume $\mathcal{S}$ is the topos of sets, and $\mathcal{X}$ is the topos of sheaves (of sets) on a topological space X, where f_* takes such a sheaf to the set of its global sections and f^* takes a set to the corresponding constant sheaf on X. And then the subobject classifier $\Omega_{\mathcal{X}} = \Omega_X$ is externally the sheaf of open sets of X and internally the set of subobjects of 1 (that is, f^*1); of course, $f_*\Omega_{\mathcal{X}}$ is the *set* of open sets of X, that is, the topology on X: so the set X and the subset $f_*\Omega_{\mathcal{X}}$ of the powerset of X, together, determine $\mathcal{X}$ and f. So our goal is to transfer them from the topos $\mathcal{S}$ of sets to the topos $\mathcal{Y}$ through the geometric morphism g. Consider the object g^*X of $\mathcal{Y}$ and the subobject $g^*f_*\Omega_{\mathcal{X}}$ of the object $(\Omega_{\mathcal{Y}})^{g^*X}$ of subobjects of g^*X; unfortunately, it is not always true that $g^*f_*\Omega_{\mathcal{X}}$ is closed under arbitrary unions, but we can take the closure in question, call it $\Omega_{X,\mathcal{Y}}$, say. We can now define the topos $\mathcal{Z}$ of sheaves $\mathcal{Y}$-sheaves on g^*X for the topology $\Omega_{X,\mathcal{Y}}$: an object of $\mathcal{Z}$ is a datum consisting of an object Z of $\mathcal{Y}$ and an arrow $Z \to \Omega_{X,\mathcal{Y}}$, together with restriction data (technically, an arrow $\Delta \times_{\Omega_{X,\mathcal{Y}}} Z \to Z$ where $\Delta \to \Omega_{X,\mathcal{Y}}$ is the subobject of $\Omega^2_{X,\mathcal{Y}}$—equipped with the second projection — that is the graph of the relation $\leq$ of inclusion) that satisfies all the usual conditions for being a sheaf, which we won't bother to write down because they're such a pain. This topos $\mathcal{Z}$, if my intuition isn't to wrong, should be (up to equivalence) the (two-)fiber product of $\mathcal{X}$ and $\mathcal{Y}$ over $\mathcal{S}$.

Even more specifically, suppose still that $\mathcal{S}$ is the topos of sets and $\mathcal{X}$ the topos of sheaves on some topological space X, but also that $\mathcal{Y}$ is the topos of sheaves on some topological space Y. Then g^*X is the constant sheaf on Y with value X, and $g^*f_*\Omega_X$ is the constant sheaf on Y with value the set $f_*\Omega_X$ of open sets of X: each section of the latter (on an open set U of Y, say) can be viewed as a subsheaf of g^X (restricted to the open set U in question). The completion $\Omega_{X,\mathcal{Y}}$ of $g^*f_*\Omega_X$ is the sheaf on Y whose sections on an open set U of Y are open sets of $X \times U$. So it is reasonably clear that the topos $\mathcal{Z} = \mathcal{X} \times_{\mathcal{S}} \mathcal{Y}$ is (equivalent to) the topos of sheaves on the topological space $Z = X \times Y$. This is rather reassuring.

It would be nice to have a definition of a topological space object in a topos, in order to be able to state that g^*X, equipped with the completion $\Omega_{X,\mathcal{Y}}$ of $g^*f_*\Omega_X$, is such an object. The following looks tempting: a topological space object in a topos $\mathcal{T}$ is an object E of $\mathcal{T}$ together with a subobject of the powerset object $(\Omega_{\mathcal{T}})^E$ of E that is closed under finite intersections and arbitrary unions (and hence contains the empty and full subobjects of E). But are there perhaps unforeseen difficulties (for example in the notion of "finite intersections")? This needs to be more carefully verified.

Now more generally, if $f\colon \mathcal{X} \to \mathcal{S}$ and $g\colon \mathcal{Y} \to \mathcal{S}$ are arbitrary geometric morphisms between arbitrary topoi, we can attempt to construct the (2-)fiber product as follows. First, using a folkloric theorem, we can factor (in an essentially unique way) f and g as a surjection followed by an embedding; it is then sufficient to construct the fiber product in the case where f and g are both surjections (that is, f^* and g^* are faithful), or both embeddings (that is, f_* and g_* are fully faithful). In the case where they are both surjections, we know $\mathcal{X}$ to be (equivalent to) the category of coälgebras on a left-exact intarnal comonad in $\mathcal{S}$ (see **2002-03-12:035**), and it is then probably not too difficult to transfer the comonad in question from $\mathcal{S}$ to $\mathcal{Y}$ using g, and the topos of coälgebra on the internal comonad in question in $\mathcal{Y}$ should be the desired fiber product. In the case where f and g are both embeddings, then $\mathcal{X}$ and $\mathcal{Y}$ are (equivalent to) the topoi of sheaves on Lawvere-Tierney topologies $j_{\mathcal{X}}$ and $j_{\mathcal{Y}}$ on $\mathcal{S}$ (see **2002-12-05:051**): then although it is probably not the case that $j_{\mathcal{X}} \circ j_{\mathcal{Y}}$ is a Lawvere-Tierney topology, the upper bound of $(j_{\mathcal{X}} \circ j_{\mathcal{Y}})^{\circ k}$ for all $k \in \mathbb{N}$ is probably well-defined ans certainly a Lawvere-Tierney topology, whose topos of sheaves should then be the desired fiber product.

2002-12-21:054

A wee bit of intuitionist mathematics.

First, concerning terminology, we say that the logic is *boolean* (i.e. classical) iff $(\neg\neg p) \Longrightarrow p$ holds for every p, or, equivalently, iff $p \vee \neg p$ holds for every p. We naturally always have $p \Longrightarrow \neg\neg p$; even if the converse holds, that is $(\neg\neg p) \Longrightarrow p$ for *some* p, we cannot conclude that $p \vee \neg p$ holds for *that* p; on the other hand, if $p \vee \neg p$ then certainly $(\neg\neg p) \Longrightarrow p$. We also have $(\neg p) \Longleftrightarrow (\neg\neg\neg p)$ for all p, but $(\neg p) \vee (\neg\neg p)$ does not hold in general. To assume that $(\neg p) \vee (\neg\neg p)$ holds for all p is weaker than to assume that $p \vee \neg p$ hold for all p: in the latter case, the logic is boolean; in the former, we shall say that it is *quasi-boolean*. We have remained vague as to what "the logic" means. These terms can apply, for example, to a Heyting algebra, such as the complete internal Heyting algebra of truth values in a topos, or (a direct image of the former) the complete Heyting algebra of open sets in a topological space. In this particular case, the logic is boolean exactly when every open set is closed (a very strong condition, which, even in presence of very mild separation axioms, implies that the space is discrete), or, equivalently, that every open set is regular; now, to say that the logic is quasi-boolean just means that the closure of an open set is open, or, in other words, that the space is "extremally disconnected".

