COGNITIVE CONTROL IN MATHEMATICS

by

Jukka Petri Mikael Keränen

A.B., Princeton University, 1995

M.Sc., University of Cambridge, 1997

Submitted to the Graduate Faculty of

Arts and Sciences in partial fulfillment

of the requirements for the degree of

Doctor of Philosophy

University of Pittsburgh

2005

UNIVERSITY OF PITTSBURGH

SCHOOL OF ARTS AND SCIENCES

This dissertation was presented

by

Jukka Keränen

It was defended on

September 26, 2005

and approved by

Nuel Belnap, Professor, Department of Philosophy

Robert Brandom, Professor, Department of Philosophy

John Earman, Professor, Department of History and Philosophy of Science

John McDowell, Professor, Department of Philosophy

Dissertation Advisor: Kenneth Manders, Professor, Department of Philosophy

University of Pittsburgh

2005

COGNITIVE CONTROL IN MATHEMATICS

Jukka Keränen, PhD

University of Pittsburgh, 2005

The nature of mathematical theorizing underwent a dramatic transformation in the late 19th and early 20th centuries. Mathematicians are prone to describe this transformation by saying that mathematics became more 'conceptual' and that, consequently, we have come to enjoy more and better 'understanding' in mathematics. The purpose of my dissertation is to introduce a constellation of philosophical notions that allows us to analyze the epistemic significance of these changes. In order to arrive at such a constellation, I conduct a case study in which I compare two approaches to the solvability of polynomial equations by radicals, one characteristic of 19th century mathematics, another characteristic of 20th century mathematics. I use the pre-philosophically visible differences between the two approaches to motivate a new epistemological notion I call *cognitive control*. To have cognitive control over an epistemic process such as reading or writing a proof is to have *epistemic guidance* for the process in virtue of having an *epistemic scaffolding*. To have epistemic guidance at a given juncture in a process is to have a constellation of cognitive resources that allows one to represent the different possible ways of pursuing the process further; to have an epistemic scaffolding for a process is to have a suitably organized representation of the epistemically possible facts in the range of facts one has chosen to examine. I apply the notion of cognitive control to two proofs of the fact that there is no general formula for a solution by radicals for polynomial equations of degree 5, again one characteristic of 19th century mathematics, another characteristic of 20th century mathematics. I argue that we enjoy much better cognitive control over the process of reading the 20th century proof than we do over the process of reading the 19th century proof. This suggests that the epistemic significance of the said changes in the nature of mathematical theorizing consists, at least in part, in the circumstance that the conceptual resources of 20th century mathematics allow us to enjoy more and better cognitive control over the epistemic processes in mathematical research and learning.

TABLE OF CONTENTS

PREFACE

This dissertation is dedicated to the crew of the space shuttle *Columbia* who lost their lives in the pursuit of science on February 1, 2003.

1.0 INTRODUCTION

It is widely recognized that the nature of mathematical theorizing changed dramatically in the latter half of the 19th century.[1] Mathematicians are prone to describe this change by saying that mathematics became more "conceptual" and that, as a consequence, there was a dramatic increase in the epistemic power of mathematical theories. It is widely recognized, indeed, that mathematics in the 20th century was far more *successful as a science* than in the previous centuries. It is not at all obvious, however, in what this success consists—it is not at all obvious, that is, how we should characterize the *epistemic significance* of the theoretical accomplishments of 20th century mathematics. It is clear, I take it, that merely pointing to the fact that we have acquired more mathematical knowledge would not be adequate.

[1] See Gray, "The nineteenth-century revolution in mathematical ontology"; Stein, "Logos, *Logic*, and Logistiké: *Some Philosophical Remarks on Nineteenth-Century Transformation of Mathematics*"; and Mac Lane, "Structure in Mathematics". For example, Stein writes: "Mathematics underwent, in the nineteenth century, a transformation so profound that it is not too much to call it a second birth of the subject—its first birth having occurred among the ancient Greeks..." (p. 238).

One attractive suggestion would be that the principal epistemic significance of the pivotal accomplishments of 20th century mathematics is that they have made it possible to *understand* many ranges of mathematical facts *better* and, indeed, to understand ranges of mathematical facts we were not able to understand before *at all*. Thus, the thought would be that the scientific success of mathematics in the 20th century consists, at least in part, in the circumstance that we have acquired more and better understanding in mathematics. This suggestion is attractive because it is natural to think that one of the aims of any science, empirical or not, just is to help us understand various ranges of facts; indeed, mathematicians have long maintained that coming to understand mathematical facts is one of the central aims of mathematics.[2] We do not currently have a philosophical analysis of what it *is* to understand mathematical facts, however.[3] Thus, we are not in a position to properly evaluate this attractive suggestion.

[2] See, for example, G.F. Gauss, *Disquisitiones Arithmeticae*; Mac Lane, "Structure in Mathematics"; Thurston, "On Proof and Progress in Mathematics". For example, Thurston, one of the pre-eminent geometers of the latter part of the 20th century, writes: "what we are doing [in mathematics] is finding ways for *people* to understand and think about mathematics." (p. 162)

[3] There is to my knowledge not a single paper devoted specifically to understanding in mathematics, though there has been some recent work on *explanation* in mathematics. See Mancosu's "Mathematical explanation: problems and prospects" for an exhaustive overview of the existing literature. There is likewise very little work devoted specifically to understanding in general. See Cooper, "The Epistemology of Understanding" and Österman, "Is there a General Sense of Understanding?" The latter contains an essentially complete list of references on the literature concerning understanding.

In order to formulate a hypothesis about what it is to understand mathematical facts, I conducted a number of mathematical case studies. In each one, I compared two theoretical approaches aimed at solving the same mathematical problem: one characteristic of 19th century mathematics, another characteristic of 20th century mathematics. I made sure to pick cases in which both approaches can solve the problem and yet, the consensus among mathematicians would be that the 20th century approach is epistemically superior to the 19th century one. The most suggestive among my case studies turned out to be one in which I examined the shift from Abel's 1826 approach to the *solvability of polynomial equations by radicals* to Artin's 1940 approach, a development that is widely considered to be pivotal in the evolution of modern mathematics.

Thus, by comparing the two approaches in each case, I was hoping to identify sets of epistemic resources—concepts, methods of acquiring knowledge, and bits of knowledge—the significance of which could plausibly be that they allow us to understand some range of mathematical facts. At the same time, I remained open to the possibility that the significance of the sets of resources I considered might be something different altogether. I was led to conclude that while many of the resources characteristic of 20th century mathematics do in fact allow us to understand some range of mathematical facts better than do the corresponding 19th century resources, this is typically not the fundamental difference between them. As I will argue in this essay, typically the fundamental difference is that the 20th century resources allow us to attain better *cognitive control* over our mathematical *epistemic processes* such as proving theorems and solving problems: they make it possible for us to attain a higher grade of a certain kind of rational mastery over what we *do* in mathematics, one I chose to call "cognitive control."

The idea is this. In our mathematical epistemic projects, we are constantly being placed in particular situations in which we need to reach some particular *epistemic aim*: to find a solution to a computation problem, to prove a theorem, to describe some objects. Let us consider the following question: How do we succeed in reaching such an aim when the epistemic resources we have at the outset of our epistemic process are insufficient for reaching it? The platitudinous answer is that we need to acquire new bits of knowledge or new concepts. My case studies convinced me that there is also a non-platitudinous answer: blind luck and genius aside, we need to acquire a particular kind of configuration of epistemic resources, one the having of which amounts to having cognitive control over the process of pursuing our aim; for it is in virtue of having cognitive control that we can *bring reason to bear* on the epistemic challenges we face in our projects. Since the characterization of cognitive control will be rather complicated, I will not attempt even to sketch it here. Suffice it to say that cognitive control over an epistemic process will turn out to be a particular kind of configuration of knowledge, representational abilities, and abilities to manipulate conceptually constituted representations in a way that allows us to pursue the aims of our processes in a *rationally orchestrated* manner.

My purpose in this essay is to present a tentative characterization of cognitive control and employ that characterization to analyze the pre-philosophically felt differences in the epistemic power of the approaches of Abel and Artin. I will argue that the theoretical resources of Artin's approach allow us to maintain much better cognitive control over the process of proving the central result common to the two approaches. I hope to show that the notion of cognitive control allows us to provide a nuanced and illuminating analysis of the various ways in which Artin's approach is epistemically superior to Abel's.

My analysis will show that the differences in the quality of cognitive control the two approaches afford us are due to the fact that Artin's approach is organized by representations that involve much richer sets of concepts than those that organize Abel's approach. Foremost among these concepts are the concepts of various kinds of algebraic structures such as *group*, *subgroup*, *quotient group* and *field extension*, and the concepts of various kinds of morphisms between such structures. Thus, I will argue that the ability to construct and manipulate conceptually constituted representations is one of the most important sources of cognitive control in mathematics.

I want to emphasize that my characterization of cognitive control is intended to describe an epistemically significant *pattern* in our mathematical cognitive activity. In particular, I want to guard against the impression that the argumentative structure of my analysis is circular. Even though the components my characterization are motivated by considering the mathematically specific features of the two proofs, I think that once they are in place, they will be seen to constitute a coherent epistemological notion intelligible on its own right. Further, this notion can readily be seen to apply to mathematical epistemic processes that are not intrinsically associated with the case study: after articulating each of the components of my characterization, I will show that it applies to a variety of mathematical situations unrelated to and, indeed, decidedly different from the ones found in the epistemic processes of Abel and Artin.

In further work, I intend to strengthen the motivation for my characterization of cognitive control in three ways. First, I will apply that characterization to other contrastive case studies. This work is well underway, and the results are promising. The conclusion, one recommended already by the analysis of Abel and Artin, will be that the basic epistemic significance of many of the conceptual resources characteristic of 20th century mathematics is that they make it possible to acquire excellent cognitive control over *wide ranges* of mathematical epistemic processes. Second, I will argue that to *understand* a range of mathematical facts amounts to having cognitive control over the processes of proving those facts. This analysis will have the philosophically interesting feature that it is equally compatible with nominalism and realism about the ontology of mathematics.

Third, I will show that my characterization of cognitive control can be applied to analyze epistemic processes in *empirical* science and, indeed, epistemic processes in our epistemic activity quite generally. Thus, ultimately I hope to argue that to understand a range of empirical facts can be analyzed in terms of having cognitive control over the processes of coming to know those facts. The structure of the theory in the empirical case will be more complicated because there we need to account also for the intuition that understanding a range of empirical facts involves, somehow or other, knowing how those facts were *produced* by the causal-nomological structure of the world. Thus, the thought is that understanding in mathematics is a particular kind of configuration in our epistemic life, and that while understanding in empirical cognition is also a configuration of that kind, it is one acquired in virtue of knowing some range of facts that can only be characterized by appealing to metaphysical notions like *causation* or *law of nature*.

2.0 SOLVABILITY OF POLYNOMIAL EQUATIONS

In this chapter, we will compile the mathematical database for the analysis to be undertaken in Chapter 3. I will discuss two markedly different approaches to the solvability of polynomial equations by radicals. In particular, I will examine two proofs of a crucial result in this area, the fact that the general polynomial equation $\mathbf{p}_5(x) = 0$ of degree 5 is not solvable by radicals.

2.1 BACKGROUND

Polynomial equations and their solutions have always been among the foremost objects of interest in mathematics. Indeed, until the early 19th century, almost all of mathematics aside from geometry consisted of the study of polynomial equations, and they remain the lifeblood of areas such as abstract algebra, geometry, and number theory.

The intellectual context for my case study is furnished by two fundamental facts.

Fundamental Theorem of Algebra *Let*

$$\mathbf{p}(x) = x^n + a_1 x^{n-1} + ... + a_{n-1} x + a_n$$

be any polynomial with coefficients $a_1, ..., a_n$ *in the rational numbers* $\mathbf{Q}$. *Then the polynomial equation* $\mathbf{p}(x) = 0$ *has n solutions in the complex numbers* $\mathbf{C}$.

The first proof of this theorem now considered rigorous was given by Gauss in his 1799 doctoral dissertation.[4] There is the complication that sometimes the solutions may not be *distinct*, but this wrinkle will not concern us here.

The second fundamental fact is that there exists a *general formula for a solution by radicals* for polynomial equations of degrees 2, 3, and 4 each. For example, let $\mathbf{p}(x) = x^2 + bx + c$ be any polynomial of degree 2 with rational coefficients b and c, and consider the equation

$$x^2 + bx + c = 0.$$

We know that the two solutions of this equation, call them x_1 and x_2, can be expressed in terms of the *coefficients* of $\mathbf{p}(x)$ by using the familiar formulae:

$$x_1 = (-b + (b^2 - 4c)^{1/2})/2, \qquad x_2 = (-b - (b^2 - 4c)^{1/2})/2.$$

[4] The history of attempted proofs of the **Fundamental Theorem of Algebra** is complex, and it is difficult to say who really has the priority here. Suffice it to say that there had been earlier proofs which, if transposed into conceptually mature modern settings appropriate to their respective approaches, would be very nearly correct, and that even Gauss' 1799 proof would have to be amended slightly to count as fully rigorous. Gauss distinguishes himself here by the fact that he went on to give three more proofs of the **Fundamental Theorem** and his second proof, one of two he gave in 1816, is certainly correct even by modern standards. See Ebbinghaus *et al*, *Numbers*, pp. 97-109.

Notice that the formulae for x_1 and x_2 above only involve the field operations (*addition*, *subtraction*, *multiplication* and *division*) and the operation of *extracting the square root*, applied to the coefficients of the polynomial. An expression of the form $\mathrm{A}^{1/n}$ is called a *radical* of degree n and hence, it is customary to describe our second fundamental fact by saying that there exists a general formula for a *solution by radicals* for polynomial equations of degrees 2, 3, and 4.

Given these two fundamental facts, it is natural to ask whether there exists a general formula for a solution by radicals for polynomial equations of degree n,

$$\mathbf{p}(x) = x^n + a_1 x^{n-1} + \ldots + a_n = 0,$$

when $n > 4$; that is, whether, for a given degree $n > 4$, there exists a family of expressions $\beta_1, \ldots, \beta_n$, where each β_i involves only the coefficients of $\mathbf{p}(x)$, the field operations and the operation of extracting roots (possibly of degree greater than 2), such that

$$\beta_i^n + a_1 \beta_i^{n-1} + \ldots + a_n = 0,$$

for each $i = 1, \ldots, n$. This question can be naturally phrased by considering the *general polynomial equation* of degree n:

$$\mathbf{p}_n(x) = x^n + a_1 x^{n-1} + a_{n-1} x + a_n = 0$$

where the coefficients are considered *independent variables* with values in $\mathbf{Q}$. It is easy to see that there exists a general solution formula for equations of degree n if and only if the general equation of degree *n* is solvable by radicals. For when we treat the coefficients of the general equation as independent variables, we are in effect assuming that there are no nontrivial arithmetic relations between those coefficients. Hence, on the one hand, a general solution formula will, as such, express the solution of the general equation. On the other hand, a solution of the general equation will specialize to express the solutions of any particular polynomial equation upon substituting numerical values for the variables that are the coefficients of the general equation.

That there exists a general formula for a solution by radicals for polynomial equations of degrees 2, 3 and 4 each was known by the mid 16th century.[5] The 18th century saw a sequence of attempts to find such a general formula for equations of degree 5, but none succeeded. While it was known that there are particular kinds of equations of degrees 5 and greater that have a solution by radicals, gradually the feeling began to emerge that there may be no general formula for degrees greater than 4.[6] Thus, the basic challenge for the algebraists of the early 19th century was to either find such a formula or else, show that none exists. Should it turn out that there is no general formula for a solution by radicals for equations of degree 5, it would be an easy consequence that no such formula exists for any of the degrees greater than 5, either.

[5] The formula for equations of degree 2 was discovered by Arab mathematicians around 900 CE. The formula for equations of degree 3 was discovered by del Ferro in the early 16th century, and independently by Tartaglia (by 1535); the formula was published by Cardan in his monumental *Ars Magna* (1545). *Ars Magna* also contains the formula for equations of degree 4 discovered by Ferrari around 1540. See, for example, Fenrick, *Introduction to the Galois Correspondence*, p. *v*.

[6] See, for example, Kiernan, p. 44.

2.2 UNSOLVABILITY OF THE QUINTIC

Here, then, is the fact that will occupy us for the rest of this essay: *there is no general formula for a solution by radicals for polynomial equations of degree* 5; again, this is equivalent with the fact that *the general polynomial equation* $\mathbf{p}_5(x) = 0$ *of degree* 5 *is not solvable by radicals*. I will adopt the phrase standard in mathematical parlance and say that *the quintic is unsolvable*.

The first proof of the unsolvability the quintic now considered complete was given by the Norwegian Niels Henrik Abel. He recorded a highly condensed version of his argument in a self-published pamphlet in 1824; a fuller version appeared two years later in the inaugural volume of *Journal für die reine und angewandte Mathematik.*[7] Abel's proof was considered very difficult by his contemporaries, and there was no consensus as to whether it was correct until Hamilton carefully reconstructed it in his reports to the Royal Irish Academy in 1839 and 1841—ten years after Abel's death from poverty.[8]

Ivo Radloff has recently rearticulated the 1826 version of Abel's proof in modern terms; this should be considered a valuable scholarly achievement. As Radloff makes clear, Abel's proof is in fact correct and conclusive, save only for a couple of minor amendments that make explicit certain assumptions Abel's approach requires. Much of my exposition of Abel's proof

[7] See Kiernan, p. 67.

[8] Hamilton, "On the Argument of Abel" (1839) and "Investigations Respecting Equations of the Fifth Degree" (1841).

will depend on Radloff's rearticulation, even if in a highly processed form; see Ivo Radloff, "Abels Unmöglichkeitsbeweis im Spiegel der modernen Galoistheorie" (1998).

The reason Abel's approach to solvability is not better known is that only a few years after its publication, it was almost completely superseded by a radically different approach, one that was to transform the science of mathematics. This is the approach due to Evariste Galois, after whom the modern approach to solvability, *Galois Theory*, is named. Galois' ideas about the solvability of polynomial equations come to us mainly from unpublished manuscripts and a letter he wrote to a notable French mathematician Auguste Chevalier the night before his death in a duel in 1832.[9] If Abel's proof was considered difficult, Galois' was considered downright obscure—or, more to the point, not considered at all for a decade and a half. In the fullness of time, however, his ideas were recovered from the manuscripts he left behind, and after being refined and clarified by a number of mathematicians in the latter part of the 19th century, they have became part of the bedrock of modern mathematics. In its modern formulation, Galois Theory is considered one of the most beautiful pieces of mathematics known to us.[10]

[9] See, for example, Kiernan, p. 78. Galois published three papers during his lifetime, all in 1830. While the latter two do not have a direct bearing on the issue of solvability by radicals, the first one deals with the solvability of equations of the form $x^m - 1$. These results would find their proper place in Galois' general theory which he never managed to publish. He submitted a paper that contained an exposition of the said general theory to the Academy of France three times; the first two submissions were lost, and the third one was rejected in 1831. See Kiernan, pp. 74-6.

[10] For a mathematically conscientious account of Galois' original approach, see Radloff, "Évariste Galois: Principles and Applications."

It would not be possible here to do justice to all the various ways in which Galois' ideas have influenced the evolution of mathematics. To single out just one of the many pivotal themes Galois introduced, he was the first mathematician to study properties of arithmetic objects like polynomial equations by studying the internal organization of algebraic structures associated with them. In particular, Galois may be regarded as the progenitor of the concept *group* or, at any rate, the concept *group of permutations* of an algebraic system.[11] This concept and its cognates are part of the foundation of modern mathematics. A critical and strikingly modern aspect of Galois' approach is that he made a decisive shift away from considering properties and relations of individual permutations, and focused on properties and relations of groups of permutations. His approach is strikingly modern also in that he was careful to emphasize that his proof of the unsolvability of the quintic was but one *application* of his general theoretical machinery.[12] Finally, Galois was a vocal advocate of the pregnant idea that mathematical theories should seek to identify the "essential properties" of the objects under consideration and the arguments should proceed by reasoning "directly" about those properties, rather than by carrying out heavy symbolic computations.[13] We will return to these ideas time and again in this essay.

[11] For the purposes of this essay, I will take it that Galois did in fact have the mathematical concept *group* in play in his work. It would be a matter of considerable subtlety to make a philosophically informed judgment as to whether this is what we should want to say, however. Certainly Galois 'recognized' many group-theoretic features of the system of permutations of the roots of a polynomial, but at least some of them, arguably, not quite 'directly' or at any rate, not in their full generality. See, for example, Radloff, "Évariste Galois: Principles and Applications."

[12] See Kiernan, p. 42 and pp. 72-9.

[13] See especially Kiernan, p. 92 and Gray, p. 236.

I will in my case study contrast Abel's approach to solvability by radicals with what I will call "Artin's approach." This is just the standard, conceptually mature modern form of the approach initiated by Galois. While a number of mathematicians made critical contributions to this approach in the late 19th and early 20th centuries, its definitive articulation was given by Artin in his famous 1942 monograph *Galois Theory.*[14] Thus, "Artin's approach" is a misnomer, but a harmless one, given that the details of the actual historical evolution of this approach are irrelevant for my purposes. Since I want to bring out the contrast between the two approaches as clearly as possible, I will focus on the most fully developed form of the approach first initiated by Galois, and that form was given to us by Artin.

There is a significant difference in the *scope* of applicability of the approaches of Abel and Artin we should note from the start. The resources of Abel's approach are sufficient for showing that the quintic is unsolvable, but it gets no grip *at all* on the solvability of *special polynomial* equations, ones with actual numerical coefficients. The resources of Artin's approach, in contrast, yield a general theory of solvability by radicals that applies uniformly to special as well as general polynomial equations. It is for this reason that Artin's approach can, while Abel's can not, be applied *in a uniform way* to address a wide range of well-known classical problems, including certain famous geometric construction problems such as the trisection of an arbitrary angle, the duplication of an arbitrary cube, and the constructibility of the regular polygons.[15] For it turns out that these problems can be translated into problems about the solvability or not of various special polynomials. For example, Galois Theory yields a complete

[14] Emil Artin, *Galois Theory* (Notre Dame Mathematical Lectures, Number 2. Notre Dame: Notre Dame University Press).

[15] See, for example, Fenrick, pp. 163f.

classification of the natural numbers *n* for which a regular polygon with *n* sides is constructible. While the resources of Abel's approach (or, at any rate, pre-Galois Theoretic resources) do allow us to address some of these problems, it is clear from the outset that Artin's approach has greater epistemic power in the sense that it allows us to *prove more*. Here, however, I am not interested in this aspect of the situation: I only want to compare the character of the proofs of the unsolvability of the quintic under the two approaches. For it is in this way we can bring into focus the differences as well as the similarities in just how the two approaches function epistemically.

2.3 ARTIN'S APPROACH

Let $\mathbf{p}(x)$ be any polynomial, general or special. Artin shows that the equation $\mathbf{p}(x) = 0$ is solvable by radicals if and only if the so-called Galois group of $\mathbf{p}(x)$ has the property of being a *solvable group*. He can then easily show that the general equation $\mathbf{p}_5(x) = 0$ of degree 5 is not solvable by radicals because the Galois group of $\mathbf{p}_5(x)$ is not solvable.[16]

Synopsis

Given a polynomial $\mathbf{p}(x)$, we can naturally associate with it two algebraic structures called the *ground field* F and the *splitting field* E; F is the smallest field that contains the coefficients of $\mathbf{p}(x)$, and E is the smallest field that contains F and all the *roots* of $\mathbf{p}(x)$, that is, all the *solutions* of the equation $\mathbf{p}(x) = 0$. The definition of *field* can be found in **Appendix A**; for example, the rational numbers **Q** are a field that is contained in the field of real numbers **R**, and **R** is in turn contained in the field of complex numbers **C**. All the fields we will consider contain **Q** and are contained in **C**; as such, they are infinite structures with enormously rich internal organization.

If a field K_2 contains another field K_1, we say that K_2 is a *field extension* of K_1, denoted K_2/K_1. If a third field K is contained in K_2 and contains K_1, we say that K is an *intermediate field* of the extension K_2/K_1.

[16] Virtually any modern textbook on abstract algebra has an account of the basic components of Galois Theory. I have used Grillet, *Algebra* as my primary reference.

It is easy to show that a polynomial equation **p**(x) = 0 is solvable by radicals if and only if the splitting field E of **p**(x) is contained in an extension field L of the ground field F that has a certain structural property called being a *radical extension*. This is a property of the system of intermediate fields of L/F. Under certain assumptions, the fact that E/F is contained in a radical extension implies that E/F is itself a radical extension, though this is not in general true and not essential to the theory.

The epistemically critical component of Artin's approach is to associate with the splitting field extension E/F another algebraic structure, the *Galois group* G(E/F) of **p**(x). Galois groups are particular kinds of *groups*; the definition of *group* can again be found in **Appendix A**. For example, the integers **Z** are an infinite group, while the Galois groups in our case study will be *finite* groups and, crucially, will have much simpler internal organization than the field extensions with which they are associated.

If a group G contains another group H, we say that H is a *subgroup* of G. The centerpiece of Artin's approach is the so-called **Main Theorem of Galois Theory** that establishes a *bijective correspondence* between the intermediate fields of the splitting field extension E/F and the subgroups of the Galois group G(E/F) for any polynomial **p**(x). In particular, this correspondence is set up in such a way that E/F has the property of being contained in a radical extension if and only if G(E/F) has a certain property called being a *solvable group*. Being a solvable group is a property of the system of subgroups of the group G(E/F) just as being a radical extension is a property of the system of intermediate fields of the extension L/F.

Since the groups that occur as Galois groups in our case study are finite and have much simpler internal organization than the corresponding field extensions, the task of determining whether a given polynomial equation $\mathbf{p}(x) = 0$ is solvable by radicals now becomes much more manageable.

In particular, it is quite easy to determine what the Galois group of the general equation $\mathbf{p}_5(x) = 0$ of degree 5 is, and easy to show that this group is not solvable. Thus, the proof that the quintic is unsolvable is an easy application of Artin's approach or, if you prefer, an easy application of Galois Theory.

It is worth emphasizing that the proof of the unsolvability of the quintic is just one in a *vast* range of applications of Galois Theory. Many areas of modern mathematics are organized by the technique of associating with a field extension K_2/K_1 its Galois group G and using the group-theoretic properties of G to study the field-theoretic properties of K_2/K_1. What makes this technique so useful is the dual circumstance that all kinds of mathematical concerns give rise to field extensions, and that groups lend themselves to be studied in all kinds of theoretically powerful ways. Thus, the **Main Theorem of Galois Theory** plays a constitutive role in the organization of areas such as abstract algebra, number theory, geometry, topology and mathematical physics. It is a *good* thing.

2.3.1 Artin's Proof of the Unsolvability of the Quintic

This subsection contains a detailed account of the proof of the unsolvability of the quintic under Artin's approach. Its principal function is to serve as the first part of the database for my philosophical analysis and it can be skipped without a serious loss of continuity.

Stage 1 Our aim at this stage is to formulate a criterion for solvability by radicals. Let **Q** be the field of rational numbers and let **A** be an *algebraic closure* of **Q**; this is by definition a field that contains all the roots of all polynomials with coefficients in **Q**. The field **A** is contained in the field of complex numbers **C** and is *algebraically closed*: every polynomial with coefficients in **A** has all its roots in **A**. All the other fields considered in the theory will be contained in **A** and will in turn contain **Q**.

Let K_1 be an intermediate field of **A**/**Q**, and consider a polynomial $\mathbf{p}(x)$ in $K_1[x]$, that is, a polynomial whose coefficients are in K_1.[17] It is easy to show that **A** is also the algebraic closure of K_1 and hence, **A** contains all the roots of $\mathbf{p}(x)$.

Much as an integer can be *factored* into a product of prime numbers in the ring of integers **Z**, the polynomial $\mathbf{p}(x)$ can be factored into a product of linear factors in the ring $\mathbf{A}[x]$: if $x_1, ..., x_n$ are the roots of $\mathbf{p}(x)$, then

$$\mathbf{p}(x) = c(x - x_1)(x - x_2) \ ... \ (x - x_n) = cx^n + ca_1x^{n-1} + ... + ca_n,$$

where the coefficients a_i are the so-called *elementary symmetric functions* of the roots: for example, $a_1 = - \ (x_1 + ... + x_n)$, $a_n = (x_1 \times ... \times x_n)$, while the other a_i's are sums of products with fewer than n factors. We may assume for convenience that the leading coefficient $c = 1$ as this will not affect the roots. Note that the factors $(x - x_i)$ need not be distinct.

[17] This is the ring of all polynomials with coefficients in the field K_1; see Appendix A.

Given a field K_1 contained in **A**, some of the roots x_i may not lie in K_1, in which case $\mathbf{p}(x)$ will not factor all the way down to factors of the form $(x - x_i)$ in the ring $K_1[x]$, but will have factors of degree greater than one. If K_1 contains none of the roots, then $\mathbf{p}(x)$ has no non-trivial factors in $K_1[x]$ and we say that $\mathbf{p}(x)$ is *irreducible over* K_1.

One of the fundamental facts about a field extension K_2/K_1 is that K_2 is a *vector space* over K_1 and as such, has a *basis* $\{b_1, b_2, ...\}$ over K_1 so that any element of K_2 can be written in the form $a_1b_1 + a_2b_2 + ...$ with the b_i in K_2 and the a_i in K_1. We will focus on extensions that are *finite* in the sense that any basis of K_2 over K_1 is finite. In this case, there exists an element c of K_2 such that $\{1, c, c^2, ..., c^{n-1}\}$ is a basis for K_2 over K_1; in particular, any element of K_2 can be written as a *polynomial* $a_1c^{n-1} + ... a_{n-1}c + a_n$ for some a_i in K_1. Such c is called a *primitive element* of K_2 over K_1, and the extension K_2/K_1 is called *simple*; we write $K_2 = K_1(c)$. This notation is extended inductively so that $K_1(c_1, ..., c_n) = K_1(c_1)(c_2)...(c_n)$. Note that the elements in the parentheses do not constitute a basis for K_2 over K_1, but rather a set of *generators*; in general a basis would include *powers* of these elements.

Any finite extension K_2/K_1 has the important property of being *algebraic*: each e in K_2 satisfies a polynomial equation $\mathbf{p}(x) = 0$ with $\mathbf{p}(x)$ in $K_1[x]$. It is not hard to show that, in particular, for each e in K_2 there is a unique polynomial $\mathbf{m}_e(x)$ in $K_1[x]$ *irreducible over* K_1 whose leading coefficient is 1 and $\mathbf{m}_e(e) = 0$; it is called the *minimal polynomial of e* over K_1 and plays a central role in Artin's approach.

A field extension K_2/K_1 is called a *simple radical extension* if there exists an element r in K_2 such that (1) $K_2 = K_1(r)$, and (2) the m-th power r^m of r is in K_1 for some positive integer m (even though r *itself* is not in K_1). This means that each element in K_2 is of the form $a_1r^{m-1} + a_2r^{m-2} + ... + a_{m-1}$ with the a_i in K_1. We say that r is an *m-th order radical over* K_1.

A field extension K_2/K_1 is called a *radical extension* if it can be 'built up' from simple radical extensions: there exist elements $r_1, ..., r_n$ in K_2 and positive integers $m(1), ..., m(n)$ such that (1) $K_2 = K_1(r_1, ..., r_n)$, and (2) $r_1^{m(1)}$ is in K_1 and $r_i^{m(i)}$ is in $K_1(r_1, ..., r_{i-1})$ for $i = 2, ..., n$. Thus, there is in K_2 a sequence of simple radical extensions

$$K_1 \subset K_1(r_1) \subset K_1(r_1)(r_2) \subset ... \subset K_1(r_1)(r_2)\ldots(r_n) = K_2;$$

I will call such a sequence a *radical sequence* from K_1 up to K_2.

Given a polynomial $\mathbf{p}(x)$ of degree n in $F[x]$, the *splitting field* E of $\mathbf{p}(x)$ over F is the smallest field that contains F and all the n roots of $\mathbf{p}(x)$; thus, $F \subseteq E \subseteq \mathbf{A}$ and $\mathbf{p}(x)$ splits into linear factors in $E[x]$; indeed, E is just the field $F(x_1, ..., x_n)$ generated by the roots of $\mathbf{p}(x)$ in $\mathbf{A}$.

We can now formulate a criterion for solvability by radicals:

> *A polynomial equation* $\mathbf{p}(x) = 0$ *with* $\mathbf{p}(x)$ *in* $F[x]$ *is solvable by radicals if and only if the splitting field* E *of* $\mathbf{p}(x)$ *is contained in a radical extension* L *of* F.

While this is little more than a rearticulation in field-theoretic terms of what it means to be solvable by radicals, it turns out to be crucially important to Artin's approach. Indeed, we will see how conceptual rearticulation of an arithmetic property, while in and of itself almost trivial, can open up an algebraically organized theoretical approach that is extremely powerful.

I will now outline a proof of this criterion. The next two paragraphs may be skipped without loss of continuity.

On the one hand, suppose the splitting field E of **p**(x) is contained in a radical extension L of F. We then have a tower of simple radical extensions $F = F_0 \subset F_1 \subset ... \subset F_n = L$, with $E \subseteq L$, and so each element in E, including the solutions of **p**(x) = 0, can be expressed in the form

$$a_1 r^{m(n) - 1} + a_2 r^{m(n) - 2} + ... + a_{m(n) - 1} \qquad (*)$$

where $a_1, ..., a_{m - 1}$ are in $F_{n - 1}$ and r is an $m(n)$-th order radical over $F_{n - 1}$. Since $r^{m(n)}$ is in $F_{n - 1}$, each term in (*) can be written as

$$a_i(r^{m(n)})^{(m(n) - i)/m(n)},$$

which is a radical over $F_{n - 2}$. This process can be repeated, so that each element in E, including the solutions of **p**(x) = 0, can be expressed as nested radicals over F. This is what it means to be solvable by radicals.

On the other hand, suppose that **p**(x) = 0 is solvable by radicals. Each element of the splitting field E of **p**(x) can be expressed in terms of the roots of **p**(x), since E is by definition generated over F by those roots. But since **p**(x) = 0 is solvable by radicals, the roots of **p**(x) can be expressed as nested radicals over F. Thus, these radicals generate a radical extension L of F that contains E.

Stage 2 The overall aim now is to determine whether the splitting field extension E/F of the general polynomial $\mathbf{p}_5(x)$ of degree 5 is contained in a radical extension. So we need some way of testing a field extension for this property.

We now come to the key insight in Artin's proof. Given a field extension K_2/K_1, we can associate with K_2/K_1 the *Galois group* $G(K_2/K_1)$ of K_1-automorphisms of K_2; this is the group of all field automorphisms ρ of K_2 that leave K_1 fixed pointwise in the sense that $\rho(x) = x$ for all x in K_1; the group operation is just the composition of mappings. The idea now is to set up a *correspondence* between the intermediate fields of K_2/K_1 and the subgroups of $G(K_2/K_1)$ in such a way that the property of being a *radical extension* of the system of intermediate fields of K_2/K_1 is reflected by some highly tractable property of the system of subgroups of $G(K_2/K_1)$.

This is exactly what Artin achieves. It turns out, first, that for any extension K_2/K_1 with a property called being *normal*, there is a *bijective* correspondence between the intermediate fields of K_2/K_1 and the subgroups of $G(K_2/K_1)$. There are many different ways of characterizing this property; the ones most directly relevant to the issue of solvability by radicals are that (*a*) an extension K_2/K_1 is normal if and only if K_2 is the *splitting field* of some polynomial in $K_1[x]$; and (*b*) given any element t of K_2, *all the roots* of the minimal polynomial $\mathbf{m}_t(x)$ of t over K_1 are contained in K_2; that is, K_2 contains all the roots of $\mathbf{m}_t(x)$ in the algebraic closure of K_1.

Being normal is a mathematically 'natural' property of extensions, one that allows us to execute arguments we would intuitively think should go through; indeed, as (*b*) suggests, it may be thought of as a kind of K_1-*relative completeness property* of K_2.

The said bijective correspondence is now set up as follows. Let K_2/K_1 be a normal extension. On the one hand, given an intermediate field K of K_2/K_1, we associate with K the Galois group $G(K_2/K)$; it is immediate from the definitions that this group is a subgroup of the Galois group $G(K_2/K_1)$. On the other hand, given a subgroup H of $G(K_2/K_1)$, we associate with H its *fixed field* K_2^H in K_2. This is the set of all elements of K_2 that are fixed pointwise by all the K_1-automorphisms in H. It is again immediate from the definitions that this set is in fact an intermediate field of the extension K_2/K_1. The heart of the proof of the **Main Theorem of Galois Theory** consists of showing that these mappings are mutually inverse, so that each one is one-to-one and onto.

Thus, we can finally state the striking

Main Theorem of Galois theory *Let* K_2/K_1 *be a normal extension*.

(*i*) *If* K *is an intermediate field of* K_2/K_1, *then* K *is the fixed field of* $G(K_2/K)$; *in particular*, K_2/K *is a normal extension*.

(*ii*) *If* H *is a subgroup of* $G(K_2/K_1)$, *then* H *is the Galois group* $G(K_2/K_2^H)$; *in particular*, K_2/K_2^H *is a normal extension*.

(*iii*) *The maps* $K \to G(K_2/K)$ *and* $H \to K_2^H$ *are mutually inverse inclusion-reversing bijections between the lattice of intermediate fields of the extension* K_2/K_1 *and the lattice of subgroups of its Galois group* $G(K_2/K_1)$; *that is*, *we have*

$$\begin{tikzcd}
K_2 \arrow[r, leftrightarrow] & G(K_2/K_2) = \{1\} \\
\cup & \cap \\
K \arrow[r, leftrightarrow] & G(K_2/K) \\
\cup & \cap \\
K_1 \arrow[r, leftrightarrow] & G(K_2/K_1).
\end{tikzcd}$$

(*iv*) K/K_1 *is normal if and only if* $G(K_2/K)$ *is a normal subgroup of* $G(K_2/K_1)$ *and if so*, $G(K/K_1) \approx G(K_2/K_1)/G(K_2/K)$.

I will now briefly discuss three lemmas that constitute the heart of the proof of the **Main Theorem**. This subsection may be skipped without a loss of continuity.

Lemma 1 *Let* K_2/K_1 *be a normal extension. Then* K_1 *is the fixed field of* $G(K_2/K_1)$.

It is clear from the definitions that K_1 is contained in the fixed field of $G(K_2/K_1)$; this lemma says that if K_2/K_1 is a normal extension, then the fixed field of $G(K_2/K_1)$ is *no larger* than K_1 itself. Thus, the map $H \rightarrow K_2/K_2^H$ is the inverse of $K \rightarrow G(K_2/K)$.

Lemma 2 (Artin) *Let* E *be a field*, G *a finite group of automorphisms of* E.

Then E/E^H *is a normal extension and* $G(E/E^G) = G$.

It is clear from the definitions that the group G is contained in $G(E/E^G)$; this lemma says that E/E^G is indeed normal, and that $G(E/E^G)$ is no larger than G itself. Thus, the map $K \rightarrow G(K_2/K)$ is the inverse of $H \rightarrow K_2/K_2^H$. One could regard this lemma as the core of Galois Theory.

One of the nice things about the property of being normal is that it is inherited by extensions contained in a normal extension:

Lemma 3 *Let* K_2/K_1 *be a normal extension and let* K *be an intermediate field of* K_2/K_1. *Then* K_2/K *is a normal extension also.*

This lemma is required to apply **Lemma 1** to the intermediate fields of a given normal extension K_2/K_1 in the proof of the **Main Theorem**. The thing to note here is that the 'bottom' extension K/K_1 need *not* be normal even if the ambient extension K_2/K_1 is. Part (*iv*) of the **Main Theorem** addresses this issue: the extension K/K_1 is normal if and only if the Galois group $G(K_2/K)$ is a 'normal' subgroup of $G(K_2/K_1)$.

