Journal of Pure and Applied Algebra 25 (1982) 227–247
North-Holland Publishing Company

ABSTRACT GALOIS THEORY II*

Michael BARR
Department of Mathematics, McGill University, Montreal, Quebec, Canada H3A 2K6

Communicated by F.W. Lawvere
Received 11 September 1981

Introduction

Galois theory was classically described as an order inverting correspondence between subgroups of the galois group and intermediate fields in a galois extension. Later the correspondence was extended to one between open subgroups of the group of automorphisms of the separable closure, equipped with the pointwise convergence topology, and finite separable extensions. (Also between closed subgroups and locally separable extensions.)

In 1961 Grothendieck observed that the essential content of the galois theory was contained in the statement that the category of separable extensions of field was the opposite of a *galois category:* the category of continuous actions of a profinite group on a finite discrete space. This duality gives much more comprehensive information than the lattice isomorphism, yet is not appreciably harder to prove. See [10], especially Exposé V.

Meanwhile several people were generalizing the galois theory to more-or-less arbitrary commutative rings, although the generalization was really satisfactory only for connected ones (i.e. those with no idempotents except 0 and 1). See [1,4,5,11,12,13,9]. Recently, I found a convenient setting in which to include the above results for the connected case. See [2]. Meantime, jointly with Diaconescu, I was describing the fundamental group of a topos satisfying suitable local connectedness properties. This was done by finding a suitable definition of covering; the fundamental group is just the group of deck transformations. In this paper, we show that if you stick to finite coverings in a connected topos, the local connectedness is unnecesary. Moreover, the galois theory over a connected ring can be most conveniently described in terms of finite coverings, thus describing the galois group as a finitization (or profinitization) of the fundamental group – a point first made by Grothendieck. In particular, we show that the Chase–Harrison–Rosenberg theory is applicable to a connected commutative ring object in any topos.

* This work has been supported by the National Science and Engineering Research Council as well as by the Ministère de l'Education du Québec.

1. The functor Δ

For any topos $\mathscr{E}$, let Δ denote the functor from the category of finite sets to $\mathscr{E}$ whose value at n is the sum of n copies of 1.

Proposition 1.1. *The functor Δ preserves finite limits and finite colimits.*

Proof. $\Delta 1 = 1$ by assumption while the fact that pullbacks in a topos commute with sums implies that Δ preserves pullbacks. As for the colimits, it is clear that Δ preserves sums, images and coequalizers of equivalence relations. Any relation generates an equivalence relation. Begin by making it reflexive and symmetric with a three term sum and image and then apply a finite number of operations of pulling back and forming an image.

Proposition 1.2. *In any topos $\mathscr{E}$, if $\Delta n \cong \Delta m$ then either $n \cong m$ or $0 = 1$ in $\mathscr{E}$. If $\varphi, \theta : m \to n$ are distinct, so are $\Delta\varphi, \Delta\theta$.*

Proof. According to Freyd [6, 7] every topos in which $0 \neq 1$ has a $\mathscr{S}et$-valued functor Φ which is left exact and preserves finite sums. Evidently $\Phi\Delta n = n$ and $\Phi\Delta m = m$. Similarly, $\Phi\Delta\varphi = \varphi$ and $\Phi\Delta\theta = \theta$.

Henceforth, we will suppose without explicit mention that $0 \neq 1$ in every topos we consider.

Corollary 1.3. *In any topos, if $U \neq 0$ is such that $\Delta n \times U \cong \Delta m \times U$ over U, then $n \cong m$. If $\varphi, \theta : n \to m$ such that $\Delta\varphi \times U = \Delta\theta \times U$, then $\varphi = \theta$.*

Proof. Consider $\mathscr{E}/U$.

Lemma 1.4. *Suppose A_0 and A_1 are objects of $\mathscr{E}$ such that $A_0 + A_1 \cong \Delta n$. Then there is a finite decomposition $1 = \sum U_\alpha$, $\alpha \in I$, into non-empty subobjects and unique integers $n_{0\alpha}, n_{1\alpha}$ such that for each $\alpha \in I$,*

$$A_0 \times U_\alpha \cong \Delta n_{0\alpha} \times U_\alpha \quad \textit{over } U_\alpha,$$

$$A_1 \times U_\alpha \cong \Delta n_{1\alpha} \times U_\alpha \quad \textit{over } U_\alpha,$$

and $n_{0\alpha} + n_{1\alpha} \cong n$.

Proof. For $i = 0, \dots, n-1$, let $\langle i \rangle : 1 \to n$ denote the map taking the element of 1 to i. This gives a map

$$\Delta\langle i \rangle : 1 \to \Delta n \cong A_0 + A_1.$$

The map of 1 into the sum breaks it up into a sum $1 = U_0^i + U_1^i$, defined by having

$$\begin{tikzcd}
U_j^i \arrow[r] \arrow[d] & 1 \arrow[d, "\Delta\langle i\rangle"] \\
A_j \arrow[r] & \Delta^n
\end{tikzcd}$$

be a pullback. For each function $\alpha : n \to 2$ (that is, subset of n), let $U_\alpha = \bigcap_{i=1}^n U^i_{\alpha(i)} = \prod_{i=1}^n U^i_{\alpha(i)}$ since these are subobjects of 1. Then

$$1 = \prod_{i=0}^{n-1} (U_0^i + U_1^i) \cong \sum_\alpha \prod_{i=0}^{n-1} U^i_{\alpha(i)} = \sum_\alpha U_\alpha .$$

For any $i = 0, \dots, n-1$, we have

$$\begin{aligned} U_1^i \cap U_\alpha &= U_1^i \cap U^0_{\alpha(0)} \cap \cdots \cap U^i_{\alpha(i)} \cap \cdots \cap U^{n-1}_{\alpha(n-1)} \\ &= \begin{cases} U_\alpha & \text{if } \alpha(i) = 1, \\ 1 & \text{if } \alpha(i) = 0. \end{cases} \end{aligned}$$

Thus if $\#\alpha$ denotes the number of indices i for which $\alpha(i) = 1$,

$$\begin{aligned} A_1 \times U_\alpha &\cong (U_1^0 + \cdots + U_1^{n-1}) \times U_\alpha \\ &\cong U_1^0 \times U_\alpha + \cdots + U_1^{n-1} \times U_\alpha \\ &\cong \Delta(\#\alpha) \times U_\alpha , \end{aligned}$$

the isomorphism being over U_α. Similarly, $A_0 \times U_\alpha \cong \Delta(n - \#\alpha) \times U_\alpha$. The uniqueness follows as soon as we sum only those α for which $U_\alpha \neq 0$.

Lemma 1.5. *Let $f : \Delta m \to \Delta n$ in $\mathscr{E}$. Then there is a finite decomposition $1 = \sum U_\alpha$, $\alpha \in I$, into non-empty subobjects of 1 and for each α a unique function $\varphi_\alpha : m \to n$ such that for each α, $f \times U_\alpha = \Delta\varphi_\alpha \times U_\alpha$.*

Proof. First consider the case that $m = 1$. Then f is a monomorphism (any map with domain 1 is) and a map $1 \to 1 + \cdots + 1$ induces, by pulling back, a decomposition $1 = U_0 + \cdots + U_{n-1}$ such that $f \times U_i = \Delta\langle i\rangle \times U_i$.

