Galois Theory and Algebraic Closures

by Alex Waldron

Supervised by William Stein and Grigor Grigorov

1 Introduction.

This paper explores the generalization of classical (finite-dimensional) Galois theory via the Krull topology. The proofs behind the Galois theory of finite extensions are not given, but rather the formalism of the infinite case is examined in depth. The Galois group of the algebraic closure of a finite field is characterized both through its profinite structure and via a construction analogous to the Krull topology. We are thus able to prove that this extension is isomorphic to the Cartesian product over all primes of the p-adic integers.

2 Section. Finite Galois Theory.

Definition 1. The Galois group of a given field extension K/F, $\mathrm{Gal}(K/F)$, is defined as

$$\{\sigma \in \mathrm{Aut}(K) \mid \sigma(f) = f \ \forall \ f \in F\}, \tag{1}$$

forming a group under composition. The extension K/F is called "Galois" if it is the splitting field for a collection of polynomials $P \subset F[x]$ (K/F is normal), where each $f \in P$ is separable (K/F is separable). Then K/F is the minimal field extension in which each separable polynomial $f \in P$ splits into its distinct linear factors in $K[x]$.

Example 2. [5]The algebraic closure (or the maximal algebraic extension) of a field G, finite or with $\mathrm{char}(G) = 0$, is Galois. This holds since $\bar{G}/G$ is the splitting field for the collection of every separable polynomial in G, since (in fields such as G where every minimal polynomials is separable) a non-separable polynomial has the same splitting field as the largest separable polynomial that divides it.
A field H whose algebraic closure is not Galois must be infinite but with finite characteristic, such as the field $R(\mathbb{F}_q[x])$ of all rational functions in $\mathbb{F}_q[x]$. Such a field R has multiplicative inversion just as $\mathbb{Q}$; but the identity = 1 has additive order q, so $\mathrm{char}(H) = q$. The minimal polynomial of $\sqrt{x}$, $y^2 + x = 0$, does not "separate" in the given rational field: $y^2 + x = (y + \sqrt{x})(y + \sqrt{x})$.[5]

Theorem 3. Let K be a finite Galois extension of F; let $G = \mathrm{Gal}(K/F)$. For any group H of automorphisms of K, let $K^H \subset K$ denote the "H-invariant subfield" of K, the unique maximal field satisfying $h(K^H) = K^H \ \forall \ h \in H$. Then
a. There is a 1-1 correspondence between sub-extensions $K \supset L \supset F$ and sub-groups $H < G$ such that $H = \mathrm{Gal}(K/L)$, via $L = K^H$. This is an "order-reversing" correspondence (by inclusion) since larger field extensions of F correspond to smaller subgroups of G.

b. For any normal subgroup $H \lhd G$ such that $H = \mathrm{Gal}(K/K^H)$,

$$[K : K^H] = |H| \text{ and } [K^H : F] = [G : H], \tag{2}$$

where [ ] denotes degree of an extensions or the index of H in G (the cardinality of G/H). $||$ is the order of a group.

c. The extension K^H/F is Galois $\Leftrightarrow$ the subgroup H is normal $\Leftrightarrow \mathrm{Gal}(K^H/F) \cong G/\mathrm{Gal}(K/K^H)$ via the restriction $\sigma \in G \mapsto \sigma|_{K^H}$.[1,2,3,4,9,10]

Definition 4. An inverse system is a pair $(\{M_i\}, \phi_{ji})$, a collections of appropriate objects (often groups or modules over a commutative ring) and corresponding homomorphisms such that

$$\phi_{ji} : M_j \to M_i \, , i \leq j \tag{3}$$

$$\phi_{ii}(m) = m, \ \forall \ m \in M_i \tag{4}$$

$$i \leq j \leq k \Rightarrow \phi_{ki} = \phi_{ji} \circ \phi_{kj}. \tag{5}$$

Definition 5. [5]The inverse limit, denoted $\lim_{\leftarrow}$, of a given inverse system $(\{M_i\},\ \phi_{ji})$ can be constructed as follows:

$$\varprojlim M_i = \{(m_i)_{i\in I} : \text{if } i \le j, \text{then } m_i = \phi_{ji}(m_j)\} \subset \prod_{i\in I} M_i \tag{6}$$

Thus the inverse limit is the set of all sequences of elements such that each member of the sequence is the image of any other sequence (with index not less) under their corresponding homomorphism.

