Infinite Galois theory, Stone spaces, and profinite groups

0. Prerequisites, and notation. In addition to elementary Galois theory, this note assumes familiarity with the concept of inverse limit, and the particular example of the ring of p-adic integers. Starting in §2, basic point-set topology is also assumed.

We shall regard elements of inverse limit sets $\varprojlim_{i\in I} X_i$ as families $(x_i)_{i\in I}$ $(x_i \in X_i)$ satisfying the conditions

$$f_{i,i'}(x_i) \;=\; x_{i'},$$

where the $f_{i,i'}$ are the maps of the given inverse system. We will call the above equations the ''compatibility conditions''.

1. Infinite Galois groups. The Galois group of an infinite-dimensional normal algebraic extension is easily described in terms of the Galois groups of its subextensions of finite degree.

Theorem 1. *Suppose E/K is a normal algebraic field extension, possibly of infinite degree. Let I be the set of intermediate fields normal of finite degree over K. If $F_2 \subseteq F_1$ are members of I, let f_{F_1,F_2}: $\mathrm{Aut}_K F_1 \to \mathrm{Aut}_K F_2$ denote restriction of automorphisms from F_1 to F_2. Then $\mathrm{Aut}_K E$ (regarded as mapped into each of these groups by restriction) may be identified with the inverse limit of the system of finite groups $\mathrm{Aut}_K F$ $(F\in I)$ and surjective homomorphisms f_{F_1,F_2}.*

More generally, the same conclusion holds with I replaced by any subset $J \subseteq I$ which has union E, and is directed under inclusion (equivalently, inversely directed under the ordering of I by reverse inclusion. Which ordering is preferable depends on the precise formalism one adopts for inverse limits).

Sketch of Proof. Let J be as in the second paragraph.

Given $\sigma \in \mathrm{Aut}_K E$, restriction of σ to the subfields $F\in J$ yields a system of elements of the groups $\mathrm{Aut}_K F$ satisfying the compatibility conditions for an element of the inverse limit group; thus we get a natural homomorphism $\mathrm{Aut}_K E \to \varprojlim_{F\in J} \mathrm{Aut}_K F$. Because $E = \bigcup_{F\in J} F$, this homomorphism is one-to-one.

To see that it is onto, let us be given an element $(\sigma_F)_{F\in J}$ $(\sigma_F \in \mathrm{Aut}_K F)$ of the inverse limit. For each $x\in E$, let $\sigma(x)$ denote the common value of $\sigma_F(x)$ as F ranges over all $F\in J$ which contain x. These values are indeed all equal, because given $F_1,\ F_2 \in J$ both containing x, there will exist $F_3\in J$ containing F_1 and F_2, and the compatibility conditions on $(\sigma_F)_{F\in J}$ give $\sigma_{F_1}(x) = \sigma_{F_3}(x) = \sigma_{F_2}(x)$. One verifies that σ is a homomorphism using the fact that for any $x,y\in E$ we can find an $F\in J$ with $x,y \in F$; the conditions $\sigma(x+y) = \sigma(x) + \sigma(y)$ etc. then follow from the same conditions on σ_F. Thus, σ is an element of $\mathrm{Aut}_K F$, and it clearly maps to the given element $(\sigma_F)_{F\in J}$ of the inverse limit. □

Example 1. Let $K = \mathbf{Q}$ and let E be the extension gotten by adjoining to $\mathbf{Q}$ the square roots of all positive integers, equivalently, of all primes. Let us write this as the union of the chain of extensions

$$\mathbf{Q} \;\subseteq\; \mathbf{Q}(\sqrt{2}) \;\subseteq\; \mathbf{Q}(\sqrt{2},\,\sqrt{3}) \;\subseteq\; \mathbf{Q}(\sqrt{2},\,\sqrt{3},\,\sqrt{5}) \;\subseteq\; \dots\,.$$

Now consider the extension of $\mathbf{Q}$ gotten by adjoining the square roots of finitely many primes $p_1, \dots, p_n$. An automorphism of this field can take each of those square roots to itself or its negative; thus we get an embedding of the Galois group of each such finite extension in $(\mathbf{Z}/2\mathbf{Z})^n$. This embedding is, in fact, an isomorphism. (Sketch of proof: any proper subgroup of $(\mathbf{Z}/2\mathbf{Z})^n$ is annihilated by some $(\mathbf{Z}/2\mathbf{Z})$-linear functional. If the image of our Galois group in $(\mathbf{Z}/2\mathbf{Z})^n$ were annihilated by a functional having coordinates $(\varepsilon_1, \ldots, \varepsilon_n)$ where each $\varepsilon_i = 0$ or 1, then the fixed field of the Galois group would contain $(p_1^{\varepsilon_1} \ldots p_n^{\varepsilon_n})^{1/2}$, but this is not a rational number. For a much more general result see [**4**, §VI.8].) Hence $\mathrm{Aut}_{\mathbf{Q}} E$ is the inverse limit of a system of group homomorphisms

$$\ldots \ \to\ (\mathbf{Z}/2\mathbf{Z})\times(\mathbf{Z}/2\mathbf{Z})\times(\mathbf{Z}/2\mathbf{Z}) \ \to\ (\mathbf{Z}/2\mathbf{Z})\times(\mathbf{Z}/2\mathbf{Z}) \ \to\ \mathbf{Z}/2\mathbf{Z} \ \to\ \{0\},$$

where each map chops off the last coordinate. This inverse limit is an infinite product of $(\mathbf{Z}/2\mathbf{Z})$'s.

