UNRAMIFIED CLASS FIELD THEORY FOR ORDERS

PETER STEVENHAGEN

ABSTRACT. The main theorem of unramified class field theory, which states that the class group of the ring of integers of a number field K, is canonically isomorphic to the Galois group of the maximal totally unramified abelian extension of K over K, is generalized and proved for all infinite commutative rings with unit that, like rings of integers, are connected and finitely generated as a module over $\mathbf{Z}$. Modulo their nilradical, these rings are exactly the connected orders in products of number fields.

1. INTRODUCTION

Let H be the Hilbert class field of an algebraic number field K, i.e. the maximal abelian extension of K that is unramified at both finite and infinite primes of K. A famous theorem from class field theory, conjectured by Hilbert [8] in 1902 and proved by Furtwängler (1907), Takagi (1920) and Artin (1927) then states that the Galois group of H over K is canonically isomorphic to the class group of the ring of integers A of K. The isomorphism $\psi : \mathrm{Cl}(A) \xrightarrow{\sim} \mathrm{Gal}(H/K)$ is given by $\psi([\mathfrak{p}]) = (\mathfrak{p}, H/K)$ for the ideal class $[\mathfrak{p}]$ of a finite prime $\mathfrak{p}$ of K. Here the Artin symbol $(\mathfrak{p}, H/K)$ is defined as the unique element of $\mathrm{Gal}(H/K)$ that induces the Frobenius automorphism on the residue class field extensions at $\mathfrak{p}$. More details and a proof of the theorem can be found in [9].

It is the aim of this paper to state and prove an analogous theorem for all infinite commutative rings with unit that are connected with finitely generated additive group. Examples of such rings are orders R in number fields and group rings $R[G]$ over such R for finite abelian groups G. Since "class group" and "Hilbert class field" do not have an obvious meaning for these rings we have to make use of suitable generalizations.

A convenient generalization of the class group is provided by the Grothendieck group of the category of finitely generated modules over the ring in question, or, more precisely, the torsion subgroup of this group. The Galois group of the Hilbert class field is replaced by an algebraic fundamental group, which is defined for all connected commutative rings with unit element. In this way the

main theorem of unramified class field theory quoted above can be formulated as an isomorphism between the torsion subgroup of the Grothendieck group of a ring of integers and a suitable factor group of the fundamental group of this ring. The ramification of infinite primes needs special care in this formulation. It turns out that in this form, the theorem admits an almost direct generalization to the class of rings mentioned above.

The generalized theorem is essentially a theorem for orders in products of number fields. We show that, by dividing out the nilradical of our ring and embedding the factor ring in a product of rings of integers B, we may reduce immediately to this case. Using the explicit form of the Grothendieck group of the larger ring B and an exact sequence for Grothendieck groups valid in a fairly general context, we obtain a description of the Grothendieck group we are interested in. An analogous procedure is followed for the fundamental group, but now the exact sequence is replaced by an algebraic van Kampen theorem. A van Kampen theorem expresses the fundamental group of a space in terms of the fundamental groups of spaces that somehow constitute the space. The natural formulation of such a theorem makes use of groupoids rather than groups. It appears that the computation of our fundamental group matches that of the Grothendieck group to a certain extent. This similarity is employed to obtain the required map from the isomorphism in the number field case.

In the next section we give a precise statement of the theorems that were informally discussed in this section. The main theorem 2.2 appears as a generalization of the classical result as formulated in Theorem 2.1. §3 contains all we need about Grothendieck groups, §4 discusses the van Kampen theorem for fundamental groups and treats our special case in detail. After the reformulated classical theorem has been dealt with in §5, §6 completes the proof of our main result.

2. STATEMENT OF RESULTS

For the rest of this paper, we define a *ring* to be a commutative ring with unit element. A ring homomorphism maps unit elements to unit elements.

For a ring A, let $\mathrm{Id}(A)$ denote the set of idempotent elements of A. We endow $\mathrm{Id}(A)$ with a vector space structure over the finite field $\mathbf{F}_2$ by defining an addition & in $\mathrm{Id}(A)$ as $e_1 \& e_2 = e_1 + e_2 - 2e_1 e_2$. A ring A is said to be *connected* if $\mathrm{Id}(A) = \{0, 1\}$, $0 \neq 1$. One easily sees that a ring is connected if and only if its spectrum $\mathrm{spec}\, A$ [6, II.2] is connected as a topological space. We say that A has finitely many connected components if $\mathrm{spec}\, A$ has. One can show that if the number of connected components of A is finite, it is equal to the *idempotent rank* $\dim_{\mathbf{F}_2} \mathrm{Id}(A)$ of A.

For any connected ring A with geometric point x, we denote by $\pi(A, x)$ the fundamental group of A with respect to x (cf. [13] or [5]). The fundamental group $\pi(A)$ in itself is only defined up to inner automorphisms. The abelianized fundamental group $\pi(A)_{\mathrm{ab}}$ of A is the quotient group $\pi(A, x)/C$, where C is the closure of the commutator subgroup of $\pi(A, x)$. It is independent of

the choice of the geometric point x, and the assignment $A \mapsto \pi(A)_{\text{ab}}$ defines a contravariant functor from the category of connected rings to the category of profinite abelian groups. For a ring homomorphism $f: A \to B$ we denote the induced homomorphism $\pi(B)_{\text{ab}} \to \pi(A)_{\text{ab}}$ by f^*.

If K is a field and x maps K into a separable closure K^{sep} of K, there is a canonical isomorphism $\pi(K, x) \cong \text{Gal}(K^{\text{sep}}/K)$. In particular, if $K = \mathbf{F}_q$ is a finite field of q elements, we have isomorphisms $\pi(\mathbf{F}_q) \cong \text{Gal}(\mathbf{F}_q^{\text{sep}}/\mathbf{F}_q) \cong \widehat{\mathbf{Z}}$. Here $\widehat{\mathbf{Z}}$ is the profinite completion of the ring of rational integers $\mathbf{Z}$. Under the isomorphism $1 \in \widehat{\mathbf{Z}}$ corresponds to the Frobenius automorphism of $\mathbf{F}_q^{\text{sep}}/\mathbf{F}_q$ raising all elements to the q th power. More generally, let A be a connected ring and $\mathfrak{m}$ a maximal ideal of finite index in A. Then the Frobenius in $\pi(A)_{\text{ab}}$ at $\mathfrak{m}$ is defined as the image of the Frobenius automorphism under the canonical map $\text{Gal}((A/\mathfrak{m})^{\text{sep}}/(A/\mathfrak{m})) \cong \pi(A/\mathfrak{m}) \to \pi(A)_{\text{ab}}$.

The *Grothendieck group* $G(A)$ of a ring A is the group generated by elements $[P]$, one for each isomorphism class of finitely generated modules P over A, where a relation $[P_1] + [P_2] = [P_3]$ is imposed for each short exact sequence $0 \to P_1 \to P_3 \to P_2 \to 0$ of finitely generated A-modules.

The following theorem shows that the main theorem of unramified class field theory can be formulated in terms of Grothendieck groups and fundamental groups.

2.1   Theorem. *Let K be a number field, A its ring of integers and H its Hilbert class field. Then the four arrows in the following diagram are well defined and establish isomorphisms of finite abelian groups.*

$$
\begin{array}{ccc}
\text{Cl}(A) & \xrightarrow{\ \psi\ } & \text{Gal}(H/K) \\
\downarrow & & \downarrow \\
G(A)_{\text{tor}} & \longrightarrow & \pi(A)_{\text{ab}}/\langle \tau^* \pi(\mathbf{R}) \rangle_{\tau:\, A \to \mathbf{R}}
\end{array}
$$

$$
\begin{array}{ccc}
[\mathfrak{p}] & \longmapsto & (\mathfrak{p}, H/K) \\
\downarrow & & \downarrow \\
[A/\mathfrak{p}] & \longmapsto & \overline{\phi}_{\mathfrak{p}}
\end{array}
$$

Here we use the notation $\langle \tau^* \pi(\mathbf{R}) \rangle_{\tau:\, A \to \mathbf{R}}$ for the subgroup of $\pi(A)_{\text{ab}}$ generated by the images $\tau^* \pi(\mathbf{R})$ of $\pi(\mathbf{R})$ when τ runs over the ring homomorphisms $A \to \mathbf{R}$. Further $\mathfrak{p}$ denotes a nonzero prime ideal of A with Artin symbol $(\mathfrak{p}, H/K)$ in $\text{Gal}(H/K)$ and Frobenius $\phi_{\mathfrak{p}}$ in $\pi(A)_{\text{ab}}$. The class of the module $A/\mathfrak{p}$ in the torsion subgroup $G(A)_{\text{tor}}$ of the Grothendieck group $G(A)$ is denoted by $[A/\mathfrak{p}]$.