3 Infinite-Dimensional Galois Extensions.

An infinite algebraic extension K/F is Galois if it is the union of finite subfields E each Galois over F, since then K is the splitting field for the union of all collections of separable polynomials split by E. However, the characterization of the Galois group is more difficult. The Galois group of E_i is given by the quoteints of $\mathrm{Gal}(K/F)$ by infinite normal subgroups, not by finite subgroups.
Section 3.1 describes the Krull topology and gives two lemmas, and 3.2 generalizes the fundamental theorem.

Note 6. Here I worked from two very concise formulations of the generalization to the infinite case, refs. (1) and (3). I tried to flesh out all proofs sketched or omitted there.

3.1 Topology on the Galois Group.

Inital lemmas are given along with the construction of the Krull topology, used for the proof of theorem 15.

Lemma 7. Let $K \supset L \supset F$ be fields with K/F Galois, not necessarily of finite degree. Then $K^{\mathrm{Gal}(K/L)} = L$.

Note 8. This is not immediately true since it is conceivable that one element of the extension cannot be permutated without perturbing the base field (though theorem 3 prohibits this for the finite case).

Proof. [3]$K^{\mathrm{Gal}(K/L)} \supset L$ by the basic definition of the Galois group. Obtain the opposite inclusion by contrapositive: take an arbitrary element $\xi \in K - L$. To satisfy the conditions for Zorn's lemma,[6,10] let the subextensions L', where $K \supset L' \supset L$, form a partially ordered set inclusion. Let the same order apply to the corresponding Galois groups $\mathrm{Gal}(L'/L)$; call $\mathcal{G}$ the (po)set of all such Galois groups not fixing ξ. All finite extensions containing ξ are in $\mathcal{G}$ by theorem 3. Then $\mathrm{Gal}(K/L)$ is an upper bound on $\mathcal{G}$. Since K is a union of finite extensions, there exists a chain of finite $L'' \supset L$ such that no maximal element can be distinct from K. Then $\mathrm{Gal}(K/L)$ must be a maximal element in $\mathcal{G}$ of the chain of corresponding $\mathrm{Gal}(L''/L) \in \mathcal{G}$, and so does not fix arbitrary $\xi \in K - L$.

Note 9. (3) did not specify how Zorn's lemma was to be applied. □

[3]Consider the collection of all E_i, $K \supset E_i \supset F$, with $[E_i\colon F] < \infty$ and E_i/F Galois. Then let $\mathrm{Gal}(K/E_i) = G_i$ and $\mathrm{Gal}(E_i/F) = S_i$.

Lemma 10. [3]$G_i \lhd G$, therefore $G/G_i \cong S_i$.

Proof. Given any finite Galois $E_i' \supset E_i$, $G_i|_{E_i'} = \mathrm{Gal}(E_i'/E_i) \lhd \mathrm{Gal}(E_i'/F) = G|_{E_i}$ by theorem 3, and since K is a union of E_i', it must hold that $G_i \lhd G$.
If there exists $\xi \in E_i$ for which $\sigma(\xi) \notin E_i$ for some $\sigma \in G$, then $\sigma(\xi)$ will be moved by some $\gamma \in G_i$ (by lemma 7) so that (since G_i is a normal subgroup) $\gamma(\xi) = \sigma^{-1}\gamma\sigma(\xi) \neq \xi$ which is impossible since G_i fixes E_i. Then $\sigma|_{G_i}$ is an automorphism of G_i. Two members ς, δ of a coset in G/G_i satisfy $\varsigma^{-1}\delta|_{E_i} = \mathrm{id}_{E_i}$, the identity on E_i, so $\varsigma|_{E_i} = \delta|_{E_i}$. Thus the group $G/G_i \cong \{\sigma|_{E_i}\ \forall\ \sigma \in G\}$ is the complete set of automorphisms of E_i fixing F.