We now have two basic components in play. On the one hand, we know that a polynomial equation $\mathbf{p}(x) = 0$ is solvable by radicals if and only if the splitting field E of $\mathbf{p}(x)$ is contained in a radical extension L of F, and we know the **Main Theorem**: for any normal extension K_2/K_1, there is a bijective correspondence between the intermediate fields of K_2/K_1 and the subgroups of $G(K_2/K_1)$. Thus, there are three basic challenges. First, in the situation where E is the splitting field of a polynomial contained in a radical extension L of F, we need to make sure that we have enough normal extensions in play to apply the **Main Theorem**; second, given the **Main Theorem**, we need to determine what property of the system of subgroups of G(L/F) corresponds to the property of there being a radical sequence in L/F. Finally, the natural aim is to show that the group G(E/F) has this property also. As I noted in the foregoing synopsis, the result turns out to be that a polynomial equation $\mathbf{p}(x) = 0$ is solvable by radicals if and only if the Galois group G(E/F) of the splitting field extension E/F of $\mathbf{p}(x)$ has the structural property of being a solvable group. I will not give a complete proof this result here, but I will indicate how the foregoing three challenges are met. There are four main steps.

(1) Suppose L/F is a radical extension and, as such, contains a radical sequence. Since a radical sequence consists of simple radical extensions, the first thing to examine is a simple radical extension $F(r)/F$. There are two questions here: is the extension $F(r)/F$ normal, and what does the group $G(F(r)/F)$ look like? As to the first, suppose that r is an m-th order radical over F,

so that r^m is in F. Then F(r)/F is a normal extension provided that F contains a primitive m-th root of unity. Thus, in order to apply the **Main Theorem**, we will need to adjoin such m-th root to the field of coefficients of **p**(x), and so the proof will involve considering intermediate extensions of L/F other than F(r)/F itself. Second, when this condition is satisfied, we find that G(F(r)/F) is a finite abelian group: one such that for any s and t in G, $s + t = t + s$.[18]

(2) The most obvious thing one would hope to do now is to apply the foregoing result to the simple radical extensions that constitute a radical sequence in L/F. In particular, in view of part (*iv*) of the **Main Theorem**, we would hope to show that G(F(r)/F) ≈ G(L/F)/G(L/F(r)). In order to do this, however, we need to make sure that the extension L/F is itself normal. Now this is not in general true, but it turns out that we can always replace L with a field N that is a finite radical extension of F and is normal over F. Finally, we will see that if G(N/F) has the property of being a solvable group, then so do G(L/F) and G(E/F). Thus, we may assume without loss of generality that G(L/F) is normal.

(3) The upshot of these considerations is that if L/F is a normal radical extension, the Galois group G(L/F) contains a sequence of subgroups

$$\{1\} = H_1 \subset \ldots \subset H_k = G(L/F),$$

where H_{i-1} is normal subgroup of H_i and the quotient group H_i/H_{i-1} is abelian; a sequence of this form is called a *normal series with abelian quotients*, and a group that contains one is, again,

[18] In fact even more is true: in the situation under consideration, F(r)/F is a *cyclic* group, the simplest kind of abelian group, but we will not need this feature in our analysis.

called *solvable*. Thus, our first result is that if L/F is a radical extension, then the Galois group G(L/F) is solvable.

The proof of this result is somewhat delicate, and I will not reproduce it here. Again, there are two principal complications: first, we would need to consider intermediate extensions of L/F that result from adjoining to F the requisite roots of unity; second, we would need to show that L/F may be assumed to be a normal extension. Indeed, we will see in our discussion of Abel's approach that, in order for his proof to go through, we must take him to be assuming that the requisite roots of unity are already contained in the ground field F. With this assumption in force, a stronger result is available: not only is E contained in a radical extension of F, E/F is *itself* a radical extension.

(4) Once it is established that G(L/F) is a solvable group, it is easy to show, first, that G(L/E) is a solvable group also. For it is immediate from the definitions that G(L/E) is a subgroup of G(L/F) and an easy group-theoretic fact that any subgroup of a solvable group is solvable. It is then easy to show that G(E/F) itself is solvable, as desired. For first, the splitting field extension E/F is normal (see above), and so by part (*iv*) of the **Main Theorem**, we have G(E/F) ≈ G(L/F)/G(L/E); but it is another easy group-theoretic fact that a quotient group of any solvable group by a normal subgroup is solvable.

The converse is also true: if G(E/F) is a solvable group, then E is contained in a radical extension of F. Thus, we have the following criterion for solvability by radicals:

> *A polynomial equation* $\mathbf{p}(x) = 0$ *is solvable by radicals if and only if the Galois group* G(E/F) *of the splitting field extension* E/F *of* $\mathbf{p}(x)$ *is a solvable group*.

I will not address the converse result here, however, since it is the first one that matters for our purposes: in order to show that a polynomial equation $\mathbf{p}(x) = 0$ is *not* solvable by radicals, it suffices to show that the Galois group G(E/F) of the splitting field extension E/F is *not* a solvable group.

Stage 3 The aim now is to compute the Galois group of the general polynomial $\mathbf{p}_5(x)$ of degree 5 and show that this group is not solvable.

Let $a_1, ..., a_5$ be five independent variables with values in $\mathbf{Q}$; then the general polynomial of degree 5 is

$$\mathbf{p}_5(x) = x^5 + a_1 x^4 + a_2 x^3 + a_3 x^2 + a_4 x + a_5,$$

again assuming without loss of generality that the leading coefficient is 1. Suppose now that $x_1, ..., x_5$ are the five roots of $\mathbf{p}_5(x)$; these are essentially just formal symbols, subject only to the condition that the five symmetric functions in them equal the five coefficients. For by definition of root, we must have $\mathbf{p}_5(x) = (x - x_1) \ldots (x - x_5)$ and by multiplying out the product on the right, we would see that the coefficients are the five elementary symmetric functions of the roots. Thus, the splitting field E of $\mathbf{p}_5(x)$ is just the field of rational functions $\mathbf{Q}(x_1, ..., x_5)$, and the ground field F is $\mathbf{Q}(a_1, \ldots, a_5)$.

So now we only need to determine the Galois group of the extension E/F, but this task turns out to be trivial. For first, since there are no non-trivial arithmetic relations between the roots of $\mathbf{p}_5(x)$, *any* permutation of the roots extends by linearity to a mapping on E, one that is easily shown to be an automorphism of E. Second, since the coefficients are symmetric functions of the roots, any such automorphism leaves them all fixed. Hence, the Galois group G(E/F) is (isomorphic to) the full symmetric group $\mathbf{S}_5$, the group of all permutations on five letters.

We are now almost done: we only need to determine whether $\mathbf{S}_5$ is a solvable group. But simple group-theoretic considerations show that any normal series in $\mathbf{S}_5$ must begin with the unique normal subgroup of index 2, the alternating group $\mathbf{A}_5$. However, since $\mathbf{A}_5$ is a non-abelian simple group (a group that has no proper normal subgroups), the only possible normal series in $\mathbf{A}_5$ would be $\{1\} \subset \mathbf{A}_5$, and the quotient $\mathbf{A}_5/\{1\} = \mathbf{A}_5$ is not abelian.

Thus, we now know that there is no normal series with abelian quotients in $\mathbf{S}_5$ and hence, $\mathbf{S}_5$ is not a solvable group. By the criterion for solvability noted above, this implies that $\mathbf{p}_5(x) = 0$ is not solvable by radicals.

It follows at once that the general polynomial equation of any degree n with $n > 5$ is not solvable by radicals. For, suppose that we had a solution formula ϕ, only involving the coefficients $a_1, ..., a_n$, of

$$\mathbf{p}_n(x) = x^n + a_1 x^{n-1} + ... + a_{n-1} x + a_n = 0.$$

We could then put $a_6 = 0, ..., a_n = 0$, and the formula ϕ would specialize to give a solution by radicals in terms of $a_1, ..., a_5$ of

$$\mathbf{p}_n(x) = x^n + a_1 x^{n-1} + ... + a_{n-5} x^{n-5} = 0.$$

But, dividing this expression by x^{n-5}, we obtain the general equation of degree 5, and clearly ϕ would then yield the solutions of that equation, a contradiction.

2.4 ABEL'S APPROACH

The most immediately obvious difference between the approaches of Abel and Artin is that where Artin's proof turns on first associating with the polynomial its splitting field and with the splitting field its Galois group, Abel directly examines the possible formulae for a solution by radicals for the general equation $\mathbf{p}_5(x) = 0$ of degree 5 and shows that no such formula in fact exists. This has the consequence that Abel's proof is much more *computational* than Artin's. In what follows, however, I won't actually be interested in this particular contrast between the two proofs, for reasons I will explain in Chapter 3. Accordingly, I will not in my exposition give a detailed account of the computations on which Abel's proof finally depends. [19]

Synopsis

Just as the first part of Artin's proof, we can view the first part of Abel's proof as identifying a criterion for solvability by radicals. Let $\mathbf{p}_n(x) = 0$ be the general polynomial equation of degree n. By carrying out symbolic computations, Abel obtains a canonical expression for the general form any solution by radicals would have to have. He exploits this canonical expression to show that any term in such a solution would have to be expressible as a *rational function* in the n roots of $\mathbf{p}_n(x)$; for Abel, a rational function is a quotient of two polynomials. In particular, he shows that

[19] Again, I will be using Radloff [1998] as the primary source for my exposition of Abel's proof. I will include a translation of Radloff's paper as **Appendix B**. A brief account of Abel's proof can also be found in Kiernan, pp. 67-72. An annotated translation of Abel's 1824 paper can be found in Appendix A and the first part of the 1826 paper in Appendix B of Pesic, *Abel's Proof*.

the radicals in a solution by radicals would have to be so expressible. Thus, the overall aim of the proof becomes to show that not enough such radicals exist for a solution by radicals to exist in the case $n = 5$.

In the second part of his proof, Abel focuses on the case of the general equation $\mathbf{p}_5(x) = 0$ of degree 5. Now the key point is that the roots of the general equation may be regarded as independent variables. Accordingly, Abel's principal theoretical device is to reason about the *number of values* a rational function in five independent variables can take under the *permutations* of those variables. A *value* of a rational function ϕ under the permutation ρ is simply the particular formal expression that results from applying ρ to the variables in ϕ; two values of ϕ are *distinct* if they are different as formal expressions, except that A + B is considered to be the same expression as B + A and likewise for AB and BA. The crucial idea in Abel's proof is what I will call the **Combinatorial Principle**: if ϕ is a rational function that is also a radical over the ground field F of $\mathbf{p}_5(x)$, then the number of distinct values ϕ has under the permutations of the roots is the same as the number of values ϕ has as a radical over F. The latter number is the degree of the minimal polynomial of ϕ over F; for most purposes, this is just the *order* over F of the radical. Thus, for example, a square root has two values as a radical; a cube root has three, and so on.

Thus, Abel's strategy in the second part of his proof is to identify constraints on the number of possible values a rational function in five independent variables can take, and thereby use the **Combinatorial Principle** to constrain the range of possible orders the radicals in a solution by radicals can have. It is determined that the only (prime) orders that could in principle occur are 2 and 5. Thus, at the end of the second part, Abel goes on to obtain explicit expressions for rational functions that have 2 values and for functions that have 5 values; these expressions are required to rule out certain possibilities in the final part of the proof.

The third part of Abel's proof is a *reductio*. By using the results he has obtained in the second part, he enumerates the possible orders a radical in a solution formula could have, and shows that not enough of those possibilities are realized for there to be a solution by radicals for $\mathbf{p}_5(x)$. He first shows that in order to appear in such a solution, any radical over the ground field F would have to have order 2. He then shows that there are no such radicals at all over the field generated by such an order 2 radical. Both steps involve ruling out possible orders of radicals by showing that any radical of a given order would have a different number of values as a radical than it has as a rational function of the roots, violating the **Combinatorial Principle**.

I take this occasion to point out that, contrary to most popular accounts, it is not compulsory or even very natural to view Abel's proof as a one long *reductio*. The first part of Abel's proof amounts to identifying a criterion for solvability by radicals for general equations, one that is *satisfied* for equations of degrees 2, 3 and 4; no *reductio* here. The second part of the proof is an assemblage of results which, in modern terms, can be understood as being about the structure of the splitting field extension E/F of the general polynomial $\mathbf{p}_5(x)$ of degree 5. These results do not in any way depend on the assumption that $\mathbf{p}_5(x) = 0$ is solvable by radicals; thus, no *reductio* here, either. It is only the third part that involves a number of 'local' *reductios*, but the epistemic yield even of the third part as a whole is a positive result about which radicals there are over the ground field F of $\mathbf{p}_5(x)$. I will revisit this theme in Chapter 4.

2.4.1 Abel's Proof of the Unsolvability of the Quintic

As with my detailed account of Artin's proof of the unsolvability, this subsection can be skipped without a serious loss of continuity.

Stage 1 The overall aim of the first part of Abel's proof is to identify a criterion for solvability by radicals for the general equation $\mathbf{p}_n(x) = 0$ for any degree n. Since Abel anticipates that the equation $\mathbf{p}_5(x) = 0$ of degree 5 is not solvable by radicals, his specific aim is to identify some highly testable consequence of being solvable by radicals.

In the modern approach to solvability, we took the coefficients $a_1, ..., a_n$ of the general polynomial equation of degree n,

$$\mathbf{p}_n(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + ... + a_n = 0,$$

to be independent variables over $\mathbf{Q}$; in Abel's approach one takes the *n solutions* $x_1, ..., x_n$ of $\mathbf{p}_n(x) = 0$ to be independent variables, and *defines* the coefficients $a_1, ..., a_n$ to be the n elementary symmetric functions in the $x_1, ..., x_n$ (see above). The significance of treating the solutions as independent variables will become clear presently. This approach is not substantially different from the modern one, however: we still take E = $\mathbf{Q}(x_1, ..., x_n)$ as the splitting field of $\mathbf{p}_n(x)$ and F = $\mathbf{Q}(a_1, ..., a_n)$ as the ground field.

By carrying out intricate but elementary algebraic manipulations, Abel obtains the following fundamental

Theorem 1 *Any solution by radicals of* $\mathbf{p}_n(x) = 0$ *can be put in the form*

$$y = q_0 + q_1 r^{1/p} + q_2 r^{(2/p)} + \ldots + q_{p-1}\, r^{(p-1/p)}, \qquad (*)$$

where p is some prime number, and $q_0, ..., q_{p-1}, r$ *are functions of the same form as y, and so on, until we come to rational functions of the coefficients* $a_1, ..., a_n$.

Again, a *rational function* for Abel is any function of the form $\mathbf{p}_1(x)/\mathbf{p}_2(x)$, where the $\mathbf{p}_i(x)$ are polynomials. Thus, any solution of $\mathbf{p}_n(x)$ by radicals can be put in a form that contains multiply nested radicals, but after a finite number of nestings, we come to expressions that are rational functions of the coefficients of $\mathbf{p}_n(x)$. Abel further shows that, by making suitable substitutions, one can take $q_1 = 1$.

For example, for the general quadratic equation $\mathbf{p}_2(x) = x^2 + bx + c$, we have $p = 2$ and

$$y = b/2 + (1/2)(b^2 - 4c)^{1/2},$$

so that $q_0 = b/2$, $q_1 = 1/2$, $r = b^2 - 4c$. Since the square root of a real number R has two values, the positive and the negative, we obtain the two familiar solution formulae.

It is *not* known from the outset what the primes p in a solution by radicals would have to be for a given $\mathbf{p}_n(x)$. Some basic constraints may be noted, however. First, there is the very fact that the order of the radicals involved can be taken to be prime: since $(r^{1/m})^{1/n} = r^{1/mn}$, any non-prime order radical could be factored into nested radicals of prime order.

Second, in proving **Theorem 2** (below), Abel shows that the order p of any radical in the solution formula must be less than or equal to n, the order of the equation itself; we see this instantiated in the case of the formulae for $n = 2$, 3, and 4.

Finally, and this is really the key idea of the entire proof, in certain circumstances that arise naturally in considering solvability by radicals, the order p of the radical r is also the *number of distinct values of r as a radical*. In order to explain what this means, note, first, that the notion radical is relative to a field: r is an *m-th order radical over* K if r is not in K but there is some (least) natural number m such that r^m is in K; for example, the square root of 2 is a 2nd order radical over **Q** because $\sqrt{2}$ is not in **Q**, but $(\sqrt{2})^2 = 2$ is in **Q**. Second, this means that an m-th order radical r over K is a solution of the polynomial equation

$$x^m - \mathrm{A} = 0$$

for some A in K; the minimal polynomial $\mathbf{m}_r(x)$ of r over K divides this polynomial and hence, has degree less than or equal to m. The solutions of $\mathbf{m}_r(x) = 0$ are called the *values of r as a radical over K*; given the definition of minimal polynomial, these solutions are distinct. In the situation with which we are concerned, $m = p$ is a prime, $x^p - \mathrm{A} = 0$ itself is the minimal polynomial of r over K, and has p distinct solutions $r, \alpha r, \alpha^2 r, ..., \alpha^{p-1} r$, where α is a primitive p-th root of unity, namely, a solution in **C** of $x^p - 1 = 0$.

Thus, assuming now that the ground field F contains all the requisite roots of unity, *the order of the radical r over F is precisely the number of distinct values of that radical*. It is natural to expect that this might put some constraints on which p can occur as orders of the radicals in the solution formula for $\mathbf{p}_n(x)$. Indeed, what Abel ends up showing is that in the case of $\mathbf{p}_5(x)$, there are not enough primes p for which the required radicals have the right number of values and, hence, not enough primes p for which such radicals exist.

MODERN Let K(r) / K a simple radical extension of degree p, with **Q** contained in K. Abel shows, in effect, that any element v in K(r) can be written in the form

$$v = q_0 + q_1 r + \ldots + q_{p-1} r^{p-1} \qquad (1)$$

for some $q_0, \ldots, q_{p-1}$ in F. Moreover, for v in K(r) – K, one can take $q_1 = 1$, so that we can write any such v in the form

$$v = q_0 + r + \ldots + q_{p-1} r^{p-1} \qquad (2)$$

Now let E = $\mathbf{Q}(x_1, ..., x_n)$ be the splitting field of $\mathbf{p}_n(x)$, and let F = $\mathbf{Q}(a_1, \ldots, a_n)$, where the a_i are the elementary symmetric functions in the x_i. We saw in our discussion of Artin that $\mathbf{p}_n(x) = 0$ is solvable by radicals if and only if E is contained in some radical extension L of F. Thus, under the assumption that $\mathbf{p}_n(x)$ is solvable by radicals, there is a tower of extensions $\mathrm{F} = \mathrm{K}_0 \subset \mathrm{K}_1 \subset \ldots \subset \mathrm{K}_n = \mathrm{L}$ with $\mathrm{E} \subset \mathrm{L}$ and each $\mathrm{K}_i / \mathrm{K}_{i-1}$ a simple radical extension. Hence, any v in $\mathrm{E} - \mathrm{K}_{n-1}$ can be written in the form (2), where the coefficients q are in K_{n-1} and r is a p-th order radical over K_{n-1} for some prime p. Thus, what Abel shows is, in effect, that we can repeat this process for the coefficients and the radicals alike, and by rearranging the terms as necessary, will ultimately arrive at an expression of the form (2) where the coefficients q are in F = $\mathbf{Q}(a_1, ..., a_n)$, and the innermost radicals will be radicals over F. Thus, they will all be rational functions of the coefficients of $\mathbf{p}_n(x)$, as required.

Abel's general expression for a solution by radicals makes it clear that an equation is solvable by radicals only if there are enough primes p for which the required p-th order radicals exist, and as we noted, this can happen only if there are enough primes for which these radicals have a suitable number of values. Thus, it is clear that if the issue of solvability of $\mathbf{p}_5(x)$ can be settled by examining the structure of the foregoing general expression for a solution, then it can be settled by examining the structure of the radicals that would have to appear in such a solution. In particular, the other features of the expression in **Theorem 1** can from here on out be more or less ignored. Hence, what one would like now is a more inferentially engageable representation of the required radicals. Again, given the paucity of Abel's conceptual resources, the only natural device for pursuing this aim is to carry out symbolic manipulations.

Thus, we now come to the result that provides orientation for the rest of Abel's proof: he manages to give a more explicit representation of the individual terms in any solution by radicals and, crucially, a more explicit representation of the radicals therein:

Theorem 2 *If the general polynomial equation* $\mathbf{p}_n(x) = 0$ *is solvable by radicals, then any solution by radicals can be put in such a form that all the terms in it are rational functions of the roots of* $\mathbf{p}_n(x)$.

Note carefully: *rational functions of the roots, not of the coefficients*.

Abel's proof of **Theorem 2** starts from the fact that if

$$y_1 = q_0 + r + \ldots + q_{p-1}\, r^{p-1}$$

is an expression for a solution by radicals of $\mathbf{p}_n(x) = 0$ of the form recorded in **Theorem 1**, and if α is a primitive p-th root of unity, then

$$\begin{aligned} y_2 &= q_0 + \alpha r + \alpha^2 q_2 r^2 + \ldots + \alpha^{p-1} q_{p-1} r^{p-1}, \\ &\ \ldots \\ y_p &= q_0 + \alpha^{p-1} r + \alpha^{p-2} q_2 r^2 + \ldots + \alpha q_{p-1} r^{p-1}. \end{aligned} \tag{3}$$

are also expressions for solutions by radicals of $\mathbf{p}_n(x) = 0$. It is easy to show that these solutions would be *distinct* and hence, p cannot exceed the degree n of the equation, in view of the **Fundamental Theorem of Algebra**: a polynomial equation of degree n has exactly n solutions in its splitting field.

Now comes the crucial step. By employing the elementary fact about roots of unity that

$$\alpha^{p-1} + \alpha^{p-2} + \ldots + \alpha + 1 = 0,$$

Abel solves the system of equations (3) for each term $q_\nu r^\nu$, $\nu = 0, \ldots, p - 1$, to obtain

$$q_\nu r^\nu = (1/p)(y_1 + \alpha^{-\nu} y_2 + \alpha^{-2\nu} y_3 + \ldots + \alpha^{-(p-1)\nu} y_p),$$

where $q_1 = 1$ as before. In particular, for $v = 1$, we have the crucial expression

$$r = (1/p)(y_1 + \alpha^{p-1} y_2 + \ldots + \alpha y_p),$$

where α is a primitive p-th root of unity and the $y_1, ..., y_p$ are distinct roots of $\mathbf{p}_n(x)$. This is the heart of Abel's approach: *any radical that appears in a solution by radicals would have to be a rational function of the roots of* $\mathbf{p}_n(x)$.

By way of clarification, p is the order of the "outermost" radical in the expression for the solution; for example, in the formula for the general equation of degree 2, $p = 2$. More generally, there would be multiply nested radicals and so we would have a sequence of radicals of orders $p_1, ..., p_k$. Thus, the foregoing expressions should not be taken to imply that $\mathbf{p}_n(x)$ has p roots.

MODERN The modern formulation changes the point of view fairly dramatically:

Theorem 2 *Let* $\mathbf{p}(x)$ *be a polynomial with ground field* F *and splitting field* E.

If E *is contained in a radical extension* L *of* F, *then* E *itself is a radical extension of* F, *provided that* F *contains enough primitive roots of unity*.

We already commented on this result in our discussion of Artin's approach.

Abel's proof of **Theorem 2** involves establishing the crucial

Lemma *If v is in* K(r) – K, *the minimal polynomial* $\mathbf{m}_v(x)$ *of v over* K *has p distinct roots* $y_1, \ldots, y_p$, *and*

$$r = (1/p)(y_1 + \alpha^{p-1}y_2 + \ldots + \alpha y_p),$$

where α is a primitive p-th root of unity, *r is a solution of* $x^p - \mathrm{A}$, *and r not in* K.

That the solutions are distinct follows from the irreducibility of x^p – A in view of the following

Proposition 1 *Given a field* K, *either all the roots of* x^p – A *are contained in* K, *or else none of them are*. *That is*, *either* x^p – A *splits into linear factors in* K[x], *or else it is irreducible over* K.

This proposition is not explicitly stated by Abel, but he does employ it implicitly in his proof of what we have called **Theorem 2**. Again, **Proposition 1** requires the assumption that the field K contains enough primitive p-th roots of unity 1, α, α^2, ..., α^{p-1}. The point is that if r is a solution of $x^p - \mathrm{A} = 0$, then αr, $\alpha^2 r$, ..., $\alpha^{p-1} r$ are the other solutions in **C** of x^p – A. Thus, the fact that r is in K entails that the other solutions are in K only if these primitive p-th roots belong to K. Thus, we have here a lapse of rigor in Abel, but in the context of Abel's project, one may assume without loss of generality that K contains the required roots of unity, as we have done. For if **p**(x) is solvable by radicals over some field K, then it is certainly solvable by radicals over a field extension of K obtained by adjoining the requisite roots of unity to K; contrapositively, if **p**(x) is not solvable over the latter field, it is not solvable over K, either.

The proof of **Theorem 2** is the most difficult part of Abel's proof; relying on intricate symbolic computations, it occupies most of the first half of his 1824 paper. At the end of the section addressed to it, Abel remarks that "[**Theorem 2**] being established, it is not hard to complete the demonstration" of the unsolvability of the general equation of degree 5.[20] Indeed, it is clear that Abel has now managed to extract a highly testable consequence of solvability by radicals, one that he could reasonably hope to show leads to a contradiction.

[20] See Pesic, p. 162.

Stage 2 We now know that the radicals that would have to appear in the solution formula can be expressed as rational functions of the five roots of $\mathbf{p}_5(x)$. Clearly the aim now is to exploit this fact to show that not enough such radicals exist.

A crucial bit of Abel's mathematical background now comes into play; the following result used to be known as *Lagrange's theorem*:

Theorem 3 *The number of distinct values a rational function $f(x_1, ..., x_n)$ in n independent variables can take under the permutations of those variables divides the factorial n! of n, namely the product n!* = $n \times (n - 1) \times ... \times 2 \times 1$.

MODERN A rational function v of the roots is just an *element of the splitting field* E of $\mathbf{p}_5(x)$; this is immediate from the definitions. Thus, let v be in E – F and let E(v) be the splitting field of the minimal polynomial of v over F. It is again immediate from the definitions that the distinct values of a rational function v in E are actually just the distinct images of v under the action on E of the Galois group G(E/F), the so-called *conjugates* of v in E. By the **Main Theorem of Galois Theory**, the number of conjugates of v is equal to the index of G(E/E(v)) in G(E/F). But, by the group-theoretic result now known as Lagrange's Theorem, the cardinality of any subgroup H of any group G divides the cardinality of G and so the index #G/#H also divides #G. Hence, the index of G(E/E(v)) divides the cardinality of G(E/F), but the latter group is isomorphic to the group of all permutations of n letters, the symmetric group $\mathbf{S}_n$, whose cardinality is n!.

Theorem 3 may seem like a fairly weak result, and indeed it is as far as Abel's final aim is concerned. Nevertheless, it provides a crucial clue as to how one might go about constraining the range of radicals that could appear in a solution by radicals.

On the one hand, by **Theorem 2**, Abel knows that these radicals can be expressed as rational functions in five independent variables, namely the roots of $\mathbf{p}_5(x)$, and here we have a result that puts a constraint on the number of values such an expression can take under the permutations of the roots. On the other hand, as we explained above, Abel knows that a radical will take some number of distinct values as a radical. This, then, is the crucial point: Abel realizes that *these two numbers must be equal*. We may state this as the following

Combinatorial Principle *Let r in* E *be a radical over* F, *expressed as a rational function $r = f(x_1, ..., x_n)$ of the n roots of $\mathbf{p}_n(x)$; then $f(x_1, ..., x_n)$ has exactly as many distinct values as a rational function under the permutations of $x_1, ..., x_n$ as r has as a radical over* F *in the sense explained above.*

MODERN Again, if E/F is any field extension, the conjugates over F of any e in E are the elements in the orbit of e under the action of G(E/F), the group of E-automorphisms of F. Thus, what is going on here is simply that we have two different ways of representing the conjugates of an element r in E when r happens to be a radical over F.

On the one hand, if r is in E – F and is a radical over F, that is, a solution of $x^p - \text{A} = 0$ with A in F, then $x^p - \text{A}$ is its minimal polynomial over F, and the p distinct roots of this polynomial, $r, \alpha r, \alpha^2 r, ..., \alpha^{p-1}r$ are the values of r as a radical. It is a basic fact in the modern theory of fields that these solutions are precisely the conjugates of r over F. On the other hand, since E = $\mathbf{Q}(x_1, ..., x_n)$ is the splitting field of $\mathbf{p}_n(x)$, any element in E is a rational function of the roots. Finally, since each F-automorphism of E is obtained from some permutation ρ of the roots by extending ρ to all of E by linearity, the conjugates of $e = f(x_1, ..., x_n)$ are obtained by permuting the $x_1, ..., x_n$ among themselves.

Thus, **Theorem 3** and the **Combinatorial Principle** dictate the overall path for the rest of **Stage 2** of Abel's proof: he will try to identify as many constraints as possible on the numbers of values a rational function in 5 independent variables can take, thereby constraining the range of orders of radicals that could appear in a solution by radicals for $\mathbf{p}_5(x) = 0$.

Abel does not state the **Combinatorial Principle** in his 1824 paper.[21] A charitable way of looking at this would be that Abel is implicitly regarding the permutations of the roots as F-automorphisms of the splitting field E and, as such, it is 'clear' that the two ways of counting the conjugates must yield the same answer. In his 1826 paper, however, Abel states the following result in which he recognizes that the values of a rational function *v* in E under the permutations of the roots are the solutions of the minimal polynomial of *v* over F, thereby making the connection between the two ways of representing the orbit of an element in E.

[21] In his careful reconstruction of Abel's proof in the late 1830s, William Hamilton, the inventor of the quaternions, states the **Principle** in the form we have stated it here and, indeed, takes great pains to emphasize its importance.

Theorem 7 *If $v = f(x_1, ..., x_n)$ has m distinct values under the permutations of the $x_1, ..., x_n$, there exists an equation $\mathbf{m}_v(x) = 0$ of degree m that has these values as solutions and whose coefficients are symmetric functions in $x_1, ..., x_n$; moreover, no equation of this form but with degree less than m has any of these values as solution.*[22]

MODERN Let v be in E = $\mathbf{Q}(x_1, ..., x_n)$. **Theorem 7** says that if such v has m field conjugates in E, there exists a polynomial $\mathbf{m}_v(x)$ of degree m with coefficients in F = $\mathbf{Q}(a_1, ..., a_n)$ whose roots are precisely those field conjugates of v, and that no polynomial of degree less than m with coefficients in F has any of these conjugates as a solution; in other words, $\mathbf{m}_v(x)$ is irreducible over F and, indeed, it is just the minimal polynomial of v over F. Finally, recall that the values of r as radical over F are just the solutions of the minimal polynomial of r over F. Thus, **Theorem 7** makes the crucial connection between the two ways of representing the orbit of r. In particular, by **Lemma**, a p-th order radical r over F has precisely p values as a radical. This amounts to the **Combinatorial Principle**. In modern terms, this is essentially a fact about the structure of the extension E/F, and in view of the **Main Theorem of Galois Theory**, indirectly a fact about the subgroup structure of the symmetric group $\mathbf{S}_5$. Note that while Abel presents **Theorem 7** at the end of Section III of his 1826 paper, its proof does not require any of the earlier theorems, and so it could just as well have been stated and proved at the very beginning of the paper.

[22] See **Satz 7** in Radloff [1998], p. 138.

Abel now needs to find further constraints on the number of values a rational function $f(x_1, ..., x_5)$ in five independent variables can take under the permutations of those variables. As it turns out, the tradition of attacks on the solvability of the general equation of degree 5 had made available to Abel just the sort of result needed at this stage: the following **Theorem 4** restricts the range of possible values a rational function can take. Abel gets this result from an 1815 paper of Cauchy's, in which he notes that it is a generalization of a result due to Ruffini from 1804.

Theorem 4 (Ruffini) *For n greater than* 4, *a rational function* $f(x_1, ..., x_n)$ *cannot take* 3 *or* 4 *distinct values under the permutations of the variables* $x_1, ..., x_n$.

MODERN This theorem can be understood as stating a fact about the structure of the splitting field extensions E/F of general polynomials $\mathbf{p}_n(x)$ for degrees greater than 4: no element in E can have exactly 3 or exactly 4 field conjugates. This puts considerable constraints on the system of intermediate fields in these extensions and is, of course, a part of the 'reason' why there is no radical sequence in any such extension for *n* greater than 4.

The following pieces of terminology will come in handy. If a polynomial in *n* variables is invariant under all the permutations in $\mathbf{S}_n$, it is called *symmetric*; if a polynomial is invariant under (at least) all the permutations in the alternating group $\mathbf{A}_n$, it is called *alternating*. Again, any v in E = $\mathbf{Q}(x_1, ..., x_n)$ can be viewed as a polynomial with coefficients in F = $\mathbf{Q}(a_1, ..., a_n)$. Thus, specializing now to the case $n = 5$, we can restate **Theorem 4** as follows:

Theorem 4 *Any v in* E *with fewer than 5 conjugates is either alternating or symmetric.*

For recall that the conjugates of v in E are precisely the elements in the orbit of v under the action of the Galois group G(E/F) which, in our situation, is $\mathbf{S}_5$. Thus, a symmetric v is an element of F; an alternating v is an element of some extension of F of degree 2.

MODERN This means that any intermediate field of the splitting field extension E/F of $\mathbf{p}_5(x)$ that has a prime degree over F must have degree 2 or 5. This is a strong constraint, and certainly suggests that there might not be a radical sequence in E/F.

In sum: by **Lagrange's Theorem**, the number of values of $f(x_1, ..., x_5)$ divides 5!. If this number is a prime (or 1), the possibilities are 1, 2, 3, and 5, and by **Ruffini's Theorem**, the possibilities are actually just 1, 2, and 5. Finally, Abel knows that if r is a p-th order radical over F, the number of values of r as a radical over F is p and hence, in view of the **Combinatorial Principle**, any prime order radical over F that could appear in a solution by radicals must have order $p = 2$ or $p = 5$.

Note, however, that one might have to consider prime order radicals r over fields that are *extensions* of F = $\mathbf{Q}(a_1, ..., a_5)$; this is clear from the general expression in **Theorem 1**, and in fact already from the known solution formulae for equations of degrees 3 and 4. It is still true, of course, that the order p must be less than or equal to 5. However, such an element r need not be a *radical over the field F* at all: there need be no m such that r^m = A for some A in F. Nevertheless, we can still consider the minimal polynomial $\mathbf{m}_r(x)$ of r over F, although $\mathbf{m}_r(x)$ need not have the form x^p – A and, indeed, may have more than 5 solutions. Thus, **Ruffini's Theorem** need not apply to all the possibilities one has to consider. However, the general principle that the number of solutions of $\mathbf{m}_r(x)$ must equal the number of values of r under the permutations of the roots of $\mathbf{p}_5(x)$ still applies. Some of the crucial contradictions in **Stage 3** will be violations of this general form of the **Combinatorial Principle**.

The most obvious aim now is to find a more inferentially engageable representation of the rational functions with 2 or 5 distinct values. We have, first, the following

Theorem 5 *A rational function $f(x_1, ..., x_5)$ in* E *with exactly two distinct values under the permutations of the variables $x_1, ..., x_5$ is of the form $p + \rho q$, where p and q are symmetric functions in $x_1, ..., x_5$, and ρ^2 is the discriminant of $\mathbf{p}_5(x)$.*

MODERN Since E = $\mathbf{Q}(x_1, ..., x_5)$ and F = $\mathbf{Q}(a_1, ..., a_5)$, where the a_i are symmetric functions of the x_i, any element of F can be expressed in terms of symmetric functions of the $x_1, ..., x_5$ and so we can restate **Theorem 5** as follows:

Theorem 5 *Each v in* E *that has fewer than five distinct conjugates is contained in the field* F(ρ), *where ρ^2 is the discriminant of $\mathbf{p}_n(x)$.*

By **Theorem 4**, any v in E with fewer than 5 distinct conjugates must have either 1 or 2. If v has 1 conjugate—*itself*—it is symmetric and belongs to the fixed field of G(E/F), namely F. If v has 2 distinct conjugates, it is alternating and its minimum polynomial over F has degree 2, so its splitting field E(v) over F is a normal extension of F of degree 2. Hence, by the **Main Theorem of Galois Theory**, the field F must be the fixed field of some subgroup of G(E/K) of index 2; but $\mathbf{A}_5$ is the *only* such subgroup. Hence, there is in fact *only one normal extension* K *of* F *of degree*

2, so that any v with just two distinct conjugates belongs to this field. Finally, one verifies directly that ρ is alternating but not symmetric, and hence, this field K is generated by ρ over F.

Theorem 6 *A rational function $f(x_1, ..., x_5)$ in* E *with exactly five distinct values under the permutations of the variables $x_1, ..., x_5$ is of the form*

$$r_0 + r_1 x + r_2 x^2 + r_3 x^3 + r_4 x^4,$$

where $r_0, ..., r_4$ are symmetric functions of $x_1, ..., x_5$ and x is one of the $x_1, ..., x_5$.

MODERN In its modern formulation, this theorem and its proof are much clearer.

Theorem 6 *If v in* E *has exactly* 5 *distinct conjugates*, $\mathrm{F}(v) = \mathrm{F}(x_\mu)$ *for some root x_μ of* $\mathbf{p}_5(x)$.

The isotropy groups $\mathfrak{I}_1, ..., \mathfrak{I}_5$ in G(E/F) ≈ $\mathbf{S}_5$ of the elements $x_1, ..., x_5$ are the only subgroups of $\mathbf{S}_5$ of index 5. By the **Main Theorem of Galois Theory**, the associated 5 fields $\mathrm{F}(x_1), ..., \mathrm{F}(x_5)$ are the only extension fields of F of degree 5. Since the splitting field F(v) of v has degree 5 over F, it must be one of the fields $\mathrm{F}(x_j)$, $j = 1, ..., 5$. I will consider this result in detail in Chapter 4.

Stage 3 We are now ready to prove that the general polynomial equation $\mathbf{p}_5(x) = 0$ of degree 5 is not solvable by radicals. Starting at F, Abel shows that the only simple radical extension of F is of degree 2, generated by the quantity ρ in **Theorem 5**; this is **Proposition 2**. He then shows that there is no simple radical extension of F(ρ) at all; this is **Proposition 3**. Thus, since F(ρ) is certainly not all of E, the field E is not a radical extension of F.

Proposition 2 *If r is a p-th order radical over* F, *then $p = 2$ and* $F(r) = F(\rho)$.

As always, r is a solution of $x^p - A$ with A in F. By **Proposition 1**, $x^p - A$ is irreducible over F since r is not in F, and in particular, it is the minimal polynomial of r over F with p distinct solutions. By the **Combinatorial Principle** (or by **Theorem 7**), p is the number of values of r as a rational function of the roots. Hence, by **Theorem 3**, p divides 5!, so it is 2, 3, or 5. But by **Theorem 4**, the option $p = 3$ is ruled out, so $p = 2$ or $p = 5$.

Suppose first that r in E has 5 distinct conjugates. By **Theorem 6**, $F(r) = F(x_1)$. Thus, x_1 is in $F(r) - F$. By the **Lemma** following **Theorem 2**, the minimal polynomial of x_1 over F has 5 distinct solutions and we can write:

$$r = 1/5(x_1 + \alpha^4 x_2 + \alpha^3 x_3 + \alpha^2 x_2 + \alpha x_5).$$

since these five solutions are just the five roots of $\mathbf{p}_5(x)$. But it is clear from this representation that the right-hand side takes 120 values under the permutations of the roots. Yet, the left-hand side takes by assumption 5 distinct values. But this is a violation of the **Combinatorial Principle**, a contradiction.

In case $p = 2$, we have $r = p + \rho q$ by **Theorem 5**, with alternating ρ.

Proposition 3 *There is no proper radical extension of* $F(\rho)$ *contained in* E.