Beyond the empty set $\varnothing$ (or simply 0) and the singleton 1, we have a very important set Ω, the set of truth values, which is the powerset $\mathcal{P}(1)$ of the singleton. More generally, for every subset $E' \subseteq E$ (technically, equivalence class of monomorphisms, i.e. injective functions) we have a characteristic function $\chi\colon E \to \Omega$ such that E' is precisely the set of $x \in E$ such that $\chi(x) = \mathit{true}$. That is, Ω is endowed with an element true, or, more precisely, a map $\mathit{true}\colon 1 \to \Omega$, and every injection $E' \to E$ is the pullback of $\mathit{true}\colon 1 \to \Omega$ by a unique $\chi\colon E \to \Omega$ which is the characteristic function of (the image of) the injection. The unique function $0 \to 1$ (the empty subset of the singleton) defines another map $1 \to \Omega$, that is, another element of Ω, which is called false. Since $\neg(\mathit{true} = \mathit{false})$, the two maps $1 \to \Omega$ given by true and false define a map $2 \to \Omega$ (where $2 = 1 + 1$ is the disjoint union of two singletons, i.e. the set with two elements) that is (always) an injection, and that is a surjection exactly when the logic is boolean.

If E is any set, the diagonal $E \to E^2$, which is always injective (and thus defines a subset of E^2) has a characteristic function $E^2 \to \Omega$ which is called *equality*. A set E is said to have *at most one* element iff the image of the equality function $E^2 \to \Omega$ falls in the singleton of true: this is trivially equivalent to saying that the unique function $E \to 1$ is injective, so E is a subset of the singleton. More generally, let us say that a set E is *precise* iff the image of the equality function $E^2 \to \Omega$ falls in the doubleton $2 \to \Omega$ of true and false (we have already pointed out that this arrow is injective). In Ω we have p equal to (the truth value of) $p = \mathit{true}$ for all p (this means that the characteristic function $\Omega \to \Omega$ of $\mathit{true}\colon 1 \to \Omega$ is the identity); and we define $\mathit{not}(p)$ to be (the truth value of) $p = \mathit{false}$ (again, we define $\mathit{not}\colon \Omega \to \Omega$ to be the caharacteristic function of the singleton $\mathit{false}\colon 1 \to \Omega$); we define $\mathit{and}\colon \Omega^2 \to \Omega$ to be the characteristic function of $(\mathit{true}, \mathit{true})\colon 1 \to \Omega$; and we define $p \Longrightarrow q$, or $p \leq q$ (in Ω, for all $p, q \in \Omega$: that is, we are defining an arrow $\Omega^2 \to \Omega$) to mean $(p \wedge q) = p$. As for constructing the $\mathit{or}\colon \Omega^2 \to \Omega$ arrow, the following should work: take the arrow $\Omega^3 \to \Omega$ given by $(p, q, r) \mapsto (p \Longrightarrow r) \wedge (q \Longrightarrow r)$, which gives an arrow $h\colon \Omega^2 \to \Omega^\Omega$ by abstracting the third (r) variable, and consider the constant function $i\colon \Omega^2 \to \Omega^\Omega$ with value the identity function $\Omega \to \Omega$ (seen as a singleton $1 \to \Omega^\Omega$): the value of $h = i\colon \Omega^2 \to \Omega$ (that is, compose (h, i) with the equality relation $(\Omega^\Omega)^2 \to \Omega$) is precisely the desired $\mathit{or}\colon \Omega^2 \to \Omega$; it can also be defined as the characteristic function of the image of the morphism $2 \times \Omega \to \Omega^2$ which sends $p \in \Omega$ to (p, true) for the first component and to (true, p) for the second—the problem with this definition is that it requires "the image" of a non injective function to be known (in a topos, this comes logically later, so it would be begging the question). But let us abandon such logical subtleties and any pretense at distinguishing, for example, $p \vee q$ (the logical statement) from $\mathit{or}(p, q)$ (its semantic interpretation, an element of Ω). Anyway, a set E is precise iff for all $x, y \in E$ we have $x = y \vee \neg x = y$.

2003-10-18:055

The answer to the "am I just being utterly naïve" question in **2001-12-18:011** is "yes": there are true statements in $\mathbb{N}$ which are not decidable in PA^∞ (the system obtained by Gödelizing Peano's axioms to the point where they cannot be Gödelized any further). Indeed, by induction on α we see that ZF provides a model of PA^α, hence proves $\mathrm{Consis}(\mathrm{PA}^\alpha)$, so ZF is stronger than PA^∞. But even ZF does not settle all arithmetic questions (even though it proves

$\mathrm{Consis}(\mathrm{PA})$, $\mathrm{Consis}(\mathrm{PA}^1)$ and so on): for example, it does not settle $\mathrm{Consis}(\mathrm{ZF})$, so in particular PA^∞ does not. This means that PA^∞ is not complete.

But is this reasoning correct? The induction is dubious at transfinite α; the problem being that the way induction breaks down, and how far it can go (the smallest countable ordinal that cannot be defined by a recursive well-order on $\mathbb{N}$, perhaps? or by one that is definable in the language of arithmetic?) is very unclear.

2003-10-18:056

Peano's axioms PA can be defined with no particular difficulty in intuitionist logic. We can define a Gödel statement G in the language of PA stating that "G is not a theorem of PA using classical logic", and a Gödel statement $\tilde{G}$ in the same langage stating that "$\tilde{G}$ is not a theorem of PA using classical logic".

Now G is not a theorem of PA (if PA is classically consistent, which we assume) in classical logic (for if it were so, then G would be true in $\mathbb{N}$, hence unprovable, a contradiction), so it is also certainly not the case in intuitionist logic; now this fact can be proven, with this very argument, within PA even using intuitionist logic, except for the assumption that PA is classically consistent, so "G is not a theorem of PA using classical logic", i.e. G itself, is a consequence of $\mathrm{PA} \wedge \mathrm{Consis}(PA)$ even using intuitionist logic. And certainly $\neg G$ is not a theorem of PA (using classical logic, and *a posteriori* using intuitionist logic) if PA is classically consistent, and this fact is provable within PA even using intuitionist logic.

Concerning $\tilde{G}$ we can say that $\tilde{G}$ is not a theorem of PA using intuitionist logic, provided PA is intuitionistically consistent (we write this $\widetilde{\mathrm{Consis}}\,\mathrm{PA}$), and similarly for $\neg\tilde{G}$. So $\tilde{G}$ is a consequence of $\mathrm{PA} \wedge \widetilde{\mathrm{Consis}}\,\mathrm{PA}$ using intuitionist logic.

Questions: is $\tilde{G} \vee \neg\tilde{G}$ a consequence of PA using intuitionist logic? Is $\tilde{G}$ a consequence of PA using classical logic?

My ideas on the subject are still very fuzzy.

2003-10-18:057

(Here k is an arbitrary (commutative) ring.) We call $k[\varepsilon] = k[t]/(t^2)$ the ring of "dual numbers" (a horrible terminology), and of course for any (commutative) k-algebra A we let $A[\varepsilon] = A[t]/(t^2) = A \otimes_k k[\varepsilon]$.

If X is a sheaf (for some reasonable topology) on the category $\mathbf{AffScm}_k$ of affine k-schemes (see **2002-03-24:039** and **2001-12-21:013** for some background), we call TX the sheaf taking a commutative k-algebra A to $(TX)(A) = X(A[\varepsilon])$ (and morphisms in the obvious way): this is actually $X^{\mathrm{Spec}\, k[\varepsilon]}$, where the exponent denotes an internal Hom in the category of sheaves (over affine k-schemes). We call TX the *(total) tangent bundle* to X.

