Summer 8-21-2015

On Dedekind's "Über die Permutationen des Körpers aller algebraischen Zahlen"

Joseph JP Arsenault Jr
University of Maine - Main, joe.arsenault@umit.maine.edu

ON DEDEKIND'S "ÜBER DIE PERMUTATIONEN DES KÖRPERS ALLER ALGEBRAISCHEN ZAHLEN"

By

Joseph J.P. Arsenault, Jr.

B.S. University of Maine, 1995

A THESIS

Submitted in Partial Fulfillment of the

Requirements for the Degree of

Master of Arts

(in Mathematics)

The Graduate School

The University of Maine

August 2015

Advisory Committee:

William M. Snyder, Professor Emeritus of Mathematics, Co-Advisor

Eisso J. Atzema, Lecturer in Mathematics, Co-Advisor

Andrew H. Knightly, Associate Professor in Mathematics

LIBRARY RIGHTS STATEMENT

In presenting this thesis in partial fulfillment of the requirements for an advanced degree at The University of Maine, I agree that the Library shall make it freely available for inspection. I further agree that permission for "fair use" copying of this thesis for scholarly purposes may be granted by the Librarian. It is understood that any copying or publication of this thesis for financial gain shall not be allowed without my written permission.

Signature: ____________________________________ Date: ____________
Joseph J.P. Arsenault, Jr.

ON DEDEKIND'S "ÜBER DIE PERMUTATIONEN DES KÖRPERS ALLER ALGEBRAISCHEN ZAHLEN"

By Joseph J.P. Arsenault, Jr.

Thesis Co-Advisors: Dr. William M. Snyder
Dr. Eisso J. Atzema

An Abstract of the Thesis Presented
in Partial Fulfillment of the Requirements for the
Degree of Master of Arts
(in Mathematics)
August 2015

We provide an analytic read-through of Richard Dedekind's 1901 article "Über die Permutationen des Körpers Aller Algebraischen Zahlen," describing the principal results concerning infinite Galois theory from both Dedekind's point of view and a modern perspective, noting an apparently uncorrected error in the supplement to the article in the *Collected Works*. As there is no published English-language translation of the article, we provide an annotated original translation.

THESIS ACCEPTANCE STATEMENT

On behalf of the Graduate Committee for Joseph J.P. Arsenault, Jr., we affirm that this manuscript is the final and accepted thesis. Signatures of all committee members are on file with the Graduate School at the University of Maine, 42 Stodder Hall, Orono, Maine.

Signatures: ______________________________________ Date: ____________
Dr. William M. Snyder
Professor Emeritus of Mathematics

______________________________________ Date: ____________
Dr. Eisso J. Atzema
Lecturer in Mathematics

TABLE OF CONTENTS

Chapter

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1

INTRODUCTION

In the 1901 paper “Über die Permutationen des Körpers aller algebraischen Zahlen” (“On the Permutations of the Field of All Algebraic Numbers”), Richard Dedekind demonstrates the failure of the Fundamental Theorem of Galois Theory for infinite degree algebraic extensions of the rational numbers $\mathbb{Q}$. Dedekind’s original work concerning infinite Galois Theory is in effect the genesis of a field whose beginning is generally credited to Wolfgang Krull [7], some quarter century later. Dedekind provides a coherent exploration of fundamental characteristics of infinite Galois extensions (within an algebraic closure of $\mathbb{Q}$). The supplement from Dedekind’s *Nachlass*, published with the paper in the Collected Works, suggests that Dedekind in fact devised a natural characterization of the closed subgroups of the Galois group, in Krull’s sense, without the modern devices (e.g., general topology, general field theory, general set theory with the Axiom of Choice) Krull had at his disposal.

Dedekind establishes the failure of the Fundamental Theorem for the case of infinite Galois extensions over $\mathbb{Q}$ by showing that, for any infinite degree p-power cyclotomic extension (for fixed odd prime p), there is a proper subgroup of its Galois group that has the same fixed field as the full group.[1] Cyclotomic extensions had been thoroughly studied before the 1890s, making construction of the counterexample as straightforward as possible. But in fact, until the mid-1890s, the entire subject of infinite-degree extensions for Dedekind “hat bisher ein *Noli me tangere* gegolten [had hitherto been considered a *Noli me tangere* (Touch me never)].”[2] It is perhaps then unsurprising that

[1] Dedekind’s finding for a field of characteristic zero is found to hold for general characteristic, e.g., as when J. Neukirch shows that both the proper subgroup of the Galois group of the algebraic closure of $\mathbb{F}_p$ generated by the Froebenius automorphism has precisely $\mathbb{F}_p$ for its fixed field. The limitation to algebraic subfields of $\mathbb{C}$ is a practical matter for Dedekind: The paper seeks to demonstrate the failure of the Fundamental Theorem of Galois Theory when the degree of the extension is nonfinite by constructing a single example.

[2] Letter to Frobenius, April 18, 1897, quoted in [3], V. II.

Dedekind sought a concise, efficient proof advancing the understanding of field theory and its connections to Galois theory for the case of infinite degree extensions.

In this work, a modern presentation of Dedekind's proof is first provided. Our elementary description of his proof uses relevant contemporary mathematical machinery. Thereafter an overview of the paper itself is given, connecting modern with Dedekind's concepts and terminology. Finally, an annotated translation of Dedkind's article is presented, as there is presently no English translation of the article available.

Appendix A provides proofs of results mentioned in the modern exposition.

CHAPTER 2

MODERN EXPOSITION OF RESULTS AND SYNOPSIS OF ARTICLE

2.1 Introduction

B. M. Kiernan, in “The Development of Galois Theory from Lagrange to Artin” [6], describes the evolution of Galois theory through 1950 as having three stages. Its initial phase was “computational,” developing the theory of equations. (This phase includes work from Lagrange to Galois himself.) The second phase was “one of abstraction” involving the development of group theory and field theory. (Cauchy, Serret, and even C. Jordan may be included in this phase.) The third phase was “one of generalization, even universalization,” epitomized for Kiernan by E. Artin’s seminal work, *Galois Theory* [1] establishing the theory as the study of the Galois groups of field extensions. Further significant generalization and universalization of the theory was provided by W. Krull [7], who extended the central theorem of the one-to-one correspondence between the intermediate fields of a finite Galois extension and the subgroups of the Galois group to the case of infinite Galois extensions. Krull did so by imposing a topology on the group and deriving a one-to-one correspondence between the intermediate fields of the Galois extension and the closed subgroups of the Galois group.

Bridging all three phases and contributing fundamentally to Artin’s and Krull’s formulations is R. Dedekind. Dedekind was apparently the first mathematician to offer lectures in algebra that covered Galois theory. Dedekind’s Göttingen lectures on higher algebra given the winter semester 1857-1858 (see [12] for a published copy of the lectures) introduced Galois’ concepts and results to German-speaking mathematicians, including Henrich Weber. In the forward to his *Lehrbuch der Algebra*, Vol. 1, [14], Weber mentions his appreciation of Dedekind’s 1857-1858 lectures, particularly his inclusion of Galois theory. Dedekind’s subsequent consideration of Galois’ work was, as with his non-constructivist approach to mathematics, with an eye toward abstraction and well-founding. His reformulation of finite Galois theory, as a study of vector spaces over subfields of the complex numbers and groups of isomorphisms ("permutations") is precisely surveyed in his Eleventh Supplement to Dirichlet's *Vorlesungenüber Zahlentheorie*, [4]; cf. § 160–§ 166. This work provides one bridge between the second and third phases of Galois theory. Indeed, comparison of Dedekind's with Artin's formulations makes clear how closely Artin's generalization and universalization of Galois theory is indebted to Dedekind's approach, extended to fields of arbitrary characteristic. Dedekind built a second bridge to the modern theory of Galois theory in the 1890s through his consideration of infinite-degree Galois extensions. His principal result in this area, "Über die Permutationen des Körpers Aller Algebraischen Zahlen" (see [3], Vol. II, Article XXXI), provided the kernels of insight Wolfgang Krull needed to successfully develop infinite Galois theory in the 1920s. Similar to Artin's development, Krull's main ideas follow quite closely those presented by Dedekind, over a quarter of a century earlier. One is reminded of Emmy Noether's observation, "Es steht schon bei Dedekind" ("It is already in Dedekind").

The purpose of this work is to describe this second bridge, Dedekind's investigation into infinite Galois theory, and give a translation of the work. First we review general Galois extensions, finite and infinite. We then give a synopsis of Dedekind's paper, after which we present our translation.

2.2 A Review of Infinite Galois Extensions

We first present a brief review of (finite and infinite) Galois theory from a modern standpoint. To this end, let K/k be a Galois extension of fields, i.e., a normal separable extension (not necessarily finite), within a fixed separable algebraic closure $\overline{k}$, which exists by the well-ordering principle.[1] Let $G = \mathrm{Gal}(K/k)$ be its Galois group. Note we

[1] See the article [13] of E. Steinitz. This work, published in 1910, is a rather modern axiomatic treatment of field extensions (excluding Galois theory). The most popular types of fields at the turn of the twentieth century were number fields and algebraic function fields. But this changed with Hensel's development of p-adic numbers. As Steinitz mentions, this creation of Hensel motivated Steinitz to give an

have $\mathrm{Gal}(\overline{k}/k)$ as a special case. Endow the Galois group G with the Krull topology, by which we decree that a fundamental system of neighborhoods of the identity, id_K, be the set of subgroups of the form $\mathrm{Gal}(K/E)$, where E is finite Galois over k and an intermediate field $k \subseteq E \subseteq K$. The group G is a topological group under the Krull topology. Notice that when G is finite, $\mathrm{Gal}(K/K) = \{id_K\}$ is an open set and this implies that G is discrete with respect to the Krull topology. (Cf. Appendix Section A.3.)

With this machinery we can state the fundamental theorem of Galois theory.

Theorem [Galois Correspondence] *Let K/k be a Galois extension. Then the mapping*

$$F \mapsto \mathrm{Gal}(K/F)$$

gives a one-to-one correspondence between all intermediate fields F, i.e., $k \subseteq F \subseteq K$, and all closed subgroups of $\mathrm{Gal}(K/k)$.

This theorem subsumes the fundamental theorem of finite Galois theory which determines a one-to-one correspondence between all intermediate extensions and all subgroups of G, since in the finite case the group G has the discrete topology, so in particular all subgroups are closed. (Cf. Appendix Section A.4.)

The Krull topological group can also be described as a profinite group. Consider the Cartesian product $\prod = \prod_E \mathrm{Gal}(E/k)$ of all finite Galois extensions of k contained in K. Endowing the finite groups $\mathrm{Gal}(E/k)$ with the discrete topology, the Cartesian product becomes a topological group with respect to the product topology (since the product topology is defined as the coarsest topology on the product such that projections onto components, $(\dots, \sigma_E, \dots) \mapsto \sigma_E$, for all E as above, are continuous). Forming

axiomatic treatment of general field theory, including for the first time a study of extensions of fields of non-zero characteristic. This work includes a proof of the existence of algebraically closed fields using the well-ordering principle of Zermelo, based on ideas of G. Cantor.

the inverse (projective) limit

$$\varprojlim_{E} \mathrm{Gal}(E/k) = \Big\{(\dots, \sigma_E, \dots, \sigma_F, \dots) \in \prod \, : \, \sigma_F|_E = \sigma_E, \text{whenever } E \subseteq F\Big\},$$

where $\sigma|_E$ denotes the restriction of the map σ to E, we observe that it is a closed subgroup of the product $\prod$ when endowed with the subspace topology.

The inverse limit is thus compact by Tychonov's theorem and also totally disconnected. Indeed we find:

Theorem *The mapping*

$$\mathrm{Gal}(K/k) \;\to\; \varprojlim_{E} \mathrm{Gal}(E/k)$$

defined by

$$\sigma \mapsto (\dots, \sigma|_E, \dots),$$

is a topological isomorphism between the two groups.

(Cf. Appendix Section A.5.)

We next consider, from a modern point of view, two examples Dedekind investigated. The first example Dedekind investigates is $\mathrm{Gal}(\overline{\mathbb{Q}}/k)$ for any subfield k of $\overline{\mathbb{Q}}$, the algebraic closure of $\mathbb{Q}$ in $\mathbb{C}$, the field of complex numbers. $\mathrm{Gal}(\overline{\mathbb{Q}}/k)$ is the group of all automorphisms of $\overline{\mathbb{Q}}$ fixing k elementwise. By the surjectivity of the map in the previous theorem, any automorphism of a finite Galois extension E/k extends to an element of $\mathrm{Gal}(\overline{\mathbb{Q}}/k)$. More generally, if F/k is any finite extension, then any isomorphism of F into $\mathbb{C}$ fixing k extends to an element of $\mathrm{Gal}(\overline{\mathbb{Q}}/k)$, by first extending to the normal closure of F and then repeating the previous argument.

Dedekind establishes that $\mathrm{Gal}(\overline{\mathbb{Q}}/k)$ is a group and that any isomorphic embedding of k into $\mathbb{C}$ extends to at least one automorphism of $\mathrm{Gal}(\overline{\mathbb{Q}}/k)$, infinitely many when $[\overline{\mathbb{Q}} : k]$ is infinite. He also shows for this case that the mapping in the theorem [Galois Correspondence] above is indeed injective. Initially however, as evidenced in surviving manuscripts of the 1901 article, Dedekind also thought this mapping was surjective when all subgroups are considered. However, he discovered a counterexample by considering the sorts of infinite-degree cyclotomic fields to be described next.

The second example involves the infinite cyclotomic field $\mathbb{Q}(\zeta_{p^\infty}) = \bigcup_{n\in\mathbb{N}} \mathbb{Q}(\zeta_{p^n})$ where p is a prime and $\zeta_m = \cos(2\pi/m) + i\,\sin(2\pi/m)$ is a primitive m^{th} root of unity. If $\sigma \in \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$, then σ is uniquely determined by its action on all the ζ_{p^n}, for $n \in \mathbb{N}$. But $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \simeq (\mathbb{Z}/p^n\mathbb{Z})^\times$ where the automorphisms are given by $\zeta_{p^n} \mapsto \zeta_{p^n}^{c_n}$. Thus $\sigma\zeta_{p^n} = \zeta_{p^n}^{c_n}$ for some $c_n \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ and by compatibility $c_{n+1} \equiv c_n \pmod{p^n}$. By taking projective limits, this gives us the following chain of topological group isomorphisms:

$$\mathbb{Z}_p^\times \simeq \varprojlim_n (\mathbb{Z}/p^n\mathbb{Z})^\times \simeq \varprojlim_n \mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}).$$

(Cf. Appendix Section A.6.) Now the direct sum decomposition of $(\mathbb{Z}/p^nq\mathbb{Z})^\times$ for $n \geq 0$, namely

$$(\mathbb{Z}/p^nq\mathbb{Z})^\times \simeq (\mathbb{Z}/q\mathbb{Z})^\times \times (1+q\mathbb{Z})/(1+qp^n\mathbb{Z}),$$

where $q = p$ if p is odd and $q = 4$ if $p = 2$, induces, by taking projective limits, a topological group isomorphism

$$\mathbb{Z}_p^\times \simeq (\mathbb{Z}/q\mathbb{Z})^\times \times (1+q\mathbb{Z}_p).$$

The closed subgroups are readily determined to be

$$H_e \times G_m, \quad \text{for all } e|\varphi(q) \text{ and } m \in \mathbb{N}\cup\{0,\infty\},$$

where H_e is the subgroup of $(\mathbb{Z}/q\mathbb{Z})^\times$ of index e and $G_m = 1+qp^m\mathbb{Z}_p$, with $G_\infty = \{1\}$.

(Cf. Appendix Section A.7.)

On the other hand, we can also list all the subfields of $\mathbb{Q}(\zeta_{p^\infty})$. Namely, let $\mathbb{B}_{p^\infty q}$ be the fixed field of the subgroup $H_1 = (\mathbb{Z}/q\mathbb{Z})^\times$ in $\mathbb{Q}(\zeta_{p^\infty})$ and furthermore, let $\mathbb{B}_{p^m q} = \mathbb{B}_{p^\infty q} \cap \mathbb{Q}(\zeta_{p^m q})$. Notice, too, that $\mathbb{Q}(\zeta_{p^m q})$ is the fixed field of G_m for all m as above. Finally let $\mathbb{Q}_e$ be the (unique) field in $\mathbb{Q}(\zeta_q)$ of degree e over $\mathbb{Q}$. Then the composite fields

$$F = \mathbb{Q}_e \cdot \mathbb{B}_{p^m q}, \quad \text{for all } e|\varphi(q) \text{ and } m \in \mathbb{N} \cup \{0, \infty\},$$

exhaust all subfields of $\mathbb{Q}(\zeta_{p^\infty})$. Moreover the Galois correspondence is given by

$$F \mapsto \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/F) \simeq H_e \times G_m.$$

(Cf. Appendix Section A.8.)

As we will see, Dedekind determines this correspondence between the subfields of $\mathbb{Q}(\zeta_{p^\infty})$ and this family of subgroups, when p is odd. Since there are other subgroups of this infinite Galois group, the fundamental theorem in general fails to extend to the infinite case if all subgroups are considered, as Dedekind proves.

2.3 A Synopsis of Dedekind's Article

Dedekind's article, as it appears in his collected works, contains six sections and a short supplement based on material from his *Nachlaß*.

The first two sections offer a summary of finite degree algebraic field extensions and Galois theory of finite extensions. In the first Dedekind defines a field (which is always a subfield of $\mathbb{C}$), subfields, intersection and composite fields (although with different terminology), dependence and independence of finite sets of elements over a field, algebraic elements over a field, finite degree extensions. The section ends with the definition of an infinite degree extension of fields. No consideration of infinite cardinal numbers is given here. Hence infinite means not finite. The second is devoted to field isomorphisms, called "permutations" by Dedekind.[2] He considers restrictions and extensions of an isomorphism. The section ends with the isomorphism extension theorem for finite algebraic extensions: If K/k is a finite degree extension and φ an isomorphism on k, then there exists an extension of φ to K (in fact $[K : k]$ of them).

In the third section, Dedekind considers infinite degree algebraic extensions within $\mathbb{C}$. He asks if it is possible to extend the non-identity automorphism on $\mathbb{Q}(\sqrt{2}\,)$ to an isomorphism of $\mathbb{R}$ into $\mathbb{C}$. He then makes the conjecture that the only isomorphism of $\mathbb{R}$ into $\mathbb{C}$ is the identity map. This conjecture was shown to be false by A. Ostrowski, [10], whose work is based very closely on that of Steinitz, [13]. Had Dedekind considered only automorphisms on $\mathbb{R}$, however, his conjecture would have been correct. Dedekind then proceeds to show that any isomorphism on a subfield k of $\overline{\mathbb{Q}}$ extends to an isomorphism on $\overline{\mathbb{Q}}$, in fact infinitely many if $\overline{\mathbb{Q}}/k$ is of infinite degree. The proof uses an extension to $\overline{\mathbb{Q}}$ of Cantor's result that $\overline{\mathbb{Q}} \cap \mathbb{R}$ is countable. Let $\{a_n : n \in \mathbb{N}\} = \overline{\mathbb{Q}}$, where $n \mapsto a_n$ is a bijection from $\mathbb{N}$ to $\overline{\mathbb{Q}}$, and let k be a subfield of $\overline{\mathbb{Q}}$ with $[\overline{\mathbb{Q}} : k] = \infty$, (the case of finite degree is covered by the extension theorem in the previous section). Now suppose φ is an isomorphism on k (into $\mathbb{C}$). Let $n_1 = \min\{n : a_n \notin k\}$ and define $k_1 = k(a_{n_1})$. Continuing in the same way, Dedekind obtains a chain of fields $k_1 \subsetneq k_2 \subsetneq k_3 \subsetneq \ldots$, with $\cup k_n = \overline{\mathbb{Q}}$. Similarly, Dedekind extends φ one step at a time. He defines φ_1 on k_1 by requiring that $\varphi_1(a_{n_1}) = a_r$ where r is the minimal positive integer such that a_r is a root of the irreducible polynomial of a_{n_1} over k. Continuing, he obtains a chain of extensions $\varphi, \varphi_1, \varphi_2, \ldots$. Finally, he shows that $\cup\varphi_n$ is an isomorphism on $\overline{\mathbb{Q}}$.

[2] Dedekind's use of the term goes back at least as far as Lagrange, who considered permutations as arrangements of the roots of a polynomial. Cauchy (1815) defined a permutation as a correspondence of objects, emphasizing the operation rather than the actual arrangements of the objects. It was with Galois that permutations evolved essentially into field isomorphisms.

Section 4 generalizes the main results of § 3 to arbitrary extensions K/k with K a subfield of $\overline{\mathbb{Q}}$; namely, any isomorphism of k extends to one on K (infinitely many when $[K : k] = \infty$). This follows easily from § 3 by first extending to $\overline{\mathbb{Q}}$ and then restricting to K.

Section 5 finally introduces normal extensions and Galois groups. Dedekind states the main result of the Galois theory of finite extensions: Given a finite normal extension K/k, there is a one-to-one correspondence between the intermediate fields and the subgroups of the Galois group $G = \mathrm{Gal}(K/k)$ of the extension. The argument given uses the following theorem. If G is a finite subgroup of the group of automorphisms of a field K, then the fixed field, k, of G satisfies the equality $|G| = [K : k]$. Dedekind gives a proof of this result in [4]. Dedekind's proof anticipates the modern proofs of Artin, for example, in that Dedekind proves and then uses the independence of the elements of G over K. This is all done for a comparison with the infinite degree case handled in the last section.

In section 6, Dedekind starts by considering the group $G = \mathrm{Gal}(\overline{\mathbb{Q}}/k)$ for some subfield k in $\overline{\mathbb{Q}}$. He defines a mapping from the intermediate fields F and subgroups of G by the rule

$$F \mapsto \mathrm{Gal}(\overline{\mathbb{Q}}/F),$$

i.e., by mapping any intermediate field to its associated group. This gives, as Dedekind shows, an injection from the fields to the subgroups. He then mentions that he tried in vain to prove that any subgroup was the associated group for some intermediate field, until he came up with a counterexample. As he also observes, in any counterexample there would exist two distinct subgroups with the same fixed field.

To construct a counterexample, Dedekind considers the infinite cyclotomic extension $\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}$ for fixed odd prime p (this is not a major restriction, cf. Appendix A Section A.2), In effect, he shows that $G = \mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$ is isomorphic to $\mathbb{Z}_p^\times$. While Dedekind was constructing this counterexample, the p-adic numbers were being formalized by K. Hensel. Still, Dedekind gives an equivalent characterization of the p-adic units by, in essence, using the fact that they are characterized as an inverse limit of the groups $(\mathbb{Z}/p^n\mathbb{Z})^\times$. From this, Dedekind is able to determine the torsion subgroup of G. Since $\mathbb{Z}_p^\times \simeq (\mathbb{Z}/p\mathbb{Z})^\times \times (1 + p\mathbb{Z}_p) \simeq (\mathbb{Z}/p\mathbb{Z})^\times \times \mathbb{Z}_p$, the last component as a group under addition, which is torsion-free, we see (as Dedekind concludes) that the torsion group is of order $p - 1$. (Recall that p is assumed to be an odd prime.) On the other hand, he finds what in modern terms we would identify as a topological generator β of G. Then as Dedekind notices, the fixed field of G and $\langle\beta\rangle$, the cyclic subgroup generated by β is, in both cases, $\mathbb{Q}$.

But he then observes that $\langle\beta\rangle \neq G$.

Though today we would satisfactorily conclude the matter with the observation that $|\mathbb{Z}_p^\times| = |\mathbb{R}|$ whereas $|\langle\beta\rangle| = |\mathbb{N}|$, Dedekind argues without consideration of cardinality. Instead, he notes that the torsion subgroup of G has order $p - 1 > 1$, while the torsion subgroup of the infinite cyclic group $\langle\beta\rangle$ consists of the identity map only. This counterexample establishes that the fundamental theorem of finite Galois theory does not hold of necessity for infinite extensions.

Dedekind does not list all the intermediate fields and all corresponding fixed groups. He mentions in the article that he could but would not do so in the paper. This is the subject of the supplement. Dedekind also makes an imprecise remark after relating the automorphisms in $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$ to (in essence) $\mathbb{Z}_p^\times$. He says that $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$ forms, in a certain sense, a *continuous manifold*. He does not provide details to determine what he means.[3] Krull observes that this remark is a fundamental idea that he exploits in endowing general Galois groups with the appropriate topology, cf. [7].

[3] In *Stetigkeit und irrational Zahlen*, see [3], Vol. III, Dedekind observes that $\mathbb{R}$ is in essence a topological ring. Hence it is perhaps not too much of a stretch to suspect that he has an analogous topological group structure in mind here.