Suppose that $L(r) \neq L = F[\rho]$ is a radical extension, so that r is a solution of

$$x^p - A \in L[x] \qquad (*)$$

with p a prime. Then r is not in L, and by **Proposition 1**, (*) is irreducible over L. On the other hand, A is not in F, for otherwise by **Proposition 2** we would have $L(r) = F(r) = L$. Hence, A is alternating but not symmetric. In order to apply the results established thus far, Abel now needs to determine the minimal polynomial of *r over* F. It turns out that r has $2p$ conjugates in E, and this allows one to rule out each of $p = 1, 2, 3, 4$, and 5. In each case, one can show that a contradiction arises either with **Theorem 4** or the **Combinatorial Principle**.

Thus, we have finally arrived at

Theorem 8 *The general polynomial equation of degree* 5 *is not solvable by radicals*.

Proof If the general equation $\mathbf{p}_5(x) = 0$ of degree 5 is solvable by radicals over F, then it is certainly solvable by radicals also over the extension of F obtained by adjoining all the roots of unity to F. Hence, we can suppose that F contains all the roots of unity. With this wrinkle out of the way, we can now apply all the results established thus far.

If $\mathbf{p}_5(x) = 0$ is solvable by radicals over F, its splitting field E is contained in a radical extension of F and hence, by **Theorem 2**, E is itself a radical extension of F. So there would have to exist a tower of simple radical extensions

$$F = F_0 \subset F_1 \subset \ldots \subset F_{\eta-1} \subset F_\eta = E.$$

But we have just seen that no such tower of simple radical extensions exists.

More pedantically, $\mathbf{p}_5(x)$ is irreducible over F by **Theorem 7**, so that $F \neq E$, and hence $\eta \neq 0$. By **Proposition 2**, the first simple extension $F_1 = F[\rho]$. Since each element of $F[\rho]$ has two conjugates, $E \neq F_1$, and so $\eta > 1$. But, by **Proposition 3**, E contains no proper radical extension of $F[\rho]$ and hence, $\mathbf{p}_5(x) = 0$ is not solvable by radicals.

3.0 COGNITIVE CONTROL

In this chapter, I will attempt to characterize the differences in the epistemic power of the two approaches to solvability by radicals. I will introduce a configuration of notions that allows us to articulate those differences in a systematic way and, as I hope to show, to analyze the nature and source of those differences. My central notion will be, of course, *cognitive control*, but in order to introduce this notion, some preparation is required.

3.1 EPISTEMIC RESOURCES AND EPISTEMIC PROCESSES

Our systematic epistemic life can be thought of as having two notionally distinct aspects: the *epistemic resources* an agent has at a given time on the one hand, and the *epistemic processes* she may engage in with those resources on the other. The epistemic resources are the ambient framework of capacities that allow one to pursue various epistemic goals, and the processes are sequences of exercising those capacities in order to pursue some specific epistemic goal. Thus, an epistemic process is individuated by the actual cognitive operations that constitute it *and* by its overall aim.

The epistemic resources of an agent include the *concepts* she has mastered, her *methods of acquiring knowledge*, and whatever bits of *knowledge* she actually has. For example, Abel's epistemic resources would include the concepts *permutation* and *radical*, the algorithmic methods for computing the solutions for equations of degrees 2, 3, and 4, and knowing the **Fundamental Theorem of Algebra**; his main epistemic process under consideration here would be the search for a proof of the unsolvability of the general equation of degree 5.

I should emphasize that the set of resources relevant to pursuing one's goal will typically grow in the process of pursuing that very goal. Indeed, the process of searching for a proof will always involve the acquisition of many new bits of knowledge—the many propositions one proves in the course of proving the result one wants. But the more momentous proofs will typically involve the acquisition of epistemic resources that turn out to be relevant to pursuing a variety of epistemic processes, not just the one in the course of which they are acquired. The invention of a new concept is probably the most typical advancement of this kind. For example, in searching for a criterion for solvability by radicals, Galois (in effect) invents the concept *group*, a concept that turns out to be critically important not only to his particular epistemic process, but to much of modern mathematics.

The distinction between epistemic resources and epistemic processes provides the general framework within which I will articulate the notion of cognitive control: I will take it that cognitive control is an epistemic standing enjoyed *over an epistemic process in virtue of having a suitable configuration of epistemic resources*. Thus, the principal aim of this essay is to give a general characterization of the standing I am calling "cognitive control" and to identify some of the most typical kinds of configurations of resources in virtue of which one enjoys this standing over mathematical epistemic processes.

The general idea of *occupying an epistemic standing over a process* is modeled on the idea that a cognitive agent can be said to 'occupy' various 'epistemic standings' with respect to a *question*. For example, given the question *Is p the case?*, here are some of the different standings one might occupy: *to understand a sentence s that represents p*; *to have evidence that p*; *to have a method of finding out whether p*; *to have an unjustified but true belief that p*; and, indeed, *to know that p*.[23] Thus, to say that an agent occupies a particular epistemic standing *S* with respect to a question *Q* is to say that she has some particular kind of configuration of epistemic resources *S* relevant to answering *Q* and she knows that this is so; to occupy an epistemic standing is, in part, to know that one has certain resources relevant to the question. Similarly, to say that an agent *occupies an epistemic standing S over a process* is to say that she has some particular set of epistemic resources *S* that are relevant to pursuing that process and she knows that this is so. In view of what I just noted, one's epistemic standing over a process will typically change over the course of pursuing that process. The thought about cognitive control, then, is that it is the kind of epistemic standing that is occupied more or less from the outset of the process, if at all. Thus, my aim is to identify a particular kind of configuration of epistemic resources the having of which amounts to occupying the standing I am calling "cognitive control."

I distinguish two basic types of epistemic processes pertinent to our case study: *searching for a proof* and *reading a proof*. In order to render our philosophical grammar uniform, I will say

[23] By way of clarification, I am taking it that an agent can occupy many different epistemic standings with respect to a question or an epistemic process at a given time. Usually, however, the 'stronger' standings tend to absorb the 'weaker' ones. For example, *to know that p* would absorb *to have justification for believing that p*, and so on.

that each kind of a process is *aimed* at answering some specific *question* such as, for example, "Is the quintic solvable by radicals?" or, perhaps, "Why is the quintic not solvable by radicals?"

It is clear, I take it, that we need to distinguish the process of searching for a proof from the process of reading a proof: the epistemic standings occupied by a mathematician at the various stages of searching for a proof will typically be quite different from those occupied by a mathematician at the various stages of reading that proof *once completed*. A proof, once completed and 'properly laid out,' might allow a mathematician reading it to maintain good cognitive 'grip' at each stage, even if the one who discovered that proof did not have very good grip at the various stages of searching for it. In this paper I will only consider completed proofs and examine the standings a competent mathematician equipped with a standard background appropriate to that proof will enjoy at the various stages of reading it. I want to stress, however, that ultimately the notion of cognitive control is meant to provide an analysis also of the kind of cognitive standings that enable working mathematicians to prove new results.

This is the plan. I will motivate my characterization of cognitive control by identifying a sequence of important differences in the epistemic standing we enjoy at the various stages of reading the proofs of Abel and Artin. Once the characterization is complete, I will turn around and apply it to the two proofs in greater detail; this will be the centerpiece of the essay. I will conclude that with the epistemic resources of modern algebra in hand, we enjoy much better cognitive control over the process of reading Artin's proof than we do over the process of reading Abel's proof with the resources that were available at his time. It would certainly be interesting to analyze the differences in the character of cognitive control Abel and Artin enjoyed at the various stages of searching for their respective proofs, but addressing this issue adequately is just as certainly beyond the scope of this brief treatment.

3.2 BASIC EPISTEMIC CHALLENGES

Cognitive control is meant to be an epistemic standing that allows us to negotiate the epistemic challenges we face in the course of mathematical research in a way that is, so to speak, rationally orchestrated. In view of our case study, I propose to get the notion of cognitive control off the ground by considering the following idealized reconstruction of those challenges.

Knowing a target range We need to be able to identify at least one terrain of facts we know we can profitably examine in order to answer the question driving our epistemic process; I will call any such terrain of facts a *target range* for the process. The basic epistemic significance of having identified what one knows is a target range is that doing so creates a more or less determinate *space of epistemic options* for the rest of the process: a more or less determinate range of things one *might do* in order to address the question. Abel and Galois both know that the question as to whether the polynomial equation $\mathbf{p}_5(x) = 0$ is solvable by radicals can be answered by examining the relations of the roots of $\mathbf{p}_5(x)$, and this determines the overall direction of their respective projects. As much, I suppose, is obvious. *However*—

Representing the target range —One might know a target range and yet not be able to *represent* it or any one of the individual facts in it in a way that allows one to address the question one is trying to answer. Thus, the second fundamental challenge in an epistemic process is to find a useful representation of one's target range in a situation in which one does not yet know many, or any, of the individual facts in it. In particular, one wants a representation that allows one to determine the general *location* of facts *directly relevant* to addressing the question. I will call a representation of a target range as a whole an *organizing representation* provided it affords a way of constructing a structured representation of the epistemically possible individual facts in that range—facts that, for all one knows, may belong to the target range; I will call a representation of the latter kind an *epistemic scaffolding*. The basic epistemic significance of being able to construct an organizing representation and an epistemic scaffolding is that these representations will *organize* and *delimit* the space of epistemic options for the process; I will describe this contribution by saying that they provide *aim* and *location guidance*.

I will argue that, strictly speaking, Abel does not manage to construct an organizing representation or a scaffolding for his epistemic process as a whole. Artin, in contrast, can use the *Galois group of the splitting field of* $\mathbf{p}_5(x)$ as his organizing representation; the range of epistemically possible sequences of subgroups emerges as one of his principal epistemic scaffoldings. For Abel and Artin alike, locating the facts directly relevant to solvability by radicals amounts to finding a *criterion* for solvability by radicals they can actually employ to determine whether the general equation of degree 5 is solvable by radicals. I will again argue that, strictly speaking, Abel does not manage to do this but, to be charitable, we may think of **Theorem 2** as showing that $\mathbf{p}(x) = 0$ is solvable by radicals if and only if the splitting field extension of $\mathbf{p}(x)$ is a radical extension. Artin, in contrast, employs the **Main Theorem of Galois Theory** to locate the facts directly relevant to solvability by radicals in the organization of the system of subgroups of the Galois group. Thus, he succeeds in finding a criterion that is much more readily employed: $\mathbf{p}(x) = 0$ is solvable by radicals if and only if the Galois group G(E/F) of the splitting field extension of $\mathbf{p}(x)$ is a solvable group.

Extracting Facts Mirroring the distinction between the foregoing two challenges, one might be able to locate facts that are directly relevant to answering the question driving one's epistemic process without being able to *represent* them in a way that would allow one to actually answer that question. I will call the challenge of discovering and, crucially, *articulating* facts directly relevant in a way that allows one to employ them in answering one's question *extracting* them from the target area. The basic epistemic significance of being able to extract facts directly relevant to answering one's question is, of course, that this just is what finally puts one in a position to answer it.

Our ability to extract facts will depend on two kinds of factors. On the one hand, it will depend on how precisely we are able to locate those facts. On the other hand, it will depend on the extent to which we are able to *manipulate* our representations of the target range effectively. I will identify some of the *devices for* and *modes of manipulating* representations characteristic of the two approaches, and show how one might begin to analyze the epistemically significant differences between them.

For Abel and Artin, extracting facts directly relevant amounts to determining whether their respective criterion for solvability is satisfied for $\mathbf{p}_5(x)$. Again, it is not clear to what extent Abel can be considered to extract features directly relevant to solvability. In contrast, it is clear that Artin does manage to do so: he shows with that the Galois group $\mathbf{S}_5$ of $\mathbf{p}_5(x)$ does not contain a normal series with abelian quotients.

3.3 CHARACTERIZATION OF COGNITIVE CONTROL

In view of the foregoing three fundamental challenges, I propose that we consider the epistemic standing characterized by the following configuration of epistemic resources.

> *An agent enjoys **cognitive control** over an epistemic process aimed at answering a question* **Q** *to the extent to which*
>
> (1) *she has identified a **target range** of facts for her process*; *that is*, *a set of facts such that*, *given her overall epistemic resources*, *knowing those facts makes it possible to correctly infer a direct answer to* **Q**;
>
> (2) *she has adopted an **organizing representation** for her epistemic process*; *that is*, *one that represents the target range **as a whole** and*, *along with her overall epistemic resources*, *allows her to erect an **epistemic scaffolding** for examining that range*;
>
> (3) *her epistemic scaffolding*, *along with her overall epistemic resources*, *provides her **epistemic guidance** for examining the target range*; *and*,
>
> (4) *given the epistemic guidance provided by her scaffolding and her overall epistemic resources*, *she is able to **locate** and **extract** features of the target range that are **directly relevant** to answering* **Q** *by using her devices for manipulating representations*.

Comments

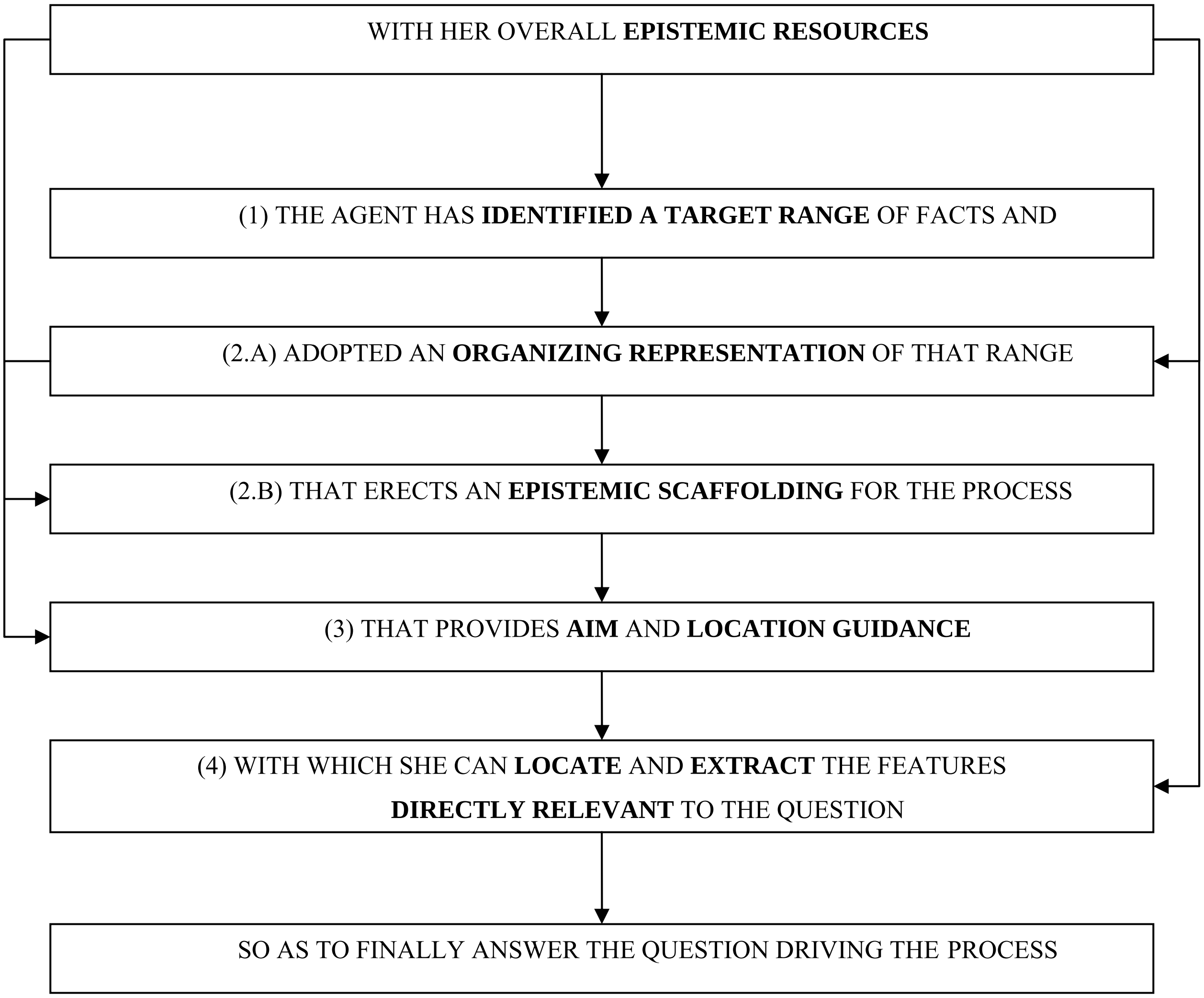
(1) To erect an epistemic scaffolding is to set up a structured representation of the space of *epistemically possible facts* in the target range one has adopted; as such, a scaffolding is a way of *representing what one does not yet know* about the target range. A scaffolding is structured in the sense that it consist of a determinate range of determinate *locations* each one of which contains a range of mutually exclusive *epistemically possible facts*. Thus, discovering that one of the epistemically possible facts in a given location actually obtains allows one to rule out the others; I will say that a scaffolding is *inferentially responsive*. We will see that there are also other ways in which a scaffolding can be inferentially responsive.

(2) A proper epistemic scaffolding provides the agent epistemic guidance in the sense of providing clues as to what the *rational* way to proceed is at each stage in the process. There are three types of epistemic guidance: *aim guidance* provides clues as to which piece of knowledge one should pursue at a given stage; *location guidance* provides clues as to where in the target range the facts relevant to pursuing a given particular aim are likely to be; and, *manipulation guidance* provides clues as to which devices for manipulating representations one should employ in exploring those locations.

Synopsis

An agent has cognitive control over an epistemic process aimed at answering a question **Q** to the extent to which she has identified a target range for her process and adopted an “organizing” representation of that range as a whole, a representation that erects an epistemic scaffolding; and further, to the extent to which the scaffolding provides her guidance for examining the target range and, in virtue of enjoying that guidance, she is able to locate and extract features of the target range that are directly relevant to answering **Q**.

We can characterize the organization of the components of cognitive control as follows:


WITH HER OVERALL **EPISTEMIC RESOURCES**
(1) THE AGENT HAS **IDENTIFIED A TARGET RANGE** OF FACTS AND
(2.A) ADOPTED AN **ORGANIZING REPRESENTATION** OF THAT RANGE
(2.B) THAT ERECTS AN **EPISTEMIC SCAFFOLDING** FOR THE PROCESS
(3) THAT PROVIDES **AIM** AND **LOCATION GUIDANCE**
(4) WITH WHICH SHE CAN **LOCATE** AND **EXTRACT** THE FEATURES **DIRECTLY RELEVANT** TO THE QUESTION
SO AS TO FINALLY ANSWER THE QUESTION DRIVING THE PROCESS

An arrow from one box to another indicates that, when one enjoys cognitive control, the epistemic accomplishment described in the latter box is achieved, at least in part, *in virtue of* the epistemic resources or accomplishments described in the first box; see below.

The overall idea is that to have cognitive control over an epistemic process is to have a configuration of epistemic resources that makes it possible to negotiate the major epistemic challenges along the way to answering the question in an ‘organized’ and ‘systematic’ way. Indeed, while I do not want to place too much emphasis on this, it would be natural to put the intuition as follows: when one has cognitive control over an epistemic process, *one is in control of what one is doing* throughout that process—cognitive control is a kind of epistemic self-mastery. If gathering *justifications* is the activity of rationality that looks *back* in our epistemic processes, to ensure that the requirements of reason have been met, then acquiring cognitive control is the activity that looks *forward*.

I want to emphasize two aspects of what is involved in having cognitive control. On the one hand, when one has cognitive control, one is able to approach the question, so to speak, *from top-down*: one’s epistemic resources make it possible to start the epistemic process with something like a *panoptic overview* of the situation and gradually *home in* on the particular features thereof that allow one to answer the question. This idea finds its implementation in the cumulative sequence of requirements in my characterization: the organizing representation is an overview of the target range as a whole; the epistemic scaffolding is a structured overview of what is and is not known about the target range at the outset of the process; aim and location guidance allow one to start homing in on the appropriate areas of the target range; to have located and extracted features directly relevant to answering the question just is to have homed in on those features.

On the other hand, when one has cognitive control, one is able to approach the question, so to speak, in an *organized manner*. First, in virtue of having an organizing representation of the target range, one has a well-defined *scaffolding* of facts into which one can plug further facts as they are discovered. Second, and perhaps most importantly, one's epistemic resources provide one *guidance* at each stage in the process. I will try to spell out the notion of guidance in great detail in what follows. For now, the idea is that to have guidance at a given stage in one's epistemic process is to have a clear idea of the *range* of potentially productive ways of proceeding at that stage, and at least some idea of the *relative merits* of the various ways of proceeding. Finally, in order to count as having guidance, of course one needs to be able to *select* and *try out* the various alternative ways of proceeding. I should emphasize that none of this is to require that one has from the start a definite course of investigation *laid out*; the idea is rather that to have cognitive control is, in part, to have the ability to navigate the space of possible ways of proceeding as one moves from one local challenge in the process to the next: there is no stage in the process where one is 'lost'—one has a firm idea of "what needs to be done next" and at least a general idea of "how one might do it."

I want further to emphasize that the components of my characterization are meant to mark out a *cumulative* sequence of epistemic accomplishments where each one is built on the ones preceding it and, at least to some extent, is *produced* by the ones preceding it. Thus, the organizing representation is the kernel for erecting an epistemic scaffolding; the scaffolding is the principal epistemic structure that provides aim and location guidance; the actual locating and extracting is accomplished, at least in part, in virtue of having aim, location and manipulation guidance from one's scaffolding. When one has cognitive control over a process, one is able to *make the process hang together*.

The note of caution here is that of course one's *overall epistemic resources* tend to make contributions to each component of cognitive control in a way that is not filtered directly through the components preceding it in the characterization. It will be clear, for example, that we often bring established methods or bits of knowledge to bear on our investigation in a way that is not 'intrinsically' or 'organically' structured by the epistemic scaffolding. Similarly, it will be clear that aim guidance is often enjoyed simply in virtue of being able to *think rationally* about what one might do at a given juncture in the process. In order for them to count as contributions to cognitive control, these activities need to take place within the overall context provided by the organizing representation and epistemic scaffolding, but they do not need to be rigidly structured by those representations.

Finally, even though the components of cognitive control are obviously heterogeneous *among themselves*, I want to recommend that they constitute a unitary configuration of epistemic resources *with respect to the epistemic process* and, as such, they are mutually complementary components of a particular kind of epistemic standing. I see three basic ways of motivating this idea. First, when an agent has cognitive control over a process, she is able to negotiate the foregoing three epistemic challenges in a fully rational manner. As such, it should be at least plausible that having cognitive control is a unitary kind of epistemic standing with respect to the *process as a whole*. Second, our case study will make it visible that if any one of the components is missing, there is a clear sense in which the agent's epistemic standing is *different* from what it would be in the presence of that component. That is, one's epistemic standing would be not just *weaker*, but have a different character in the sense in which, for example, having a true but unjustified belief *that p* has a character different from *knowing that p*. Finally, as I just stressed, the four components of cognitive control are meant to constitute a *cumulative sequence*. So it is possible to have many or even all of the resources required by the individual components of my characterization and yet, not occupy the epistemic standing I am calling having cognitive control.

In order to keep my analysis focused on its intended target, I want to mark out the general type of epistemic accomplishments to which having cognitive control is meant to belong by distinguishing it from two other types of accomplishments often considered in philosophy of mathematics. First, the epistemic accomplishment that in most minds (including mine) stands out as the fundamental one is that an epistemic process has provided *justification* for some mathematical claim. The overwhelming majority of philosophical inquiry focused on epistemic processes in mathematics has sought to identify just what such justification consists in and how such justification is possible. Second, in the past few decades, some philosophical attention has been paid to the accomplishment that an epistemic process has provided an *explanation* for some mathematical claim. There is now a handful of papers addressed to the issue of what might make a proof explanatory, but nothing by way of a serious contender for a theory exists at this time.[24] Finally, some philosophers and many philosophically minded mathematicians have intermittently but persistently urged that there are objective differences in what one might call the *efficiency* of mathematical epistemic processes. One of the principal intuitions here is that proofs that rely on heavy symbolic computations tend to be less efficient than proofs that operate mostly in terms of reasoning about the content of concepts; the contrast between the proofs of Abel and Artin would qualify as an eminent example of this contrast.

Among these three broad types of epistemic accomplishments—justification, explanation and efficiency—the analytical target of the notion *cognitive control* is meant to belong squarely

[24] The first modern paper examining this topic was Steiner's "Mathematical Explanation." See also Mancosu, "Mathematical explanation: problems and prospects".

with explanation or, more to the point, with *understanding*. While I cannot present any extended arguments to this effect here, I think it is clear that cognitive control picks out just the kind of epistemic mastery that is often informally described as *understanding a proof* or *understanding how to go about proving* a result. In further work I will argue that this is indeed so and, moreover, that we can analyze *understanding mathematical facts* as having cognitive control over various kinds of epistemic processes targeted at those facts. Thus, I hope to show that understanding in mathematics is a particular form of cognitive control.

In contrast, that the notion *cognitive control* is not addressed to issues of justification will be quite clear; what I want to emphasize here is that it is not addressed to issues of efficiency either. There will be junctures throughout this essay where what I am calling "cognitive control" could easily get conflated with a certain kind of efficiency of reasoning. This preamble is meant to guard against such conflations. Certainly I think that there is a *factual* connection between cognitive control and efficiency: when we enjoy control over an epistemic process, we tend to be able to pursue our aim efficiently and sometimes, perhaps, *vice versa*; yet, I mean cognitive control to be an epistemic standing conceptually independent from having achieved efficiency in one's mathematical reasoning.

Cognitive control as characterized here is an epistemic standing occupied by individual cognitive agents. However, as one would expect, ultimately the object of analytical interest is not the features of cognitive control enjoyed by this or that individual mathematician, but rather the features of cognitive control *made available* to be acquired by various sets of concepts, methods, and bits of knowledge, once mastered. One important aspect of this is that a set of epistemic resources might make cognitive control available over a *more or less wide* and a *more or less diverse* range of epistemic processes. Though I cannot argue for this here, my case studies strongly suggest that the resources characteristic of 20th century mathematics tend to make cognitive control available over vast and vastly diverse ranges of epistemic processes, while the resources characteristic of 19th century mathematics typically do not. Galois theory is a case in point: the concepts and results of Galois theory have found deep and diverse applications in many areas of modern mathematics; Abel's resources have had no such impact.

Indeed, the notion of cognitive control is meant to capture the following widely felt intuition about the nature of progress in mathematics: the truly significant advances tend to be characterized by the fact that they transform problems that were 'hard' into ones that are 'easy' or, at any rate, considerably 'easier.' Now one might think that this is a *merely psychological* issue. But what I am hoping to show is that there is an objective difference in epistemic character between 'hard' and 'easy' questions: a question is rendered easier when new epistemic resources make it possible to attain better cognitive control over some process of answering that question. An extreme way in which a hard question can become easy is that we find an algorithmic procedure for answering it. Typically, however, the advance is not this radical: it is a matter of introducing concepts, methods, and bits of knowledge which, once mastered, allow a competent mathematician to enjoy non-algorithmic control over a process of pursuing an answer to the question. Mastering the new concepts, methods and bits of knowledge may often be hard in the psychological sense, and success is not guaranteed even once they are mastered.

An epistemic process of any substantial complexity, such as searching for or reading the proofs of Abel and Artin, can be thought of as consisting of a number of more or less autonomous, modular *subprocesses*. For example, in the course of his proof of the unsolvability, both Abel and Artin establish a number of results that are largely independent of one another. The processes of establishing those results have their own epistemic aims, organizing representations, scaffoldings, and manipulational challenges. The process of proving a substantial subsidiary result may in turn split up into further subprocesses, and so on.

It would now be natural to suppose that cognitive control over a long epistemic process should be analyzed in terms of cognitive control over its subprocesses. As we will see, however, this is just one of two analytically complementary points of view. For mathematicians routinely seek to organize long proofs so as to mark out a sequence of 'main results' which, *if taken as given*, afford one good cognitive control over the 'overall structure' of the proof, even if there are subproofs over which one's control may be rather poor. That is, mathematicians seek to organize proofs in a way that creates a highly controllable superstructure in which less controllable 'local' components are treated as black boxes. We will see that this idea dovetails nicely with the widely felt intuition that the point of breaking long proofs into lemmas and propositions is to *make the proof as a whole understandable*. I will explore this issue in more detail in Section 3.5.

There is one final prefatory remark I need to make about the notion of cognitive control. The two principal types of mathematical epistemic processes to which the notion is meant to apply are *searching for a proof* of a putative theorem and *reading a proof* of an established theorem. Now, cognitive control is enjoyed over particular epistemic processes, and epistemic processes are individuated, in part, by their *aims*. Thus, in order to make sure that the notion is structurally fit to apply to processes of searching for and reading proofs, I need to be very explicit about the way I am thinking about the aims of such processes. For the purposes of my analysis, it strikes me as innocuous to take it as follows: the aim of a process of searching for a proof is to *find a way to justify* the putative theorem; the aim of a process of reading a proof is to *learn one way to justify* the theorem already established. This brings out the obvious analogy between the two types of processes; what concerns me here, however, are the disanalogies that could be a source of some perplexity. Thus, two remarks.

First, to have cognitive control over the process of searching for a proof is to maintain a clear view of "what needs to be done next" and "how one might do it"—this is to have epistemic guidance in virtue of having an epistemic scaffolding. And this, I think, should seem fine. The potential source of perplexity is that when one is *reading* a proof, one is *told* what needs to be done next, and *shown* at least one way of doing it. Thus, it might seem that the notion of cognitive control does not get a grip on a process in which one is following what is from the start known to be, in effect, a complete set of *instructions*.

Perhaps the most direct way to clarify this issue is to point out that mathematicians routinely speak of *reading a proof without understanding it*. This kind of reading is typically characterized by being able to 'check' each individual inferential move in the proof and yet, not having any 'sense' for the proof as a whole: why the proof is structured the way it actually is; why it involves the particular representational choices it does; why it takes the particular inferential path it does; and so on. So my thought is that when one has cognitive control over the process of reading a proof, one is precisely not in this kind of predicament. At each stage, the reader has a structured representation of the epistemically possible facts in the target range and, in virtue of her overall epistemic resources, knows what the range of potentially productive ways of proceeding looks like. Clearly one may fail to occupy a cognitive standing of this kind even if one knows from the start that the proof is a complete and correct set of instructions for justifying the theorem. Indeed, to speak of having cognitive control over the process of reading a proof is one way of capturing of the intuitive idea of *understanding a proof*.

So as to provide just a little bit more perspective: a proof may provide its reader more or less *help* in maintaining cognitive control. A proof provides a lot of help if it clearly articulates the hierarchy of its internal aims, clearly identifies its target range, clearly sets up an organizing representation and scaffolding and, perhaps crucially, clearly indicates the main choice points and alternative available inferential routes; a proof that does the opposite provides little help. It is one of the permanent professional frustrations of mathematicians that they are forced to contend with proofs that provide very little help in maintaining cognitive control.[25]

[25] The note of caution to be sounded here is that no matter how much help a proof provides, of course an agent may still fail to maintain cognitive control in the course of reading that proof because her background of epistemic resources is not rich enough—no proof can provide *all* the epistemic tools for maintaining control over the process of reading it.

3.4 FACTS, CONCEPTS, REPRESENTATIONS AND NOMINALISM

Before we can go on to discuss the four components of cognitive control, I shall have to say a few words about the metaphysical underpinnings of my project. The purpose of this section is not in any way to argue for the superiority of the conceptions I will adopt, but merely to make my commitments explicit.

(*a*) *Facts*

I will take the notion of *fact* as an unanalyzed primitive of my theory; informally, a fact is a *feature of the world*, a *particular way* the world is. While most of the facts we will have the occasion to consider are of the form *the object x has the property* ϕ, where the object can be a universal as well as a particular, I will also countenance logically compound facts such as *conditional* and *conjunctive* facts. In particular, in my analysis of Abel's proof, I will take it that he deals with many conditional facts of the form *If the general polynomial equation* $\mathbf{p}_5(x) = 0$ *of degree five is solvable by radicals*, *then*... For **Stage 3** of Abel's proof is a *reductio*, and in my metaphysical framework it would be difficult to make sense of *reductios* without countenancing conditional facts. Finally, we will of course have to consider many facts that would be naturally articulated with quantified sentences. I want to emphasize, however, that my analysis will make no appeal to any distinction between 'general' and 'particular' facts, if one there be.

So far, I hope, so good. There is however one potentially controversial stipulation I shall have to make about facts, mathematical facts in particular: the individuation of facts is conceptually *fine-grained*.

One of the fundamental aims of this essay is to provide resources for *articulating* differences in epistemic standing we occupy at the various stages of reading the proofs of Abel and Artin. We will see time and again that if we adopted a sufficiently unexacting individuation of facts, Abel and Artin could be said to be investigating the *same* range of facts and many of their central results articulate the *same* fact as some set of results in the other proof. This is the kind of attitude many philosophically innocent mathematicians would be prone to adopt. Such an attitude, however, would ill serve the purposes of our analysis: it would rob us of the ability to articulate the subtle and yet, crucial differences in epistemic standing.

Accordingly, I will adopt a conception of facts that goes hand in hand with *fine-grained content* of the Fregean kind. The idea is that contents can be as finitely individuated as our concepts allow, and I am simply stipulating that facts are as finely individuated as contents. One way to motivate this stipulation comes from the following conception of contents: the content of a conceptually articulated statement or a thought is a proposition and propositions *are* facts. Thus, clearly we want facts to be at least as fine-grained as our concepts allow us to articulate. This conception of contents has the virtue that it makes it intelligible how language and thought can *impinge directly* on the world; as such, it is a form of *direct realism*. A metaphysical picture of this shape may be described by saying that as the totality of all facts, the *world is conceptually structured*. This conception of contents and the attendant metaphysical picture is adopted, *inter alia*, by John McDowell in his *Mind and World*.

The fine-grained conception of facts and contents allows us to distinguish the sets of facts Abel and Artin adopt as the target ranges for their respective approaches. While both of them are in some sense examining facts about arithmetic relations of the roots of $\mathbf{p}_5(x)$, we can say that, properly speaking, Abel is examining facts about the effect of permutations on rational expressions of the roots, Artin facts about the organization of the system of intermediate fields of the splitting field extension of $\mathbf{p}_5(x)$. And this is only the beginning: the fine-grained conception will later on allow us to capture the crucial idea that a mathematician can know all the 'ground-level' facts in a target range and yet, not know any 'high-level' facts that capture *patterns* in the target range directly relevant to answering the question driving the epistemic process; I will take up this theme in Section 3.6.5.

(*b*) *Mathematical Concepts*

I will be working with the following conception of mathematical concepts:

> *A mathematical concept is a certain kind of constellation of norms that governs the propriety of producing symbolic artifacts*.

The phrase "certain kind" is a place-holder for the various conditions on just what sort of components and internal structure a 'properly constituted' mathematical concept would have to have; clearly making these conditions explicit cannot be attempted here.

The phrase "constellation of norms that govern the propriety of producing" signals that I conceive concepts as denizens of the normative domain. A norm is something that dictates what it is *correct to do* in a particular kind of situation. The phrase "symbolic artifact" refers to things like numerals and mathematical symbols quite generally, as well as to mathematical sentences constructed by producing combinations thereof.

Mathematical concepts are often *keyed* to specific symbolic artifact *types* in the sense that the norms that constitute a concept govern the propriety of producing tokens of that type as well as the propriety of responding to tokens of that type by producing tokens of other artifact types.

Thus, I think that our mathematical concepts are interconnected in complicated ways and, indeed, much of the time it may be somewhat artificial to think of the totality of our mathematical norms as neatly demarcated into *disjoint* concepts. For example, who's to say where the concept *addition* ends and the concept *multiplication* begins? After all, there are many norms the two concepts clearly share, such as the ones pertaining to distributivity of multiplication over addition. The likely idea here is that at least many mathematical concepts are *individuated* by some core constellation of norms, one that has around it a halo of norms that may or may not be thought of as belonging to that concept, perhaps depending on the context in which the issue is raised.

It is clear that as sets of norms, mathematical concepts are very complex, and it would be very difficult to display one explicitly. There are two types of examples that may be used to fix our intuitions, however. First, concepts of logical operations such as *conjunction* may be thought of as individuated by the *introduction* and *elimination rules* for the corresponding connective, the connective being a symbolic artifact type. Second, axiomatically defined concepts such as *group* in the modern theory of abstract groups may be thought of as individuated by the norms that are encoded in the definition of "group". Yet, there is a sense in which such explicit articulations are at best 'summaries' of the total set of norms that constitute these concepts.

In order to *have* ("grasp," "possess") a mathematical concept one needs to have mastered the norms that individuate that concept. But there is more. I take it that an agent who knows more *general facts* about the correct ways of producing tokens of the symbolic artifact type to which the concept is keyed has a *richer* concept than someone who knows fewer. A bit more bluntly, it seems vacuous to say that an agent has the concept *group* if the only way she can apply that concept is by unpacking the axiomatic definition.[26]

(*c*) *Representations in Pure Mathematics*

The principal epistemic significance of concepts is that they make it possible for us to *construct representations*. The idea is that a conceptually constituted representation is a constellation of symbolic artifacts which, *in virtue of being intentionally produced in a way that respects the norms that individuate certain concepts*, picks out some aspect of the world. That is, it is the norms that endow them with representational content, in virtue of what we do in our conceptual practice. Whether there are representations that are not conceptually constituted will not concern me here; for all the representations we employ in the intellectual practice of pure mathematics are conceptually constituted.

We will have the occasion to consider three basic types of representations in pure mathematics: ones of *facts*, ones of *objects* and ones of *properties*. The sentence *The Galois group* G(E/F) *of the splitting field extension* E/F *of the polynomial* $\mathbf{p}_5(x)$ *is not solvable* is a representation of a fact. The phrase *the splitting field extension* E/F is a representation of an object. The phrase (being) *solvable* is a representation of a property.

[26] More generally, the point is that it is not sufficient that one knows the *circumstances* of correct application of a concept; in order to count as having a concept, one also needs to know (at least some of) the *consequences* of correct application of that concept.

(*d*) *Nominalism*

My considered view about the ontology of mathematics is *nominalism*: there are no non-physical objects of any kind and, as such, there are no mathematical objects or properties. For the purposes of this essay, however, I will in effect pretend that realism in ontology is true; that singular terms in true mathematical sentences denote non-physical objects. However, I will be conscientious to formulate my proposals in such a way that they can be eventually reinterpreted without assuming realism in ontology. This will be a task for another essay.

In view of my nominalism, ultimately I want to do away with mathematical facts altogether and recast my analysis of cognitive control in terms of conceptually articulated *mathematical contents* without any commitment as to the specific metaphysical nature of those contents. Thus, the only aspect of the metaphysical picture canvassed under (*a*) that is indispensable to my account is that we have contents that are sufficiently fine-grained.

3.5 THREE LEVELS OF ANALYSIS

I have already noted that long proofs can typically be viewed as consisting of several modular subproofs. I will now develop this idea just a little bit further since I will need it in structuring my analyses of the proofs of Abel and Artin.

Taking my cue from the way in which mathematicians organize their proofs, I will distinguish three *levels* on which we might analyze cognitive control enjoyed in the epistemic process of reading a proof: *global*, *semi-local* and *local*.[27] These levels will be demarcated by two factors: the way in which the proof breaks down into subproofs, and the degree of granularity on which we consider the proof.

Hierarchy of Epistemic Processes

It is a thoroughly familiar idea that mathematical proofs and, indeed, epistemic processes more generally, tend to have a *hierarchy of aims*: there is the aim of the process as a whole; a few 'top-level' subsidiary aims which, if reached, would allow us to reach the aim of the process as a whole; perhaps a few more 'medium-level' subsidiary aims under the top-level ones; and so on, until we come to 'local' aims that are reached by individual inferential moves taken to be justificationally primitive in the context of that proof—the 'ground level' of the proof. Such moves may be, for example, computations carried out according to some specific set of rules, or

[27] For some quasi-philosophical reflections on the sort of organization I have in mind here, see Uri Leon, "Structuring Mathematical Proofs".

simply logically valid inferences from bits of knowledge already in one's set of epistemic resources at that stage in the proof.