The proof of this theorem will be given in §5. Our main result generalizes the Artin isomorphism as follows.

2.2   Theorem. *Let A be an infinite ring that is connected and finitely generated as an additive group. Then there is an exact sequence of abelian groups*

$$0 \to .G(A)_{\mathrm{tor}} \xrightarrow{f} \pi(A)_{\mathrm{ab}}/\langle \tau^*\pi(\mathbf{R})\rangle_{\tau:\, A\to\mathbf{R}} \to \widehat{\mathbf{Z}}^k \to 0$$

where f maps the class of $A/\mathfrak{p}$ in $G(A)_{\mathrm{tor}}$ to the residue class of the Frobenius in $\pi(A)_{\mathrm{ab}}$ at $\mathfrak{p}$ for each maximal ideal $\mathfrak{p}$ of A. The integer k is equal to the idempotent rank $\dim_{\mathbf{F}_2}[\mathrm{Id}(\widehat{A}\otimes_{\mathbf{Z}}\mathbf{Q})/(\mathrm{Id}(\widehat{A}) \,\&\, \mathrm{Id}(A\otimes_{\mathbf{Z}}\mathbf{Q}))]$ with $\widehat{A} = \varprojlim A/nA$, $n \in \mathbf{Z}_{\geq 1}$.

An explicit form of the integer k will appear from the proof of the theorem in §6.

Remark. Just as in the number field case, there exists an Artin isomorphism for function fields of curves over finite fields. It may be expected that an analogue of our generalization 2.2 can be proved in this context. Geometrically speaking, this would give an Artin isomorphism for (possibly singular or reducible) curves over a finite field. We shall not pursue this matter any further in this paper.

3. GROTHENDIECK GROUPS

In the previous section we defined the Grothendieck group $G(A)$ of a ring A as the Grothendieck group of the category of finitely generated A-modules. In case A is the ring of integers of a number field or, more generally, a Dedekind domain, there is an explicit description of the group $G(A)$. This is due to the fact that finitely generated modules over a Dedekind ring are easily classified.

3.1   Proposition. *Let M be a finitely generated module over a Dedekind ring A. Then there are nonzero ideals $\mathfrak{a}_1, \mathfrak{a}_2, \ldots, \mathfrak{a}_r$ and $\mathfrak{b}_1, \mathfrak{b}_2, \ldots, \mathfrak{b}_s$ of A such that*

$$M \cong \left(\bigoplus_{i=1}^{r} A/\mathfrak{a}_i\right) \oplus \left(\bigoplus_{i=1}^{s} \mathfrak{b}_i\right).$$

For a proof, see [4, Proposition 4.16]. The following description of the Grothendieck group is obtained.

3.2   Theorem. *Let A be a Dedekind ring with class group Cl. Then there is an isomorphism*

$$\begin{array}{ccc} G(A) & \xrightarrow{\;\sim\;} & \mathrm{Cl}\oplus\mathbf{Z} \\[2mm] \left[\left(\displaystyle\bigoplus_{i=1}^{r} A/\mathfrak{a}_i\right) \oplus \left(\displaystyle\bigoplus_{i=1}^{s} \mathfrak{b}_i\right)\right] & \longrightarrow & \left(\displaystyle\prod_{i=1}^{r}[\mathfrak{a}_i]\cdot\prod_{i=1}^{s}[\mathfrak{b}_i]^{-1},\, s\right). \end{array}$$

We see from 3.2 that for a ring of integers of a number field, the torsion part of the Grothendieck group is indeed isomorphic to the class group. The main result in this section (Theorem 3.4) is the existence of an exact sequence that generalizes 3.2 to the class of rings we are interested in in this paper. We will show later that 3.2 can be obtained as a special case of 3.4. Most of the

preparatory work for 3.4 is contained in a result of Heller and Reiner as stated in [2].

For a ring A, the group $G^{\text{tor}}(A)$ will be the Grothendieck group of the category of finitely generated torsion modules over A. An A-module M is said to be *torsion* if $M \otimes_A K = 0$ for the total ring of fractions K of A. Recall that the *total ring of fractions* of the ring A is the localization $K = S^{-1}A$ with S the set of nonzero elements of A that are not zero-divisors. A finitely generated M is torsion if and only if $sM = 0$ for some $s \in S$.

A ring A is said to be *reduced* if its nilradical nil(A) is trivial.

What we need is the following specialization of the Heller-Reiner result.

3.3 Theorem. *Let A be a reduced Noetherian ring with total ring of fractions $K = S^{-1}A$. Then there is an exact sequence of groups*

$$K^* \xrightarrow{f} G^{\text{tor}}(A) \xrightarrow{g} G(A) \xrightarrow{h} G(K) \to 0.$$

Here g is the canonical map induced by the inclusion of categories, h sends $[M] \in G(A)$ to $[M \otimes_A K] \in G(K)$ and $f(\beta/\gamma) = [A/\beta A] - [A/\gamma A] \in G^{\text{tor}}(A)$ for $\beta, \gamma \in S$.

Proof. Since A is Noetherian its number of minimal prime ideals is finite. Denote them by $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$, then the natural map $A \to \prod_{i=1}^t A/\mathfrak{p}_i$ is injective as A is reduced. One easily verifies that the localization $K_i = A_{\mathfrak{p}_i}$ may be identified with the quotient field of $A/\mathfrak{p}_i$ and that there is an isomorphism $S^{-1}A = K \xrightarrow{\sim} \prod_{i=1}^t K_i$ mapping the set S into $\prod_{i=1}^t K_i^*$. Since A is Noetherian and $S^{-1}A$ is Artinian the following exact sequence is furnished by [2, IX 6.2]:

$$G_1(K) \xrightarrow{\partial} G^{\text{tor}}(A) \xrightarrow{g} G(A) \xrightarrow{h} G(K) \to 0.$$

Using the fact that K is a product of fields one easily applies [2, IX 2.1 and V 2.1] to see that the *Whitehead group* $G_1(K)$ is isomorphic to K^*. It follows from [2, IX 6.1] that $\partial = f$. This proves 3.3.

An explicit form of 3.3 can be given if A is of dimension ≤ 1, i.e., if every prime ideal of A is minimal or maximal. Since the sequence in 3.3 for a product of rings is the "direct sum" of the sequences for the constituents we may assume that A is connected. The importance of the dimension condition lies in the fact that over a connected Noetherian ring of dimension one, a module is finitely generated torsion if and only if it is *of finite length* (cf. [3, IV.5 Proposition 7]). If M is such a module, the number of times $l_{\mathfrak{m}}(M)$ that a quotient in a composition chain is isomorphic to $A/\mathfrak{m}$ for a maximal ideal $\mathfrak{m}$ of A depends only on M.

3.4 Theorem. *Let A be a reduced connected Noetherian ring of dimension one and t the number of connected components of its total ring of fractions $K = S^{-1}A$. Then there is an exact sequence*

$$K^* \xrightarrow{f} \bigoplus_{\mathfrak{m} \in \mathfrak{M}} \mathbf{Z} \cdot e_{\mathfrak{m}} \xrightarrow{g} G(A) \to \mathbf{Z}^t \to 0$$

where $\mathfrak{M}$ *is the set of maximal ideals of* A *and* $e_{\mathfrak{m}}$ *is the characteristic function of* $\{\mathfrak{m}\} \subset \mathfrak{M}$. *Here* $f(s) = (l_{\mathfrak{m}}(A/sA))_{\mathfrak{m}}$ *if* $s \in S$ *and* $g(e_{\mathfrak{m}}) = [A/\mathfrak{m}]$.