Example 2. Again let $K = \mathbf{Q}$. Let p be any prime, and now let E be the union of the chain

$$\mathbf{Q} \ \subseteq\ \mathbf{Q}(\zeta_p) \ \subseteq\ \mathbf{Q}(\zeta_{p^2}) \ \subseteq\ \mathbf{Q}(\zeta_{p^3}) \ \subseteq\ \ldots,$$

where ζ_n denotes a primitive nth root of unity. Now $\mathrm{Aut}_{\mathbf{Q}}\, \mathbf{Q}(\zeta_{p^i})$ is isomorphic to the group of units of the ring $\mathbf{Z}/p^i\mathbf{Z}$ [**2**, Proposition V.8.3(iii)] [**4**, Theorem VI.3.1], and we see that the restriction maps among these automorphism groups are induced by the ring homomorphisms $\mathbf{Z}/p^i\mathbf{Z} \to \mathbf{Z}/p^{i-1}\mathbf{Z}$. We deduce that $\mathrm{Aut}_{\mathbf{Q}} E$ is isomorphic to the group of units of the inverse limit of this system of ring homomorphisms, i.e., the units of the ring of p-adic integers.

Example 2′. Take E as above, but take $K = \mathbf{Q}(\zeta_p)$. Then we find that $\mathrm{Aut}_K E$ corresponds to the multiplicative group of p-adic integers congruent to 1 mod p; a subgroup of the full group of units.

Example 3. Let p be a prime, and let k be a field containing primitive p^ith roots of unity for all i. Let K be a pure transcendental extension $k(x)$, and let E be the union of the chain

$$k(x) \ \subseteq\ k(x^{1/p}) \ \subseteq\ k(x^{1/p^2}) \ \subseteq\ k(x^{1/p^3}) \ \subseteq\ \ldots.$$

The Galois group of the ith term of this chain, $\mathrm{Aut}_{k(x)}\, k(x^{1/p^i})$, is isomorphic to the *additive* group $\mathbf{Z}/p^i\mathbf{Z}$ [**2**, Theorem V.7.11] [**4**, Theorem VI.6.2(ii)], and the restriction maps are again the obvious ones, so $\mathrm{Aut}_K E$ is isomorphic to the additive group of the p-adic integers.

We note briefly an example of a noncommutative infinite Galois group, leaving the details to the interested reader.

Example 4. Let p be a prime, let $K = \mathbf{Q}(x)$ with x an indeterminate, and let E be obtained by adjoining, for each i, both a primitive p^ith root of unity and a p^ith root of x. It is not hard to show that $\mathrm{Aut}_K E$ is generated by a copy of the multiplicative group of units of the p-adic integers (permuting the roots of unity) and a copy of the additive group of all p-adic integers (acting on the fractional powers of x), and has the structure of the *semidirect product* of these groups, determined by the natural action of the former group on the latter by multiplication in the ring of p-adic integers; equivalently, it is isomorphic to the group of matrices of the form $\begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix}$ where a is a unit and b an arbitrary element of that ring.

Our last example, again abelian, is

Example 5. Let p be a prime, let K be the field of p elements, and let E be the algebraic closure of K. Then the subfields of E of finite degree over K are the fields of p^n elements, as n ranges over the positive integers. Each of these is Galois over K, with Galois group generated by the map $a \mapsto a^p$, which on the field of cardinality p^n has order n, so the Galois groups are the groups $\mathbf{Z}/n\mathbf{Z}$ [**2**, Theorem V.5.3] [**4**, Theorem V.5.4]. The restriction homomorphisms are the natural maps $\mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/m\mathbf{Z}$ $(m \mid n)$. $\mathrm{Aut}_K E$ is thus the inverse limit of these groups and maps, i.e., the additive group of the inverse limit of the rings $\mathbf{Z}/n\mathbf{Z}$. That inverse limit can be shown to be the direct product, over all primes p, of the rings of p-adic integers. (Idea: each $\mathbf{Z}/n\mathbf{Z}$ is a direct product of rings $\mathbf{Z}/p^i\mathbf{Z}$.) Thus, our Galois group can be described as the direct product over all primes p of the additive group of p-adic integers.

2. Intermediate fields and closed subgroups. For E/K an infinite algebraic extension we can, as in the finite case, associate to each intermediate field L the subgroup $L^* \subseteq \mathrm{Aut}_K E$ of automorphisms that fix all elements of L, and to each subgroup $H \subseteq \mathrm{Aut}_K E$ its fixed field $H^* \subseteq E$. If E is Galois (i.e., separable and normal) over K, then every intermediate field L is still uniquely determined by the group L^*; that is, $L = L^{**}$ [**2**, Theorem V.3.12] [**4**, Theorem VI.1.2].

On the other hand, a *subgroup* $H \subseteq \mathrm{Aut}_K E$ is in general no longer determined by its fixed field H^*; i.e., H^{**}, which has the same fixed field, can be strictly larger than H. For instance, in the situation of Example 1, let H be the group consisting of all those automorphisms that change the signs of square roots of only *finitely* many primes. This is a proper subgroup, but its fixed field is the same as that of the whole group, since any element $u \in E$ involves square roots of only finitely many primes, hence if u is moved by a member of the whole automorphism group, i.e., is not in $\mathbf{Q}$, it will be moved by some member of H. Thus, here $H^{**} = K^* = \mathrm{Aut}_K E$.