For the general case, we have for each $j = 0, \dots, m-1$ a decomposition of $1 = U_0^j + \cdots + U_{n-1}^j$ such that $f \cdot \Delta\langle j\rangle \times U_i^j = \Delta\langle i\rangle \times U_i^j$. Now let $\varphi : m \to n$ be any function. Then φ is uniquely determined by the formula $\varphi\langle j\rangle = \langle \varphi j\rangle$. We have $f \cdot \Delta\langle j\rangle \times U^1_{\varphi j} = \Delta\langle \varphi j\rangle \times U^j_{\varphi j} = \Delta\varphi \cdot \Delta j \times U^j_{\varphi j}$ from which we see that $f \times U^j_{\varphi j} = \Delta\varphi \times U^j_{\varphi j}$. Then if $U_\varphi = \bigcap_{j=0}^{n-1} U^j_{\varphi j}$ we have also that $f \times U_\varphi = \Delta\varphi \times U_\varphi$. Since

$$1 = \prod_{j=0}^{m-1} \sum_{i=0}^{n-1} U_i^j \cong \sum_\varphi \prod_j U^j_{\varphi j} = \sum_\varphi U_\varphi ,$$

the conclusion follows by restricting the sum to those φ for which $U_\varphi \neq 0$.

Corollary 1.6. *The image of any map $\Delta n \to \Delta m$ has a complement.*

Corollary 1.7. *If $f,g:\Delta n\to\Delta m$ are two morphisms then both their equalizer can be embedded as a complemented subobject of an object of the form ΔP.*

Proof. By applying 1.5 to $(f,g):\Delta(n+n)\to\Delta m$ we find a finite decomposition $1=\sum U_\alpha$ such that $f\times U_\alpha=\Delta\varphi_\alpha\times U_\alpha$ and $g\times U_\alpha=\Delta\theta_\alpha\times U$ for maps $\varphi_\alpha,\theta_\alpha:n\to m$. Since Δ preserves finite limits and colimits, we can form the equalizer (resp. coequalizer)

$$\begin{tikzcd} p_\alpha \arrow[r] & n \arrow[r, shift left, "\varphi_\alpha"] \arrow[r, shift right, "\theta_\alpha"'] & m \arrow[r] & q_\alpha \end{tikzcd}$$

and then

$$\begin{tikzcd} \Delta p_\alpha\times U_\alpha \arrow[r] & \Delta n\times U\alpha \arrow[r, shift left, "f\times U_\alpha"] \arrow[r, shift right, "g\times U_\alpha"'] & \Delta m\times U_\alpha \arrow[r] & \Delta q_\alpha\times U_\alpha \end{tikzcd}$$

is an equalizer (resp. coequalizer) as well. If p is largest of the p_α and q the largest of the q_α, it is clear that the equalizer (resp. coequalizer) is a complemented subobject of Δp (resp. Δq).

We note that a functor analogous to Δ with the above properties can be defined in any category with finite limits and finite sums that are disjoint and universal.

2. Finite coverings

Let $\mathscr{E}$ be a non-trivial topos. An object A of $\mathscr{E}$ is called a *finite covering* if there is a cover $U\twoheadrightarrow 1$ and a finite set n such that $A\times U\cong\Delta n\times U$ over U. If that happens we say that A is an n-fold covering *split by U*. A morphism $f:B\to A$ is called a *finite covering* if it is so as an object of $\mathscr{E}/A$.

Remark. We should note the definition of finite covering given here is really the right one only in the case that $\mathscr{E}$ is connected (see Section 3). There are at least three other possibilities otherwise.

(1) A is a finite covering if there is a cover U such that $A\times U$ is a complemented subobject of $\Delta n\times U$ over U. Equivalently, there is a finite epimorphic family $\{U_\alpha\to 1\}$ such that for all α, $A\times U_\alpha\cong\Delta n_\alpha\times U_\alpha$.

(2) There is an epimorphic family $\{U_\alpha\to 1\}$ such that $A\times U_\alpha\cong\Delta n_\alpha\times U_\alpha$ over U_α for each α.

(3) There is a cover U such that $A\times U$ is a finite cardinal in $\mathscr{E}/U$ in the sense of Johnstone [14, p. 173].

If the coproduct of countably many copies of 1 exists in $\mathscr{E}$, the last two definitions coincide.

Proposition 2.1. *Let A and B be finite coverings. Then,*

(i) *if $U\twoheadrightarrow 1\twoheadleftarrow V$ are covers such that there is a map $U\to V$, then any finite covering split by V is also split by U;*

(ii) *if A is an n-fold covering and an m-fold covering, then $n=m$ or $0=1$ in $\mathscr{E}$;*

(iii) *there is a cover $U \twoheadrightarrow 1$ that splits both A and B;*

(iv) *$A+B$ is a finite covering; 0 is a finite covering;*

(v) *$A\times B$ is a finite covering; 1 is a finite covering;*

(vi) *the image any $B \to A$ is a complemented subobject of A;*

(vii) *the equalizer and coequalizer of any pair of maps $B \rightrightarrows A$ are complemented subobjects of finite coverings.*

Proof. (i) If $A\times V \cong \Delta n \times V$, then

$$A\times U \cong (A\times V)\times_V U \cong (\Delta n \times V)\times_V U \cong \Delta n \times U.$$

(ii) If $A\times U\cong \Delta n\times U$ and $A\times V\cong \Delta m\times V$, then $U\times V$ is a cover mapping to both U and V, whence $A\times U\times V$ is isomorphic over $U\times V$ to both $\Delta n\times U\times V$ and $\Delta m\times U\times V$.

(iii) If U splits A and V splits B, $U\times V$ splits both.

(iv) If U splits A and B, it splits $A+B$.

(v) As well as $A\times B$.

(vi) From 1.6 it follows that the image of $U\times B \to U\times A$ is complemented. It can be proved directly in any regular category with stable sums that a subobject has a complement if it does so locally, but R. Paré showed me the following elegant proof in a topos. A subobject is complemented iff its characteristic map factors through 2. We have

$$\begin{tikzcd}
A\times U \arrow[r, two heads] \arrow[d] & A \arrow[d] \\
2 \arrow[r, tail] & \Omega
\end{tikzcd}$$

and the diagonal fill-in gives the desired arrow.