It is a central part of my analytical set-up that epistemic processes are individuated, in part, by their aims. Thus, corresponding to the hierarchy of its aims, a mathematical epistemic process will typically have a hierarchy of nested subprocesses. For example, the process of *writing a proof* has the aim of justifying the theorem; this aim is reached by justifying a number of subsidiary results, and the aim of justifying each such result will demarcate an epistemic subprocess. The process of *reading a proof* has the aim of learning one way to justify the theorem; this aim is reached by learning one way to justify a number of subsidiary results, and the aim of learning one way to justify each such result will demarcate an epistemic subprocess. Since this way of speaking would become cumbersome very quickly, I will from now on speak of the proof and its various subproofs, ignoring the reference to the actual epistemic process of writing or reading the proof.

For example, a given epistemic process might consist of three disjoint global processes L_1, L_2, and L_3, where each one of them consists of some number of disjoint semi-local subprocesses $M_{1,1}$, $M_{1,2}$, ..., and finally, each semi-local process consists of some number of disjoint local subprocesses $S_{1,1,1}$, $S_{1,1,2}$, ... At any one level of scale, an admissible decomposition to subprocesses must be such that the processes at that level are disjoint and jointly exhaust the global process P.

Thus, we can in principle distinguish as many individual epistemic processes as there are individual epistemic aims. For the purposes of our analysis, this would be too detailed a view, for just about every inferential step could be considered its own process and at this level, we would not be able to discern meaningful differences in the character of cognitive control. In order for such differences to emerge, we will need to pull back from the level of individual inferences. The smallest subproofs we would typically want to consider tend to be proofs of what mathematicians would consider subsidiary lemmas in a long proof, usually consisting of at least a dozen or so individual inferences.

Granularity

When considering the character of cognitive control we have over a substantial epistemic process, we could of course consider the control we have over each of its subprocesses and so on, until we come to individual inferential moves. There is, however, a very natural alternative way of considering such a process whereby we consider the subprocesses immediately under it as *given* in the sense that we regard the results obtained in them as part of our set of epistemic resources. This point of view is natural in a number of ways. On the one hand, by the time we actually justify the result at given level, the results from the ones below it will have been justified and hence, they have indeed become part of our set of epistemic resources. On the other hand, when mathematicians present an outline or an overview of a long proof, this is just what they do: they map out major, 'large-scale' results and indicate how the aim of the proof overall can be reached with those results in hand. In so doing, they are treating the results of the subprocesses as given in the sense I am proposing—if you will, as 'black boxes'. In providing further 'explanations' of the proof, they will typically focus on one of the subsidiary processes, again treating it in the manner they first treated the global process; and so on.

Now the significance of this for my analysis is that it is possible to come out as having good cognitive control over a process at a given level without having good control over some, or even any, of the subprocesses below it. This flexibility of point of view will help us better identify and appreciate the differences in the character of control Abel and Artin enjoy over their respective processes.

Naturally all of this still allows that we can, if we so desire, adopt a completely local point of view wherein the character of control over an epistemic process is taken to be simply the sum total of control enjoyed over the smallest theoretically meaningful subprocesses. This point of view alone would not give us a very illuminating account of the nature of epistemic accomplishment in mathematics, however. The organization of proofs into hierarchies of aims and nested subproofs is a central feature of mathematical practice, one that is often regarded as epistemically important in informal analyses of their trade by working mathematicians. For example, Thurston clearly regards the ability to present proofs at different levels of granularity as an aspect of *understanding*.[28] As such, we should do our best to keep this feature in view in our philosophical analysis.

[28] See Thurston, p. 164. See also Van Bendegem, "Non-Formal Properties of Real Mathematical Proofs." Van Bendegem writes: "If a proof has a simple proof-outline, then the quality of that proof is considered to be high by mathematicians. Conversely, if the proof has a highly complicated proof-outline, then the quality of the resulting proof is low" (p. 254).

3.6 COMPONENTS OF COGNITIVE CONTROL

I will now give a general discussion of the four components of my characterization of cognitive control. In Chapter 4, I will examine the various ways in which these components are or are not present in the proofs of Abel and Artin.

3.6.1 Identifying a Target Range

Abel and Artin can be thought of as trying to answer the same question: Is the general polynomial equation $\mathbf{p}_5(x) = 0$ of degree 5 solvable by radicals? They both anticipate the negative answer, and know that this would imply that no general polynomial equation of degree greater than 5 is solvable by radicals. Yet, the two appear to be investigating very different *terrains of facts* in order to prove the same result. Abel is investigating facts about the effect of permutations of the roots of $\mathbf{p}_5(x)$ on rational expressions of the roots; Artin is investigating the organization of the splitting field extension E/F of $\mathbf{p}_5(x)$ and the organization of the Galois group G(E/F) of this extension.

There is a strong intuition to the effect that an epistemically significant difference exists between the ways in which the two investigations begin: one feels that Artin has a clearer view of *which* range of facts his investigation is targeted at than Abel does—he has 'identified' his target range more sharply; one further feels that Artin has more of an initial justification for thinking that his target range will yield an answer to the question, whereas Abel has no assurance *ab initio* that this is so. For it is clear that the facts about the organization of the system of intermediate fields are sufficient to settle the issue of solvability either way. In contrast, for all Abel knows at the beginning of his proof, there might not be enough constraints on the number of values rational expressions of the roots of $\mathbf{p}_5(x)$ can take under the permutations of those roots to rule out the existence of a solution by radicals. Thus, the range of facts Abel has chosen to examine is not known to be sufficient to settle the issue of solvability of $\mathbf{p}_5(x) = 0$.

There are two conceptually independent issues I need to address here: first, I need to say what a target range *is* and, second, I need to say what it is to *identify* a target range. From the point of view of my analysis, it is important to keep these two issues separate and, further, to keep the issue of what it is to identify a target range separate from what it is to represent a target range in a way that affords scaffolding and guidance. For as we will see, these issues must be kept separate if we are to identify and analyze the central differences in epistemic standing between Abel and Artin.

(*a*) *Target Range*

A set of facts is a *target range* for an epistemic process aimed at answering a question **Q** relative to a set of epistemic resources **R** provided that knowing those facts makes it possible to correctly infer a correct direct answer to **Q**, given the resources in **R**. I stipulate that no set of facts is a target range relative to a set of resources **R** if **R** contains a direct answer to **Q**. For once a direct answer α to **Q** is known, *any* set of facts Γ can be used to infer that answer: Γ and α, hence α.

The choice of terminology is meant to reflect the idea that a target range is a set of facts on which the investigation may be fruitfully *targeted*. When the agent has chosen to examine some range of facts that is in fact a target range in this sense, we may speak of *the* target range for her process.

Comments

(1) I want to emphasize that *target range* is an *epistemic* notion: a set of facts is a target range for an epistemic process provided that *knowing* those facts makes it possible to *infer* a direct *answer* to the question at which the process is aimed. In mathematical epistemic processes, this will typically amount to there being a sequence of *logically valid inferences* from sentences articulating those facts to a direct answer. Accordingly, I allow that a set of facts **S** can *become* a target range when some fact is discovered such that, with that new fact in hand, it is possible to correctly infer an answer to the question from the facts in the set **S**; the new fact may or may not belong to the set **S** itself.

(2) I want further to emphasize that *target range* is a *normative* notion: a set of facts is a target range for an epistemic process provided that knowing those facts makes it *possible to correctly* infer a *correct* answer to the question at which the process is aimed. Thus, whether or not a set of facts is a target range will depend on what the *norms* of the ambient conceptual setting are, centrally including the norms governing the proprieties of logical and non-logical inference. Accordingly, I allow that a set of facts can become a target range when the norms of the practice are expanded in such a way that, with the new norms in hand, it is possible to correctly infer an answer to the question from the facts in that set.

(3) I most especially want to emphasize that *target range* is *not* a *metaphysical* or *ontological* notion. What is more, I do not think there is a set of general metaphysical or ontological criteria that would guarantee that a set of facts is a target range for a given epistemic process.

In particular, I want to steer well clear of the *prima facie* attractive idea our case study might suggest—namely, that a target range for a mathematical epistemic process is always a set of facts about some single object or a 'coherent' system of objects. For I want to formulate the notion of cognitive control in such a way that having cognitive control over an epistemic process does not place any *a priori* metaphysical requirements on the set of facts one must investigate. More bluntly, I do not want having cognitive control to require that the process is targeted at the 'metaphysically right' set of facts, facts that 'metaphysically govern' the answer to the question driving the process, whatever that might mean. Rather, I want the notion of cognitive control to capture an organizational configuration in our epistemic life that is *conceptually* independent of whether or not we have pointed our gaze at the 'metaphysically right' bit of the world. Of course this still allows ample room for the possibility that having cognitive control tends to *in fact* require that we have focused on the 'right' bit of the world. In particular, this allows ample room for the possibility that facts about relational structures tend in fact to be 'appropriate' target ranges at least in some areas of mathematics. Again, certainly our case study suggests something of this general shape. But what I want to urge is that the epistemically crucial differences between target ranges are not to be analyzed in metaphysical or ontological term, but rather in terms of the character of the organizing representations and scaffoldings that become available when we take some suitable relational structure as our target.

I have two motivations for adopting this anti-metaphysical approach. On the one hand, as I indicated in the previous section, I am a nominalist about mathematical objects. Thus, I want to develop the notion of cognitive control in such a way that having control over a mathematical epistemic process does not presuppose that one has discovered the 'metaphysically right' mathematical objects, relations or properties.

On the other hand, I believe and will argue in another essay that *understanding* in empirical cognition has two conceptually independent aspects: in order to understand a range of physical phenomena, we need to have a description of a system of objects and their relations that *produce* those phenomena, be it causally or otherwise; however, in order for such a description to yield understanding, it also needs to engender a certain kind of epistemic standing with respect to that range of phenomena—one I believe is characterized by my definition of cognitive control. I will argue that many different kinds of descriptions can serve to engender understanding: describing *individual causes* of an event, describing a *causal mechanism* that produces a range of events or, indeed, furnishing a theory that *unifies* our picture of the world can all engender understanding provided that they engender cognitive control. Thus, I will hope to advocate a spirit of tolerance and diversity about accounts of understanding and explanation in empirical thought.

My anti-metaphysical approach to cognitive control creates room for a somewhat more radical suggestion: which set of facts is regarded as the 'metaphysically right' one may in some situations depend, at least in part, on the character of cognitive control the various candidates afford us. For example, in another essay I will explore the idea that in *singular causal explanations*, the 'explanatory' causes among the causal history of an event are typically the ones that afford us cognitive control over that history as a whole.

(4) As is by now clear, I allow that there are typically more than one target range for an epistemic process. Given my anti-metaphysical approach, however, the possibility of more than one target range does not matter much in my analysis of cognitive control. In my analysis of understanding, however, I will argue that certain varieties of understanding require that one has targeted the epistemic process on a range of facts with a specific metaphysical status—such as,

for example, a stable causal mechanism that as a matter of fact produces the phenomena to be understood.

(5) I do not require that one needs to know *all* the facts in a target range in order to infer an answer to the question driving one's epistemic process; in the situation typical in mathematics, knowing some subset of the facts chosen as the target range will suffice. Certainly we could define *minimal target range* in the obvious fashion, but it turns out that this notion would not have much analytical traction in our case study. For what we will see is that the agent typically starts out by identifying some mathematically natural, non-minimal target range and the epistemic challenge is precisely to *home in* on some particular locations in that range.

(6) The fine-grained conception of facts and contents allows us to distinguish the sets of facts Abel and Artin adopt as the target ranges for their respective approaches. While both of them are in some sense examining facts about arithmetic relations of the roots of $\mathbf{p}_5(x)$, we can say that, properly speaking, Abel is examining facts about the effect of permutations on rational functions of the roots, while Artin is examining facts about the organization of the system of intermediate fields of the splitting field extension of $\mathbf{p}_5(x)$. And this is only the beginning: the fine-grained conception will later on allow us to capture the crucial idea that a mathematician can know all the "ground-level" facts in a target range and yet, not know the "large-scale" patterns in those facts that are directly relevant to answering the question driving the epistemic process.

(*b*) *Identifying a Target Range*

An agent has *identified a target range* for her epistemic process provided that she has a *referring expression that picks out* a determinate set of facts and she *knows*, or has substantial justification for believing, that the set of facts picked out by that expression is a target range for her process in the sense above.

In order to avoid an obvious trivialization, we must further require that a referring expression cannot be used to identify a target range if its meaning depends essentially on some expression denoting the aim of the epistemic process in question. Thus, one cannot identify a target range just by saying: *whichever range of facts would allow me to infer a correct answer to my question*.

For example, it is quite clear that Artin has identified a target range in this sense: given his epistemic resources, he knows that the facts about the organization of system of intermediate fields of the splitting field extension will allow one to settle the issue of solvability either way. The verdict is much less clear in Abel's case. For he does not know any general facts that would show at the outset of his project that there are enough constraints on the range of possible values of rational expressions of the roots to rule out the possibility of there being a solution by radicals.

Comments

We will see in our discussion of Abel that being able to identify a target range at the outset of an epistemic process is by no means a trivial accomplishment, and that it is certainly possible to reach an answer to the question driving the process without having done so. The requirement that in order to count as having cognitive control one must have identified a target range is meant to capture part of the intuition that one way in which a cognitive agent may fail to have 'control' over her epistemic process is that she is merely ‘groping around in the dark.’ Without having identified a target range, one’s epistemic process is *blind*.

3.6.2 Organizing Representation and Epistemic Scaffolding

Recall the second component of our characterization of cognitive control:

The agent has adopted an organizing representation for her epistemic process; *that is*, *one that represents the target range as a whole and*, *along with her overall epistemic resources*, *allows her to erect an epistemic scaffolding for examining that range*.

One of the most striking differences between the proofs of Abel and Artin is that Artin’s proof overall is firmly *organized* around the representation *the splitting field extension* E/F *of the polynomial* **p**(x). At **Stage 3**, it becomes organized around the representation *Galois group of the extension* E/F; thus, the focus of the project gets tighter while remaining within the structure provided by the initial representation. Further, these representations are representations of two target ranges of facts as a whole. In contrast, no representation plays this kind of role in Abel’s proof. There are two representations that come close: the general expression for the form a solution by radicals would have to have, and the representation of the structure the radicals in such a solution would have to have. There are two epistemically crucial differences between the two sets of representations, however. First, while Artin’s representations are representations of his target ranges of facts, Abel’s are representations of certain isolated features one possible target range (the arithmetic relations of the roots) would have if $\mathbf{p}_5(x) = 0$ were solvable by radicals. Thus, they play a fundamentally different epistemic role in his proof, namely the role played by Artin’s criterion for solvability. Second, while Artin’s representations provide firm structure and *guidance* for his proof as a whole, in Abel’s case the verdict is much less clear.

3.6.3 *Organizing Representation*

An organizing representation is a conceptually constituted representation of the target range as a whole, a representation that allows the agent to erect an epistemic scaffolding for the process.

Once the agent has chosen a target range of facts for her process and adopted a particular organizing representation of that range, we may speak of *the* organizing representation.

The idea is that the organizing representation provides an *overview* of the terrain of facts one is setting out to investigate and, in so doing, orients the epistemic process as a whole by allowing one to erect the kind of representation I am calling an "epistemic scaffolding." Thus, in order to count as having cognitive control over one's process, it is not enough that one has a target range in view somehow or other: the process must be oriented and informed in an organic way by a suitable representation of a deliberately chosen target range as a whole.

Comments

Since the notion *organizing representation* depends on the notions *scaffolding* and *guidance*, the significance of having an organizing representation won't be fully in view until I have explained the latter two notions; still, a few prefatory remarks can be made.

(1) We can isolate the epistemic significance of having an organizing representation by noting that cognitive control involves three distinct, broadly *representational* accomplishments: the agent has identified a target range, she has adopted an organizing representation of that range, and she has erected an epistemic scaffolding.

There are two points I want to make about organizing representations in the context of this three-way distinction. First, an organizing representation need not to be a representation of any of the *individual facts* in the target range. The epistemic role of providing representations of individual facts in or about the target range is in my analysis played by the epistemic scaffolding.

Second, having an organizing representation is independent of having identified a target range. On the one hand, the agent can have identified a target range without having an organizing representation for the process; for example, the referring expression she uses to identify the target range might fail to provide scaffolding and guidance. On the other hand, having an organizing representation need not amount to having identified a target range simply because the agent might not know, or even have much justification for believing, that the facts in the range she has chosen to investigate are sufficient for inferring an answer to the question driving her epistemic process. For example, she might discover that she has been examining what is in fact a target range only towards the end of her epistemic process; I suppose that this is not altogether too uncommon.

(2) As with having identified a target range, it is certainly possible to engage in an epistemic process and complete it successfully without an organizing representation.

I should emphasize that a representation of a target range of facts can count as an organizing representation only if it is available more or less at the outset of the process; for only in this case can it actually provide scaffolding and guidance for the process. This guards against the following attempt to trivialize the notion: if an agent has correctly inferred a correct answer to the question driving her epistemic process, she must have had a representation of some set of facts that counts as a target range—the individual sentences that allowed her to infer the answer.

(3) The requirement that in order to have cognitive control one must have adopted an organizing representation is meant to capture part of the same intuition as the requirement that one must have identified a target range: one way in which an agent may fail to have ‘control’ over her epistemic process is that she is merely ‘groping around in the dark.’

(4) I have defined an organizing representation to be a representation of a target range of facts. Yet, there are many situations in which it is more natural to regard a representation of an *object* or a *system* of objects as the organizing representation.

For example, the representation one would most naturally consider to be the organizing representations for **Stage 1** of Artin’s proof is *the splitting field extension* E/F *of* $\mathbf{p}_5(x)$. This is just a definite description that picks out certain algebraic structure and, as such, it is a representation of a system of objects. However, it is employed in a context in which it is known that the objects in this system stand in determinate arithmetic relations to one another. Indeed, the set of facts about the relations of the elements in the splitting field contains all the facts about the arithmetic relations of the roots of $\mathbf{p}_5(x)$ to the coefficients, and this is just the range of facts we would naturally consider the target range for Artin’s **Stage 1**. Hence, there seems to be no harm in regarding *the splitting field extension* E/F *of* $\mathbf{p}_5(x)$ to be a representation of Artin’s target range in the sense in which an organizing representation is required to be a representation—for again, it need not be a representation of any of the individual facts in the target range.

For another example, consider the representation that organizes much of Abel’s proof, his general expression for the radicals in a solution by radicals as rational functions of the roots of the polynomial. While this representation is ‘embedded’ in a fact, namely

Any radical in a solution by radicals must have the form

$$r = (1/p)(y_1 + \alpha^{p-1}y_2 + \ldots + \alpha y_p)$$

for some prime p,

it does not do its job of organizing the proof just in virtue of being so embedded. More to the point, this representation in a sense ‘shows’ in its structure as a *symbolic artifact* what one might expect to be able to do with it; I will revisit this idea in Chapter 4.

For one final example, in Euclidean geometry, the paradigmatic epistemic process is aimed at solving some *geometric construction problem*. In such a process, the *diagram* that sets up the problem is certainly part of the organizing representation and, again, not in any obvious sense a propositionally articulated representation of a fact or a set of facts—even if it could no doubt be translated into one.

Thus, while admitting to a slight “abuse of notation,” I will regard representations of objects and systems of objects as candidates for being organizing representations. In fact, we will see that having an organizing representation of this kind can be a positive epistemic boon: an ontologically organized representation of a range of facts tends to lend itself to various kinds of representational manipulations that are epistemically powerful; this will be one of the central themes of Chapter 4.

3.6.4 *Epistemic Scaffolding*

Let us consider the following question: *What is the epistemic significance of knowing mathematical facts at the outset of a process aimed at proving a putative theorem?* One might think that the only correct answer is: the facts one knows at the outset will or will not allow one to deduce a statement of the theorem. Thus, one might think that the only epistemic significance of knowledge in this context is that one may or may not be able to *justify* a further claim to knowledge. What I hope to argue in this essay is that bits of mathematical knowledge an agent has at the outset of an epistemic process have at least two other important, and importantly different types of epistemic significances: they may or may not allow the agent to erect an *epistemic scaffolding*, and they may or may not provide her *epistemic guidance*.

In this section, I will discuss the notion of epistemic scaffolding; in the next one, I will consider locating and extracting facts directly relevant to answering the question driving the process; I will conclude this chapter by discussing what is perhaps the most important component of cognitive control, epistemic guidance. I shall have to take guidance and locating and extracting, components (3) and (4) in my characterization of cognitive control, in the reverse order: guidance is in the first instance guidance for pursuing these two aims, and so it is not possible to properly explain these components in the order in which they naturally appear in the characterization.

Epistemic Scaffolding

At the outset of an epistemic process, the agent will typically know some fairly limited set of facts that belong to the target range, and perhaps a few 'high-level' facts about the target range. For example, an undergraduate student reading Artin's proof of the unsolvability of the quintic might know that the splitting field extension E/F of the general polynomial $\mathbf{p}_5(x)$ of degree 5 is generated by the roots of $\mathbf{p}_5(x)$, but she would not know many of the particular facts about its structure; she might know some general field-theoretic facts about the organization of the extension E/F—that is, high-level facts about the target range. I think that something structurally similar would typically be true of a professional mathematician at the outset of a research program in an area with which she is not particularly familiar.

The notion of cognitive control is intended to identify a particular kind of configuration of epistemic resources that allows us to bring reason to bear on our epistemic process in a situation in which we do not yet know many of the individual facts in our target range. In order to bring reason to bear on our process in such a predicament, it is critical that we have available to us a representation of our target range that has *at least some degree of surveyable structure*. Without such a representation, all we have available to us is a *chaos* of unknown facts; to erect an epistemic scaffolding is to open up a *cosmos* of facts we can proceed to explore in a rationally orchestrated manner. Indeed, the notion of epistemic scaffolding may be thought of as capturing the familiar intuition that one way in which a cognitive agent may be *lost* in an epistemic process is that she *does not even know what she doesn't know*: a scaffolding is a structured representation of *what one does not yet know*. Thus, I recommend, one of the principal epistemic significances of knowing general facts about a target range at the out set of an epistemic process is that they are the kinds of facts that typically allow us to erect an epistemic scaffolding.

I want to emphasize, then, that having erected an epistemic scaffolding is the pivotal component of cognitive control: the contributions of having identified a target range and having adopted an organizing representation flow into the scaffolding, while the epistemic guidance for the process flows from the scaffolding. Having a scaffolding is the critical nexus for the other components of cognitive control.

Definition

Let **T** be the target range an agent has chosen for her epistemic process. She has an *epistemic scaffolding* for her process to the extent to which her organizing representation along with her overall epistemic resources affords her a representation of **T** as a *logical space of epistemically possible facts* in the following sense:

> *she has constructed*, *or can construct at will*, *a conceptually constituted representation of her target range as a set of properly individuated* ***locations*** **L** *such that*
>
> (*a*) *she can* ***pick out*** *each location in that set*;
>
> (*b*) *each location* ***covers*** *a determinate stretch of her target range*;
>
> (*c*) *she knows that each location* ***contains*** *a determinate range of epistemically possible facts* {α}; *that is, she knows that the facts covered by that location have one of the facts* {α} *as a consequence*;
>
> (*d*) *each fact* α *contained in a given location* ***rules out*** *the others in that location if it in fact obtains*; *and*,
>
> (*e*) *the facts contained in the various locations* ***exhaust*** *the space of epistemically possible facts about* **T** *that are directly relevant to inferring an answer to the question driving the process*.

Synopsis

To erect an epistemic scaffolding is to carve up the target range into cleanly demarcated, mutually distinguishable locations such that the facts in each location have as a consequence one among a determinate range of mutually exclusive, epistemically possible facts; and the totality of the latter facts is known to contain the ones directly relevant to answering the question one is trying to answer.

It is visible, I hope, that *having an epistemic scaffolding* constitutes a component of one possible answer to the question I used to motivate the notion of cognitive control: having erected a scaffolding is just the sort of representational accomplishment that facilitates reaching our epistemic aim when the resources we have initially are insufficient for actually reaching that aim. A scaffolding is a representation of our target range as consisting of a determinate range of locations one needs to examine in order to discover the facts that will eventually allow one to infer an answer to the question driving the process. I will say that *to locate an answer* is to *know the location* or locations one needs to examine in order to infer that answer, and to *collapse* a location is to find out which fact in the range of epistemically possible facts in it actually obtains.

When one is equipped with a scaffolding, one's epistemic process will typically consist of examining a number of locations by employing whatever epistemic resources one has, and gradually producing a representation of some stretch of the target range—a representation, that is, of the actual facts rather than just ranges of epistemic possibilities. As I noted above, target ranges in mathematics tend to be much larger than the set of facts actually required to infer an answer to the question driving the process. It is therefore usually not necessary to collapse all the locations in one's scaffolding in order to be in a position to infer an answer to one's question.

Let us start with a simple illustration.

(1) *Maps*

Suppose you are looking for El Dorado, the fabled City of Gold. While you do not know the exact location where the City is supposed to be hidden, through years of hard work, you have managed to determine that, if it exists at all, it would have to be located within a certain 500-square mile area covered by a dense jungle. In order to discover El Dorado or determine that it does not exist, you know that this is the area you need to explore; the set of all facts about the items in this stretch of terrain is your target range. Thus, you start out your epistemic process by conducting aerial survey of the area, generating what is an essentially accurate, albeit not very detailed map of the jungle. This map displays a number of rivers, a large lake, some mountains jutting out of the jungle, and so on. You can now divide up the terrain to be explored into determinate regions: the area between the rivers; the shores of the lake; the foothills of the mountains; and so on. These regions demarcate the locations in your (rather crude) epistemic scaffolding: each one covers a stretch of the target range and contains a determinate range of epistemically possible facts: *El Dorado is located here* and *it is not*. Given the size of the region to be explored, and given the difficulty of the terrain, it is not practicable to explore all of it in one go. But now given your scaffolding and your background of epistemic resources pertaining to your quest, you can plan out a number of expeditions. For example, some ancient bit of lore gives you a reason to believe that the City is located not too far from a body of water; so you might start out by exploring the shores of the lake. Another bit of lore gives you a reason to believe that there is a mountain to the west of the City; so you might explore the area between the rivers and east of the mountains in your map; and so on. This is epistemic guidance provided by your scaffolding. Of course there is still a indefinite number of epistemic challenges in your way: exploring the various particular locations is hard and dangerous work; some of them you may be able to explore from a boat; others might require cutting a path into the jungle; and so on. But the point is that your scaffolding allows you to map out the overall range of possible courses of action which, if carried out successfully, would eventually allow you to reach your epistemic aim: to determine the location of the fabled City of Gold.

Let us now turn to more serious examples.

(2) ***Artin's Epistemic Scaffolding for Stage 3***

Artin's target range at the beginning of **Stage 3** of his proof is the range of combinatorial facts about the relations of (sets of) elements in the Galois group G(E/F), where E/F is, again, the splitting field extension of the general polynomial $\mathbf{p}_5(x)$ of degree 5. I will focus on this target range because it allows us to appreciate the epistemic power of what Artin achieves in **Stage 2** and, indeed, appreciate how much *more* powerful his standing has become from what it was at the end of **Stage 1**.

Let us suppose that we do not at this stage know any of the particular facts about the relations of elements in G(E/F); this is a natural supposition at the beginning of **Stage 3**, since the aim of **Stage 3.1** is to determine *which* group G(E/F) actually is. We will suppose, however, that we know many of the basic general facts about finite groups.[29] Recall now that the aim of **Stage 3** is to show that G(E/F) is not a solvable group—that is, to show that there is no normal series with abelian quotients in this group. Hence, with the foregoing resources in place, one very natural way to look at the situation this: we have an epistemic scaffolding in which the locations are *sequences of embedded subgroups* of the form $\{1\} = G_1 \subset G_2 \subset ... \subset G_h = G(E/F)$. Our logical space has a good bit of structure:

[29] These may be regarded as 'high-level' facts about our target range (see Section 3.6.5(*b*)).

(1) Since G(E/F) is a finite group, we know from the get-go that any sequence of embedded subgroups in G(E/F) has a finite length, and that there is only a finite number of such sequences. Further, it is easy to see that G(E/F) is in fact isomorphic to the symmetric group $\mathbf{S}_5$ on five letters *without* even determining what the group-theoretic structure of G(E/F) ≈ $\mathbf{S}_5$ is. Thus, before we even work out the subgroups of $\mathbf{S}_5$, we know that the space of locations in our scaffolding is finite and fully determinate. Once we do work out these subgroups, we acquire excellent resources for explicitly identifying the various possible normal sequences in G(E/F) in terms of the various permutations that generate the groups in them. Thus, any sequence of subgroups can be picked out with the sets of generators $\{S_1, \ldots, S_h\}$ for the individual groups in it. This does require, of course, that we have in fact worked out what the subgroups of $\mathbf{S}_5$ are; an epistemic scaffolding does not come for free.

(2) Each location covers some as of yet unknown stretch of facts about the relations of elements in G(E/F) and contains two epistemically possible facts: *the sequence is a normal sequence* or *it is not*. That is, *each group in the sequence is a normal subgroup of the one in which it is contained* or *it is not*.

Further, as a location in our scaffolding, we can think of any normal sequence as 'containing' a range of 'smaller' locations: given any two consecutive groups G_j and G_{j+1} in a normal sequence, we can think of $\{G_j , G_{j+1}\}$ as demarcating a location on its own right, one that contains two epistemically possible facts: *the quotient group* G_{j+1}/G_j *is abelian* or *it is not.*

It is clear that in both cases the range of epistemically possible facts in each location is fully determinate, and that the epistemically possible facts in each location are mutually exclusive, as required by parts (3) and (4) of my definition, respectively.

Finally, and this is really the main point, this scaffolding contains a location for every epistemically possible fact that is relevant to the question of solvability of the group G(E/F). Now of course there are all sorts of epistemically possible facts about the structure of G(E/F) that are not packaged into one of our locations. The point is precisely that we can organize the range of epistemically relevant, as of yet unknown facts in this highly regimented fashion.

In order fully to appreciate just how powerful this mode of organizing the logical space is, we should keep in mind that the fact as to whether a subgroup A is normal in B, and the fact as to whether the quotient group B/A is abelian, depend in complicated ways on the mutual relations of the elements in each one, as well as on the relations of those elements to the elements of the other one; these are the facts covered by the various locations. So to have this much structure in play at the outset of **Stage 3** is *really* quite remarkable: we can organize our logical space so as to 'package' and 'store away' vast amounts of mathematical data *we do not yet have*. Finally, this packaging leaves out in the open *precisely* those features of the situation that are directly relevant to the solvability by radicals of the polynomial. With this scaffolding in place, *we can go to work*.

It deserves to be emphasized out that while our epistemic standing at the end of **Stage 1** of Artin's proof is in structurally similar to the one at the beginning of **Stage 3**, in many ways it is significantly weaker. Recall that Artin's initial criterion for solvability is that a polynomial equation $\mathbf{p}(x) = 0$ is solvable by radicals if and only if the splitting field E of $\mathbf{p}(x)$ is *contained* in a radical extension L of F. Thus, one might think that we can view *sequences of intermediate fields in* E/F as locations in much the same way we have viewed sequences of subgroups of G(E/F) as locations; the epistemically possible facts in each one would be *the sequence is a radical sequence* or *it is not*. But this would fail to incorporate most of the epistemically relevant, epistemically possible facts in the target range: for the extension E/F need not *itself* be a radical extension even if it is *contained* in one. The closest we can get to the sort of scaffolding we have at the beginning of **Stage 3** is to take the scaffolding just sketched and add a parameter 'L' for the possible finite extensions of E. Clearly this *explodes* the range of epistemically possible facts under consideration. In particular, there is *no* hope of being able to pick out all the epistemically possible finite extensions of E explicitly the way my definition requires.

This gives us a way of appreciating just how difficult it would be to attack the issue of solvability by directly considering the organization of the splitting field extension E/F and, concomitantly, just how remarkable the epistemic contribution of Artin's **Stage 2** really is.

(3) *Character Table for a Finite Group G*

The following sequence of results in the theory of *group characters* allows us to erect a real nice epistemic scaffolding for the process of computing the *irreducible characters* of a finite group G. With these results in hand, a competent mathematician would typically be able to work out at least portions of the character table for a given finite group G, provided that the cardinality of G is not exceedingly large.[30]

1. *Any character is constant on the conjugacy classes of* G;

2. *The number of irreducible characters of* G *is the number of conjugacy classes of* G;

3. *The degree of any irreducible character* χ *divides the cardinality* #G *of* G;

4. $\sum_{\chi} \deg(\chi)^2 = \#G$, *the sum on the left taken over the irreducible characters of* G;

5. *The orthogonality relations for irreducible characters.*

Results 1 and 2 determine the basic structure of our epistemic scaffolding: we need to fill out an *h*-by-*h array* of entries where *h* is the number of conjugacy classes of G. The (*n*, *m*) entry is to be

[30] See, for example, Serre, *Linear Representations of Finite Groups*.

filled with the value of the *n*-th irreducible character on the *m*-th conjugacy class of G—that is, by some particular complex number. Thus, we can think of the (*n*, *m*) entry as one of h^2 locations in the scaffolding, occupied by the range of epistemically possible values of the *n*-th irreducible character on the *m*-th conjugacy class. This range is fully determinate and each location can be picked out simply by enumerating the entries as we have done. One of the interesting features of having this scaffolding is that before we start working on the actual contents of the entries, we tend to work on the scaffolding itself. For example, one might try to work out a generator for each of the conjugacy classes of G and, typically, at least some of the degrees of the as of yet unknown irreducible characters.

Certainly the epistemically possible facts contained in the various locations exhaust the range of facts directly relevant to determining the irreducible characters of G: each irreducible character is individuated by its values on the *h* conjugacy classes.

Results 3, 4 and 5 provide our scaffolding a fair bit of inferentially engageable structure. In particular, we can use the orthogonality relations to compute values of a character at conjugacy classes, given enough known values for other classes or other characters. In a sense to be spelled out later, Result 3 provides a good bit of guidance for the search for irreducible characters, especially at the stage where none or only very few of the characters have been found. Finally, results 4 and 5 provide further guidance throughout the search process, and especially towards the end: once we have discovered a few characters, we can typically rule out a whole range of epistemic options. Note that this fits what I required in component (3) of my characterization of cognitive control: *scaffolding provides guidance*.

Comments

(1) Let us begin with a few brief clarifications concerning the five components of my definition of scaffolding.

(*a*) To be able to *pick out* a location is, simply, to have a referring expression that is known to uniquely denote that location among the set of all locations in the scaffolding. This is not to require that the expression in question allows one to represent the facts covered by or contained in that location; it is merely to require that the range of locations is fully determinate and that one can *distinguish* the locations from one another.

(*b*) The requirement that each location in an epistemic scaffolding covers a stretch of the target range is meant to ensure that a scaffolding is in fact a representation of the target range, one we can have when we do not yet know many, or even any, of the individual facts in that range. Unlike the organizing representation, a scaffolding is not required to be a representation of the target range *as a whole*. The idea is rather that a scaffolding is a representation of those parts of the target range that are known, or thought to be, directly relevant to inferring the answer to the question driving the epistemic process.

(*c*) The requirement that each location in an epistemic scaffolding *contains a determinate range of epistemically possible facts* allows that one may not be able to *explicitly specify* the individual possible facts in that range. We saw an instance of this in our third example above: one typically does not know at the outset just which complex numbers could occupy a given entry in the *h*-by-*h* array that is the yet to be completed character table. Nevertheless, the range of epistemically possible facts in each location is fully determinate in the sense that each actual entry is known to be a complex number; there are many other constraints one can find for important special cases. Note, for contrast, that the requirement on one's ability to represent the contents of the locations is *much* less demanding than the requirement on one's ability to represent the range of locations itself. This is a central part of the notion of scaffolding: even if we do not know many of the particular facts, we have a determinate superstructure into which we can plug those facts as they become available during our investigation.

(*d*) The requirement that the epistemically possible facts contained in each location are *mutually exclusive* is a central part of the notion of scaffolding: we can mark out inferentially meaningful packages in our target range. That the facts in each location are mutually exclusive is one way in which a scaffolding provides an *inferentially responsive* framework for the epistemic process; I will return to this theme in paragraph (8) below.

(*e*) The requirement that the epistemically possible facts contained in the scaffolding exhaust the range of facts directly relevant to answering the question allows, first, that some of the locations do *not* contain any such facts and, second, that the agent does not know *which* of the locations contain facts directly relevant. Indeed, it is a central part of my account of cognitive control that the agent may have to do a good deal of hard work in order to locate the facts directly relevant to answering her question—that is, to identify the locations that actually contain such facts.

That the epistemically possible facts in the scaffolding *exhaust* the set of facts in the target range directly relevant to answering the question is often clear by the time one is able to construct a representation that satisfies the other three requirements. We saw in our second and third examples that the contents of the locations exhausted the range of facts directly relevant to answering the question almost "by construction." This does, of course, depend on exactly what is meant by "directly relevant." For now, the intuitions will have to suffice; I will take up this issue in Section 3.6.5(*c*).

(2) While it should be beyond serious contestation that the notion *scaffolding* does in fact apply in the foregoing examples, one might justifiably wonder just how typical it is to have a scaffolding in the fairly exacting sense required by my definition. Thus, let me hasten to make two remarks.

First, as having cognitive control overall, having an epistemic scaffolding is a matter of degree. It is certainly possible to have a representation of one's target range that has some features of an epistemic scaffolding but lacks others. For example, we may be able to represent the range of locations 'abstractly,' but not be able pick out many, or even any, of the individual locations; this would be the case, for example, with Artin's scaffolding at the end of **Stage 1**, where we had the parameter L ranging over the finite extensions of E.

Second, having a fully constructed scaffolding at the outset of one's process is meant to be a substantial requirement and is, perhaps, not met altogether too often. One will typically have to have a fair bit of knowledge about high-level features of the target range in order to erect a fully constructed scaffolding, and typically such knowledge is not yet available at the very beginning of the process.

I am happy with these two states of affairs. First, they fit my overall policy of making the notion of cognitive control demanding enough to bring out subtle differences in the quality of control over epistemic processes. There is no harm in saying that most actual agents fall a little short of having full control over their processes as long as we can use the notion to discern epistemically significant differences between them. The real danger would be in making the definitive criteria for having cognitive control too easy to satisfy, for then the notion would lose its discriminatory power. Second, even if mathematicians typically do not to have fully constructed scaffoldings at the beginning of their epistemic processes, we will see in our case study that scaffoldings are often erected during the early stages of the process, and that this is indeed one of the hallmarks of well-orchestrated epistemic processes.

(3) An epistemic scaffolding is an *object* only in whatever sense a representation is an object; for to say that an agent *has* an epistemic scaffolding is just a compact and, so I hope, intuitively suggestive way of saying that she has a certain kind of representation of the target range. I suppose one could say that the object called "epistemic scaffolding" is the logical space of epistemically possible facts in the target range, organized in the manner just described; however, this kind of talk should be seen as nothing more than an informal device adopted for convenience. I don't know what a logical space is anyway.

(4) The notion of scaffolding allows us to appreciate the crucial importance of knowing at least a few *general*, *high-level facts* at the outset of one's epistemic process. For as our case study will strongly suggest, epistemic scaffoldings in mathematics are typically erected by highly conceptually articulated representations of ranges of high-level facts about the target range. We will see this in more detail in Chapter 4.

(4) One of the principal challenges in mathematical epistemic processes is to *create locations* one can then proceed to investigate. In particular, I will argue that *concepts of objects* and *concepts of systems of objects* are among the most important tools we have for creating locations in mathematical target ranges. In another essay, I will argue that part of the epistemic significance of being able to conceive the *physical world* as consisting of properly individuated objects and determinate systems of objects is that doing so is one of the basic ways we have of creating locations for our empirical epistemic processes and, as such, one of the basic ways of acquiring cognitive control over epistemic processes in empirical cognition.