In the situation of Example 3, to get a similar phenomenon, let α be the automorphism of E taking x^{1/p^n} to $\zeta_{p^n} x^{1/p^n}$ for all n (where we assume that our roots of unity and of x are labeled so that $(\zeta_{p^n})^p = \zeta_{p^{n-1}}$ and $(x^{1/p^n})^p = x^{1/p^{n-1}}$), and let $H = \langle\alpha\rangle \subseteq \mathrm{Aut}_K E$. We find that the restriction of α to each field $K(x^{1/p^n})$ is a generator of the whole Galois group of that field, hence α has no fixed elements in any of these subfields other than elements of K, which means it has no fixed elements in E other than elements of K. So $\langle\alpha\rangle^{**} = K^* = \mathrm{Aut}_K E$, though the inclusion of $\langle\alpha\rangle$ in $\mathrm{Aut}_K E$ is certainly proper: it is essentially the inclusion of $\mathbf{Z}$ in the p-adic integers. One can get infinite cyclic subgroups with similar properties in Example 2′ when $p \neq 2$, and in Example 5; in the first case using the automorphism carrying ζ_{p^n} to $(\zeta_{p^n})^{1+p}$ for all n, and in the second, the pth power map (the Frobenius automorphism). (In each of these cases one can, of course, also get cases of $H^{**} \neq H$ in which H^{**} is a proper subgroup of $\mathrm{Aut}_K E$. You might try to verify that for each prime p_0, there is a cyclic subgroup H of the group of Example 5 such that H^{**} is precisely the additive group of p_0-adic integers, regarded as a subgroup of the direct product group of that example.)

Clearly, what is happening in the above examples is that the subgroup H has the same image in each of the finite groups $\mathrm{Aut}_K F$ as does the whole group $\mathrm{Aut}_K E$. In other words, every element of $\mathrm{Aut}_K E$ can be *approximated*, in terms of its behavior on each *finite* subextension, by elements of H. This formulation in terms of approximation suggests that a topology is involved, and indeed it is:

Theorem 2. *Let E/K be a normal algebraic field extension, possibly of infinite degree, let J be any system of normal intermediate fields of finite degree over K which is directed under inclusion and has union E, and let H be any subgroup of $\mathrm{Aut}_K E$. Then the following subgroups of $\mathrm{Aut}_K E$ are equal.*

(i) *H^{**}, i.e. the group of all elements of $\mathrm{Aut}_K E$ fixing the fixed field H^* of H.*

(ii) *The group of all elements of $\mathrm{Aut}_K E$ whose images in each of the finite groups $\mathrm{Aut}_K F$ (under the restriction maps, which we shall write $\pi_F\colon \mathrm{Aut}_K E \to \mathrm{Aut}_K F$) are also images of elements of H; we may write this subgroup loosely as*

$$\varprojlim_{F\in J} \pi_F(H) \subseteq \varprojlim_{F\in J} \mathrm{Aut}_K F = \mathrm{Aut}_K E.$$

(iii) *The closure of* H *in* $\mathrm{Aut}_K E$ *under the topology on this group having for a basis of open sets the inverse images, under the restriction maps* π_F, *of the singleton subsets of the groups* $\mathrm{Aut}_K F$ $(F \in J)$; *equivalently, the topology having for basis of open sets the sets* $\{\alpha \in \mathrm{Aut}_K E \mid \alpha(a) = b\}$ $(a, b \in E)$.

Sketch of Proof. (ii) $\subseteq$ (i) is immediate (cf. the examples discussed above). Conversely, consider an element $\alpha \in \mathrm{Aut}_K E$ whose restriction to some intermediate field F of finite degree is *not* equal to the restriction of any element of H. The Fundamental Theorem of Galois Theory, applied to F/K, implies that there is some $a \in F$ fixed by the restrictions of elements of H but not by the restriction of α. This will be an element of H^*, hence as it is not fixed by α, we have $\alpha \notin H^{**}$.

The equivalence of (ii) with (iii), using the first description of the topology on $\mathrm{Aut}_K E$ in (iii), is immediate. To see the equivalence of this with the other description of the topology, note on the one hand that for any $a, b \in E$, if we take $F \in J$ such that $a, b \in F$, then $\{\alpha \in \mathrm{Aut}_K E \mid \alpha(a) = b\}$ will be the inverse image under π_F of a subset of $\mathrm{Aut}_K F$. In the other direction, given $F \in J$, the Theorem of the Primitive Element [**2**, Proposition V.6.15] [**4**, Theorem V.4.6] allows us to write $F = K(a)$, and the inverse image under π_F of any $\alpha_0 \in \mathrm{Aut}_K F$ can now be described as $\{\alpha \in \mathrm{Aut}_K E \mid \alpha(a) = \alpha_0(a)\}$. □

Thus, we get a bijective correspondence between intermediate fields, and subgroups of $\mathrm{Aut}_K E$ closed in the above topology.

The next Lemma, though we will apply it to Galois groups, is stated for general inverse limits of finite sets, so we need to make an explicit choice of how we will index objects of an inversely directed system (which we avoided doing in the last sentence of Theorem 1). From this point on, therefore, let us understand that in such a system, the maps $f_{j,j'}: X_j \to X_{j'}$ are defined for $j \leq j'$ (as in [**1**] and [**5**], but in contrast to the convention of [**4**]).

Lemma 3. *If* X *is the inverse limit of an inversely directed system of finite sets* $(X_j)_{j\in J}$ *and surjective set-maps* $X_{j,j'}: X_j \to X_{j'}$ $(j \leq j')$, *then the canonical maps* $\pi_j: X \to X_j$ *are also surjective.*

Sketch of Proof. Naively, we might hope to show this by starting with any $x_0 \in X_{j_0}$ $(j_0 \in J)$, applying Zorn's Lemma to partial families $(x_j)_{j\in J'}$ with $j_0 \in J' \subseteq J$ that satisfy the compatibility conditions $f_{j,j'}(x_j) = x_{j'}$ $(j \leq j' \in J')$ to get a maximal such family, and hoping that this will be an element of X mapping to x_0.