If X is an algebraic affine k-scheme, that is, $X = \mathrm{Spec}(k[t_1, \ldots, t_n]/(f_1, \ldots, f_r))$ where $f_1, \ldots, f_r$ are relations on the variables $t_1, \ldots, t_n$, then TX is again of this kind, and can explicitely be described as $TX = \mathrm{Spec}(k[t_1, \ldots, t_n, t'_1, \ldots, t'_n]/(f_1, \ldots, f_r, df_1, \ldots, df_r))$ where df_j is the (formal) total differential of f_j, namely $df_j = \frac{\partial f_j}{\partial t_1} t'_1 + \cdots + \frac{\partial f_j}{\partial t_n} t'_n$. Indeed, X represents the functor taking a k-algebra A to the set of n-tuples $(x_1, \ldots, x_n)$ of elements of A satisfying the relations $f_1, \ldots, f_r$; and TX is the set of n-tuples of elements of $A[\varepsilon]$, seen as $(x_1 + \varepsilon x'_1, \ldots, x_n + \varepsilon x'_n)$ with $x_1, \ldots, x_n, x'_1, \ldots, x'_n$ in A, satisfying the same relations, which gives us the stated relations on $x_1, \ldots, x_n$, $x'_1, \ldots, x'_n$. Actually, *mutatis mutandis*, this still holds for an arbitrary (not necessarily finite) family of generators and relations (and in particular, TX is affine whenever X is affine).

Taking X to TX is functorial in X: if $Y \to X$ is a morphism of sheaves, then we get a morphism $TY \to TX$ which on a given k-algebra A is seen as the map $Y(A[\varepsilon]) \to X(A[\varepsilon])$ given by the original morphism $Y \to X$ (this is also clear if we see TX as $X^{\mathrm{Spec}\, k[\varepsilon]}$).

Now when X is *(representable by) an (affine) k-scheme*, we have more: then TX has a natural structure as an $\mathscr{R}$-module bundle over X (where $\mathscr{R} = \mathrm{Spec}\, k[t]$); in other words, there are morphisms of identity $X \to TX$, of addition $TX \times_X TX \to TX$, and of scalar multiplication $\mathscr{R} \times_{\mathrm{Spec}\, k} TX \to TX$, all defined over X, which satisfy the obvious diagrams. Actually, identity and scalar multiplication can be defined in full generality: identity $X \to TX$ over a k-algebra A is the map $X(A) \to X(A[\varepsilon])$ taking an element $x \in X(A)$ to its inverse image by the arrow $A[\varepsilon] \to A$

which sends ε to zero; scalar multiplication $\mathscr{R} \times TX \to TX$ over a k-algebra A is the map $A \times X(A[\varepsilon]) \to X(A[\varepsilon])$ taking a scalar $\lambda \in A$ and an element $x \in X(A[\varepsilon])$ to the inverse image of x by the arrow $A[\varepsilon] \to A[\varepsilon]$ which sends ε to $\lambda\varepsilon$. However, there is no way to define addition $TX \times_X TX \to TX$ in full generality: if we try to define a morphism $X(A[\varepsilon]) \times_{X(A)} X(A[\varepsilon]) \to X(A[\varepsilon])$ canonically in A, we have no idea what to do given two elements of $X(A[\varepsilon])$ whose images in $X(A)$ (by the inverse image by $A \to A[\varepsilon]$) coincide; now if X is actually an affine scheme, then $X(A[\varepsilon]) \times_{X(A)} X(A[\varepsilon]) = X(A[\eta,\zeta])$ where $A[\eta,\zeta] = A[y,z]/(y^2, yz, z^2)$ (this follows from the description given above of TX when X is affine), and then we can use the arrow $A[\varepsilon] \to A[\eta,\zeta]$ sending ε to $\eta + \zeta$.

Now for the usual topologies on the category of affine k-schemes (e.g., fp[qc]), there exist sheaves X such that $X(A[\varepsilon]) \times_{X(A)} X(A[\varepsilon])$ does not coincide with $X(A[\eta,\zeta])$: this means that for such X the tangent bundle $TX \to X$ cannot naturally acquire an $\mathscr{R}$-module bundle structure. This is most unfortunate. This hints that it would make much sense to look for topologies for which the two arrows $\operatorname{Spec} A[\varepsilon] \rightrightarrows \operatorname{Spec} A[\eta,\zeta]$ sending on the one hand η to ε and ζ to 0 and on the other hand η to 0 and ζ to ε, would be a covering. Question: is there a natural way to define a topology that would allow such a covering (*among many others*, naturally)? So that $TX \to X$ would naturally have an $\mathscr{R}$-module bundle structure for any sheaf X for that topology (with, of course, the arrows $TY \to TX$ deduced from $Y \to X$ by functoriality, being morphisms)—among other properties. Note for further thoughts: what about the *canonical* topology?

2003-10-26:058

To answer a question asked (more or less implicitly) in **2003-10-18:057**, the arrow $\operatorname{Spec} k[\varepsilon_1] \uplus \operatorname{Spec} k[\varepsilon_2] \to \operatorname{Spec} k[\eta,\zeta]$ (where $k[\varepsilon_i] = k[x]/(x^2)$ and $k[\eta,\zeta] = k[y,z]/(y^2, yz, z^2)$) given by $k[\eta,\zeta] \to k[\varepsilon_1] \times k[\varepsilon_2]$ taking η to $(\varepsilon_1, 0)$ and ζ to $(0, \varepsilon_2)$ is *not* a covering for the canonical topology (or, consequently, for any "reasonable") topology on the category of affine k-schemes. Indeed consider its pullback by $\operatorname{Spec} k[\delta] \to \operatorname{Spec} k[\eta,\zeta]$ (where again $k[\delta] = k[t]/(t^2)$) given by $k[\eta,\zeta] \to k[\delta]$ taking both η and ζ to δ. Now we can describe $k[\eta,\zeta]$-algebras as data consisting of a k-algebra A together with two elements u and v of A such that $u^2 = uv = v^2 = 0$; tensoring such an algebra with $k[\varepsilon_1] \times k[\varepsilon_2]$ gives the direct product $(A/(u)) \times (A/(v))$ of the quotients $A/(u)$ and $A/(v)$; so if A is $k[\delta]$ with $u = v = \delta$ as proposed, then that tensor is just $k \times k$, and since $\operatorname{Spec} k \to \operatorname{Spec} k[\varepsilon]$ is certainly not a covering, we lose.

To summarize, in the category of affine k-schemes, the arrow $\operatorname{Spec} k[\varepsilon_1] \uplus \operatorname{Spec} k[\varepsilon_2] \to \operatorname{Spec} k[\eta,\zeta]$ is an effective epimorphism, but not a *universal* effective epimorphism (i.e., covering for the canonical topology). What happens if we try to consider sheaves X such that $X(V \times_U V) \rightrightarrows X(V) \to X(U)$ is exact for all effective epimorphisms $V \to U$ rather than just universal effective epimorphisms? Do we get something nasty (I imagine the resulting category of such X is not a topos)? Certainly all representable X are of this kind (and perhaps even all k-schemes X?). Uh...