In the supplement added to the article when his collected works were published, Dedekind (or perhaps the editors) gives the list of all subfields and corresponding associated groups of the extension $\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q}$ (p again an odd prime). As we now know, these subgroups are precisely the closed subgroups of (via an isomorphism) $\mathbb{Z}_p^\times$. In retrospect these subgroups are apparent from the topological isomorphism of $\mathbb{Z}_p^\times$ and $(\mathbb{Z}/p\mathbb{Z})^\times \times (1 + p\mathbb{Z}_p)$. Closed subgroups are then of the form

$$H_e \times \langle 1 \rangle \quad \text{and} \ \ H_e \times (1 + p^m \mathbb{Z}_p),$$

where H_e is a subgroup of $(\mathbb{Z}/p\mathbb{Z})^\times$ of index e (so e is a divisor of $p-1$) and m is an positive integer. Subfields corresponding to these groups are then, respectively, the composites

$$\mathbb{Q}_e \cdot \mathbb{B}_{p^\infty} \quad \text{and} \ \ \mathbb{Q}_e \cdot \mathbb{B}_{p^m},$$

where $\mathbb{Q}_e$ is the unique subfield of $\mathbb{Q}(\zeta_p)$ of degree e over $\mathbb{Q}$, $\mathbb{B}_{p^\infty}$ is the fixed field of $(\mathbb{Z}/p\mathbb{Z})^\times$ in $\mathbb{Q}(\zeta_{p^\infty})$, and $\mathbb{B}_{p^m} = \mathbb{B}_{p^\infty} \cap \mathbb{Q}(\zeta_{p^m})$.

CHAPTER 3

TRANSLATION

[1]On the Permutations [2] of the Field of all Algebraic Numbers.

The purely algebraic presentation considered here has the goal of extending certain theorems on finite fields to infinite fields.[3] But in order to better appreciate the subject, it is necessary to recall the meaning of the expressions in the title of this paper, as well as some theorems related to them. One can find a detailed development of these concepts and the proofs in the fourth edition (1894) of Dirichlet's *Vorlesungen über Zahlentheorie* (Supplement XI), which I shall allude to by (D.) in the following.[4] Here, in the first two sections, I restrict myself to extracting from this work (with proofs omitted) only that which is indispensable for our purposes.

[1] Note that two types of footnotes appear in this translation: Numeric footnote by the translators (such as this footnote), and Dedekind's original footnotes, which are marked here by one or more asterisks followed by a right parenthesis, followed by a numeral.

[2] As we keep to Dedekind's terminology, a chart of Dedekind's terms and contemporary equivalences is given at the end of this translation. In particular, Dedekind's use of "permutation" corresponds to the contemporary notion of field isomorphism. An evolution of vocabulary of field and Galois theory seems to have occurred between 1900 and the 1920's, presumably with the rise of the abstract, structuralist approach to conceptualizing mathematics. E.g., Baer and Hasse's Appendix (1929) of their edited and expanded reprint of Steinitz (1910) explicitly defines an automorphism as an isomorphism mapping from a field to itself, and Artin's (1942) vocabulary agrees with contemporary usage.

[3] Here, for Dedekind, finite (infinite) fields mean finite- (infinite-) degree field extensions.

[4] Throughout our annotative footnotes we will not distinguish between "D." as Dirichlet or Dedekind, since Suppliment XI is the only portion of the *Vorlesungen* to which Dedekind refers, and Dedekind wrote the supplement.

§ 1.

Fields and Irreducible Systems.

A system[5] A of real or complex numbers is called a *field* (D. § 160), if the sums, differences, products, and quotients [6] of any two of these numbers belong to the same system A. The smallest field R consists of all rational numbers, the largest field Z of all complex numbers. A field A is called a *divisor* of a field B, and at the same time B is called a *multiple* of A, when every number contained in A also belongs to the field B.[7] The field R is a common divisor, the field Z a common multiple of all fields A. If B is a multiple of A and a divisor of C, then A is a divisor of C. Every given system of fields A, whether finite or infinite, has a uniquely determined[8] greatest common divisor D; this field consists of those numbers which are common to all these fields A, and every divisor common to all these fields A is a divisor of D. The same system of fields has a least common multiple M; this field M is the greatest common divisor of all those fields which (as, e.g., Z) are a common multiple of the fields A.[9]

A finite system T of m numbers $t_1, t_2, \ldots, t_m$ is called *reducible with respect to the field* A, if there exist m numbers $a_1, a_2, \ldots, a_m$ in A, not all vanishing, which satisfy the condition

$$a_1t_1 + a_2t_2 + \cdots + a_mt_m = 0.$$

In the contrary case the system T is called *irreducible over* A (D. § 164).[10]

[5] *Das System* is colloquial, much as *collection* in English, and is to be distinguished from *der Inbegriff*, which carries the sense of a totality of things, a collection of things *such that* ..., which we will understand and translate as a *set (of elements) such that*. Dedekind does not use Cantor's term, *die Menge* for *set*, although Dedekind had followed Cantor's development of *Mengenlehre* (set theory) well before the 1896 publication in *Mathematische Annalen* of Cantor's "Beiträge zur Begründung der transfiniten Mengenlehre."

[6] In D. § 160 it is explicitly noted that the denominator of a quotient cannot be 0.

[7] Dedekind uses "divisor" for subfield and "multiple" for extension field. Cf. the table on the last page of this chapter.

[8] *"...besitzt einen bestimmten..."*

[9] I.e., D is the intersection of the set of fields A; M, their composite.

[10] In D. § 164, these terms are introduced in the same order. The text goes on to say that "[a]ccording to whether the form or latter case occurs, we will also say that the m numbers ... are *dependent* on, or

A number t is called *algebraic with respect to the field* A, if there is a natural number n, for which the $n+1$ powers

$$1, t, t^2, \ldots, t^{n-1}, t^n$$

form a reducible system over A; the smallest number n, for which this occurs, is called *the degree of* t, and we say that t is an algebraic number of n^{th} degree with respect to A. Obviously such a number t is the root of an (irreducible) equation

$$t^n + a_1 t^{n-1} + \cdots + a_{n-1} t + a_n = 0,$$

whose coefficients $a_1, a_2, \ldots, a_n$ are numbers of the field A, whereas the n powers

$$1, t, t^2, \ldots, t^{n-1}$$

form an irreducible system over A. One can easily see (D. § 164, IX) that the set U of all numbers u of the form

$$u = x_1 t^{n-1} + x_2 t^{n-2} + \cdots + x_{n-1} t + x_n,$$

where $x_1, x_2, \ldots, x_{n-1}, x_n$ denote any arbitrarily chosen numbers in A, is again a field, and indeed is a multiple of A.[11] We denote this field U by $A(t)$, and we say that it is generated from A by adjoining t. Every $n+1$ numbers of this field $A(t)$ form a reducible system over A, whence every number u is algebraic with respect to A, and its degree is no larger than n.[12] If this degree $= n$, then $A(u)$ and $A(t)$ are identical.

independent of, each other (over A).” I.e., a reducible (resp. irreducible) set is linearly dependent (resp. independent) over A.

[11] So the set (*Inbegriff*) is closed under inversion; i.e., $A[t] = A(t)$.

[12] See D. §164, VII.

A field B is said to be *finite*[13] with respect to the field A and of degree n, if there is in B an irreducible system over A consisting of n numbers, while any $n+1$ numbers of the field B form a reducible system over A. We denote this degree n, which is always a natural number, by the symbol (B, A).[14] Then all the numbers in B are algebraic with respect to A, and among these there are also (infinitely many) numbers t, whose degree $= n$ (D. § 165, VI),[15] and the field $A(t)$ generated from A by adjoining t is the least

[13] It should be clear that Dedekind's use of "finite field" is not synonymous with the contemporary notions of "finite field" (Dedekind considers only subfields of $\mathbb{C}$), "finite degree extension field" (see footnote following), or even "finite dimensional vector space" (since, as fields, not all products of scalars in A and vectors in B are necessarily closed with respect to B).

[14] Notice here that A need not be a subfield of B. For example, by Dedekind's definition $(\mathbb{Q}(\sqrt{3}\,), \mathbb{Q}(\sqrt{2}\,)) = 2$.

[15] Perhaps Dedekind should have put this parenthesis at the end of the sentence, as D § 165, VI includes that $A(t) = M$ for each such t. It may be of interest here to note that Dedekind's proof relies on results in D § 161 obtained prior to the introduction of algebraic elements or vector spaces (in D § 163). In § 161, Dedekind shows that if $\Phi = \{\phi_i\}_{i=1}^{n}$ is a set of n distinct isomorphisms, each with domain A (a field), then there exists in A infinitely many numbers which are n-valued with respect to Φ. To explain: In full generality, Dedekind first considers a set Φ of n arbitrary field isomorphisms, restricts to their common domain A (a subfield of $\mathbb{C}$), then partitions the common domain, each partition containing elements whose orbit under Φ is a fixed cardinality. Accordingly, an element α of the common domain is said to be *one-valued*, *two-valued*, etc. with respect to Φ if the orbit of α consists of one, two, etc. elements (cf. § 2 below). As all fields under consideration are subfields of $\mathbb{C}$, certainly all elements of the prime subfield $\mathbb{Q}$ are one-valued for every possible Φ. To prove D § 161, Dedekind must exhibit at least one such n-valued number. The nontrivial part of the proof by induction considers the case when, for some $a \in A$, the images $a\phi_r = a_r$ are distinct for $r > 1$ but, without loss of generality, $a_1 = a_2$. In detail, as $\phi_1 \neq \phi_2$ one can find some $b \in A$ such that $b_1 \neq b_2$. Now for any $x \in \mathbb{Q}$ surely $y = ax + b \in A$ and so $y\phi_r = y_r = a_r x + b_r$, also $y_r - y_s = (a_r - a_s)x + (b_r - b_s)$, $(r, s \in \{1, 2, \ldots, n\}, r \neq s)$. In particular, for $r = 1$ and $s = 2$, since $a_1 = a_2$ and $b_1 \neq b_2$, one finds $y_1 - y_2 \neq 0$. For any other choice of r, s, $a_r \neq a_s$, so $y_r = y_s$ if and only if $\frac{b_s - b_r}{a_r - a_s} \in \mathbb{Q}$. Then choosing $x \in \mathbb{Q} - \{\frac{b_s - b_r}{a_r - a_s} | r \neq 1, s \neq 2\}$) ensures that y is n-valued with respect to Φ. Dedekind further notes here a connection with the Vandermonde determinant: As all $y_r - y_s$ with $r < s$ are surely non-zero, so is their product

$$\prod_{1 \leq r < s \leq n} (y_r - y_s) \quad = \quad \begin{vmatrix} y_1^{n-1} & y_1^{n-2} & \cdots & y_1 & 1 \\ y_2^{n-1} & y_2^{n-2} & \cdots & y_2 & 1 \\ . & . & . & . & . \\ y_n^{n-1} & y_n^{n-2} & \cdots & y_n & 1 \end{vmatrix}$$

non-zero. Now with respect to D § 165, VI, the proof proceeds by choosing arbitrary $\theta \in M = AB$ and considering the set T of periodic elements θ^r, $r \in \{0, 1, 2, \ldots, n-1\}$; or, more precisely, considering the determinant $(T) = \det(\theta^r \pi_s)$, $s \in \{1, 2, \ldots, n\}$, which he defined while proving D § 165, IV (that the necessary and sufficient condition for a set $T \subseteq M$ to be linearly independent over A and form a basis for M is for $(T) \neq 0$). The π_s are elements of Π, the set of all isomorphisms of M that restrict to the identity isomorphism on A. But now $(T) = \det(\theta^r \pi_s) = \det((\theta\pi_s)^r)$ is a Vandermonde determinant of the periodic elements, so $(T) = \prod_{1 \leq r < s \leq n} (\theta\pi_r - \theta\pi_s)$. Hence the set T is (by D § 161) independent over A if and only if θ is n-valued with respect to Π. Since B is a field of nth degree over A, every independent set of n numbers in B or M forms a basis for M over A (D § 164, VIII). Thereby every element of M is algebraic with respect to A and of degree at most n. Thus every n-valued number θ and no other is of degree n. But again, from § 161, since Ψ consists of n distinct isomorphisms of field B, there must common multiple M of the two fields A, B. Hence we have the statement

$$(B, A) = (M, A). \tag{3.1}$$

If B is itself a multiple of A, so $M = B$, then in this case B is called a *finite multiple* of A; if in addition the field C is a finite multiple of B, then C is also a finite multiple of A, and the following statement holds (D. § 164, X)

$$(C, A) = (C, B)(B, A). \tag{3.2}$$

exist infinitely many numbers θ that are n-valued in Ψ, hence (by extension) in Π. This proof yields a version of the Theorem of the Primitive Element for finite degree algebraic extensions. (Dedekind will immediately consider the question of the number of possible intermediate fields K given an algebraic extension field B of field A of degree $[B : A] = n$ and show there can be but finitely many intermediate fields distinct from A and B. Interestingly, Dedekind does so by noting how K is uniquely determined by some subgroup $\Pi^{'}$ of Π and the possible partitions of Π by cosets of subgroups is finite.)

It might also be noted in passing that Dedekind was well aware that should the field M be normal over A, with Π the automorphism group of M/A, the determinant (T), if non-zero, gives a cyclic presentation of the elements θ^r whose value can be expressed in terms of the elements and group characters of the π_s. Cf. [5]. Lang [8] notes that Dedekind "expressed the theorem [of the independence of group characters]" in the case when "K is a finite normal extension of a field k, and when the characters are distinct automorphisms $[\sigma_s]$... of K over k... [which he proved] by considering the determinant constructed from $\sigma_i\omega_j$ where ω_j is a suitable set of elements of K, and proving...this determinant is not 0." This is precisely the form of the determinant (T).

Tangentially, Lang describes Dedekind's proof in contrast to Artin's proof [1], indicating that the form of the theorem in [1] and "its particularly elegant proof are due to Artin." Lang's emphasis on his former teacher's elegance does not account for the degree to which Artin's elegance may have been achieved using the template Dedekind provides in Supplement XI. By contrast, Kiernan [6] notes that "much of [ARTIN's] work was prefigured in the presentations of DEDEKIND and WEBER" (144) and that Artin "took up the concept stated implicitly by GALOIS and announced, *unheard*, by DEDEKIND and WEBER...[namely, that the] theory is concerned with the relation between field extensions and their groups of automorphisms," (emphasis added) and that "Armed with DEDEKIND's view of a field extension as a vector space over the ground field...ARTIN *began* the discussion with the splitting field of the polynomial" (emphasis in original). Still, Kiernan does not seem to appreciate the apparent parallels between Artin and Dedekind's presentations (after making appropriate adjustments for the great conceptual developments in mathematics between the 1890s and the 1940s.) Not only are the large-scale outlines the same (introduction of fields, followed by vector spaces, followed by algebraic field extensions and iso/automorphsims on such), but the structure of at least five of Artin's key proofs parallel Dedekind's (Theorem 6 parallels § 165 X, Theorem 14 parallels § 166 I, Theorem 26 parallels § 165 VI, converse, Theorem 27 parallels § 165 VI). Even an unmotivated detail such as Artin's definition of a *fixed point* of a field (with respect to some set of isomorphisms) aligns with Dedekind's definition of a *one-valued number* (with respect to some set of isomorphisms). By attentively summarizing sections 160-166 of the Supplement, Dean [2] provides a substantial argument that Artin's version of the Fundamental Theorem of Galois Theory is in fact Dedekind's version, excepting the generalization to fields of arbitrary character. It appears however, at present, that the literature contains no detailed analysis of structural and conceptual similarities and differences between Dedekind's and Artin's presentations of Galois Theory by which to evaluate the validity of apparent parallels.

That D is a divisor of field M can be completely characterized by $(D, M) = 1$.

But if B is not finite with respect to A—so that there always exists in B, however large a natural number m as we choose, m numbers in B which form an irreducible system over A—then we shall set $(B, A) = \infty$.*)[16] Whereby we see that the two statements (3.1) and (3.2) hold in general, the latter of course subject again to the earlier assumption that B is a multiple of A and divisor of C.[17]

§ 2.

Permutations of a Field.

A function φ of a field A, by which every number a contained in A is mapped to a corresponding number $a\varphi$, is called a *permutation* of A, if the four laws

$$(u + v)\varphi = u\varphi + v\varphi, \qquad (u - v)\varphi = u\varphi - v\varphi,$$
$$(uv)\varphi = (u\varphi)(v\varphi), \qquad \left(\frac{u}{v}\right)\varphi = \frac{u\varphi}{v\varphi}$$

are obeyed, where u, v are arbitrary numbers in A (D. § 161); we also say that the permutation φ is defined on A and call for brevity the latter *the field of* φ, in order to emphasize the fact that the mapping φ may not be applied to any number not in A.[18] If furthermore T is a part of A, i.e., a system of numbers[19] t, which are all contained in A,[20] then we

[16] *) Compare the conclusion with D. § 164, where for this case $(B, A) = 0$ was given. This is less advantagous in the present work.

[17] Dedekind takes no account here of the cardinality of these sets, which provides another avenue to proving the failure of the Fundamental Theorem of Galois Theory in the case of an infinite degree Galois extension of $\mathbb{Q}$. Dedekind seems to maintain a conceptual distinction between an “infinite set” and an “infinite number.” Yet, insofar as Dedekind has the dimension of a vector space over a base field in mind, it is not clear why he would not have considered the degree of an extension in determining the equipollency of sets, in which case, a nonfinite degree extension would be subject to cardinality considerations.

[18] The difficulty of extensions is foreshadowed: How to enlarge the domain is nontrivial.

[19] *“...ein System von Zahlen...”*

[20] I.e., T is a subset of A.

denote by $T\varphi$ the set of all images[21] $t\varphi$ of these numbers t. The number $t\varphi$ is said to be *conjugate* to t.

From this definition it follows easily that the number system $A\varphi$ is again a *field*, and that every two distinct numbers of A map under φ to two distinct numbers in the *conjugate* field $A\varphi$.[22] For this reason, the permutation φ can be inverted, and if one denotes by φ^{-1} the mapping of the field $A\varphi$, by which every number $a\varphi$ contained in $A\varphi$ is mapped to a, then it is clear that the *inverse* φ^{-1} is a permutation of $A\varphi$, and that $(A\varphi)\varphi^{-1} = A$.

Every field A possesses at least one permutation, namely the so-called *identity* permutation, by which each of its numbers is mapped to itself; we shall denote it in what follows by A_0.[23] If φ is an arbitrary permutation on A, and r a rational number, which is therefore also contained in A, then it follows that $r\varphi = r$, whence the field R of rational numbers has only a single [permutation], the identity permutation R_0.

If the field A is a divisor of the field B, then for every permutation ψ of B, there is a corresponding permutation φ of A, which is defined by $a\varphi = a\psi$ for each number a of the field A; whence it follows at once that the field $A\varphi = A\psi$ is therefore a divisor of $B\psi$. This permutation φ is called the *divisor with respect to A of ψ*, and at the same time, ψ is called a *multiple of φ with respect to B* (D. § 163).[24] In the case that $A = B$, obviously $\varphi = \psi$; but if A is distinct from B, thus a so-called proper divisor of B, then φ is substantively different from ψ, since the domains of definition of the two permutations are distinct. The sole permutation R_0 of R, the field of rational numbers, is the common divisor of all field permutations, and every divisor of an identity permutation is likewise an identity permutation. If the permutation φ of the field A is

[21] *"...den Inbegriff aller Bilder..."*

[22] See D. §161, p. 458.

[23] It is curious that Dedekind uses this symbol, for all other maps are denoted by Greek letters; moreover, this symbol could be confused as representing a field, consistent with his notation later in this article. In (D.), the identity map is not assigned a particular symbol, though it is repeatedly represented by the generic symbol φ.

[24] Hence a divisor, resp. multiple is a restriction, resp. extension map.

a divisor of the permutation ψ, and further if the latter is a divisor of a permutation χ, then φ is the divisor of χ with respect to A.

From the infinite collection of theorems[25] related to these concepts, we wish to single out here only two which are particularly important; in order to be able to state them conveniently, we start with the following discussion (D. $\S$ 161). If $\mathfrak{P}$ is a (finite or infinite) system of permutations ψ of arbitrary fields B, then a number t contained in the greatest common divisor of these fields B is mapped by every permutation ψ to a corresponding number $t\psi$, and it is called *n-valued by* $\mathfrak{P}$, if n is the number of distinct values which appear among the numbers $t\psi$. Clearly every rational number is single valued by $\mathfrak{P}$. From this our first theorem, which is easily proved (D. $\S$ 163), is given as:

I. *If $\mathfrak{P}$ is a system of field permutations ψ, then the totality of all the numbers single valued by $\mathfrak{P}$ forms a field A; the permutations ψ all have one and the same divisor φ with respect to A, and every common divisor of all the permutations ψ is a divisor of this permutation φ.*

For brevity we call this field A, which is completely determined by the system $\mathfrak{P}$, the *field of* $\mathfrak{P}$, and its permutation φ will be called the greatest common divisor of the permutations ψ or in brief the *residue of* $\mathfrak{P}$. If the system $\mathfrak{P}$ consists of only a single permutation ψ, then clearly A is in the earlier sense the field of ψ, and $\varphi = \psi$.

Whereas the existence of divisors of a given field permutation is immediately seen, the reverse question is much deeper; it can be answered at least in part by the following second theorem (D. $\S$ 165, III):

II. *If the field B is a* finite *multiple of the field A,*[26] *and φ is a permutation of A, then the degree (B, A) is also the number of distinct permutations ψ of B, which are multiples of φ; moreover A is the field and φ the residue of the system $\mathfrak{P}$ of these permutations ψ.*

[25] *"...Menge von Sätzen..."*

[26] B/A is not necessarily normal.

The most well-known example of this theorem arises by considering the field Z of all complex numbers and the field X of all real numbers. Obviously, $Z = X(i)$, where i is a root of the quadratic equation $i^2 + 1 = 0$; the two numbers $1, i$ form an irreducible system over X, and every number in Z is uniquely representable in the form $x_1 + i\,x_2$, where x_1, x_2 are contained in X, and consequently $(Z, X) = 2$. Now if φ denotes the identity permutation of X, then there are actually two and only two distinct permutations ψ on Z, which are multiples of φ; one is the identity permutation of Z, while the other is defined by $(x_1 + i\,x_2)\psi = x_1 - i\,x_2$.

§ 3.

Permutations of the Field of all Algebraic Numbers.

The most recently emphasized Fundamental Theorem II assumes that the field B is a *finite* multiple of the field A; if we omit this assumption, then it seems to me that the answer to the question of whether every permutation φ of A has at least one multiple ψ with respect to B is of the greatest difficulty to determine. Let us consider, for example, the real quadratic field $A = R(\sqrt{2}\,)$, which is formed from the rational field R by adjoining $\sqrt{2}$. Then A has a permutation φ, which is not the identity permutation, by which $\sqrt{2}$ is mapped to $-\sqrt{2}$, and since A is a divisor of the field X of all real numbers, the following question thus arises: Does there exist a multiple of φ with respect to X? I do not know, but nevertheless I believe that the answer is “No”. The numbers in the real field X seem to me to be so intimately connected by continuity that I suspect that there cannot exist any permutation of X other than the identity. From this it would follow that the field Z possesses only the two permutations given at the end of § 2.[27] After several futile attempts to come up with a proof, I gave up this research; it would thus make me

[27] This conjecture turns out to be false, cf. Ostrowski [10]. However, if Dedekind had considered only automorphisms on $\mathbb{R}$, then he would have been correct in that the only automorphism on $\mathbb{R}$ is the identity map.

all the more happy, if another mathematician wanted to inform me of a definitive answer to this question.

But the same question can be completely answered if we confine ourselves to the discontinuous domain H of all algebraic numbers. By an algebraic number, we simply mean here any number t which is algebraic with respect to the rational field R, thus a root of an equation

$$t^n + a_1 t^{n-1} + a_2 t^{n-2} + \cdots + a_{n-1} t + a_n = 0$$

with rational coefficients $a_1, a_2, \ldots, a_n$. The set H of all these numbers t is a field, as is well known, and by an *algebraic field* we merely mean any divisor of H; clearly H is not a finite multiple of R, thus $(H, R) = \infty$. We mention further that every conjugate number $t\psi$ (§ 2) of an algebraic number t is likewise algebraic; for because the rational coefficients $a_1, a_2, \ldots, a_n$ are fixed by every permutation ψ, $t\psi$ must satisfy the same equation as the root t. From this we proceed to the proof of the following existence theorem:

III. *If φ is a permutation of an algebraic field A, then the field H of all algebraic numbers possesses at least one permutation ω which is a multiple of φ.*

If H is a finite multiple of A, then our theorem is an immediate consequence of the main theorem II mentioned above (in § 2);[28] hence we confine ourselves in the following to the contrary case that $(H, A) = \infty$, while (A, R) can be finite or infinite. The proof is then based principally on an important property of the field H, first emphasized by *G. Cantor**)[29], and which is that all the numbers of the field H can be ordered

[28] Dedekind in his handwritten manuscript explicitly gives $A = H \cap R$.