Unfortunately, the above compatibility conditions on partial families are not strong enough to guarantee that these can be extended to compatible families whose domain is all of J; hence the maximal families that Zorn's Lemma gives us may not have $J' = J$. To get around this, let us call a family $(x_j)_{j\in J'}$ ''robustly compatible'' if it has the property that for any finite set of elements $j_1, \ldots, j_n \in J'$, there exists a $j \in J$ less than or equal to all of these elements, and a $y \in X_j$ such that $f_{j,j_i}(y) = x_{j_i}$ for $i = 1, \ldots, n$. This is easily seen to imply the ordinary compatibility condition noted in the preceding paragraph.

We now claim that any robustly compatible family $(x_j)_{j\in J'}$ can be extended so as to adjoin to J' any $j_0 \in J - J'$. Indeed, given $(x_j)_{j\in J'}$ and $j_0 \notin J'$, suppose that for each $x \in X_{j_0}$, the assignment $x_{j_0} = x$ failed to give a robustly compatible family. Then for each such x we could choose a finite set of elements of J' for which the existence statement required by robust compatibility was false. Let us now apply to the union of these finitely many finite sets the robust compatibility assumption on $(x_j)_{j\in J'}$. This gives a certain $j \in J$ and $y \in X_j$. By the inverse directedness of J we can choose a $j' \in J$ that is $\leq j_0$ and also $\leq j$; by surjectivity of $f_{j',j}$ we can lift y to an element $y' \in X_{j'}$; and if we now let $x = f_{j',j_0}(y') \in X_{j_0}$, we get a contradiction to our choice of the finite subset of J' that allegedly gave a counterexample to the robust compatibility of the assignment $x_{j_0} = x$.

Hence the Zorn's Lemma argument sketched in the first paragraph, which fails for families that are merely compatible, works for robustly compatible families, completing our proof. □

Recall that every *finite* group can be represented as the Galois group of some Galois field extension of finite degree. There is a corresponding result for infinite Galois extensions.

Lemma 4. *Let G be a topological group. Then the following conditions are equivalent.*

(i) *G is isomorphic as a topological group to the inverse limit of an inversely directed system of finite groups and surjective group homomorphisms, topologized by taking for a basis of open sets the inverse images of singleton subsets of these groups.*

(ii) *G is isomorphic as a topological group to the Galois group of a Galois (i.e., separable normal algebraic) field extension E/K, topologized by taking for a basis of open sets the sets $\{\alpha\in G \mid \alpha(a) = b\}$ $(a, b\in E)$.*

Proof. We have seen that (ii)⇒(i). Suppose conversely that G is the inverse limit of a system of groups $(G_j)_J$ as in (i). Let us represent each G_j as a group of permutations of a finite set X_j, taking these sets to be disjoint. Since G has a natural map to each G_j, it acquires a natural action on each X_j, hence it acts on their union, $X = \cup X_j$. Let k be any field disjoint from the set X, make X a set of indeterminates over k, let E be the field of rational functions $k(X)$, let G act on E by its permutation action on the indeterminates, and let K be the fixed field of this action. Finally, for each $j\in J$, let $F_j = K(X_j) \subseteq E$.

Since the X_j are disjoint, it is not a priori evident that there are *any* inclusion relations among the fields F_j. We claim, nevertheless, that if $j\leq j'$ in J, then $F_j \supseteq F_{j'}$. To see this, consider the action of G on the compositum $F_j F_{j'} \subseteq E$. This compositum is generated over K by $X_j \cup X_{j'}$. The kernel of the action of G on this union is also the kernel of its action on the subset X_j, since the map of G into $G_{j'}$ factors through the map into G_j; so the groups of automorphisms of F_j and of $F_j F_{j'}$ induced by the actions of G can both be identified with G_j. Further, the fixed field of the action of G on each of these fields is K, since K is the fixed field of its action on E, and by construction both subfields contain K. Hence $[F_j : K] = |G_j| = [F_j F_{j'} : K]$, so the latter field cannot be strictly larger than the former, proving $F_j \supseteq F_{j'}$. Assertion (ii) now follows by the last paragraph of Theorem 2, applied to the system of subfields F_j. □

(In the above proof, we used Lemma 3 to conclude that G mapped surjectively to G_j, so that we could identify its action on X_j with that of G_j. However, if we had not proved that Lemma, we could actually have given the same argument, referring to $\pi_j(G)$ instead of G_j.)

Most of the further basic results of finite Galois theory go over to the infinite case. The main adjustment needed is that when one equates indices of subgroups with degrees of extensions, one does *not* have equalities of cardinality when these are infinite, but merely the statement that one is infinite if and only if the other is. I leave the formulation and verification of these results to the interested reader, noting only a key step that is useful in reducing results on index and degree to the finite case:

Lemma 5. *Let G be an inverse limit of finite groups $(G_j)_{j\in J}$, with projection maps written $\pi_j\colon G \to G_j$. Let $H_1 \subseteq H_2$ be subgroups of G, with H_1 closed in the topology described above, and let n be a positive integer. Then $[H_2 : H_1] \geq n$ if and only if there exists some $j\in J$ with $[\pi_j(H_2) : \pi_j(H_1)] \geq n$. Moreover, if this holds, then $[\pi_{j'}(H_2) : \pi_{j'}(H_1)] \geq n$ for all $j' \leq j$.*

Idea of Proof. From the definition of our topology it follows that any element not in H_1 has image outside the image of H_1 in some G_j. It follows that two elements in different right cosets of H_1 have images in different right cosets of the image of H_1 in some G_j. This property of G_j is preserved on going to smaller j, and using the inverse directedness of J, one can deduce that elements in n different right cosets of H_1 have images in n different right cosets of the image of H_1 in some G_j. □

3. Stone spaces. What topological groups do in fact occur as inverse limits of systems of finite groups?

Recall that a *topological group* means a group given with a topology with respect to which the group operations are continuous. Most authors also require that the topology be Hausdorff, but we shall not make this a part of our definition, because a stronger condition will soon be imposed. Actually, we have not yet proved that the group operations of our inverse limit groups *are* continuous in our topology, but we shall see this soon. Let us first note some basics.