2003-10-26:059

Let p be a prime. The Teichmüller map is a morphims of groups $\eta\colon \mathbb{F}_p^\times \to \mathbb{Z}_p^\times$ such that $\overline{\eta(\bar{x})} = \bar{x}$. Extend it to $\eta\colon \mathbb{F}_p \to \mathbb{Z}_p$ by taking 0 to 0. Unfortunately this is not additive, but it is at least multiplicative: $\eta(\bar{x}\bar{y}) = \eta(\bar{x})\eta(\bar{y})$.

Now any element x of $\mathbb{Q}_p^\times$ can be uniquely written $\eta(\bar{x}_0)p^{v(x)}(1+p)^{\alpha}(x)$ where $v(x)$ is of course the valuation of x and $\bar{x}_0 \in \mathbb{F}_p^\times$ is the reduction mod p of $p^{-v(x)}x$, and $\alpha(x) \in \mathbb{Z}_p$. This describes $\mathbb{Q}_p^\times$ as isomorphic to $\mathbb{F}_p^\times \times \mathbb{Z} \times \mathbb{Z}_p$. Define a symbol $\frac{d^*}{dp}\colon \mathbb{Q}_p \to \mathbb{Q}_p$ by letting $\frac{d^*x}{dp} = \eta(\bar{x}_0)\,[v(x) + (v(x) + H\,\alpha(x))p]\; p^{v(x)-1}\,(1+p)^{\alpha(x)-1}$ for $x \neq 0$ and $\frac{d^*0}{dp} = 0$; here, $H \in \mathbb{Q}_p$ is some constant of definition ("fiddle factor"), $H = \frac{d^*(1+p)}{dp}$. This symbol is not additive, but it satisfies $\frac{d^*}{dp}(xy) = x\,\frac{d^*y}{dp} + \frac{d^*x}{dp}\,y$ for all $x, y \in \mathbb{Q}_p$. Perhaps $H = 1$ is the most natural choice—and perhaps not.

It does not *seem* possible (even by fiddling with the value of H) to obtain the most naïve Taylor formula (for $x \in \mathbb{Z}_p$)

$$x = \eta(\bar{x}) + \eta\left(\overline{\frac{d^*}{dp}x}\right)p + \frac{1}{2}\,\eta\left(\overline{\frac{d^{*2}}{dp^2}x}\right)p^2 + \frac{1}{6}\,\eta\left(\overline{\frac{d^{*3}}{dp^3}x}\right)p^3 + \cdots$$

—but note that the formula *is* valid mod p^2 so long as H is 1 mod p. Since $\frac{1}{2}\eta(\bar{t})$ is not $\eta(\overline{\frac{1}{2}t})$ and neither is $\frac{d^*}{dp}(\frac{1}{2}t)$ equal to $\frac{1}{2}(\frac{d^*}{dp}t)$, there are dozens of ways the formula could be (less "naïvely") written: is it perhaps true that for an intelligently chosen H and an intelligent way of writing the formula, we have a positive result not just mod p^2?

Another natural question: how about demanding that the image of $\mathbb{Q}$ by $\frac{d^*}{dp}$ falls in $\mathbb{Q}$ (seen within $\mathbb{Q}_p$, naturally), or perhaps at least the algebraic closure of $\mathbb{Q}$ in $\mathbb{Q}_p$?

2003-11-18:060

What difficulties do we encounter in trying to construct relativistic quantum field theory in the most naïve way possible? Assume, say, we wish to perform second quantization of a real self-interacting scalar field ϕ satisfying the field equation $(\Box^2 + m^2)\phi + \alpha\phi^3 = 0$ (here, $\Box^2$ is the Dalembertian given by $\Box^2 = \frac{\partial^2}{\partial t^2} - \frac{\partial^2}{\partial x^2} - \frac{\partial^2}{\partial y^2} - \frac{\partial^2}{\partial z^2}$, and $\alpha > 0$ is a self-interaction parameter), which comes from a Lagrangian density $\mathcal{L} = \frac{1}{2}g^{\mu\nu}\frac{\partial\phi}{\partial x^\mu}\frac{\partial\phi}{\partial x^\nu} - \frac{1}{2}m^2\phi^2 - \frac{1}{4}\alpha\phi^4$: if not too much nonsense lies behind variational equations at the core, then the field equation should state exactly the fact that ϕ is such that $\int \mathcal{L}\, d^4\boldsymbol{x}$ is extremal (make mathematical sense out of this!); or should ϕ be constrained so that $\int \phi^2\, d^4\boldsymbol{x} = 1$?

Now basically we would like to construct a Very Large (Indeed) Hilbert space of functions having one variable $\xi_{\boldsymbol{x}}$ for each space-time point $\boldsymbol{x}$. Then the world state is determined by a unitary vector Φ in this space, and for each $\boldsymbol{x}$, $\phi(\boldsymbol{x})$ becomes a linear operator $\frac{1}{\sqrt{2}}(\xi_{\boldsymbol{x}} + \frac{\partial}{\partial\xi_{\boldsymbol{x}}})$ on acting on Φ (probably highly unbounded): note that $\phi^\dagger(\boldsymbol{x}) = \frac{1}{\sqrt{2}}(\xi_{\boldsymbol{x}} - \frac{\partial}{\partial\xi_{\boldsymbol{x}}})$ (assuming the space is any bit sane, which, of course, is a very dangerous assumption) so that $\phi(\boldsymbol{x})\,\phi^\dagger(\boldsymbol{y}) - \phi^\dagger(\boldsymbol{y})\phi(\boldsymbol{x}) = \delta(\boldsymbol{x} - \boldsymbol{y})$ for some meaning of δ and up to some normalization. (This is a lot of hand-waving, now, of course.) The vacuum state would be $\prod_{\boldsymbol{x}} e^{-\frac{1}{2}\xi_{\boldsymbol{x}}^2}$, assuming there were a way for this product to make sense (probably by defining all other functions somehow with respect to this one). Now can we make something of the Lagrangian variational principle? Is there some way to make the whole thing a little more meaningful on mathematical grounds (I'm not asking for a solution to relativistic QFT, of course, merely a way to state the problem).

2003-11-18:061

A typical independence result in the absence of Choice: it is consistent that there exists an infinite set of reals without a(n infinite) countable subset. How do we do this?

As a forcing condition we take the partially ordered set P of finite functions $\omega^2 \to 2$, partially ordered by inclusion (that is, $p \leq q$, or "p is stronger than q" iff $p \supseteq q$ as a finite set of pairs). Embed P in the boolean algebra $\mathbf{B}$ of regular open sets of 2^{ω^2} (with the product topology) by taking p to the clopen (and hence regular open!) set $e(p)$ consisting of all functions $\omega^2 \to 2$ which extend p: evidently this embeds P as a dense subset of $\mathbf{B} \setminus \{\varnothing\}$ (the clopen sets in question form a basis for the topology of 2^{ω^2}). For commodity we will write $\top$ and $\bot$ for the maximal and minimal elements of $\mathbf{B}$. We construct the boolean-valued model $V^{\mathbf{B}}$ as usual. For $n \in \omega$ we let $\boldsymbol{x}_n$ be the name which takes any $k \in \omega$ (or rather, the canonical name $\check{k}$ for k) to the truth value $\{(n, k, 1)\} \in P$: thus $\{(n, k, 1)\} \Vdash \check{k} \in \boldsymbol{x}_n$ (and, of course, $\{(n, k, 0)\} \Vdash \check{k} \notin \boldsymbol{x}_n$). After quotienting by a generic ultrafilter, the $\boldsymbol{x}_n$ determine a sequence of generic reals (it is, of course, equivalent to define a single generic real or an ω-sequence of such, since ω^2 can be put in "canonical" bijection with ω; the point of using a sequence appears when we start introducing permutation groups).