[29] *) *Über eine Eigenschaft des Inbegriffs aller reellen algebraischen Zahlen.* (Crelles Journal, Bd. 77). I had also discovered this result extended to the field H, but I had my doubts about its utility, until I thought better of it due to the beautiful proof of the existence of transcendental numbers, which Cantor introduced in § 2 of his paper.

in a simple infinite sequence

$$h_1, h_2, h_3, \ldots, h_r, h_{r+1}, \ldots \tag{h}$$

in such a way that every natural number r corresponds to a unique algebraic number h_r, and conversely that every algebraic number t corresponds to one (and only one) natural number r, for which $h_r = t$. Such an ordering (a mapping of the field H by the sequence of natural numbers r) can be accomplished in infinitely many different ways; for our proof we consider a fixed ordering (*h*), and we call the natural number r the *index* of the algebraic number h_r.

Now since we have assumed $(H, A) = \infty$, A is a proper divisor of H, i.e., there exist in H, thus in the sequence (*h*), numbers which are not contained in A; among all of these numbers there is a unique number $t = h_r$, which has the *smallest* index r, and we call this number r the *index of the field* A. If $r > 1$, then the $r - 1$ numbers $h_1, h_2, \ldots, h_{r-1}$ preceding the number t all lie in A. Now since the number t is algebraic with respect to A, the field

$$A_1 = A(t),$$

obtained by adjoining t to A (by § 1) is a finite multiple of A and also a divisor of H. For brevity we shall call this field A_1, which is uniquely determined by A and our ordering (*h*), the *succeeding* multiple of A. But the field H cannot be a finite multiple of A_1, for otherwise [by (3.2) in § 1] H would be a finite multiple of A, whence $(H, A_1) = \infty$. One can hence apply the same reasoning to A_1 as with A, and so by continuing in the same manner we obtain from A an infinite chain (*A*) of fields

$$A,\ A_1,\ A_2,\ \ldots, A_s,\ A_{s+1}, \ldots, \tag{A}$$

in which each successive term A_{s+1} is the succeeding multiple of the previous A_s, while at the same time they are all divisors of H. Furthermore, since the field $A_1 = A(t)$ contains the new number $t = h_r$ along with the numbers $h_1, h_2, \ldots, h_{r-1}$ which are already in A, the index of A_1 must be $\geq r+1$, and by repeating this argument, it follows that the field A_s surely contains all those numbers in the sequence (*h*) whose index is $< r+s$. Now since every algebraic number has a uniquely determined finite index, so that if one or more such [numbers] $u, v, \ldots$ be given, then we can always choose a natural number s sufficiently large, so that all these numbers are in the field A_s, and thence also contained in all the successive fields $A_{s+1}, A_{s+2}, \ldots$.

Now let us assume that φ is an arbitrary permutation of the field A. Since the number $t = h_r$ is not contained in A, and so the finite degree $(A_1, A) \geq 2$, there always exist, by Fundamental Theorem II (in § 2), [which is] valid for finite multiples, several distinct permutations ψ of the field $A_1 = A(t)$ which are multiples of φ, and every permutation ψ is completely determined by the conjugate number $t\psi$ to which t is mapped. For our proof it would be completely immaterial whichever of these (A_1, A) permutations ψ we wished to select; but in order to obtain a well-defined rule, we proceed as follows. Since the numbers $t\psi$ (as is mentioned above) are likewise algebraic, and are thus contained in the sequence (*h*) and moreover are all distinct, we therefore decree to choose that permutation ψ for which the index of $t\psi$ is as small as possible. This permutation of A_1, which is completely determined by φ and the ordering (*h*), we denote by φ_1 and call it the *succeeding multiple* of φ. Clearly one can now proceed with this permutation φ_1 of the field A_1, just as with the permutation φ of the field A, and by continuing in this way, we obtain from the given permutation φ an infinite chain

$$\varphi,\ \varphi_1,\ \varphi_2,\ \ldots, \varphi_s,\ \varphi_{s+1},\ \ldots, \qquad (\varphi)$$

in which the general φ_s is a permutation of A_s, and φ_{s+1} the succeeding multiple of φ_s.

Once the two chains (*A*) and (φ) of the fields A_s and their permutations φ_s have been formed, the proof of our theorem III proceeds very easily. We define a *mapping* ω on H in the following manner. If u is any algebraic number, then there exists, by an earlier observation, a field A_s in the chain (*A*), in which the number u is contained, and if n denotes the smallest number s for which this holds, then we decree that u under ω be the image

$$u\omega = u\varphi_n.$$

By this, the mapping ω on H is completely determined, and we now wish to prove that it is a *permutation of* H, and moreover a *multiple of* φ. First we observe that the number u of the field A_n is also in all the successive fields $A_{n+1}, A_{n+2}, \ldots$ of the chain (*A*), thence in general contained in A_s, when $s \geq n$, and since at the same time φ_s is a multiple of φ_n, it follows from the definition of ω that

$$u\omega = u\varphi_s.$$

If now v is likewise an algebraic number, then one can choose s so large that the two numbers u, v and consequently also their sum, difference, product, and quotient belong to the same field A_s; whence it follows, as just observed, that

$$\begin{aligned} u\omega &= u\varphi_s, & v\omega &= v\varphi_s, \\ (u+v)\omega &= (u+v)\varphi_s, & (u-v)\omega &= (u-v)\varphi_s, \\ (uv)\omega &= (uv)\varphi_s, & \left(\frac{u}{v}\right)\omega &= \left(\frac{u}{v}\right)\varphi_s. \end{aligned}$$

Now since φ_s is a permutation of the field A_s, and thus obeys the laws given in § 2, it follows immediately that the map ω of the field H obeys the same laws, therefore is a permutation of H. Furthermore if a denotes any number in the field A, then it follows from the definition of ω that $a\omega = a\varphi$, and therefore ω is a multiple of φ, q.e.d.

§ 4.

Generalization.

In the following observations we now wish to extend and generalize theorem III which was just proved; as always H denotes the field of all algebraic numbers. First one easily sees that the theorem remains valid if the field H is replaced by any algebraic field B which is a multiple of A. Namely, if φ is again a permutation of A, then as we now know, there exists at least one permutation ω of H which is a multiple of φ. Now if ψ denotes the divisor of ω with respect to B, then by an earlier observation (§ 2), φ is at the same time the divisor of ψ with respect to A. Thus we have the following theorem:

IV. *If the field A is a divisor of the algebraic field B, then every permutation of A has at least one multiple with respect to B.*

When B is a *finite* multiple of A, then this is clearly only a special case of theorem II (in § 2), which at the same time yields the stronger condition, that the degree (B, A) is the exact number of all the distinct permutations ψ. We can now also easily prove, in the contrary case when B is not a finite multiple of A, that the number of permutations ψ of B, which are multiples of the same permutation φ of A, is infinitely large, therefore again $= (B, A)$, if we retain the meaning of the symbols given at the end of § 1.[30] To this end, consider any field A', which (as, e.g., A itself) is a finite multiple of A and at the same time a divisor of B. Since every such field A' differs from B, and so is a proper divisor of B, there certainly exist in B numbers t which are not contained in A', and consequently there is a field $A'' = A'(t)$ obtained from A' by adjoining one such algebraic t. The field A'' is a finite multiple of A', thus also of A, and is again at the same time a divisor of B. Furthermore, since $(A'', A') \geq 2$, and so $(A'', A) = (A'', A')(A', A) \geq 2(A', A)$, it is clear that, if m denotes any arbitrarily large natural number, then among all the fields A' there is also such a one for which

[30] This extension is valid since Dedekind defines infinite as not finite. However, the result is false if we consider cardinalities. For example, $[\overline{\mathbb{Q}} : \mathbb{Q}] = |\mathbb{N}|$, whereas $|\operatorname{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})| = |\mathbb{R}|$.

$(A', A) \geq m$. By theorem II (in § 2) such a field A' certainly possesses at least m distinct permutations

$$\varphi_1', \varphi_2', \ldots, \varphi_m',$$

which are multiples of the given permutation φ of A, and since A' is a divisor of B, each of these m permutations φ' has by theorem IV at least one multiple ψ with respect to B; the resulting m permutations

$$\psi_1, \psi_2, \ldots, \psi_m$$

are consequently also multiples of φ, and they are all distinct, because each permutation ψ of B has just one, uniquely determined divisor φ' with respect to A'. Since m can be taken arbitrarily large, it follows that the number of all permutations ψ of B, which are multiples of the same permutation φ of A, is infinitely large, therefore $= (B, A)$, q.e.d.

Lastly, under the same assumption, we want to show that the last part of theorem II (in § 2) also remains valid. The system $\mathfrak{P}$ of all permutations ψ of B, which are multiples of the permutation φ of A, possesses (by theorem I in § 2) a greatest common divisor χ, and since φ is a divisor of all permutations ψ, and so a divisor of χ, it follows that the field C of this permutation χ is a multiple of A and at the same time a divisor of B. Now assume that C differs from A, and so $(C, A) \geq 2$, then C possesses, as was just proved, at least one permutation χ' *distinct* from χ and which is likewise a multiple of φ. Furthermore, since C is a divisor of B, it follows that B has at least one permutation ψ' which is a multiple of χ', and thus also a multiple of φ; consequently, it belongs to the system $\mathfrak{P}$. Whence χ, being a residue of $\mathfrak{P}$, must be a divisor of ψ', too. Therefore ψ' would possess two different divisors χ, χ' with respect to the same field C, which is impossible. Our assumption above, that the fields A, C are different, is thus not possible, and whence it clearly follows that $\chi = \varphi$. From this we can extend theorem IV above in the following way:

V. *If the field A is a divisor of the algebraic field B, and φ a permutation of A, then the degree (B, A), be it finite or infinite, is the number of all distinct permutations ψ of B which are multiples of φ; also, A is the field and φ the residue of the system $\mathfrak{P}$ of these permutations ψ.*

§ 5.

Groups of Permutations.

It follows immediately from the preceding that the field H of all algebraic numbers has infinitely many different permutations ω. Now since every number t contained in H is mapped by a permutation ω again to an algebraic number $t\omega$, it follows that the conjugate field $H\omega$ is clearly a divisor of H; but we can easily show that always $H\omega = H$. For consider again any equation with rational coefficients, which has as a root a given algebraic number t, and denote by $t_1, t_2, \ldots, t_m$ all the m distinct roots of this equation, which thus also belong to the field H. These numbers are mapped (as mentioned in § 2) by ω to as many likewise distinct numbers $t_1\omega, t_2\omega, \ldots, t_m\omega$; but since the latter satisfy the same equation, one of them must coincide with the given number t. Therefore, every number t of the field H also belongs to $H\omega$, from which the above claim that $H\omega = H$ clearly follows. We signify this property of the field H, by which all its permutations map it into[31] itself, by calling it a *normal field* (cf. D. § 166). An immediate consequence, or rather merely another formulation, of this property is that the inverse ω^{-1} of a permutation ω of H is also a permutation of H (§ 2).

Now it is time to recall a concept from the general theory of field permutations, namely their *composition* (D. § 162). For this we restrict ourselves for brevity to the following special case *).[32] Let M be an arbitrary field, and $\mathfrak{E}$ the set of permutations ε

[31] We would say *onto*, as normal should always be within an algebraic closure. Perhaps Dedekind is considering transcendental elements.

[32] *) By the way, I wish to observe here, that one can define in complete generality the composition $\varphi\psi$ when φ, ψ are permutations of two arbitrary fields A, B ; there exists a unique divisor A' of A which

of M, by which M is mapped into M, thus satisfying the condition $M\varepsilon = M$.[33] [34] There is always at least one such [permutation], namely the identity permutation M_0 of M, and every inverse ε^{-1} is likewise in $\mathfrak{E}$. Now every two (equal or distinct) such permutations φ, ψ generate a *resultant* $\varphi\psi$, which is defined for each number x contained in M by

$$x(\varphi\psi) = (x\varphi)\psi$$

and is likewise a permutation of M in $\mathfrak{E}$. From this the two statements

$$(\varphi\psi)^{-1} = \psi^{-1}\varphi^{-1}, \;\; (\varphi\psi)\chi = \varphi(\psi\chi)$$

follow, where χ is also any permutation in $\mathfrak{E}$, and the resultant $\varphi\varphi^{-1}$ is the identity permutation M_0. A system $\mathfrak{A}$ of permutations α contained in $\mathfrak{E}$ is called a *group*, if 1. the resultant of any two permutations α, and 2. all inverses α^{-1} belong to the same system $\mathfrak{A}$, and it is called finite or infinite according as the number of permutations α is finite or infinite; in the first case, one can easily conclude that the condition 2. is already a necessary consequence of condition 1. The set $\mathfrak{E}$ is itself a group, and also the identity permutation M_0 alone forms a group, which is contained in every group $\mathfrak{A}$. For finite groups the following fundamental theorem holds (D. § 166, I):

VI. *If a finite group $\mathfrak{A}$ consists of n permutations of the field M, and if A is the field of $\mathfrak{A}$,*[35] *then $(M, A) = n$, M a finite multiple of A, and the residue of $\mathfrak{A}$ is*

is mapped by φ to the greatest common divisor of $A\varphi$ and B, and the composition $\varphi\psi$ is defined as the permutation of A' given by $x(\varphi\psi) = (x\varphi)\psi$, where x is any arbitrary number in A'. The two statements $(\varphi\psi)^{-1} = \psi^{-1}\varphi^{-1}$, and $(\varphi\psi)\chi = \varphi(\psi\chi)$ remain valid, whereas other statements require certain modifications.

[33] I.e., an automorphism, but Dedekind does not conceptually isolate such permutations.

[34] Cf. footnote 28. To conclude that the mapping ε is surjective, Dedekind appears to assume that M is a subfield of $\overline{\mathbb{Q}}$. However, if M contains transcendental elements (over $\mathbb{Q}$), then the permutation may not be onto.

[35] Hence A is the fixed field of $\mathfrak{A}$.

the identity permutation A_0 of A. Moreover, it follows from theorem II (in $\S\,2$) that the group $\mathfrak{A}$ is also the collection of all multiples of A_0 with respect to M.[36]

One can convince oneself easily that theorem VI along with theorem II (in $\S\,2$) fully encompasses Galois theory. To go into this in more detail, we assume that the above group $\mathfrak{E}$ is finite,[37] from which it of course follows that all the groups $\mathfrak{A}$ contained in $\mathfrak{E}$ are also finite. Let E be the field of the group $\mathfrak{E}$, and E_0 its identity permutation, then by VI M is a finite multiple of E, the residue of $\mathfrak{E}$ is E_0, and conversely,[38] $\mathfrak{E}$ is the set of all multiples of E_0 with respect to M. The key result of Galois theory is that on one hand, the fields A which are divisors of M and at the same time multiples of E and, on the other hand, the groups $\mathfrak{A}$ contained in $\mathfrak{E}$, are in biunique correspondence.[39] *Firstly*, each such group $\mathfrak{A}$ possesses a particular field A, which consists of all the numbers in the field M which are single valued with respect to $\mathfrak{A}$,[40] thus is a divisor of M, and since each number in E, thus single valued with respect to $\mathfrak{E}$ and also with respect to $\mathfrak{A}$, so A is also a multiple of E. Furthermore, since by VI $\mathfrak{A}$ is the set of all the multiples of the identity permutation A_0 of A with respect to M, it follows that two distinct groups $\mathfrak{A}$ possess two distinct fields A, too. *Secondly*, we have hence only to show that conversely every field A which is a divisor of M and a multiple of E is also actually the field of a group $\mathfrak{A}$ contained in $\mathfrak{E}$. First, it follows from the statement $(M, E) = (M, A)(A, E)$ mentioned in $\S\,1$ that M is a finite multiple of A, whence by theorem II (in $\S\,2$) the degree (M, A) is also the number of all those permutations α of M which are multiples of the identity permutation A_0 of A, and moreover A is the field and A_0 the residue of the system $\mathfrak{A}$ of these permutations α. Thus we need only to prove that this system $\mathfrak{A}$ is a group contained in $\mathfrak{E}$. Since A is a multiple of E, so that E_0 is the divisor of

[36] The proof given in (D.) of this theorem anticipates the modern proofs of Artin [1]. As Dean [2] notes, for example, the independence of the automorphisms over M, whose proof can be found in (D. §161, last paragraph), is used.

[37] More precisely, the assumption here is that $\mathfrak{E}$ is a finite subgroup of the automorphism group of M.

[38] Unclear whether *umgekehrt* is meant here in a vernacular or logical sense; we chose the logical sense.

[39] *“...sich gegenseitig eindeutig entsprechen.”*

[40] The field A is thus the fixed field of $\mathfrak{A}$.

A_0 with respect to E, it follows that each permutation α is also a multiple of E_0 and consequently contained in the group $\mathfrak{E}$. Furthermore, for every number x of the field A, we have $x = x\,A_0 = x\alpha$, thus also $x\alpha^{-1} = x$, and if α_1, α_2 are two such permutations α, it then also follows that $x(\alpha_1\alpha_2) = (x\alpha_1)\alpha_2 = x\alpha_2 = x$, and therefore the resultant $\alpha_1\alpha_2$ belongs to the same system $\mathfrak{A}$, which is consequently a group, q.e.d.

From the correspondence between the fields A and the groups $\mathfrak{A}$ just proved, the other theorems of Galois theory, which involve relations between several such fields A and the corresponding groups $\mathfrak{A}$, follow immediately (D. § 166). We need not go into all of this, as it is sufficiently well known, and we needed the above only to call attention to the divergent behavior of *infinite* permutation groups.

§ 6.

Infinite Groups of Permutations.

We have seen that the field of all algebraic numbers H has infinitely many permutations ω, and that it [H] is mapped into itself by all of them; these permutations ω therefore form an *infinite group*, which we denote by $\mathfrak{G}$, and we ask whether here as well there is a one-to-one correspondence between the algebraic fields A (the divisors of H) and the groups $\mathfrak{A}$ contained in $\mathfrak{G}$.

If we start with an arbitrary algebraic field A, and denote by A_0 its identity permutation, then by the theorem V (in § 4), which completely replaces theorem II (in § 2), there always exist permutations α of the field H which are multiples of A_0; be the number (H, A) finite or infinite, it is always the case that A is the field and A_0 the residue of the system $\mathfrak{A}$ of these permutations α. Furthermore, since A_0 is the identity permutation, it follows easily (as at the end of § 5) that this system $\mathfrak{A}$ contained in $\mathfrak{G}$ is a group; we will call it the *identity group of the field A*.[41] Furthermore, as already

[41] The "identity group" of A is thus simply the subgroup of $\mathfrak{G}$ leaving A fixed element-wise.

observed, since A is the field of $\mathfrak{A}$, it follows that two distinct fields A have distinct identity groups $\mathfrak{A}$. The question raised above can therefore be answered affirmatively, if one could prove that every group $\mathfrak{A}$ contained in $\mathfrak{G}$ is the identity group of a field A, which is actually the case for finite groups $\mathfrak{A}$ by the theorem VI (in § 5). Now to be sure each *infinite group* $\mathfrak{A}$ has a certain[42] field A [namely, the field of $\mathfrak{A}$],[43] which being a divisor of H is thence algebraic, and since the identity permutation of H belongs to $\mathfrak{A}$, it follows that the residue of $\mathfrak{A}$ is surely the identity permutation A_0 of this field A, therefore $\mathfrak{A}$ contains only those permutations α of H which are also contained in the identity group $\mathfrak{A}'$ of A. But the proof is lacking that conversely every permutation α' in $\mathfrak{A}'$, i.e., every multiple of A_0 with respect to H, is also contained in the given group $\mathfrak{A}$; or in other words, that the fields of two different groups are distinct. At first I regarded this as most likely valid, and then after several futile attempts to prove it, I succeeded to convince myself of the fallacy of this supposition by an example which I now want to present to end this article.

This example is not related to the full field H, but rather to the simplest class of *infinite cyclotomic fields*. If p is a fixed prime number, then each natural number n corresponds to a root of unity

$$u_n = \cos\frac{2\pi}{p^n} + i\,\sin\frac{2\pi}{p^n}\,. \tag{1}$$

and we denote by P_n the cyclotomic field $R(u_n)$ generated by this [root], which is of degree $\varphi(p^n) = (p-1)p^{n-1}$, while P_0 is the field R of rational numbers. From

$$u_n = u_{n+1}^p, \tag{2}$$

[42] *"...bestimmten..."*

[43] I.e., "The field of $\mathfrak{A}$." We have $\mathfrak{A} \subseteq \mathrm{Aut}(H/H^{\mathfrak{A}}) = \mathfrak{A}'$ where $H \leftrightarrow (1)$ and $H^{\mathfrak{A}} \leftrightarrow \mathfrak{A}$.

it follows that in the infinite chain of fields

$$P_0,\; P_1,\; P_2,\; P_3, \ldots$$

every term P_n is a divisor of the immediately succeeding P_{n+1}, and thence also of every succeeding term P_{n+s}.

If any arbitrary chain of fields P_n is considered, which satisfy this last property, then their least common multiple M can contain no other numbers t than those which belong already to at least one field P_n and thus all succeeding fields P_{n+s}. For the set of all these numbers t surely form, as is easily seen, a field which obviously is a divisor of M, but is at the same time also a multiple of all P_n, therefore also a multiple of M, whence $= M$. One can therefore usefully denote this multiple by P_∞. If now ε is any permutation of M and ε_n the divisor of ε with respect to P_n, then there exists an infinite chain of permutations

$$\varepsilon_0,\; \varepsilon_1,\; \varepsilon_2,\; \varepsilon_3, \ldots,$$

in which each term ε_n is the divisor of all the succeeding terms ε_{n+s}. Conversely, if a particular chain of permutations ε_n of the fields P_n is given, which satisfies this last property, then it follows easily from the above mentioned constitution of the field M (as in § 3), that there is a unique permutation ε of M which is a multiple of all these permutations ε_n.

If we apply this to our case of cyclotomic fields $P_n = R(u_n)$, and denote by $\mathfrak{E}$ the set of all permutations ε of their smallest multiple $M = P_\infty$, then the divisor ε_n of ε with respect to P_n is completely determined by the conjugate number $u_n\varepsilon_n = u_n\varepsilon$ of u_n, and, as is well known, this is always a power of u_n the exponent of which is a number not divisible by p and which may be replaced by any number congruent to it modulo p^n.

Let us denote this number by (n, ε), and so it follows that

$$u_n \varepsilon_n = u_n \varepsilon = u_n^{(n,\varepsilon)}, \tag{3}$$

and since by (2) also

$$u_n \varepsilon = (u_{n+1} \varepsilon)^p,$$

hence

$$u_n^{(n,\varepsilon)} = u_{n+1}^{p(n+1,\varepsilon)} = u_n^{(n+1,\varepsilon)};$$

therefore

$$(n, \varepsilon) \equiv (n+1, \varepsilon) \pmod{p^n}, \tag{4}$$

and this congruence expresses that ε_n is a divisor of ε_{n+1}. Conversely, if a chain of such numbers (n, ε), which are not divisible by p, is given, which satisfies the conditions (4), then it follows from the general remarks above that it corresponds to a unique permutation ε of M, which is determined by (3). With this one may decree that (n, ε) should be positive and less than p^n, and if one sets $(n+1, \varepsilon) = (n, \varepsilon) + c_n p^n$, then $0 \leq c_n < p$; every arbitrarily chosen infinite sequence of such numbers $c_1, c_2, c_3, \ldots$ together with each of the $p-1$ numbers $(1, \varepsilon)$ produces a definite permutation ε, and whence it follows that the set $\mathfrak{E}$ of all ε form in a certain sense a *continuous* manifold, into which we shall not go any further.[44] [45]

As is well known, the field P_n is mapped into itself by every permutation, so hence $P_n \varepsilon = P_n \varepsilon_n = P_n$, and from this it also obviously follows that $M\varepsilon = M$; therefore the set $\mathfrak{E}$ forms a *group* (by § 5). If $\varepsilon, \varepsilon'$, thus also $\varepsilon\varepsilon'$, are contained in $\mathfrak{E}$, then

[44] Dedekind seems to be anticipating the development of topological groups here. This is not a new phenomenon for him. In his publication *Stetigkeit und irrationale Zahlen*, he observes that the operations on $\mathbb{R}$ "possess a certain continuity", cf. [3], Vol. III, page 331, the last two paragraphs. This is apparently the first ideas of a topological group or ring and is the germ of algebraic topology, cf. Dugac's article in [12], pp. 134-144.

[45] W. Krull [7] mentions that this remark is a fundamental idea which inspired him to endow a topology on automorphism groups.

it follows from (3) that

$$u_n(\varepsilon\varepsilon') = (u_n\varepsilon)\varepsilon' = (u_n\varepsilon')^{(n,\varepsilon)} = u_n^{(n,\varepsilon)(n,\varepsilon')},$$

therefore [also]

$$(n, \varepsilon\varepsilon') \equiv (n, \varepsilon)(n, \varepsilon') \pmod{p^n}, \tag{5}$$

and since the right side is not changed by switching $\varepsilon, \varepsilon'$, it follows that

$$\varepsilon\varepsilon' = \varepsilon'\varepsilon, \tag{6}$$

so therefore $\mathfrak{E}$ is an *abelian* group.