(vii) Let $f,g: B\to A$ have equalizer C (resp. coequalizer D). After crossing with aU that splits both A and B, we have

$$\begin{tikzcd}
C\times U \arrow[r] & B\times U \arrow[r, shift left, "f\times U"] \arrow[r, shift right, "g\times U"'] & A\times U \arrow[r] & D\times U
\end{tikzcd}$$

both an equalizer and a coequalizer. By 1.7 there are sets p and q so that $C\times U$ and $D\times U$ are complemented subobjects of $\Delta p\times U$ and $\Delta q\times U$ respectively. Moreover, by examining the proof of 1.7 we see that what really happens is that there is a finite decomposition $U=\sum U_\alpha$ such that

$$C\times U_\alpha \cong \Delta p_\alpha \times U_\alpha, \qquad D\times U_\alpha \cong \Delta q_\alpha \times U_\alpha.$$

Then if we let $C'=\Delta(p-p_\alpha)$, $D'=\Delta(q-q_\alpha)$, we see that

$$(C+C')\times U_\alpha \cong \Delta p\times U_\alpha, \qquad (D+D')\times U_\alpha \cong U_q\times U_\alpha$$

for all α so that

$$(C+C')\times U\cong\Delta p\times U,\qquad (D+D')\times U\cong\Delta q\times U.$$

Proposition 2.2. *Let $\Delta n\times A$ be a finite covering. Then A is a finite covering as well.*

Proof. Let U be a cover for which

$$\Delta n\times A\times U\cong\Delta m\times U.$$

Then by 1.4 applied to $\Delta n\times A\times U\cong A\times U+\Delta(n-1)\times A\times U$, there is a finite decomposition $U=\sum U_\alpha$ such that for each α there is a p_α with $A\times U_\alpha\cong\Delta p_\alpha\times U_\alpha$ and $\Delta(n-1)\times A\times U_\alpha\cong\Delta(m-p_\alpha)\times U_\alpha$. The uniqueness implies that $(n-1)p_\alpha=m-p_\alpha$ or $m=np_\alpha$. But then $p_\alpha=m/n$ is independent of α and $A\times U\cong\Delta(m/n)\times U$.

Theorem 2.3. *Let $0\neq B\to A$ in $\mathscr{E}$. Then of the following conditions, any two imply the third.*

(i) *A is a finite covering;*

(ii) *B is a finite covering of A;*

(iii) *B is a finite covering.*

Moreover, if A is an n-fold covering and $B\to A$ is an m-fold covering, then B is an nm-fold covering.

Proof. Suppose (i) and (ii) hold. Then there is a cover U such that $A\times U\cong\Delta n\times U$ and $V\twoheadrightarrow A$ such that

$$\begin{tikzcd}
\Delta m\times V \arrow[r] \arrow[d] & B \arrow[d] \\
V \arrow[r] & A
\end{tikzcd}$$

is a pullback. Crossing with U gives the inner square of the diagram

$$\begin{tikzcd}
\Delta m\times V_i \arrow[rrrrr, dashed] \arrow[rrd] \arrow[ddddd] & & & & & B_i \arrow[lld] \arrow[ddddd] \\
& & \Delta m\times V\times U \arrow[r] \arrow[dd] & B\times U \arrow[dd] & & \\
& \text{III} & & & \text{I} & \\
& & V\times U \arrow[r] & \Delta n\times U & & \\
& & & \text{II} & & \\
V_i \arrow[rruu] \arrow[rrrrr] & & & & & U \arrow[lluu, "\Delta\langle i\rangle\times U"']
\end{tikzcd}$$

The objects B_i and V_i are defined so that the squares labelled I and II are pullbacks.

Since both vertical maps in the square labelled III are projections, it is clear that square is a pullback as well. The dotted arrow exists from the mapping properties of pullbacks and a diagram chase shows that the outer square is a pullback. Summarizing, we conclude that $B_i \times_U V_i \cong \Delta m \times V_i$. Next observe that $V \twoheadrightarrow A$ whence $V \times U \twoheadrightarrow A \times U$ or $V \times U \twoheadrightarrow \Delta n \times U$ so that by pulling back, $V_i \twoheadrightarrow U$. An easy induction gives that $W = V_0 \times_U V_1 \times_U \cdots \times_U V_{n-1} \twoheadrightarrow U$ and that W is a cover. It is immediate that $B_i \times_U W \cong \Delta m \times W$ for $i = 0, \ldots, n-1$ and adding this up over all i gives $\sum (B_i \times_U W) \cong \Delta mn \times W$. Now

$$\sum (B_i \times_U W) \cong \left(\sum B_i\right) \times_U W \cong (B \times U) \times_U W.$$

The map $B \times U \to U$ is computed from

$$\begin{tikzcd}
B_i \arrow[r] \arrow[d] & B \times U \arrow[d] \arrow[ddr] & \\
U \arrow[r] \arrow[drr, "="'] & \Delta n \times U \arrow[dr] & \\
& & U
\end{tikzcd}$$

to be just the projection on U so that $(B \times U) \times_U W \cong B \times W$. Thus B is split by W. Moreover, B is locally isomorphic to Δmn.

Suppose (i) and (iii) hold. Then we have

$$A \times U \cong \Delta n \times U, \qquad B \times V \cong \Delta p \times V.$$

Thus,

$$(\Delta n \times B) \times_A (A \times U \times V) \cong \Delta n \times B \times U \times V$$
$$\cong \Delta(np) \times U \times V \cong \Delta p \times (A \times U \times V)$$

so that $\Delta n \times B \to A$ is a covering, whence by 2.2, $B \to A$ is as well.

Suppose (ii) and (iii) hold. Let $B \times_A U \cong \Delta m \times U$ and $B \times V \cong \Delta p \times V$. Then if $B \times B$ is considered an object over A via the second projection, we have

$$(B \times B) \times_A (U \times V) \cong B \times \Delta m \times U \times V \cong \Delta(pm) \times U \times V$$

so that $B \times B \to A$ is a covering. Since $B \times_A B \to A$ is a covering (being a product, in $\mathscr{E}/A$, of coverings) it follows from 1.6 that $B \times_A B$ is complemented subobject – in $\mathscr{E}/A$, a fortiori in $\mathscr{E}$ – of $B \times B$. It follows from 1.4, applied in $\mathscr{E}/V$, that there is a decomposition $V = \sum V_\alpha$ such that

$$B \times_A B \times V_\alpha \cong q_\alpha \times V.$$

Moreover, we can suppose the decomposition refined to the point that both projections

$$B \times_A B \times V_\alpha \rightrightarrows B \times V_\alpha$$

are induced by set maps. It follows that the coequalizer is isomorphic to $\Delta n_\alpha \times V_\alpha$. But $B \neq 0$ implies $m \neq 0$ so that $B \times_A U \to A$ is epi whence $B \to A$ is epi as well. Thus the coequalizer above is $A \times V_\alpha$. Then in $\mathscr{E}/V_\alpha$,

$$A \times V_\alpha \cong \Delta n_\alpha, \qquad B \times V_\alpha \cong \Delta p \times V_\alpha,$$

while

$$(B \times V_\alpha \to A \times V_\alpha) \cong (\Delta m \times V_\alpha \to A \times V_\alpha)$$

whence by the first part, $p = n_\alpha m$. Thus $n_\alpha = p/m$ does not depend on α and we conclude that $A \times V \cong \Delta(p/m) \times V$.

3. Connected coverings

We say that an object of $\mathscr{E}$ is *connected* if it is non-zero and not possible to write it as a sum of two non empty subobjects. We say that *$\mathscr{E}$ is connected* if 1 is. Throughout this section we suppose that $\mathscr{E}$ is connected.