Now consider the group $G = \mathfrak{S}(\omega)$ of bijections $\omega \to \omega$ (which acts on ω by $\sigma \cdot n = \sigma(n)$). Make G act on $\mathbf{B}$ by $\sigma \cdot u = \{f : \omega^2 \to 2 : ((n, k) \mapsto (f(\sigma(n)), k)) \in u\}$ (and on P by $\sigma \cdot \{(n, k, v)\} = \{(\sigma(n), k, v)\}$ so that $\sigma \cdot e(p) = e(\sigma \cdot p)$). Define $\mathscr{H}$ the set of subgroups of G which contain the fixator subgroup of a finite subset of ω: then $\mathscr{H}$ is a normal subgroup. As usual, we say that an element of $\mathbb{B}$ is $\mathscr{H}$-symmetric, or simply, symmetric, when its stabilizer is in $\mathscr{H}$. And similarly for an element of $V^{\mathbf{B}}$ (more, precisely, a name); and we define hereditarily symmetric names in the obvious manner. Evidently, $\boldsymbol{x}_n$ has a symmetric (and therefore hereditarily symmetric) name: its stabilizer is the set of $\sigma \in G$ which fix n (and more generally $\sigma \cdot \boldsymbol{x}_n = \boldsymbol{x}_{\sigma(n)}$). The name $\boldsymbol{X}$, which takes $\boldsymbol{x}_n$ to $\top$ for all n, is also symmetric (and hence hereditarily symmetric). And $\top \Vdash \boldsymbol{x}_m \neq \boldsymbol{x}_n$ for all $m \neq n$ because below any forcing condition it is possible to force $\ell \notin \boldsymbol{x}_m$ and $\ell \in \boldsymbol{x}_n$ for some $\ell \in \omega$. Therefore $\boldsymbol{X}$ is infinite (in the generic

ultrafilter quotient, or simply in the boolean-valued model in the sense that the truth value of "$\boldsymbol{X}$ is infinite" is $\top$), so it is also in the symmetric model.

Now assume there exists some hereditarily symmetric name $\boldsymbol{h}$ and some forcing condition $p_0 \in P$ such that p_0 forces "$\boldsymbol{h}$ is an injection $\omega \to \boldsymbol{X}$". Let E be a finite subset of ω such that the fixator of E stabilizes $\boldsymbol{h}$. Since p_0 forces "the image of $\boldsymbol{h}$ is not contained in $\{\boldsymbol{x}_n : n \in E\}$" (note that this makes sense since E is finite), there is $p \leq p_0$, $i \in \omega$ and $n \notin E$ such that $p \Vdash \boldsymbol{h}(i) = \boldsymbol{x}_n$. Now find $\sigma \in G$ such that σ fixes E, $\sigma \cdot p$ is compatible with p and $\sigma(n) = n' \neq n$ (it suffices to take for σ the permutation which exchanges n with some n' greater than anything mentioned in E or p): then if $q = p \cup (\sigma \cdot p)$ is the conjunction of p and $\sigma \cdot p$ (which makes sense since p and $\sigma \cdot p$ are compatible), we see that $q \Vdash \boldsymbol{h}(i) = \boldsymbol{x}_n$ and $q \Vdash \boldsymbol{h}(i) = \boldsymbol{x}_{n'} \neq \boldsymbol{x}_n$, a contradiction.

Therefore, in the symmetric model, $\boldsymbol{X}$, although an infinite set of reals, has no (infinite) countable subset.

It is instructive to see what happens if we try to show that (in the symmetric model) $\boldsymbol{X}$ cannot be totally ordered (an absurdity, since it is a set of reals, so it has a canonical total order!): we take a hereditarily symmetric name $\boldsymbol{t}$ and some forcing condition $p_0 \in P$ such that p_0 forces "$\boldsymbol{t}$ is a total order on $\boldsymbol{X}$". Again, let E be a finite subset of ω such that the fixator of E stabilizes $\boldsymbol{t}$. Then find $p \leq p_0$ and $m, n \notin E$ such that $p \Vdash (\boldsymbol{x}_m, \boldsymbol{x}_n) \in \boldsymbol{t}$. Only, this time: if σ is the permutation which exchanges m and n, there is no reason that p and $\sigma \cdot p$ should be compatible; and if we seek a permutation σ such that p and $\sigma \cdot p$ are compatible, we can exchange m with some larger m' or n with some larger n', but there is no reason why we should be able to exchange m and n (so as to get a contradiction). In fact, Lévy has shown that every set can be totally ordered in this model. We can get a set that cannot be totally ordered, however, by considering a set of sets of reals (this is classical).

2003-11-30:062

Recall that the probability distribution function of a Gaussian variable with mean 0 and standard deviation 1 is $\frac{1}{\sqrt{2\pi}} e^{-x^2/2}$.

If X and X' are independent Gaussian variables with mean 0 and standard deviation 1, then the expectation of $\max(X, X')$ is $\frac{1}{\sqrt{\pi}}$ (according to Mathematica, or an easy computation), which is approximately $0.56418958354775628694807945$. The expectation of the maximum of *three* independent such variables is $\frac{3}{2\sqrt{\pi}}$ (according to Mathematica), or approximately $0.84628437532163443042211918$. However, the expectation of the maximum of *four* independent variables does not appear to be expressible in a simple form (at least, it is almost certainly not a rational over square root of pi, and it is also unknown to the Plouffe inverter); an approximate value is $1.02937537300396413205698 66$. Similarly for *five* independent variables in which case the value is close to $1.16296447364051961277226 80$.

Now consider the game where a player, whose goal is to maximize his score, must choose between two independent Gaussian variables with mean 0 and standard deviation 1, but only the value of the first variable is known when the choice must be made. That is, the player must choose between keeping X (whose value is then known) and taking X' (whose value is unknown). Evidently (?), the optimal strategy consists of keeping X when its value exceeds the expected value for X', which is 0: that is, take X when it is positive, otherwise take X'. If this strategy is followed, the expected score is $\frac{1}{\sqrt{2\pi}}$ (because the expectation of a Gaussian variable of mean 0 and standard deviation 1 subject to the condition that it be positive is $\sqrt{\frac{2}{\pi}}$). This is approximately $0.39894228040143267793994606$. Next, suppose the player has three chances instead of just two: he is shown a first Gaussian value, X, and can choose to stop here or move on to a second one, X', which he can either keep or take the third X'', which he then cannot reject. Then his optimal strategy is to keep the first variable, X, just in case its value exceeds $\frac{1}{\sqrt{2\pi}}$, otherwise demand to see the second X'', and choose that when its value is positive. The expectation for the final score is approximately $0.62974579055999158292799866$.