Lemma 6. *Any inversely directed system of topological spaces* $(X_i)_I$ *has an inverse limit* X, *which has for underlying set the inverse limit of the underlying sets of the spaces* X_i, *and for a basis of open sets the inverse images of all open sets of the spaces* X_i *(or, alternatively, the inverse images of the members of any family of bases of open sets of the* X_i*).*

Any inversely directed system of topological groups $(G_i)_I$ *has an inverse limit* G. *Its underlying set is the inverse limit of the underlying sets of the* G_i, *and its topology and group structure respectively are those of these inverse limits of these objects in the categories of topological spaces and of groups.*

Sketch of Proof. It is straightforward to verify that the set-theoretic inverse limit of the X_i together with the indicated topology has the universal property of an inverse limit of the given topological spaces. Let us note why in our description of the inverse limit group G, the group multiplication $G \times G \to G$ is continuous in the inverse limit topology. By the universal property of that topology, it suffices to show that for every $i \in I$, the map $G \times G \to G_i$ gotten by following the group multiplication of G by the projection $\pi_i \colon G \to G_i$ is continuous. But this map can be gotten by projecting the two G's on the left to G_i and applying the multiplication operation of G_i, which is continuous by hypothesis. Continuity of the inverse operation is established in the same way.

It is now straightforward to verify that G, so topologized, has the universal property of an inverse limit of the given groups. □

We now see that the topology introduced in the preceding section is that of the inverse limit of the *discrete* topologies on the given finite groups; the discrete topology being, indeed, the only Hausdorff topology a finite set admits.

Let us note a few more facts that we will need about inverse limits of topological spaces. Recall that a topological space is called *totally disconnected* if for distinct points $x, y \in X$, there exists an *open-closed* subset $U \subseteq X$ containing x but not y.

Lemma 7. *Let* X *be the inverse limit of an inversely directed system* (X_i) *of topological spaces.*

The topology on X *is the topology induced by regarding* X *as a subset of* $\Pi\, X_i$ *with the product topology.*

If all X_i *are Hausdorff, then* X *is Hausdorff, and forms a closed subspace of* $\Pi\, X_i$.

If all X_i *are compact and Hausdorff, then* X *is compact and Hausdorff.*

If all X_i *are totally disconnected, then* X *is totally disconnected.*

Sketch of Proof. The first assertion is deduced by noting that the cylinders which form a basis of the topology of ΠX_i intersect X in sets which we have seen form a basis of the inverse limit topology.

That Hausdorffness carries over to products, and hence to subspaces of products, is clear. To show that in the Hausdorff case X is closed in ΠX_i, let $x \in (\Pi X_i) - X$. Then for some $i < j$ we have $f_{i,j}\pi_i(x) \neq \pi_j(x)$. If we take disjoint open sets U and V in X_j containing $f_{i,j}\pi_i(x)$ and $\pi_j(x)$ respectively, then the intersection of the inverse images in ΠX_i of $f_{i,j}^{-1}(U) \subseteq X_i$ and $V \subseteq X_j$ will be an open subset containing x but disjoint from X, as required.

To see that compactness carries over from the X_i to X when the former are Hausdorff, we may use Tychonoff's Theorem [**3**, Theorem 5.13], which says that compactness carries over to ΠX_i, together with the fact that a closed subspace of a compact space is compact.

The assertion on total disconnectedness is immediate. □

Let us now prove

Theorem 8. *A topological space can be written as an inverse limit of finite discrete spaces if and only if it is totally disconnected, compact, and Hausdorff.*

Proof. ''$\Rightarrow$'' follows from the preceding Lemma, since a finite discrete space is totally disconnected compact and Hausdorff.

To prove the reverse implication, let X be a totally disconnected compact Hausdorff space. Let I be the set of *partitions* of X into disjoint open-closed subsets, where we understand such a partition to mean a set of nonempty pairwise disjoint open-closed subsets of X having union X. Let us partially order I by writing $i < j$ if the partition i is a *refinement* of the partition j, i.e., if every member of i is a subset of a member of j. Given arbitrary $i, j \in I$, note that the set of nonempty intersections of members of i with members of j gives a partition of X into open-closed sets which refines both i and j; so the partially ordered set I is inversely directed.

Every member of I is finite because X is compact; let us regard each such i as a finite discrete topological space. If $i < j$, define $f_{i,j}: i \to j$ to take each member of i to the member of j which contains it. Let us likewise map X into each $i \in I$ by sending each $x \in X$ to the member of i in which it lies. We note that these maps $X \to i$ are continuous because the members of i are open in X. Since these maps are compatible with the $f_{i,j}$, they induce a continuous map $X \to \varprojlim_I i$.

To see that this map is surjective, let us write any $y \in \varprojlim_I i$ as a family $(U_i)_{i \in I}$, noting that for each $i \in I$, $U_i \in i$ is a nonempty open-closed subset of X. Using the compatibility condition on this member of the inverse limit, we can see that any finite subset of the U_i's has nonempty intersection in X; hence by compactness of X, they all have nonempty intersection. A point of this intersection will be an element of X mapping to y. To see that our map is one-to-one, note that the total disconnectedness condition on X says that any two points of X are distinguished by the map into some two-set partition.

Now our map $X \to \varprojlim_I i$, being a continuous bijection from a compact Hausdorff space to a compact Hausdorff space, is a homeomorphism [**3**, Theorem 5.8], completing the proof of ''$\Leftarrow$''. □

Totally disconnected compact Hausdorff spaces are often called *Stone spaces* after Marshall Stone (who himself called them *Boolean spaces*, for good reasons which we can't go into here; cf. [**3**, Exercise 5.S]). Lemma 6 and Theorem 8 imply in particular that every inverse limit of *finite groups* has a Stone space for underlying topological space.