Proposition 3.1. *Let A and B be objects of $\mathscr{E}$ such that $A+B$ is a covering. Then so are A and B.*

Proof. Suppose U is a cover such that $(A+B) \times U \cong \Delta n \times V$. By applying the functor $U^*: \mathscr{E} \to \mathscr{E}/U$ given by $U^*(A) = A \times U \to U$, we have

$$U^*(A) + U^*(B) \cong \Delta n.$$

From 1.4 we get a finite decomposition $U = \sum U_\alpha$ and integers m_α such that

$$A \times U_\alpha \cong \Delta m_\alpha \times U_\alpha, \qquad B \times U_\alpha \cong \Delta(n - m_\alpha) \times U_\alpha.$$

By putting together all the terms belonging to any m_α, we can suppose that $\alpha \neq \beta$ implies $m_\alpha \neq m_\beta$. But $A \times U_\alpha \times U_\beta \cong \Delta m_\alpha \times U_\alpha \times U_\beta \cong \Delta m_\beta \times U_\alpha \times U_\beta$ so that $m_\alpha \neq m_\beta$ implies $U_\alpha \times U_\beta = 0$ (see 1.3). If V_α is the support of U_α then $U_\alpha \twoheadrightarrow V_\alpha$, $U_\beta \twoheadrightarrow V_\beta$ implies

$$0 = U_\alpha \times U_\beta \twoheadrightarrow V_\alpha \times V_\beta = V_\alpha \cap V_\beta.$$

Thus $1 = \sum V_\alpha$ is a disjoint sum which contradicts the connectedness of 1 unless there is only one index. But that means $U_\alpha = U$, $m = m_\alpha$ and

$$A \times U \cong \Delta m \times U, \qquad B \times U \cong \Delta(n-m) \times U.$$

Corollary 3.2. *Every covering is a sum of a finite number of connected ones.*

Proof. If A is an n-fold covering and

$$A \cong A_1 + \cdots + A_m$$

with each $A_i \neq 0$, then each A_i is an n_i-fold covering with $\sum_{i=1}^m n_i = n$ so that $m \leq n$.

Thus A cannot be written as the sum of an indefinitely large number of subobjects, from which the conclusion is easily derived.

Proposition 3.3. *Every morphism of connected coverings is an epi.*

Proof. Every morphism has a complemented image.

Proposition 3.4. *Let $f:A\to B$ be a map of coverings and U split both A and B. If A is an n-fold covering and B an m-fold covering, then there is a map $\varphi:n\to m$ such that $f\times U\cong\Delta\varphi\times U$.*

Proof. Let $U=\sum U_\alpha$ so that $f\times U_\alpha\cong\Delta\varphi_\alpha\times U_\alpha$. Joining together U_α and U_β whenever $\varphi_\alpha=\varphi_\beta$, we can suppose that when $\alpha\neq\beta$, $\varphi_\alpha\neq\varphi_\beta$. Now consider the diagram all of whose squares (including the outer) are pullbacks,

$$\begin{tikzcd}
A\times U_\alpha\times U_\beta \arrow[rrr] \arrow[ddd] \arrow[dr, "f\times U_\alpha\times U_\beta"] & & & A\times U_\alpha \arrow[ddd] \arrow[dl, "f\times U_\alpha"'] \\
& B\times U_\alpha\times U_\beta \arrow[r] \arrow[d] & B\times U_\alpha \arrow[d] & \\
& A\times U_\beta \arrow[r] & B & \\
A\times U_\beta \arrow[rrr] \arrow[ur, "f\times U_\beta"'] & & & A \arrow[ul, "f"']
\end{tikzcd}$$

This is equivalent to

$$\begin{tikzcd}
\Delta n\times U_\alpha\times U_\beta \arrow[rrr] \arrow[ddd] \arrow[dr] & & & \Delta n\times U_\alpha \arrow[ddd] \arrow[dl, "\Delta\varphi_\alpha\times U_\alpha"'] \\
& \Delta m\times U_\alpha\times U_\beta \arrow[r] \arrow[d] & \Delta m\times U_\alpha \arrow[d] & \\
& \Delta m\times U_\beta \arrow[r] & B & \\
\Delta n\times U_\beta \arrow[rrr] \arrow[ur, "\Delta\varphi_\beta\times U_\beta"'] & & & A \arrow[ul, "f"']
\end{tikzcd}$$

from which it follows that $\Delta\varphi_\alpha\times U_\alpha\times U_b=\Delta\varphi_\beta\times U_\alpha\times U_\beta$ so that $U_\alpha\times U_\beta=0$ (see 1.3). The argument then finishes exactly as that of 3.1.

Proposition 3.5. *Let A be an n-fold covering and B be a connected covering. Then the number of components of $A\times B$ is $\leq n$.*

Proof. Let B be an m-fold cover and

$$A\times B=C_1+\cdots+C_q$$

where C_i is a p_i-fold covering. It follows that $mn=\sum_{i=1}^{q} p_i$. Each

$$C_i \to A \times B \to B$$

is epi because B is connected (see 3.3) whence $p_i \geq m$. It follows that $q \leq n$.

4. The galois category

A category which is equivalent to a category of finite G-sets (discrete but with continuous action) for a profinite group G is called a *galois category*. These categories are characterized in Barr [2] using a characterization from V.4 of Grothendieck [10].

Theorem 4.1. *Let $\mathscr{E}$ be a connected topos. Then the full subcategory of finite coverings of $\mathscr{E}$ is a galois category.*

Proof. Let $\mathscr{A}$ be the full subcategory of connected finite coverings and $\mathscr{B}$ the full subcategory of finite coverings. We will verify duals of the conditions of Barr [2] according to the numbering used there.

(1) Every map in $\mathscr{A}$ is a regular epimorphism (see 3.3).

(2) Every pair of maps

$$\begin{tikzcd} B \arrow[r, "f"] & A & C \arrow[l, "g"'] \end{tikzcd}$$

can be completed to a commutative square

$$\begin{tikzcd} D \arrow[r] \arrow[d] & B \arrow[d] \\ C \arrow[r] & A \end{tikzcd}$$

It follows from 2.1(v), (vii) that the pullback $B \times_A C$ is a complemented subobject of a finite covering and from 3.1 that it is a finite covering. Take D to be any component of it.

(3) For each object A, there is a number $r(A)$ such that for all B, there are objects $C_1, \dots, C_r$ and pairs of morphisms $A \leftarrow C_i \rightarrow B$ such that $r \leq r(A)$ and whenever $A \leftarrow C \rightarrow B$ there is a unique i and unique $C \rightarrow C_i$ such that

$$\begin{tikzcd} & C \arrow[dl] \arrow[dr] \arrow[dd] & \\ A & & B \\ & C_i \arrow[ul] \arrow[ur] & \end{tikzcd}$$

commutes. To prove this, take $C_1, \dots, C_r$ to be the connected components of $A \times B$. Any map $C \to A \times B$, C connected, must factor through a unique C_i. The conclusion follows from 3.5.

(4) There is a terminal object 1.

(5) Every parallel pair $A \rightrightarrows B$ has a coequalizer; products in $\mathscr{B}$ preserve them.