(5) It is often convenient to consider *collections* of locations as 'large-scale' locations on their own right. For example, in our presentation of Artin's scaffolding, each sequence of subgroups in G(E/F) was seen as a location, and the normal sequences were seen as containing a number of 'smaller' locations.

(6) Sometimes as we move through the stages in a proof, the scaffolding keeps getting more and more structured as we acquire new epistemic resources.

I think that this is one of the many different kinds of features a proof may have that triggers the response that the proof is *understandable*. A proof in which the master scaffolding keeps getting more and more structured might be said to *stack up*: the bits of knowledge are integrated so as to provide a single coherent, ever improving overview of the terrain of facts under investigation. The proofs of Abel and Artin both stack up quite nicely; at any rate, considered on their own terms, they stack up nicely, even if Artin still clearly comes out on top.

(7) One of the basic features of a scaffolding is that it is *inferentially responsive*. There are at least two distinct aspects to this. On the one hand, I required in my definition that each location is occupied by a range of epistemically possible facts that are *mutually exclusive*. Thus, to discover one is to *collapse* that location in the sense that the others are thereby ruled out. On the other hand, we will see in Chapter 4 that there are various ways in which the locations may be *connected*. The most obvious sense in which locations may be connected is that the contents of one location constrain the epistemically possible contents of another. This is precisely what we saw in our third example: the orthogonality relations of the characters are connections in the scaffolding. We will see, further, that Artin's scaffolding for his **Stage 3** is more connected in an epistemically important way than Abel's. My definition allows, however, that locations in a scaffolding may not be connected. For example, the locations in our second example are not

connected: the fact as to whether one sequence of intermediate fields in E/F is a radical sequence does not in general have any consequences about the other sequences in E/F. A highly connected epistemic scaffolding is a bonus, not a requirement for having control.

(8) Having an epistemic scaffolding has two principal significances as a component of cognitive control. On the one hand, a scaffolding is a conceptually structured overview of the terrain of epistemically possible facts, one that is highly inferentially engageable. As such, it captures part of the idea that to have cognitive control is to have a panoptic overview of the epistemic terrain. On the other hand, a scaffolding provides guidance for the epistemic process; I will discuss the latter role of scaffoldings in Section 3.6.6.

(9) In Section 3.5, I explored the idea that a substantial mathematical process will typically contain a hierarchy of multiply embedded subprocesses. This suggests that we might wish to require in our characterization of cognitive control that the scaffolding of a subprocess is connected in some 'organic' fashion with the scaffolding of the process in which it is embedded. This would be yet another way of implementing the idea that having cognitive control involves being able to start with an overview of the situation and 'home in' on the details. We will see in our analysis of Abel and Artin, however, that this would be too exacting a requirement. While the aim and, typically, the target range of a subprocess are indeed dictated by the process in which it is contained, we must allow that a subprocess can be autonomous in that it has its own organizing representation and so, a scaffolding not intrinsically connected with the scaffolding of the ambient process.

(10) Finally, I need to clarify the role of epistemic scaffoldings in situations where the agent *does* know quite a few individual facts in her target range already at the outset of the epistemic process.

The notion of scaffolding is intended to capture a certain type of representational ability an agent may have in a situation in which she knows which terrain of facts she needs to investigate, but does not yet know many of the particular facts in that terrain. She will explore the various locations, find out which fact they actually contain and, if all goes well, she will eventually be able to infer an answer to her question. In this process, the organization of the scaffolding provides her aim and location guidance.

We can imagine an idealized process in which the agent collapses *all* the locations in the scaffolding so as to gradually transform the scaffolding into a representation of the particular facts in the target range. Most actual mathematical processes do not, however, involve collapsing all the locations. As we noted above, in real-life mathematical research the target range tends to be much larger than the set of facts actually required to infer the answer, and just which ones are required will typically become clear somewhere in the course of the process.

Either way, there will be a point in the process at which the scaffolding has served its purpose and will, in effect, be abandoned: once enough of the facts in the target range are known, the rest of the proof will consist of simple logical parsing together of these facts to infer the answer. At this stage, the agent no longer needs to reach into her background of epistemic resources for new bits of knowledge; she does not need to apply any new concepts to articulate new facts or demarcate new locations; she does not need to "go out" and look for new bits of knowledge. Everything she needs to infer the answer is already at hand. This is what the very final stage in long proofs will typically look like.

Now consider a situation in which the agent is already in this situation at the outset of her epistemic process. This is what often happens in subproofs embedded deep in the structure of a long proof: with all the setting up that has taken place in the subproofs leading up to the one in question, the epistemic process may consist of little more than applying a few rules of inference to the bits of knowledge at hand.

In such a situation, one natural thing to say is that the process has no scaffolding: the known facts are already sufficient for reaching the aim, and the agent either knows or has good justification for thinking that this is so. Thus, the set of sentences articulating those facts can be thought of as taking over the role of a scaffolding: it is already an explicit representation of a target range—a set of facts sufficient for inferring the answer.

But there is a fairly natural way to apply the notion of scaffolding to describe this kind of epistemic standing. In the situation the basic notion of scaffolding is intended to capture, the scaffolding is typically a set of locations organized by concepts of objects; thus, we might speak of an *ontic scaffolding*. In the kind of situation under consideration here, we might speak of an *inferential scaffolding*. The locations are demarcated by the available rules of correct inference directly applicable to the facts explicitly articulated.

For example, in a formal derivation of the kind that might be given as an exercise to a beginning logic student, we have a set of explicitly articulated premises along with the desired conclusion, and the student is asked to apply the rules of inference in some specific system of deduction to produce a derivation of the conclusion from the given premises. In a situation like this, the locations are demarcated by the rules of inference of the system: we can think of each location as containing all the epistemically possible derivations that begin with the application of the corresponding rule of inference. If a given rule does not apply to the premises, then the location, once collapsed, would be empty. If a given rule does apply, one can explore that location further by pursuing an inferential path that begins by applying the corresponding rule.

Thus, locations in an inferential scaffolding will typically have locations embedded in them in the sense discussed in paragraph (6) above.

The point of applying the notion of scaffolding in this way is that we can still make sense of the idea of the scaffolding providing guidance. Location guidance might be enjoyed, for example, in virtue of having enough experience with the rules of inference to know which rules are likely to be useful in deriving a certain kind of conclusion from a certain kind of set of premises; this is just the sort of epistemic mastery we want our students to acquire in an introductory course on formal logic. Aim guidance can be acquired in various ways; I will discuss this in the section on guidance.

The notion of scaffolding and, in particular, the contrast between ontic and inferential scaffoldings gives me the occasion to make an actual philosophical point about the epistemic character of mathematical research as a human conceptual enterprise. One of the things the notion of cognitive control is meant to bring out is that real-life mathematical research is not in the first instance an activity of drawing logically valid inferences. It is an activity of *making rational choices* about how to proceed: choices as to which terrain of facts one should examine; choices as to how to conceptually represent the terrain one has chosen to examine; choices as to how to organize one's representation of the as of yet unknown facts in that terrain; choices as to which particular piece of knowledge to pursue at a given juncture in the process; which particular locations to examine, which manipulational devices to apply. The sort of epistemic activity that is happily described *simply* as drawing logically valid inferences constitutes only a small fragment of the overall range of epistemic activities in mathematical epistemic processes, and tends to happen at the very end at that. We will see this quite concretely in our analysis of the processes of Abel and Artin in Chapter 4.

The temptation, if it is one, to think that mathematical epistemic activity can be happily described simply as an activity of drawing logically valid inferences is no doubt due to focusing on completed proofs ready to be 'archived.' But even in the course of reading a proof, the real epistemic task is not in following the individual inferential moves. It is in having a view of the choices, and the range of possible choices, of the sort just described. And when such choices are in view, I will say, the agent has cognitive control over the process of reading the proof. Now of course it is possible in one sense to 'read' a proof without having any of this in view; but, as we discussed in Section 3.3, that is just the sort of reading that mathematicians routinely characterize as reading without understanding.

3.6.5 Locating and Extracting Features Directly Relevant to the Question

Recall the fourth component of our characterization of cognitive control:

Given the epistemic guidance provided by her scaffolding and her overall epistemic resources, *the agent is able to locate and extract features of the target range that are directly relevant to answering the question* **Q** *driving the process by using her devices for manipulating representations*.

In my experience, when working mathematicians are called upon to reflect on the proofs of Abel and Artin, what they usually single out as the most striking difference is that Abel does not manage to *make explicit* any features *directly relevant* to the solvability by radicals of $\mathbf{p}_5(x) = 0$, whereas Artin does manage to do so. Abel merely rules out *case by case* the existence of the radicals that would have to exist in order for there to be a solution by radicals, whereas Artin shows that all of this *comes into focus* in the fact that the Galois group of $\mathbf{p}_5(x)$ is not solvable: the facts directly relevant to solvability are certain facts about the organization of the system of subgroups and quotient groups of the Galois group. Thus, one might say, Artin manages to *locate* the crucial facts in the organization of the system of subgroups of G(E/F), while Abel does not manage to locate anything in this sense.

Such, anyhow, are the ordinary mathematician's intuitions. Obviously there is an imposing philosophical task here: what sense can we make of the ideas of *making explicit* a feature of the target range, a feature's being *directly relevant* to answering a question, and *locating* a feature in some system of facts or objects? The purpose of this section is to make some initial headway on these issues.

One remark before we proceed. I want to acknowledge from the start that, much as with the notion of target range, there is an obvious and tempting approach to analyzing the differences between Abel and Artin at issue in this section: one might say that Abel does not see the 'metaphysically right' features of the set of permutations, whereas Artin does—something like, the features that 'produce' the facts about solvability by radicals. However, keeping with my anti-metaphysical orientation, I will try to analyze the differences in what Abel and Artin accomplish epistemically without appealing to ontological or metaphysical notions. Hence, I will try to analyze ideas such as "directness of relevance" in epistemic terms. I will not try to produce sustained arguments against the metaphysical order of explanation: I take it that no such explanation now exists, but should a candidate emerge, I would be happy to consider it.

(*a*) *Internal Aims of Mathematical Epistemic Processes*

In the course of his proof, Artin achieves a number of interconnected *internal aims*. Thus, for example, all the facts relevant to the solvability by radicals of $\mathbf{p}_5(x) = 0$ are *collected in one place* as facts about the organization of its splitting field extension of $\mathbf{p}_5(x)$. This greatly facilitates looking for *patterns* among those facts. Further, the field and group-theoretic concepts and general facts about fields and groups allow Artin to *locate* the facts most directly relevant to solvability in the organization of the Galois group G(E/F) of $\mathbf{p}_5(x)$. Finally, with further such concepts in hand, he can explicitly articulate those features. It is much less clear whether Abel achieves any of these aims: there seems to be little by way of collecting facts in one place, little by way of locating features directly relevant to the question of solvability, and even less by way of explicitly articulating those features.

I propose, accordingly, that mathematical epistemic processes, particularly processes of writing and reading proofs, have three recurring *internal aims*:

(*a*) *consolidating facts*: Artin uses the splitting field extension E/F to consolidate arithmetic facts relevant to the question of the solvability by radicals of $\mathbf{p}(x) = 0$;

(*b*) *locating facts*: Artin uses the Galois correspondence to locate facts directly relevant to solvability in the system of subgroups of the Galois group; thus, a polynomial equation $\mathbf{p}(x) = 0$ is solvable by radicals if and only if the Galois group G(E/F) of its splitting field is a solvable group—that is, contains a normal series with abelian quotients.

(*c*) *extracting facts*: Artin uses the group-theoretic concepts and facts to extract the facts directly relevant to solvability: the general polynomial equation $\mathbf{p}_5(x) = 0$ is not solvable by radicals 'because' its Galois group does not contain a normal sequence with abelian quotients.

These are *engineering aims* in the sense in which it is an engineering aim to make sure that the foundation of a building does not sink, or that a particular load-bearing wall can support the required weight, and so on; they are intermediate aims in the service of the final aim of erecting a structure that is comfortable and safe to inhabit. The idea is that the success of a mathematical epistemic process often depends on the extent to which we are able to extract at least some facts directly relevant to the question we are trying to answer; this, in turn, often depends on the extent to which we are able first to locate those facts; finally, this often depends on the extent to which we have managed to consolidate our target range.

It is certainly possible to complete a mathematical epistemic process successfully without being particularly successful in pursuing these three internal aims, however. In fact, reaching them has exactly the same status as having the first two components of cognitive control: while not necessary for successfully completing the process, reaching them amounts to having a specific kind of epistemic mastery over the process.

The requirements that one can consolidate one's target range, locate the features directly relevant to the question driving the process and, finally, extract those features fit my overall ideology about cognitive control: to have cognitive control is, in part, to occupy an epistemic standing wherein one begins with a panoptic overview of the epistemic terrain and, in virtue of having the appropriate concepts and bits of knowledge, one can home in on the critical features of that terrain.

I do not regard consolidating to be as essential as locating and extracting; in turn, I do not regard locating to be as essential as extracting. After all, from the point of view of reaching the final aim of the process, extracting the critical features is clearly the prime requirement, whereas locating and consolidating are in a sense 'merely' preparation for it. Consolidating is particularly problematic in the sense that, as we will presently see, it is an epistemic accomplishment that has an expressly *ontological* aspect. As such, I refrain from including it in my characterization of cognitive control, thus keeping with my anti-metaphysical orientation. In any case, the bottom line for the task at hand is that all three accomplishments mark out epistemically significant differences between what Abel and Artin achieve in their respective proofs. Whether consolidating, or even locating, should be considered a part of the very notion of cognitive control or merely particular ways of acquiring cognitive control is of no great consequence here.

(*b*) *Consolidating Facts*

To consolidate a set of facts is to adopt a mode of representation that justifies treating those facts as facts about a single object or a coherent system of objects.

In order to avoid an obvious trivialization, we must further require that one be able to refer to the consolidating object in a way that does not depend on referring to the facts to be consolidated or the act of consolidating itself. Thus, given a set *S* of facts, we cannot consolidate them just by saying: *let x be the object the facts in S are about*.

Consolidating a set of facts can have a number of different epistemic significances depending on the specific context in which it takes place. Here, however, I will only be interested in consolidation as preparation for locating and extracting features. Before we go on to consider this significance of consolidating, let us note the following two distinctions.

Single Object and System of Objects

There are two epistemically different basic types of consolidation: one in which a set of facts is consolidated by a single object, and we examine the overall features of that object, another in which a set of facts is consolidated by a system of distinct objects, and we examine the mathematical relations of those objects.

In Galois' original approach to solvability by radicals, there are instances of both kinds of consolidating critical to the approach as a whole. First, Galois appears to have been the first mathematician to regard the set of permutations of the roots as a single, coherent object on its own right. It is not that the mathematicians before him could not use expressions such as "the permutations of the roots," but they did not employ in their *reasoning* the idea that the totality of the permutations can itself be meaningfully regarded as an object. Second, Galois considered certain subsets of the group of permutations and, in particular, the ways in which those sets got mapped to one another under certain operations on the group as a whole. He noticed that the way in which the group of permutations splits up into subsets under those operations is relevant to the issue of solvability by radicals. He did not quite take the next step where those subsets are regarded as elements in yet another consolidating object, however. Those subsets would now be thought of as the *cosets* of a *normal subgroup* N in G(E/F), and the consolidating object would be the *quotient group* G/N.

It is of course essential to Artin's approach that the F-automorphisms of E form a group, the Galois group G(E/F), and further, that they can also be regarded as consolidated into a system of objects with determinate relations among them, namely the subgroups of G(E/F) and their relations of (normal) containment.

Combination and Ontological Innovation

There are two principal ways of effecting consolidation: we *combine* a number of previously recognized objects into a single object broadly of the same sort, and we come to *recognize an entirely new type of object*.

Perhaps the most pervasive example of the first way of effecting consolidation is the use of *homomorphisms to embed* a number of distinct structures in a single more encompassing structure. Thus, we form the *direct sum* of algebraic structures; we consider the *regular representation* of a group G that consolidates all the distinct non-isomorphic irreducible representations of G; we consider the *p*-adic numbers. Aside from these more specialized modes of employing embeddings, the general technique of putting a number of structures inside a larger one fairly permeates modern mathematics.

Perhaps the most pervasive example of the second way of effecting consolidation is the recognition of various *sets* of objects as objects on their own right, as “completed totalities.” In our case study, we saw multiple levels of this way of effecting consolidation in Artin’s approach, and just now noted that consolidation of this kind was crucial to Galois’ approach.[31]

Epistemic Significance of Consolidating

As far as my notion of cognitive control is concerned, I only need to examine one of the no doubt numerous epistemic functions of consolidating: to consolidate a set of facts is one way of setting the stage for locating and extracting.

Let us first of all focus on *organizing representations* that consolidate a target range for the process and, in particular, on *consolidation by a system of objects*. We have already seen, and will see in more detail in Chapter 4, that having such a representation has two principal epistemic significances.

[31] Among the mathematicians of the late 19th century, Richard Dedekind was the most forceful and certainly the most successful advocate of the intellectual power of consolidation. His theory of *ideals*, now part of the foundation of modern mathematics, is a superb example of a theory that essentially involves consolidation on multiple levels. Dedekind also pushed the idea of treating the various *number systems* as objects on their own right. See Avigad, “Methodology and metaphysics in the development of Dedekind’s theory of ideals” for a representative sample of quotes from Dedekind. The primary source here is Dedekind’s epoch-making 1877 treatise *Sur la théorie des nombres entiers algébrique*, translated by John Stillwell as *Theory of Algebraic Integers*.

First, this kind of consolidation allows one to *erect an ontic scaffolding*, one in which the locations are demarcated by objects in the consolidating system. This is exactly the sort of scaffolding Artin has for his process, while Abel does not: Abel does not have a representation that could effect consolidation by a system of objects. The set of permutations of the roots of $\mathbf{p}_5(x)$ might be thought capable of playing this role, but in fact it is not: Abel does not have the group-theoretic concepts, such as *group*, *subgroup* or *quotient group*, that are required for the set of permutations to function as a consolidating system. Again, it was Galois' pivotal contribution to introduce these concepts, at least in an embryonic form. The epistemic significance of an ontic scaffolding, in turn, is that it often facilitates *locating* the features crucial to the process.

Second, this kind of consolidation makes it possible to recognize and articulate *large-scale patterns* in one's target range—essentially, facts about collections of facts. The epistemic significance of such large-scale patterns is that often they are just the facts *directly relevant* to answering the question driving the epistemic process; we will come back to this in the next section. The basic idea is, simply, that the features of the consolidating system of objects are, so to speak, *sensitive* to patterns among the facts that system consolidates.

This is exactly what we see in Artin's epistemic process. For example, that a given set of permutations is a *subgroup* of G(E/F) is in a very natural sense a pattern in the facts about the arithmetic relations of the permutations: the product of all permutations in that set is again a permutation in that set, and so on. Thus, Artin can articulate facts such as *the group of automorphisms of the splitting field extension of* $\mathbf{p}_5(x) = 0$ *is not a solvable group*. This fact cannot even in principle be articulated until multiple levels of consolidation have taken place. First, we need to have consolidated the rational expressions of the roots into the splitting field, and learned to recognize intermediate fields in it; second, we need to have consolidated the automorphisms of this field into to the Galois group, and learned to recognize subgroups in it; third, we need to have consolidated cosets of normal subgroups into quotient groups. Abel is clearly not in a position even to begin articulating such large-scale patterns.

I will not attempt to give a formal analysis of the notion of large-scale pattern, given that the intuitive notion exemplified here is quite sufficient for the purposes of this essay. Again, a large-scale pattern is essentially a *fact about a set of facts* or, as it is often more intuitive to think, a fact about the consolidating object or system of objects.

(*c*) *Locating an Answer*

Artin locates facts directly relevant to the solvability by radicals of $\mathbf{p}(x) = 0$ in the *system of intermediate fields* of the splitting field extension E/F of $\mathbf{p}(x)$ and, later on, he locates further facts even more directly relevant in the *system of normal subgroups* of the Galois group G(E/F) of the splitting field extension. It is not clear that Abel locates anything in this sense; at any rate, it does not seem that he locates anything *very well*.

To have located an answer to the question **Q** *in a location* **L** *in one's epistemic scaffolding is to know or have substantial justification for believing that the facts that are directly relevant to inferring an answer to* **Q** *are contained in* **L**.

Thus, to simplify just a little, to locate an answer is to come to *know the location* of the facts directly relevant to inferring that answer. I am here using "location" in the sense introduced in our discussion of scaffoldings—a location is a well-individuated range of epistemically possible facts. Hence, locating can be thought of as a more high-grade form of identifying a target range of facts for the process.

Directness of Relevance

Artin infers the fact that $\mathbf{p}_5(x) = 0$ is not solvable by radicals from the fact that the Galois group G(E/F) of the splitting field extension E/F of $\mathbf{p}_5(x)$ is not a solvable group. But finite groups can instantiate the property *being solvable* in arbitrarily many different ways; for there are arbitrarily many different normal series with abelian quotients a finite group can have.

The intuition, then, is that the property of the Galois group of being solvable (or not) is more directly relevant to the solvability by radicals of the polynomial than the *particular facts* about the sequences of subgroups, and the latter are more directly relevant to the solvability of the polynomial than the particular facts about the arithmetic relations of the individual elements in the group. The thought is that what *matters* for the solvability are not the *particular configurations* of facts about the subgroups or individual elements, but rather the *large-scale pattern* that there is a normal series with abelian quotients in the group. For there are many different such configurations that *would* have the consequence that $\mathbf{p}(x)$ is solvable, but the Galois group of any solvable $\mathbf{p}(x)$ *must* have a normal sequence.

These observations suggest that we try to capture the idea of directness of relevance with something like the following definition. If **S** is a sentence, let M(**S**) be the class of models of **S**.

Let **A**, **B** *and* **C** *be sentences. Then* **B** *is more directly relevant than* **A** *to* **C** *just in case*

$$\mathrm{M}(\mathbf{A}) \subset \mathrm{M}(\mathbf{B}) \subseteq \mathrm{M}(\mathbf{C}).$$

That is, any model of **A** is a model of **B** and any model of **B** is a model of **C**, but there are models of **B** *that are not models of* **A**.

For example, suppose that **A** is the conjunction of some sentences specifying the relations of elements in some particular solvable group *A*, and suppose that **B** is the sentence *G contains a normal sequence*; finally, suppose that **C** is the sentence *any polynomial whose Galois group is G is solvable by radicals*. Certainly any model of **A** is a model of **B**, and any model of **B** is a model of **C**; finally, there are a great many models of **B** that are not models of **A**, namely all the various solvable groups other than *A*. Thus, according to the foregoing definition, **B** would be more directly relevant to **C** than **A**. Likewise, suppose that **A** is a conjunction of some sentences describing some particular normal sequence *S* in some particular group *A*, and suppose that **B** and **C** are as before. Again, any model of **A** is a model of **B**, and any model of **B** is a model of **C**, while there are again many models of **B** that are not models of **C**. Thus, **B** would again be more directly relevant to **C** than **A**.

Now I think that the foregoing definition captures an aspect of our intuitions pertaining to directness of relevance. After all, the sentence **B** in each of the two cases may be thought of as articulating the 'pattern' directly relevant to the solvability by radicals of $\mathbf{p}(x)$, while in each case the sentence **A** is, intuitively, the 'underlying' configuration of particular facts that 'instantiates' this pattern. It is not surprising that it might be possible to capture this intuition about patterns in terms of *generality*—after all, a pattern is a *kind* of configuration of facts that may be instantiated in a number of different ways. Further, there is a healthy intuition to the effect that, in the situation of the definition, the sentence **B** is more directly relevant to **C** than **A** simply in virtue of the fact that, against a suitable background theory, **C** can be inferred both from **B** and **A**, but from **B** 'more directly' in the sense that **B** can be inferred from **A** but not *vice versa*.

There is a problem, however: it is very difficult to see how this definition should be applied when comparing two *sets* of sentences and, in particular, two *proofs*. For suppose we took **A** to be the *conjunction* of the sentences in one of the proofs and **B** the conjunction of the sentences in the other. In many cases, the two conjunctions will have the same models. This is a problem because there are situations in our case study where there is a strong intuition to the effect that Artin's approach manages to identify the relevant pattern while Abel's does not and yet, both proofs deal with the same structure from the start.

This is the case, for example, with their respective proofs of **Theorem 6**. This theorem states that any rational function in five independent variables with 5 distinct values under the permutations of those variables can be expressed in a certain canonical form. I will consider the two proofs in detail in Chapter 4, but the essentials are as follows:

Abel

1. Let $v_1, ..., v_5 \in \mathrm{E}$ be the five distinct conjugates of $v = v_1$, and let $v_1, ..., v_\eta$ be the conjugates of v_1 one obtains by applying all the permutations that fix x_1; call the set of such permutations $\mathfrak{I}_1$. Then the expression

$$v_1 + v_2 + ... + v_\eta \qquad (*)$$

is clearly invariant under the permutations in $\mathfrak{I}_1$, since $\mathfrak{I}_1$ just permutes the $v_1, ..., v_\eta$ among themselves. So we can apply **Theorem 6*a*** which says that any such expression is a polynomial in x_1 with symmetric coefficients, which is what we needed; call this expression $\varphi(x_1)$. So we now want to show that v itself has this form.

2. There are five possibilities: $\varphi(x_1) = v_1$, $\varphi(x_1) = v_1 + v_2$, $\varphi(x_1) = v_1 + v_2 + v_3$, $\varphi(x_1) = v_1 + v_2 + v_3 + v_4$, and $\varphi(x_1) = v_1 + v_2 + v_3 + v_4 + v_5$. Abel's proof proceeds by considering each one in turn. In the first case, the result is, as such, established; in the third case, Abel shows that the expression

at hand yields the desired one; finally, Abel rules out cases 2, 4 and 5 by appealing to elementary combinatorial considerations.

Artin

1. The Galois group G(E/F) is the symmetric group $\mathbf{S}_5$ on five letters.

2. The five inertia groups $\mathfrak{I}_\mu$ of the five solutions are the only subgroups of $\mathbf{S}_5$ of index 5.

3. By the **Main Theorem of Galois Theory** it follows at once that the 5 fields $F(x_\mu)$ are the only extension fields of F of degree 5.

4. It is (just about) immediate from the definitions that any element v in E with five distinct conjugates generates an extension field $F(v)$ of F of degree 5.

5. Thus, $F(v) = F(x_\mu)$ for some x_μ. Hence, any v with five distinct conjugates can be expressed as a polynomial in x_μ with coefficients in F, as required.

If we simply took as our **A** and **B** the conjunctions of the sentences in the two proofs, the only model of each one would be the splitting field extension of E/F of $\mathbf{p}_5(x)$.

The intuition here is that Abel's proof does not manage to bring out the 'pattern' directly relevant to deriving the desired expression whereas Artin's does: the pattern articulated by the statement that $F(x_\mu) = F(v)$ for any of the roots x_μ of $\mathbf{p}_5(x)$. In contrast, it is intuitively clear that no one of the results reached in the five individual cases Abel considers in his proof amounts to an articulation of this 'pattern'. Finally, at least in this case, it seems clear that the conjunction of those five statements does not amount to such an articulation, either. Yet, the conjunction of the five statements in Abel's proof has the same set of models as Artin's statement that $F(x_j) = F(v)$, namely just the splitting field extension E/F. Finally, there does not appear to be any natural way to pick a subset of sentences from either proof for comparison.

This suggests that our initial intuitions about directness of relevance are not adequately captured by the foregoing model-theoretic notion of ‘relative generality’ after all. For what has emerged is that directness of relevance seems to pertain to the nature of *conceptual articulation* of facts: the field-theoretic concepts allow Artin to articulate the fact that $F(x_\mu) = F(v)$; Abel does not have these concepts in play and, hence, is not able to articulate this fact. So it seems likely that it is not possible to capture our intuitions about directness of relevance just by appealing to formal notions such as the notion of semantic consequence.

In our case study, the facts more directly relevant to the central results in the two proofs are virtually always facts about the ‘large-scale’ *organization of algebraic structures*. As such, articulating such facts tends to require various concepts that are not required in the articulation of the facts less directly relevant, such as combinatorial relations of permutations or roots. We see this in the two the proofs of the unsolvability as a whole: Artin determines that a polynomial equation $\mathbf{p}(x) = 0$ is solvable by radicals if and only if the Galois group G(E/F) of the splitting field extension E/F of $\mathbf{p}(x)$ is solvable; Artin does not have the concepts for articulating this property of groups nor, indeed, the concepts for discussing groups as such.

Thus, let us consider the following idea: a set of sentences **B** is directly relevant to **C** to *the extent to which* **B** *involves the same level of conceptual articulation as* **C**. For example, the sentence *G contains a normal series with abelian quotients* is more directly relevant to $\mathbf{p}(x)$ *is solvable by radicals* than a conjunction of sentences articulating individual facts about relations of elements in G. The former is articulated at the same ‘level’ as $\mathbf{p}(x)$ *is solvable by radicals* whereas the latter is articulated at a ‘lower’ level.

The first thing to sort out here is what sense we might be able to make of the idea of *levels of conceptual articulation*. We have seen in our examples that the sentences that should count as being at a 'lower' level are ones articulated in terms of concepts pertaining to relations of individual elements in various algebraic systems, while the sentences at a 'higher' level are ones the articulation of which requires concepts that are *defined in terms of* the 'lower' level concepts. For example, the conditions of application of the concept *group* are articulated in terms concepts that pertaining to relations of individual elements in some system of objects.

I propose to capture this idea as follows. Recall my suggestion in Section 3.4 that a mathematical concept is a certain kind of constellation of norms that governs the propriety of producing symbolic artifacts. Thus, if α is a concept, let $\Gamma(\alpha)$ be the set of norms that constitutes this concept. I will say that a concept β is *at a higher level relative to* α just in case the set of norms that constitutes α is a proper subset of the norms that constitutes β, $\Gamma(\alpha) \subset \Gamma(\beta)$. Two concepts are *comparable* only if either $\Gamma(\alpha) \subseteq \Gamma(\beta)$ or $\Gamma(\beta) \subseteq \Gamma(\alpha)$.

For example, the concept *group* is at a higher level relative to the concepts *set*, *element*, *composition of elements*, *equality*, and so on. This definition has the obvious consequence that if we have an explicit definition of a concept α, then α is at a higher level relative to all the concept employed in its definition. As I emphasized in Section 3.4, however, we can rarely give a complete, fully explicit definition of a concept: the sets of norms that constitute even the simplest mathematical concepts are incredibly complex, and the explicit definitions should be seen as summaries of the concepts themselves.

There are two obvious ways to extend this notion to sentences. Let **S** be a sentence, and let C(**S**) be the set of concepts required to articulate **S**. We can define Γ(**S**) to be the union of the sets $\Gamma(\sigma)$, where σ ranges over all of C(**S**). Thus, the simple way of extending the notion of levels would be to say that a sentence **B** is at a higher level than **A** just in case Γ(**A**) $\subset$ Γ(**B**). The more exacting way would be to say that **B** is at a higher level than **A** just in case (*a*) for any concept β required to articulate **B**, either there is some concept α required to articulate **A** such that $\Gamma(\alpha) \subseteq \Gamma(\beta)$ or else β is not comparable with any α; and

(*b*) for some β and α, $\Gamma(\alpha) \subset \Gamma(\beta)$.

I think that the latter is more faithful to the intuitions engendered by our case study, and so it is the one I shall adopt for now; I will write $\mathbf{A} < \mathbf{B}$ to denote that **B** is at a higher level than **A**.

Finally, there is an obvious way to extend this notion to sets of sentences. We will say that {**A**} *is at a higher level relative to* {**B**} just in case

(*a*) for every **B** in {**B**}, either there is some **A** in {**A**} such that $\mathbf{A} \leq \mathbf{B}$ or else **B** is not comparable with any **A**; and

(*b*) for some **A** and **B**, $\mathbf{A} < \mathbf{B}$.

This proposal is, no doubt, very rough. I would like to think, however, that it is rough in the right sort of way: there is a number of immediately visible avenues for refining it, perhaps into a number of different proposals, ones that might be able to capture different aspects of our intuitions about directness of relevance. For example, one refinement of my rudimentary notion might involve requiring that β is at a higher level relative to α just in case the norms in β that specify the circumstances of application of β contain the ones in α that specify the circumstances of application of α. But this is not the place to explore these epistemic options.

We can now apply this notion in an obvious fashion to analyze the notion of directness of relevance. Let $\Gamma(\mathbf{A})$ denote the set of concepts required to articulate a set of sentences **A**, and let $M(\mathbf{A})$ denote the class of models of **A**.

Let {**A**}, {**B**} *and* {**C**} *be sets of sentences*. *Then* {**B**} *is more directly relevant than* {**A**} *to* {**C**} *just in case*

(*a*) $\mathrm{M}(\mathbf{A}) \subseteq \mathrm{M}(\mathbf{B})$ (*model-theoretic generality*);

(*b*) $\Gamma(\mathbf{A}) < \Gamma(\mathbf{B})$ (*conceptual generality*); and,

(*c*) $\mathrm{M}(\mathbf{B}) \subseteq \mathrm{M}(\mathbf{C})$ (*inferential relevance*).

The motivation for condition (*b*) is as follows. We might expect that the condition should be

$$\Gamma(\mathbf{A}) < \Gamma(\mathbf{B}) \ \leq \Gamma(\mathbf{C}).$$

This condition has an obvious intuitive appeal. However, there are situations in our case study in which the intuitively more directly relevant set of sentences {**B**} *overshoots* the set {**C**} in its level of conceptual articulation. We saw this in considering **Theorem 6** above: the statement of the theorem is articulated at a lower level than the crucial sentences in Artin's proof of that theorem. It seems to me that the intuitions here are stable and strong enough to warrant allowing overshooting of this type. Indeed, parts (*a*) and (*b*) can be seen as capturing two distinct senses in which a set of sentences {**B**} is directly relevant to {**C**}, both constrained by part (*c*): on the one hand, (*a*) {**B**} is as *model-theoretically general* as possible while (*c*) still allowing us to infer {**C**}; on the other hand, (*b*) {**B**} is as *conceptually general* as possible while (*c*) still allowing us to infer {**C**}. Thus, (*a*) and (*b*) can be seen as complementary ways of capturing the idea with which we began this section: a fact is directly relevant to the extent it isolates what really *matters* for the conclusion and, in so doing, *abstracts away* from the irrelevant details.

It is clear that we can now discriminate the two proofs of **Theorem 6**. For it is easy to see that the concepts Artin uses to articulate sentences such as the crucial $\mathrm{F}(x_\mu) = \mathrm{F}(v)$ are at a higher level than the sentences Abel uses to articulate the various combinatorial facts, and it seems clear that each sentence in Artin's proof is either at a higher level than some (usually many) sentences in Abel's proof or else, is not comparable.

Comments

(1) Strictly speaking, I only endorse a *relative* notion of directness of relevance. Yet, sometimes it is intuitively suggestive to say that {**B**} *is directly relevant to* {**C**} provided that $\mathrm{M}(\mathbf{B}) = \mathrm{M}(\mathbf{C})$ and $\Gamma(\mathbf{B}) = \Gamma(\mathbf{C})$. For when this happens, no set can be more directly relevant to {**C**} than {**B**}.

(2) We have spoken of relative level of conceptual articulation of *sentences*. But recall now that I am taking it that the articulation of facts can be as fine-grained as our concepts allow. Thus, it is clear that the foregoing definitions can be translated into definitions for facts.

(3) My notion of directness of relevance is decidedly *non-formal*. For as I emphasized in Section 3.5, it is not a formal issue as to which norms should be considered to belong to a given concept. Thus, while my notion of directness has a vaguely formalistic casting, the *actual assessments* of relative directness of relevance will depend on potentially complicated non-formal considerations. For example, such assessments will typically be sensitive to the overall intellectual context in which the sentences at issue are employed. It is clear that there is much work to be done here.

(*d*) *Extracting Facts*

Artin shows that a polynomial equation $\mathbf{p}(x) = 0$ is solvable by radicals if and only if the splitting field extension E/F of $\mathbf{p}(x)$ is contained in a radical extension. And not only does he prove this fact; given his conceptual resources, he can articulate it in the fully 'direct' and 'explicit' way we have done here. Given that Abel does not have the requisite field-theoretic concepts, he cannot articulate this fact in this kind of way. Yet, there is a very real sense in which he is *responsive* to it in his reasoning. For example, **Theorem 2** can be understood as 'implicitly' saying that if a polynomial equation is solvable by radicals, then (given the assumptions noted above) not only is the splitting field extension contained in a radical extension, but it is itself a radical extension. Indeed, all the results at **Stage 2** in Abel's approach are 'indirectly' or 'implicitly' facts about the organization of the system of intermediate fields of the splitting field extension E/F.

I propose that we consider the following notion.

To have extracted a fact α *is to know that* α *obtains and to have articulated* α *in such a way that one is able to directly respond to* α *in one*'*s reasoning aimed at answering the question* **Q** *driving one*'*s epistemic process*.

Much as with locating, my definition of extracting has a trivial component and a tricky component. On the one hand, to extract a fact α is to acquire the piece of knowledge that α is the case; in mathematics, this amounts to proving α. On the other hand, to extract α is to articulate α in a particular kind of way—in a way that allows one to directly respond to α in the mathematical context at hand.

Responding Directly and Responding Indirectly

While Abel is in a sense responding to high-level features of the splitting field extension, such as the fact that it is generated by the roots of the polynomial, he is not responding to those features *directly*. He is responding to them *through* features of individual elements in that extension, namely the rational functions of the roots, and of course, the number of distinct values such functions take under the permutations of the roots.

Thus, we want a definition of what it is to "respond" to a mathematical fact and a stable distinction between responding "directly" and "indirectly." Again, we must keep firmly in mind that we are trying to capture epistemically significant differences between what Abel and Artin accomplish in their respective proofs: we want to be able to say that Artin does, while Abel does not, manage to extract the features of the set of permutations of the roots that are directly relevant to the solvability by radicals of $\mathbf{p}_5(x)$.

First, minimally, responsiveness has to involve *responding differentially*: we will *react* differently to the presence or absence of that feature, once recognized.

Second, I will take it that the responses at issue are *correct* or *incorrect* in view of the constitutive norms of the conceptual setting in which one is operating; so I am only considering responses governed by determinate norms.

Third, there is no loss of generality in focusing on responsiveness to *facts*; for it is clear that responsiveness to objects or properties in any case means responsiveness to the way in which objects instantiate properties—that is, facts.

Fourth, however, it seems clear that in the practice of pure mathematics, the items creatures like us can 'directly' respond to are constellations of *symbolic artifacts*. Thus, it seems natural and innocuous to say that to be responsive to a mathematical fact is to be responsive to some constellation of symbolic artifacts that represents that fact. So I will take it that in order to be able to be respond to a mathematical fact, one must have the conceptual resources to represent that fact—and I mean *that* fact and not some fact merely logically equivalent with it; again, I am insisting on the fine-grained individuation of contents and facts (see Section 3.4).

In view of these considerations, it seems to me that a natural way to characterize responses to mathematical facts within the overall structure of my story is through the notion of *manipulating* conceptually constituted representations in the following sense:

To ***manipulate*** *a set* **S** *of conceptually constituted representations is to apply some concept, method or rule to the representations in* **S** *so as to justify producing a representation* **r** *not contained in* **S**.

For example, to apply a valid rule of inference to a set of sentences so as to derive a new sentence is a paradigmatic case of manipulating representations. In the next section we will turn to considering the various modes of manipulating representations that make it possible to reach the various internal aims of mathematical epistemic processes. There I will defend the foregoing definition of manipulating. But for now taking this definition as established and justified, let us consider the following two applications:

To ***directly respond*** *to a fact* α *is to manipulate a set* **S** *of conceptually constituted representations containing a sentence* **p** *representing* α *so as to* (1) *produce a representation* **r** *not contained in* **S** *such that* (2) *without* **p**, *the representation* **r** *could not be correctly produced from the set* **S**.