Proof. This is 3.3 with explicit forms of $G^{\mathrm{tor}}(A)$ and $G(K)$. We proved in 3.3 that K is a product of t fields. Since the Grothendieck group of a field is $\mathbf{Z}$ (it counts dimensions), we conclude that $G(K) \cong \mathbf{Z}^t$.

We observed already that $G^{\mathrm{tor}}(A)$ is isomorphic to $G^{\text{finite length}}(A)$. The isomorphism $G^{\text{finite length}}(A) \cong \bigoplus_{\mathfrak{m} \in \mathfrak{M}} \mathbf{Z} \cdot e_{\mathfrak{m}}$ is standard.

As a special case of 3.4 we prove 3.2.

Proof of 3.2. Let A be a Dedekind ring in 3.4. Then $t = 1$ and 3.4 gives

$$G(A) \cong \left(\bigoplus_{\mathfrak{m} \in \mathfrak{M}} \mathbf{Z} \cdot e_{\mathfrak{m}} / \mathrm{im}[K^*] \right) \oplus \mathbf{Z}.$$

Since the class of $[A/\alpha A] \in G^{\mathrm{tor}}(A)$ corresponds to $(\mathrm{ord}_{\mathfrak{m}}(\alpha))_{\mathfrak{m}} \in (\bigoplus_{\mathfrak{m} \in \mathfrak{M}} \mathbf{Z} \cdot e_{\mathfrak{m}})$ the first summand may be identified with the class group $\mathrm{Cl}(A)$ of A. Choosing the lift $G(A) \leftarrow \mathbf{Z}$ such that $[A] \in G(A)$ is the image of $1 \in \mathbf{Z}$ we obtain the isomorphism for $G(A)$ as stated in 3.2.

All results in this section were obtained for *reduced* rings A. The following elementary result shows that for Noetherian A, no information on the Grothendieck group is lost if we pass from A to the reduced ring $A_0 = A/\mathrm{nil}(A)$.

3.5   Theorem. *If* A *is Noetherian the natural map* $G(A_0) \to G(A)$ *is an isomorphism.*

Proof. This is a special case of [2, IX 2.3].

4. An algebraic van Kampen theorem

In this section we derive a van Kampen theorem for affine schemes. It will be our main tool in describing the structure of the group $\pi(A)_{\mathrm{ab}}$ occurring in our main theorem 2.2. As we observed in the introduction, the most convenient way to phrase a van Kampen theorem makes use of *groupoids* rather than groups.

A groupoid is a small category in which all morphisms are invertible. Its objects are called *vertices*, its morphisms *edges*. The edges from a vertex v to itself form a group, the *vertex group in* v. A *map* or *morphism* between groupoids is simply a functor. From a projective system of groupoids with a fixed vertex set one can form the projective limit. If all groupoids in the system have finite vertex groups, the resulting groupoid is called a *profinite groupoid*. Such groupoids have profinite vertex groups. They form the objects of a category **Pgrpd** of profinite groupoids. The morphisms in this category are the groupoid maps that induce *continuous* homomorphisms on the vertex groups. For a groupoid G, a *G-set* is a functor from G to the category of finite sets. Each vertex group of G acts on the set corresponding to the vertex. If G

is profinite, we only consider G-sets with continuous G-action. (Finite sets are viewed as discrete.) In the category G-**sets** of G-sets, morphisms are simply morphisms of functors. We refer the reader to [7] for further terminology and basic facts on groupoids.

In Galois theory for rings, the extensions of a ring A under consideration are the *projective separable A-algebras*. An A-algebra B is said to be projective separable if B is finitely generated projective as an A-module and the trace map $\mathrm{Tr} = \mathrm{Tr}_{B/A}$ induces an isomorphism

$$B \xrightarrow{\ \sim\ } B^* = \mathrm{Hom}_A(B, A),$$

$$b \longmapsto \quad (\beta \mapsto \mathrm{Tr}(b\beta)).$$

The main theorem of Galois theory for rings (cf. [11, Theorem I.5.3] or [5, V 4.1]) states that for a connected ring A with geometric point x, the fundamental group $\pi(A, x)$ of A at x classifies all projective separable A-algebras in the following way. Let $\mathbf{FEt}_A$ denote the category of finite étale coverings of $\mathrm{spec} A$, i.e. the coverings $\mathrm{spec} B \to \mathrm{spec} A$ coming from projective separable A-algebras B. The fundamental functor $F_x \colon \mathbf{FEt}_A \to \mathbf{sets}$ to the category of finite sets assigns to each $\mathrm{spec} B \in \mathbf{FEt}_A$ the set of extensions of x to B. Now $\pi(A, x)$ is defined as the automorphism group of the functor F_x. It is a profinite group acting naturally on each set $F_x(B)$, and the theorem states that an equivalence of $\mathbf{FEt}_A$ with the category $\pi(A, x)$-**sets** of finite sets with continuous $\pi(A, x)$-action is thus obtained.

If the ring A has finitely many connected components, an analogous theorem can be formulated using fundamental groupoids (cf. [5, V.9]). One chooses a set S of geometric points of A that is *sufficiently large* in the sense that for each connected component of $\mathrm{spec} A$, there is a point in S with kernel in this component. The groupoid $\pi(A, S)$ has vertex set S and for each pair $s_1, s_2 \in S$ the morphisms from s_1 to s_2 are the isomorphisms of the fundamental functors $F_{s_1} \xrightarrow{\sim} F_{s_2}$. Note that no such morphisms exist if s_1 and s_2 factor via different components of A and that the vertex groups are again profinite. As above, the set of geometric points S induces a functor $\mathbf{FEt}_A \to \pi(A, S)$-**sets** and it follows from the corresponding theorem for connected rings that this is an equivalence of categories.

The following van Kampen theorem computes the fundamental groupoid of a fibred product of rings in terms of the fundamental groupoids of the constituting rings. We will only be interested in abelian groupoids, i.e. groupoids whose vertex groups are abelian. Each profinite groupoid has an associated *abelianized* groupoid on the same vertex set. It is obtained by imposing an equivalence relation on the edges: one defines two edges $\alpha, \beta \colon s \to t$ to be equivalent if $\beta^{-1}\alpha$ is contained in the closure of the commutator subgroup of the vertex group at s. Note that the construction of the abelianized groupoid is functorial, and that it is left adjoint to the inclusion functor from the category of profinite

abelian groupoids to the category of profinite groupoids. For the categorical notions here and in the following theorem, we refer again to [7].

4.1 Theorem. *Suppose we are given rings* R_0, R_1, R_2 *and ring homomorphisms* $f_i: R_i \to R_0$, $i = 1, 2$, *satisfying the following hypotheses:*
  (i) f_1 *is surjective.*
  (ii) R_0, R_1 *and* R_2 *have finitely many components.*
Suppose further that there are sets S_i, $i = 0, 1, 2$, *of geometric points of* R_i *satisfying*
  (iii) S_i *is sufficiently large for* R_i.
  (iv) $s_0 \circ f_i \in S_i$ *for each* $s_0 \in S_0$ $(i = 1, 2)$.
Now let
$$R = R_1 \times_{R_0} R_2 = \{(r_1, r_2) \in R_1 \times R_2 : f_1(r_1) = f_2(r_2)\}$$
and $S = \bigcup_{i=1,2}\{s_i p_i : s_i \in S_i\}$ *with* p_i *the projection* $R \to R_i$. *Then* S *is sufficiently large for* R *and there is the following natural push-out square of fundamental groupoids in* **Pgrpd**.

$$
\begin{array}{ccc}
\pi(R_0, S_0) & \longrightarrow & \pi(R_1, S_1) \\
\downarrow & & \downarrow \\
\pi(R_2, S_2) & \longrightarrow & \pi(R, S)
\end{array}
$$

In the category of profinite abelian groupoids, the same statement is true for the abelianized fundamental groupoids.

Remark. Condition (i) is essential. One can show that this condition ensures that $\mathrm{spec}\,R$ is the fibred sum of $\mathrm{spec}\,R_1$ and $\mathrm{spec}\,R_2$ over $\mathrm{spec}\,R_0$ in the category of topological spaces.