Another interesting procedure in this line of thought is the following *game of appeal*. This time, there are two players, the goal of the first player (the plaintiff) being to maximize the final score (damages) whereas the goal of the second player (the defendant) is to minimize it. A first Gaussian variable X of mean 0 and standard deviation 1 is dealt (the first hearing). After this, the plaintiff may choose to appeal or not: if he does, another variable X', with

the same distribution and independent of X, is dealt. Whether or not the plaintiff has appealed, the defendant may then choose to appeal: if he does, another variable (X' or X'', whichever it may be) is taken, again independent of the previous one(s) and with identical distribution. Lastly, if the defendant has appealed but the plaintiff has not appealed yet, the latter may appeal, which gives a third variable X''. The last chosen variable is the final score. Then the optimal strategy for both players is as follows: plaintiff appeals if the first score X is less than $-\frac{1}{\sqrt{2\pi}}$ (because appealing puts the defendant in the position of getting two chances, whereby by the previous analysis his best expectation is $-\frac{1}{\sqrt{2\pi}}$), whereas defendant appeals if the first score X is at greater than $\frac{1}{\sqrt{2\pi}}$. (Actually, this is a *petitio principii*, and this should be checked: but it seems that this is indeed the best possible strategy for both players.) A computation (largely done in Mathematica, but not too hard by hand either) shows that the variance of the overall score is $1 - \frac{e^{-1/(4\pi)}}{\pi}$ or approximately $0.706038760095823229070369 28$: that this is less than 1 is satisfactory, since the whole point behind the appeals process is to make the system more "just" (i.e. as close as possible to the ideal value 0); and the score's expectation is of course zero. Incidentally, the expected number of trial hearings (variables dealt in the whole process) is $\frac{1}{2}(5 - 3\,\mathrm{erf}(\frac{1}{2\sqrt{\pi}}))$, numerically barely more than two.

Now consider the same questions but changing the distribution to a uniformly distributed variable between $-\sqrt{3}$ and $\sqrt{3}$ (so that it also has expectation 0 and variance 1). Then the expectation of the max of two independent such variables is $\frac{3}{7}\sqrt{3}$ — this is better than in the Gaussian case. For three variables it is $\frac{9}{14}\sqrt{3}$, for four it is $\frac{69}{91}\sqrt{3}$ and for five it is $\frac{75}{91}\sqrt{3}$. Playing the game of maximizing the score, with only two chances, gives an score expectation of $\frac{1}{4}\sqrt{3}$ — again better than the Gaussian case. With three chances, $\frac{25}{64}\sqrt{3}$ — still better than for Gaussian (but we know that in the limit it will get worse, since in the Gaussian case the limit for infinitely many trials must tend to infinity whereas here it is $\sqrt{3}$). In the appeals game, the variance of the overall score is $\frac{49}{64}$ or 0.765625 (and the expected number of hearings is $\frac{17}{8}$).

Fascinating.

2003-11-30:063

A clarification (thanks to Joël Riou for some remarks on this). Let $i\colon X \hookrightarrow \mathbb{P}^N$ be a closed immersion, and $\mathscr{L} = i^*\mathscr{O}(1)$ the very ample invertible sheaf associated to the situation. We say that $\mathscr{L}$ is the sheaf of "hyperplane sections" of X embedded in $\mathbb{P}^N$ through i, but this *does not mean* that every global section of $\mathscr{L}$ is indeed determined by a hyperplane in $\mathbb{P}^N$: that is, the canonical map $H^0(\mathbb{P}^N, \mathscr{O}(1)) \to H^0(X, \mathscr{L})$ need not be surjective.

Here is an example: consider the map $i\colon \mathbb{P}^2 \hookrightarrow \mathbb{P}^4$ taking $(T_0 : T_1 : T_2)$ to $(T_0^2 : 2T_0T_1 : T_1^2 + 2T_0T_2 : 2T_1T_2 : T_2^2)$ (this is a form of the Veronese embedding). Then $\mathscr{L} = i^*\mathscr{O}(1)$ is the sheaf $\mathscr{O}(2)$ on $\mathbb{P}^2$ of (*all*) homogeneous polynomials of degree 2 in T_0, T_1, T_2, so for example $T_1^2 - 2T_0T_2$ is a global section of $\mathscr{L}$ on $\mathbb{P}^2$, whereas it is not a hyperplane section in the naïve sense: the image by i of the plane conic $T_1^2 - 2T_0T_2 = 0$ is a (rational) quartic curve in $\mathbb{P}^4$ which is not contained in any hyperplane.

Let us examine the previous example in a little more detail and explain *why*, in fact, $T_1^2 - 2T_0T_2 \in \Gamma(\mathbb{P}^2, i^*\mathscr{O}(1))$. First of all we have the sheaf $i^{-1}\mathscr{O}(1)$, which is a sheaf of *abelian groups* (or k-vector spaces, k being the base field) on $\mathbb{P}^2$, not of $\mathscr{O}_{\mathbb{P}^2}$-modules, namely the inverse image of $\mathscr{O}_{\mathbb{P}^4}(1)$ by i as a sheaf of abelian groups (or k-vector spaces); this is actually a sheaf of modules over $i^*\mathscr{O}_{\mathbb{P}^4}$ (a sheaf of rings); to define $i^*\mathscr{O}(1)$ we must then tensor $i^{-1}\mathscr{O}(1)$ with $\mathscr{O}_{\mathbb{P}^2}$ over $i^*\mathscr{O}_{\mathbb{P}^4}$. Now $T_1^2 - 2T_0T_2$ is not in $\Gamma(\mathbb{P}^2, i^{-1}\mathscr{O}(1))$. Nor can it be written as the tensor product of two *global* sections of $i^{-1}\mathscr{O}(1)$ and $\mathscr{O}_{\mathbb{P}^2}$. However, on each of the open sets $T_0 \neq 0$, $T_1 \neq 0$ and $T_2 \neq 0$, we can define a section of $i^*\mathscr{O}(1)$, respectively by $T_0^2 \otimes (\frac{T_1^2}{T_0^2} - 2\frac{T_2}{T_0})$, $(T_1^2 + 2T_0T_2) - 4(T_0T_1) \otimes (\frac{T_2}{T_1})$ and $T_2^2 \otimes (\frac{T_1^2}{T_2^2} - 2\frac{T_0}{T_2})$: these sections glue correctly on intersections, hence define a global section of $i^*\mathscr{O}(1)$.

Reverting to a more general picture, let $\mathscr{L}$ be any invertible sheaf on a proper (integral) variety X. Given any non-zero global sections $s_0, \dots, s_N$ of $\mathscr{L}$ on X, we can define a rational map $\varphi\colon X \dashrightarrow \mathbb{P}^N$ by taking x of X to $(s_0(x) : \cdots : s_N(x))$ (which makes sense up to scalar, exactly what we need), provided not all of $s_0, \dots, s_N$ vanish at x. This is defined as a morphism provided the s_i never all vanish simultaneously: this means exactly that the s_i generate $\mathscr{L}$ in the sense that the obvious morphism $\mathscr{O}_X^{N+1} \to \mathscr{L}$ is an epimorphism (as a morphism of sheaves of $\mathscr{O}_X$-modules). Moreover, φ is a closed immersion when it separates points and tangent vectors: this means (well, at

least for X smooth...) that φ is injective and that its differential is injective everywhere. The latter condition means that the matrix of partial differentials of s_i (with respect to some local system of parameters) is of rank the dimension of X plus one (the "plus one" comes from the fact that the direction colinear to $(s_0(x), \dots, s_N(x))$ is lost).