Every permutation ε generates by repeated composition with itself and its inverse ε^{-1} the sequence of all powers ε^r, which forms a group that we denote by $[\varepsilon]$.[46] Of some interest now is the question of whether there exist, aside from the identity permutation M_0 of M, which by itself forms a group, other finite permutations; i.e., [whether] there exist such permutations α which generate a finite group $[\alpha]$.[47] If m denotes the number of distinct permutations α^r in such a group $[\alpha]$, then $\alpha^m = M_0$ as is well known, and conversely, if a natural number m satisfies this condition, then it follows from this that α is finite. This requirement thus expresses by (3), (4), (5) that for every natural number n, α must satisfy the conditions

$$(n, \alpha)^m \equiv 1, \ (n, \alpha) \equiv (n+1, \alpha) \pmod{p^n}. \tag{7}$$

[46] Of course this is simply the cyclic group generated by ε.

[47] Hence of finite order.

If we disregard the case $p = 2$, then it follows by close examination, which presents no great difficulty, that there are only $p - 1$ finite permutations α; these are determined by

$$(n, \alpha) \equiv (1, \alpha)^{p^{n-1}} \pmod{p^n}, \tag{8}$$

and one obtains all of these, when one lets $(1, \alpha)$ run over an arbitrary complete system of incongruent numbers modulo p, which are not divisible by p; the corresponding numbers (n, α) form all $p - 1$ roots x_n of the congruence

$$x_n^{p-1} \equiv 1 \pmod{p^n}, \tag{9}$$

and from this it follows that these $p - 1$ permutations α satisfy the condition

$$\alpha^{p-1} = M_0. \tag{10}$$

They form a group $\mathfrak{A}$ and if one chooses for $(1, \alpha)$ a primitive root modulo p, then this group $\mathfrak{A} = [\alpha]$. Furthermore, if A denotes the field of $\mathfrak{A}$, then it follows from the theorem VI (in § 5), that $(M, A) = p - 1$, therefore M is a finite multiple of A *).[48]

Now it is also not hard to find all finite and infinite divisors of the field M and to determine the corresponding identity groups contained in $\mathfrak{E}$. For reasons of brevity, we do not carry this out,[49] and to conclude we wish merely to produce an example of the proof promised above, that not every group in $\mathfrak{E}$ is an identity group, or in other words, that two distinct groups can have the same field.

[48] *) In the case $p = 2$ omitted above, one easily finds that there are two finite permutations of M, namely the identity and one other, which is determined by mapping each root of unity u_n to u_n^{-1}.

[49] Determination of the divisors of M was included as an appendix to Dedekind's article in his collected works and is likewise included at the end this translation.

We denote by g a fixed choice of primitive root modulo all powers of the (odd) prime number p and define a permutation β of our field M by the congruence

$$(n, \beta) \equiv g \pmod{p^n},$$

for every natural number n, from which the existence condition (4) is satisfied. If again β_n denotes the corresponding divisor of β with respect to P_n, then

$$u_n \beta_n = u_n^g,\ u_n \beta_n^r = u_n^{g^r}$$

holds, and since the powers

$$g,\ g^2,\ g^3,\ \ldots, g^{\phi(p^n)}$$

form a complete system of incongruent numbers modulo p^n not divisible by p, the powers

$$\beta_n,\ \beta_n^2,\ \beta_n^3,\ \ldots, \beta_n^{\phi(p^n)}$$

exhaust all the permutations of the finite field P_n. Thus by a well-known theorem (or by II in § 2) each number t contained in P_n, which satisfies the condition $t\beta = t$, hence also the conditions $t\beta^r = t$, must be rational, and so must belong to the field R. Now we return to the permutation β of the field M, consider the group $\mathfrak{B} = [\beta]$ consisting of all powers of β, and look for its field, i.e., the set B of all numbers t of M single valued with respect to $\mathfrak{B}$.[50] This single-valuedness is completely determined by the requirement that $t\beta = t$, because thus from this $t\beta^{-1} = t$ and generally $t\beta^r = t$ follow. Now since, as noted earlier, every number t of the infinite field M surely also belongs to a finite P_n, whence $t\beta = t\beta_n$, so then must t also satisfy the condition $t\beta_n = t$ and consequently be rational; therefore $B = R$. But on the other hand, it is clear that the identity group of R, i.e., the set of all multiples of the identity permutation R_0 of M, is the full group $\mathfrak{E}$ of

[50] Hence B is simply the fixed field of $\mathfrak{B}$.

all permutations ε of M, and that R is the field of the group $\mathfrak{E}$, because every number single valued with respect to $\mathfrak{E}$ must be single valued with respect to $\mathfrak{B}$. Finally, that the group $\mathfrak{B}$ contained in $\mathfrak{E}$ is *distinct* from $\mathfrak{E}$ already follows from the fact that of the $p-1$ finite permutations α determined above, only a single one, namely the identity permutation M_0, is contained in $\mathfrak{B}$. Therefore, the two distinct groups $\mathfrak{B}$ and $\mathfrak{E}$ have the same field R, q.e.d.

Determination of the Divisors of M and their Identity Groups.

We now find all the divisors D of M. If D contains a number μ of exponent p^s (where $s \geq 1$) *),[51] then because D is a multiple of $R = A_s \cdot Q_e$ **),[52] [53] also a multiple of A_s. Thus if there exist numbers μ in D, whose exponent p^s exceeds every given value, then D is a common multiple of all A_s and consequently also an extension of A, whence

$$(M, A) = (M, D) \cdot (D, A) = p - 1$$

$$(D, A) = e,\ (M, D) = f;\ p - 1 = e \cdot f$$

and consequently (easy)

$$D = A \cdot Q_e\,.$$

In the contrary case, D is not a multiple of A; then there exists a number s such that A_s is a divisor of D, but A_{s+1} is not a divisor of D; whence the exponents of all the numbers contained in D are $\leq p^s$, i.e., D is a divisor of $P_s = A_s \cdot P_1$, and therefore D is a finite field,

$$D = A_s \cdot Q_e. \quad [\text{ In the case that } s = 0,\ D = R.\ ]$$

[51] *) Every number μ in M has a uniquely determined exponent p^s, i.e., it is contained in P_s, but not in P_{s-1}.

[52] **) If e is any divisor of $p - 1 = e \cdot f$, then denote by Q_e the field of degree e contained in P_1; hence all the finite fields which are contained in M are of the form

$$A_s \cdot Q_e \ \ [s = 1, 2, \ldots],$$

where A_s is the intersection of the fields A with P_s.

[53] The field A is the fixed field of the torsion subgroup $\mathfrak{A}$ of $\mathfrak{E}$ mentioned in § 6.

Identity Groups of the Subfields[54] of M.

field $M_{s,e} = A_s \cdot Q_e\,;\;\; p-1 = e \cdot f.$

identity group $\mathfrak{E}_{s,e}$: All permutations ε of M, which are multiples of the identity permutation of $A_s \cdot Q_e$.

$$u_n\varepsilon = u_n^{(n,\varepsilon)}\,;\;\; (n,\varepsilon) \equiv (1,\varepsilon)^{p^{n-1}} \pmod{p^n},$$ [55]

$$(s,\varepsilon)^f \equiv 1 \pmod{p^s}.$$

field $A \cdot Q_e\,;$ *identity group* $\mathfrak{E}_{\infty,e}$:

$$u_n\varepsilon = u_n^{(n,\varepsilon)}\,;\;\; (n,\varepsilon) \equiv (1,\varepsilon)^{p^{n-1}} \pmod{p^n},$$

$$(1,\varepsilon)^f \equiv 1 \pmod{p}.$$

[54] *sic*, as the original reads “Identitätsgruppen der Unterkörper von M”

[55] This misprint appears in the *Collected Works*. It should read simply $(n,\varepsilon) \equiv (n+1,\varepsilon) \mod p^n$.

German expression	**English translation**	**Modern terminology**
Permutation	permutation	(field) isomorphism
R	field of rational numbers	$\mathbb{Q}$
X	field of real numbers	$\mathbb{R}$
Z	field of complex numbers	$\mathbb{C}$
H	field of algebraic numbers	$\overline{\mathbb{Q}}$
Divisor	divisor	subfield
Multiplum	multiple	extension (field)
reducibel	reducible	independent
System	system	set
Inbegriff	set	set of elements such that . . .
endlich Körper	finite field	finite degree extension
(B, A)	degree of B w.r.t. A	$[AB : A]$
ein Teil on	a part of	a subset of
A_0	identity map on A	id_A or ι_A
Identitätsgruppe von A	identity group of A	associated group of A or group belonging to field A
u_n	primitive p^n-th root of unity	ζ_{p^n}
Resultante	resultant	composition (of mappings)

Table 3.1. German expressions and terms used by Dedekind

REFERENCES

[1] Artin, E. *Galois Theory*, 2nd ed., North State, Hammond, 1964.

[2] Dean, E. *Dedekind's treatment of Galois theory in the* Vorlesungen, Technical Report No. CMU-PHIL-184, Carnegie Mellon, Pittsburgh, 2009.

[3] Dedekind, R. *Gesammelte mathematische Werke*, I-III, Vieweg Verlag, Braunschweig, 1930-1933. Reprinted by Chelsea Publishing Co., New Year, 1969.

[4] Dirichlet, L., Dedekind, R. *Vorlesungen über Zahlentheorie*, 4th ed., Vieweg Verlag, Braunschweig, 1894. Reprinted by Chelsea Publishing Co., New Year, 1968.

[5] Hawkins, T. *The Origins of the Theory of Group Characters*, Arch. Hist. Exact Sciences **7**, No. 2 (1971), 142-170.

[6] Kiernan, B. M. *The Development of Galois Theory from Lagrange to Artin*, Arch. Hist. Exact Sciences **8**, (1971/72), 40-154.

[7] Krull, W. *Galoissche Theorie der unendlichen algebraischen Erweiterungen*, Mat. Ann. **100**, (1928), 687-698.

[8] Lang, S. *Algebra*, Revised 3rd ed., Springer, New York, 2002.

[9] Neukirch, J. *Algebraic Number Theory*, Springer Verlag, Berlin, 1999.

[10] Ostrowski, A. *Über einige Fragen der allgemeinen Körpertheorie*, Journ. f. Math. **143**, Heft 4, (1913), 255-284.

[11] Ramakrishnan, Dinakar, Valenza, Robert J. *Fourier Analysis on Number Fields*, Springer-Verlag, New York, 1999.

[12] Scharlau, W., *Richard Dedekind 1831-1981*, Vieweg Verlag, Braunschweig, 1981.

[13] Steinitz, E. *Algebraische Theorie der Körper*, Journ. f. Math. **137**, Heft 3, (1910), 167-309.

[14] Weber, H. *Lehrbuch der Algebra*, 2nd ed., vol. 1, (1898), Vieweg Verlag, Braunschweig.

APPENDIX

RELATED PROOFS

A.1 Introduction

In this appendix we provide proofs of properties and theorems mentioned in Chapter 2. As we aim to detail Dedekind's construction of the correspondence of the subfields of the Galois cyclotomic field $\Omega = \cup_{n=1}^{\infty}\mathbb{Q}(\zeta_{p^n})$ over $\mathbb{Q}$ and the closed subgroups of its associated Galois group $G = \mathrm{Gal}(\Omega/\mathbb{Q})$, we first characterize the *finite* cases $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n}/\mathbb{Q})$ from which the infinite case is constructed (Section A.2). From a modern perspective the relevant properties of the group G are best expressed with respect to a topology on G, so we next (Section A.3) study the Krull topology, which quite naturally yields (Section A.4) a revised form of the Fundamental Theorem of Galois Theory (applicable to finite and infinite degree Galois extensions alike), and with it, consideration of profinite groups. The relation of G as a profinite group to the finite groups $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})$ is then clarified using the notion of a projective limit (Section A.5). As G is topologically isomorphic to the multiplicative group $\mathbb{Z}_p^\times$ of p-adic units, we establish basic properties of the ring $\mathbb{Z}_p$ and its profinite topology (Section A.6). We then (Section A.7) characterize the *closed* subgroups of $\mathbb{Z}_p^\times$, which, by the Fundamental Theorem of Galois Theory, correspond one-to-one to the subfields of Ω. Finally, we put the pieces together (Section A.8), linking up the modern analysis with Dedekind's notation, nomenclature and description of the correspondence, as given in the Supplement (in [3]) to the article.

Note: *Sections A.3-A.5 of this Appendix provide detailed readings of aspects of Chapter 4 of Neukirch [9].*

A.2 The structure of $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})$ for p odd and even.

We recall the structure of $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})$ for prime p, odd and even. Setting $\zeta_{p^n}{=}e^{\frac{2\pi i}{p^n}}$ $(n \in \mathbb{N})$, note that $(\mathbb{Z}/p^n\mathbb{Z})^\times \simeq \mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})$, given by, e.g., $\overline{a} \mapsto \sigma_a$, where $\overline{a} = a + p^n\mathbb{Z}$ and $\sigma_a : \zeta_{p^n} \mapsto \zeta_{p^n}^a$. Clearly $|(\mathbb{Z}/p^n\mathbb{Z})^\times| = \phi(p^n)$.

Proposition A.1. *For p an odd prime, $(\mathbb{Z}/p^n\mathbb{Z})^\times \simeq \mathcal{C}_{p^{n-1}} \times \mathcal{C}_{p-1}$, where $\mathcal{C}_k$ denotes the cyclic group of order k.*

Proof. For p an odd prime, p^n is known to have a primitive root a, so immediately $(\mathbb{Z}/p^n\mathbb{Z})^\times =< \overline{a} > \simeq \mathcal{C}_{\phi(p^n)}$. But as $\phi(p^n) = p^{n-1}(p-1)$ with $p-1$ and p^{n-1} relatively prime, we have by either Sylow or consequences of the Fundamental Theorem of Finite Abelian Groups, $\mathcal{C}_{\phi(p^n)} \simeq \mathcal{C}_{p^{n-1}} \times \mathcal{C}_{p-1}$.[1]

Alternatively, we may determine an explicit isomorphism ψ between $(\mathbb{Z}/p^n\mathbb{Z})^\times$ and $\mathcal{C}_{p^{n-1}} \times \mathcal{C}_{p-1}$. First, taking primitive root a modulo p^n, note that

$$a = a^{p^{n-1}} \cdot \frac{a}{a^{p^{n-1}}} = a^{p^{n-1}} \cdot (a^{p^{n-1}-1})^{-1}$$

where clearly $a^{p^{n-1}}$ has order $p-1$ and so is a generator for $\mathcal{C}_{p-1}$. Also note that

$$(\overline{a}^{p^n-1})^{p^{n-1}} = \overline{a}^{p^{n-1}(p-1)(p^{n-1}+\cdots+1)} = (\overline{a}^{\phi(p^n)})^{(p^{n-1}+\cdots+1)} = 1,$$

which must be of order p^{n-1}, again as a is a primitive root modulo p^n. Hence $(a^{p^{n-1}-1})^{-1}$ is a generator for $\mathcal{C}_{p^{n-1}}$. Thus consider the natural map ψ given by the action $\overline{a} \mapsto (\overline{a}^{p^{n-1}}, (\overline{a}^{p^{n-1}-1})^{-1})$. That ψ is a surjective homomorphism is immediate from above. To show ψ injective, note that $\overline{a} \in \ker\psi$ implies $\overline{a}^{p^{n-1}} = \overline{a}^{p^{n-1}-1} = \overline{1}$. But $(p^{n-1}, p^{n-1}-1) = 1$ forces $\overline{a} = \overline{1}$. Hence ψ is an isomorphism such that, given generator $\overline{a}$ of $(\mathbb{Z}/p^n\mathbb{Z})^\times$, we find $\mathcal{C}_{p^{n-1}} =< \overline{a}^{p^{n-1}-1} >$ and $\mathcal{C}_{p-1} =< \overline{a}^{p^{n-1}} >$. □

[1] Or: Let $\mathcal{C}_{p^{n-1}} =< x >$, $\mathcal{C}_{p-1} =< y >$ for $x, y \in (\mathbb{Z}/p^n\mathbb{Z})^\times$. Then $(p^{n-1}, p-1) = 1$ implies $|xy| = lcm(p^{n-1}, p-1) = \phi(p^n)$. I.e., $< xy > = \mathcal{C}_{\phi(p^n)}$. The result now follows by order considerations and the definition of internal direct product.

We further note that a single generator may be used for $\mathcal{C}_{p^{n-1}}$ regardless of n, namely $\overline{p+1}$. For observing that $(1+p)^{p^k} = 1 + p^{k+1} + p^{k+2}\alpha$, where α denotes all outstanding terms, we see $(1+p)^{p^k} \equiv 1 + p^{k+1} \bmod p^{k+2}$ for each $k \in \mathbb{N}$. In particular, $(1+p)^{p^{n-1}} \equiv 1 + p^n \bmod p^{n+1}$, which is $\equiv 1 \bmod p^n$. Thus the order of $1+p$ divides p^{n-1}. However, $(1+p)^{p^{n-2}} \equiv 1 + p^{n-1} \bmod p^n$ and consequently $(1+p)^{p^k} \not\equiv 1 \bmod p^n$ for any degree $k < n-1$. I.e., we have the

Proposition A.2. *For* odd *prime p, $\zeta_{p^n} = e^{\frac{2\pi i}{p^n}}$ $(n \in \mathbb{N})$, and primitive root $\overline{a}$ modulo p,* $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}) \simeq \mathcal{C}_{p^{n-1}} \times \mathcal{C}_{p-1} \simeq < \overline{1+p} > \times < \overline{a} >$.

We immediately exhibit the Galois correspondence between subfields of Galois extension $\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}$ and subgroups of $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})$, taking advantage of the expression of the Galois group as a direct product of cyclic groups. Note the lattice substructure contributed by $\mathcal{C}_{p^{n-1}}$ is one-dimensional, being $1 \leq \mathcal{C}_p \leq \mathcal{C}_{p^2} \leq \cdots \mathcal{C}_{p^{n-2}} \leq \mathcal{C}_{p^{n-1}}$. However, the dimension of the substructure contributed by $\mathcal{C}_{p-1}$ will be determined by the number of distinct prime factors of $p-1$. For arbitrary factor (not necessarily prime) e of $p-1$, let H_e be the unique cyclic subgroup of $\mathcal{C}_{p-1}$ of index e, so that $H_e \simeq \mathcal{C}_{\frac{p-1}{e}}$. Similarly, for positive integer m where $0 \leq m \leq n-1$, let G_{p^m} be the unique cyclic subgroup of $\mathcal{C}_{p^{n-1}}$ of index p^m, so that $G_{p^m} \simeq \mathcal{C}_{p^{(n-1)-m}}$. The sublattice generated by H_e and G_{p^m} is given by Figure A.1 (following page), with parallel segments having the same index.

Formally, the corresponding subfield structure, setting $K = \mathbb{Q}(\zeta_{p^n})$ (over $\mathbb{Q}$) and denoting by K^S the fixed field of subgroup S of $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^n})/\mathbb{Q})$, is given by Figure A.2 (following page), with parallel segments having the same degree.

We recall that $K^{<1>} = K$, $K^{\mathcal{C}_{p^{n-1}}} = \mathbb{Q}(\zeta_p)$, $K^{\mathcal{C}_{p-1} \cdot \mathcal{C}_{p^{n-1}}} = \mathbb{Q}$, and $K^{H_e} = \mathbb{Q}(\sum_{\sigma \in H_e} \sigma(\zeta_p))$. As we will not be more deeply concerned with these results, we forgo further analysis.

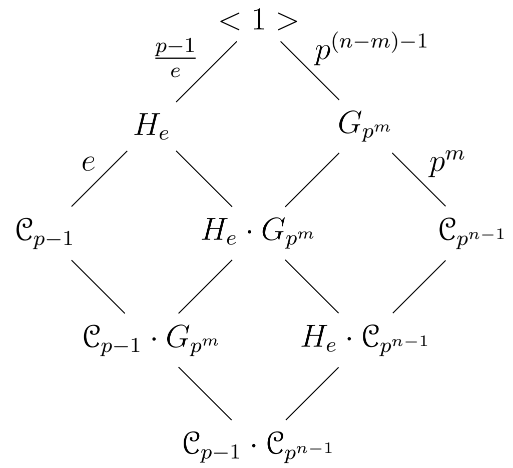


Figure A.1. Sublattice generated by H_e and G_{p^m}

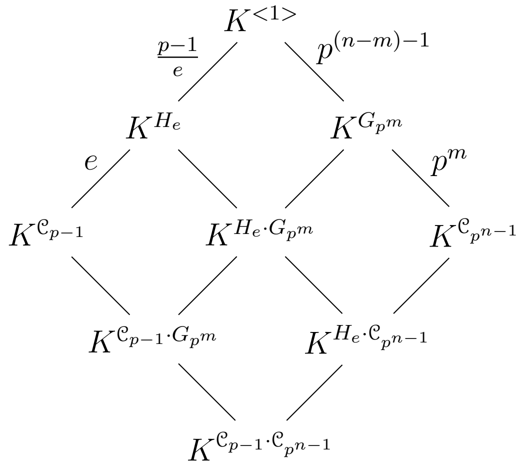

$K^{<1>}$
$\frac{p-1}{e}$
$p^{(n-m)-1}$
K^{H_e}
$K^{G_{p^m}}$
e
p^m
$K^{\mathcal{C}_{p-1}}$
$K^{H_e \cdot G_{p^m}}$
$K^{\mathcal{C}_{p^{n-1}}}$
$K^{\mathcal{C}_{p-1} \cdot G_{p^m}}$
$K^{H_e \cdot \mathcal{C}_{p^{n-1}}}$
$K^{\mathcal{C}_{p-1} \cdot \mathcal{C}_{p^{n-1}}}$

Figure A.2. Corresponding sublattice of $K = \mathbb{Q}(\zeta_{p^n})$ (over $\mathbb{Q}$)

However, we wish to sketch the corresponding case for the ordinary prime case excluded in the above discussion. Toward that end, as we have already seen that $\mathrm{Gal}(\mathbb{Q}(\zeta_{2^n}/\mathbb{Q}) \simeq (\mathbb{Z}/2^n\mathbb{Z})^\times$ we note that (taking cases $n = 1, 2$ as obvious)

Proposition A.3. *For $n \in \mathbb{N}$ with $n \geq 3$,* $(\mathbb{Z}/2^n\mathbb{Z})^\times = <\overline{-1}>\cdot<\overline{1+2^2}> \simeq \mathcal{C}_2 \times \mathcal{C}_{2^{n-2}}$.

Proof. Clearly we cannot proceed as in the odd prime case, as the order of $(\mathbb{Z}/2^n\mathbb{Z})^\times$ does not admit a relatively prime factorization by which we could apply the Sylow theorems. For $n = 3$, $(\mathbb{Z}/2^n\mathbb{Z})^\times$ is isomorphic to the (non-cyclic) Klein four-group, as no element has order greater than two.[2] Now observe, for $n \geq 3$, that $| < \overline{5} > | = 2^{n-2}$, since $(1+2^2)^{2^k} = \sum_j \binom{2^k}{j} 2^{2j} \equiv (1 + 2^{k+2}) \bmod 2^{k+3}$ for all k, by induction on k. Further, $-1 \not\in < \overline{5} >$ else $\overline{-1} = \overline{5^{\nu} 2^n}$ for some nonnegative integers ν, n, implying $-1 \equiv 5^{\nu} 2^n \equiv 1 \bmod 4$. The claim follows. □

Applying the proposition, we can immediately construct the subgroup lattice of $\mathrm{Gal}(\mathbb{Q}(\zeta_{2^n}/\mathbb{Q}))$ (see Figure A.3).

The corresponding formal lattice of subfields of $K = \mathbb{Q}(\zeta_{2^n})$ (over $\mathbb{Q}$) is given in Figure A.4, or, more substantively, in Figure A.5, where $H_1 = \mathbb{Q}(i(\zeta_8 + \zeta_8^{-1}))$, $H_2 = \mathbb{Q}(\zeta_8 + \zeta_8^{-1})$, $I = \mathbb{Q}(\zeta_{2^{n-3}} + \zeta_{2^{n-3}}^{-1})$, $J_1 = \mathbb{Q}(\zeta_{2^{n-2}}(\zeta_{2^{n-1}} + \zeta_{2^{n-1}}^{-1}))$, $J_2 = \mathbb{Q}(\zeta_{2^{n-1}} + \zeta_{2^{n-1}}^{-1})$, $K_1 = \mathbb{Q}(\zeta_{2^{n-1}}(\zeta_{2^n} + \zeta_{2^n}^{-1}))$ and $K_2 = \mathbb{Q}(\zeta_{2^n} + \zeta_{2^n}^{-1})$.

[2] This follows from the fact that 2^n has no primitive root, which is what this proof amounts to.