4.2 Lemma. *Let the hypotheses be as in* 4.1 *and suppose projective separable algebras* B_i *over* R_i $(i = 0, 1, 2)$ *and* R_0-*algebra isomorphisms* $f_i: B_i \otimes_{R_i} R_0 \to B_0$ *are given. Then the ring*
$$B = B_1 \times_{B_0} B_2 = \{(b_1, b_2) \in B_1 \times B_2 : f_1 \phi_1(b_1) = f_2 \phi_2(b_2)\}$$
with $\phi_i: B_i \to B_i \otimes_{R_i} R_0$ *the natural map, is in a natural way a projective separable R-algebra. Conversely, every projective separable R-algebra B is isomorphic to an algebra* $B_1 \times_{B_0} B_2$ *defined in this way and the constituents* B_i *of B are naturally isomorphic to* $B \otimes_R R_i$.

Proof of 4.2. The result is proved in [12, Theorems 2.1–2.3] with 'projective separable algebra' everywhere replaced by 'finitely generated projective module'. It is here that condition 4.1(i) is used. If all B_i are algebras (over the respective rings) and the f_i are R_0-algebra isomorphisms, it is clear that B is an R-algebra. The converse is also true, so the result extends immediately to finite projective algebras.

   If B is projective separable over R, then B_i is projective separable over R_i since projective separability is stable under base extension. Conversely, let B_i

be projective separable over R_i, $i = 1, 2$. In order to prove separability of B over R we have to show that any R-module homomorphism $\phi \colon B \to R$ is given by $\phi(b) = \mathrm{Tr}_{B/R}(b\beta)$ for some unique element $\beta \in B$ and all $b \in B$. Here Tr denotes the trace map. Tensoring ϕ with id_{R_i} one obtains unique $\beta_i \in B_i$ such that the R_i-module homomorphisms $\phi \otimes \mathrm{id}_{R_i} \colon B_i \to R_i$, $i = 1, 2$, are given by $\phi_i(b_i) = \mathrm{Tr}_{B_i/R_i}(b_i \beta_i)$ for some uniquely determined element $\beta_i \in B_i$. Using the commutativity of the diagrams

$$
\begin{array}{ccc}
\mathrm{End}_R(B) & \xrightarrow{\ \otimes_R \mathrm{id}_{R_i}\ } & \mathrm{End}_{R_i}(B_i) \\[2mm]
\downarrow{\scriptstyle \mathrm{Tr}_{B/R}} & & \downarrow{\scriptstyle \mathrm{Tr}_{B_i/R_i}} \\[2mm]
R & \longrightarrow & R_i
\end{array}
$$

one easily checks that $\beta = (\beta_1, \beta_2)$ is the wanted element. This proves 4.2.

Proof of 4.1. Given 4.2, the proof of 4.1 is nothing more than a purely categorical manipulation. The idea is to translate the statement in 4.2 that the category of projective separable algebras over the fibred product R can be viewed as the fibred product of the categories of projective separable algebras over the respective rings into a corresponding statement for the fundamental groupoids. We restrict ourselves to a rough outline of the procedure to be followed, disregarding all set-theoretic precautions required in working with 'large' categories.

What we need is a category **MGal** of *multi-Galois categories* in the sense of [5, V.9], i.e. categories that are equivalent to a product of finitely many Galois categories as defined in [5]. Our standard example of a multi-Galois category will of course be the category of finite étale coverings of the spectrum of a ring having finitely many connected components. As this example already shows, the 'components' of a multi-Galois category are essentially unique: they correspond to the minimal subobjects of the terminal object different from the initial object. A *fundamental functor* on a multi-Galois category is the composition of a projection onto a component (which is a Galois category) with a fundamental functor of this component. A set of fundamental functors on a multi-Galois category is said to be *sufficiently large* if for each component of the category there is a fundamental functor factoring via this component.

The objects of **MGal** are pairs (C, F) with C a multi-Galois category and F a sufficiently large set of fundamental functors. A morphism $(C_1, F_1) \to (C_2, F_2)$ is an *equivalence class* of functors $(C_1, F_1) \to (C_2, F_2)$; a functor $(C_1, F_1) \to (C_2, F_2)$ is a functor $\Phi \colon C_1 \to C_2$ such that $\Phi f \in F_1$ for every $f \in F_2$ and two functors Φ and Φ' of this type are equivalent if $\Phi f = \Phi' f$ for all $f \in F_2$ and there is a natural equivalence of functors $\Phi \to \Phi'$.

To any (C, F) one may associate a profinite groupoid π_C that has vertex set F and isomorphisms $f \xrightarrow{\sim} f'$ of fundamental functors $f, f' \in F$ as its edges. Note that there are no isomorphisms between functors factoring via different components of C. We obtain a contravariant functor $\mathfrak{F} \colon \mathbf{MGal} \to \mathbf{Pgrpd}$ to

the category of profinite groupoids. In the other direction there is a functor $\mathfrak{G}$: **Pgrpd** → **MGal** sending $\pi \in$ **Pgrpd** to π-sets with the forgetful functor to **sets** at each vertex understood. From the definition of morphisms in **MGal** it follows that (C, F) is *isomorphic* to π_C-**sets**. On the other hand, $\mathfrak{F}(\pi_C$-**sets**) is canonically isomorphic to π_C. We conclude that the functors $\mathfrak{F}$ and $\mathfrak{G}$ induce an anti-equivalence **MGal** $\cong_{\text{anti}}$ **Pgrpd**.

Now we can rephrase 4.2 as follows in terms of the categories of finite étale coverings of the respective spectra. There is a natural pull-back square in **MGal**

$$
\begin{array}{ccc}
(\mathbf{FEt}_R, S) & \longrightarrow & (\mathbf{FEt}_{R_1}, S_1) \\
\downarrow & & \downarrow \\
(\mathbf{FEt}_{R_2}, S_2) & \longrightarrow & (\mathbf{FEt}_{R_0}, S_0).
\end{array}
$$

Here we use the fact that R has finitely many connected components and that its set S of geometric points is sufficiently large (by condition (iii)). Now the existence of the push-out square from 4.1 is a direct consequence of the anti-equivalence mentioned above.

The statement for abelianized groupoids follows from the previous case since, being a left adjoint functor, abelianizing preserves push-outs. This finishes the proof of 4.1.

The following example gives an explicit computation of the abelianized push-out groupoid we need in §6.

A groupoid is said to be *connected* if it has an edge between any two of its vertices, and *totally disconnected* if it has no edges between different vertices.

4.3   Proposition. *Suppose we are given profinite abelian groupoids π_0, π_1 and π_2 and morphisms $f_i: \pi_0 \to \pi_i$, $i = 1, 2$, for which the following conditions are satisfied:*

(i) *π_0 is totally disconnected with finite vertex set U and vertex groups $\widehat{\mathbf{Z}}$.*

(ii) *π_1 has t connected components with vertex groups G_j, $j = 1, 2, \ldots, t$, and vertex set U.*

(iii) *π_2 is totally disconnected with finite vertex set S and vertex groups H_s, $s \in S$.*

(iv) *f_1 is the identity on U and $f_2: U \to S$ is surjective.*

(v) *The graph obtained from π_1 by identification of vertices having the same image in S under f_2 is connected.*

Then the push-out π of π_1 and π_2 over π_0 in the category of abelian profinite groupoids is connected with vertex groups

$$
\left(\left(\prod_{s \in S} H_s \times \prod_{j=1}^{t} G_j \right) \Big/ \overline{\langle\langle (h_u, g_u^{-1}) \rangle\rangle}_{u \in U} \right) \times \widehat{\mathbf{Z}}^k.
$$

Here g_u and h_u are the images of $1 \in \widehat{\mathbf{Z}}$, the vertex group of π_0 at $u \in U$, under f_1 and f_2, naturally embedded in $\prod_{j=1}^{t} G_j$ and $\prod_{s \in S} H_s$, respectively. The bar denotes the closure of the subgroup.

Let c_s denote the number of vertices of π_0 mapped to $s \in S$ under f_2. Then the integer k equals $1 - t + \sum_{s \in S}(c_s - 1)$.