To ***indirectly respond*** *to a fact* α *is to manipulate a set* **S** *of conceptually constituted representations such that* (1) **S** *does not contain a representation of* α *and* (2) **S** *has a sentence* **p** *representing* α *as a logical consequence.*

Given these definitions, to have extracted a fact α is to know that α obtains and to have a representation of α one can manipulate in pursuing the answer to one's question. This should seem like a welcome convergence: extracting is an aim of manipulating representations which, once achieved, facilitates *further* representational manipulation. And indeed: part of what it is to have cognitive control over an epistemic process is to be able to *put oneself in a position* to push that process further towards completion.

Let us first consider two simple illustrations.

(*a*) Let the set **S** be $\{p, p \rightarrow q\}$; given *modus ponens*, one can correctly infer q from **S**, but not from $\mathbf{S} \setminus \{p\} = \{p \rightarrow q\}$. Thus, making this inference is a case of manipulating representations and in particular, a case of directly responding to p.

(*b*) If N is a normal subgroup of a group G, I know that I can correctly form the quotient group G/N; if N is not normal, I know that this construction is not available. Thus, I am in my reasoning differentially responsive to the presence or absence of a certain property, in a way that respects certain norms in abstract group theory. In particular, when I form the quotient G/N, I am directly responding to the property that N is normal in G.

But suppose now that I consider a representation of some particular group and carry out symbolic computations that show that this group splits up into a number of sets disjoint from a certain subset N and from one another (while noting certain features of these sets we need not make explicit here). In so doing, I am *indirectly* responding to the fact that these sets are the *cosets of the subgroup* N. There are further computations I can carry out on the elements belonging to these sets (which we again need not make explicit here) that would amount to indirectly responding to the fact that N is normal in G. As it happens, this is exactly what Galois did in his early investigations on solvability.

These definitions allow us to articulate the difference we see between Abel and Artin. Abel examines many sets of facts that would have as a logical consequence some fact about the structure of the splitting field extension; again, **Theorem 2** may serve as an example. What he is directly responsive to therein, however, are various combinatorial facts about rational functions of the five roots of $\mathbf{p}_5(x)$.

Comments

(1) The definitions make it clear that an act of manipulating cannot count both as directly and as indirectly responding to α.

(2) We need to distinguish *articulating* a fact from directly responding to that fact. It seems obviously right that being able to articulate a fact is a necessary condition for being able to directly respond to that fact; clearly my definition has this consequence. However, it is not sufficient. For example, there is the following minimal sense in which someone might have the concepts *group* and *subgroup*: one knows the definitions but no facts, general or particular, about groups. In such an epistemic predicament, one cannot actually inferentially engage any general group theoretic statements except by explicitly appealing to the definitions. Thus, even though one is able to articulate, say, the fact that the order of a subgroup divides the order of the ambient group, one cannot respond to it directly—one can only engage it through the definitions.

This means, in particular, that even if one is able to articulate some fact directly relevant to answering the question driving one's epistemic process, one need not thereby be able to directly respond to that fact in a way that would allow one to pursue the aim. This occasions a note of caution about my definition of extracting: even if one has extracted a fact, so that she can respond to it directly, it is typically a *further* challenge to find the particular ways of utilizing that fact in the pursuit of one's overall epistemic aim. This is, I think, as it should be: it does not seem in the least realistic to think that there is some sort of general analysis to be given about the innumerable ways in which we finally manage to reach the aims we want to reach in our mathematical reasoning. The notion of cognitive control is meant to identify broad patterns of epistemic mastery that *put us in a position* to reach such aims, not the particular ways in which we reach them.

(*e*) *Manipulating Representations*

Having representations of facts in or about the target range is, in and of itself, of no use in trying to answer the question driving the epistemic process: we need to be able to *do something with* those representations and typically doing something with them amounts to doing something *to them*. This, then, is what I am calling *manipulating*: all the various things one can do, correctly or incorrectly, to a conceptually constituted representation in the setting in which one is operating.

I will only consider acts of manipulating that are *correct* or *incorrect* according to the norms of the ambient conceptual setting. Thus, again,

To ***manipulate*** *a set* **S** *of conceptually constituted representations is to apply some concept, method or rule to the representations in* **S** *so as to justify producing a representation* **r** *not contained in* **S**.

For example, to *apply a valid rule of inference* to a set of sentences so as to justify writing down a further sentence is to manipulate those sentences; to carry out a *numerical computation* in accordance with the rules governing base 10 notation is to manipulate the given numerals; to add a line segment to a geometric diagram in accordance with the norms constitutive of the Euclidean geometric practice is to manipulate that diagram. In contrast, to use a yellow crayon to fill in a circle in a diagram so as to produce a drawing of the sun is not an act of manipulating in the Euclidean practice because to do so is neither correct nor incorrect according to the norms of that practice.

Devices for and Modes of Manipulating

An ordinary mathematical proof, such as the proofs of Abel and Artin we have presented, can be thought of as a *sequence of instructions*: if you make these inferential moves, filling in some gaps here and there, you will have justified asserting the theorem. Thus, the epistemic process of reading a proof consists of taking in such a sequence of instructions and making the inferential moves indicated; the cognitive agent reading the proof may or may not actually make all the moves she is instructed to make, depending on how attentive and conscientious she is.

But this point of view is not compulsory. We could with equal justification view a proof as a sequence of instructions for *manipulating conceptually constituted representations*. If a proof is viewed merely as a sequence of instructions as to which valid inferences one should make at a given juncture, we are not going to see much by way of epistemically interesting *patterns* in that proof. If, on the other hand, we allow the initially more generic point of view where the steps in a proof are viewed as instructions for manipulating representations, we can begin to see patterns other than ones of valid inference.

For example, Artin repeatedly considers the *fixed field* of some given group; he considers the *minimal polynomial* of an element in an extension; he considers the *effect* of the Galois group on an element in an extension. Abel reduces his considerations of the radicals to the *prime-order* case; in his computations, he groups terms of the same *degree* together; he considers the number of *distinct values* an expression can take under the permutations of the variables. These are all stable and recurring modes of manipulating conceptually constituted representations some of which are sentential while others, such as the expressions for the radicals, are non-sentential.

This point of view is liberating: it provides us a new avenue for theorizing about the relative epistemic power of different approaches. For it is *prima facie* plausible that the range of ways of manipulating representations available in an approach is going to have a direct bearing on the character of cognitive control available in that approach.

I will identify a number of recurring *modes* of manipulating representations and a number of *devices* for manipulating that make those modes available. From the point of view of my analysis of cognitive control, the crucial point here is that different devices and modes tend to have different *epistemic roles* in the mathematical practice overall. In particular, some modes of manipulating may be particularly well or ill suited for effecting consolidating, others locating, yet others extracting. Hence, an obvious but analytically fruitful thought emerges: the character and extent of cognitive control in principle available in a conceptual setting depends, at least in part, on the availability of devices and modes that are well-suited for pursuing each one of these three internal aims. In Chapter 4, I will try to make it visible that in Artin's approach, we find ourselves equipped with robust ranges of devices and modes well-suited to pursuing each of the three internal aims, while in Abel's approach, we do not. It is already clear that the lack of devices for consolidating is particularly acute in Abel, and this has the consequence that it is difficult to manufacture effective devices for pursuing locating and extracting, either. A proper examination of these issues would require much more space than I am allowed here, however.[32]

[32] The idea that we find in our mathematical practice devices of and modes for manipulating representations resembles, at least superficially, the idea explored by Marquis in his "Abstract Mathematical Tools and Machines for Mathematics".

3.6.6 Epistemic Guidance

(*a*) *Characterization of Guidance*

Recall the third component of our characterization of cognitive control:

The agent's epistemic scaffolding, *along with her overall epistemic resources*, *provides her epistemic guidance for examining the target range*.

The basic challenge facing a cognitive agent at each stage in her epistemic process is *to make a rational decision as to what to do next*. Another way of putting this is that the agent is faced with the challenge of determining what she *should* do next—determining what reason requires. The notion of epistemic guidance is meant to capture the intuition that when one has 'control' over a process, one is at each stage able to make such a determination.

In order to articulate the notion of epistemic guidance, I shall need the notion of *space of epistemic options*. An *epistemic option* at a given stage in an epistemic process is a possible way of *correctly proceeding* at that stage; the epistemic process itself consists of all the epistemic options the agent actually takes. In a mathematical epistemic process, a typical epistemic option is a possible act of correctly manipulating a conceptually constituted representation in the sense discussed above—applying a concept, a method, or a rule. The space of epistemic options is, in the first instance, the totality of all of them.

The space of epistemic options at a given stage in an epistemic process arises from the interaction of the representations the agent has chosen to consider and the *norms* that govern the ways in which one could correctly manipulate those representations. This is a direct consequence of my conception of mathematical concepts as sets of norms, and the (just about tautologous) idea that mathematical methods and rules are norm-governed. Thus, once an agent working in a particular conceptual setting has adopted a determinate set of representations and a determinate epistemic goal, it is an *agent-independent fact* what her space of epistemic options is. For what her options are is ultimately determined by the norms constitutive of that setting.

For a simple but surprisingly representative example, let us consider a system of *natural deduction* of the kind one might learn in an introductory course on formal logic. The typical exercise involves writing down a derivation from a given set of premises to a given conclusion by using the rules of inference of that system. Writing down a derivation is obviously an example of a mathematical epistemic process in my sense. At each stage in this process, the student has available to her a determinate set of representations, namely the sentences so far derived, and a determinate set of rules she could correctly apply at that stage, namely the rules of inference that apply to those sentences. The space of epistemic options consists of all the various acts of writing down a new line in the derivation where that line is justified by using some rule of inference in the system. This space is infinite: for given any sentence p, *disjunction introduction* allows one to write down $p \vee q$ for any q, which already amounts to infinitely many potential candidates.

Now the point of the notion of space of epistemic options is that one's ability to make a rational decision as to how to proceed at a given juncture in the process is largely a function of the way in which one can *represent* the space of epistemic options and, more specifically, what one knows about that space. As is clear already from our simple example, an agent need not be able to represent her space options or, at any rate, she need not be able to represent all of it, in a way that allows her actually to pursue any of those options. So the student might know the rules (by rote, say) but not be able to apply them to the given sentences; there is a sense in which she knows what the options are, but she is not able to represent them in a way that allows her to pursue them.

More systematically, we may consider the following aspects of the ‘character’ of one’s representation of the space of epistemic options:

(1) Given one’s overall epistemic resources, and given one’s representation of the space of epistemic options, one may be more or less able to ***pursue*** individual epistemic options. We already saw this in the foregoing example. More generally, it is common in mathematics that one in some sense knows what the options are, but does not have the manipulational ability to pursue any one of them as represented. I take it to be clear that in order to capture the intuition that one is in ‘control’ of the epistemic process at a given stage, we must require that one is in fact able to proceed somehow or other and, hence, can represent at least some of the possible ways of proceeding in a way that allows one actually to pursue them.

(2) One’s representation of the space of epistemic options may be more or less ***complete*** in the sense that it fails to include some of the options in fact available. Having a representation of the various correct ways of proceeding that is as complete as possible is clearly essential to being able to identify the most favorable one. Thus, reason requires that one try to acquire a representation that is as complete as possible.

(3) One’s representation of the space of epistemic options may include items that are ***not in fact*** correct ways of proceeding. This is just a particular kind of way in which one can make a mistake in the course of pursuing one’s epistemic aim. Since this kind of mistake is of little analytical interest, I will ignore it in what follows.

(4) One’s representation of the space of epistemic options may or may not allow one to rationally assess the ***probabilities*** of the various options’ leading to an answer to the question driving that stage in the epistemic process. The ability to assign (subjective) probabilities in a rational fashion to the options is clearly a fundamental aspect of being able to make a rational decision as to how to proceed. A minimal requirement would be that one is able to assign probabilities in a way that respects the probability calculus.

(5) One’s representation of the space of epistemic options may be more or less ***surveyable*** in the sense that it may or may not provide a structured *overview* of the range of options and their relationships. I will consider examples presently.

I will say that one has ***epistemic guidance*** at a given stage in an epistemic process to the extent one has a representation of the space of epistemic options at that stage which, along with one’s overall epistemic resources, gets a high score on each of the five aspects itemized above. Thus, one would have perfect guidance if one’s representation of the space of options is complete, contains no false options and is highly surveyable; and, given one’s resources, one can pursue any one of the options and can assign any one of them a probability of leading to success at that stage in the process.

Comments

(1) Having epistemic guidance is very much a *matter of degree*. It seems to me that this is exactly what we want: on the one hand, it fits what we will see in our case study; on the other hand, one’s ability to make a rational decision as to how to proceed is surely a matter of degree.

(2) Having guidance is a *multi-dimensional* affair. Again, this seems to me to be what we want both in view of our case study as well as speaking abstractly about one’s ability to make rational decisions. I have not attempted, and think it would be futile to attempt, some sort of

system of weighting the different aspects of guidance against one another. For which aspect is the more important one will always depend on the particular epistemic challenges one is facing at a given stage in the process. I have arranged the five aspects in an order of something like dominance: one wants a representation that is highly surveyable, but *not at the cost* of having one that allows one to assess the relative merits of the options; but not at the cost of having one that is free of mistakes; but not at the cost of having one that is complete; but not at the cost of having that allows one actually to pursue the options. Ultimately, however, it is my inclination to think that there isn't much to be said about the order of these aspects in the abstract.

(3) I want to emphasize that the foregoing list of five aspects of guidance is meant to be *open-ended*. I make no claim to having exhaustively enumerated what might be included under the notion of guidance—that is, what might go into the ability to make a rational decision as to how to proceed at a given stage in one's epistemic process. It does seem to me, however, that the five items I have selected to include are among the more important ones.

(4) To have guidance is to be able to determine what one *should* rationally do at a given stage in one's epistemic process. This idea might seem to be subject to the following trivialization: what one should do is relative to what one knows. For example, if one is aware of only one epistemic option, then it is rational to pursue that option. Hence, it might seem that the character of one's representation of the space of epistemic options is simply irrelevant to the question of the rationality of one's decision. But this attempted trivialization turns on an overtly narrow conception rationality. It is part of the very idea of making a rational decision that one has done one's best to determine what the range of available courses of action is and one's best to assess the relative merits of those courses of action. One is simply not in a position to make a fully rational decision regarding how to proceed until one has done one's best to acquire a

representation of the space of epistemic options that scores as high as possible on the five dimensions of guidance.

(5) There are two issues pertaining to one's ability to proceed at a given stage in an epistemic process. On the one hand, there is the character of one's representation of the space of epistemic options, what I have called guidance. On the other hand, there is the space of epistemic options *itself*. Depending on the epistemic resources available at a given stage in the process, there may be dramatic differences in the number of epistemic options in principle available to be pursued, and the character of what would be involved in pursuing those options. We see this very concretely in the contrast between Abel and Artin. While Abel's space of options typically consist of pursuing some sequence of symbolic computations, Artin's space of options involves in addition various modes of reasoning about the content of concepts such as *subgroup* and *field extension*.

Obviously the space of available ways of proceeding is of great interest from the point of view of analyzing the epistemic accomplishments of modern mathematics. The question would be, what are the relevant epistemic notions for characterizing differences between epistemic options themselves. First of all, I take it to be clear that when we want to make comparative evaluations of epistemic options, what we are really interested in comparing are the *epistemic processes that ensue* from taking those options. Accordingly, my suggestion is that there is no further heavy lifting to be done here: we are already in the business of analyzing differences between epistemic processes. Thus, as from the outset, there are two principal dimensions of comparison: an epistemic option may lead to an epistemic process that is more or less efficient in answering the question at which it is aimed, and an epistemic option may lead to a process over which one enjoys more or less cognitive control. Thus, again setting the issue of efficiency aside, my suggestion is that no further notions need be introduced to analyze the differences between the spaces of epistemic options themselves.

(6) I want to ensure that we have the nature of our enterprise firmly in focus. The notion of cognitive control and the notion of guidance in particular are meant to identify a *recurring pattern* in our epistemic activity. As such, the articulation of these notions must come to a stop at some appropriate level of generality before we start hitting the various particular things mathematicians actually do in their epistemic activity. Now it seems to me that the five aspects of epistemic guidance identified above belong to that level. For there is no end to the potential diversity of what might be involved in making a rational decision as to which epistemic option to pursue, especially if we mean to include in the purview of cognitive control not only the pursuit of mathematics but also the pursuit of empirical science. Thus, the five aspects of guidance must necessarily be rather general in order to stand a chance of capturing patterns in that diversity.

So two remarks. First, as I will presently argue in the context of our case study, there is much that can be done by way of identifying and categorizing the types of devices and strategies used to acquire the various aspects of guidance in mathematics. Indeed, I see effecting such identification and characterization as the principal analytical challenges in the way to coming to a nuanced philosophical appreciation of the epistemic character of theoretical progress in mathematics.

Second, my analysis of guidance is not structurally different from the analyses of knowledge as *justified true belief* or explanation as a *description of a causal mechanism*. For there is no end to the potential diversity of what is involved in acquiring justification for one’s beliefs or what is involved in furnishing descriptions of causal mechanisms in the structure of the physical universe.

In sum, the real concern is whether the analysis of the range of accomplishments I am looking to demarcate with the notions of cognitive control and guidance has stabilized at the right level of generality: at a level where the recurring pattern is clearly in view, and in a way that allows us to home in on the particular ways in which that pattern is instantiated in particular epistemic processes. Much of the point of the analysis of our case study is to argue that this is indeed so.

(7) I conclude our general discussion of guidance with a brief remark about what I consider to be the most analytically fruitful of the five aspects of guidance, the extent to which one's representation renders the space of options surveyable.

The idea is that a representation is surveyable to the extent it allows us to discern the epistemically relevant *relations* of the epistemic options. It should be clear that epistemic options in mathematics can be related in a great number of different ways. Perhaps the most fundamental type here are the various relations of *dependence* and *independence* of epistemic options. For example, it is common that one possible way of proceeding is a *special case* of some more general or more comprehensive approach. Thus, to pursue an option can be, as such, to pursue a number of options. It is not possible to give a systematic discussion of these issues here, but we will see a number of examples in our case study. We will see, for example, that *parametrizations*, numerical or otherwise, are key devices in making available more surveyable representations of ranges of options.

(*b*) *Aim, Location and Manipulation Guidance*

We may distinguish three basic types of decisions one has to make regarding how one should proceed at a given stage in an epistemic process: which piece of knowledge one should pursue at that stage, which particular range of facts one should examine in order to pursue that piece of knowledge, and which devices and modes of manipulating one should deploy in examining it. Corresponding to these three basic types of decisions to be made, I recommend that we distinguish three types of epistemic guidance: *aim*, *location* and *manipulation guidance*. I will need to show, of course, that the foregoing five aspects of guidance are intelligible with respect to these particular types of decisions.

The principal motivation for introducing these three varieties of guidance is that they allow us to get a tighter grip on the details of our case study than the general notion alone and, thereby, they allow us to give a more structured analysis of the differences between the two approaches to solvability. Further, distinguishing the three varieties affords us yet another way of implementing the intuition that when one has 'control' over the process, one can start with a panoptic overview and home in: when one enjoys guidance of all three kinds at a given context, one can start with a large-scale representation of the space of epistemic options for proceeding and home in towards the particular options.

(*a*) *Aim guidance*. At a given stage in the process, there is usually a more or less well-defined range of *immediate epistemic aims* one might adopt: aims which, if reached, would ultimately allow one to reach the aim driving the process overall. The notion of correctness of a subsidiary aim is just this: the result one would establish in reaching that aim could in fact be employed to pursue the aim driving the process. Thus, the space of correct subsidiary aims is dictated by the overall aim of the epistemic process on the one hand, and the epistemic resources available at that stage, centrally including the results so far established.

One has ***aim guidance*** *at a given stage in an epistemic process provided that one has a representation of the range of correct aims one might adopt at that stage, a representation that has the five characteristics above.*

There is no difficulty in applying the five aspects of guidance to one's grip on the range of potential aims one might adopt. First, clearly we can make sense of the idea that one may or may not be able to pursue an aim as represented; second, we can make sense of the idea that one's representation of the range of aims may be more or less complete and may contain aims that would not in fact allow one to reach the final aim of the process; certainly it seems possible and right to say that when one is in control of a process, one can rationally assess the relative likelihood of a subsidiary aim's leading to an answer to the question driving the process as a whole; indeed, this is just the sort of assessment mathematicians routinely make; finally, the range of aims may be represented in a way that is more or less surveyable. Of particular importance here would be having a clear view of the dependence or independence of the various aims one might adopt.

We will see that an appropriately trained mathematician enjoys reasonably good aim guidance throughout the sequence of main stages in the proofs of Abel and Artin. Differences will begin to emerge as we consider the character of aim guidance enjoyed in the course of proving some of the particular results in their approaches. I will argue that Artin's approach tends to afford better aim guidance when the epistemic processes are analyzed 'locally' in the sense introduced in Section 3.5.

What I am calling aim guidance is one of the principal items philosophically minded mathematicians like to draw attention to when they are out to identify epistemically crucial features of their trade. In the course of searching for a proof of a putative theorem we typically seek to identify a small number of subsidiary propositions and lemmas, which, if established, would (probably) allow us to establish the theorem.

This intellectual strategy can be illustrated by using our example of searching for a derivation within the confines of a system of natural deduction. One effective way of acquiring aim guidance is to *backtrack*: one starts with the desired conclusion and looks for a sentence and a rule of inference that would allow one to derive the conclusion from that sentence and the premises one has. Having found such a sentence, one can repeat the procedure; in this way, one generates a sequence of sentences any one of which could be taken as a subsidiary aim in the epistemic process overall. This strategy tends to be quite effective especially when even the shortest possible derivation is lengthy.

Something similar happens in Euclidean geometry when one *analyzes* a geometric construction problem. In such an analysis, the problem is diagrammatically represented as solved; again backtracking from the solution, one proceeds to identify a sequence of subsidiary construction stages, thereby establishing a sequence of subsidiary aims. While this process does not always provide good aim guidance, it can be very useful.[33]

(*b*) *Location guidance*. At any given stage in an epistemic process, there is usually a well-defined range of locations one might choose to examine in order to pursue the aim one has chosen for that stage. A location is a *correct location* to examine just in case, given one's overall

[33] See Manders, "The Euclidean Diagram" (unpublished).

epistemic resources, knowing the actual facts in that location makes it possible to infer a direct answer to one's question.

Thus, we have the obvious definition:

One has ***location guidance*** *at a given stage in an epistemic process provided that one has a representation of the range of correct locations one might examine at that stage, a representation that has the five characteristics discussed above.*

We will see that an appropriately trained mathematician will enjoy quite excellent location guidance throughout the process of reading Artin's proof. This is because, as we have seen, Artin's set of epistemic resources contains all the group and field theoretic concepts required to create a scaffolding with a robust range of locations pertinent to the solvability of polynomials by radicals. The verdict is much more ambivalent in Abel's case, but we will see that he does actually enjoy pretty good location guidance towards the end of his proof; for as we will see, his scaffolding is not half bad, even if it takes him most of the proof to build it. Even if Abel arguably never manages to locate and extract any features very directly relevant to solvability by radicals, there is a sense in which his location guidance at the local level in the proof, relative to the local aims of the various subprocesses, is not bad at all.

Comments

(1) It is clear that the issue of location guidance cannot arise until one has chosen some particular aim for the stage; likewise, as will become evident presently, the issue of manipulation guidance cannot arise until one has chosen some particular location to examine. Thus, there is a sense in which the three varieties of guidance constitute an embedded sequence of epistemic mastery: they gradually take us closer to being able to make a rational choice for a specific device and mode for proceeding.

(2) Location guidance is in some sense the prototype for the general notion of guidance. It is the type of guidance most directly derived from the epistemic scaffolding: after all, the epistemic options in location guidance correspond to some subset of all the locations one has managed to demarcate in one's scaffolding. As such, location guidance occupies a central role in the overall scheme of cognitive control. It is also the type of guidance that perhaps most directly captures the intuition that in order to have 'control' over an epistemic process, one must have a structured and surveyable overview of the terrain of facts one is investigating.

(*c*) *Manipulation Guidance*. We identified three internal aims in mathematical epistemic processes: consolidating ranges of facts, locating facts that are directly relevant to answering the question, and extracting such facts. When one has cognitive control over the epistemic process, one is able to reach these aims; accordingly, it would be natural to think that when one has cognitive control, one enjoys *epistemic guidance as to how to pursue* these three aims. These aims are pursued by employing the various devices and modes of manipulating representations. This suggests that in addition to aim and location guidance, we might consider *manipulation guidance*.

At any given stage in an epistemic process, there is usually a well-defined range of modes of manipulating one might choose to apply to the representations available at that stage. A mode of manipulating is correct if it is in fact applicable at that stage and if it is in fact possible to reach one's manipulational aim in part by employing that mode.

One has ***manipulation guidance*** *at a given stage in an epistemic process provided that one has a representation of the range of correct modes of manipulating one might employ to pursue one's current manipulational aim, a representation that has the five characteristics discussed above.*

Typically manipulation guidance is enjoyed in virtue of having a comprehensive overview of the ‘standard’ devices and modes of manipulating available in the conceptual setting, and having some way to assess which of those devices and modes would likely be useful for the task at hand.

We will see examples of manipulation guidance in Section 4.3.

4.0 COGNITIVE CONTROL IN EPISTEMIC PROCESSES OF ABEL AND ARTIN

I will now further articulate and illustrate the notion of cognitive control by applying it to a number of subprocesses in the proofs of Abel and Artin. I will first show that both proofs can be naturally thought of as consisting of three stages, and provide a *global* analysis of all of them in the sense introduced in Section 3.5. I will then provide a *semi-local* analysis of two subprocesses falling under the second of the three stages in each proof. Finally, I will provide a *local* analysis of one characteristic sub-subprocess in each of the latter two subprocesses.

My claim will be that the concepts, methods, and bits of knowledge that constitute the set of epistemic resources of Artin's approach to solvability allow someone who has mastered those resources to maintain excellent cognitive control in the course of reading his proof. In contrast, the resources of Abel's approach do not allow us to maintain as good a control over his proof. In particular, the differences in the character of control in the two proofs become more pronounced as we move down towards the subprocesses.

4.1 EPISTEMIC PROCESSES OF ABEL AND ARTIN

Our first task is to describe the way in which the epistemic processes of Artin and Abel break down into stages. In so doing, we need to identify the aim and the principal result reached at each stage, as well as clearly display the nesting of the stages. Once the stages have been identified, we shall examine to what extent the individual components of cognitive control are or are not present at each stage.

Each stage is individuated by the aim stated at the beginning. If a stage does not have subsidiary stages, it will contain one major result that amounts to reaching that aim. If a stage has subsidiary stages, the result that amounts to reaching the aim only comes at the end of the last one. Thus, the upper level need not contain anything more than the statement of the aim; the actual 'details of the derivation' will then take place at the stages subsumed under it.

4.1.1 Artin's Epistemic Process

Aim. ***Prove*** *that the general polynomial equation* $\mathbf{p}_5(x) = 0$ *of degree* 5 *is not solvable by radicals*.

(1) ***Find*** *a criterion for solvability by radicals.*

Result. *A polynomial equation* $\mathbf{p}(x) = 0$ *is solvable by radicals if and only if the splitting field* E *is contained in a radical extension* L *of the ground field* F.

(2) ***Find*** *a way of showing that this criterion is not satisfied for* $\mathbf{p}_5(x)$.

(2.1) ***Associate*** *some organizationally simpler structure with the splitting field extension of an arbitrary polynomial* $\mathbf{p}(x)$; *we associate with* E/F *its Galois group* G(E/F).

(2.2) ***Establish*** *a bijective correspondence between intermediate fields and subgroups in such a way that the property of being contained in a radical extension is reflected in the organization of the latter*; *this will be the* **Main Theorem of Galois Theory**: *there is a bijective*, *order-reversing correspondence between the intermediate fields of* E/F *and the subgroups of* G(E/F) *for any extension* E/F *that has a certain critical property*.

(2.2.1) ***Identify*** *the property required by such a correspondence*; *this is being* ***normal***.

(2.2.2) ***Prove*** *that the association* $H \to E^H$ *of a subgroup* H *of* G(E/F) *with its fixed field is one-to-one*; *this is* **Lemma 1** which shows that $K \to G(E/K)$ is the inverse of $H \to E^H$.

(2.2.3) ***Prove*** *that the association* $K \to G(E/K)$ *of an intermediate field* K *of* E/F *with its Galois group is one-to-one*; *this is* **Lemma 2**, *Artin's lemma*, which shows that $H \to E^H$ is the inverse of $K \to G(E/K)$.

(2.2.4) ***Prove*** *that being normal is inherited by intermediate fields*; *this is* **Lemma 3**.

(2.3) ***Identify*** *the feature of the organization of* $G(K_2/K_1)$ *that corresponds to* K_2/K_1 *being a radical extension*; *this is the property being a* ***solvable*** *group*; *that is*, $G(K_2/K_1)$ *contains a normal series with abelian quotients*.

(2.4) ***Prove*** *that since* G(L/F) *is solvable*, G(E/F) *is solvable also*; *it is*.

Result. *We will try to prove that the Galois group* G(E/F) *of* $\mathbf{p}_5(x)$ *is not a solvable group*.

(3) ***Prove*** *that the Galois group* G(E/F) *of* $\mathbf{p}_5(x)$ *is not a solvable group*.

(3.1) ***Identify*** *the Galois group* G(E/F) *of* $\mathbf{p}_5(x)$; *this group is the symmetric group* $\mathbf{S}_5$.

(3.2) ***Prove*** *that the symmetric group* $\mathbf{S}_5$ *does not contain a normal series with abelian quotients*; *it does not*.

Result. *The general polynomial equation* $\mathbf{p}_5(x) = 0$ *of degree* 5 *is not solvable by radicals*.

4.1.2 Abel’s Epistemic Process

Aim. ***Prove*** *that the general polynomial equation* $\mathbf{p}_5(x) = 0$ *of degree* 5 *is not solvable by radicals*.

(1) ***Find*** *a criterion for solvability by radicals*.

(1.1) ***Find*** *an inferentially engageable representation of the general form the solution formula would have to have*; *this is the expression in* **Theorem 1**.

(1.2) ***Find*** *an inferentially engageable representation of the structure the terms and*, *in particular*, *the radicals in the solution formula would have to have*; *this is the expression in* **Theorem 2** *for the terms and the radicals as rational functions of the roots*.

Result. *The terms and*, *in particular*, *the radicals in any solution formula for* $\mathbf{p}(x)$ *would be expressible as rational functions of its roots with certain explicitly specified structure*.

(2) ***Find*** *a way of showing that this criterion is not satisfied for* $\mathbf{p}_5(x)$.

(2.1) ***Find*** *a more inferentially engageable representation of the rational functions whose number of values would allow them to be expressions for radicals in a solution formula*.

(2.1.1) ***Restrict*** *the range of rational functions that could be expressions for radicals in a solution formula*; *it turns out that we have justification for restricting our attention to rational functions with* 2 *or* 5 *distinct values*.

(2.1.2) ***Find*** *an artifactually determinate expression for a rational function v of the roots of* $\mathbf{p}_5(x)$ *with* 2 *distinct values*; *this expression is* $\mathrm{p} + \rho\mathrm{q}$ *where* p *and* q *are symmetric and* ρ *is a certain alternating function, the square root of the discriminant of* $\mathbf{p}_5(x)$.

(2.1.3) ***Find*** *an artifactually determinate expression for a rational function v of the roots of* $\mathbf{p}_5(x)$ *with* 5 *distinct values*; *this expression is* $r_0 + r_1 x + r_2 x^2 + r_3 x^3 + r_4 x^4$, *where* $r_0, ..., r_4$ *are symmetric functions of the roots* $x_1, ..., x_5$ *and* x *is one of the* $x_1, ..., x_5$.

Result. *We will try to apply the* **Combinatorial Principle** *within the scaffolding provided by* (2.1) *to show that not enough radicals exist that have the same number of values as a radical as they have as a rational function of the roots*.

(3) ***Prove*** *that not enough radicals with the right number of values exist for there to be a solution formula by radicals for* $\mathbf{p}_5(x) = 0$.

(3.1) ***Determine*** *for which p there are radicals of order p over the field of coefficients* F; *only radicals of order* 2 *can exist over* F, *and the field generated by any such radical is isomorphic to* F(ρ).

(3.2) ***Determine*** *for which p radicals of order p exist over the field generated by* ρ; *there are none*.

(3.3) ***Prove*** *that this is not enough radicals*; *but this is just about trivial*.

Result. *The general polynomial equation* $\mathbf{p}_5(x) = 0$ *of degree* 5 *is not solvable by radicals*.

4.2 GLOBAL ANALYSIS

I will first undertake an analysis of the epistemic processes of each of the three main stages in the two proofs. Thus, when we assess the four components of cognitive control in what follows, we will be assessing them *internally* to the epistemic processes of **Stage 1**, **Stage 2**, and **Stage 3**. In each case, that process will be viewed globally in the sense of Section 3.5: we will treat the results obtained in modular subprocesses as given.

4.2.1 Stage 1: Orienting the Process

Aim. Find a criterion for the solvability by radicals of $\mathbf{p}(x) = 0$.

Artin's Result. The criterion is that a polynomial equation $\mathbf{p}(x) = 0$ *is solvable by radicals if and only if the splitting field* E *of* $\mathbf{p}(x)$ *is contained in a radical extension of the ground field* F.

Abel's Result. The criterion is that the terms and, in particular, the radicals in the solution formula would have to be expressible as rational functions of the roots with the structure specified in **Theorem 2**.

The principal epistemic significance of **Stage 1** in both proofs is that in it we identify the overall target range for the rest of the proof. Concretely, this is accomplished by identifying an initial criterion for solvability by radicals. It should be emphasized, however, that Artin and Abel both refine the orientation of their processes considerably at the early substages of **Stage 2** and, in particular, it would *not* be right to say that **Stage 1** sets up the principal scaffolding for the rest of the proof.

(1) ***The agent has identified a target range***

Since this is the first stage in the process overall, the target range would be suggested, more or less loosely, by whatever background resources Artin and Abel have available to them.

For Abel and Artin alike, I suppose that the epistemic resource most directly pertinent to finding a criterion for solvability and, thereby, to identifying a target range, is simply knowing the *definition* of what it is for a polynomial equation $\mathbf{p}(x) = 0$ to be solvable by radicals. For now we may treat $\mathbf{p}(x)$ as the arbitrary polynomial.

It is clear from the definition that the fact as to whether $\mathbf{p}(x) = 0$ is solvable by radicals is a consequence, somehow or other, of the *arithmetic relations of the roots with the coefficients*; after all, to say that $\mathbf{p}(x) = 0$ is solvable by radicals just means that it is possible to express each of the roots of $\mathbf{p}(x)$ in terms of its coefficients by using only the arithmetic operations and the operation of extracting roots.

But more is clear. For there is a sense in which the arithmetic relations of the roots with the coefficients *are always the same*: the coefficients are just the elementary symmetric functions of the roots. Thus, we can identify a more focused target range: the *arithmetic relations of the roots*. This can be seen as follows. Let $\mathbf{p}(x) = x^n + a_{n-1}x^{n-1} + ... + a_1$, and consider the set of all possible radical expressions $\mathrm{R}(a_1, ..., a_{n-1})$. If $\mathbf{p}(\mathrm{R}) = 0$ for some such expression, then $\mathbf{p}(x) = 0$ is solvable by radicals; otherwise it is not. But clearly whether or not $\mathbf{p}(\mathrm{R}) = 0$ for a given R just depends on what the coefficients are. More specifically, it depends on the arithmetic relations of the coefficients: for $\mathbf{p}(x) = \mathrm{R}^n + a_{n-1}\mathrm{R}^{n-1} + ... + a_1 = 0$ can be taken to articulate a particular non-trivial arithmetic relation of the $a_1, ..., a_n$. But these $a_1, ..., a_n$ are elementary symmetric functions f_k of the roots $b_1, ..., b_n$ of $\mathbf{p}(x)$, so that $a_k = f_k(b_1, ..., b_n)$ for $k = 1, ..., n - 1$. Thus, by substituting each f_k for a_k in $\mathbf{p}(x) = x^n + a_{n-1}x^{n-1} + ... + a_1$, we can repeat the foregoing line of thought and conclude that whether **p**(x) = 0 is solvable by radicals is a consequence of the way the *roots are related to one another*. This is not to say that it isn't a non-trivial task to determine just how the roots must be related in order for the polynomial to be solvable by radicals.

As it turns out, Artin can be seen as adopting the arithmetic relations of the roots with the coefficients as his target range: he goes on to identify a criterion of solvability in terms of a large-scale pattern in these relations that obtains if and only if the polynomial is solvable. Abel, in contrast, can be seen as adopting the arithmetic relations of the roots with the coefficients as his very first target range, but he goes on to identify a criterion of solvability in terms of the arithmetic relations of the roots themselves.

(2) ***The agent has an organizing representation that allows her to erect a scaffolding***

Artin's Organizing Representation and Scaffolding

Artin has the concepts *field* and *field extension*, and he knows the elementary general facts about field extensions. Given that his target range are the arithmetic relations of the roots of **p**(x), the obvious organizing representation for him to adopt is *the splitting field extension* E/F *of* **p**(x), where **p**(x) may again be thought of as the arbitrary polynomial. For the splitting field E of **p**(x) is the unique smallest extension of the ground field F that contains all the roots of **p**(x); thus, the extension E/F certainly consolidates all the facts about the arithmetic relations of the roots of **p**(x) with its coefficients.

Since the aim of **Stage 1** is to identify a criterion for solvability by radicals, one natural approach to erecting a scaffolding is to try to determine whether there is some field-theoretic feature of the splitting field extension E/F that is present if and only if **p**(x) = 0 is solvable by radicals. This is one way in which the field-theoretic concepts provide orientation for the process from the start.

Now clearly the splitting field extension E/F consolidates a vast array of arithmetic facts, not all of them relevant to the issue of solvability. As an algebraic structure, however, the two most salient features of this extension are, first, that it contains a *system of intermediate fields* and, second, that E is *generated* over F by the roots of **p**(x). Given the second feature, it is clear from the outset that the field-theoretic organization of the extension E/F is intimately connected with the relations of the roots among themselves as well as their relations with elements of the ground field F. But it is facts about just these relations that ultimately govern the solvability or not of the equation **p**(x) = 0. Thus, one is justified in thinking that the fact as to whether **p**(x) = 0 is solvable might be in some way reflected in the organization of the system of intermediate fields of E/F. As such, it is natural to think that we might be able to erect a scaffolding in which the locations are demarcated by the intermediate fields of E/F.

In order to erect our scaffolding for **Stage 1**, let us then suppose that **p**(x) = 0 is solvable by radicals, so that the roots of **p**(x) can be expressed in terms of some finite set of radicals, all of them contained in the algebraic closure of F. Thus, given any such set of radicals, it is immediate that the splitting field E is contained in a finite extension L of F generated by those radicals. Conversely, if E is contained in such an extension, it is easy to show that **p**(x) = 0 is solvable by radicals. Thus, we need to adjust our initial expectations somewhat: it is now more natural to focus on the extension L/F, rather than the extension E/F itself. Yet, in view of the foregoing considerations, it is still natural to consider the organization of the system of intermediate fields of L/F. Thus, we may regard this system as the scaffolding for **Stage 1** as a whole, built around the organizing representation *the splitting field extension* E/F *of* **p**(x). What we want is to identify some field-theoretically salient feature of this system and, if possible, to determine in what way this feature might be inherited by the extension E/F. Thus, we can take the locations to be demarcated by the intermediate fields of L/F, and the challenge now is to examine the relations of these fields.

Abel’s Scaffolding

Given that Abel does *not* have the concepts *field* and *field extension*, he needs a different way of approaching the arithmetic relations of the roots with the coefficients.