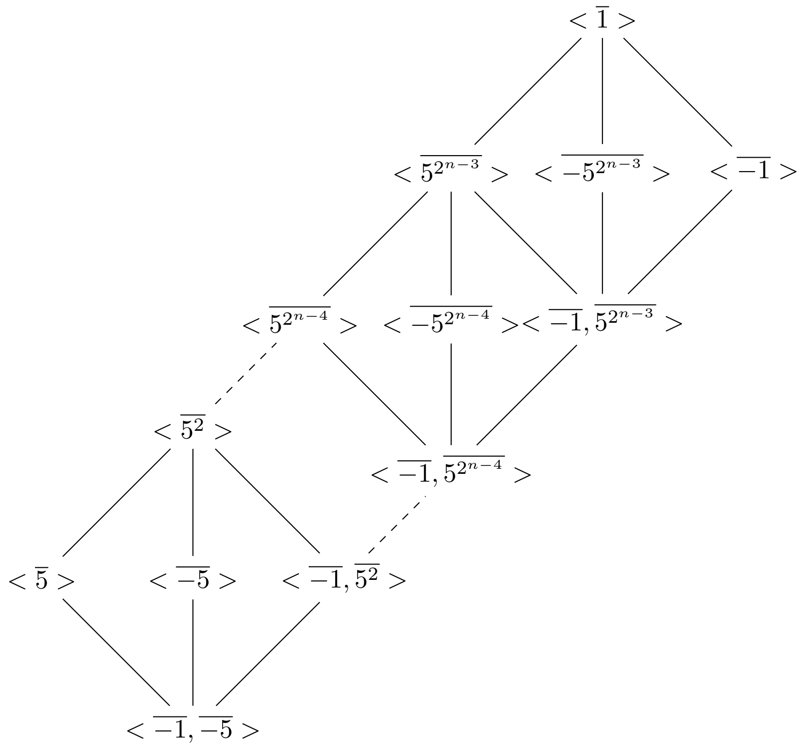

$<\overline{1}>$
$<\overline{5^{2^{n-3}}}>$
$<\overline{-5^{2^{n-3}}}>$
$<\overline{-1}>$
$<\overline{5^{2^{n-4}}}>$
$<\overline{-5^{2^{n-4}}}>$
$<\overline{-1},\overline{5^{2^{n-3}}}>$
$<\overline{5^2}>$
$<\overline{-1},\overline{5^{2^{n-4}}}>$
$<\overline{5}>$
$<\overline{-5}>$
$<\overline{-1},\overline{5^2}>$
$<\overline{-1},\overline{-5}>$

Figure A.3. Subgroup lattice of $\mathrm{Gal}(\mathbb{Q}(\zeta_{2^n}/\mathbb{Q}))$

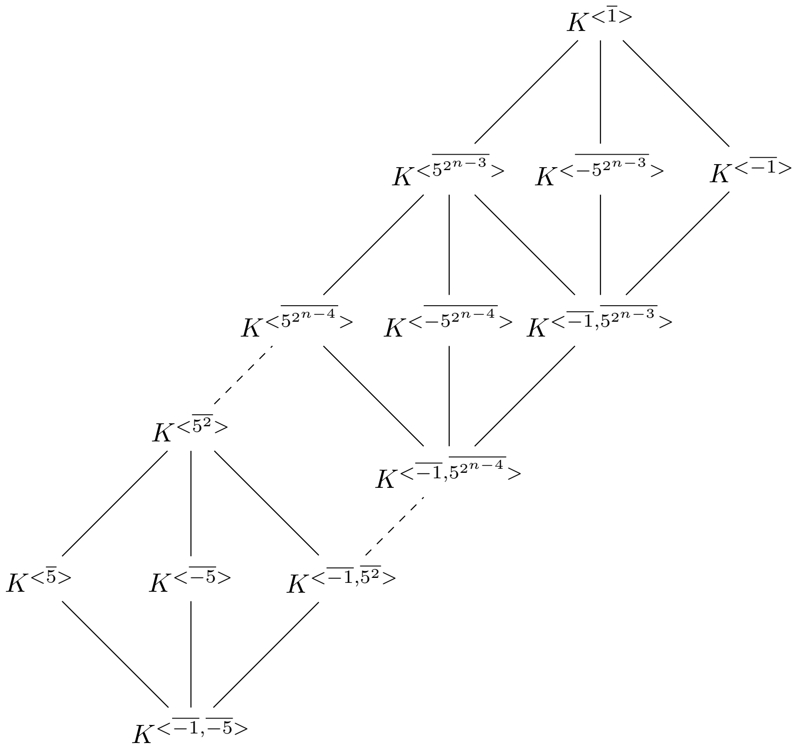

$K^{<\overline{1}>}$
$K^{<\overline{5^{2^{n-3}}}>}$
$K^{<\overline{-5^{2^{n-3}}}>}$
$K^{<\overline{-1}>}$
$K^{<\overline{5^{2^{n-4}}}>}$
$K^{<\overline{-5^{2^{n-4}}}>}$
$K^{<\overline{-1},\overline{5^{2^{n-3}}}>}$
$K^{<\overline{5^{2}}>}$
$K^{<\overline{-1},\overline{5^{2^{n-4}}}>}$
$K^{<\overline{5}>}$
$K^{<\overline{-5}>}$
$K^{<\overline{-1},\overline{5^{2}}>}$
$K^{<\overline{-1},\overline{-5}>}$

Figure A.4. Corresponding formal lattice of subfields of $K = \mathbb{Q}(\zeta_{2^n})$ (over $\mathbb{Q}$)

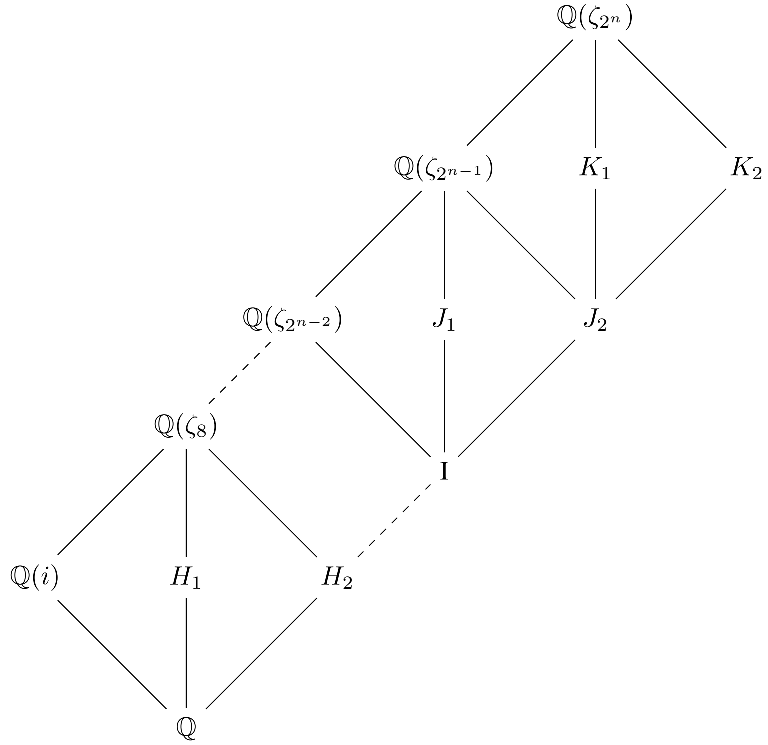

$\mathbb{Q}(\zeta_{2^n})$
$\mathbb{Q}(\zeta_{2^{n-1}})$
K_1
K_2
$\mathbb{Q}(\zeta_{2^{n-2}})$
J_1
J_2
$\mathbb{Q}(\zeta_8)$
I
$\mathbb{Q}(i)$
H_1
H_2
$\mathbb{Q}$

Figure A.5. Lattice of subfields of $K = \mathbb{Q}(\zeta_{2^n})$ (over $\mathbb{Q}$)

A.3 The Krull topology of a Galois extension

We define a topology (the *Krull topology*) on an arbitrary Galois extension with the aim of establishing a generalization of the Fundamental Theorem of Finite Galois Theory. Let k be a field and Ω/k a Galois extension of k. That is, for every $a \in \Omega$, a is algebraic over k, the minimum polynomial of a over k splits completely in Ω, and Ω is a separable extension. Set $G = \operatorname{Gal}(\Omega/k)$, the Galois group of Ω/k, and define the set $\mathcal{B} = \{\sigma \operatorname{Gal}(\Omega/K) : \sigma \in G, K \subseteq \Omega,\ K \text{ finite Galois over } k\}$.

Proposition A.4. *$\mathcal{B}$ is a basis for a unique topology on G.*

Proof. Recall that a basis $\mathcal{B}$ for a unique topology on non-empty set S is a subset of the power set of S satisfying the conditions: (1) $S = \cup_{B\in\mathcal{B}} B$; and, (2) For arbitrary $B, B^{'} \in \mathcal{B}$ and $\sigma \in B \cap B^{'}$, there exists $B^{''} \in \mathcal{B}$ such that $\sigma \in B^{''} \subseteq B \cap B^{'}$.

In this case, we find:

(1) Setting $K = k$ implies $G = \operatorname{Gal}(\Omega/k) \in \mathcal{B}$.

(2) Take $B = \tau \operatorname{Gal}(\Omega/K)$, $B^{'} = \tau^{'} \operatorname{Gal}(\Omega/K^{'})$ with $\tau, \tau^{'} \in G$ and K/k, $K^{'}/k$ finite Galois, and let $\sigma \in B \cap B^{'}$. Then, as cosets, note that

$$\begin{aligned} B \cap B^{'} &= \sigma \operatorname{Gal}(\Omega/K) \cap \sigma \operatorname{Gal}(\Omega/K^{'}) \\ &= \sigma(\operatorname{Gal}(\Omega/K) \cap \operatorname{Gal}(\Omega/K^{'})) \\ &= \sigma(\operatorname{Gal}(\Omega/KK^{'})) \\ &\in \mathcal{B}. \end{aligned}$$

□

We denote the resulting topological space simply by G where no confusion is likely to arise. Open subgroups of G have the form $\operatorname{Gal}(\Omega/K)$ where $K \subseteq \Omega$ and K has finite degree over k (cf. Prop. A.9). We observe several useful properties of the Krull topology.

Proposition A.5. *The open subgroups of G are also closed in the Krull topology.*[3]

Proof. Each open subgroup is the complement of the union of its open cosets. $\square$

Proposition A.6. *Let S be an arbitrary subgroup of G. Let Ω^S denote the fixed field of S. Then $\overline{S} = \mathrm{Gal}(\Omega/\Omega^S)$, where $\overline{S}$ denotes the topological closure of S in G.*

Proof. As by construction $S \subseteq \mathrm{Gal}(\Omega/\Omega^S)$, certainly $\overline{S} \subseteq \overline{\mathrm{Gal}(\Omega/\Omega^S)}$. We wish to show that $\mathrm{Gal}(\Omega/\Omega^S) = \overline{\mathrm{Gal}(\Omega/\Omega^S)}$. Toward that end, let us pick σ in the complement of $\mathrm{Gal}(\Omega/\Omega^S)$ arbitrarily. There must be some $x \in \Omega^S$ moved by σ. As Ω is Galois, it surely contains some finite Galois subextension K/k containing x. Then, for every $\tau \in \mathrm{Gal}(\Omega/K)$, we have $\tau(x) = x$ whereas $\sigma\tau(x) \neq x$. Suppose now there were some $\rho \in \mathrm{Gal}(\Omega/\Omega^S) \cap \sigma\,\mathrm{Gal}(\Omega/K)$. Then, for every $z \in \Omega^S \cap K$, $z = \rho(z) = \sigma\tau(z) = \sigma(z)$ for some $\tau \in \mathrm{Gal}(\Omega/K)$. In particular, this would hold for $z = x$, contradicting our assumption. Hence the sets are disjoint. As σ is arbitrary, every element of $G - \mathrm{Gal}(\Omega/\Omega^S)$ is contained in some (basic) open neighborhood disjoint from $\mathrm{Gal}(\Omega/\Omega^S)$, and so $\mathrm{Gal}(\Omega/\Omega^S)$ is closed. Thus $\overline{S} \subseteq \mathrm{Gal}(\Omega/\Omega^S)$.

For the reverse inclusion, recall that[4] $\overline{S} = \{\tau \in G | S \cap U \neq \emptyset$ for all open $U \ni \tau\}$ and let $\sigma \in \mathrm{Gal}(\Omega/\Omega^S)$. Clearly it will suffice to show that S has nonempty intersection with every basic open set containing σ. If $\tau \in S \cap \sigma\,\mathrm{Gal}(\Omega/K)$ with K/k arbitrary finite Galois, then by coset considerations $\sigma\,\mathrm{Gal}(\Omega/K) = \tau\,\mathrm{Gal}(\Omega/K)$. K/k finite Galois ensures that the compositum $\Omega^S K/\Omega^S$ is also finite Galois[5]. Since obviously $K \subseteq \Omega^S K$, it follows by inclusion reversal that $\mathrm{Gal}(\Omega/\Omega^S K) \subseteq$

[3] This proposition is true in any topological group.

[4] Since $\sigma \notin \overline{S}$ iff σ is in the open complement of $\overline{S}$, which implies the existence of some nonempty open set U with $U \cap S = \emptyset$; and, conversely, for $\sigma \in U$, U open with nonempty intersection with S, the complement of U is closed and contains S, hence also $\overline{S}$, and so $\sigma \notin \overline{S}$.

[5] Since $\Omega^S K$ contains K, the generators of K over k will suffice to prove Ω^S Galois, and clearly $[\Omega^S K : \Omega^S] \leq [K : k] < \infty$.

$\mathrm{Gal}(\Omega/K)$ or $\sigma\,\mathrm{Gal}(\Omega/\Omega^S K) \subseteq \sigma\,\mathrm{Gal}(\Omega/K)$, the latter being a basic open neighborhood of σ (in the relative topology induced on $\mathrm{Gal}(\Omega/\Omega^S)$). Hence it suffices to show $S \cap \ \sigma\,\mathrm{Gal}(\Omega/\Omega^S K) \neq \emptyset$ for arbitrary $\sigma \in \mathrm{Gal}(\Omega/\Omega^S)$ and arbitrary $k \subseteq K \subseteq \Omega$ (K/k finite Galois).

So now let K/k finite Galois be given and consider the canonical restriction homomorphism $\chi : S \to \mathrm{Gal}(\Omega^S K/\Omega^S)$ mapping $\tau \mapsto \tau|_{\Omega^S K}$. We claim χ is surjective. Clearly $\chi(S)$ is a subgroup of $\mathrm{Gal}(\Omega^S K/\Omega^S)$. Further, for any $\tau \in S$ and $x \in \Omega^S$, $\tau|_{\Omega^S K}(x) = x$ by definition, so $\Omega^{\chi(S)} \supseteq \Omega^S$. The reverse inclusion is given by definition. Hence $\Omega^{\chi(S)} = \Omega^S$. By the Fundamental Theorem of Finite Galois Theory, we thus have $\chi(S) = \mathrm{Gal}(\Omega^S K/\Omega^S)$. I.e., χ is surjective.

Hence given any $\sigma \in \mathrm{Gal}(\Omega/\Omega^S)$, there is a $\tau \in S$ such that $\tau|_{\Omega^S K} = \sigma|_{\Omega^S K}$ or $\tau\sigma^{-1}|_{\Omega^S K} = id|_{\Omega^S K} \in \mathrm{Gal}(\Omega/\Omega^S K)$, or $\tau \in \sigma\,\mathrm{Gal}(\Omega/\Omega^S K)$. Thus $S \cap \sigma\,\mathrm{Gal}(\Omega/\Omega^S K) \neq \emptyset$ for any $\sigma \in \mathrm{Gal}(\Omega/\Omega^S)$ and any K/k finite Galois. From this and the above considerations, $\mathrm{Gal}(\Omega/\Omega^S) \subseteq \overline{S}$ follows. □

We next observe that G, endowed with the topology $\mathcal{T}$ resulting from basis $\mathcal{B}$, is a topological group; i.e., the group and inversion operators are continuous (where, for the group operator, the topology is extended naturally to the Cartesian product $G \times G$).

Proposition A.7. *G is a topological group.*

Proof. It will suffice to prove the continuity of the group multiplication operator (Φ) on basis $\mathcal{B} \times \mathcal{B}$ of $G \times G$ and of the group inversion operator (Ψ) on basis $\mathcal{B}$.

(1) For Ψ: Though $\Psi^{-1}(\sigma\,\mathrm{Gal}(\Omega/K)) = \mathrm{Gal}(\Omega/K)\sigma^{-1}$, we have $\mathrm{Gal}(\Omega/K)\sigma^{-1} = \sigma^{-1}\,\mathrm{Gal}(\Omega/K) \in \mathcal{B}$ since $\mathrm{Gal}(\Omega/K) \lhd G$ (as K/k Galois).

(2) For Φ: Take arbitrary $(\sigma, \tau) \in \Phi^{-1}(\eta\,\mathrm{Gal}(\Omega/K))$. Note for $\sigma\phi \in \sigma\,\mathrm{Gal}(\Omega/K)$, $\tau\psi \in \tau\,\mathrm{Gal}(\Omega/K)$ we have simply $\Phi(\sigma\phi, \tau\psi) = \sigma\phi\tau\psi = \sigma\tau\tau^{-1}\phi\tau\psi = \sigma\tau(\tau^{-1}\phi\tau)\psi \in \sigma\tau\,\mathrm{Gal}(\Omega/K) = \eta\,\mathrm{Gal}(\Omega/K)$, again since $\mathrm{Gal}(\Omega/K) \lhd G$. Hence

$\Phi(\sigma\,\mathrm{Gal}(\Omega/K) \times \tau\,\mathrm{Gal}(\Omega/K)) \subseteq \eta\,\mathrm{Gal}(\Omega/K)$ for every pre-image (σ, τ) and so continuity follows. □

Proposition A.8. *G is a compact Hausdorff topological group.*

Proof. We will proceed first by way of two lemmas. Toward that end, consider the product topology on the Cartesian product of finite Galois extensions, $\mathcal{G} = \prod_{K/k \text{ finite}} \mathrm{Gal}(K/k)$, where each finite extension is endowed with the discrete topology. Clearly every projection map $\pi_{K_0} : \mathcal{G} \to \mathrm{Gal}(K_0/k)$, i.e., $(\sigma_K)_K \mapsto \sigma_{K_0}$, is continuous for each K_0 since $\pi_{K_0}^{-1}(\{\sigma_{K_0}\}) = \{\sigma_{K_0}\} \times \prod_{K \neq K_0} \mathrm{Gal}(K/k)$ is open in $\mathcal{G}$ by construction. Further, the set

$$\mathcal{S} = \{\{\sigma_{K_0}\} \times \prod_{K \neq K_0} \mathrm{Gal}(K/k) : K_0/k \text{ finite Galois}, \ \sigma_{K_0} \in \mathrm{Gal}(K_0/k)\}$$

is a subbasis for $\mathcal{G}$, i.e., a collection of subsets of $\mathcal{G}$ such that the union of its elements yields $\mathcal{G}$ (obviously $\mathcal{G} = \cup_{S \in \mathcal{S}} S$) and the collection of finite intersections of its elements forms a basis for $\mathcal{G}$ (obvious as well). Also note that subbasis elements are closed in $\mathcal{G}$ (components not consisting of the entire space are nevertheless closed since each component space is discrete).

Now to the first lemma:

Lemma A.1. *$\mathcal{G}$ is a compact, Hausdorff topological group.*

Proof. Compactness is clear by Tychonov. Hausdorff is trivial since two distinct elements are contained in open sets differing on some component. That $\mathcal{G}$ is a topological group is also trivial. □

For the second lemma, define[6]

$$\mathcal{P} = \{(\sigma_K)_K \in \mathcal{G} : \forall L \supseteq K, \ L, K \text{ finite Galois over } k, \ \sigma_L|_K = \sigma_K\}.$$

[6] Note $\mathcal{P}$ is $\varprojlim_{K} \mathrm{Gal}(K/k)$, the projective limit of the finite Galois groups over k. Cf. Section 4.5.

$\mathcal{P}$ is made into a group in the natural way, and into a topological space by endowing it with the relative topology of $\mathcal{G}$ (a subbasis consists of elements $P \cap S$, $P \in \mathcal{P}$, $S \in \mathcal{S}$).

Lemma A.2. *$\mathcal{P}$ is a compact, Hausdorff topological group.*

Proof. The latter two properties are inherited from $\mathcal{G}$. For compactness, it suffices to show that $\mathcal{P}$ is closed in $\mathcal{G}$. Toward that end, let $L^{'} \supseteq L$ be finite Galois extensions of k and define the set $M_{L'/L} = \{(\sigma_K)_K \in \mathcal{G} : \sigma_{L'}|_L = \sigma_L\}$. Immediately observe that $\mathcal{P} = \cap_{L'/L} M_{L'/L}$, so it suffices to show $M_{L'/L}$ is closed.

By the isomorphism extension theorem, $L^{'} \supseteq L$ ensures that elements of $\mathrm{Gal}(L^{'}/k)$ are extensions of elements of $\mathrm{Gal}(L/k)$. We find (cf. Figure A.6) that $\mathrm{Gal}(L^{'}/k) = \cup_{i=1}^{n} S_i$, where $S_i = \cup_{j=1}^{m}\{\sigma_{i,j}\}$ such that $\sigma_{i,j}|_L = \sigma_i$ and $m = [\mathrm{Gal}(L^{'}/k) : \mathrm{Gal}(L^{'}/L)]$.

$$\begin{tikzcd}
\Omega \arrow[d, dash] \\
L^{'} \arrow[d, dash, "m"'] \\
L \arrow[d, dash, "n"'] \\
k
\end{tikzcd}$$

Figure A.6. Intermediate field extension tower in Ω/k

Hence, setting $\mathcal{K} = \prod_{\substack{K \notin \{L, L'\} \\ \text{finite Galois} \\ \text{over } k}} \mathrm{Gal}(K/k)$, we find

$$M_{L'/L} = \bigcup_{i=1}^{n} \left(\{\sigma_j\} \times S_i \times \mathcal{K}\right) = \bigcup_{i=1}^{n} \bigcup_{j=1}^{m} \left(\{\sigma_j\} \times \{\sigma_{ij}\} \times \mathcal{K}\right),$$

the finite union of an intersection of subbasis elements, each of which is closed. I.e., $M_{L'/L}$ is a finite union of closed sets in $\mathcal{G}$, thus closed. $\square$

Finally, to conclude the proof of the proposition, consider the natural mapping $h : G \to \mathcal{P} \subseteq \mathcal{G}$ given by $\sigma \mapsto (\sigma|_K)_K$. As h is a restriction mapping, it is clearly a homomorphism. The kernel of h is trivial as $\sigma \in \ker h$ if and only if $\sigma|_K = id$ for every K, which is the case only if $\sigma = id \in G$. That h is onto is also immediate, since for arbitrary $(\sigma_K)_K \in \mathcal{P}$ we may define σ on Ω by $\sigma(a) = \sigma_K(a)$ for every $a \in K$. To show σ is well-defined, let $a \in L$ where L/k is also finite Galois and note $\sigma_K(a) = \sigma_K|_{K\cap L}(a) = \sigma_{K\cap L}(a) = \sigma_L|_{K\cap L}(a) = \sigma_L(a)$. It is also easy to see that $\sigma \in G$. Hence h is a group isomorphism.

Further, h is also readily seen to be a topological homeomorphism (i.e., a continuous mapping with continuous inverse, also a continuous and open map): Let K_0 be some fixed finite Galois extension over k. Set $\mathcal{K}^{'} = \prod_{K\neq K_0} \mathrm{Gal}(K/k)$ and notice that

$$h^{-1}\left(\left(\{\sigma_{K_0}\} \times \mathcal{K}^{'}\right) \cap \mathcal{P}\right) = \sigma \,\mathrm{Gal}(\Omega/K_0)$$

where $\sigma \in G$ is chosen (by an application of Zorn's lemma) such that $\sigma|_{K_0} = \sigma_{K_0}$.[7] Hence h is continuous, and trivially also an open mapping (i.e., a map sending open sets to open sets):

$$hh^{-1}((\{\sigma_{K_0}\} \times \mathcal{K}^{'}) \cap \mathcal{P}) = (\{\sigma_{K_0}\} \times \mathcal{K}^{'}) \cap \mathcal{P} = h(\sigma \,\mathrm{Gal}(\Omega/K_0)).$$

□

A.4 The Fundamental Theorem of Galois Theory and Profinite Groups

We may now prove the Fundamental Theorem of Galois Theory:

Proposition A.9. *Let Ω/k be a Galois extension of field k. Then the mapping Ψ given by $K \mapsto \mathrm{Gal}(\Omega/K)$ gives a bijection between intermediate fields $k \subseteq K \subseteq \Omega$ and closed subgroups of $G = \mathrm{Gal}(\Omega/k)$. Every open subgroup H of G has the form $\mathrm{Gal}(\Omega/K)$ for some finite degree extension K/k.*

[7] If $\varphi \in \mathrm{Gal}(\Omega/K_0)$, then $h(\sigma\varphi) = (\sigma\varphi|_K)_K = \sigma\varphi|_{K_0} \times (\sigma\varphi|_K)_{K\neq K_0} = \sigma|_{K_0} \times (\sigma\varphi|_K)_{K\neq K_0}$.