Note 11. This statement was given without explanation in reference 3. □

If $E_i \supset E_j$, then there is a natural homomorphism

$$\phi_{ij} : S_i = \mathrm{Gal}(E_i/F) \to S_j = \mathrm{Gal}(E_j/F) \tag{7}$$

where ϕ_{ij} restricts $\sigma \in E_i|_{E_j}$. Then (E_i, ϕ_{ij}) forms an inverse system.

Theorem 12. [3] $G = \varprojlim S_i = \varprojlim G/G_i$, with $\phi_i : G \to G/G_i = S_i$ being the canonical projection as in (7).

Proof. Since K/F is algebraic, any $\xi \in K$ lies in some E_i. Then $\forall\, \sigma \in G$, $\sigma(\xi) = (\phi_i\sigma)(\xi)$ for that same i. Hence σ is uniquely determined by the nature of all the $\phi_i\sigma$ (since the values of σ over all ξ are determined by some E_i), and thus can be written as the inverse limit. □

Now we continue to describe the Krull topology. Construct the map[1]

$$\sigma \mapsto \sigma|_{E_i} : G \to \prod_{E_i \subset K} \mathrm{Gal}(E_i/F) \tag{8}$$

As above, this is correct since each restriction is in fact an automorphism of E_i. Give every finite $\mathrm{Gal}(E_i/F)$ the discrete topology. Give $\prod \mathrm{Gal}(E_i/F)$ the product topology. We can give $\mathrm{Gal}(K/F)$ the subspace topology in $\prod \mathrm{Gal}(E_i/F)$ since (8) is injective by definition of K. So equivalently, two elements are in the same open set if their restriction to a given E_i is the same (and unions of these sets can form any larger open sets generated by the product topology).
Note that any set G/G_i corresponding to a finite Galois extension is also trivially closed since its complement is null. In fact, the product topology is the least refined topology such that all projections from the product to the components are continuous; so each ϕ_i is continuous exactly between G and its finite Galois subextensions, allowing for a sharp application of finite Galois theory resulting in the "if and only if" statement of theorem 15.[5]
Furthermore, we can make several statements about $\mathrm{Gal}(K/F)$. Each subgroup $\mathrm{Gal}(E_i/F)$ is dicrete, therefore compact: so $\prod \mathrm{Gal}(K/F)$ is compact by the Tychonoff theorem. The image of $\mathrm{Gal}(K/F)$ is closed in the product since any product element $\chi \notin \mathrm{Gal}(K/F)$ contains a pair of restrictions prohibited for $\sigma \in \mathrm{Gal}(K/F)$ by inclusion of E_i, a pair of inclusions which can be required by the open set containing χ. Thus $\mathrm{Gal}(K/F)$ is compact, since it is a closed subset of a compact set. It is Hausdorff, since two distinct elements contain a distinct restriction to some E_i. It is also "totally disconnected" since any open set can be partitioned by any E_i since all are discrete. In fact, these last three are general properties of the "profinite topology" which apply here since we have simply adapted the profinite topology to exclude non-Galois normal extensions.
Furthermore, the open subgroups $\mathrm{Gal}(K/E_i)$ form a system of neighborhoods of 1 (the identity) in $\mathrm{Gal}(K/F)$.

3.2 Generalized Galois Correspondence

Lemma 13. [3] Let $H < G$. Then, $H = \mathrm{Gal}(K/L)$ for some field $L, K \supset L \supset F$ (namely $L = K^H$) $\Leftrightarrow$ H is closed in G.