Proof. By assumption (v) we can choose a set V of $\#S - 1$ edges in π_1 that give a spanning tree in the graph in (v). Then V is a union of trees in π_1, so we may extend V to a set of edges W in π_1 forming spanning trees in each component of π_1. Taking the edges in W as 'neutral elements' we can label the edges of π_1 by triples (g, u_1, u_2), with $g \in G_j$ for some j and $u_1, u_2 \in U$ in the connected component associated to G_j, such that

(1) (g, u_1, u_2) is an edge from u_1 to u_2,

(2) composition in π_1 is given by $(g, u_2, u_3)(g', u_1, u_2) = (gg', u_1, u_3)$,

(3) $(g, u_1, u_2) \in W \Rightarrow g = 1 \in G_j$.

We take π to be the connected groupoid with vertex set S and vertex groups $C \times D$ with $D = \hat{\mathbf{Z}}^{W-V}$ and $C = (\prod_{s \in S} H_s \times \prod_{j=1}^{t} G_j)/\langle\langle(h_u, g_u^{-1})\rangle\rangle_{u \in U}$. The edges of π are labeled analogously as elements of $C \times D \times S \times S$. Note that C is written multiplicatively and D additively. We let $\tilde{g}$ and $\tilde{h}$ denote the images in C of $g \in G_j$ and $h \in H_s$, respectively.

The map $p_2: \pi_2 \to \pi$ is defined as the identity on S and sends $h \in H_s$ to $(\tilde{h}, 0, s, s)$.

Now choose a $\hat{\mathbf{Z}}$-basis $(1_w)_{w \in W-V}$ for D. Since $\#W = \#U - t$ we have $\#(W - V) = 1 - t + \#U - \#S = 1 - t + \sum_{s \in S}(c_s - 1)$, so $D = \hat{\mathbf{Z}}^k$ with k as stated in the proposition.

The map $p_1: \pi_1 \to \pi$ is defined as follows:

(1) $p_1(u) = f_2(u)$ for $u \in U$.

(2) $p_1(v) = (1, 0, p_1(u_1), p_1(u_2))$ if $v: u_1 \to u_2$ is in V.

(3) $p_1(w) = (1, 1_w, p_1(u_1), p_1(u_2))$ if $w: u_1 \to u_2$ is in $W - V$.

(4) $p_1((g, u, u)) = (\tilde{g}, 0, p_1(u), p_1(u))$.

One checks that p_1 is well defined and determined on all edges of π_1. Further it is easily verified that $p_1 f_1 = p_2 f_2$: on vertices this is immediate from defining property (1) of p_1 and for edges in π_0 it follows precisely from the definition of C.

To finish the proof one has to show that π has the required universal property. This is a tedious but straightforward verification that is left to the reader. This finishes the proof of 4.3.

We conclude this section with the analogue of 3.5 for fundamental groups.

4.4 Theorem. *For any connected Noetherian ring A with geometric point x, the natural map $\pi(A_0, x_0) \to \pi(A, x)$ is an isomorphism. Here x_0 is the geometric point of $A_0 = A/\mathrm{nil}(A)$ lying over x.*

Proof. [13, 7.2.1].

Remark. The Noetherian hypothesis in 4.4, though common in the literature, is actually superfluous (see [14, Theorem 7.3]).

5. PROOF OF THEOREM 2.1

Let A be the ring of integers of a number field K. What we need for Theorem 2.1 is a description of the abelianized fundamental group $\pi(A)_{ab}$ of A. It is known [10, 6.14 or 11, I.5.2(b)] that every projective separable A-algebra B can be written as a finite product $B = \prod_{i=1}^{n} B_i$, where each B_i is the ring of integers of some finite unramified extension L_i of K. Here *unramified* means 'unramified at all finite primes'. Conversely, every algebra of this form is projective separable over A. It follows that $\pi(A)$ is isomorphic to the Galois group $\mathrm{Gal}(K^{unr}/K)$, where K^{unr} is the maximal unramified extension of K inside some algebraic closure $\overline{K}$ of K. Upon abelianizing, we obtain a canonical isomorphism $\mathrm{Gal}(H^+/K) \xrightarrow{\sim} \pi(A)_{ab}$, where the *extended Hilbert class field* H^+ of K is the maximal unramified abelian extension of K. By class field theory, H^+/K is a finite extension, so the groups are finite. To prove 2.1, we still have to deal with the Artin symbol and with the ramification of real primes.

First we give the Galois theoretic interpretation of Frobenius elements in $\pi(A)_{ab}$. This comes down to studying the natural maps $\pi(A/\mathfrak{p}) \to \pi(A)_{ab}$ for the prime ideals $\mathfrak{p} \neq 0$ of A. Thus, let F be the residue class field at some finite prime $\mathfrak{p}$ of A and $y: F \to F^{sep}$ the embedding of F in a separable closure. We denote by $x: A \to A^{unr}$ the embedding of A in its integral closure in K^{unr}. Then we have canonical isomorphisms $\pi(F) \cong \mathrm{Gal}(F^{sep}/F)$ and $\pi(A, x) \cong \mathrm{Gal}(K^{unr}/K)$. In order to obtain a homomorphism between these two fundamental groups, we choose an extension $\phi: A^{unr} \to F^{sep}$ of the natural map $\chi: A \to F$. Note that this involves the choice of a prime $\mathfrak{P} = \ker \phi$ in A^{unr} extending $\mathfrak{p}$. Then $\phi \circ x$ is a geometric point of A and $y \circ \chi = \phi \circ x$, so there is a canonical map $\pi(F, y) \to \pi(A, \phi \circ x)$. As we still want to identify $\pi(A, \phi \circ x)$ with $\mathrm{Gal}(K^{unr}/K)$, we view the finite set of A-algebra homomorphisms $\mathrm{Alg}_A(B, F^{sep})$ corresponding to a projective separable algebra B over A as a $\mathrm{Gal}(K^{unr}/K)$-set in the following way. Let $\sigma \in \mathrm{Alg}_A(B, F^{sep})$. Then it factors uniquely via A^{unr} as $\sigma = \phi \circ i$ with $i \in \mathrm{Alg}_A(B, A^{unr})$. We let $\alpha(\sigma) = \phi \circ \alpha \circ i$ for $\alpha \in \mathrm{Gal}(K^{unr}/K)$. To see what the map $\pi(F, y) \to \pi(A, \phi \circ x)$ becomes in terms of Galois groups, we observe that $\pi(F, y) = \mathrm{Gal}(F^{sep}/F)$ acts on $\mathrm{Alg}_A(B, F^{sep}) = \mathrm{Alg}(B \otimes_A F, F^{sep})$ by 'composition'. We see that an element $\beta \in \mathrm{Gal}(F^{sep}/F)$ must be sent to the unique element $\alpha \in \mathrm{Gal}(K^{unr}/K)$ for which $\beta \circ \phi \circ i = \phi \circ \alpha \circ i$ for *all* pairs (B, i). This is obviously the element α satisfying $\phi \circ \alpha = \beta \circ \phi$. Thus the map on the Galois groups sends $\pi(F, y)$ to the *decomposition group* of $\mathfrak{P}/\mathfrak{p}$ in $\pi(A, x) = \mathrm{Gal}(K^{unr}/K)$, mapping the Frobenius in $\pi(F, y)$ to the *Frobenius* of $\mathfrak{P}/\mathfrak{p}$ (cf. [9] or [15]). After abelianizing this means that, in accordance with all reasonable expectations, the Frobenius element in $\pi(A)_{ab}$ at $\mathfrak{p}$ corresponds to the Artin symbol of $\mathfrak{p}$ in $\mathrm{Gal}(H^+/K)$.