The first thing to say here is that Abel does not have epistemic resources that would allow him to adopt an organizing representation properly speaking. Let $\mathbf{p}_n(x)$ be the arbitrary general polynomial; it is clear that Abel has no means to represent the set of all arithmetic relations of the roots of $\mathbf{p}_n(x)$ with its coefficients in a way that could organize his proof at this stage. Certainly Abel knows that the coefficients are elementary symmetric functions of the roots, and in this sense he can represent the relations of the roots with the coefficients. There is no obvious way to exploit this fact at this point, however—indeed, one way to look at what Abel accomplishes in the first two stages of his proof is that he finds the proper epistemic framework for exploiting these relations. Further, certainly Abel has available to him some expression that has the same meaning and referent as “the arithmetic relations of the roots of $\mathbf{p}_n(x)$ with its coefficients.” Such an expression, however, would be far too conceptually barren to allow him to erect an epistemic scaffolding—it does not have enough inferentially engageable structure.

Among the epistemic resources Abel has, the ones most obviously pertinent to erecting a scaffolding for the process of **Stage 1** are, simply, knowing the *expressions* for the solutions of the general equations of degrees 2, 3 and 4, and his overall proficiency in *manipulating symbolic expressions*. Thus, he does the most obvious thing: he identifies a canonical expression for the general form a solution by radicals would have to have; see Pesic, pp. 171ff. This expression then organizes the rest of **Stage 1**: combined with certain general facts about relations of roots of unity, it allows Abel to erect quite an effective scaffolding for **Stage 1.2**; we will see this in more detail under our discussion of guidance.

(3) ***The scaffolding provides guidance***

Artin's aim. *Find a criterion for the solvability of* **p**(x) = 0.

Aim Guidance. Artin's scaffolding now provides aim guidance: the most natural thing to do is to examine the relations of the intermediate fields in the extension L/F.

Manipulation Guidance. With the field-theoretic concepts in place, it is very natural to consider the sequence of simple extensions obtained by adjoining the radicals that generate L over F one at a time.

Result. It is easy to show that L/F is a radical extension—that is, L/F contains a sequence of simple radical extension from F up to L.

Aim Guidance. Once we know that the splitting field E is contained in a radical extension L of F, the only obvious aim is to show that the converse also holds. Again, this is easy to do.

Result. Thus, Artin's criterion turns out to be that **p**(x) = 0 is solvable by radicals if and only if the splitting field extension E/F of **p**(x) is contained in a radical extension.

It want to emphasize just how naturally the criterion falls out once the field-theoretic concepts are in place. Indeed, as I already noted in my exposition of Artin's proof, the result with which **Stage 1** culminates is little more than a rearticulation of the definition of solvability; and yet, as we shall now see, it is an epistemically powerful one.

Abel's aim. *Find a criterion for the solvability of* $\mathbf{p}(x) = 0$.

Stage 1.1

Abel does not have much by way of a scaffolding for **Stage 1.1**. As noted above, however, he does draw some degree of aim guidance from knowing the solution formulae for equations of degrees 2, 3, and 4: the only natural aim available to Abel is to find a useable expression for the form a solution by radicals would have to have.

Result. By carrying out fairly intricate but elementary symbolic computations, Abel finds just such an expression: he proves that any solution by radicals of $\mathbf{p}_n(x) = 0$ would have to be expressible in the form we recorded in **Theorem 1**, namely

$$y = q_0 + q_1 r^{1/p} + q_2 r^{(2/p)} + \ldots + q_{p-1} r^{(p-1/p)},$$

where p is some prime number, q_0, ..., q_{p-1}, r are functions of the same form as y, and so on, until we come to rational functions of the coefficients a_1, ..., a_n of $\mathbf{p}_n(x)$.

Since we are here analyzing **Stage 1** globally, I will not discuss the details of Abel's derivation of this expression. Suffice it to say that he does enjoy some degree of aim and manipulation guidance in virtue of knowing various basic strategies for manipulating symbolic expressions. For example, he makes judicious use of *substitutions* and *collecting together terms* with a suitably chosen common factor, and so on. Still, I think it would be fair to say that he has to make quite a few *ad hoc* decisions about how to proceed in the process of deriving his general expression for the solutions. As such, I think we would find that the quality of his guidance is poorer than Artin's in the subprocesses involved in deriving his criterion of solvability.

Stage 1.2

Aim Guidance. Abel now has some aim guidance for his proof as a whole: he needs to show that no actual solution satisfies his general expression for a solution by radicals. The trick is to acquire more specific aim guidance as to what to do *next*.

The most structurally salient feature of the general expression is, of course, the way it is composed out of multiply nested radicals, with the innermost radicals being radicals over the ground field $\mathbf{Q}(a_1, ..., a_n)$. This strongly suggests that the overall aim of the proof should be to show that in the case $n = 5$, not enough such radicals exist, for some reason or another. Indeed, it is clear that the other structural features of the general expression can be more or less ignored.

Thus, Abel would be justified in thinking that he needs to examine which radicals could appear in a solution that satisfies his general expression, and show that not enough such radicals exist. This suggests a more determinate immediate aim: it seems very likely that Abel needs to find an *inferentially engageable representation* of the radicals that could appear in a solution by radicals. Perhaps the most obvious epistemic option would be to look for an *explicit*, *artifactually determinate* expression for such radicals; for given the paucity of Abel's conceptual resources, his principal mode of inferential engagement is to carry out symbolic computations. Thus, we obtain the following

Aim. Find an artifactually determinate expression for the radicals that could appear in a solution by radicals.

Location guidance. Given how vague this aim is, it is fortunate that Abel has just the right kind of location guidance to complement it. For there is really only one terrain of facts for Abel to examine at this point, namely the facts as to which radicals could occupy the formal positions marked out by the terms in his general expression. This expression by itself would not be enough to provide Abel any substantial amount of guidance, but his familiarity with Gauss' work on cyclotomic equations and primitive roots of unity allows him to erect a more structured scaffolding.[34] For if the order of the outmost radical r in the general expression is p, then Abel has p separate expressions for the solutions:

$$y_1 = q_0 + r + \ldots + q_{p-1} r^{p-1}$$
$$y_2 = q_0 + \alpha r + \alpha^2 q_2 r^2 + \ldots + \alpha^{p-1} q_{p-1} r^{p-1}$$
$$\ldots$$
$$y_p = q_0 + \alpha^{p-1} r + \alpha^{p-2} q_2 r^2 + \ldots + \alpha q_{p-1} r^{p-1}$$

and these solutions are distinct.

This system of expressions can be regarded as Abel's epistemic scaffolding for **Stage 1.2**. The terms demarcate locations: each covers a range of epistemically possible expressions, and contains a determinate range of epistemically possible facts relevant to solvability: *the term is occupied* or *it is not*. This scaffolding now provides aim and location guidance: the only obvious aim is to find a way of representing the possible values of the terms in these expressions in a way that allows us to rule out enough of them to rule out the existence of a solution formula.

The crucial feature of the situation is that the locations demarcated by the terms in the different expressions are not independent. In the terminology of Section 3.4, Abel's scaffolding is highly *connected*. This is, indeed, the mathematically specific feature of the situation that allows him to proceed. For it is now a standard exercise to express the summands on the right-hand side in terms of the solutions $y_1, \ldots, y_p$, and so Abel obtains the following

[34] See Radloff [1998], p. 68 and Pesic, p. 159.

Result. **Theorem 2**, regarded by Abel himself as his central innovation,[35] expresses the terms in the general expression as rational functions of the roots, centrally including the radicals therein:

$$r = (1/p)(y_1 + \alpha^{p-1}y_2 + \ldots + \alpha y_p).$$

This result can be regarded as having acquired mastery over the epistemically possible contents of the locations in the scaffolding. Note in particular that, at least in some cases, this expression is inferentially engageable because one can *directly see* what the effect of the permutations of the roots would be.

All this depends organically on Abel's understanding of the arithmetic relations of the primitive roots of unity 1, α, α^2, ..., α^{p-1} and in particular on knowing the relation

$$1 + \alpha + \alpha^2 + \ldots + \alpha^{p-1} = 0.$$

Thus, this piece of knowledge can be regarded as structuring his scaffolding and in virtue of doing so, providing aim guidance for Abel's symbolic computations.

If we were to consider the subprocess of deriving this expression locally, we would again find that Abel does enjoy some degree of manipulation guidance. Still, many of the individual computations would have to be considered rather *ad hoc*.

[35] See Pesic, p. 162.

(4) ***The agent can locate and extract features directly relevant to answering the question***

The aim of **Stage 1** is to identify a criterion for the solvability by radicals of polynomial equations or, to be fair to Abel, a criterion for the solvability of *general* polynomial equations. Thus, we can take it that the question one is trying to answer here is, *Under what circumstances is the general polynomial equation solvable by radicals?* Both Abel and Artin manage to answer this question, and so the only issue to address here is how to assess the comparative directness of relevance. Now, keeping in mind that we are analyzing the quality of cognitive control over the epistemic process of **Stage 1** *rather than the proof as a whole*, the relevant question is: To what extent have Abel and Artin located and extracted features of their target ranges directly relevant to their respective criteria? I think that the answer is that they both have managed to locate and extract features very highly relevant: for the issue here is *not* how directly relevant the feature in terms of which they have articulated their respective criteria is to *solvability*; rather, the issue is how directly relevant their proofs in **Stage 1** are to their respective criteria. The former issue—the one in which we are ultimately interested—will arise only at **Stage 3**. In any case, since Abel and Artin articulate different criteria, it is properly speaking not possible to make a comparative assessment as to which one has found the features more directly relevant. Thus, as far as their epistemic processes in **Stage 1** go, there isn't much to be said here.

It is worth noting that Abel does not articulate his criterion in terms of any feature that could be naturally construed as a *property of some single object* or a coherent system of objects, while Artin does. I do not think, however, that there is any reason *at this stage* to regard this as an epistemic shortcoming in Abel's approach—at any rate, no reason that isn't directly motivated by some *a priori* conception of the nature of mathematical ontology. As we will see later on, however, their respective criteria take them down very different epistemic paths, and many of the virtues of cognitive control in Artin's process, as well as the failures in Abel's, can be traced back to the character of these criteria. It does turn out that the fact that Artin's criterion is articulated in terms of a single property of a coherent system of objects allows him epistemically critical moves that are just not available to Abel.

4.2.2 Stage 2: Transforming the Task

Aim. Find a way of showing that the criterion is not satisfied for $\mathbf{p}_5(x)$.

Artin's Result. We will try to prove that the Galois group G(E/F) *of* $\mathbf{p}_5(x)$ *is not a solvable group.*

Abel's Result. We will try to apply the **Combinatorial Principle** *within the scaffolding provided by* **Stage 2** *to show that not enough radicals exist that have the same number of values as a radical as they have as a rational function of the roots.*

The principal epistemic significance of **Stage 2** in both proofs is that the original task is transformed into one each mathematician is able to negotiate with their respective tools.

Artin's criterion is that a polynomial equation $\mathbf{p}(x) = 0$ is solvable by radicals if and only if the splitting field extension E/F of $\mathbf{p}(x)$ is contained in a radical extension. Abel's criterion is that a polynomial equation $\mathbf{p}(x) = 0$ is solvable by radicals if and only if an expression for the roots in terms of the coefficients of a certain standard form exists. He then shows that if such an expression does exist, the roots of $\mathbf{p}(x)$ must have certain arithmetic relations, namely the ones articulated in **Theorem 2**.

Thus, at the beginning of **Stage 2**, the target range for Artin's proof would be the set of all facts about the organization of the systems of intermediate fields of the various finite field extensions L that contain the splitting field extension E of $\mathbf{p}_5(x)$; the target range for Abel's proof would be the set of all facts about the arithmetic relations of the roots of $\mathbf{p}_5(x)$. For clearly Artin needs to examine the organization of these systems and show that the particular features such a system would have if $\mathbf{p}_5(x) = 0$ were solvable by radicals are not in fact present; Abel needs to examine the arithmetic relations of the roots of $\mathbf{p}_5(x)$ and show that the particular relations that would hold if $\mathbf{p}_5(x) = 0$ were solvable by radicals do not in fact hold. It is clear, indeed, that when one has proven a criterion for the obtaining of some property articulated in terms of some particular set of facts, one thereby knows that any terrain of facts that contains them is a target range. Thus, by my lights, Artin and Abel would count as having identified target ranges for the rest of their epistemic processes.

The problem is that it is difficult to examine either one of these two target ranges directly. Even with Artin's relatively rich epistemic resources, it would be *very* difficult to examine all the various extensions L of the splitting field E of $\mathbf{p}_5(x)$ directly so as to determine whether E is contained in a radical extension. With Abel's relatively meager resources, it would be very difficult indeed to examine the relations of the roots of $\mathbf{p}_5(x)$ directly so as to determine whether they are related in the way his criterion for solvability requires; it is not even clear what doing so would amount to in Abel's conceptual setting.

Thus, the overall aim of **Stage 2** becomes to identify a target range to replace the said two ranges and, in particular, construct an organizing representation and scaffolding that in **Stage 3** can be used to determine whether $\mathbf{p}_5(x) = 0$ is solvable by radicals.

(1) ***The agent has identified a target range***

In Artin's approach, the initial target range for **Stage 2** is the organization of the systems of intermediate fields of finite extensions L of an *arbitrary* finite field extension E/F; in Abel's approach, it is the arithmetic relations of the roots of the general polynomial $\mathbf{p}_5(x)$ of degree 5. Thus, it is here at **Stage 2** where the two proofs first diverge in that Artin continues to examine issues pertaining to solvability quite generally, whereas Abel focuses on the case of $\mathbf{p}_5(x)$.

The aim of the early substages of **Stage 2** in each proof is to find a different set of facts naturally related with the target range identified at **Stage 1**, one that can be adopted as the target range for the rest of **Stage 2**. In view of the overall aim of **Stage 2**, these new ranges should be ones we can examine more readily and, in particular, ones in which we can locate features that are directly relevant to solvability by radicals.

At **Stage 2.1**, Artin adopts as his target range the facts about the compositional relations of the F-automorphisms of E, where E/F is the arbitrary field extension, and as his organizing representation *the Galois group* G(E/F) *of* E/F; it is clear that this representation consolidates his target range. I will examine the justification for adopting this set of facts as the target range in my semi-local analysis in Section 4.3.

The facts about the compositional relations of the F-automorphisms of E, and the concept *Galois group* are such a natural fit that, to someone familiar only with the modern approach, it might seem contrived to say that there are two epistemically independent accomplishments here; at any rate, it might seem contrived to say that Artin *first* focuses on the facts about the relations of the F-automorphisms of E and *then* adopts the *Galois group* G(E/F) as the representation of that set of facts: if anything, it is the other way around. As the historical evolution of Galois theory attests, however, there are other ways of representing this range of facts. In his 1830 approach to solvability, Galois himself did indeed focus on the said relations but did not have an explicitly articulated concept of group to represent them as a whole; he certainly did not have the concepts *subgroup*, *coset* and *quotient group* to represent large-scale patterns in this group. These conceptual shortcomings account for the felt lack of clarity and precision in Galois' treatment—as I would put it, but cannot argue here, they are responsible for the lapses of cognitive control in Galois' proof of the unsolvability of $\mathbf{p}_5(x)$. Thus, in order to appreciate the epistemic accomplishments of Artin's conceptually mature approach, it is *vital* to distinguish the feat of identifying a target range from the feat of adopting a useful organizing representation of that range.

Given the results he has obtained at **Stage 1**, Abel knows that in order to show that no solution formula exists for $\mathbf{p}_5(x)$, it is sufficient to show that not enough radicals of the right orders exist. In particular, given **Theorem 2**, he is justified in thinking that this might be accomplished by showing that not enough radicals can be expressed as rational functions of the five roots of $\mathbf{p}_5(x)$. For he knows the **Combinatorial Principle**: the number of distinct values of a radical as a radical is the same as its number of values as a rational function. As I noted in Chapter 3, however, for all Abel knows at this stage in his proof, there might not be enough constraints on the number of possible values rational expressions of the roots of $\mathbf{p}_5(x)$ can take to rule out the existence of a solution by radicals. Thus, the range of facts he has chosen to examine is not at this point known to be sufficient to settle the issue of solvability of $\mathbf{p}_5(x) = 0$. As such, Abel does not count as having *identified* a target range for **Stage 2** of his process.

I need to emphasize, moreover, that Abel stands no chance of consolidating this target range: there is no single object or a coherent system of objects we could think of these facts as facts about. We will come back to this.

The sets of facts Artin and Abel adopt as their target ranges for **Stage 2** are closely related, yet importantly different. While Artin is examining the structure of the Galois group G(E/F) *itself*, in modern terms, Abel is examining the *effect* of the action of G(E/F) on individual elements in the extension E/F: for the number of distinct values of a rational function of the roots under the permutations of those roots is, in modern terms, the number of field conjugates of an element in E, that is, the number of distinct images of an element under the action of G(E/F).

As will become clear in this section, most of the epistemically crucial differences between the two approaches can be traced back to this difference in their target ranges and, specifically, the organizing representations of those ranges available to Artin and Abel. Artin is able to consolidate his target range, while Abel is not; as a consequence, Artin is able to extract a feature of his target range directly relevant to solvability; Abel is not. Artin can erect a highly connected epistemic scaffolding for the final stage of his proof; Abel cannot. Finally, though this is not an issue of cognitive control, we should keep in mind that since the splitting field of any polynomial, general or special, has a Galois group, Artin's approach can in principle be used to examine the solvability by radicals of any polynomial; Abel's cannot. His approach depends essentially on the field extension under consideration being the splitting field of the general polynomial of degree five.

(2) ***The agent has an organizing representation that erects a scaffolding***

I will consider the epistemic contributions of *the Galois group* in the next section in the context of our semi-local analysis of the subprocesses falling under Artin's **Stage 2**. I will try to make it visible that this representation allows Artin to erect an excellent epistemic scaffolding that provides him wonderful aim and location guidance throughout **Stage 2**.

Abel can represent his target range only with some non-consolidating expression that has the same meaning and referent as the expression "the number of possible values various rational expressions of the roots of $\mathbf{p}_5(x)$ can take under the permutations of those roots." As it turns out, however, this failure to organize the representation of his target range ontologically does not hamper the quality of the scaffolding Abel erects for the later subprocesses falling under in his **Stage 2**. This should seem somewhat surprising. For it would be natural to suppose that this is the stage where the quality of Abel's cognitive control begins to deteriorate significantly; for it is at this stage that his proof begins to diverge substantially from the modern one organized by the group-theoretic concepts. In particular, it would be natural to expect that this deterioration is occasioned by the nature of his organizing representation and the scaffolding he erects.

We will see in our analysis of **Stage 3** that in many ways these expectations are borne out. I want to emphasize, however, that Abel's scaffolding for **Stage 2** *itself* is actually quite excellent. This is one of the places where I want to recommend that an attentive reconstruction of the structure of Abel's epistemic process allows us to see the very real strengths of his epistemic standing. It is after all remarkable that Abel accomplishes what he does with such a meager set of resources; I want to recommend that he succeeds precisely by squeezing every bit of control he can from the resources he has.

Thus, I take it that the expression "the facts about the number of possible values various rational functions of the roots $\mathbf{p}_5(x)$ can take under the set of all permutations of those roots" is the organizing representation for Abel's **Stage 2**, even if he does not count as having identified a target range. This expression allows Abel to erect an epistemic scaffolding, as follows. (*a*) The locations $\mathbf{L}_m$ are parametrized by numbers between 1 and 120, inclusive: since there are 120 different permutations of five independent variables, and since Abel is treating the roots of $\mathbf{p}_5(x)$

as independent variables, 120 is the largest number of distinct values a rational function of the roots can take under those permutations. (*b*) Each location $\mathbf{L}_m$ covers a determinate stretch of Abel's target range, namely the epistemically possible rational functions of the roots of $\mathbf{p}_5(x)$ with *m* distinct values, and (*c*) contains two epistemically possible facts: *yes*—some such rational function takes *m* distinct values and *no*—none does. Certainly (*d*) either one would rule out the other; finally, it is clear that (*e*) these locations contain all the epistemically relevant facts about Abel's target range.

It can be difficult to properly appreciate the tremendous epistemic importance of having a representation of one's target range that is organized in this way already at the outset of one's investigation. It is helpful to compare the situation Abel is in now with the situation he was in at the end of **Stage 1**: given his conceptual resources, he has cannot represent the epistemically possible facts about the relations of the roots of $\mathbf{p}_5(x)$ in a way that would be at all structured and organized. I do not deny that having a numerical parametrization is one of the epistemically 'thinnest' ways of erecting a scaffolding; indeed, we will see that such scaffoldings tend to have serious shortcomings. But these shortcomings are *insignificant* when compared with the deep, fundamental contributions of having a determinate range of numerically parametrized locations in view: Abel now has a fully determinate epistemic space to operate in, a fully determinate range of facts to go after.

I want to make the relationship between Abel's **Stage 2** and **Stage 3** as clear as possible, for there is something potentially confusing here. On the one hand, the overall aim of his **Stage 2** is, essentially, to erect a scaffolding for **Stage 3**. On the other hand, the scaffolding for **Stage 3** is built on top of the one Abel erects for **Stage 2** itself. The reason I am fussing over this point is that I want to articulate the structural parallels between the processes of Abel and Artin as clearly as possible so as to put us in as good a position as possible to compare the character of cognitive control in them. The distinction between the organizing representations and scaffoldings between **Stage 2** and **Stage 3** in Artin's process are easier to see because his **Stage 2** is still fully general, and it is only at **Stage 3** that he focuses on the case of $\mathbf{p}_5(x)$. Abel, in contrast, focuses on the case of $\mathbf{p}_5(x)$ already at his **Stage 2** and, consequently, it can be harder to see the distinction between the epistemic significances of **Stage 2** and **Stage 3** and, consequently, harder to see the epistemically significant parallels between **Stages 2** and **3** in the two proofs.

(3) ***The scaffolding provides guidance***

In the next section, I will provide a semi-local analysis of the guidance Artin and Abel enjoy in the subprocesses falling under **Stage 2** in their respective proofs. We will see there that Artin's scaffolding provides him excellent aim, location and manipulation guidance; what may be a bit surprising is that Abel's scaffolding provides him excellent aim guidance, although his location and manipulation guidance are not very good.

The theorems in Abel's set of epistemic resources at the beginning of **Stage 2** provide his scaffolding with a good bit of structure. **Lagrange's theorem** tells Abel that only the locations for which m divides 120 can contain *yes*, while **Ruffini's theorem** tells him that for m less than or equal to 5, the only locations that can contain *yes* are the ones for $m = 1$, 2 and 5. This fact is significant because, in the course of proving **Theorem 2**, it becomes clear that Abel may get away with only investigating radicals with p distinct values as a radical where p is a prime not exceeding 5. At any rate, he knows that all the radicals over the field F of coefficients of $\mathbf{p}_5(x)$ that could appear in a solution formula would have p different values as radicals.

Thus, once all the foregoing bits of knowledge are factored into his scaffolding, Abel has excellent aim guidance for the rest of **Stage 2**: it is clear that his aim should be to find expressions for rational functions with 2 and 5 distinct values, expressions that are highly inferentially engageable in a way that would facilitate ruling out enough of the remaining options at **Stage 3**. This is just what Abel sets out to do at the later two subsidiary stages of **Stage 2**; we will consider these stages in more detail in Section (4.3) below.

(4) ***The agent can locate and extract features directly relevant to answering the question***

The aim of **Stage 2** is to find a way of showing that the criterion for solvability identified at **Stage 1** is not satisfied for the general polynomial of degree 5. Thus, we can take the questions to be, *Under what circumstances is the splitting field* E *of* **p**(*x*) *not contained in a radical extension of the ground field F?* for Artin and, *Under what circumstances does there not exist a formula satisfying the general expression for a solution by radicals?* for Abel. Again, as in **Stage 1**, both Abel and Artin manage to find some feature of their mathematical situation they can hope to test in the case of the general equation of degree 5. And, again, since they are focusing on different criteria, it is properly speaking not possible to compare the directness of relevance of what they accomplish. Less formally, it seems right to say that Artin has managed to locate and exactly the features very highly relevant to answering his question—indeed, one wants to say, exactly the *right* features: if the Galois group G(E/F) is not solvable, then E is not contained in a radical extension of F. This is just the sort of conceptually articulated, 'high-level' feature of a target range my definition of directness of relevance is intended to capture. Note, in particular, that the concept *Galois group* is at a higher level relative to the *concept field extension* and, as such, the sentence *The Galois group is not solvable* is at a higher level of conceptual articulation than to *The splitting field extension is not contained in a radical extension*. That the Galois group is not solvable is just the sort of pattern in the target range these notions are meant to capture.

Abel's answer, in contrast, is articulated at the same level of conceptual articulation as his criterion. In particular, as in **Stage 1**, Abel does not manage to identify any feature of his mathematical situation that could be naturally construed as a property of some single object or a coherent system of objects. Indeed, I think that here this intuition is even stronger—in **Stage 1**, we at least had the general expression for a solution as a radical as a kind of a 'formal' object. But again, there is no denying that Abel has identified a feature of the mathematical situation as a whole: if there aren't enough radicals with the appropriate number of values, there is not enough radicals to constitute a solution formula. Thus, while it is properly speaking possible to compare the two proofs for directness of relevance, it seem very compelling to say that, with the obvious relaxation in our attitude, that Artin *clearly* manages to answer his question more directly than Abel his.

This, then, is where the two proofs diverge decisively. Given the wonderful consolidating representation of his target range, *the splitting field extension*, Artin is able to identify a single coherent structure associated with it, the Galois group, and extract a property of groups that is directly relevant to determining whether the splitting field extension is contained in a radical extension: being a solvable group. Artin accomplishes this feat of locating at **Stage 2.3** by considering the property of being a radical extension, and uses the Galois correspondence to locate a corresponding property in the system of normal subgroups of the Galois group; further work shows that the relevant property is being a solvable group.

In sum, Artin's epistemic standing with respect to his criterion of solvability has now become decisively different from Abel's to his. Artin has a coherent system of objects he can investigate by using the concepts and methods of group theory. Abel, in contrast, will need to investigate all the possible orders individually, and rule them out one at a time.

4.2.3 Stage 3: Answering the Question

Artin's Aim. Prove that the Galois group of $\mathbf{p}_5(x)$ *is not a solvable group.*

Abel's Aim. Prove that not enough radicals with the right number of values exist for there to be a solution formula by radicals for $\mathbf{p}_5(x) = 0$.

(1) *The agent has identified a target range*

At **Stage 2**, Artin showed that a finite field extension K_2/K_1 is contained in a radical extension if and only if the Galois group $G(K_2/K_1)$ of that extension is a solvable group. Thus, at **Stage 3**, he adopts as his target range the facts about the organization of the system of subgroups of the Galois group G(E/F) of the splitting field extension of $\mathbf{p}_5(x)$. It is of course clear that Artin knows this is a target range, given the result from **Stage 1** and **Stage 2**.

Abel has managed to build an epistemic scaffolding around the possible values a rational function of the roots of the polynomial can take, and he has acquired an explicit expression for the rational functions that take 2 and 5 distinct values. He adopts as his target range the facts about the possible values radicals of various orders not exceeding 5 can take. The idea is now to apply the scaffolding constructed in **Stage 3**, along with the said expressions, to show that not enough radicals exist for there to be a solution formula for $\mathbf{p}_5(x)$. His **Stage 3** is as a *reductio ad absurdum* in which a number of independent possible classes of radicals are ruled out by showing that their existence would violate the **Combinatorial Principle**.

I want to take this occasion to note that the **Combinatorial Principle** plays two different epistemic roles in Abel's process. At **Stage 2**, it was used to structure the scaffolding being built for **Stage 3**; at **Stage 3**, it is used to show that the criterion for solvability from **Stage 1** is not satisfied for $\mathbf{p}_5(x)$ by showing that certain radicals that could appear in a solution formula do not in fact exist. This is done by showing that for a given value of *p*, the radical of order *p* that could appear in a solution formula has a different number of values as a radical (not necessarily *p*, though) than the rational expression of the roots that represents that radical, or else, that the radical would have to have a number of values as a radical already prohibited at **Stage 2**. Thus, it is *only* at **Stage 3** that the **Principle** should be seen as facilitating a *reductio ad absurdum*. I want to emphasize this point because Abel's proof is usually represented as a one long *reductio*. As my analysis shows, however, this point of view is at best unhelpful since it prevents us from seeing the structural similarities between the proofs of Abel and Artin; at worst, it is downright mistaken since it misrepresents the contributions of the central elements in Abel's set of epistemic resources.

(2) ***The agent has adopted an organizing representation that erects scaffolding***

Certainly both Abel and Artin have an organizing representation, and certainly both have scaffoldings. But while Artin's scaffolding turns out to be connected in a crucial way, the locations in Abel's scaffolding are largely independent.

At **Stage 3.1**, Artin's organizing representation is *the Galois group* G(E/F) *of the splitting field of* $\mathbf{p}_5(x)$; at **Stage 3.2**, it becomes the symmetric group $\mathbf{S}_5$ on five letters; for Artin proves at **Stage 3.1** that G(E/F) ≈ $\mathbf{S}_5$. The scaffolding at the first stage is really just the possible permutations of the roots; the scaffolding at the latter is the epistemically possible normal series of subgroups in $\mathbf{S}_5$. It is the structure of this scaffolding that makes the epistemically crucial difference for Artin's proof; we will consider it below.

At **Stage 3.1**, Abel's organizing representation is again really just the expression "the number of values radicals of orders not exceeding 5 can take." Much as in **Stage 2**, there is no way to construe this terrain of facts as facts about any single property or a coherent system of objects.

The scaffolding for Abel's **Stage 3** will be essentially a fragment of the one constructed in **Stage 2**. The locations $\mathbf{L}_m$ are parametrized by *the order m of the radical over the field of coefficients*. Thus, we need to emphasize that this scaffolding contains locations for m that are not primes and are greater than 5. Each location contains two epistemically possible facts: *yes*—a radical of this order over F exists, and *no*—a radical of this order over F does not exist. It is not clear from the outset just which m would be large enough to contain all the epistemically possible orders, although it is clear that m must divide 120.

(3) ***The scaffolding provides guidance***

Guidance in Artin

I will consider the following two stages in more detail in Section (4.3). For now, I will consider them briefly as components of **Stage 3** considered globally and, as such, I will treat the results obtained in them as given.

Stage 3.1

Aim. Identify the Galois group G(E/F) *of the splitting field extension* E/F *of* $\mathbf{p}_5(x)$.

Location Guidance. The coefficients a_1, ..., a_5 of $\mathbf{p}_5(x)$ are just the five elementary symmetric functions in five letters representing the roots x_1, ..., x_5, hence fixed by any permutation of those letters. Thus, we can take $\mathbf{Q}(x_1, ..., x_5)$ as the splitting field of $\mathbf{p}_5(x)$ and $\mathbf{Q}(a_1, ..., a_5)$ as the field of coefficients. So now we only need to determine the group of this extension.

Result. But this task is trivial: since there are no non-trivial arithmetic relations between the roots of $\mathbf{p}_5(x)$, *any* permutation of the roots, extended by linearity to a mapping on E, is an F-automorphism of E/F. Hence, the Galois group G(E/F) is isomorphic to the symmetric group $\mathbf{S}_5$.

Thus, we come to the final local stage in Artin's proof. As one might expect, this is where the epistemic differences between the two approaches really come into focus. The task in Artin's **Stage 3.2** is to determine whether $\mathbf{S}_5$ is a solvable group; the task in Abel's **Stages 3.1** and **3.2**, which may be thought of as jointly corresponding to **Stage 3.2** in Artin, is to show that there aren't enough radicals for there to be a solution formula for $\mathbf{p}_5(x)$.

Stage 3.2

Aim. Show that $\mathbf{S}_5$ *does not contain a normal series with abelian quotients*

Location Guidance. Simple group-theoretic considerations show that any normal series in $\mathbf{S}_5$ must begin with the unique normal subgroup of index 2, the alternating group $\mathbf{A}_5$.

Result. However, since $\mathbf{A}_5$ is a non-abelian simple group, the only possible normal series in $\mathbf{A}_5$ would be $\{1\} \subset \mathbf{A}_5$, and the quotient $\mathbf{A}_5/\{1\} = \mathbf{A}_5$ is not abelian. Thus, the group $\mathbf{S}_5$ is not solvable and hence, $\mathbf{p}_5(x) = 0$ is not solvable by radicals.

Guidance in Abel

In view of the results established at **Stage 2**, it is clear what Abel needs to do to collapse the various locations: he needs to consider them one by one, employ the explicit expressions for rational functions with 2 and 5 distinct values, and use the **Combinatorial Principle** to show that no radical with the given number of values exists.

Stage 3.1

Aim. Determine for which p there are radicals of order p over the field of coefficients F.

This is the obvious first aim since it is here that the foregoing results apply most directly.

Location Guidance. The only locations in the scaffolding we need to investigate at this stage are the ones parametrized by $p = 2$ and $p = 5$; for we know that when the order of the radical r over F is a prime, it is exactly the number of values of r as a radical.

Manipulation Guidance. This is clear: we need to consider the expression for a radical r that is assumed to appear in the solution formula, and consider the effect of the permutations of the roots on that expression. In the case r is assumed to have five distinct values as a radical, we find that the said expression would have 120 values. This violates the **Combinatorial Principle**.

Result. Thus, we find that any radical over the ground field F = $\mathbf{Q}(a_1, ..., a_5)$ must have order 2. From **Theorem 5** we know that such a radical has the form $p + \rho q$. In modern terms, this is to say that the only simple radical extension of F is isomorphic to the one generated by the square root ρ of the discriminant of $\mathbf{p}_5(x)$.

Stage 3.2

Aim. Determine for which p radicals of order p exist over the field generated by ρ.

Location Guidance. The task at this stage is more complicated than at **Stage 3.1** because the order of the radical r over F(ρ) no longer equals the number of values of r as a radical, namely the order of the minimal polynomial of r over F.

Manipulation Guidance. The idea is exactly the same as in **Stage 3.1**, except that some of the possible numbers of values need to be ruled out by using other means.

The logical structure of the proof here is more complicated because the number of possible distinct values of such a radical could be greater than 5, and so we cannot apply **Theorem 3** directly. Nevertheless, the final contradictions turn out to be violations of our crucial

Combinatorial Principle: the number of distinct values of a radical considered as a radical would be different from its number of values as a rational function of the roots.

Result. We find that there are no radicals over F(ρ) that could satisfy all the constraints we have found.

Thus, we see an epistemically crucial difference between the scaffoldings of Artin and Abel for their respective **Stages 3.2**. They are both out to show that their respective criterion for solvability is not satisfied for $\mathbf{p}_5(x)$. On the one hand, having extracted a single property of groups directly relevant to solvability, all Artin needs to do is to show that $\mathbf{S}_5$ does not have this property, and given the known structure of this group, the task is trivial: there is only one possible normal sequence to consider. Abel, in contrast, has to rule out a whole array of epistemically possible primes for which a radical of the requisite form might exist. The task at the first level is not too bad, but already at the second level, there is a rapid multiplication of locations in Abel's scaffolding he needs to examine. Artin, in contrast, can collapse his scaffolding by only examining one location. This is because in Artin's approach the locations, the epistemically possible normal series, are all fused together at the top; in Abel's approach, the locations are *independent*. As I emphasized in my discussion of scaffoldings in Chapter 3, this is one way in which the locations in a scaffolding may (Artin) or may not (Abel) be connected in a way that makes the scaffolding inferentially responsive.

(4) ***The agent can locate and extract features directly relevant to answering the question***

Artin has certainly located and extracted features of G(E/F) that are highly directly relevant to showing that G(E/F) is not solvable: indeed, the fact that any normal series in $\mathbf{S}_5$ must begin with $\mathbf{A}_5$ is just such a feature. Abel, too, may be regarded as having located and extracted features of the overall mathematical situation that are quite directly relevant to showing that there aren't enough radicals for there to be a solution by radicals of the form he identified in **Theorem 2**. However, as we have already discussed, these are not features cannot be construed as properties of any single object or a coherent system of objects.

We have now reached the aim of the two epistemic processes as a whole:

Result. The general polynomial equation $\mathbf{p}_5(x) = 0$ *of degree 5 is not solvable by radicals.*

As I have noted time and again, there is a strong intuition to the effect that Artin manages to locate and extract *just* the features directly relevant to solvability by radicals, whereas Abel does not. Indeed, it is easy to see that my definition of directness of relevance yields this verdict. First, it is clear that the model-theoretic conditions are satisfied for the notion to be applicable. Second, it is clear that the fact in which Artin's proof culminates, that the Galois group of $\mathbf{p}_5(x)$ is not solvable, is articulated at a much conceptually higher level than any fact Abel manages to extract. As I have noted, it is not even clear whether we should regard Abel as having located any single feature at all relevant to solvability: given the paucity of his conceptual resources, the fact that there aren't enough radicals for there to be a solution by radicals does not come into view as a property of any object or a coherent system of objects. In modern terms, of course, we can identify the fact to which Abel is indirectly responding: the splitting field extension of the general polynomial of degree 5 is not a radical extension.

4.3 SEMI-LOCAL ANALYSIS

Artin's Stage 2.1

Aim. Associate some organizationally simpler structure with the splitting field extension E/F *of a polynomial* **p**(*x*); *we associate with* E/F *its Galois group* G(E/F).

This stage is essentially preparation for **Stages 2.2** and **2.3**. While in many ways it is *the* epistemically pivotal stage in Artin's approach, its internal organization is very simple. This is our first example of a subprocess where we start out with all the relevant facts already at hand, and the scaffolding is an *inferential scaffolding* in the sense introduced in Section 3.6.4. As we will now see, the notion of guidance applies just as it does in the case of ontic scaffoldings.

(3) *The Scaffolding Provides Guidance*

Aim. Associate some organizationally simpler structure with the splitting field extension E/F *of a polynomial* **p**(*x*).

Aim Guidance. Given an organizationally complex structure **A**, it is a standard strategy in structural mathematics to try to associate with it a simpler one **B** in such a way that the large-scale organization of **A** is reflected in the large-scale organization of **B**.

Location Guidance. It is a standard strategy in structural mathematics to consider the *group of automorphisms* of a given algebraic structure **A**; indeed, we know generally that the organization of this group tends to reflect the organization of **A** itself.

Indeed, we know that each permutation of the roots of **p**(x) extends by linearity to an F-automorphism of E and that these automorphisms form a group; this is a finite group naturally associated with the extension E/F. In particular, it is clear that each subgroup H of G has a *fixed field* in E, the set of all elements left fixed by all the automorphisms in H. Thus, we are justified in thinking that features of the organization of the lattice of subgroups of G(E/F) might reflect features of the organization of the lattice of intermediate fields of E/F.

Finally, we are justified in thinking that the organization of the lattice of subgroups of the Galois group G(E/F) might have features relevant to solvability by radicals of **p**(x) = 0. For it is clear at this stage that the *orbit* of a root x of **p**(x) under the action of G(E/F) consists of all the roots of an *irreducible factor* of **p**(x), namely the *minimal polynomial* of x. Thus, we are justified in thinking that the organization of G(E/F) might reflect the relations of the roots in some way and the latter, we have noted, is what ultimately governs the solvability or not of **p**(x) = 0.

Result. We will consider the group G(E/F) of F-automorphisms of E.

Artin's Stage 2.2: ***The Galois Correspondence***

Aim. Thus, we want to establish a *correspondence* between the intermediate fields of the splitting field extension E/F of **p**(x) and the subgroups of G(E/F) in such a way that some feature of the organization of the latter system reflects those features of the former that are directly relevant to solvability—namely, *being contained a radical extension* should have a tractable group-theoretic counterpart.

Aim Guidance. Again, the obvious way to start is to consider a radical extension L/F, rather than E/F itself, and try to set up a correspondence between the system of intermediate fields of L/F and the system of the subgroup G(L/F) and then proceed to consider what this might tell us about the organization of the group G(E/F).

In order for the correspondence to track the property of *being a radical extension*, it needs to track the relationship of *being a simple radical extension* between intermediate fields of L/F. It seems likely that in order for this to happen, the correspondence needs to be *bijective*; for in general an intermediate field K in a radical extension L/F will have some extensions in L/F that are simple radical extensions and others that are not.