4. Profinite groups. Is the converse true – given a topological group G whose underlying space is a Stone space, can we write G as an inverse limit of finite groups? To do this, we would have to find, among the finite discrete spaces that are continuous images of G, enough that admit group operations compatible with that of G to express G as their inverse limit. Since these discrete spaces correspond to partitions of G into open-closed sets, we need to study the relation between partitions and operations on sets.

Definition 9. *Given a map of sets,*

$$\alpha\colon\ X^{(1)}\times\ldots\times X^{(n)}\to\ Y, \tag{10}$$

and given a partition $p^{(m)}$ of one of these sets $X^{(m)}$ and a partition q of Y, we shall say that $p^{(m)}$ is compatible *with the mth argument of the map* (10) *and with the partition q if, for any two n-tuples $(x^{(1)},\ldots,x^{(m)},\ldots,x^{(n)})$, $(x^{(1)},\ldots,x'^{(m)},\ldots,x^{(n)})\in X^{(1)}\times\ldots\times X^{(n)}$, differing only in that the mth coordinate of the first is replaced in the second by an element in the same member of $p^{(m)}$, the images of these n-tuples under α lie in the same member of q.*

(*This use of the word ''compatibility'' should not be confused with our use of that term for the conditions relating the components of an inverse limit.*)

If in the above situation we are given a partition $p^{(m)}$ of $X^{(m)}$ for each m, it is easy to see that a necessary and sufficient condition for there to exist a map β making a commuting diagram

$$\begin{array}{ccc} X^{(1)}\times\ldots\times X^{(n)} & \xrightarrow{\alpha} & Y \\ \downarrow & & \downarrow \\ p^{(1)}\times\ldots\times p^{(n)} & \xrightarrow{\beta} & q \end{array}$$

is that for each m, $p^{(m)}$ is compatible with the mth argument of α and the partition q of Y.

Let us also note that given any map α as in (10) and any integer $m\le n$, there is a unique *coarsest* partition $p^{(m)}$ on $X^{(m)}$ that is compatible with the mth argument of (10) and the partition q, namely the partition that puts two elements $x^{(m)}$ and $x'^{(m)}$ in the same class if and only if every two elements of $X^{(1)}\times\ldots\times X^{(n)}$ that differ only by replacing $x^{(m)}$ by $x'^{(m)}$ in the mth coordinate have images under (10) in the same member of q.

Now consider a map (10) in which the $X^{(m)}$ and Y are all the same set X, and in which we take the same partition p for all the $p^{(m)}$ and also for q. If p is compatible with each argument of (10) and with the partition p, let us say it is *self-compatible* under (10). The next Lemma reformulates our problem in these terms.

Lemma 11. *Let X be a Stone space* (*a totally disconnected Hausdorff space*)*, and $\alpha\colon X^n\to X$ a continuous n-ary operation on X. Then the following conditions are equivalent.*

(i) *X is the inverse limit of an inversely directed system of finite discrete sets X_i with n-ary operations.*

(ii) *For every two distinct points $x, x'\in X$, there exists a partition p of X into open-closed subsets which is self-compatible under α, and such that x and y lie in distinct members of p.*

(iii) *Every partition of X into open-closed subsets can be refined to a partition into open-closed sets which is self-compatible under α.*

More generally, given a finite family of operations on X, the same equivalences hold, with self-

compatibility under all these operations replacing self-compatibility under α.

Sketch of Proof. Clearly (iii)⇒(ii). (ii)⇒(i) is proved in essentially the same way we proved Lemma 8, by noting that the partitions in question form an inversely directed system, and showing that the natural homomorphism from X to the inverse limit of that system is a homeomorphism.

To prove (i)⇒(iii), suppose X is the inverse limit of a system of finite sets X_i with n-ary operations, and p any partition of X into open-closed sets. Each member of p, being open, is a union of members of our basis of the inverse limit topology on X, that is, inverse images of points of various of the X_i. Since X is compact, we can find a *finite* family of these basic open sets, each wholly contained in some member of p, which cover X. To each open set U in this finite covering, let us associate an index i such that U is the inverse image of a point of X_i. If we take an index j which is $\leq$ each of these finitely many indices i, we find that each member of p is a union of inverse images of points of X_j, and since X_j is a homomorphic image of X as a set with n-ary operation α, the partition of X into these inverse images is self-compatible under α.

The case where there are more than one operations works the same way; we gave the arguments in the one-operation case merely for verbal convenience. □

Thus, for a given Stone space with algebraic structure, the question of whether (i) holds translates into that of whether (iii) holds. As a first step, we may ask to what extent, in the general context of (10), the passage from a partition q on Y to the coarsest partition compatible with q and with one of the arguments of α takes ''good'' partitions to ''good'' partitions. This, of course, depends on the sense of ''good''; for a negative example, it does not in general take finite partitions to finite partitions. This can be seen from the set-map

$$\alpha:\ \mathbf{Z}\times\mathbf{Z} \ \to\ \{0,1\}$$

taking (m,n) to 1 if $m=n$ and to 0 otherwise. If q is the nontrivial partition of $\{0,1\}$, then the coarsest partition of $\mathbf{Z}$ compatible with the first argument of α and with the partition q is the partition into infinitely many singletons.

On the other hand, the next Lemma gives a positive result in the context we are interested in.