Proof. [3] ($\Rightarrow$) Let $H = \mathrm{Gal}(K/L)$, let $\sigma \in \bar{H}$ in G, and let $\xi \in L$.
If $\sigma(\xi) = \xi$, then, $\sigma \in H$ so that $\bar{H} = H$ implies that H is closed, hence done.
Let $K_0 \subset K$ be the splitting field of the minimal polynomial of ξ over F, so that K_0/F is Galois and $[K_0\colon K] < \infty$. Let $G_0 = \mathrm{Gal}(K/K_0)$, $S_0 = \mathrm{Gal}(K_0/F)$, and $\phi_0 : G \to S_0 = G/G_0$ be the projection. Since S_0 is discrete, $\phi_0 H \subset S_0$ is closed. Hence $\phi_0^{-1}\phi_0 H$ is closed in G by continuity of ϕ_0. Leave ξ fixed; then since σ lies in the closure of H, and $\phi_0^{-1}\phi_0 H$ is a closed set containing H (and hence its closure), $\sigma \in \phi_0^{-1}\phi_0 H$ so that $\sigma(\xi) = \xi$.

($\Leftarrow$) Let $H < G$ be closed. $H \subset \mathrm{Gal}(K/K^H)$ follows by definition 1. Then prove the contrapositive of $H \supset \mathrm{Gal}(K/K^H)$, the statement $\sigma \notin H \Rightarrow \sigma \notin \mathrm{Gal}(K/K^H)$. H is closed $\Rightarrow H^c \ni \sigma$ is open $\Rightarrow \exists$ open basis set $N \ni \sigma$ s. t. $H \cap N = \emptyset \Rightarrow \exists$ finite Galois extension K_1/F with $\phi_1 : G \to S_1 = \mathrm{Gal}(K_1/F)$ such that $\phi_1\sigma \notin \phi_1 H$ ($\Rightarrow \sigma|_{K_1} \notin H|_{K_1}$). Then $K_1^{\phi_1 H} \subset K_1$ is fixed by H so that $K_1^{\phi_1 H} \subset K^H$; and $\phi_i\sigma \notin \phi_i H = \mathrm{Gal}(K_1^{\phi_1 H}/F) \Rightarrow K_1^{\phi_1 H}$ is not fixed by $\phi_1\sigma$ by the 1-1 correspondence of theorem 3, establishing the contrapositive.

Note 14. The Krull topology results in this precise statement because the open basis sets correspond to the elements only of finite Galois extensions, so that H is closed implies that every element of the complement projects to a finite Galois extension allowing the use of the inclusions of finite Galois theory in ($\Leftarrow$). The ($\Rightarrow$) implication would hold for any continuous projection in a profinite topology. □

Theorem 15. [3]Generalized Theorem 3. Let K/F be an arbitrary Galois extension. Then there is a one to one correspondence between fields L with $K \supset L \supset F$ and closed subgroups $H < G$.

Proof. The maps defining the correspondence are exactly as in theorem 3, with the exception that they refer only to closed subgroups, not arbitrary subgroups. Lemma 7 ensures that this correspondence is an injection from subfields to subgroups; lemma 13 identifies the image of the subgroups as the set of all closed subgroups of G. □