Actually, the cited reference does not refer to $\mathscr{B}$ but to a category $\sum \mathscr{A}$ (remember, we are dualizing) of formal sums of objects of $\mathscr{A}$. However it is an easy exercise (based on the fact that when A is connected a map $A \to \sum B_i$ factors through one summand) to show that $\sum \mathscr{A} \cong \mathscr{B}$. Now if

$$\begin{tikzcd} A \arrow[r, shift left, "f"] \arrow[r, shift right, "g"'] & B \arrow[r] & C \end{tikzcd}$$

is a coequalizer in $\mathscr{E}$, A and B are in $\mathscr{A}$ and V splits both A and B, we have

$$\begin{tikzcd} \Delta n \times U \arrow[r, shift left, "\Delta\varphi \times U"] \arrow[r, shift right, "\Delta\gamma \times U"'] & \Delta m \times U \end{tikzcd}$$

and if

$$\begin{tikzcd} n \arrow[r, shift left, "\varphi"] \arrow[r, shift right, "\gamma"'] & m \arrow[r] & p \end{tikzcd}$$

is a coequalizer in $\mathscr{S}et$, then $C \times U \cong \Delta p \times U$. Now let D be another object of $\mathscr{A}$. To see that

$$A \times D \rightrightarrows B \times D \to C \times D$$

is a coequalizer (in $\mathscr{B}$) we assume that U splits D as well, say $D \times U \cong \Delta q \times U$. Then crossing with U gives

$$\Delta n \times \Delta q \times U \rightrightarrows \Delta m \times \Delta q \times U \to \Delta p \times \Delta q \times U$$

or

$$\Delta(nq) \times U \rightrightarrows \Delta(mq) \times U \to \Delta(pq) \times U$$

which is coequalizer (in $\mathscr{C}/U$) because

$$nq \rightrightarrows mq \to pq$$

is. That follows because $\mathscr{S}et$ is a topos.

Finally, from the fact that in the diagram

$$\begin{tikzcd} & B \times D \times U \times U \arrow[r] \arrow[d, shift left] \arrow[d, shift right] & C \times D \times U \times U \arrow[d, shift left] \arrow[d, shift right] \\ A \times D \times U \arrow[r, shift left] \arrow[r, shift right] \arrow[d] & B \times D \times U \arrow[r] \arrow[d] & C \times D \times U \arrow[d] \\ A \times D \arrow[r, shift left] \arrow[r, shift right] & B \times D \arrow[r] & C \times D \end{tikzcd}$$

the uppermost arrow is epi and the second row and two right columns are coequalizers, it follows that the bottom row is too.

This completes the proof.

We let Gal($\mathscr{E}$) denote the group, unique up to isomorphism, such that the category of finite coverings – $\mathscr{E}$ is equivalent to the category of G-sets. The reason Gal($\mathscr{E}$) is unique is that G may be recovered from $\mathscr{S}et^G$. Here is how that is done. First cut down to the full subcategory of connected G-sets. Among these, define an object A to be normal if every component of $A \times A$ is isomorphic (via either projection) to A. Then G is the group of automorphisms of the identity functor of the full subcategory of normal connected objects. The subgroup of these automorphisms which restrict to the identity on a given object is taken as open.

5. Galois subcategories

In this section we show:

Theorem 5.1. *Let $\mathscr{B}$ be a galois category and $\mathscr{C}$ a full subcategory closed under finite limits, finite sums and quotients by finite group actions. Then $\mathscr{C}$ is a galois category.*

Proof. We will show that G is a profinite group such that $\mathscr{B}$ is the category of G-sets, then there is a closed normal subgroup $N \subsetneq G$ such that $\mathscr{C}$ is the category of G/N-sets. We may assume without loss of generality that $\mathscr{C}$ is replete – that is, any object isomorphic to an object of C belongs to $\mathscr{C}$. Let $\mathscr{U}$ be the set of all open subgroups U of G such that G/U is in $\mathscr{C}$.

Lemma 5.2. *If $A+B$ belongs to $\mathscr{C}$ so do A and B.*

Proof. There is an equalizer

$$\begin{tikzcd} A \arrow[r] & A+B \arrow[r, shift left, "d_0"] \arrow[r, shift right, "d_1"'] & A+B+A+B \end{tikzcd}$$

in which d_0 is inclusion of the first and second and d_1 the inclusion of the first and fourth summands.

This shows that $\mathscr{C}$ is completely determined by $\mathscr{U}$.

Lemma 5.3. *Let $U \in \mathscr{U}$. Then any conjugate of U also belongs to $\mathscr{U}$.*

Proof. If U and V are conjugate, $G/U \cong G/V$ as a G-set.

Lemma 5.4. *If U and V belong to $\mathscr{U}$, so does $U\cap V$.*

Proof. Map $G\to G/U\times G/V$ by sending σ to $(\sigma U,\sigma V)$. Then σ and τ have the same image iff $\sigma U=\tau U$ and $\sigma V=\tau V$. Equivalently, $\tau^{-1}\sigma\in U$ and $\tau^{-1}\sigma\in V$ so $\tau^{-1}\sigma\in U\cap V$. Thus the image is $G/U\cap V$. Of course the image is a sub-G-set which is complemented so $G/U\cap V$ is in $\mathscr{C}$ by 5.2.

Lemma 5.5. *If $U\in\mathscr{U}$, so does $\bigcap_{\sigma\in G}\sigma U\sigma^{-1}$.*

Proof. This follows immediately as soon as we know there are only finitely many conjugates. But an open subgroup in a compact hausdorff group has finite index, whence so does its normalizer.

Lemma 5.6. *Let $V\supset U\in\mathscr{U}$. Then $V\in\mathscr{U}$.*

Proof. Let $W=\bigcap\sigma U\sigma^{-1}$. Then W is open and normal. Since $G/V\cong(G/W)/(V/W)$, there is a coequalizer

$$G/W\times_{G/V}G/W\rightrightarrows G/W\to G/V.$$

But $G/W\times_{G/V}G/W\cong V/W\times G/W$ and so G/V is a quotient modulo the action of V/W on G/W.

Lemma 5.7. *Let $N=\bigcap\{U\mid U\in\mathscr{U}\}$. Then any open $V\supset N$ belongs to $\mathscr{U}$.*

Proof. For any $U_1,\dots,U_n\in\mathscr{U}$, $U_1\cap\cdots\cap U_n-V$ is a closed subset of the compact group G and the set of all possible sets of that form is closed under finite intersection. If none of them were empty, $H-V$ would be non-empty by compactness. Thus V contains some finite intersection whence $V\in\mathscr{U}$.

This completes the proof of 5.1.

6. Finitely additive sites

Let $\mathscr{C}$ be a standard left exact site. We say that $\mathscr{C}$ is an additive site if

(i) $\mathscr{C}$ has finite sums which are disjoint and universal;
(ii) $1+1\to1$ is a cover;
(iii) the two coproduct injections $1\to1+1\leftarrow1$ are a cover;
(iv) the empty sieve covers the initial object.

We let $\mathscr{F}(\mathscr{C})$ denote the category of sheaves on a site $\mathscr{C}$.

Proposition 6.1. *Let $\mathscr{C}$ be an additive site. Then,*

(i) *If $\{A_i\to A\}$ and $\{B_j\to B\}$ are covers, so is $\{A_i,B_j\to A+B\}$;*
(ii) *If $A=A_1+\cdots+A_n$, then $\{A_i\to A\}$ is a cover;*
(iii) *The Yoneda embedding $\mathscr{C}\to\mathscr{F}(\mathscr{C})$ preserves sums.*

Proof. (i) Since

$$\begin{tikzcd}
A \arrow[r] \arrow[d] & A+B \arrow[d] & B \arrow[l] \arrow[d] \\
1 \arrow[r] & 1+1 & 1 \arrow[l]
\end{tikzcd}$$

are pullbacks, it follows that $\{A, B \to A+B\}$ is a cover, from which the conclusion follows.