Proof. First recall that G endowed with the Krull topology is a topological group. To show $\mathrm{Gal}(\Omega/K)$ is closed[8] in G, assuming $G \neq \mathrm{Gal}(\Omega/K)$, arbitrarily choose $\sigma \notin \mathrm{Gal}(\Omega/K)$. Then there exists some element $a \in K$ such that $\sigma(a) \neq a$. Take the normal closure L_σ of $k(a)/k$, a finite Galois extension of k. Note that, for every $\tau \in \sigma\,\mathrm{Gal}(\Omega/L_\sigma)$, we have, for some $\varphi \in \mathrm{Gal}(\Omega/L_\sigma)$, $\tau = \sigma\varphi$ and so $\tau(a) = \sigma(\varphi(a)) = \sigma(a) \neq a$, whereas $\chi(a) = a$ for every $\chi \in \mathrm{Gal}(\Omega/K)$ and $a \in K$, and hence $\sigma\,\mathrm{Gal}(\Omega/L_\sigma) \cap \mathrm{Gal}(\Omega/K) = \emptyset$. As $\sigma \in G - \mathrm{Gal}(\Omega/K)$ is arbitrary, it follows, for some appropriate finite Galois extension L_σ/k in Ω chosen with respect to σ, that

$$\mathrm{Gal}(\Omega/K) \quad \bigcap \quad \left[\bigcup_{\sigma \in G - \mathrm{Gal}(\Omega/K)} (\sigma\,\mathrm{Gal}(\Omega/L_\sigma)) \right] = \emptyset$$

where

$$\bigcup_{\sigma \in G - \mathrm{Gal}(\Omega/K)} \sigma\,\mathrm{Gal}(\Omega/L_\sigma)$$

is open, as a union of basic open sets. And clearly this latter union is precisely $G - \mathrm{Gal}(\Omega/K)$. Hence $\mathrm{Gal}(\Omega/K)$ is closed in G.

That Ψ is injective is immediate: For let $\mathrm{Gal}(\Omega/K) = \mathrm{Gal}(\Omega/L)$ and suppose $K \neq L$. Without loss of generality, take $a \in L - K$. Then there exists $\sigma \in \mathrm{Gal}(\Omega/K)$ such that $\sigma(a) \neq a$, so $\sigma \notin \mathrm{Gal}(\Omega/L)$, contradiction.

That Ψ is surjective is not immediate: Let $H < G$ and $K = \Omega^H$. Clearly $H \subseteq \mathrm{Gal}(\Omega/K)$. Thence $\overline{H} \subseteq \overline{\mathrm{Gal}(\Omega/K)} = \mathrm{Gal}(\Omega/K)$ (cf. Proposition 4.6). For the reverse inclusion, let L/k be finite Galois, $\sigma \in \mathrm{Gal}(\Omega/K)$. Consider $\sigma\,\mathrm{Gal}(\Omega/L) \cap H$. We wish to show this intersection to be nonempty. Define a mapping $\Phi : \mathrm{Gal}(\Omega/K) \to \mathrm{Gal}(KL/K)$ given by $\eta \mapsto \eta|_{KL}$. Figure A.7 suggests the motivation for considering Φ, recalling that as L/k is finite Galois, so is KL/K: By construction $\Phi(H) < \mathrm{Gal}(KL/K)$. Note, as $K = \Omega^H$, $(KL)^{\Phi(H)} = K$. For suppose $a \in KL - K$: Then there exists $\sigma \in H$ such that $\sigma(a) \neq a$, so $\sigma|_{KL}(a) \neq a$, implying $\sigma|_K \notin \mathrm{Gal}(KL/K)$. But as

[8] This is obvious if K/k is finite by Prop. A.5.

$[KL : K] < \infty$, we have, by the Fundamental Theorem of Finite Galois Theory, $K = (KL)^{\mathrm{Gal}(KL/K)}$. Now $(KL)^{\Phi(H)} = (KL)^{\mathrm{Gal}(KL/K)}$, forcing $\Phi(H) = \mathrm{Gal}(KL/K)$. So $\sigma \in \mathrm{Gal}(\Omega/K)$ implies $\Phi(\sigma) = \sigma|_{KL}$ and, as $\sigma|_{KL} \in \Phi(H)$, there exists $\tau \in H$ such that $\tau|_{KL} = \sigma|_{KL}$. This is the same as saying there exists $\tau \in H$ such that $\tau|_{KL} = \sigma|_{KL}$, hence that $\tau \in H \cap \sigma\,\mathrm{Gal}(\Omega/KL)$ since, for every $\varphi \in \mathrm{Gal}(\Omega/KL)$, we have $\sigma\varphi|_{KL} = \sigma|_{KL}(1_G)$. But $H \cap \sigma\,\mathrm{Gal}(\Omega/KL) \subseteq H \cap \sigma\,\mathrm{Gal}(\Omega/L)$ since $KL \supseteq L$. Hence for every $\sigma \in \mathrm{Gal}(\Omega/K)$ we find $\sigma\,\mathrm{Gal}(\Omega/L) \cap H \neq \emptyset$.

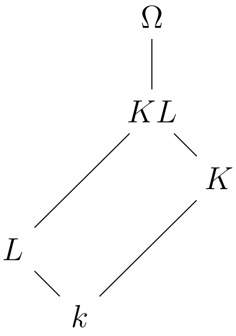


Figure A.7. Composite lattice over a Galois & an arbitrary extension of k

To show $H < G$ open, we can proceed in at least two ways:

(1) Note that $G = \underset{\sigma \in G/H}{\cup} \sigma H$ implies H also closed. Thus by above $H = \mathrm{Gal}(\Omega/K)$ for some K. Now as G is compact, the coset cover has a finite subcover. Hence $[G : H]$ is finite and immediately so is $[K : k]$.

(2) If K/k is finite (not necessarily normal), take L to be its normal closure in Ω. As L/k is finite Galois, $\mathrm{Gal}(\Omega/L)$ is a basic open set. Now merely observe that $\mathrm{Gal}(\Omega/K) = \underset{\sigma \in \mathrm{Gal}(\Omega/K)}{\cup} \sigma\,\mathrm{Gal}(\Omega/L)$, a union of basic open sets.

Thus the proposition follows. □

We define (with Neukirch [9]) a *profinite group* as a Hausdorff compact topological group with a basis of neighborhoods of the identity consisting of normal subgroups.

Proposition A.10. *For profinite group G the set $\mathcal{N} = \{N : N \lhd G,\ N \text{ open}\}$ is a basis of neighborhoods of 1_G.*

Proof. The proposition is nearly self-evident, as

(1) $1_G \in N$ $(\forall N \in \mathcal{N})$;

(2) $\forall M, N \in \mathcal{N},\ N \cap M \in \mathcal{N}$; and

(3) For every open subset U of G containing the identity, there exists an $N \in \mathcal{N}$ such that $N \subseteq U$. □

We note here a result perhaps useful in the following:

Proposition A.11. *A compact Hausdorff topological group is totally disconnected if and only if it admits a basis of neighborhoods of the identity consisting entirely of normal subgroups (i.e., if and only if it is profinite).*

Proof. First recall that a topological space X is called *disconnected* if there exist nonempty open sets U and V whose intersection is null and whose union is X, a space that is not disconnected is called *connected*, a maximal connected subset of a space is called a *component*, and a *totally disconnected* space is one in which only points (single-element subsets) are connected.

In the following, let G be a compact Hausdorff topological group.

For sufficiency, let $\mathcal{N} = \{N_i \lhd G : i \in I\}$ for I an index set denote a basis of neighborhoods of the identity 1_G of G and let $\mathcal{C}(1_G)$ denote the component of G containing 1_G. Suppose there exists $\sigma \in \mathcal{C}(1_G) - \{1_G\}$. As the space is Hausdorff, $\sigma \notin N_i$ for some $N_i \in \mathcal{N}$. Since N_i is open implies N_i closed, both N_i and its complement $G - N_i$ are open in G. Hence we have $\mathcal{C}(1_G) = (\mathcal{C}(1_G) \cap N_i) \cup (\mathcal{C}(1_G) \cap (G - N_i))$, a disjoint union of nonempty open sets. But this implies $\mathcal{C}(1_G)$ is disconnected; a contradiction. Therefore $\mathcal{C}(1_G) = \{1_G\}$. Since multiplication by a fixed element of the group is a homeomorphism on G and $\sigma(\mathcal{C}(1_G)) = \{\sigma\}$ for every $\sigma \in G$, sufficiency follows.

For necessity, suppose G is totally disconnected. To show that G is a profinite group, let $\mathcal{N}$ be the set of open normal subgroups of G. To show that $\mathcal{N}$ is a basis of neighborhoods of 1_G, we note first that $1_G \in N$ for every $N \in \mathcal{N}$. Secondly, certainly $N_1, N_2 \in \mathcal{N}$ implies $N_1 \cap N_2 \lhd G$.

Lastly, we need to show that for every open set U in G such that $1_G \in U$, there exists some $N \in \mathcal{N}$ such that $N \subseteq U$. To show this, following [11], we first show (Lemma A.3) that every open set U containing the identity contains some open compact subset K containing the identity. This result relies on a technical result about compact Hausdorff spaces that we relegate to a footnote for the sake of continuity of exposition. We then proceed by two additional lemmas (A.4, A.5) to show that any such open compact subset K must itself contain some element N of $\mathcal{N}$.

Lemma A.3. *Let U be an arbitrary open neighborhood of the identity in G (as given above). There exists a compact open subset K of G containing the identity and contained in U.*

Proof. Let $\mathcal{K}_1$ denote the collection of compact open subsets of G containing the identity 1_G. Certainly the set is nonempty as G itself is a compact open subset containing 1_G. Note that the set $\cap_{K \in \mathcal{K}_1} K$ is connected in G.[9] But as G is a totally disconnected space

[9] Again, following [11], we show a more general result: *Let X be a compact Hausdorff space and let $x \in X$. Define collection $\mathcal{K}_x = \{K : K \text{is a compact open subset of} X \text{containing} x\}$. The set $Y = \cap_{K \in \mathcal{K}_x} K$ is connected in X.* We first note that $\mathcal{K}_x$ is nonempty as X is an element of the set. The proof proceeds by contradiction: Suppose Y is a disconnected set in X. Then, for some disjoint relatively closed sets Y_1 and Y_2 in Y we have $Y = Y_1 \cup Y_2$. But then, as Y is itself a closed set (as an intersection of closed sets), Y is compact, and hence each of Y_1 and Y_2 is compact in Y. However, a relatively compact subset in a subspace of a compact Hausdorff space S is itself a compact subset of S. Hence Y_1 and Y_2 are compact in X and thus closed. So we take $Y = Y_1 \cup Y_2$ for disjoint closed sets Y_1 and Y_2 in X. Next, as a compact Hausdorff space is normal, there exist disjoint open sets U_1 containing Y_1 and U_2 containing Y_2. So now $Y \subseteq U_1 \cup U_2$ and $X - (U_1 \cup U_2) \subseteq X - Y = Y^c$. Set $Z = X - (U_1 \cup U_2)$. Trivially the set $\mathcal{K}_x$ covers Y, so the set $\mathcal{K}_x^c$ of complements in X of $K \in \mathcal{K}_x$ surely covers Y^c and so also Z, which is a closed subset of X, hence compact (as X is compact Hausdorff). Now $Y^c = (\cap_K K)^c = \cup_K K^c \supseteq Z$, so the collection $\mathcal{K}_x^c$ is an open cover of Z (since each K, as a compact set in a Hausdorff space, must be closed). Hence $\mathcal{K}_x^c$ contains a finite subcover of Z, say $\{K_i^c\}_{i=1}^r$. Then $Z \cap (\cap_{i=1}^r K_i) = \emptyset$. Set $W = \cap_{i=1}^r K_i$. W is an open compact neighborhood of x. So $W \in \mathcal{K}_x$. As $Z \cap W = [X - (U_1 \cup U_2)] \cap W = \emptyset$, we have $W \subseteq U_1 \cup U_2$. So we may write $W = (W \cap U_1) \cup (W \cap U_2)$, where the union is disjoint. Now $x \in W$ implies either $x \in (W \cap U_1)$ or $x \in (W \cap U_2)$, say the former without loss of generality. Clearly $W \cap U_i$ ($i = 1, 2$) is open in X. Each is also compact, as any open cover $\mathcal{C}$ of e.g. $W \cap U_1$ can be extended to an open cover $\mathcal{C}^{'}$ of W by taking $\mathcal{C}^{'} = \mathcal{C} \cup \{\{W \cap U_2\}\}$, which admits a finite subcover, some elements of which must be distinct from $W \cap U_2$ and thus form a finite subcover of $\mathcal{C}$. Hence $W \cap U_1$ is in $\mathcal{K}_x$ and so $Y \subseteq W \cap U_1$. Now $W \cap U_1 \subseteq Y_1$ implies $Y \subseteq Y_1$. But $Y = Y_1 \cup Y_2 \subseteq U_1 \cup U_2$ (each union disjoint) and $Y \cap U_2 = \emptyset$ imply $Y_2 = \emptyset$, contradicting our supposition. Therefore, Y is connected in X.

and $1_G \in \cap_{K \in \mathcal{K}_1} K$, we must have $\cap_{K \in \mathcal{K}_1} K = \{1_G\}$. Now let U be an arbitrary open neighborhood of the identity in G. Then $G - U$ is a closed, hence compact, subset of G. The set $\mathcal{K}_1^c$ of complements in G of $K \in \mathcal{K}_1$ covers $G - \{1_G\}$, and since $G - U \subseteq G - \{1_G\}$, the collection $\mathcal{K}_1^c$ covers $G - U$. But since every compact subset of a Hausdorff space is closed, every element of $\mathcal{K}_1$ is closed. Hence $\mathcal{K}_1^c$ is an open cover of compact set $G - U$ and so admits of a finite subcover, say $\{K_i^c\}_{i=1}^r$.

Next, as $G - U \subseteq \cup_i K_i^c$, we find $\cap_i K_i \subseteq U$. Set $K = \cap_i K_i$. As each K_i is open and contains 1_G, the finite intersection K is open and contains 1_G. Also, as each K_i is a closed set (hence compact), K is closed, hence compact. Thus K is a compact open set containing 1_G and contained in U. □

Lemma A.4. *Let K be a compact open subset containing 1_G of the topological group G. There exists a subset V containing 1_G that is open, symmetric, and such that $KV \subseteq K$.*

Proof. Consider the map $\varphi : K \times K \to G$ given by $(\eta, \lambda) \mapsto \eta\lambda$. For open U in G, preimage $\varphi^{-1}(U) = \mu^{-1}(U) \cap (K \times K)$ where μ is the (continuous) group operation for G. As K is open in G, $K \times K$ is open in $G \times G$ and so φ is continuous. In particular, $\varphi^{-1}(K)$ is open in $K \times K$. As $(\kappa, 1_G) \in \varphi^{-1}(K)$ for every $\kappa \in K$, there exist sets U_κ, $\tilde{V}_\kappa$ open in G, contained in K, such that $\kappa \in U_\kappa, 1_G \in \tilde{V}_\kappa$. Let $V_\kappa = \tilde{V}_\kappa \cap \tilde{V}_\kappa^{-1} \subseteq K$. Clearly $1_G \in V_\kappa$. Further, $(\kappa, 1_G) \in U_\kappa \times V_\kappa \subseteq \varphi^{-1}(K)$ implies $\kappa \in U_\kappa V_\kappa \subseteq K$. As $K = \underset{\kappa \in K}{\cup} U_\kappa$, compactness implies $K = \cup_{i=1}^n U_{\kappa_i}$ for some $n \in \mathbb{N}$. Set $V = \cap_{i=1}^n V_{\kappa_i}$, where V_{κ_i} corresponds as given above to the U_{κ_i}. Then note that $V \ni 1_G$, is open and symmetric. Finally, since $U_{\kappa_i} V \subseteq U_{\kappa_i} V_{\kappa_i} \subseteq K$, we have $KV = \cup_{i=1}^n U_{\kappa_i} V \subseteq K$. □

Lemma A.5. *Let K be a compact open subset containing 1_G of topological group G. Then there exists $N_0 \in \mathcal{N}$ such that $N_0 \subseteq K$.*

Proof. Take $H = \cup_{n=1}^\infty V^n$, where V is as given in Lemma A.4. That H is an open subgroup of G is proved in the routine way: As V is open, so is vV for every $v \in V$ (more generally, gV is homeomorphic to V for every $g \in G$). Hence V^2, a union of open sets, is open and, by induction, so is V^n. Immediately it follows H is open. Now $V^n = V^{-n}$ since $V = V^{-1}$ and so $H = H^{-1}$ (H contains all inverses). Also, for any $x, y \in H$, there must be $V^m \ni x$ and $V^n \ni y$ and so $xy \in V^m V^n \subseteq H$ (closure and identity). I.e., $H < G$. Now, by the previous lemma, $H \subseteq KH \subseteq K$. By compactness, $[G : H] = k < \infty$ and so $G = \cup_{i=1}^{k} \sigma_i H$ for some $\sigma_i \in G$. To conclude, set $N_0 = \cap_{\sigma \in G} \sigma H \sigma^{-1} = \cap_{i=1}^{k} \sigma_i H \sigma_i^{-1}$. Hence $N_0 \in \mathcal{N}$ and $N_0 \subseteq K$. □

To conclude the proof of Proposition A.11: By Lemma A.3 open neighborhood U of the identity of G contains some compact open subset K that contains the identity. By Lemma A.5 every such compact open neighborhood K of the identity contains some element $N \in \mathcal{N}$. Hence we have shown that for every open set U in G such that $1_G \in U$, there exists some $N \in \mathcal{N}$ such that $N \subseteq U$. □

A.5 Projective Limits, Relation to Profinite Groups

Let $(\mathfrak{I}, \leq)$ be a directed set, $\{(X_i, f_{ij}) : i, j \in \mathfrak{I}, i \leq j\}$ a projective system over $\mathfrak{I}$. For our purposes, we take the X_i to be topological spaces, the f_{ij} to be continuous homomorphisms from X_i to X_j satisfying appropriate compatibility conditions; namely $f_{ii} = id_{X_i}$, $f_{ij} \circ f_{jk} = f_{ik}$ for $i \leq j \leq k$. Define the *projective limit of the* X_i to be the set $X = \{(x_j)_{j \in \mathfrak{I}} : \forall i \leq j \;\; f_{ij}(x_j) = x_i\}$, where the Cartesian product $\prod_i X_i$ is endowed with the product topology and X with the relative topology.[10] We also denote the projective limit as $\varprojlim_{i} X_i$.

Proposition A.12. *If X_i is Hausdorff for every $i \in \mathfrak{I}$, then (1) Both $\prod_i X_i$ and X are Hausdorff, and (2) X is closed in $\prod_i X_i$.*

Proof. (1) is immediate. To show (2), first define $X_{ij} = \{(x_l)_l \in \prod_i X_i : f_{ij}(x_j) = x_i$ whenever $i \leq j\}$ and observe that $X = \bigcap_{i \leq j} X_{ij}$. Hence it suffices to show X_{ij} closed

[10] Recall the product space has a subbasis consisting of sets of the form $U_j \times \prod_{i \neq j} X_i$ where U_j is open in X_j.

for $i \leq j$. Next, note that $X_{ij} = \{(x_l)_l \in \prod_i X_i : \pi_i((x_l)_l) = f_{ij} \circ \pi_j((x_l)_l)\}$, where again all f_{ij} and projection mappings π_i, π_j are continuous.

The argument proceeds from the following generic topological property:

Lemma A.6. *If X, Y are topological spaces, Y is Hausdorff, and f, g are continuous maps from X to Y, then the set $E = \{x \in X : f(x) = g(x)\}$ is closed.*

Proof. We show that the complement $X - E$ is open. Choose any $z \in X - E$. Then $f(z) \neq g(z)$ and there exist disjoint open sets $U \ni f(z)$ and $V \ni g(z)$, as X is Hausdorff. Now $z \in f^{-1}(U) \cap g^{-1}(V) = \mathcal{K}_z$, which is open in X (continuity of f and g). But $f(\mathcal{K}_z) \subseteq U$ and $g(\mathcal{K}_z) \subseteq V$ imply $\mathcal{K}_z \cap E = \emptyset$. As $z \in X - E$ is arbitrary, E is open and the lemma follows. □

The claim now follows immediately. □

Proposition A.13. *If X_i is a nonempty compact Hausdorff space for every $i \in \mathfrak{I}$, then the projective limit X is compact and nonempty.*

Proof. As the product space $\prod_i X_i$ is compact (by Tychonov) and X is closed in $\prod_i X_i$, X is compact. Now suppose $X = \emptyset$. By the finite intersection property on compact X, there exist $i_1 \leq j_1, \cdots, i_n \leq j_n$ such that $\gamma = \cap_{k=1}^{n} X_{i_k j_k} = \emptyset$. But observe: Choose $k \in \mathfrak{I}$ such that $j_\nu \leq k$ for all $\nu = 1, \ldots, n$. As $X_k \neq \emptyset$, we can choose some $x_k \in X_k$. Choose element $(x_l)_l \in \prod_i X_i$ where $x_l = f_{lk}(x_k)$ if $l \leq k$ and x_l is chosen at will when $l \not\leq k$. Note that $i_\nu \leq j_\nu \leq k$ and $f_{i_1 j_1}(x_{j_1}) = x_{i_1}$. By compatibility,

$$f_{i_1 j_1}(x_{j_1}) = f_{i_1 j_1}(f_{j_1 k}(x_k)) = f_{i_1 k}(x_k) = x_{i_1}.$$

Thus $(x_l)_l \in \gamma$, contradicting the conclusion drawn from the supposition using the finite intersection property. □

Proposition A.14. *("Universal Property"): Let $\{G_i, g_{ij}\}_{i \leq j}$ be a projective system of topological groups, with each g_{ij} a continuous group homomorphism. Let $G = \varprojlim_i G_i$*

be the projective limit of the G_i. For each i, define $g_i = \pi_i|_G$. Suppose H is a topological group and, for each i, suppose $h_i : H \to G_i$ is a continuous homomorphism such that the diagram

$$\begin{tikzcd}
H \arrow[r, "h_j"] \arrow[dr, "h_i"'] & G_j \arrow[d, "g_{ij}"] \\
& G_i
\end{tikzcd}$$

commutes ($h_i = g_{ij} \circ h_j$). Then there exists a unique continuous homomorphism $h : H \to G$ such that the diagram

$$\begin{tikzcd}
H \arrow[r, "h"] \arrow[dr, "h_i"'] & G \arrow[d, "g_i"] \\
& G_i
\end{tikzcd}$$

commutes ($h_i = g_i \circ h$) for each i.

Proof. For $\sigma \in H$, define $h : H \to G$ by $\sigma \mapsto (h_i(\sigma))_{i\in\mathfrak{I}} \in \prod_i G_i$. If $i \leq j$, then note $h_i(\alpha) = g_{ij}(h_j(\alpha))$, so h is a group homomorphism. Also, $g_i \circ h(\sigma) = g_i((h_i(\sigma))_{i\in\mathfrak{I}}) = h_i(\sigma)$ for all $i \in \mathfrak{I}$.

Uniqueness follows trivially from the assumed commutativity of the first of the two above diagrams: If h and f both satisfy the requisite conditions, then $h_i = g_i \circ f = g_i \circ h$ for every $i \in \mathfrak{I}$.