4 Extensions of a Finite Field.

All finite extensions of a finite field $\mathbb{F}_q$ must have order in powers of q since each basis element of the extension is cyclic of order q under scalar multiplication; non-prime-power orders are not allowed since divisors of zero would occur. Thus any finite field extension is of the form $\mathbb{F}_{p^m}/\mathbb{F}_{p^n}$ where $n|m$. Then the order of $\mathbb{F}_q^*$, the group $(\mathbb{F}_q - \{0\}, \times)$, is $q-1$, i. e. $x^{q-1} = 1$.
In order to construct such a field extension, one can take $\mathbb{F}_{p^n} = \mathbb{F}_p[x]/i_n(x)$, where $i_n(x)$ is an irreducible polynomial of degree n in $\mathbb{F}_p$. There are p^n elements of degree $< n$, the members of $\mathbb{F}_{p^n}$; no divisors of 0 exist since the polynomial is irreducible.
The following recasting is more practical: take $\mathbb{F}_{p^n} = \mathbb{F}_p[j_n]$, where j_n satisfies $i_n(j_n) = 0$. Then $\mathbb{F}_{p^n}$ is the set of all polynomials in j_n of degree less than n. Likewise no divisors of 0 exist. Then it remains to verify that such an $i_n(x)$ can be found in all cases.

Theorem 16. In any polynomial ring $\mathbb{F}_p[x]$, there exists an irreducible polynomial of degree n $\forall n$.

Proof. As for any field, any polynomial over a finite field can be split completely into linear factors in some extension. Consider the polynomial $f(x) = x^{p^n-1} - 1$. Then $f(x) = 0 \ \forall \ x \neq 0 \in \mathbb{F}_{p^n}$, since the order of $\mathbb{F}_{p^n}^* = p^n - 1$. Thus $f(j_n) = 0$, so if $\mathbb{F}_{p^n}$ exists, there must be an irreducible polynomial of degree n among the factors of f, so we can show that this is required for unique factorization in $\mathbb{F}_p$. Then $f(x) = x^{(p-1)(p^{n-1}+p^{n-2}+\ldots+1)} - 1$. As with $\mathbb{F}_{p^n}$, all irreducible factors of $f(x)$ come from a field of order equal to some factor of the exponenent. Since $(p^{n-1} + p^{n-2} + \ldots + 1) \neq p^{n'} - 1$ for any $n' \leq n$, the irreducible factors are of degree either 1 or n. Since every element not containing j_n is a root, their product, $x^{p-1} - 1$, divides $f(x)$. Then $f(x)/(x^{p-1} - 1) = (x^{p^n-p} + x^{p^n-2p+1} + x^{p^n-3p+2} + \ldots + 1) = x^{p(p^{n-1}-1)} + x^{p^n-1-2(p-1)} + x^{p^n-1-3(p-1)} + \ldots + 1 = \sum_{i=0}^{i=m} x^{i(p-1)}$, where $m = p^{n-1} + p^{n-2} + \ldots + p$. Then for $\mathbb{F}_p$, in which each element has order $p-1$, each term is equal to 1, so the sum is equal to $p^{n-1} + p^{n-2} + \ldots + p + 1$, which is not divisible by p. Thus there are no further linear factors in $\mathbb{F}_p$, and the remaining factors must be irreducibles of degree n. □

Note 17. This proof was attempted by induction on n, but the combinations of reducibles and irreducibles did not fit a convenient analytical description.

The Galois group of such an extension consists strictly of powers of the Frobenius automorphism $\sigma_p^n : a \to a^{n\,p}$, for $n \leq m = \deg(\mathbb{F}_{q^m}/\mathbb{F}_q)$ since the extenion has order $\deg(\mathbb{F}_{q^m}/\mathbb{F}_q)$. This is the only nontrivial mapping that fixes the elements of the original field. Hence the Galois group is cyclic of order m.

5 Two proofs of isomorphism of $\mathrm{Gal}(\overline{\mathrm{F}_{p^n}}/\mathrm{F}_{p^n})$ to $\Pi_{p\,\mathbf{prime}}\mathrm{Z}_p$.

This final section uses the Krull topology and theorem 15 to characterize the Galois group of a finite field, proving its isomorphism to the product (over all primes p) of the ring of p-adic integers.

Theorem 18. $\mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q) \simeq \prod_{p\,\mathrm{prime}} \mathbb{Z}_p$.