(ii) Follows by induction from (i).

(iii) Obvious.

Since $\mathscr{C}$ has disjoint universal sums, there is a functor Δ from finite sets to $\mathscr{C}$, just as in the case of a topos. We will say that an object A is a finite covering if there is a cover $\{U_i \to 1\}$ and a finite set n such that $A \times U_i \cong \Delta n \times U_i$ for each i.

Proposition 6.2. *Suppose that the covers $\{U_i \to 1\}$ have the property that $U_i \times -$ preserve coequalizers. Let the finite group G act on the finite covering A and suppose*

$$\Delta G \times A \rightrightarrows A$$

has a coequalizer. Then the coequalizer is preserved by the Yoneda embedding.

Proof. Let

$$\Delta G \times A \rightrightarrows A \to A/G$$

be a coequalizer. Let $\{U_i \to 1\}$ be a cover such that $U_i \times -$ preserves coequalizers. Then for each i, the rows of

$$\begin{tikzcd}
\Delta G \times A \times U_i \times U \arrow[r, shift left] \arrow[r, shift right] \arrow[d, shift left] \arrow[d, shift right] & A \times U_i \times U_i \arrow[r] \arrow[d, shift left] \arrow[d, shift right] & A/G \times U_i \times U_i \arrow[d, shift left] \arrow[d, shift right] \\
\Delta G \times A \times U_i \arrow[r, shift left] \arrow[r, shift right] \arrow[d] & A \times U_i \arrow[r] \arrow[d] & A/G \times U_i \arrow[d] \\
\Delta G \times A \arrow[r, shift left] \arrow[r, shift right] & A \arrow[r] & A/G
\end{tikzcd}$$

are coequalizers, the middle row has the form

$$\Delta G \times \Delta n \times U_i \rightrightarrows \Delta n \times U_i \to A/G \times U_i$$

and the top row is similar. Using the same considerations as in the proof of 1.5 applied in $\mathscr{C}/U_i$, we can break U_i into a finite number of pieces U_{ij} so that on each piece the maps $\Delta G \times \Delta n \times U_{ij} \rightrightarrows \Delta n \times U_{ij}$ are induced by maps $\Delta G \times \Delta n \rightrightarrows \Delta n$ where coequalizer is Δm. Then $A/G \times U_{ij} \cong \Delta m \times U_{ij}$. Applying the associated sheaf function, it is still a coequalizer. Now writing $A^\sim$ for the sheaf associated to A, we have in $\mathscr{F}(\mathscr{C})$,

$$\begin{tikzcd}
\sum \Delta G \times A^\sim \times U_{ij} \times U_{kl} \arrow[r, shift left] \arrow[r, shift right] \arrow[d, shift left] \arrow[d, shift right] & \sum A^\sim \times U_{ij} \times U_{kl} \arrow[r] \arrow[d, shift left] \arrow[d, shift right] & \sum (A/G)^\sim \times U_{ij} \times U_{kl} \arrow[d, shift left] \arrow[d, shift right] \\
\sum \Delta G \times A^\sim \times U_{ij} \arrow[r, shift left] \arrow[r, shift right] \arrow[d] & \sum A^\sim \times U_{ij} \arrow[r] \arrow[d] & \sum (A/G)^\sim \times U_{ij} \arrow[d] \\
\Delta G \times A^\sim \arrow[r, shift left] \arrow[r, shift right] & A^\sim \arrow[r] & (A/G)^\sim
\end{tikzcd}$$

in which all columns and the top two rows are reflexive coequalizers and hence so is the third.

We say that the *site* $\mathscr{C}$ is *connected* if there is no cover $\{U_i \to 1\}$ which can be decomposed into two sets $\{U_j \to 1\}$ and $\{U_k \to 1\}$ in such a way that $U_j \times U_k = 0$ for all j and k.

Let U be a cover of 1. Say that an object A is a *finite covering*, split by U, if $A \times U \cong \Delta n \times U$ for some finite cardinal n.

Theorem 6.3. *Let $\mathscr{C}$ be a connected additive site. If the covers of* 1, $\{U_i \to 1\}$ *have the property that every* $- \times U_i$ *preserve coequalizers, then the full subcategory of $\mathscr{C}$ consisting of the finite coverings is a galois category.*

Proof. This follows from the results of this section applied in 5.1.

6.4. There is a slight generalization of the conditions of this theorem which lead to the same conclusion. Begin as before with a connected additive site. Replace the condition on covers by supposing that whenever a finite group acts on an object A, there is a quotient A/G; that the canonical $A \to A/G$ is a cover; and that the canonical

$$\Delta G \times A \to A \times_{A/G} A$$

is a cover.

7. Galois theory of commutative algebras in a topos

Let $\mathscr{E}$ be a topos with an object of natural numbers. Let R be a commutative algebra object in $\mathscr{E}$, $\mathrm{Mod}\,R$ the category of R-modules in $\mathscr{E}$ and $\mathscr{C}^{\mathrm{op}}$ the category of commutative R-algebras in $\mathscr{E}$. The following facts about $\mathrm{Mod}\,R$ are found in Howe [8].

7.1. If M_1, M_2, N are R-modules, a bilinear map $f: M_1 \times M_2 \to N$ can be defined in such a way that three pairs of maps

$$M_1 \times M_1 \times M_2 \rightrightarrows M_1 \times M_2,$$

$$M_1 \times M_2 \times M_2 \rightrightarrows M_1 \times M_2,$$

$$M_1 \times R \times M_2 \rightrightarrows M_1 \times M_2$$

are simultaneously coequalized. This defines a three-place functor $\mathrm{Bilin}(M_1, M_2; N)$. With the existence of free R-modules assured by the natural number object, it is easy to see that this functor is representable by an object denoted $M_1 \otimes_R M_2$ or simply $M_1 \otimes M_2$. It is also easy to see that $- \otimes_R -$ satisfies the usual associativity and commutativity isomorphisms and that R is a 2-sided unit.

7.2 The category of R-modules is a closed category with internal hom $[M,N] \subset N^M$ and $[M_1 \otimes M_2, N] \cong [M_1, [M_2, N]]$. It follows that $M \otimes (N_1 \times N_2) \cong (M \otimes N_1) \times (M \otimes N_2)$ where $N_1 \times N_2$ is both the sum and the product of N_1 and N_2.

7.3. If $M_1' \to M_1 \to M_1'' \to 0$ is an exact sequence of R-modules, then for each R-module N,

$$0 \to \mathrm{Hom}(M_1'', N) \to \mathrm{Hom}(M_1, N) \to \mathrm{Hom}(M_1', N)$$

is an exact sequence of abelian groups. Replacing N by $[M_2, N]$ and using adjointness, we see that

$$0 \to \mathrm{Hom}(M_1'' \otimes M_2, N) \to \mathrm{Hom}(M_1 \otimes M_2, N) \to \mathrm{Hom}(M_1' \otimes M_2, N)$$

is exact from which so is

$$M_1' \otimes M_2 \to M_1 \otimes M_2 \to M_1'' \otimes M_2 \to 0.$$

Similarly $\otimes$ is right exact in the second variable.