Having finished the description of the Frobenius elements in $\pi(A)_{\mathrm{ab}}$, we turn to a related problem: the ramification of real primes of K in H^+. When we replace F by $\mathbf{R}$ in the preceding paragraph, the argument shows that for every homomorphism $\tau: A \to \mathbf{R}$, the image of $\pi(\mathbf{R})$ under the induced map $\tau^*: \tau(\mathbf{R}) \to \pi(A)_{\mathrm{ab}}$ is the decomposition group of the *real prime* τ (cf. [9, p. 153]). Letting τ range over the real primes of A, we see that $\pi(A)_{\mathrm{ab}}/\langle\tau^*\pi(\mathbf{R})\rangle_{\tau:\, A\to\mathbf{R}}$ is the Galois group over K of the largest subextension of H^+ that is unramified at all real primes. By definition, this is the Hilbert class field H of K. Thus we obtain an isomorphism

$$\mathrm{Gal}(H/K) \xrightarrow{\sim} \pi(A)_{\mathrm{ab}}/\langle\tau^*\pi(\mathbf{R})\rangle_{\tau:\, A\to\mathbf{R}}$$

by passing to factor groups in the isomorphism for H^+. The correspondence

$$(\mathfrak{p}, H/K) \mapsto \phi_{\mathfrak{p}} \mod \langle\tau^*\pi(\mathbf{R})\rangle_{\tau:\, A\to\mathbf{R}}$$

of Artin symbols and Frobenius elements is preserved since the restriction of an Artin symbol to a smaller field is again an Artin symbol.

Taking together the classical isomorphism $\mathrm{Cl}(A) \xrightarrow{\sim} \mathrm{Gal}(H/K)$ and the isomorphism $\mathrm{Cl}(A) \xrightarrow{\sim} G(A)_{\mathrm{tor}}$ from 3.2 with the isomorphism just proved, we see that we have completed the proof of 2.1.

6. PROOF OF THE MAIN RESULT

We give a proof of Theorem 2.2 under the assumption that $\mathrm{nil}(A) = 0$. It will turn out that the general case follows relatively easily from this case.

The structure of the proof for rings A with trivial nilradical is as follows. First we write A as a fibred product of 'easier' rings and compute its fundamental group using the algebraic van Kampen theorem. An exact sequence can be given for its torsion part and it turns out that an analogous sequence can be derived from the theorem of §3 for $G(A)_{\mathrm{tor}}$. When combined with Theorem 2.1, the sequences furnish a proof of 2.2, only the formula for k remains to be shown. Once this formula is proved, all results can be extended to the case in which $\mathrm{nil}(A)$ need not be trivial.

First we prove that A has no additive torsion. If we have $nx = 0$ for some $n \in \mathbf{Z}_{>0}$ and $x \notin \mathrm{nil}(A) = 0$, it follows that there is a minimal prime ideal $\mathfrak{p}$ of A containing nA. Since A/nA is finite, the ideal $\mathfrak{p}$ is maximal as well. By connectedness, we must have $A = A/nA$, so A is finite. Contradiction.

As A is torsionfree, the map $A \to A_{\mathbf{Q}} = A \otimes_{\mathbf{Z}} \mathbf{Q}$ is injective and $A_{\mathbf{Q}}$ is a finite dimensional $\mathbf{Q}$-algebra. From $\mathrm{nil}(A_{\mathbf{Q}}) = \mathrm{nil}(A) = 0$ it follows that $A_{\mathbf{Q}} \cong \prod_{i=1}^{t} K_i$ for certain finite field extensions K_i of $\mathbf{Q}$, so the natural map from $A_{\mathbf{Q}}$ to the total ring of fractions $K = S^{-1}A$ of A is an isomorphism. The image of A in K_i under the composite map $A \to K \to K_i$ is a finite $\mathbf{Z}$-algebra, so it is contained in the ring of integers B_i of K_i. Viewing A as a subring of K, we have $A \subset B = \prod_{i=1}^{t} B_i$. Thus B becomes a finite A-algebra and $(B/A) \otimes_{\mathbf{Z}} \mathbf{Q} = 0$, so $nB \subset A$ for some integer $n \in \mathbf{Z}_{>0}$. The *conductor*

of B in A is the B-ideal $I = \{\beta \in B: \beta B \subset A\}$. Since I contains nB, it is of finite index in B. Further I is immediately seen to be contained in A, so A/I is finite as well. From the diagram

$$
\begin{array}{ccc}
A & \longrightarrow & B \\
\downarrow & & \downarrow \\
A/I & \longrightarrow & B/I
\end{array}
$$

we see that A is the fibred product of B and A/I over B/I. This situation enables us to use the van Kampen theorem in the computation of the fundamental group of A. The following lemma shows that finite rings are easy to deal with.

6.1 Lemma. *Let R be a finite ring. Then the prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_r$ of R are all maximal and $R \cong \prod_{i=1}^r R/\mathfrak{p}_i^k$ for some $k \in \mathbf{Z}_{>0}$. Further $\pi(R/\mathfrak{p}_i^k) = \pi(R/\mathfrak{p}_i) \cong \widehat{\mathbf{Z}}$, $i = 1, 2, \ldots, r$.*

Proof. The isomorphism for R is standard (cf. [1, Chapter 8]). The isomorphism $\pi(R/\mathfrak{p}_i^k) = \pi(R/\mathfrak{p}_i)$ is a special case of 4.4 and $\pi(R/\mathfrak{p}_i) \cong \widehat{\mathbf{Z}}$ since $R/\mathfrak{p}_i$ is a finite field.

Choose a set S of geometric points of A/I, one geometric point for each prime of A/I and a set of geometric points U of B/I, also one point for each prime of B/I, such that U is mapped to S via $A/I \to B/I$. Then the fundamental groupoids $\pi(A/I, S)$ and $\pi(B/I, U)$ are totally disconnected with vertex groups $\widehat{\mathbf{Z}}$. View U as a set of geometric points of B via $B \to B/I$. If U is not sufficiently large in $\operatorname{spec} B$, say $U \cap \operatorname{spec} B_i = \varnothing$, then we have $A = B_i \times A'$ and consequently $A = B_i = B$ by the connectedness of A.

6.2 Lemma. *Let $c_{\mathfrak{a}}$ denote the number of prime ideals in B lying over $\mathfrak{a} \in \operatorname{spec} A$. Then there is a decomposition of the abelianized fundamental group of A as $\pi(A)_{\mathrm{ab}} \cong C \times \widehat{\mathbf{Z}}^k$, where*

$$
C = \left(\widehat{\mathbf{Z}}^{\operatorname{spec} A/I} \times \prod_{i=1}^t \pi(B_i)_{\mathrm{ab}} \right) / R,
$$

$$
R = \sum_{\mathfrak{m} \in \operatorname{spec} B/I} \widehat{\mathbf{Z}} \cdot (f_{\mathfrak{m}/\mathfrak{n}} e_{\mathfrak{n}}, \phi_{\mathfrak{m}}^{-1}),
$$

$$
k = 1 - t + \sum_{\mathfrak{a} \in \operatorname{spec} A} (c_{\mathfrak{a}} - 1).
$$

Here $\mathfrak{n} = \mathfrak{m} \cap (A/I)$ and $\phi_{\mathfrak{m}}$ denotes the Frobenius in $\pi(B_i)_{\mathrm{ab}}$ at $\mathfrak{m} \in \operatorname{spec} B_i \subset \operatorname{spec} B$. Further $f_{\mathfrak{m}/\mathfrak{n}} = [B/\mathfrak{m}: A/\mathfrak{n}]$ and $e_{\mathfrak{n}}: \operatorname{spec} A/I \to \widehat{\mathbf{Z}}$ is the characteristic function of $\{\mathfrak{n}\}$.

Proof. We may assume $A \neq B$. Then the lemma is a direct application of the van Kampen Theorem 4.1 with $\pi_0 = \pi(B/I, U)$, $\pi_1 = \pi(B, U)$ and $\pi_2 = \pi(A/I, S)$ and vertex groups $G_i = \pi(B_i)_{\mathrm{ab}}$ and $H_s = \widehat{\mathbf{Z}}$. Identify $\operatorname{spec} B/I$

and U as point sets. We have $g_m = \phi_m$ by definition of the Frobenius. The inclusion of finite fields $\mathbf{F}_q \subset \mathbf{F}_{q^n}$ induces an injection $\pi(\mathbf{F}_{q^n}) \to \pi(\mathbf{F}_q)$ on the fundamental groups sending the Frobenius in $\pi(\mathbf{F}_{q^n})$ to the nth power of the Frobenius in $\pi(\mathbf{F}_q)$. It follows that $h_m = f_{m/n} e_n$. The conditions (i)–(iv) in 4.3 are obviously satisfied and (v) follows from the connectedness of A. To prove the expression for k, we must show that $c_n = 1$ for $n \in \operatorname{spec} A - \operatorname{spec} A/I$. These n do not contain I, so the localizations $A_{(n)}$ and $B_{(n)}$ are equal. This implies that $B_{(n)}$ is a local ring with maximal ideal generated by n. In particular $c_{\{n\}} = \# \operatorname{spec}(B_{(n)}/nB_{(n)}) = 1$, which finishes the proof of the lemma.