For the continuity of $h : H \to G$, take subbasis element $\mathfrak{A} = G \cap (U_{i_0} \times \prod\limits_{i \neq i_0} G_i)$ of G, with $U_{i_0} \subseteq G_{i_0}$ open. Then note: $\sigma \in h^{-1}(\mathfrak{A})$ holds if and only if [$g_{i_0}h(\sigma) \in U_{i_0}$ holds, which holds if and only if] $h_{i_0}(\sigma) \in U_{i_0}$holds, which holds if and only if $\sigma \in h_{i_0}^{-1}(U_{i_0})$ holds. Thence $h^{-1}(\mathfrak{A}) = h_{i_0}^{-1}(U_{i_0})$. Continuity follows. □

Proposition A.15. *Given G a profinite group, $\mathcal{N} = \{N < G : N \lhd G\,open\}$. Then $G \simeq \varprojlim_{N\in\mathcal{N}} G/N$, where the isomorphism is both algebraic and topological.*

Proof. As $(\mathcal{N}, \supseteq)$ forms a directed set with $M \leq N$ iff $M \supseteq N$, consider map

$$f : G \to \varprojlim_{N \in \mathcal{N}} G/N = \{(\sigma_N N)_N : \forall M \leq N \ \sigma_M M = \sigma_N M\}$$

given naturally by $\sigma \mapsto (\sigma N)_{N \in \mathcal{N}}$. Note as $G/N \to G/M$ by $\sigma N \mapsto \sigma M$ for all $M \leq N$, the map f is well-defined. Clearly f is a group homomorphism. Further, as the quotient topology on G/N is here equivalent to the discrete topology, we may endow $\varprojlim_{N \in \mathcal{N}} G/N$ with the relative topology of G. The map is one-to-one since $\sigma \in \ker f$ implies $\sigma \in \bigcap_{N \in \mathcal{N}} N = \{1_G\}$ (as G is Hausdorff).[11]

To show f continuous, take profinite-limit basis element (writing $\prod'_N$ for $\prod_{N \notin \{N_1, \ldots, N_k\}}$)

$$\mathcal{U} = \left(\{\tau_1 N_1\} \times \{\tau_2 N_2\} \times \cdots \times \{\tau_k N_k\} \times \prod_N{}' G/N \right) \cap \varprojlim_{N \in \mathcal{N}} G/N$$

and consider $f^{-1}(\mathcal{U})$ in G: If $\mathcal{U} = \emptyset$, certainly $f^{-1}(\mathcal{U})$ is open in G; if $\mathcal{U} \neq \emptyset$, there exists $z = (\sigma_N N)_{N \in \mathcal{N}} \in \varprojlim_{N \in \mathcal{N}} G/N$ such that $z = (\ldots, \sigma_{N_0} N_1, \ldots \sigma_{N_0} N_k, \ldots)$ for every N_0 such that $N_i \leq N_0$ for $i = 1, \ldots, k$. (For instance, we may take $N_0 \subseteq \cap_{i=1}^k N_i \in \mathcal{N}$.) Whence, as $z \in \mathcal{U}$, an open basis element in the profinite limit of the G/N, we have $\sigma_{N_0} N_i \in \{\tau_i N_i\}$ and thus $\tau_i N_i = \sigma_{N_0} N_i$ for each $i = 1, \ldots, k$. I.e., $\tau_i = \sigma_{N_0}$ for $i = 1, \ldots, k$. Hence

$$\mathcal{U} = \left(\{\sigma_{N_0} N_1\} \times \{\sigma_{N_0} N_2\} \times \cdots \times \{\sigma_{N_0} N_k\} \times \prod_N{}' G/N \right) \cap \varprojlim_{N \in \mathcal{N}} G/N.$$

Now certainly $f^{-1}(\mathcal{U}) \supseteq \sigma_{N_0} \tilde{N}$ where $\tilde{N} = \cap_{i=1}^k N_i \in \mathcal{N}$ is open in G. For the reverse inclusion, let $\sigma \in f^{-1}(\mathcal{U})$. I.e., $f(\sigma) = (\sigma N)_{N \in \mathcal{N}} \in \mathcal{U}$. But $(\sigma N)_{N \in \mathcal{N}} \in \mathcal{U} =$

[11] As G is Hausdorff, if $z \neq 1_G$ were in $\cap N$ then there would exist disjoint open neighborhoods $U_1 \ni 1_G$ and $U_z \ni z$. There then would exist a fundamental neighborhood N of 1_G with $1 \in N \subseteq U_1$. But then $z \notin N$ would imply $z \notin \cap N$, contradicting supposition. The result follows.

$(\ldots, \sigma N_1, \ldots, \sigma N_k, \ldots)$ implies $\sigma N_i = \sigma_{N_0} N_i$, which implies $\sigma \in \sigma_{N_0} N_i$ for all N_i, which implies $\sigma \in \cap_{i=1}^{k} \sigma_{N_0} N_i = \sigma_{N_0} \cap_{i=1}^{k} N_i = \sigma_{N_0} \tilde{N}$. Hence we find $f^{-1}(\mathcal{U}) \subseteq \sigma_{N_0} \tilde{N}$.

From the fact that $f(G)$ is the continuous image of a compact set it follows that f is a homeomorphism, so an open (closed) set is mapped to an open (closed) set. Hence $f(G)$ is closed. Furthermore it is Hausdorf, as $f(G) \subseteq \varprojlim_{N \in \mathcal{N}} G/N$ (the profinite limit is Hausdorff).

Now to show f onto it would suffice to show $f(G)$ dense in G. I.e., for every $z \in \varprojlim_{N \in \mathcal{N}} G/N$ and every open set $U \in \varprojlim_{N \in \mathcal{N}} G/N$ containing z, $U \cap f(G) \neq \emptyset$.

For each such U there is some basic open set V_U such that $z \in V_U \subseteq U$. Recall V_U has the form $(\{\tau_1 N_1\} \times \cdots \times \{\tau_k N_k\} \times \prod_N' G/N) \cap \varprojlim_{N \in \mathcal{N}} G/N$. It would suffice to show $V_U \cap f(G) \neq \emptyset$ for every open set U. Now $z = (\sigma_N N)_{N \in \mathcal{N}} \in V_U$ implies $V = (\{\sigma_1 N_1\} \times \cdots \times \{\sigma_k N|k\} \times \prod_N' G/N) \cap \varprojlim_{N \in \mathcal{N}} G/N$ since $\tau_i N_i = \sigma_i N_i$ (coset equality). Choose $N_0 \in \mathcal{N}$ such that $N_i \leq N_0$ (i.e., $N_i \supseteq N_0$) for $i = 1, 2, \ldots k$. Then $\sigma_{N_0} N_i = \sigma_{N_i} N_i$ and so $V = (\{\sigma_{N_0} N_1\} \times \cdots \times \{\sigma_{N_0} N_k\} \times \prod_N' G/N) \cap \varprojlim_{N \in \mathcal{N}} G/N$. Hence $f(\sigma_{N_0}) \in V_U$. I.e., $f(\sigma_{N_0}) \subseteq V \cap f(G) \subseteq U \cap f(G)$. □

A.6 The p-adic integers $\mathbb{Z}_p$

The case Dedekind considers, namely the union of cyclotomic p-power extensions (for fixed odd prime p), has Galois profinite group isomorphic to the unit group of the p-adic integers. Hence, to describe Dedekind's work in modern terms, we recall the structure of profinite ring $\mathbb{Z}_p$ and its unit group.

With directed set $(\mathbb{N}, \leq)$ and canonical homomorphisms $\mathbb{Z}/p^n\mathbb{Z} \to \mathbb{Z}/p^m\mathbb{Z}$ $(m \leq n)$ as a projective system and topologizing in the usual way, we form the projective limit

$$\mathbb{Z}_p := \varprojlim_{n \in \mathbb{N}} \mathbb{Z}/p^n\mathbb{Z} = \{(a_n + p^n\mathbb{Z})_{n \in \mathbb{N}} : \forall m, n \; m \leq n \; a_m \equiv a_n \mod p^m\}.$$

Proposition A.16. *$\mathbb{Z}_p$ is an additive abelian topological group.*

Further,

Proposition A.17. *By the natural mapping $\mathbb{Z} \hookrightarrow \mathbb{Z}_p$ given by $a \mapsto (a + p^n\mathbb{Z})_{n\in\mathbb{N}}$, $\mathbb{Z}$ has dense image in $\mathbb{Z}_p$.*

Proof. Consider basic open set $\mathcal{U} = (\{a_1 + p^{n_1}\mathbb{Z}\} \times \cdots \times \{a_k + p^{n_k}\mathbb{Z}\} \times \prod_n{}' \mathbb{Z}/p^n\mathbb{Z}) \cap \mathbb{Z}_p$ and assume it to be nonempty ($\prod_n{}' := \prod_{\mathbb{N}-\{n_1,n_2,\ldots,n_k\}}$). Without loss of generality, choose $a \in \mathbb{Z}$ such that[12] $\mathcal{U} = (\{a + p^{n_1}\mathbb{Z}\} \times \cdots \times \{a + p^{n_k}\mathbb{Z}\} \times \prod_n{}' \mathbb{Z}/p^n\mathbb{Z}) \cap \mathbb{Z}_p$. Immediately note that $\mathbb{Z}$ is dense in $\mathbb{Z}_p$. □

Proposition A.18. *$\mathcal{F} = \{p^n\mathbb{Z}_p : n \in \mathbb{N}\}$ is a fundamental system of neighborhoods of the additive identity.*

Proof. (1) That $0 \in N \in \mathcal{F}$ for every such N is clear; (2) Immediately we find $p^n\mathbb{Z}_p \cap p^m\mathbb{Z}_p = p^{\max(n,m)}\mathbb{Z}_p$; (3) For any open set U in $\mathbb{Z}_p$ containing 0 there exists some basic neighborhood of 0 of the form $\mathcal{V} = (\{a + p^{n_1}\mathbb{Z}\} \times \cdots \times \{a + p^{n_k}\mathbb{Z}\} \times \prod_n{}' \mathbb{Z}/p^n\mathbb{Z}) \cap \mathbb{Z}_p$ for some $a \in \mathbb{Z}$, and thus

$$\mathcal{V} = (\{p^{n_1}\mathbb{Z}\} \times \cdots \times \{p^{n_k}\mathbb{Z}\} \times \prod_n{}' \mathbb{Z}/p^n\mathbb{Z}) \ \cap \ \mathbb{Z}_p \supseteq p^{\max\{n_i \,:\, i=1,\ldots,k\}}\mathbb{Z}_p \in \mathcal{F}.$$

□

Next observe that $\mathbb{Z}_p$ satisfies the nice property

Proposition A.19. *$\mathbb{Z}_p/p^n\mathbb{Z}_p \simeq \mathbb{Z}/p^n\mathbb{Z}$.*

Proof. We prove the isomorphism by establishing a short exact sequence of ring (module) homomorphisms $0 \to A \overset{\psi}{\to} B \overset{\varphi}{\to} C \to 0$ where ψ is injective, φ is surjective, and $\text{im}(\psi) = \ker\varphi$, which implies $B/\text{im}(\psi) \simeq C$. Toward that end, consider the homomorphism sequence $0 \to p^n\mathbb{Z} \overset{\text{i}}{\hookrightarrow} \mathbb{Z} \overset{\varphi}{\to} \mathbb{Z}_p/p^n\mathbb{Z}_p \to 0$ where

[12] We may do such, e.g., simply by taking $n \geq n_i$ for all $i = 1, \ldots, k$, for then we have $a_n \equiv a_i \mod p^{n_i}$ $(i = 1, \ldots, k)$ by definition.

$\mathfrak{i}$ is the natural injection mapping and $a \overset{\varphi}{\mapsto} (a + p^m\mathbb{Z})_{m\in\mathbb{N}} + p^n\mathbb{Z}_p$. Note that $\varphi \circ \mathfrak{i}$ acts as $a \overset{\mathfrak{i}}{\mapsto} a = p^n x \overset{\varphi}{\mapsto} \overline{0}$, so $\operatorname{im}\mathfrak{i} \subseteq \ker\varphi$. For the reverse inclusion, if $\varphi(a) = (a + p^m\mathbb{Z})_{m\in\mathbb{N}} + p^n\mathbb{Z}_p \in \ker\varphi$, i.e., if $(a + p^m\mathbb{Z})_{m\in\mathbb{N}} \in p^n\mathbb{Z}_p$, then we have, on every component (i.e., for every $m \in \mathbb{N}$), $a + p^m c_m = p^n a_m + p^m d_m$ for some integers a_m, c_m, d_m. That is, $a = p^n a_m + p^m(d_m - c_m)$, which is $\equiv 0 \mod p^m$ for every $m \geq n$. I.e., $a \in p^n\mathbb{Z}$, so $\ker\varphi \subseteq \operatorname{im}\mathfrak{i}$ and equality follows. Finally, to assure that φ is onto, take arbitrary element $z + p^n\mathbb{Z}_p \in \mathbb{Z}_p/p^n\mathbb{Z}_p$, recall that $\mathbb{Z}$ is dense in $\mathbb{Z}_p$, and note that this by definition implies $a \in z + p^n\mathbb{Z}_p$ for some integer a. □

Proposition A.20. *$\mathbb{Z}_p$ is a topological ring* $(\mathbb{Z}_p, +, \cdot)$.

Proof. $\mathbb{Z}_p$ is made into a ring in the natural way. That it is a topological ring, there is but to show that multiplication is continuous. Defining the map $\mathbb{Z}_p \times \mathbb{Z}_p \xrightarrow{\mu} \mathbb{Z}_p$ by $(z, w) \overset{\mu}{\mapsto} zw$, immediately note that $(z + p^n\mathbb{Z}_p, w + p^n\mathbb{Z}_p) \mapsto zw + p^n\mathbb{Z}_p$. □

Finally, we observe that

Proposition A.21. $(\mathbb{Z}_p)^\times = \varprojlim_{n\in\mathbb{N}} (\mathbb{Z}/p^n\mathbb{Z})^\times$.

Proof. For $z \in \mathbb{Z}_p^\times$, there exists $z^{-1} \in \mathbb{Z}_p^\times$ such that $1 = zz^{-1} = z^{-1}z$ where $z = (a_m + p^m\mathbb{Z})_{m\in\mathbb{N}}$ for $a_m \in \mathbb{Z}$, $z^{-1} = (b_m + p^m\mathbb{Z})_{m\in\mathbb{N}}$ for $b_m \in \mathbb{Z}$. Now $zz^{-1} = (a_m b_m + p^m\mathbb{Z})_{m\in\mathbb{N}} = (1 + p^m\mathbb{Z})_{m\in\mathbb{N}}$ if and only if $a_m b_m \equiv 1 \mod p^m$ for every $m \in \mathbb{N}$. Hence, in particular $a_m \in (\mathbb{Z}/p^m\mathbb{Z})^\times$ for every $m \in \mathbb{N}$, and thus, by compatibility, $z \in \varprojlim_{n\in\mathbb{N}} (\mathbb{Z}/p^n\mathbb{Z})^\times$. Conversely, if $z \in \varprojlim_{n\in\mathbb{N}} (\mathbb{Z}/p^n\mathbb{Z})^\times$, then each component has an inverse, and, by compatibility, this inverse lies in $\mathbb{Z}_p^\times$. □

A.7 Closed Subgroups of $\mathbb{Z}_p^\times$

By the Fundamental Theorem of Galois Theory, *closed* subgroups of $\mathbb{Z}_p^\times$ will correspond bijectively to subfields of $\operatorname{Gal}(\mathbb{Q}(\zeta_{p^\infty})/\mathbb{Q})$, both of which we wish to characterize, following Dedekind. We now investigate closed subgroups of $\mathbb{Z}_p^\times$, for p odd. First, note:

Lemma A.7. *For $\alpha = (a_n + p^n\mathbb{Z})_n \in \mathbb{Z}_p^\times$, we have $\alpha \in 1 + p^s\mathbb{Z}_p \iff a_s \equiv 1 \mod p^s$.*

Proof. $\alpha = (a_n + p^n\mathbb{Z})_n \in \mathbb{Z}_p^\times$ is such that, for every $m \leq n$, $a_m \equiv a_n \mod p^m$ and $(a_1, p) = 1$. Hence $\alpha \in 1 + p^s\mathbb{Z}_p$ if and only if there exist $c_0, c_1, \ldots, c_n, \ldots \in \mathbb{Z}$ such that

$$a_n = \begin{cases} 1 \mod p^n & : \ n \leq s \text{ (compatibility } \textit{down}\text{)} \\ 1 + p^s(\sum_{i=0}^{n-s-1} c_i p^i) \mod p^n & : \ n > s \text{ (compatibility } \textit{up}\text{)} \end{cases}$$

Hence $\alpha \in 1 + p^s\mathbb{Z}_p$ if and only if $a_s \equiv 1 \mod p^s$.[13] □

Proposition A.22. *Let p be an odd prime. We have the topological isomorphism $\mathbb{Z}_p^\times \simeq \mu_{p-1} \cdot (1 + p\mathbb{Z}_p)$,[14] where $\mu_{p-1} = \{\omega \in \mathbb{Z}_p^\times : \omega^{p-1} = 1\}$.*

Proof. Define $\mathbb{Z}_p^\times \xrightarrow{\varphi} \mu_{p-1} \times (1 + p\mathbb{Z}_p)$ by $(a_n + (p^n))_n = \alpha \overset{\varphi}{\mapsto} (\omega(a_1), \frac{\alpha}{\omega(a_1)})$,[15] where $\omega(a_1) = (a_1^{p^{n-1}} + p^n\mathbb{Z})_n$. Note $\omega(a_1) \in \mu_{p-1}$ for $a_1 \not\equiv 0 \mod p$.

That φ is well-defined: For some $b_1 \in \mathbb{N}$, $\frac{\alpha}{\omega(a_1)} = (b_1 + (p), \ldots)$ with $b_1 \equiv 1(p)$. As $\alpha = (a_1 + (p), \ldots)$, is a unit, immediately we have $\omega(a_1)^{-1} = \omega(a_1')$ for some natural number a_1' such that $a_1 a_1' \equiv 1(p)$.

That φ is a homomorphism: Immediately by construction, $\varphi(\alpha\beta) = (\omega(a_1b_1), \frac{\alpha\beta}{\omega(a_1b_1)}) = (\omega(a_1)\omega(b_1), \frac{\alpha\beta}{\omega(a_1)\omega(b_1)}) = (\omega(a_1), \frac{\alpha}{\omega(a_1)})(\omega(b_1), \frac{\beta}{\omega(b_1)}) = \varphi(\alpha)\varphi(\beta)$.

[13] As an aside, consider

$$a + p^s\mathbb{Z}_p = \{1 + p^s\beta \colon \beta \ni \mathbb{Z}_p\} = \{(1 + p^s b_n + p^n\mathbb{Z})_n \colon b_m \equiv b_n(p^m) \quad \forall m \leq n\},$$

where $\beta = (b_n + p^n\mathbb{Z})_n$. Note that $\alpha \in (a_n + p^n\mathbb{Z})_n \in 1 + p^s\mathbb{Z}_p$ if and only if $a_n \equiv 1 + p^s b_n(p^n)$, $a_m \equiv 1 + p^s b_m(p^m)$ and $b_m \equiv b_n(p^m)$ (for every $m \leq n$), if and only if $a_n \equiv 1 \mod p^s$ and $a_m \equiv a_n(p^m)$ (for every $m \leq n$). For $a_n \equiv 1(p^s)$ let $a_n = 1 + p^s b_n$ for some b_n (for each n) and $a_m = 1 + p^s b_m$ (for $m \leq n$). Then as $a_n \equiv a_m(p^{m+s})$ we have $1 + p^s b_n \equiv 1 + p^s b_m(p^{m+s})$ or $b_n \equiv b_m(p^m)$. Note now that by compatibility, and as $a_s \equiv 1 \mod p^s$, we have $\alpha = 1 + p\beta$ or $\frac{\alpha - 1}{p} = \beta$. Explicitly, $a_n = 1$ for $n \leq s$, $a_{s+1} = b_{s+1}$ arbitrary, and $a_{s+m} = \sum_{n+1}^{m} b_{s+n} p^n$ with $a_{s+m} \equiv a_k(p^k)$ for $k < s + n$.

[14] In the excluded case where $p = 2$, we find $\mathbb{Z}_2^\times = \{\pm 1\} \cdot (1 + 4\mathbb{Z}_2)$.

[15] Note: $< \alpha >= \frac{\alpha}{\omega(a_1)}$ is a principal unit in $\mathbb{Z}_p^\times$, i.e. $\in 1 + p\mathbb{Z}_p$.

That φ is injective: $\alpha \in \ker\varphi$ by definition if and only if both $\omega(a_1) = 1$ and $\frac{\alpha}{\omega(a_1)} = 1$.

That φ is surjective: For arbitrary element $(\omega(a_1), 1 + p\beta) \in \mu_{p-1} \times (1 + p\mathbb{Z}_p)$ note that $\alpha = \omega(a_1)(1 + p\beta)$ maps to it.

That φ is a homeomorphism: For continuity, consider open set $B = \{\omega(a_1\} \times (\frac{\alpha}{\omega(a_1)} + p^N\mathbb{Z}_p)\}$ for some $N \in \mathbb{N}$. Since $\alpha + p^N\beta \mapsto (\omega(a_1), \frac{\alpha}{\omega(a_1)} + p^N\frac{\beta}{\omega(a_1)})$, we have $\varphi^{-1}(B) = \alpha + p^N\mathbb{Z}_p$, an open preimage in $\mathbb{Z}_p^\times$. That φ is an open mapping, observe, for basic open set $1 + p^N\mathbb{Z}_p$ that $\varphi(1 + p^N\mathbb{Z}_p) = \{1\} \times (1 + p^N\mathbb{Z}_p)$.

Hence the claim is proven. □

Corollary A.1. *μ_{p-1} is the torsion subgroup[16] of $\mathbb{Z}_p^\times$.*

Proof. That $\mathrm{Tor}(\mathbb{Z}_p^\times) \supseteq \mu_{p-1}$ is apparent. For the reverse inclusion, consider $\alpha \in \mathrm{Tor}(\mathbb{Z}_p^\times)$. There exist ω, β such that $\alpha = \omega(1+p\beta)$. Suppose $\alpha \notin \mu_{p-1}$. Then $1+p\beta \neq 1$; i.e., $\beta \neq 0$. That is, $\beta \in p^N\mathbb{Z}_p - p^{N+1}\mathbb{Z}_p$ for some $N \in \mathbb{N}$; i.e., $\beta = p^N\gamma$ for some $\gamma \in \mathbb{Z}_p^\times$. Since already $\omega \in \mathrm{Tor}(\mathbb{Z}_p^\times)$, we must have $1 + p\beta \in \mathrm{Tor}(\mathbb{Z}_p^\times)$. Hence $(1 + p\beta)^M = 1$ for some $M \in \mathbb{N}$.

Now write $M = mp^s$ for $m \in \mathbb{N}$, where $(m, p) = 1$ and $s \geq 0$ and note $(1 + p\beta)^M = (1 + p^{N+1}\gamma)^{p^s m} = (1 + p^{N+s+1}\gamma')^m$ for some $\gamma' \in \mathbb{Z}_p^\times$, by binomial expansion. Again, by binomial expansion, $(1 + p^{N+s+1})^m = 1 + mp^{N+s+1}\gamma''$ for some $\gamma'' \in \mathbb{Z}_p^\times$. Hence $1 + mp^{N+s+1}\gamma'' = 1$, implying $mp^{N+s+1}\gamma'' = 0$, a contradiction. □

Proposition A.23. *Let $t \in \mathbb{N}$ and $\gamma \in \mathbb{Z}_p^\times$. Then $\overline{< 1 + p^t\gamma >} = 1 + p^t\mathbb{Z}_p$.*

Proof. For $\subseteq$: We find $< 1 + p^t\gamma > \subseteq 1 + p^t\mathbb{Z}_p$ by exhibiting an inverse of $1 + p^t\gamma$. The right-hand side is an open subgroup, thus closed, and so contains the closure of $< 1 + p^t\gamma >$.