7.4. From these facts it follows easily that a commutative R-algebra A is an R-module equipped with a map $R \to A$ and a map $A \otimes A \to A$ satisfying the evident identities. If A and B are R-algebras, their sum and product are $A \otimes B$ and $A \times B$ equipped with the obvious structures. Thus products in $\mathscr{C}$ (which recall, is the opposite of the category of R-algebras) distribute over finite sums. By replacing R by an R-algebra S, we see that pullbacks distribute as well. Moreover, it is easily checked that $A \times B \to A$ is epi, that

$$\begin{tikzcd}
A \times B \arrow[r] \arrow[d] & A \arrow[d] \\
B \arrow[r] & 0
\end{tikzcd}$$

is a pushout and that 0 is a strict terminal object in $\mathscr{C}^{\mathrm{op}}$. Hence $\mathscr{C}$ has finite sums that are disjoint and universal.

7.5. It is necessary to describe a topology. There may be other choices but one which works well is to take (as cocovers, since we are in the dual category) all finite families $\{S \to S_i\}$ such that if $S' = \prod S_i$, then each of S and S' is isomorphic, as S-modules, to a retract of a finite direct sum of copies of the other. We call such an S' an *S-progenerator*. This is not to suggest it is projective, although it is internally so.

We must show that this is a topology. Given a cover $\{R \to S_i\}$ we must show that

$$R \to \prod S_i \rightrightarrows \prod S_i \otimes S_j$$

is an equalizer. Given the couniversal products, it is equivalent to take $S = \prod S_i$ and show that $R \to S \rightrightarrows S \otimes S$ is an equalizer. To begin with, $R \to S$ must be mono because its kernel is annihilated by any R-linear $R \to S^n$ which would contradict R being a retract. Next I claim that for any R-module $M, M \to S \otimes M$ is mono. In fact if K is the kernel,

$$0 \to K \to M \to S \otimes M$$

is exact. Since S is an R-progenerator $S \otimes -$ is exact and the reciprocal condition implies it is faithful. Then

$$0 \to S \otimes K \to S \otimes M \to S \otimes S \otimes M$$

is exact. But $S \otimes M \to S \otimes S \otimes M$ is a split mono, split by the multiplication map on S, whence $S \otimes K = 0$, so that $K = 0$. Now from the exactness of

$$\begin{tikzcd}
 & 0 \arrow[d] & 0 \arrow[d] & 0 \arrow[d] & \\
0 \arrow[r] & R \arrow[r] \arrow[d] & S \arrow[r] \arrow[d] & S/R \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & S \arrow[r] \arrow[d] & S \otimes S \arrow[r] \arrow[d] & S \otimes S/R \arrow[r] \arrow[d] & 0 \\
0 \arrow[r] & S/R \arrow[r] \arrow[d] & S/R \otimes S \arrow[r] \arrow[d] & S/R \otimes S/R \arrow[r] \arrow[d] & 0 \\
 & 0 & 0 & 0 &
\end{tikzcd}$$

it follows that the upper left corner is a pullback. If $\{R \to S_i\}$ satisfies the condition, so does $\{T \to S_i \otimes T\}$ for any R-algebra T, whence the universality.

Then if we define a galois extension of R to be an R-algebra A such that $S_i \otimes A = S_i^n$ for a cover $\{R \to S_i\}$, the full subcategory of galois extensions of R forms a galois category. Of course, the $\{S_i\}$ may as well be replaced by $\prod S_i$.

How does the galois theory described here compare when $\mathscr{E} = \mathscr{S}et$ with that of Chase, Harrison and Rosenberg [4], see also Magid [9]? It is shown in Barr [2] that an R-algebra A is strongly separable iff $S \otimes A \cong S^n$ for a faithfully flat R-algebra S. It is easily seen that the topology described above considers S which are finitely generated projective generators. Clearly, then, any A which is split by such an S is strongly separable. Conversely, any strongly separable A is split by a strongly separable B which is a finitely generated projective generator. Hence the two notions coincide. In fact, using the results of DeMeyer and Ingraham [5], III.1.2, part 4), in conjunction with 6.4, it is even possible to show that the topology can be taken to be the canonical one: universally regular monomorphic families.

8. Example: Regular rings

By a commutative VNR (von Neumann regular) ring object in a category we mean a commutative ring object R equipped with an endomorphism $(\ )' : R \to R$ such that $x^2x' = x$ and $xx'^2 = x'$. One of the many characterizations of a field in $\mathscr{S}et$ is that it is a connected commutative VNR ring. This characterization has not been used as a possible definition of field in a topos, presumably because connectedness is not an internal notion. Nonetheless, it seems to be an appropriate notion for galois theory, as we will see.

First, here are two examples of connected commutative VNR rings in the category of set-valued functors on the category

$$\begin{tikzcd} \bullet \arrow[r, "u"] & \bullet \arrow[loop right, "t"] \end{tikzcd}$$

with two non-identity maps such that $t^2 = \mathrm{id}$ and $tu = u$. The first is

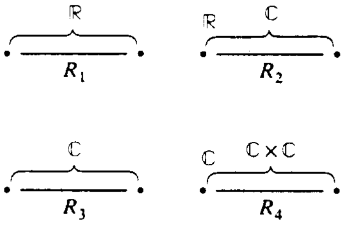
$$\begin{tikzcd} \mathbb{R} \arrow[r] & \mathbb{C} \end{tikzcd}$$

with complex conjugation as the involution. The second is

$$\begin{tikzcd} \mathbb{C} \arrow[r] & \mathbb{C} \times \mathbb{C} \end{tikzcd}$$

with the involution which exchanges the two factors. There is an obvious inclusion of the first into the second (using $(\mathrm{id}, \overline{(\ )})$ on the second value) and from the point of view of this paper the second is the separable closure of the first. Yet the first is and the second isn't a geometric field.

A similarly suggestive examples comes in the category of sheaves on the unit interval. Here are four ring objects R_1, R_2, R_3, R_4, indicated by showing what the stalks are.



Then it is not hard to see that although $R_1 \subseteq R_2 \subseteq R_3 \subseteq R_4$, R_3 is a separable extension of R_1 and R_4 is a separable extension of R_2 but none of the other inclusions is separable; that R_2 and R_4 are separably closed; that R_1, R_2 and R_3 are geometric fields but R_4 is not and that all four are connected commutative VNR ring objects.

Let $\mathcal{F}$ be any ℕ-standard topos. This means that $\mathcal{F}$ not only has a natural numbers object but that the standard morphisms $1 \xrightarrow{i} \mathbb{N}$ as runs through the ordinary integers form an epimorphic family. Freyd shows that any such topos, if countable (meaning there are countably many morphism together), has a faithful family of set-valued functors that preserve all finite limits and finite colimits as well as ℕ. Since constructions like free R-modules and tensor products are constructed using finite limits and colimits and ℕ, these are all preserved by such functors. Of course, the internal hom is not, since it is built out of the exponential, but that was only used in passing, to derive the exactness properties of the tensor.