Having finished the computation of $\pi(A)_{ab}$ we proceed with the description of the group $\pi(A)_{ab,tor}/\langle \tau^* \pi(\mathbf{R}) \rangle_{\tau: \ A \to \mathbf{R}}$ occurring in 2.2.

Since groupoids will no longer be used we write $\pi(B)_{ab}$ to denote the product $\prod_{i=1}^{t} \pi(B_i)_{ab}$ of the abelianized fundamental groups. Since each B_i is the ring of integers of a number field K_i and each $\tau: B \to \mathbf{R}$ factors via some B_i, Theorem 2.1 furnishes an identification $\pi(B)_{ab}/\langle \tau^* \pi(\mathbf{R}) \rangle_{\tau: \ B \to \mathbf{R}} = \prod_{i=1}^{t} \operatorname{Gal}(H_i/K_i)$ with H_i the Hilbert class field of K_i. Note further that for any $\tau: A \to \mathbf{R}$ there is a unique element $\tau': B \to \mathbf{R}$ such that $\tau' \circ \iota = \tau$ and that $\iota^* \circ \tau'^* = \tau^*$. The subgroups $\tau^* \pi(\mathbf{R})$ for $\tau: A \to \mathbf{R}$ lie in the torsion subgroup C of $\pi(A)_{ab} = C \times \widehat{\mathbf{Z}}^k$. The group C is finite since each $\pi(B_i)_{ab}$ is finite and each e_n has finite order because of a relation from R. It will now be clear that we do not change C if we replace every $\widehat{\mathbf{Z}}$ in its definition by $\mathbf{Z}$, thus eliminating all topology.

The preceding discussion may be summarized as follows.

6.4 Lemma. *There is a decomposition* $\pi(A)_{ab}/\langle \tau^* \pi(\mathbf{R}) \rangle_{\tau: \ A \to \mathbf{R}} \cong \mathfrak{R} \times \widehat{\mathbf{Z}}^k$, *where* $\mathfrak{R} = \pi(A)_{ab,tor}/\langle \tau^* \pi(\mathbf{R}) \rangle_{\tau: \ A \to \mathbf{R}}$ *is the finite abelian group fitting in the exact sequence*

$$0 \to \sum_{m \in \operatorname{spec} B/I} \mathbf{Z} \cdot (f_{m/n} e_n, \overline{\phi}_m^{-1}) \to \mathbf{Z}^{\operatorname{spec} A/I} \oplus (\pi(B)_{ab}/\langle \tau^* \pi(\mathbf{R}) \rangle_{\tau: \ B \to \mathbf{R}}) \xrightarrow{\gamma} \mathfrak{R} \to 0.$$

Here γ *maps* $(e_n, 0)$ *to the residue class of the Frobenius in* $\pi(A)_{ab}$ *at* n. *The element* $(0, \overline{\phi}_m)$ *for* $m \in \operatorname{spec} B$ *is mapped to* $f_{m/n}$ *times the residue class of the Frobenius in* $\pi(A)_{ab}$ *at* $n = m \cap A$.

We have proved the validity of the exact sequence in 2.2 for our A if we can exhibit an isomorphism $G(A)_{tor} \to \mathfrak{R}$ satisfying the description of f given there.

We proceed with the description of $G(A)_{tor}$. From 3.4 there is a commutative diagram with exact rows

$$
\begin{array}{ccccccccc}
\prod_{i=1}^{t} K_i^* & \to & G^{tor}(B) = & \bigoplus_{m \in \mathfrak{M}(B)} \mathbf{Z} \cdot e_m & \to & G(B) & \to & \mathbf{Z}^t & \to & 0 \\
\| & & & \downarrow & & \downarrow & & \| & & \\
\prod_{i=1}^{t} K_i^* & \to & G^{tor}(A) = & \bigoplus_{n \in \mathfrak{M}(A)} \mathbf{Z} \cdot e_n & \to & G(A) & \to & \mathbf{Z}^t & \to & 0.
\end{array}
$$

The map $G(B) \to G(A)$ is the natural map induced by $\iota: A \to B$. The natural map $G^{\mathrm{tor}}(B) \to G^{\mathrm{tor}}(A)$ sends $e_{\mathfrak{m}}$ to $f_{\mathfrak{m}/\mathfrak{n}}e_{\mathfrak{n}}$ since $B/\mathfrak{m}$ has length $f_{\mathfrak{m}/\mathfrak{n}}$ over $A/\mathfrak{n}$. For the commutativity of the left square we observe that $[B/\alpha B] = [B/A] + [A/\alpha A] - [\alpha B/\alpha A] = [A/\alpha A]$ in $G^{\mathrm{tor}}(A)$ since $B/A \cong_A \alpha B/\alpha A$ for any $\alpha \in S$.

As a result of 3.2 and 3.4, we know that, under the natural map, $G^{\mathrm{tor}}(B)$ is mapped onto $G(B)_{\mathrm{tor}}$, the finite torsion subgroup $\prod_{i=1}^{t} \mathrm{Cl}(B_i)$ of $G(B)$. It follows that $\mathrm{im}(G^{\mathrm{tor}}(A)) \subset G(A)_{\mathrm{tor}}$ and since the other inclusion is obvious from the exactness at $G(A)$ we have $\mathrm{im}(G^{\mathrm{tor}}(A)) = G(A)_{\mathrm{tor}}$.

Now consider the following modification of the preceding diagram.

$$
\begin{array}{ccccccc}
\prod_{i=1}^{t} K_i^* & \to & \mathbf{Z}^{\mathrm{spec}\, A/I} \oplus G^{\mathrm{tor}}(B) & \to & \mathbf{Z}^{\mathrm{spec}\, A/I} \oplus G(B)_{\mathrm{tor}} & \to & 0 \\
\downarrow & & \downarrow{\scriptstyle \alpha} & & \downarrow{\scriptstyle \beta} & & \\
0 \to \ker\delta & \to & G^{\mathrm{tor}}(A) & \xrightarrow{\delta} & G(A)_{\mathrm{tor}} & \to & 0.
\end{array}
$$

Here α is the sum of the map $\mathbf{Z}^{\mathrm{spec}\, A/I} \to G^{\mathrm{tor}}(A)$ sending $e_{\mathfrak{n}}$ to $[A/\mathfrak{n}]$ and the natural map $G^{\mathrm{tor}}(B) \to G^{\mathrm{tor}}(A)$. Note that α and β are surjective since $f_{\mathfrak{m}/\mathfrak{n}} = 1$ for $\mathfrak{n} \in \mathrm{spec}\, A - \mathrm{spec}\, A/I$. The diagram still commutes since $\prod_{i=1}^{t} K_i^*$ is mapped only to the second component $G^{\mathrm{tor}}(B)$. It is clear that $\ker\alpha = \sum_{\mathfrak{m} \in \mathrm{spec}\, B/I} \mathbf{Z} \cdot (f_{\mathfrak{m}/\mathfrak{n}}e_{\mathfrak{n}}, -[B/\mathfrak{m}])$, and by the snake lemma the induced map $\ker\alpha \to \ker\beta$ is surjective. We obtain the following result for $G(A)_{\mathrm{tor}}$.