Lemma 12. *Suppose that in* (10), *all* $X^{(m)}$ *and* Y *are Stone spaces,* α *is continuous, and* q *is a partition of* Y *into open-closed subsets. Then for each* m_0, *the coarsest partition of* $X^{(m_0)}$ *that is compatible with the* m_0*th argument of* α *and with the partition* q *of* Y *is also a partition into open-closed subsets.*

(*Actually, this does not require that all* $X^{(m)}$ *and* Y *be Stone, but only that all* $X^{(m)}$ *other than* $X^{(m_0)}$ *be compact; we have merely stated it under hypotheses we will later find convenient.*)

Proof. First let us simplify the problem: Let us regard the product of all the $X^{(m)}$ other than $X^{(m_0)}$ as a single compact topological space W and let us write $X^{(m_0)}$ as X; thus we have a continuous map $\alpha\colon W\times X\to Y$ and a partition q of Y into open-closed sets. Now let us fix a point $x\in X$, and note that for each $w\in W$, continuity of α implies that there exist open neighborhoods U_w of w and V_w of x such that $\alpha(U_w\times V_w)$ is contained in the open-closed member of q containing $\alpha(w,x)$. By compactness, W is covered by a finite subfamily of the open sets V_w; if we form the intersection of the corresponding finite family of open neighborhoods U_w of x, we get a neighborhood of x which, it is easy to verify, is contained in a single member of the partition of X we are interested in. Since x was an arbitrary point of X, this shows that this partition of X is into *open* sets. But a partition of any topological space into open sets is a partition into open-closed sets, since the complement of any member U of the partition is a union of open sets, hence open, hence U is closed. □

We now come to our final hurdle. Suppose X is a Stone space given with one or more continuous operations. Given a partition q of X into open-closed subsets, we may form, for each argument of each operation, the coarsest partition compatible with that argument and q. Taking the intersection (coarsest common refinement) of all these partitions and the original partition q, we get a partition q' of X into open-closed subsets, the coarsest such partition which refines q and is compatible with (all the arguments of) all the operations and q – but this does not say that it is compatible with all the operations and itself! We may repeat the process, getting a coarsest partition q'' which refines q', and is compatible with all the operations and q'. If we continue this process recursively, and take the intersection of the resulting chain of partitions, this will be the coarsest partition on X which refines q and is self-compatible under our operations. This is clearly a partition into *closed* subsets, but unless the process stopped after finitely many steps, there will be infinitely many of these, so they will not all be open; in this case, no partition into open-closed subsets refining q can be self-compatible.

Let us note briefly two examples of structures – other than groups – for which this difficulty actually occurs; which, in fact, admit *no* nontrivial partitions into open-closed subsets self-compatible under their operations. (I will show more details, if you want, in class, where I can draw pictures on the board.)

First, let X be a subset of the real unit interval consisting of 0, 1, and the members of a sequence $... < x_{-2} < x_{-1} < x_0 < x_1 < x_2 < ...$ with infimum 0 and supremum 1. This is a Stone space, and the unary operation which takes each x_n to x_{n+1} and fixes 0 and 1 is continuous; but there is no partition of X into open-closed sets self-compatible under this unary operation.

For the second example, form the compact space $2^{\mathbf{Z}}$ of all subsets of $\mathbf{Z}$, and let X be the closed subset consisting of all $x \in 2^{\mathbf{Z}}$ with the property

$$(\forall\, n \in \mathbf{Z}) \quad n-1 \in x,\ n+1 \in x \ \Rightarrow\ n \in x.$$

One finds that this set admits binary operations of greatest lower bound (namely, intersection) and least upper bound (namely, taking the union and then filling in all gaps of length 1). These operations are continuous in the given topology, so X is a topological lattice. But one can show that no nontrivial partition of X into open-closed subsets is self-compatible with respect to both lattice operations.

However, when we consider groups, the stars are favorable. The next result does not refer to topologies, but when combined with the preceding Lemma, it will give us what we have been seeking.

Lemma 13. *Let G be a group, and q a partition of the underlying set of G. Let $\alpha: G\times G\times G \to G$ denote the 3-fold multiplication map, $(x,y,z) \mapsto xyz$. Let p be the coarsest partition of G compatible with the middle argument of α and the partition q of G.*

Then p is self-compatible under the operations of G and is a refinement of q, hence is the coarsest partition with these properties.

Proof. Let us first show that p is self-compatible with respect to the first argument of the (binary) group multiplication. That is, assuming y and y' are in the same member of p, we shall prove yu and $y'u$ are also, for any $u \in G$. By definition, the latter condition holds if and only if, for arbitrary x and z, the elements $x(yu)z$ and $x(y'u)z$ are in the same member of q. But by associativity of G, these can be rewritten $x(y)(uz)$ and $x(y')(uz)$, and the assumption that y and y' are in the same member of p says that these 3-fold products are indeed in the same member of q, as required. The proof for the second argument of multiplication is, of course, the same.

For the case of the unary inverse operation, we must show, assuming y and y' in the same member of p, that y^{-1} and y'^{-1} are also, i.e., that for any x and z, the elements $x(y^{-1})z$ and $x(y'^{-1})z$ are in the same member of q. But we can write these two elements as $(xy^{-1})(y')(y'^{-1}z)$ and $(xy^{-1})(y)(y'^{-1}z)$, and again these lie in the same member of q by definition of p. (Alternatively, we could get this result on the inverse operation by noting that the results of the preceding paragraph imply that the set p inherits a multiplication, under which the map from G is a homomorphism of semigroups, and then calling on the well known fact that the image of a group under a semigroup homomorphism inherits an inverse operation.) That p refines q is seen by taking $x = z = 1$. □

A topological group or other algebraic structure which is an inverse limit of finite structures is called *profinite*. (The ''pro'' stands for ''projective'', because inverse limits are sometimes call *projective limits*. In this usage, direct limits are called *inductive limits*. What I am here loosely calling an ''algebraic structure'' can be more precisely defined as an ''algebra in the sense of universal algebra'' [**1**, §1.7 or §8.1].) Clearly, every profinite topological algebraic structure has a Stone space for underlying space. We can now combine the preceding three Lemmas to get the converse in the case of groups:

Theorem 14. *Any topological group G with underlying space a Stone space is profinite.* (*Hence, by Lemma 4, every such group can be represented as the Galois group of an algebraic field extension.*)

Proof. Given any partition q of G into open-closed subsets, let p be the refinement of q constructed in Lemma 13; by Lemma 12 this is also a partition into open-closed sets. Hence condition (iii) of Lemma 11 is satisfied, which implies the desired condition (i) of that Lemma. □

Let us record a couple of easy characterizations of profinite groups, which can be proved independently of the above hard result.