Of course, we can consider for the s_i a k-basis of all global sections of X. We then say that $\mathscr{L}$ is generated by its global sections when for all x of X there is a $s \in \Gamma(X, \mathscr{L})$ which does not vanish at x: so $\mathscr{L}$ defines a morphism $X \to \mathbb{P}(\Gamma(X, \mathscr{L}))$ (and more generally any invertible sheaf $\mathscr{L}$ having at least one non-zero global section defines a rational $X \dashrightarrow \mathbb{P}(\Gamma(X, \mathscr{L}))$); then $\mathscr{L}$ is very ample precisely when this morphism is a closed immersion. Note however, as seen above, that it is *not true* that any morphism from X to projective space is of this form; sometimes the target projective might be smaller (but certainly it can be written as the composition of such a morphism by a $\mathbb{P}(\Gamma(X, \mathscr{L})) \dashrightarrow \mathbb{P}^N$ which happens to be defined on all the image of X).

Some lines of further thought:

- Find an (illuminating) example of a $\mathscr{L}$ which has non-zero global sections but is not generated by them.
- The global sections $T_1T_2, T_0T_2, T_0T_1, T_0^2, T_1^2$ of $\mathscr{O}_{\mathbb{P}^2}(2)$ do not generate the latter; but what *do* they generate? I.e., what is the image of the morphism of sheaves $\mathscr{O}_{\mathbb{P}^2}^5 \to \mathscr{O}_{\mathbb{P}^2}(2)$ which they define? The rational map is a closed immersion of the blowup of $\mathbb{P}^2$ at $(0:0:1)$ within $\mathbb{P}^4$.
- Let $\mathscr{L}$ be an invertible sheaf on X generated by its global sections: what can be said about k-vector subspaces $E \subseteq \Gamma(X, \mathscr{L})$ such that E generates $\mathscr{L}$? (From the point of view of their combinatorial structure.) Same question, assuming $\mathscr{L}$ is very ample, about those E for which additionally the morphism thus defined is a closed immersion?
- What about rational maps? Can we give sense to them being a closed immersion of some kind? (Of course, it makes sense to ask for the map to be generically a closed immersion: can we demand more, something which would generalize being a closed immersion in the case of morphisms?) What is a "large" (or is it "big"?) invertible sheaf?

2003-12-06:064

Let us correct **2001-12-15:005** and try to get the correct definition of the projective space functor once and for all.

Let k be any (commutative) ring.

If $n \geq 0$, the projective n-space functor over k is the (covariant) functor from the category of k-algebras to the category of sets which takes a k-algebra A to the set $\mathbb{P}^n(A)$ defined as follows. Consider data $(f_1, \dots, f_m) \in A^m$ (for some m) such that the f_j generate the unit ideal in A and, for each j, data $(x_{j,0}, \dots, x_{j,n})$ with each $x_{j,i}$ belonging to the localization A_{f_j} of A which inverts f_j, such that $(x_{j,i})_i$ generates the unit ideal of A_{f_j} for all j and for all j, j' the two families $(x_{j,i})_i$ and $(x_{j',i})_i$ seen in $A_{f_jf_{j'}}$ (by the obvious canonical maps) coincide up to multiplication by a unit (which depends on j, j' but not on i); and identify two such data $((f_j), (x_{j,i}))$ and $((g_k), (y_{k,i}))$ when their union is a data satisfying the same conditions, in other words when for each j, k the two families $(x_{j,i})_i$ and $(y_{j,i})_i$ seen in $A_{f_jg_k}$ coincide up to multiplication by a unit; then the set of such data with such identifications is precisely what we call $\mathbb{P}^n(A)$. If $\varphi\colon A \to B$ is a morphism of k-algebra, we define $\mathbb{P}^n(\varphi)$ by taking data $((f_j), (x_{j,i}))$ as above to the obvious image $((\varphi(f_j)), (\varphi(x_{j,i})))$ (recall that localization is functorial, which lets us define $\varphi(x_{j,i})$). We can actually simplify the above definition slightly by observing that multiplying the $x_{j,i}$ by some power of f_j (depending only on j and not on i) we can assume that they are all in A.

Now rather than consider data $(x_{j,0}, \dots, x_{j,n})$ we can consider the kernel of the linear form on $A_{f_j}^{n+1}$ given by $(\xi_0, \dots, \xi_n) \mapsto x_{j,0}\xi_0 + \cdots + x_{j,n}\xi_n$. It should be possible to see why these kernels determine the data up to the prescribed equivalence relations, nor why it is possible to find a global $H \subseteq A^{n+1}$ which determines all the kernels in question by specialization. (This all shouldn't be difficult: for example, one important ingredient is that modules descend correctly — a family of modules M_j over the A_{f_j} with compatibility isomorphisms satisfying the nice cocycle condition determines a module M over A.) So the point is that $\mathbb{P}^n(A)$ is the set of sub-A-modules H of A^{n+1} such that A^{n+1}/H is locally free of rank 1 in the sense that for some $f_1, \dots, f_m$ generating the unit ideal in A the localizations inverting the f_j are all free of rank 1.

"Locally free" does not mean "free" (even over a ring — affine scheme — that is). The canonical example is to take $A = \mathbb{Z}[\sqrt{-5}]$, and for H the sub-A-module of A^2 generated by $(2, 1+\sqrt{-5})$ and $(1-\sqrt{-5}, 3)$: then A^2/H (which consists of the classes of elements of the form $(0, y)$ and $(1, y)$, and can be identified with the ideal generated by 2 and $1+\sqrt{-5}$ by taking $(x, y) \in A^2$ to $(1+\sqrt{-5})x - 2y$) is locally free of rank 1 (it is free, say, after inverting 2 or 3), but not free.

More generally, if E is a k-module, we can define $\mathbb{P}(E)$ to be the functor taking a k-algebra A to the set $\mathbb{P}(E)(A)$ of sub-A-modules F of $E \otimes_k A$ such that $(E \otimes_k A)/F$ is locally free of rank 1.

Note: for finitely presented modules, "locally free" and "projective" are synonymous.

2003-12-07:065

Some quick notes about intuitionist logic (also see **2002-12-21:054**).

For all natural numbers a and b we have $(a < b) \vee (a = b) \vee (a > b)$. This is proved by induction (for example, by induction on n it is easy to prove $(n = 0) \vee (n \geq 1)$, where $n \geq 1$ means that n is the successor of some natural number). Therefore the same statements holds for all integers, and for all rationals. Again: a rational number is either zero, or non-zero (in which case it is invertible). In topos semantics, the object of rationals is represented by the constant sheaf with value $\mathbb{Q}$, with the obvious addition and multiplication.

A real number can be defined as a pair (L, R) of sets of rationals, such that:

- If $r \in R$ and $s > r$ then $s \in R$; if $r \in L$ and $s < r$ then $s \in L$.
- If $r \in R$ then there exists $s < r$ such that $s \in R$; if $r \in L$ then there exists $s > r$ such that $s \in L$.
- There exists $r \in R$; there exists $r \in L$.
- There does not exist r such that $r \in R$ and $r \cap L$ (that is, $R \cap L = \varnothing$).
- If $r > s$ then either $r \in R$ or $s \in L$.

In the topos of sheaves over a topological space X, the object of real numbers is represented by the sheaf of continuous functions to $\mathbb{R}$ with the usual topology.