Proof. (1)[3](By inverse limits) For any n there is a unique finite Galois extension $K^{\sigma_q^n}$, i. e. a subextension of K invariant under the action of the q Frobenius element of n'th degree $\Rightarrow$ $S^n := \mathrm{Gal}(K^{\sigma_q^n}/K)$ is cyclic of order n and generated by σ as above. $S^n \simeq \mathbb{Z}/(n)$ via $\sigma^\nu \mapsto \nu \bmod n$, i. e. where composition of σ corresponds to addition on $\mathbb{Z}/(n)$. We thus know that $K^m \supset K^n$ if and only if $n|m$ since K^m must preserve the cyclic structure of K^n. In this case we have a homomorphism $\phi_{m,n} : \mathbb{Z}/(m) \to \mathbb{Z}/(n)$ via $\nu \bmod m \mapsto \nu \bmod n$, so that the larger structure simply reduces to the smaller structure; hence we have an inverse system of Galois groups. Now note that when $(m', n') = 1$, then the field extension $K^{m'} \cup K^{n'} = K^{m'n'}$ since they fix their least common multiple. Then $S^{m'n'} \simeq S^{m'} \times S^{n'}$ since any of $m'n'$ distinct elements of $S^{m'n'}$ corresponds to exactly one permutation of m' and one of n' in order to fix $S^{m'n'}$.
We can use an inverse limit to describe the Galois group over powers of some p since each larger group contains the smaller, so we simply want the combination of all of them out to infinity. Thus we can describe the Galois group:

$$G = \mathrm{Gal}(K/\mathbb{F}_q) = K^{\{\mathbb{N}\}} = S^{\{\prod_{p\,\mathrm{prime}} p^\nu\}}, \tag{9}$$

where the superscript at right denotes the set of all prime factorizations of the positive integers. The rightmost equality follows from the lemma 7. Then, by the two relations just given for prime powers and composite with coprime factors, and by isomorphism of an individual group to $\mathbb{Z}/(p^\nu)$:

$$G = S^{\{\prod_{p\,\mathrm{prime}} p^\nu\}} \simeq \prod_{p\,\mathrm{prime}} \varprojlim S^{p^\nu} \simeq \prod_{p\,\mathrm{prime}} \varprojlim \mathbb{Z}/(p^\nu) = \prod_{p\,\mathrm{prime}} \mathbb{Z}_p. \tag{10}$$

□

Proof. (2)[1] (by construction isomorphic to Krull topology) Retain the definitions of proof (1).
First note that by theorem 15, G is the closure of $B := \langle\sigma\rangle$ in the Krull topology, i. e. the smallest Galois group containing B, since here the algebraic closure is Galois. So we want to construct the closure of B with respect to the Krull topology.
$B \subset G$ is the set of all powers of σ. Biject each element of $\langle\sigma\rangle$ with $\mathbb{Z}$ by its power, and describe the Krull topology on $\mathbb{Z}$. Any a, $b \in \mathbb{N}$ are contained in the same open subset if they are congruent mod n for some n, as then $\sigma^a|_{\mathbb{F}_{p^n}} = \sigma^b|_{\mathbb{F}_{p^n}}$ (all finite extensions are Galois) since $\mathrm{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p)$ is cyclic order n. Then each open basis set is defined by a pair ν, n such that $x \equiv \nu \bmod n \,\forall\, x \in N$. Then given two open basis sets M, N, defined by the respective residues ν_m, ν_n, $\nu_m \equiv \nu \bmod n \Rightarrow M \supset N$ iff $n|m$ (as in proof (1)). Thus a sequence of larger n divisible by all previous n is a nested collection of neighborhoods whose intersection is the identity in B, and any open set is part of such a nested subset of the overall system of neighborhoods. These are neighborhoods of 0 in $\mathbb{Z}$, i. e. the unrestricted σ^0, the identity, 1, on G as mentioned in the general construction.
Since we are dealing strictly with a system of neighborhoods, the closure of this set is equivalent to its completion under the norm of inclusion on these neighborhoods. So we take the usual closure of such a topological group, where the set of all Cauchy sequences are included in the group. A Cauchy sequence $(a_i)_{i\geq 1}, a_i \in \mathbb{Z}$, satisfies the condition that for all $n \geq 1$, there exists N s. t. $i, j > N \Rightarrow a_i \equiv a_j \bmod n$. Call such a Cauchy sequence "trivial" if $\forall\, n \geq 1\ \exists\ n$ such that $a_i \equiv 0 \bmod n$, i. e. it behaves like the identity for n sufficiently large. The Cauchy sequences form a commutative group under addition of elements, and the trivial Cauchy sequences form a subgroup. Then define $\hat{\mathbb{Z}}$ to be the quotient of the first group by the second. It has a ring structure (by that of $\mathbb{Z}$ component-wise).