Lemma 15. *For a topological group G, the following conditions are equivalent:*

(i) *G is profinite.*

(ii) *G is compact, and has a neighborhood basis of the identity consisting of open* (*equivalently, open-closed*) *subgroups.*

(iii) *G is compact, and has a neighborhood basis of the identity consisting of open* (*equivalently, open-closed*) *normal subgroups.*

Sketch of Proof. To get the equivalences referred to parenthetically in (ii) and (iii), note that if a subgroup H of a topological group G is open, then so are all the proper right cosets of H, hence H, as the complement of the union of these cosets, is closed. Note also that if H is open and G is compact, then since G is covered by the right cosets of H, it is covered by finitely many, so H has finite index in G.

Now in any topological group G, the open-closed normal subgroups are precisely the kernels of continuous homomorphisms to discrete groups. With these observations (and, again, the idea of the last part of the proof of Theorem 8), the equivalence of (i) and (iii) is straightforward. Clearly, (iii)⇒(ii). To get the converse, note that an open subgroup H, since it has finite index, has only finitely many conjugates, so their intersection is an open normal subgroup contained in H. □

(The equivalence of (ii) and (iii) fails for non-compact topological groups. E.g., the semidirect product of the compact group $(\mathbf{Z}/2\mathbf{Z})^{\mathbf{Z}}$ and the discrete group $\mathbf{Z}$ acting by the shift has a neighborhood basis of open-closed subgroups, given by any such basis of $(\mathbf{Z}/2\mathbf{Z})^{\mathbf{Z}}$, but has no open-closed normal subgroups smaller than $(\mathbf{Z}/2\mathbf{Z})^{\mathbf{Z}}$ itself.)

5. Remarks on other algebraic structures. We have noted that the statement corresponding to Theorem 14 fails for sets with a single unary operation, and also for lattices. Some examples of algebraic systems for which it *holds*, other than groups, are monoids, semigroups, and associative rings. For monoids, the proof is exactly the same as for groups, using the same operation $(x, y, z) \mapsto xyz$, and merely omitting the discussion of the inverse operation. For semigroups not necessarily having identity element, one can get the result by taking p to be the coarsest partition that is simultaneously compatible with q and with the argument y in each of the four operations $(x, y, z) \mapsto xyz$, $(x, y) \mapsto xy$, $(y, z) \mapsto yz$ and $y \mapsto y$; or, more concisely, by adjoining a topologically isolated identity element, applying the result for monoids, and then discarding the identity element. For associative rings with 1, one uses the argument y of the 4-ary operation $(w, x, y, z) \mapsto w + xyz$; the reader is invited to work this case out, and see how nicely the ring identities yield the conditions needed. For nonunital associative rings, one can replace this with a family of operations, as for nonunital semigroups.

Note that the operations $\wedge$ and $\vee$ of a lattice are both semigroup operations. So by the above observations, a topological lattice with a Stone topology is profinite with respect to each of its operations separately (i.e., as an upper and as a lower semilattice), but not, in general, simultaneously! (For the reader who knows a bit more lattice theory, I will mention that a negative example can also be given for *modular* lattices, but that *distributive* lattices with Stone topologies are profinite, as one shows using the argument y of the operation $x \wedge (y \vee z)$.)

There is a parallel set of questions that can be treated in the same way as those treated here: If k is any field, then an inverse limit V of finite-dimensional discrete k-vector spaces, though not compact unless k is finite, will have a property called *linear compactness*: any family of *cosets of closed k-subspaces* of V which has the finite-intersection property has nonempty intersection. The topology on such an inverse limit V is also clearly what is known as a *linear* topology, meaning that open vector subspaces of V form a neighborhood basis of zero. One can show that the linearly compact Hausdorff linearly topologized vector spaces are precisely the inverse limits of finite dimensional discrete vector spaces, and establish a result analogous to Theorem 14, namely that an associative algebra with such a topology is an inverse limit of finite-dimensional discrete associative algebras. On the other hand, there are simple examples showing that the corresponding statement fails for other structures, such as Lie algebras.

REFERENCES

1. George M. Bergman, *An Invitation to General Algebra and Universal Constructions*, Berkeley Mathematics Lecture Notes, vol. 7, U. C. Berkeley Department of Mathematics, 1995.

2. Thomas W. Hungerford, *Algebra*, Graduate Texts in Mathematics, vol. 73, Springer-Verlag, 1974.

3. John L. Kelley, *General Topology*, University Series in Higher Mathematics, van Nostrand, 1955; Graduate Texts in Mathematics, vol. 27, Springer-Verlag, 1975. (My copy is the van Nostrand edition. I hope that the references I give are correct for the Springer edition as well.)

4. Serge Lang, *Algebra*, 3rd ed., Addison-Wesley, 1993.

5. Saunders Mac Lane, *Categories for the Working Mathematician*, Graduate Texts in Math., vol. 5, Springer-Verlag, 1971.