The reals form (with the straightforward addition and multiplication) a ring containing the rationals (and even a local ring in the sense that for all real x either x or $1 - x$ is invertible). We can define order relations as follows: let $x > 0$ when $0 \in R$ and let $x \geq 0$ when $r > 0$ for all $r \in R$ (which is exactly equivalent to requiring $r \geq 0$ for all $r \in R$), and extend these by translation. Let $x \lozenge y$ when $x > y$ or $x < y$: then $x \lozenge 0$ means exactly that x is invertible. Note that if $x < y$ are reals then there exists a rational r such that $x < r < y$. However, $x \leq y$ does not mean the same as $(x = y) \vee (x < y)$, which is probably not surprising, but even $x < y$ does not mean the same as $(x \leq y) \wedge \neg(x = y)$, which is perhaps a bit more surprising, and $x \lozenge y$ is stronger than $\neg(x = y)$. It is not true that for all real x and y we have $(x \leq y) \vee (x \geq y)$; however, for all real $h > 0$ it is true that $(x < y + h) \vee (x + h > y)$.

It is true that for real x, if $\neg\neg(x = 0)$ then $x = 0$. Indeed, $x = 0$ is equivalent to $-h < x < h$ for all rational $h > 0$ (this is easy to check on the cuts, because for all $h > 0$ we must have either $x < h$ or $x > 0$); now if $h > 0$ and $\neg\neg(x = 0)$ then we must have $-h < x < h$ (again because either $x < h$ or $x > 0$ and the latter is impossible). Even stronger: $\neg(x \lozenge 0)$ implies $x = 0$.

It would be naïve to hope that a non-empty (in the sense "having an element") bounded set of rationals should always have a least upper bound and a greatest lower bound in the reals, and it would be naïve to hope that a continuous real function ("continuous" in the ordinary $\forall\varepsilon\exists\delta$ sense) f such that $f(-1) = -1$ and $f(1) = 1$ should cancel somewhere. We can easily give examples in the topos of sheaves over $X = [-1; 1]$. For a set of rationals with no lower bound define $\chi(r) = X$ if $0 < r < 1$ and $\chi(r) = [-1; 0[$ if $-1 < r \leq 0$, $\chi(r) = \varnothing$ in all other cases: with the obvious abuse of language, this defines the characteristic function of a subset U of the internal rational interval $]-1; 1[$, and U is even open (in the sense that for all $r \in U$ there exists $h > 0$ such that $]r - h; r + h[\subseteq U$), contains $]0; 1[$, but does not havea a real lower bound. For a continuous and even monotone function as stated, take $F(\xi, x)$, for $\xi \in X = [-1; 1]$ and real x, so that F is continuous, $F(\xi, \cdot)$ monotone nondecreasing for all ξ, and $F(\xi, x) = 0$ exactly when $\xi \leq 0$ and $x = -\frac{1}{2}$, or $\xi \geq 0$ and $x = \frac{1}{2}$, or $\xi = 0$ and $-\frac{1}{2} \leq x \leq \frac{1}{2}$: certainly we can find such F, and internally it defines a continuous function on the reals, nondecreasing (in the sense that $x \leq y$ implies $F(x) \leq F(y)$) but for which it is not true that $\exists z(F(z) = 0)$.

On the other hand it is true that for every continuous increasing function (in the sense that $x < y$ implies $F(x) < F(y)$) with $F(-1) = 1$ and $F(1) = 1$ there exists a z with $F(z) = 0$.

Note that if $x_1, \ldots, x_k$ are real numbers (here, k is a naïve natural number), they have a well-defined least upper bound and greatest lower bound. In particular, $|x| = \sup(x, -x)$ is well-defined, and $x \geq 0$ is equivalent to $|x| = x$; and $x \Diamond 0$ is equivalent to $|x| > 0$. Note that $x \mapsto |x|$ is definitely not differentiable at 0: there exists no ℓ such that for all $\varepsilon > 0$ there exists $\delta > 0$ satisfying $0 < |h| < \delta \implies \left| \frac{|h|}{h} - \ell \right| < \varepsilon$. So while it cannot be proved that there exists a discontinuous real function (Brouwer's famous theorem), it can be proved that there exists one which is not differentiable: this also means that the line object of synthetic differential geometry is not the real numbers object in any sense.

2003-12-07:066

Some more intuitionist mathematics (see **2002-12-21:054** and possibly **2003-12-07:065**).

Need to check the following.

If X is a set, we can define the set $\tilde{X}$ of $P \subseteq X$ such that $\forall x \forall y (x \in P \wedge y \in P \implies x = y)$ and $\neg\neg(P = \varnothing)$ (that is, $\neg\forall x \neg(x \in P)$). Define an equivalence relation on $\tilde{X}$ by $P \sim Q$ iff $\neg\neg(P = Q)$, and let $\bar{X} = \tilde{X}/\sim$. Define a map $X \to \bar{X}$ by taking x to $\{x\}$. This should be the internal vision of the construction which, in the topos context, takes an object X to its associated sheaf for the $\neg\neg$ topology. So $\bar{X}$ is in many ways the "best classical object" associated to X. It seems that if X has some algebraic structure, then $\bar{X}$ also inherits that structure.

Now if $\mathbb{R}$ is the real numbers object, then it injects in $\bar{\mathbb{R}}$ (since $\neg\neg(x = y)$ implies $x = y$ for reals, see **2003-12-07:065**), and the latter is itself a ring with an order on it: it would be interesting to check what properties it has, analogously to those of $\mathbb{R}$, and perhaps see whether it is better behaved. (In the topos of sheaves over a topological space X, $\bar{\mathbb{R}}$ is represented by the sheaf of real-valued continuous functions on a *dense open subset*.)

2003-12-07:067

Still concerning intuitionist mathematics (also see **2002-12-21:054** and possibly **2003-12-07:065** and **2003-12-07:066**).

Rumor (or folklore) has it that it is consistent that all functions $\mathbb{N} \to \mathbb{N}$ are computable (recursive). How is this done?

Note that it is not possible for all subsets $E \subseteq \mathbb{N}$ to be recursively enumerable: indeed, the standard diagonalization argument works as usual (let U be a universal Turing machine, and let E be the set of k such that $U(k, k)$ does not terminate: if there exists n such that E is the set of n for which $U(n, k)$ terminates, then $U(n, n)$ terminates if and only if it does not terminate, a contradiction). But a non-r.e. set E, if all functions $\mathbb{N} \to \mathbb{N}$, cannot satisfy $E \cup (\mathbb{N} \setminus E) = \mathbb{N}$, otherwise the function which is 1 on E and 0 on $\mathbb{N} \setminus E$ would be defined on all of $\mathbb{N}$ whereas it is not computable.

2003-12-07:068

A very open question: we know that for all $n \geq 1$ the canonical injection $\mathbb{P}^n(\mathbb{Q}) \to \mathbb{P}^n(\mathbb{R})$ has dense image. But how do we proceed in practice (computationally, that is) to approximate a point $x \in \mathbb{P}^n(\mathbb{R})$ by a point in $\mathbb{P}^n(\mathbb{Q})$ of small height (the height being the max of the absolute values of integer homogeneous coordinates for the point in question)? For $n = 1$ we have Euclid's algorithm: can it be generalized in some way?