By the Chinese Remainder Theorem, an element of such a Cauchy sequence in $\mathbb{Z}$ can satisfy a finite number of arbitrary congruences (provided they reduce feasibly over powers of the individual p), so the limit can achieve countably many congruences (a set of congruences over all p and n is countable). Then each coset in $\hat{\mathbb{Z}}$ is identified with a set of congruences ν_{p^n} modulo each $p^n \in \mathbb{Z}$ achieved in the limit $i \to \infty$; the set of congruences is subject only to the requirement that reduction mod p^n is again a homomorphism of ν_i (i. e. for $n \geq m$, $\nu_{p^n} \equiv \nu_{p^m} \mod p^m$). Likewise, an element of the ring of p-adic integers $\mathbb{Z}_p$ satisfies any set of congruences over p^n allowing for reduction, since $\mathbb{Z}_p$ is the set of all $\sum_{i=0}^{\infty} a_i p^i a^i \in \{0, \ldots, p-1\}$, so that $a_i = \nu_{p^i}$, and $\prod_{p \text{ prime}} \mathbb{Z}_p$ can satisfy any set of such congruences over separate primes. Addition on $\prod_{p \text{ prime}} \mathbb{Z}_p$ is done component-wise, and maintains the exact analogy with compsition (addition of powers) on the Galois group.
Thus, by constructing the completion (closure) in the Krull Topology of the group generated by the Frobenius automorphism, we have another proof that

$$\prod_{p \text{ prime}} \mathbb{Z}_p \simeq \mathrm{Gal}(\overline{\mathbb{F}_q}/\mathbb{F}_q). \tag{11}$$ □

Bibliography

1 Milne, James. Fields and Galois Theory. August 31, 2003. www.jmilne.org/math

2 Stepanov, Serguei. Arithmetic of Algebraic Curves. Moscow, 1994: Monographs in Contemporary Mathematics.

3 Park, Jinhyun. A Personal Note on Infinite Galois Theory. 2004: www.math.uchicago.edu/~jinhyun/note/galois/galois/pdf.

4 http://planetmath.org/encyclopedia (various entries)

5 http://mathworld.wolfram.com (various entries)

6 Halmos, Paul. Finite-Dimensional Vector Fields. New York, 1984: Springer-Verlag.

7 Hellegouarch, Yves. Invitation to the Mathematics of Fermat-Wiles. Boston, 2002: Academic Press.

8 Stewart, Ian and Tall, David. Algebraic Number Theory and Fermat's Last Theorem. Natick, MA, 2002: A. K. Peters, Ltd.

9 Stewart, Ian. Galois Theory: 3rd Edition. New York, 1989: Chapman and Hall Ltd.

10 Artin, Michael. Algebra. 1991: Prentice Hall.

Note 19. The most important thing that this paper taught me is that it makes a whole lot more sense to bite the bullet and learn math from textbooks and their exercises than to try to be edified by groping for proofs yourself.