For $\supseteq$: It suffices to show $< 1 + p^t\gamma >$ is dense in $1 + p^t\mathbb{Z}$. Let $\mathcal{U}$ be an arbitrary open subset of $1 + p^t\mathbb{Z}_p$ and let $1 + p^t\beta$ be an element of $< 1 + p^t\gamma >$. Either $\beta = 0$

[16] Recall that the torsion subgroup Tor(A) of an abelian group A is the subgroup of A consisting of all elements of finite order.

or not. If $\beta = 0$, take $(1+p^t\gamma)^0 = 1$. If $\beta \neq 0$, then, as Hausdorff, note $\beta \in p^n\mathbb{Z}_p$ and distinct from 0 implies $\beta \notin \bigcap_{n\geq 0} p^n\mathbb{Z}_p = \{0\}$. Therefore $\beta = p^s\delta$ for some $s \geq 0$ and $\delta \in \mathbb{Z}_p^\times$. Without loss of generality take $\mathcal{U} = 1 + p^t\beta + p^N\mathbb{Z}_p = 1 + p^{t+s}\delta + p^N\mathbb{Z}_p$ for $N > t+s$. Let $d \in \mathbb{Z}$, $d \equiv \delta \mod p^N\mathbb{Z}_p$ (so $p \nmid d$). Then note that this, by a coset argument, implies $\mathcal{U} = 1 + p^{t+s}d + p^N\mathbb{Z}_p$ (merely replace coset rep δ with d). Also, let $g \in \mathbb{Z}$, $g \equiv \gamma \mod p^N\mathbb{Z}_p$, (so $p \nmid g$). Recall that $(\mathbb{Z}/p^N\mathbb{Z})^\times = \mu_{p-1}^{(N)} \cdot \mu_{p^{N-1}}^{(N)}$ (which $= \mathcal{C}_{p-1} \cdot \mathcal{C}_{p^{N-1}}$). Then we find $< 1 + p^tg + p^N\mathbb{Z} >= \mu_{p^{N-t}}^{(N)}$ as $(1+p^tg)^k = 1 + p^Ng + \dots$ if and only if $k \geq p^{N-t}$, or else as $|1 + p^tg + p^N\mathbb{Z}| = p^{N-t}$ because $1 + p^tg + p^N\mathbb{Z} = \{\overline{a} \in (\mathbb{Z}/p^N\mathbb{Z})^\times : \overline{a}^{p^{N-t}} = 1\}$. Hence we have a generator for $\mu_{p^{N-t}}^{(N)}$. Now note that since $1 + p^{t+s}d + p^N\mathbb{Z} \in \mu_{p^{N-t}}^{(N)}$ (simply raise to the power $N-t$), there exists $\kappa \in \mathbb{N}$ such that $1 + p^{t+s}d + p^N\mathbb{Z} \equiv (1+p^tg)^\kappa \mod p^N$. Therefore $(1+p^tg)^\kappa \in 1 + p^{t+s}d + p^N\mathbb{Z} \subseteq 1 + p^{t+s}d + p^N\mathbb{Z}_p = \mathcal{U}$, a coset equivalent to that resulting by replacing d with γ, as $\gamma \equiv g(p^N\mathbb{Z}_p)$, which yields $(1+p^t\gamma)^\kappa \equiv (1+p^tg)^\kappa \mod p^N\mathbb{Z}_p$. Thus we have $1 + p^t\gamma \in \mathcal{U}$ and so $< 1 + p^t\gamma >$ is dense in $1 + p^t\mathbb{Z}_p$. □

Proposition A.24. *Given natural numbers M, N with $1 \leq M \leq N$. Then $(1 + p^M\mathbb{Z}_p : 1 + p^N\mathbb{Z}_p) = p^{N-M}$.*

Proof. Since[17] the multiplicative factor group $\mathbb{Z}_p^\times / 1 + p^N\mathbb{Z}_p$ is algebraically and topologically isomorphic to $(\mathbb{Z}/p^N\mathbb{Z})^\times$, which is cyclic, it follows that, as a multiplicative factor group, $(1+p^M\mathbb{Z}_p)/(1+p^N\mathbb{Z}_p)$ is a finite cyclic subgroup, every element of which has order $\leq p^{N-M}$. Let us be cautious here: As a *multiplicative* factor group, every element has the form $z(1+p^N\mathbb{Z}_p)$, where $z = 1 + p^M\beta$ with $|z| \mid p^{N-M}$. Notice that, taking $\beta = 1$, $|(1+p^M)(1+p^N\mathbb{Z}_p)| = p^{N-M}$. Hence, the order of the factor group is precisely p^{N-M}. □

Proposition A.25. *The sequence $1 \to 1 + p^s\mathbb{Z}_p \hookrightarrow \mathbb{Z}_p^\times \overset{\varphi}{\to} (\mathbb{Z}/p^s\mathbb{Z})^\times \to 1$, with $(a_n + p^n\mathbb{Z})_n \overset{\varphi}{\mapsto} a_s + p^s\mathbb{Z}$, is exact.*

[17] By exact sequence $\mathbb{Z}_p^\times \to (\mathbb{Z}/p^N\mathbb{Z})^\times \to 1$ with $(a_n + p^n\mathbb{Z})_n \mapsto a_N + p^N\mathbb{Z}$.

Proof. By compatibility, $a_m \equiv a_n(p^n)$, $m \leq n$, $p \nmid a_1$ (and so $p \nmid a_n$ for every $n \in \mathbb{N}$). φ is clearly a well-defined homomorphism. It is surjective, as seen by considering elements $(a_s + p^n\mathbb{Z})_n$ for fixed a_s. For determining the kernel of φ, let $\alpha \in \mathbb{Z}_p^\times$, $\alpha = (a_n + p^n\mathbb{Z})_n$. Then $\alpha \in \ker\varphi$ if and only if $a_s \equiv 1 \mod p^s$, if and only if

$$a_n \equiv \begin{cases} 1 \mod p^n & : \quad n \leq s \\ 1 \mod p^s & : \quad n > s \end{cases}.$$

□

Proposition A.26. *If H is a closed subgroup of $\mathbb{Z}_p^\times$, then $H = \mu_f$ for some $f|p-1$ or $H = \mu_f \cdot (1 + p^s\mathbb{Z}_p)$ for some $f|p-1$ and $s \in \mathbb{N}$.*

Proof. Certainly μ_f is closed as a finite subset of Hausdorff space $\mathbb{Z}_p^\times$, and as clearly $\mu_f \cdot (1 + p^s\mathbb{Z}_p) = \bigcup\limits_{\omega \in \mu_f} \omega \cdot (1 + p^s\mathbb{Z}_p)$ is open, hence closed. So we seek to show that there are no other closed subgroups.

Toward that end, note that either $(1+p)^{p^{s-1}} \in H$ for some $s \in \mathbb{N}$ or not and consider each case.

Case 1: Suppose $(1+p)^{p^{s-1}} \in H$ for some natural number s, where s is taken to be minimal. Surely $< 1 + p >^{p^{s-1}} \subseteq H$. Taking the closure of each set, note $\overline{< 1 + p >^{p^{s-1}}} \subseteq \overline{H} = H$.

Recall that $\overline{< 1 + p >^{p^{s-1}}} = 1 + p^s\mathbb{Z}_p$ and consider the factor groups $(1) \subseteq H/(1+p^s\mathbb{Z}_p) \subseteq \mathbb{Z}_p^\times/(1+p^s\mathbb{Z}_p)$. To show a bijection exists between sets $\{H\colon 1+p^s\mathbb{Z}_p \subseteq H \subseteq Z_p^\times\}$ and $\{\Gamma = H/(1 + p^s\mathbb{Z}_p)\colon (1) \leq \Gamma \leq \mathbb{Z}_p^\times/(1 + p^s\mathbb{Z}_p)\}$, note that it would follow could we show the sequence

$$1 \to 1 + p^s\mathbb{Z}_p \xrightarrow{\phi} \mathbb{Z}_p^\times \xrightarrow{\varphi} (\mathbb{Z}/p^s\mathbb{Z})^\times \to 1$$

to be exact. But this is the content of Proposition A.25. Hence $\mathbb{Z}_p^\times/(1+p^s\mathbb{Z}_p) \simeq (\mathbb{Z}/p^s\mathbb{Z})^\times$, which is cyclic. Further as $(\mathbb{Z}_p^\times \colon 1+p^s\mathbb{Z}_p) = \phi(p^s)$, the factor group $H/(1+p^s\mathbb{Z}_p)$ has order $(H \colon 1+p^s\mathbb{Z}_p) = p^t f$ where f divides $p-1$ and $0 \leq t \leq s-1$. But now, as $(\mu_f \cdot (1+p^{s-t}\mathbb{Z}_p) \colon 1+p^s\mathbb{Z}_p) = p^t f$,[18] the uniqueness of the order of a subgroup of a cyclic group forces $H = \mu_f \cdot (1+p^{s-t}\mathbb{Z}_p)$.

Case 2: Suppose $(1+p)^{p^t} \notin H$ for every natural number t. I.e., $1+p^t\mathbb{Z}_p \nsubseteq H$ for any $t \in \mathbb{N}$. Now if $H \nsubseteq \mu_{p-1}$, then, for some $h \in H$ there would exist $\omega \in \mu_{p-1}$ and $\gamma \in \mathbb{Z}_p^\times$ such that $h = \omega(1+p^s\gamma)$. Then $h^{p-1} = \omega^{p-1}(1+p^s\gamma)^{p-1} = 1(1+p^s\gamma)^{p-1} = 1+(p-1)p^s\gamma +$ *terms with higher powers of* $p \in 1+p^s\mathbb{Z}_p$, contradicting our supposition. □

A.8 Dedekind's Results

We now wish to consider the lattice structure of the closed subgroups and construct the corresponding subfield lattice as per the generalized Galois correspondence (as per Krull) of extension $\mathbb{Q}(\zeta_{p^\infty}) = \cup_n \mathbb{Q}(\zeta_{p^n})$, where[19] $\zeta_{p^t} = e^{\frac{2\pi i}{p^t}}$ and p is an odd prime in $\mathbb{N}$ and relate these to the characterizations of elements of these subgroups, presented as a supplement to the article in the *Collected Works* and attributed to Dedekind's *Nachlass*.

Toward that end, recall $\mathbb{Z}_p^\times = \mu_{p-1} \cdot (1+p\mathbb{Z}_p)$, an internal product ($p$ odd), with $\mu_{p-1} = \{\omega \in \mathbb{Z}_p^\times \colon \omega^{p-1} = 1\} \simeq \mathcal{C}_{p-1}$, where $\omega = \omega(a) = (a^{p^{n-1}} + p^n\mathbb{Z})_n$ for $a \equiv 1, \ldots, p-1 \mod p$. Also recall, $\mu_{p-1} \simeq (\mathbb{Z}/p\mathbb{Z})^\times$ and $\omega = \omega(a)$ holds precisely when $\omega \in a + p\mathbb{Z}$. Further, all closed subgroups H have form μ_f or $\mu_f \cdot (1+p^s\mathbb{Z}_p)$, where $p-1 = ef$.

[18] As an internal direct product, we need but verify, for $t < s$, that $((1+p^s\mathbb{Z}_p) \colon (1+p^t\mathbb{Z}_p)) = p^{s-t}$. But this is immediate by noting (from above) that $(1+p)^{p^{t-1}}$ is a generator for $1+p \in \mathbb{Z}_p$, thus $((1+p)^{p^{t-1}})^{p^{s-t}} \in 1+p^s\mathbb{Z}_p$, though no lesser power than $s-t$ is contained in $1+p^s\mathbb{Z}_p$.

[19] Note, as $\alpha \in \mathbb{Z}_p^\times$, $\alpha = (a_n + p^n\mathbb{Z}_p)$, that $\zeta_{p^N}^{\alpha} = \zeta_{p^N}^{a_N}$.

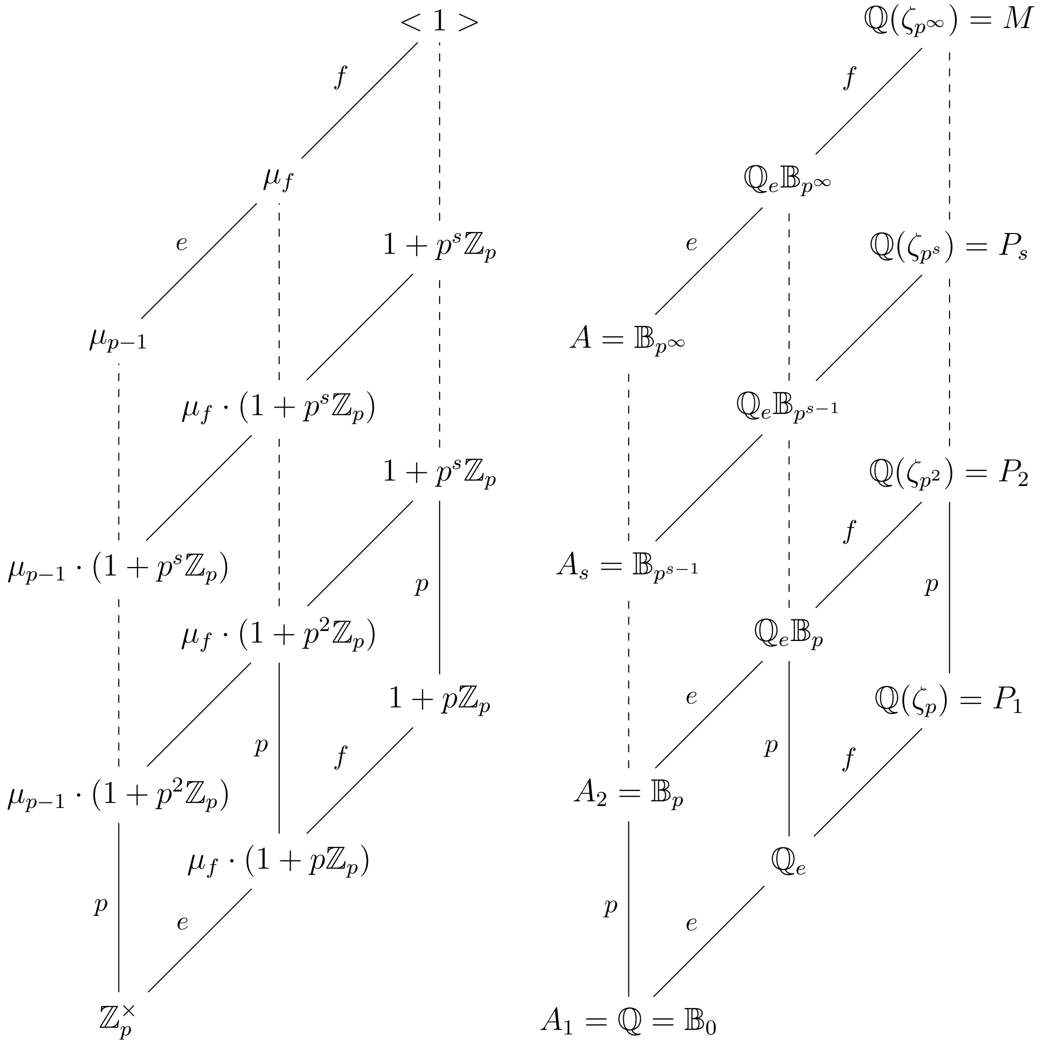

$< 1 >$
f
μ_f
e
$1 + p^s\mathbb{Z}_p$
μ_{p-1}
$\mu_f \cdot (1 + p^s\mathbb{Z}_p)$
$1 + p^s\mathbb{Z}_p$
$\mu_{p-1} \cdot (1 + p^s\mathbb{Z}_p)$
p
$\mu_f \cdot (1 + p^2\mathbb{Z}_p)$
$1 + p\mathbb{Z}_p$
p
f
$\mu_{p-1} \cdot (1 + p^2\mathbb{Z}_p)$
$\mu_f \cdot (1 + p\mathbb{Z}_p)$
p
e
$\mathbb{Z}_p^\times$
$\mathbb{Q}(\zeta_{p^\infty}) = M$
f
$\mathbb{Q}_e\mathbb{B}_{p^\infty}$
e
$\mathbb{Q}(\zeta_{p^s}) = P_s$
$A = \mathbb{B}_{p^\infty}$
$\mathbb{Q}_e\mathbb{B}_{p^{s-1}}$
$\mathbb{Q}(\zeta_{p^2}) = P_2$
f
$A_s = \mathbb{B}_{p^{s-1}}$
p
$\mathbb{Q}_e\mathbb{B}_p$
e
$\mathbb{Q}(\zeta_p) = P_1$
p
f
$A_2 = \mathbb{B}_p$
$\mathbb{Q}_e$
p
e
$A_1 = \mathbb{Q} = \mathbb{B}_0$

Figure A.8. Closed subgroup (*left*) and corresponding field extension (*right*) sublattices for $\mathbb{Q}(\zeta_{p^\infty})$ and etc., for fixed $e|\phi(p)$

Now noting the key structural fact that $\mathbb{Z}_p^\times/(1+p^s\mathbb{Z}_p) \simeq (\mathbb{Z}/p^s\mathbb{Z})^\times$, so that, e.g., $\mathrm{Gal}(\mathbb{Q}(\zeta_{p^2}/\mathbb{Q}) \simeq (\mathbb{Z}/p^2\mathbb{Z})^\times \simeq \mathcal{C}_{p-1} \cdot \mathcal{C}_p$ (recall here $\mathcal{C}_p =< 1+p+p^2\mathbb{Z} >$), we thus obtain, *for each fixed* $f|p-1$, the corresponding sublattices shown in Figure A.8. The nomenclature for subfields in the diagram accords with what appears in the the supplement to Dedekind's article (cf. Chapter 3, *Translation*).

Now for any subfield $K \subseteq M$, we observe two cases:

Case 1: $K \subseteq \mathbb{Q}(\zeta_{p^s})$ for some $s \in \mathbb{N}$, taking s to be minimal such satisfying the condition. I.e., $K \nsubseteq \mathbb{Q}(\zeta_{p^{s-t}})$ for $t < s$. Hence, by finite Galois theory, $K = A_s\mathbb{Q}_e$.

Case 2: Suppose $K \nsubseteq \mathbb{Q}(\zeta_{p^s})$ for every $s \in \mathbb{N}$. Then $[K\colon \mathbb{Q}] = \infty$, since otherwise $K = \mathbb{Q}(a)$ for some $a \in M$ would imply $a \in \mathbb{Q}(\zeta_{p^s})$ for some s and hence also $K \subseteq \mathbb{Q}(\zeta_{p^s})$. We claim that $A \subseteq K$: Recall that for every $a \in K$, $a \in \mathbb{Q}(\zeta_{p^s}) - \mathbb{Q}(\zeta_{p^{s-1}})$ for some $s \in \mathbb{N}$. Hence $\mathbb{Q}(a) \supseteq A_s$. Since $[K\colon \mathbb{Q}] = \infty$, there exist $a_n \in K$ such that $K = \cup_{n=1}^\infty \mathbb{Q}(a_n) = \cup_{n=1}^\infty K_n$, where $\mathbb{Q}(a_n) \nsubseteq \mathbb{Q}(a_{n+1})$ for each $n \in \mathbb{N}^+$; i.e., $K_n \nsubseteq K_{n+1}$. Thus we see $A_s \subseteq K$ for every s, a totally ordered chain of fields bounded by the factors of $p-1$. And, as $A = \cup_s A_s$, $A \subseteq K$.

H	M^H
μ_f	$A\mathbb{Q}_e$
$\mu_f \cdot (1+p^s\mathbb{Z}_p)$	$A_s\mathbb{Q}_e$

Table A.1. Fixed field-closed subgroup correspondence.

Table A.1 summarizes our findings. Note, e.g., μ_f is the *identitätsgruppen von* M for $A\mathbb{Q}_e$; that is, the closed subgroup for which $A\mathbb{Q}_e$ is the fixed field.[20]

Finally, we wish to describe the elements of a given closed subgroup H. To that end, we have the

[20] That $A\mathbb{Q}_e$ is necessarily the corresponding fixed field, consider the below lattices:

Proposition A.27. *Take arbitrary $\alpha = (a_n + p^n\mathbb{Z})_n \in \mathbb{Z}_p^\times$, where by definition, for every $m \leq n$ we find $a_n \equiv a_m \mod p^m$ and $(a_1, p) = 1$. Either (1) α fixes $A\mathbb{Q}_e$ (element wise) if and only if $\alpha \in \mu_f$; or (2) α fixes $A_s\mathbb{Q}_e$ if and only if $\alpha \in \mu_f \cdot (1 + p^s\mathbb{Z}_p)$.*

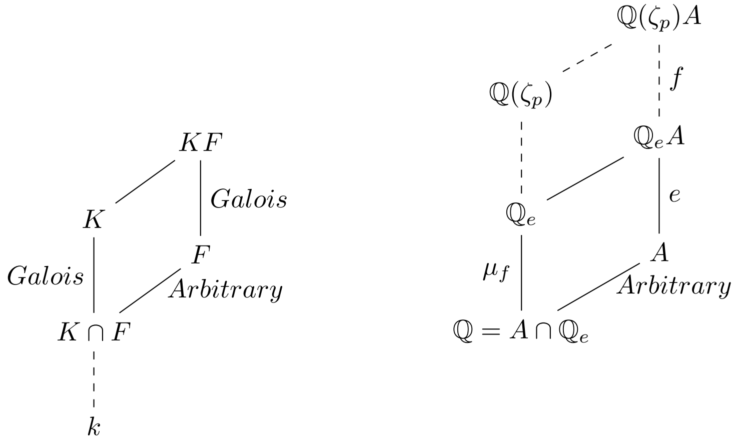
Proof. For case (1): $\alpha \in \mu_f$ if and only if

$$\begin{aligned} & \alpha = \omega(a_1), && a_1^f \equiv 1 \mod p \\ \overset{def.}{\iff} \quad & \alpha = (a_1^{p^{n-1}} + p^n\mathbb{Z})_n, && a_1^f \equiv 1 \mod p \\ \iff \quad & a_n \equiv a_1^{p^{n-1}} \mod p^n, && a_1^f \equiv 1 \mod p \end{aligned}$$

For case (2): First recall that $\alpha \in 1 + p^s\mathbb{Z}_p$ if and only if $a_s \equiv 1 \mod p^s$.[21] We now show the

Proposition A.28. *$\alpha \in \mu_f \cdot (1 + p^s\mathbb{Z}_p)$ if and only if $a_s^f \equiv 1 \mod p^s$.*

Proof. ($\Rightarrow$) Suppose $\alpha \in \mu_f \cdot (1 + p^s\mathbb{Z}_p)$. Then $\alpha = \omega(a_1)\beta$, where $\omega(a_1) = (a_1^{p^{n-1}} + p^n\mathbb{Z})_n$, $a_1^f \equiv 1 \mod p$ and $\beta \in (1 + p^s\mathbb{Z}_p)$, of the form $\beta = (b_n + p^n\mathbb{Z})_n$ such that $b_s \equiv 1 \mod p^s$. Note $a_s \equiv a_1^{p^{s-1}} b_s \mod p^s \equiv a_1^{p^{s-1}} \mod p^s$ and $a_1 = 1 + p\kappa$ for



Note $KF/F \simeq K/(K \cap F)$ and so $\mathrm{Gal}(\mathbb{Q}_eA/A) \simeq \mathrm{Gal}(\mathbb{Q}_e/(A \cap \mathbb{Q}_e))$. Now $A \cap \mathbb{Q}_e = \mathbb{Q}$ as A has p-power subgroups whereas $\mathbb{Q}_e$ has subgroups of order divisors of $p - 1$. For $A \subseteq D \subseteq M$, all Galois, with $[M\colon A] = p - 1$ and e.g. $[A\colon D] = e$, immediately the uniqueness of cyclic subgroups forces $D = \mathbb{Q}_eA$.

[21] Here is the first of the Dedekind Identity groups, with $f = 1$. But it is miswritten in the *Collected Works* and should instead read (to show compatibility): $(n, \varepsilon) \equiv (n + 1, \varepsilon) \mod p^n$.

some $\kappa \in \mathbb{Z}$. Thus

$$\begin{aligned} a_s^f &\equiv (a_1^{p^{s-1}})^f && \mod p^s \\ &\equiv (a_1^f)^{p^{s-1}} && \mod p^s \\ &\equiv (1+p\kappa)^{p^{s-1}} && \mod p^s \\ &\equiv 1 && \mod p^s \quad \textit{(Binomial theorem.)} \end{aligned}$$

($\Leftarrow$) Suppose[22] $a_s^f \equiv 1 \mod p^s$. Consider $\omega(a_1)$ as given above. Since $a_z^f \equiv 1 \mod p$, $\omega(a_1) \in \mu_f$. To show the existence of some satisfactory α, consider $\frac{\alpha}{\omega(a_1)} = \beta = (b_n + p^n\mathbb{Z})_n$. By consideration of compatibility conditions, it suffices to show $b_s \equiv 1 \mod p^s$. Since $b_s = \frac{a_s}{a_1^{p^{s-1}}}$, we have $(a_1^{p^{s-1}} b_s)^f \equiv a_s^f \mod p^s$. Now $b_s^f \equiv 1 \mod p^s$ follows immediately, since $a^f \equiv 1 \mod p$ implies $a_1^f \equiv 1 \mod p^s$.[23]

Observe in particular (for $s = 1$) $a_1^{p^{s-1}} b_s \equiv a_s \mod p^s$ (by compatibility, again), implying $a_1 b_1 \equiv a_1 \mod p$ or $b_1 \equiv 1 \mod p$ as $(a,p) = 1$. Hence $b_s \equiv b_1 \equiv 1 \mod p$, so setting $b_s = 1 + p\kappa$ for some $\kappa \in \mathbb{Z}$ we find $b_s^{p^{s-1}} \equiv (1+p\kappa)^{p^{s-1}} \equiv 1 \mod p^s$ (using the binomial theorem, again). Therefore $(f, p^{s-1}) = 1$ and $b_s^f \equiv b_s^{p^{s-1}} \equiv 1 \mod p^s$ imply $b_s \equiv 1 \mod p^s$. □

As both cases have been proven, the proposition follows. □

[22] This is the second of the first set of Identity group conditions, namely $(s, \varepsilon)^f \equiv 1 \mod p^s$.

[23] In detail, $a^{p^{s-1}} b_s \equiv a_s \mod p^s$ and $a_1^f \equiv 1(p)$ imply $a_1^{fp^{s-1}} \equiv 1 \mod p^s$. Therefore $b_s^f \equiv a_1^{fp^{s-1}} b_s^f \equiv a_s^f \equiv 1(p^s)$.

BIOGRAPHY OF THE AUTHOR

Joseph J.P. Arsenault, Jr. was born in Putnam, Connecticut on April 15, 1964. He graduated from Wiscasset High School (Wiscasset, Maine) in 1982. He received a Bachelor of Arts degree in Mathematics from University of Maine in 1995. He is a candidate for the Master of Arts degree in Mathematics from the University of Maine in August 2015.