We take for topology the same as before; a cover $\{S \to S_i\}$ is a finite sieve such that $\prod S_i$ is an S-progenerator. Now the R-algebra is a finite covering – and is strongly separable – iff there is a cover $\{R \to R_i\}$ such that $R_i \otimes A \cong R_i^n$ for each i. Since the covers are finite we can replace this sieve by $S = \prod R_i$ and say that A is a finite covering iff there is an R-algebra A which is an R-progenerator such that $S \otimes A \cong S^n$ (as an S-algebra).

Theorem 8.1. *Let R be a commutative ring object in a topos and A a finite covering. If R is a VNR ring, so is A.*

Proof. The idea is to prove it in $\mathcal{S}et$ and use the representation theorem of Freyd to do it in general.

Lemma 8.2. Let A be a commutative ring (in $\mathcal{S}et$) such that A_M is a field for every maximal ideal M. Then A is a VNR ring.

Proof. (For which, many thanks to J. Lambek). If A_M is field, the only field it can be is A/M. Thus every element in M must have a zero divisor outside of M. Thus for each $a \in M$, $\operatorname{ann}(a) \not\subset M$. On the other hand for each $a \notin M$, there is a $b \in R$ such that $ab - 1 \in M$ which means $ab - 1$ has an annihilator outside of M. Thus for each $a \in R$,

$$\operatorname{ann}(a) + \sum_{b \in R} \operatorname{ann}(ab - 1) \not\subset M.$$

Fixing a and letting M vary, the above expression defines an ideal not contained in any maximal ideal, whence it is all of R. Thus there is a finite set $b_1, \dots, b_n$ such that $1 = x + \sum y_i$ where $xa = 0$ and $y_i(ab_i - 1) = 0$. This gives $a = \sum ay_i$ while $ay_i(ab_i - 1) = 0$ gives $a^2y_ib_i = ay_i$ so $a = \sum a^2y_ib_i = a^2(\sum y_ib_i)$. Thus $\sum y_ib_i$ is a candidate for a'. (Replace a' by a'^2a to get one for which also $a'^2a = a'$.)

Now if R is a VNR ring and A a strongly separable extension, then for any maximal ideal $M \subset A$, $N = M \cap R$ is a prime ideal of R. In a VNR ring every prime is maximal, so N is maximal. Then by [5], Chapter II, Corollary 1.7 on p. 44, $R_N \otimes A$ is a separable extension of R_N, hence is a product of a finite number of field extensions. Now

$$R_N \otimes A \cong (R - N)^{-1}A = (R - M)^{-1}A \subset (A - M)^{-1}A = A_M$$

so that A_M is a localization of a finite product of separable field extensions and is local so it must be one of them. Thus A_M is a field for every M and A is VNR.

For a general topos first observe that a commutative ring object R is VNR iff for every $\Phi : \mathscr{T} \to \mathscr{S}et$ which is left exact, ΦR is. This is because these rings can be characterized by saying that if

$$W = \{(a, a') \mid a^2a' = a \,\&\, aa'^2 = a'\}$$

then the composite

$$\begin{tikzcd} W \arrow[r] & R \times R \arrow[r, "p_1"] & R \end{tikzcd}$$

is an isomorphism. Of course, instead of considering all Φ it is sufficient to take a faithful family. A standard argument shows that if Φf is an isomorphism for a faithful family of Φ, then f is.

Suppose S is an extension of R which is an R-progenerator and A is an R-algebra split by S. Let $\mathscr{T}_0$ be a countable exact subcategory of $\mathscr{T}$ (not full) which is a topos and contains $\mathbb{N}$, Ω, R, S, A, $R \otimes R$, $R \otimes R \otimes R$, $R \otimes S, \dots, S \otimes A, \dots$ as well as all maps necessary to state the universal mapping properties of these objects. This exists by standard methods. Begin with the above objects and add 0 and 1 and the terminal and initial maps along with countably many global sections of $\mathbb{N}$ and global sections true and false of Ω. You also need two global section (for the unit and zero) in $R, S, A, S \otimes A$. Then add to $\mathscr{T}_0$ all sums of pairs of objects, along with injections and maps out of the sum where coordinates already belong to $\mathscr{T}_0$. Do similar things for products, coequalizers and equalizers. Iterate countably often, taking care that along the way the maps required to describe R, S, A as rings, S and A as R-algebras and each of R and S as R-linear retracts of a finite power of the other, are included. In particular, the construction of the relevant tensor products from finite limits, colimits and $\mathbb{N}$ will be able to be carried out in the resultant $\mathscr{T}_0$. Now if $\Phi : \mathscr{T}_0 \to \mathscr{S}et$ is exact and preserves $\mathbb{N}$, then $S \otimes A \cong S^n$ implies that $\Phi S \otimes \Phi A \cong (\Phi S)^n$ so ΦA is a separable extension of ΦR and hence a VNR ring. The desired result follows from the existence of enough such Φ (Freyd [6, 5.65]).

Corollary 8.3. *Let R be a connected commutative VNR ring in a topos $\mathscr{F}$. Then the category of separable VNR extensions of R is a galois category.*

This gives, then, a galois theory for connected, commutative VNR rings.

References

[1] M. Auslander and D.A. Buchsbaum, On ramification theory in local rings, J. Algebra 11 (1969) 532–563.

[2] M. Barr, Abstract galois theory, J. Pure Appl. Algebra 19 (1980) 21–42.

[3] M. Barr and R. Diaconescu, On locally simply connected toposes and their fundamental groups, Cahiers Topologie Géométrie Différentielle 22 (1981) 301–314.

[4] S.U. Chase, D.K. Harrison and A. Rosenberg, Galois Theory and Cohomology of Commutative Rings, Mem. Amer. Math. Soc. 52 (1965).

[5] F. DeMeyer and E. Ingraham, Separable Algebras Over Commutative Rings, Lecture Notes in Math. No. 181 (Springer, Berlin–New York, 1971).

[6] P. Freyd, Aspects of topoi, Bull. Austral. Math. Soc. 7 (1972) 1–76.

[7] P. Freyd, Aspects of topoi, Corrigendum and addendum, Bull. Austral. Math. Soc. 7 (1972) 467–480.

[8] D. Howe, Module categories over topoi, J. Pure Appl. Algebra 21 (1981) 161–166.

[9] A. Magid, The Separable Galois Theory of Commutative Rings (Marcel Dekker, New York, 1974).

[10] A. Grothendieck, dir., Séminaire de Géométrie Algébrique du Bois Marie 1960/61, Lecture Notes in Math. No. 224 (Springer, Berlin–New York, 1971).

[11] O.E. Villamayor, Separable algebras and galois extensions, Osaka J. Math. 4 (1967) 161–171.

[12] O.E. Villamayor and D. Zelinsky, Galois theory for rings with finitely many idempotents, Nagoya Math. J. 27 (1966) 721–731.

[13] O.E. Villamayor and D. Zelinsky, Galois theory with infinitely many idempotents, Nagoya Math. J. 35 (1969) 83–98.

[14] P.T. Johnstone, Topos Theory, LMS Mathematical Monographs No. 10 (Academic Press, New York, 1977).