6.5 Lemma. *The group $G(A)_{\mathrm{tor}}$ fits in an exact sequence*

$$
0 \to \sum_{\mathfrak{m} \in \mathrm{spec}\, B/I} \mathbf{Z} \cdot (f_{\mathfrak{m}/\mathfrak{n}}e_{\mathfrak{n}}, -[B/\mathfrak{m}]) \to \mathbf{Z}^{\mathrm{spec}\, A/I} \oplus G(B)_{\mathrm{tor}} \xrightarrow{\beta} G(A)_{\mathrm{tor}} \to 0.
$$

Here β maps $(e_{\mathfrak{n}}, 0)$ to the class $[A/\mathfrak{n}] \in G(A)_{\mathrm{tor}}$ and induces the natural map on $G(B)_{\mathrm{tor}}$.

The resemblance of the sequences in 6.4 and 6.5 is clear. The first (nonzero) terms are obviously isomorphic under the isomorphism of the middle terms furnished by Theorem 2.1. The induced isomorphism $G(A)_{\mathrm{tor}} \to \mathfrak{R}$ is now easily seen to satisfy the description given for f in 2.2.

To finish the proof of 2.2 for rings A with trivial nilradical, we still have to show that

$$
\dim_{\mathbf{F}_2}[\mathrm{Id}(\widehat{A} \otimes_{\mathbf{Z}} \mathbf{Q})/(\mathrm{Id}(\widehat{A}) \And \mathrm{Id}(A \otimes_{\mathbf{Z}} \mathbf{Q}))] = 1 - t + \sum_{\mathfrak{n} \in \mathrm{spec}\, A} (c_{\mathfrak{n}} - 1).
$$

First we observe that any power $\mathfrak{n}^k$ of a maximal ideal $\mathfrak{n}$ of A contains nA for some $n \in \mathbf{Z}_{>0}$, so the ring $\widehat{A}$ is isomorphic to the product $\prod_{\mathfrak{n} \in \mathfrak{M}(A)} A_{\mathfrak{n}}$ of the completions at the maximal ideals $\mathfrak{n}$ of A. Since A is $\mathbf{Z}$-free, we also have $\widehat{A} \cong A \otimes_{\mathbf{Z}} \widehat{\mathbf{Z}}$. It follows that $\widehat{A} \otimes_{\mathbf{Z}} \mathbf{Q} = A \otimes_{\mathbf{Z}} \mathbf{Q} \otimes_{\mathbf{Z}} \widehat{\mathbf{Z}} = B \otimes_{\mathbf{Z}} \mathbf{Q} \otimes_{\mathbf{Z}} \widehat{\mathbf{Z}} = \widehat{B} \otimes_{\mathbf{Z}} \mathbf{Q} = \prod'_{\mathfrak{m} \in \mathfrak{M}(B)} K_{\mathfrak{m}}$. The last product is a restricted direct product with

respect to the rings $B_m \subset K_m = Q(B_m)$, so we may view this ring as the *ring of finite adèles* of B. As a consequence we note that the rings $\widehat{A}$ and $\widehat{A} \otimes_Z Q$ do not contain nonzero nilpotents. For the idempotent rank we obtain an equality $\dim_{F_2}(\text{Id}(\widehat{A} \otimes_Z Q)/\text{Id}(\widehat{A})) = \sum_n(c_n - 1)$. We have already seen that $A \otimes_Z Q = \prod_{i=1}^{t} K_i$, so $\dim_{F_2}\text{Id}(A \otimes_Z Q) = t$. The desired equality now follows from the observation that $\text{Id}(\widehat{A}) \cap \text{Id}(A \otimes_Z Q) = \text{Id}(A) = \{0, 1\}$.

In the general case, we still have our exact sequence since it follows from 3.5 and 4.4 that the natural map $A \to A_0 = A/\text{nil}(A)$ induces canonical isomorphisms $G(A_0) \xrightarrow{\sim} G(A)$ and, since all $\tau: A \to R$ factor via A_0,

$$\pi(A_0)_{\text{ab}}/\langle \tau^* \pi(R) \rangle_{\tau: A_0 \to R} \xrightarrow{\sim} \pi(A)_{\text{ab}}/\langle \tau^* \pi(R) \rangle_{\tau: A \to R}.$$

Here we use that A_0 is infinite and finitely generated as a module over Z if A is. It remains to be shown that the idempotent rank is the same for A and A_0. Since there is an isomorphism of F_2-vector spaces $\text{Id}(R) \to \text{Id}(R_0)$ for any ring R, it suffices to show that there are canonical isomorphisms $(A_0)^{\widehat{}} \cong (\widehat{A})_0$, $(A_0)^{\widehat{}} \otimes_Z Q \cong (\widehat{A} \otimes_Z Q)_0$ and $A_0 \otimes_Z Q \cong (A \otimes_Z Q)_0$.

Let $N = \text{nil}(A)$. Then the exact sequence $0 \to N \to A \to A_0 \to 0$ splits as an exact sequence of abelian groups, so we obtain an exact sequence $0 \to \widehat{N} \to \widehat{A} \to (A_0)^{\widehat{}} \to 0$ by taking profinite completions. The ideal N is nilpotent in the Noetherian ring A, so let $N^k = 0$. It follows that $\widehat{N}^k = 0$ as N is dense in $\widehat{N}$, so $\widehat{N} \subset \text{nil}(\widehat{A})$. Since, as we just observed, the ring $(A_0)^{\widehat{}} = \widehat{A}/\widehat{N}$ has no nilpotent elements, equality must hold. This proves $(A_0)^{\widehat{}} \cong (\widehat{A})_0$.

From the isomorphism just proved we obtain a surjective map $(A_0)^{\widehat{}} \otimes_Z Q = (\widehat{A})_0 \otimes_Z Q \to (\widehat{A} \otimes_Z Q)_0$ and, again by the absence of nontrivial nilpotents in the first ring, this must be an isomorphism. The same argument works for the surjective map $A_0 \otimes_Z Q \to (A \otimes_Z Q)_0$ since the first ring is a product of finite field extensions of Q.

This finishes the proof of 2.2.

REFERENCES

1. M. F. Atiyah and I. G. Macdonald, *Introduction to commutative algebra*, Addison-Wesley, Reading, Mass., 1969.

2. H. Bass, *Algebraic K-theory*, Benjamin, New York, 1968.

3. N. Bourbaki, *Commutative algebra*, Addison-Wesley, Reading, Mass., 1972.

4. C. W. Curtis and I. Reiner, *Methods of representation theory*, Vol. I, Wiley, New York, 1981.

5. A. Grothendieck, *Séminaire de géométrie algébrique* 1, *Revêtements étales et groupe fondamental*, Lecture Notes in Math., vol. 224, Springer, Berlin, 1971.

6. R. Hartshorne, *Algebraic geometry*, Springer, New York, 1977.

7. P. J. Higgins, *Notes on categories and groupoids*, Van Nostrand Reinhold, London, 1971.

8. D. Hilbert, *Über die Theorie der relativ-Abelschen Zahlkörper*, Acta Math. **26** (1902), 99–132. [Only this 'mit geringen Änderungen' reprinted version of a paper under the same title in the Nachr. d. Ges. der Wiss. zu Gött. (1898), 370–399, contains the paragraph on the Hilbert class field.]

9. S. Lang, *Algebraic number theory*, Addison-Wesley, Reading, Mass., 1970.

10. H. W. Lenstra, Jr., *Galois theory for schemes*, Mathematisch Instituut, Universiteit van Amsterdam, 1985.

11. J. S. Milne, *Etale cohomology*, Princeton Univ. Press, Princeton, N.J., 1980.

12. J. Milnor, *Introduction to algebraic K-theory*, Princeton Univ. Press, Princeton, N.J., 1971.

13. J. P. Murre, *Lectures on an introduction to Grothendieck's theory of the fundamental group*, Tata Institute of Fundamental Research, Bombay, 1967.

14. P. Stevenhagen, *Generalized unramified class field theory*, Mathematisch Instituut, Universiteit van Amsterdam, report 85-13, 1985.

15. E. Weiss, *Algebraic number theory*, McGraw-Hill, New York, 1963.

MATHEMATISCH INSTITUUT, UNIVERSITEIT VAN AMSTERDAM, ROETERSSTRAAT 15, 1018 WB AMSTERDAM, THE NETHERLANDS (Current address)

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF CALIFORNIA, BERKELEY, CALIFORNIA 94720