Aim Guidance. We already have a way of associating a subgroup H of the Galois group G(L/F) with its fixed field L^H. In the reverse direction, the most obvious thing to do would be to associate an intermediate field K in L/F with its Galois group G(L/K). For it is trivial that G(L/K) is a subgroup of G(L/F). If we can show that the two associations are *mutually inverse*, we will have shown they are both one-to-one and onto, and hence, we have our bijective correspondence. For it is trivial that if any map α: A → B has an inverse β: B → A, then α is one-to-one; if α is the inverse of β, β is one-to-one also and, in particular, both α and β are onto.

I will consider the epistemic process in **Stage 2.2** in greater detail by considering the individual subprocesses falling under it; thus, the following brief remarks are meant to be about **Stage 2.2** as a whole, not so much about those subprocesses themselves. Note in particular that we are *not* here considering these processes *locally*—that is, we are still regarding many of the particular inferential moves in them as black boxes.

Stage 2.2.1

Aim. *Identify the property required for a bijective correspondence*.

This is another central example of a subprocess where the relevant facts are already at hand, and the scaffolding is an inferential scaffolding.

(3) ***Scaffolding provides guidance***

The aim guidance is provided by the very characterizing properties of the field extensions we are dealing with: the splitting field extension E/F is characterized by the fact that some polynomial with coefficients in F splits in E. Now we know that this means that the field E contains all the field conjugates of each of the roots of that polynomial, for those conjugates are just the other roots. Thus, this suggests at once that the crucial property might be that the field E contains all the field conjugates of each of its elements.

(4) ***The agent can locate and extract features directly relevant to answering the question***

As it turns out, this property, called *normality*, is just the property directly relevant to there being a bijective correspondence. In focusing on the orbits of elements of E, we have located that property in our inferential scaffolding, and the extraction amounts to noting the required completeness property of these orbits. Now of course we do not know that this property actually works until we have completed **Stage 2.2**—again, when a stage has substages embedded in it, the actual result only comes at the end.

Our aim guidance for **Stage 2.2** as a whole now dictates two obvious immediate aims: show that the mapping $H \to E^H$ is the inverse of $K \to G(E/K)$ and that the mapping $K \to G(E/K)$ is the inverse of $H \to E^H$, where it is assumed that the ambient extension E/F is normal.

Stage 2.2.2

Aim. Show that the mapping $H \to E^H$ *is the inverse of* $K \to G(E/K)$.

Result. This was our **Lemma 1**: if E/F is a normal extension, then F is the fixed field of G(E/F). Thus, given a normal extension E/F, we can apply this to any intermediate field K for which E/K is a normal extension.

Clearly this suggests that we should show that when an extension E/F is normal, then so is E/K for any intermediate field K of E/F. But let us first consider

Stage 2.2.3

Aim. Show that the mapping $\mathrm{K} \to \mathrm{G(E/K)}$ *is the inverse of* $\mathrm{H} \to \mathrm{E}^{\mathrm{H}}$.

Result. This was our **Lemma 2**, *Artin's lemma*: if H is any subgroup of G(E/F), then the Galois group $\mathrm{G(E/E^{H})}$ of the fixed field of H is precisely the group H itself.

Stage 2.2.4

Aim. Show that if E/F is a normal extension, then so is E/K for any K contained in E/F.

Result. This was our **Lemma 3**.

Thus, when considered semi-locally, *the* central epistemic process of Artin's entire proof, **Stage 2.2**, has an inferential scaffolding—there is no mathematically heavy lifting to do. The subprocesses in **Stage 2.2**, considered semi-locally, constitute a very natural sequence, and there is absolutely no uncertainty at any point as to what the next aim should be. This is one way of bringing out the remarkable epistemic character of Artin's proof: by having made just the right choice about how to focus the investigation at the outset, the actual 'work' in the meaty middle part of the proof is quite easy. And there is more: if we considered the subprocesses in **Stages 2.2.2**, **2.2.3** and **2.2.4** *locally*, we would see that Artin has excellent scaffolding for each one. For in **Stage 2.2.2** it is trivial that H is contained in $\mathrm{G(E/E^{H})}$; in **Stage 2.2.3** it is trivial that K is contained in the fixed field of G(E/K). Thus, in each case, the aim is to show that the reverse containment also holds. Further, as we will see in Section 4.4.1, in **Stage 2.2.4** there is also excellent location and manipulation guidance, enjoyed in virtue of the scaffolding within which **Stage 2.2** overall takes place.

Artin’s Stage 2.3

Aim. Identify the feature of the system of subgroups of the Galois group G(L/F) *that corresponds to* L/F *being a radical extension.*

This is the only natural aim, given the Galois correspondence and the fact that a polynomial equation $\mathbf{p}(x) = 0$ is solvable by radicals if and only if the splitting field extension of $\mathbf{p}(x)$ is contained a radical extension. This is yet another subprocess in Artin’s proof that has an inferential scaffolding, one that is erected by the foregoing two facts and our overall group-theoretic competence.

(3) ***Scaffolding provides guidance***

Aim Guidance. Since a radical extension L/F is characterized by the fact that it contains a radical sequence from F up to L, the natural aim would be to consider the image of such a sequence in G(L/F) under the Galois correspondence. As we noted in Chapter 2, however, there are certain technical issues here that need to be handled with care. Again, first, we need to make sure that extension L/F can be taken to be normal; indeed, this is the first obvious subsidiary aim. Second, we cannot in general consider the simple radical extensions in L/F directly since they need not be normal. There are, however, several readily available ways around this problem. What is to be emphasized here is that we know from the start what the issue is: we simply need to make sure that we consider intermediate extensions that contain the requisite roots of unity; indeed, this may be considered a bit of aim guidance. The upshot is that we will consider a sequence of intermediate extensions in L/F that is closely related with the given radical sequence in L/F.

(4) ***The agent can locate and extract features directly relevant to answering the question***

The image in G(L/F) of the appropriate kind of sequence of intermediate fields in L/F turns out to be a sequence of embedded subgroups of the sort that characterizes solvable groups.

Artin's Stage 2.4

Aim Guidance. Only one obvious aim remains: to determine whether G(E/F) is itself a solvable group, given that G(L/F) is.

Result. It is, by an easy group-theoretic argument; see Section 2.3.1.

Thus, the following result amounts to reaching the aim of **Stage 2** as a whole:

Result. *If* E/F *is contained in a radical extension*, *then* G(E/F) *is a solvable group*.

The implication holds in the other direction also, but it is irrelevant here, since we are looking for a way of showing that our criterion of solvability by radicals is not satisfied for the general polynomial equation of degree 5. Thus, in **Stage 3**, we will try to show that the Galois group of $\mathbf{p}_5(x)$ is not a solvable group.

Abel's Stage 2.1

Aim Guidance. Find a more inferentially engageable representation of the rational functions whose number of values would allow them to appear in a solution by radicals.

This is the aim for **Stage 2.1** dictated by the overall aim of **Stage 2**: the radicals that could appear in a solution formula can be expressed as rational functions of the five roots of $\mathbf{p}_5(x)$ and in order to rule out enough radicals, Abel's epistemic resources force him to reason directly about explicit expressions for the rational functions.

Stage 2.1.1 *Aim Guidance. Restrict the range of rational functions that could be expressions for radicals in a solution formula.*

This is the only obvious aim, given that we will need to rule out enough such functions somehow or other. There is a specific bit of Abel's mathematical background that suggests that such a restriction might be a realistic aim:

Theorem 3 *The number of distinct values a rational function $f(x_1, ..., x_n)$ in n independent variables $x_1, ..., x_n$ can take under the permutations of the variables divides the product $n! = n \times (n-1) \times ... \times 2 \times 1$, the so-called factorial $n!$ of n.*

On the one hand, Abel knows that the radicals can be expressed as rational functions in five independent variables, namely the roots of $\mathbf{p}_5(x)$, and here we have a result that puts a constraint on the number of values such an expression can take under the permutations of the roots. On the other hand, it is clear from the outset that a p-th order radical itself will take some number of distinct values "as a radical"—this was just the number of solutions of the minimal polynomial of the radical r over $\mathbf{Q}(a_1, ..., a_5)$.

As we emphasized, Abel realizes that these two numbers must be equal—this was his crucial **Combinatorial Principle** (or else, **Theorem 7**).

Accordingly, the obvious aim now is to show that there aren't enough radicals out of which to build the solution by radicals for $\mathbf{p}_5(x)$ by showing that there aren't enough primes p for which a radical of that order could exist, given that *the two numbers of values are not equal*. Thus, in particular, the obvious aim would be to find *independent* epistemic access to these two numbers for those *specific p* that could otherwise appear in the solution formula, and show that they are not equal. Indeed, it is just such an investigation that Abel's representation of the radicals might be hoped to support.

Given only **Lagrange's theorem**, it seems that we might have to rule out quite a large range of possible orders of radicals. However, Abel knows from the start that the order of the radicals in the solution formula can be taken to be a prime. Thus, *if* we knew that the number of distinct values as a radical of any radicals in the solution formula is equal to its order, we would be justified in focusing on radicals of orders 2, 3, and 5, these being the only prime divisors of the factorial of 5. As we saw in our exposition of Abel's proof, this is not actually quite the case, but Abel does know that this equality will hold for any radicals *over the field of coefficients*. Recall also that by the end of proving **Theorem 2**, Abel knows that the prime p cannot exceed 5, for else there would be too many distinct solutions for $\mathbf{p}_5(x) = 0$. Thus, Abel has a strong reason for thinking that the place to focus on at this stage in the proof is the number of distinct values rational expressions in five independent variables can take, where the number of values is a prime and does not exceed five. Since we are trying to rule out as many radicals as possible, the natural immediate aim is to find further constraints on the number of values.

Result. As it turns out, the tradition of attacks on the solvability of the general equation of degree 5 had made available a result that contributes to just this aim:

Theorem 4 (Ruffini) *A rational function $f(x_1, ..., x_n)$ cannot have* 3 *or* 4 *distinct values under the permutations of the variables for n greater than* 4.

Thus, under the assumption that $f(x_1, ..., x_5)$ has a prime number of distinct values, and that that prime divides 5!, now *there are only two possibilities* : 2 and 5.

Stage 2.1.2 *Aim*. *Find an artifactually determinate expression for a rational function in five variables with* 2 *distinct values*.

This aim is very naturally suggested by Abel's epistemic scaffolding and the overall aim of his epistemic process; thus, this counts as aim guidance.

Result. It turns out that the square root of a quantity known as the *discriminant* of the general polynomial has just this feature:

Theorem 5 *A rational function $f(x_1, ..., x_5)$ in E with exactly two distinct values under the permutations of the variables $x_1, ..., x_5$ is of the form $p + \rho q$, where p and q are symmetric functions in $x_1, ..., x_5$, and ρ^2 is the discriminant of $\mathbf{p}_5(x)$.*

Stage 2.1.3 *Aim. Find an artifactually determinate expression for a rational function in five variables with* 5 *distinct values.*

Result. It turns out that the most obvious thing works:

Theorem 6 *A rational function* $f(x_1, ..., x_5)$ *with five distinct values under the permutations of the variables* $x_1, ..., x_5$ *is of the form*

$$r_0 + r_1 x + r_2 x^2 + r_3 x^3 + r_4 x^4,$$

where $r_0, ..., r_4$ *are symmetric functions of* $x_1, ..., x_5$ *and* x *is one of the* $x_1, ..., x_5$.

As I have already hinted, I regard **Stage 2.1** as Abel's finest hour in his entire proof. Abel has an excellent scaffolding provided by the numerical parametrization and structured by **Theorems 3** and **4**. In virtue of this scaffolding, Abel enjoys good aim and location guidance throughout **Stage 2.1**: he knows just for which *p* he needs to find an explicit expression for the rational functions with *p* values.

In order to assess whether Abel has located and extracted features directly relevant to finding the specific expressions, however, we would have to consider the proofs of **Theorem 5** and **Theorem 6**; see the next section for the latter.

4.4 LOCAL ANALYSIS

4.4.1 Artin's Stage 2.2.3

As its name might well suggest, in many ways **Stage 2.2.3**, the proof of Artin's Lemma, is the heart of Artin's approach. I aim to show that the resources of modern algebra allow us to maintain excellent cognitive control over the epistemic process of reading the standard proof and, indeed, would allow us to maintain good control also over the process of searching for it. To hark back to a theme I introduced in Chapter 3, I hope to show just how 'easy' the proof of even a substantial, crucially important result can be when we have concepts that allow us to properly orient the process from the start.

In my exposition so far, I have ignored a component of Artin's lemma, namely the claim that the fixed field extension E/E^G is *separable*. Since its proof provides a nice illustration of certain techniques characteristic of Artin's approach, I will now bring this additional component into play.

Lemma (Artin) *Let* G *be a group of automorphisms of* E, *and let* F *denote the fixed field* E^G *of* G. *Then*

(*a*) *the fixed field extension* E/F *is normal and separable*, *and*

(*b*) G *is the Galois group* G(E/F) *of this extension*.

In order to make the exposition more efficient, I will present the proof in a way that already makes explicit the kinds of guidance we enjoy in the course of reading it; I will comment on the other components of control once the proof is fully laid out.

(*a*) *Aim. Show that the fixed field extension* E/F *is normal and separable.*

1. *Aim Guidance*. In structural mathematics, and in modern mathematics generally, we typically seek to have multiple logically equivalent articulations of theoretically important properties. The epistemic worth of having such multiple articulations is that it often facilitates finding proofs: where one way of characterizing a property fails to find application, a different one may well fare better. What I hope to illustrate below is that this multiplicity of articulations can be a resource for acquiring epistemic guidance.

Thus, we have multiple articulations of normality and separability:

Lemma 1 *Let* E/F *be a field extension and let* **A** *be an algebraic closure of* F.

The following are equivalent.

(*a*) E/F *is normal: every* F*-homomorphism* E → **A** is *an* ***automorphism*** *of* E;

(*b*) *For all a* in E, E *contains* **all** *the solutions in* **A** *of the minimal polynomial of a*;

(*c*) E *is the splitting field of* ***some*** *polynomial f*(*x*) *in* F[*x*];

(*d*) *If f*(*x*) *is an* ***irreducible*** *polynomial in* F[*x*] *that has at least one root in* E,
then f(*x*) *splits in* E.

This lemma puts us in a position to acquire excellent aim guidance by allowing us to choose the characterization that is appropriate to our current task. Here we are given a field E and group G that specifies the field F; thus, perhaps the most natural thing to try would be to go with (*c*) and construct a polynomial *f*(*x*) that has coefficients stable under the action of G and splits in E[*x*].

Lemma 2 *Let* E/F *be a field extension and let* **A** *be an algebraic closure of* F.

The following are equivalent.

(*a*) E/F *is separable*: *every homomorphism* F → **A** *extends to a homomorphism* E → **A** *in exactly* [E : F] *different ways*;

(*b*) *The number of* F-*automorphisms of* E *is* [E : F]; E; that is, #(G(E/F)) = [E : F];

(*c*) *Every element a of* E *is separable over* F: *a is a solution of some polynomial in* F[*x*], *and if the degree of the minimal polynomial* $\mathbf{m}_a(x)$ *of a over* F *is n*, *then* $\mathbf{m}_a(x)$ *has n distinct* roots in E.

Part (*c*) of **Lemma 2**, along with part (*c*) of **Lemma 1**, strongly suggests that we should pick an arbitrary element a in E and try to construct a polynomial $f(x)$ in F[x] with distinct roots in E such that $f(a) = 0$. For it is an elementary fact, already known to Abel, that the minimal polynomial of a will be a factor of any $f(x)$ such that $f(a) = 0$. Thus, it is trivial that if $f(x)$ has distinct roots in E, then so does the minimal polynomial.

2. *Location Guidance*. If $S = \{s_1, ..., s_n\}$ is any set of elements in E stable under the action of a group G, then the coefficients of the polynomial $(x - s_1)(x - s_2) \dots (x - s_n)$ are symmetric functions of the elements in S and, hence, fixed by the action of G; that is, they are in $F = E^G$ as required. But which set S should we choose? Since it is the group G that is given to us, and since we would like the construction to work for any a in E, there is really just one natural choice: pick any element a in E and let $O(a) = \{a, a_2, \dots, a_r\}$ be the orbit of a under the action of G, with repetitions ignored. Thus, the number of elements r is less than or equal to #(G). Clearly this set is stable under the action of G: all the images of a under the action of G are already in it.

3. *Manipulation Guidance*. We are now more or less done: let us consider the polynomial $f_a(x)$ defined by the elements of O(a):

$$f_a(x) = (x - a_1) \dots (x - a_r) \in \mathrm{E}[x].$$

By construction, this polynomial has all of its roots in E and coefficients in F. For again, the coefficients are symmetric functions in a, a_2, …, a_r and this set is stable under G.
4. *Result*. But $f_a(x)$ is by construction a polynomial in F[x] that *splits* into linear factors $(x - a_j)$ in the ring E[x]; thus, E/F is a normal extension by the characterization (c) of normal extensions.
5. *Result*. The element a of E is by construction a root of $f_a(x)$ and so the minimal polynomial $\mathbf{m}_a(x)$ of a over F divides $f_a(x)$. Thus, since $f_a(x)$ is a product of distinct linear factors in E[x], the minimal polynomial of a over F is also a product of distinct linear factors, and as such, separable. But our choice of a was arbitrary, so this works for any a in E; thus, E/F is a separable extension by the characterization (c) of separable extensions.

The epistemic structure of this proof is so simple that there is a sense in which the components of cognitive control aside from guidance are just about trivial. Indeed, one could justifiably say that the two lemmas set up an inferential scaffolding in the sense discussed in Section 3.6.4. However, we can bring out the epistemic excellence of this proof in a more nuanced way if we take it that the scaffolding is ontic, as follows.

(*a*) *The agent has identified a target range*

The target range is the facts about the effect of automorphisms in G on the elements of E.

(*b*) *The agent has adopted an organizing representation that erects scaffolding*

The organizing representation is the set of all G-*orbits* x_1, ..., x_n of the elements x of E. The locations in the scaffolding are all the sets S in E such that it is epistemically possible that S is stable under the action of G. Given what we know about group actions in general, a set S is stable under G if and only if it is a (disjoint) union of *complete* G-orbits O(a_j) for some elements a_j of E. Thus, the locations are parametrized by the individual elements of E. While this is of course a very thin sense of parametrization, it is nevertheless just the epistemic handle we need on these sets.

(*c*) *The scaffolding provides guidance*

As we saw above, the scaffolding provides us excellent location guidance: the only thing it is even halfway rational to focus on is the G-orbit of an arbitrary element a of E.

(*d*) *The agent can locate and extract features directly relevant to answering the question*

Each of the characterizations in **Lemma 1** marks out a fact directly relevant to inferring that E/F is a normal extension. But in view of the characterization (*c*), we only need to construct a polynomial with coefficients in F that splits in E, and the G-orbit of an arbitrary element a is just the location we needed: the polynomial naturally associated with this location does the trick.

I think it is fair to say that in the first part of the proof, we enjoyed excellent aim, location and manipulation guidance. Now we will see that even though the second part of the proof has a very different character, we enjoy excellent guidance there also.

(*b*) *Aim*. *Show that* G(E/F) = G.

1. *Aim Guidance*. Every automorphism of E contained in G fixes every element in F = E^G by definition, so G is *contained* in G(E/F), the group of all automorphisms of E that fix F. The only issue is that *prima facie* there could be automorphisms of E that are not contained in G but fix F. Thus, we need to show that G is all of G(E/F).

2. *Aim Guidance*. Perhaps the most obvious point to make to start with is that since G is contained in G(E/F), we have #(G) ≤ #(G(E/F)). This strongly suggests that we should show that #(G(E/F)) ≤ #(G), so as to conclude that #(G) = #(G(E/F)).

The other obvious strategy would be to pick an arbitrary element ρ of G(E/F) and show that ρ is in G. However, we do not have an inferentially engageable representation of the arbitrary element in G(E/F), and so this epistemic option is not really open for us to pursue.

Location Guidance. Aside from the cardinalities of the two groups, there is only one other cardinality in view we can engage inferentially, namely the *degree* of the field extension E over F, denoted [E : F]: since E/F is separable, we know by part (*b*) of **Lemma 2** above that #(G(E/F)) = [E : F].

Aim Guidance. Thus, we will try to show that [E : F] ≤ #(G).

3. *Aim Guidance*. We need a way of relating the degree [E : F] to the cardinality #(G).

Now we do know one number in the context of our proof that is at most #(G): the polynomials $f_a(x)$ considered above all have degree at most #(G). Thus, the minimal polynomial over F of any element in E has degree at most #(G). So we need to find an element *c* in E such that either [E : F] ≤ deg($\mathbf{m}_c(x)$) or [E : F] ≤ deg($f_c(x)$).

Location Guidance. It is an elementary property of a finite extension E/F that there is some element b in E, called a *primitive element*, such that E = F(b); that is, the element b generates E as a vector space over F. In particular, the dimension of this space, that is, the degree [E : F], is exactly the degree of the minimal polynomial over F of b.

Result. Thus, we are done: $[E : F] = \deg(\mathbf{m}_b(x)) \leq \#(G)$, as required.

Again, this proof could justifiably be considered to have an inferential scaffolding set up by our lemmas and, indeed, the proof of the first part of the theorem. But let us again consider how we might see this proof also as having an ontic scaffolding.

(1) ***The agent has identified a target range***

We can take the target range to be either the group-theoretic relations of elements of G(E/F) or the arithmetic relations of the elements of E/F.

(2) ***The agent has adopted an organizing representation that erects a scaffolding***

The organizing representation is just the *group of automorphisms G*, conceived as a subgroup of the Galois group G(E/F). It is not actually clear what we could think of as the scaffolding until we come to Step 2: the locations are demarcated by the epistemically possible outcomes of our investigation: $\#(G) < \#(G(E/F))$ and $\#(G) = \#(G(E/F))$. We now need to examine these locations by associating some further numbers with #(G).

(3) ***The scaffolding provides guidance***

I think it is fair to say that the aim, location and manipulation guidance are excellent. Note, in particular, that there are clearly only two possible avenues of inquiry: we could either consider the groups G and G(E/F) directly, or we can revert back to the extension E/F; as it turns out, only the latter option is approachable.

(4) ***The agent can locate and extract features directly relevant to answering the question***

Clearly the fact that $\#G(E/F) = [E : F] < \#(G)$ (along with $\#(G) < \#(G(E/F))$ is highly directly relevant to showing that $G = G(E/F)$. Again, almost too easy.

One might argue that the fact that the cardinality consideration is highly directly relevant to inferring that G is all of $G(E/F)$ shows that my notion does not capture the intuitive idea that features 'directly relevant' to inferring an answer should *explain* that answer. For one might argue that the cardinality consideration does not explain why G is all of $G(E/F)$; the thought is that an explanatory proof should start by considering an arbitrary element ρ of $G(E/F)$ and show that it is in G. I have two things to say about this intuition. First, this is actually just what I want: the whole point of avoiding a metaphysically front-loaded notion of cognitive control is to leave room for the possibility that explanatoriness is a feature of the internal organization of our epistemic process. Having control does not require that one has identified some 'metaphysically privileged' feature of the situation, and it strikes me that the foregoing intuition would have to be understood as being metaphysically grounded in order for it to have any force at all. The idea is something like: the cardinality consideration does not show the 'mechanism' internal to $G(E/F)$ that 'forces' the arbitrary element into G. It is not the task of my notion of cognitive control to try to respect intuitions of this kind. Second, I do not think that the foregoing intuition is correct anyway: the cardinality of G determines the dimension of E over F, and the dimension of E over F governs the cardinality of the Galois group $G(E/F)$. All we are really doing in Step 3 is reminding ourselves just how the field F was constructed in the first place. The degree of the minimum polynomial of a primitive element is just a way of representing the degree of the field extension.

4.4.2 Abel's Stage 2.1.3

Aim. Find an artifactually determinate expression for a rational function v of the roots of $\mathbf{p}_5(x)$ *with 5 distinct values under the permutations of the roots.*

Result. The expression is $r_0 + r_1 x + r_2 x^2 + r_3 x^3 + r_4 x^4$, *where* $r_0, ..., r_4$ *are symmetric functions of the roots* $x_1, ..., x_5$ *and x is one of the* $x_1, ..., x_5$.

This expression is crucial to obtaining some of the final contradictions at **Stage 3**. What makes **Stage 2.1.3** interesting to us, however, is that it is at this stage where Abel comes closest to making statements about the structure of the splitting field E/F of $\mathbf{p}_5(x)$. Indeed, much of the reasoning at this stage consists of making inferential moves wherein Abel is *indirectly responding* to the effect of the action of certain *subgroups* of the Galois group G(E/F) on the generators of the extension E/F, namely the roots of $\mathbf{p}_5(x)$; as we will see, these are just the features that are *directly relevant* to proving the foregoing expression. He does not, however, manage to articulate those features explicitly and, as such, he is not in a position to directly respond to them in his reasoning. Thus, what I hope to argue below is that while Abel has a fairly decent scaffolding and fairly decent guidance in the sense that there is at all times visible to him a determinate range of aims and ways of pursuing them, he does not enjoy very good cognitive control: *he does not have the conceptual resources to locate or extract features directly relevant to proving the foregoing expression*. To be more careful, my claim is that while Abel does indeed enjoy some measure of control here, we enjoy much better control over the modern, conceptually articulated proof.

I take this occasion to emphasize that having cognitive control over an epistemic process is not, so to speak, merely an *internal* affair: it is not enough that one has some kind of a scaffolding and some kind of guidance that steers one towards an answer to the question driving the process. It is an essential part of my characterization of cognitive control that the scaffolding provides aim, location and manipulation guidance, and that in virtue of having such guidance, one is able to locate and extract features of the situation *directly relevant* to answering the question; the more directly relevant the features extracted are, the better one's cognitive control. This is part of the idea that to have cognitive control involves being able to 'see' clearly what the essential features of the mathematical situation are and, in virtue of having that vision, navigate oneself towards an answer to the question.

Abel's proof of the foregoing expression can be naturally divided into two parts; I will call them **Theorem 6*a*** and **Theorem 6**. Let **S** be the set of all permutations of the roots.

Theorem 6*a* *For a given root x_μ of $\mathbf{p}_5(x)$, let $\mathfrak{I}_\mu$ be the set of all permutations of the roots that fix x_μ. If a rational function v of the roots is invariant under the permutations in $\mathfrak{I}_\mu$, then v is a polynomial in x_μ with symmetric coefficients of the roots. Any v of this form either has 5 distinct values under the permutations in* **S**, *or else is symmetric*.

I will give the cleanest proof I can by using Abel's epistemic resources, and then discuss the character of cognitive control we have over the process of reading this proof.

1. Without loss of generality, we may take $x_\mu = x_1$.

2. Suppose that v is invariant under the permutations in $\mathfrak{I}_1$. It is trivial that v is a symmetric function of the roots $x_2, \ldots, x_5$.

3. By the **Main Theorem on Symmetric Functions**, such v can be expressed as a polynomial in x_1 whose coefficients are symmetric functions in the $x_2, \ldots, x_5$. But the latter can be expressed as polynomials in x_1 whose coefficients are symmetric functions in the $x_1, \ldots, x_5$. For example, $x_2 + \ldots + x_4 = a_1 - x_1$; one would explicitly verify the other cases in the same manner. This proves the first part of the claim.

4. Suppose that $v = v(x_1)$ is a polynomial in x_1 whose coefficients are symmetric functions in the $x_1, \ldots, x_5$.

5. Suppose that $v(x_1)$ has fewer than five distinct values under the permutations in **S**, and let $v(x_1), ..., v(x_5)$ be these values; that is, the $v(x_1), ..., v(x_5)$ only differ in that the variable is different in each.

6. Since there are fewer than 5 distinct values, we have $v(x_1) = v(x_m)$ for some m, and so, without loss of generality, we may suppose that $v(x_2) = v(x_1)$.

7. Now apply the four *transpositions* (x_2, x_μ) in **S** that exchange (x_2, x_μ), $\mu = 2, ..., 5$, to $v(x_1)$. Since these transpositions do not affect x_1 and since the coefficients are symmetric, we obtain $v(x_2) = v(x_1) = v(x_3) = v(x_4) = v(x_5)$. That is, v is symmetric.

Not too bad, you will think. Certainly it seems fair to say that Abel has identified a target range, namely facts about the possible values of polynomials in the five roots under the permutations in **S**; the proof can be thought of as a small-scale investigation of certain aspects of this set of facts; any expression that picks out these facts may be considered an organizing representation. Step 2 can be regarded as erecting scaffolding for the first part, and Step 5 for the second; the scaffolding for the first part is structured by the **Main Theorem of Symmetric Functions** and the known expressions for the elementary symmetric functions; the one for the second is structured simply by the fact that $v(x_1) = v(x_m)$ for some m. And certainly there is guidance: the aim at each step is perfectly clear, and that there is little doubt about what location one should examine. As for manipulation guidance, the only even remotely non-trivial move is to apply the transpositions at Step 7, but then again, given that our aim is to show that $v(x_1) = v(x_2) = v(x_3) = v(x_4) = v(x_5)$, even this should seem like the only real option.

Thus, my first conclusion is that we enjoy cognitive control over the process of reading the foregoing proof and, indeed, over the process of finding that a proof. But how good is this control? Let us now consider the modern proof of **Theorem 6*a***:

By the **Main Theorem of Galois Theory**, $\mathrm{G}(\mathrm{E}/\mathrm{F}(x_\mu)) = \Im_\mu$ and hence, $\mathrm{K}(x_\mu) = \mathrm{K}[x_\mu]$ is the fixed field of $\Im_\mu$. The elements of $\mathrm{K}[x_\mu]$ have the required form by definition.

While the Abel-style proof was not too bad, the difference is still pretty striking. Now clearly we must moderate our reaction somewhat: after all, the modern proof depends on our having available to us the **Main Theorem**, a highly non-trivial result; it is not as if the modern proof is acquired just by introducing the field- and group-theoretic concepts. Yet, perhaps the comparison here is not entirely inapt. For the epistemic location in Abel's process where **Theorem 6*a*** and **Theorem 6** are proved corresponds, in a way that I have labored to make explicit, to the epistemic location in Artin's process where the **Main Theorem** has just become available. In any case, we can always imagine the proof of the latter inserted into the proof of **Theorem 6*a***. What results is a longer proof but, as I have tried argue, one over which we enjoy excellent control.

Let us now consider the second part of **Stage 2.1.3**.

Theorem 6 *A rational function $v = f(x_1, ..., x_5)$ in* E *with exactly five distinct values under the permutations of the variables $x_1, ..., x_5$ is of the form*

$$r_0 + r_1 x + r_2 x^2 + r_3 x^3 + r_4 x^4,$$

where $r_0, ..., r_4$ are symmetric functions of $x_1, ..., x_5$ and x is one of the $x_1, ..., x_5$.

The following proof is adopted from Radloff's discussion; Abel's original proof is a great deal messier, involving as it does a number of lengthy symbolic computations. I suppose that the verdict regarding the quality of control in that proof would be less charitable than the one for this one will be. Recall, however, that our object of interest here is not what this or that particular individual has in fact accomplished, but rather, what can in principle be accomplished with a given set of epistemic resources. Thus, we should always look for the best available proof and I think that the following is it for Abel's resources.

Proof. Let $v_1, ..., v_5 \in$ E be the five distinct conjugates of $v = v_1$, and let $v_1, ..., v_\eta$ be the conjugates of v_1 one obtains by applying all the permutations in **S** that fix x_1, call it $\mathfrak{I}_1$. Then the expression

$$v_1 + v_2 + ... + v_\eta \qquad (*)$$

is clearly invariant under the permutations in $\Im_1$, since $\Im_1$ just permutes the $v_1, ..., v_\eta$ among themselves. So we can apply **Theorem 6*a*** which says that any such expression is a polynomial in x_1 with symmetric coefficients, which is what we want; call this expression $\varphi(x_1)$. So we want to show that v itself has this form. The proof now proceeds by considering each of the five options one at a time.

$\eta = 1$. In this case, $v_1 = \varphi(x_1)$, as required.

$\eta = 2$. Abel rules out this case by solving a system of equations by considering a large number of subcases. But, as Radloff observes, "this case can also be handled more easily by using Abel's own methods."[36] To begin with, there is at least one permutation S in **S** of order 5, so that after suitably renaming them,

$$v_1, \quad v_2 = \mathrm{S}v_1, \quad v_3 = \mathrm{S}^2v_1, \quad v_4 = \mathrm{S}^3v_1, \quad v_5 = \mathrm{S}^4v_1$$

are precisely the 5 distinct conjugates of v_1, for otherwise it would follow as in the proof of **Theorem 3**, that v_1 is either alternating or symmetric.

Now Abel knows from Cauchy that such a permutation S is 5-cycle. Hence, one can show that $x_{\nu+1} = \mathrm{S}^\nu x_1$, for $\nu = 1, ..., 4$. By applying S to each side of (*) in the present case, $\eta = 2$, one obtains

$$v_1 + v_2 = \varphi(x_1)$$

[36] See Radloff [1998], p. 137.

$$v_2 + v_3 = \varphi(x_2)$$

$$v_3 + v_4 = \varphi(x_3)$$

$$v_4 + v_5 = \varphi(x_4)$$

$$v_5 + v_1 = \varphi(x_5).$$

That is, at each step S pushes all indexes up by 1, at 5 “wrapping around” back to 1.

Keeping in mind that we are looking for an expression for v_1, we may eliminate v_2, ..., v_5 in this system, so as to obtain

$$v_1 = \Sigma - \varphi(x_2) - \varphi(x_4), \qquad (**)$$

where 2Σ = sum over all $\varphi(x_v)$. As a symmetric function, Σ is in K, the field of coefficients of $\mathbf{p}_5(x)$. The right-hand side must have two values.

Now $\varphi(x_2)$ cannot be symmetric, for then $\varphi(x_4)$ would also be symmetric and hence, finally, v_1, which is by assumption not the case. But, according to **Theorem 6*a***, an expression like $\varphi(x_2)$ is either symmetric or has 5 conjugates, and so the latter is the case.

By applying a suitable transposition, one shows that the right-hand side of (**) would have to have more than two conjugates under the permutations from $\Im_1$. However, in this case the left-hand side is assumed to have precisely 2 conjugates under the action of the group $\Im_1$. Hence, $\eta = 2$ does not occur.

$\eta = 3$. In this case $\varphi(x_1) + v_4 + v_5 = v_1 + v_2 + ... + v_4 + v_5$ is symmetric since these just are all the distinct conjugates of v_1. Thus, $\varphi(x_1) + v_4 + v_5 = b$ for some constant in K, so that $v_4 + v_5 = b - \varphi(x_1)$ is a polynomial in x_1 with symmetric coefficients, call it $\psi(x_1)$. Now replacing v_4 with v_1 and v_5 with v_2, one obtains a contradiction in a manner analogous with case 2.

$\eta = 4$. In this case, we are 'close enough' to having the right kind of expression for v_1 that we can just "manufacture" it. For $\varphi(x_1) + v_5 = v_1 + v_2 + ... + v_4 + v_5$ is symmetric since these just are all the distinct conjugates of v_1. Thus $\varphi(x_1) + v_5 = b$ for some constant b in K, so that $v_5 = b - \varphi(x_1)$ is a polynomial in x_1 with symmetric coefficients. Finally, we get the required expression for v_1 by applying any permutation S that takes v_5 to v_1 to both sides of this equation, so that $v_1 = b - \varphi(\mathrm{S}x_1)$. That is, the only thing that changes on the right is the particular variable, the symmetric coefficients remaining the same.

5. $\eta = 5$. Pick m large enough so that none of the polynomials $v_1, ..., v_5$ is divisible by the powers $x_1^m, ..., x_5^m$. The polynomial $x_1^m v_1 \in$ E can have at most 25 distinct conjugates. Given that $\eta = 5$, if one applies all the permutations from $\Im_1$ on $x_1^m v_1$, one obtains the polynomials

$$x_1^m v_1, \quad x_1^m v_2, \quad x_1^m v_3, \quad x_1^m v_4, \quad x_1^m v_5.$$

If one now applies to these polynomials the five transpositions $\mathrm{T}_\mu = (x_1, x_\mu)$ for $\mu = 1, ..., 5$, given the bijectivity of T_μ, one obtains the 25 polynomials $\mathrm{x}_\mu^m v_\nu$, with $\nu = 1, ..., 5$, which, given the choice of m, are pairwise distinct. Thus $x_1^m v_1$ has 25 distinct conjugates, which is impossible by **Theorem 2**. So, $\eta = 5$ cannot occur.

So that hurt a little bit more, but it should be intuitively clear by now that we can make Abel out as having a perfectly respectable target range, organizing representation, scaffolding and, indeed, perfectly respectable guidance. Here one could obviously make the case that there are lapses in his manipulation guidance, but aim guidance seems to be as tight as ever: the numerically parametrized epistemic scaffolding leaves little uncertainty as to which tasks need to be carried out in order to prove the result. Indeed, Abel's proof typifies nicely the sort of scaffoldings and guidance we tend to enjoy in 19th century mathematics: we have a parametrized space of locations, one we know to be completely represented by the parametrization, and we proceed to examine each of the epistemic locations individually; thus, the scaffolding provides us location guidance. As it often happens, there is no uniform method for treating all or even most of the options, although there may indeed be some overlap in the methods required by the various cases. This is precisely what we see here. Note, indeed, that much as in **Stage 3**, the locations are not connected, and need to be examined individually.

But let us again consider the modern proof:

If $n \neq 6$, the n inertia groups $\Im_\mu$ of the n solutions are the only subgroups of S_n of index n. From the **Main Theorem of Galois Theory** it follows that if $n \neq 6$, the n fields $K(x_\mu)$ are the only extension fields of K of degree n. Thus, $K(v) = K(x_\mu)$.

Again, while Abel maintains fairly good cognitive control 'internally' in his process, the modern proof helps us see just how far he really is from getting at features directly relevant to proving the desired expression. What is more, it seems pretty certain that without the Galois correspondence or, at any rate, without the group- and field-theoretic concepts, it is simply not possible to be more directly responsive to features more directly relevant than Abel is—his proof is as good as it gets without the modern resources.

Analysis

I want to argue is that the resources of Artin's approach allow us to extract high-level features of the splitting field extension E/F that are much more directly relevant to proving the two theorems than what the resources of Abel's approach allow.

The modern proof of **Theorem 6*a*** turned on the following two high-level features of the extension E/F:

(1) *There is a bijective correspondence between subgroups of* G(E/F) *and the intermediate fields of* E/F;

(2) $G(E/F(x_\mu)) = \mathfrak{I}_\mu$.

These are excellent examples of high-level features of the splitting field extension E/F. Again, I am taking it that since the Galois group G(E/F) is the group of F-automorphisms of E, ultimately the facts about the identity and relations of the elements in this group can be viewed as high-level features of the organization of the extension E/F itself; for the identity and relations of the automorphisms in G(E/F) are governed by the identity and relations of the elements in E/F. Nothing really depends on this, however: we could just as well talk about high-level features of the extension E/F *and* high-level features of its Galois group G(E/F).

The modern proof of **Theorem 6** turned on the following two high-level features of the extension E/F:

(1) *There is a bijective correspondence between the subgroups of* G(E/F) *and the intermediate fields of* E/F;

(2) *The only subgroups of* G(E/F) *of index* 5 *are the inertia groups* $\mathfrak{I}_\mu$ *of the* $x_1, \ldots, x_5$.

In each case, the conclusion can be inferred directly from the two facts noted.

Let us compare the two proofs of the first part of **Theorem 6*a***:

Abel

1. Without loss of generality, we may take $x_\mu = x_1$.

2. Suppose that v is invariant under the permutations in $\Im_1$. It is trivial that v is symmetric function of the roots $x_2, \ldots, x_5$.

3. By the **Main Theorem on Symmetric Functions**, such v can be expressed as a polynomial in x_1 whose coefficients are symmetric functions in the $x_2, \ldots, x_5$.

4. But the latter can be expressed as polynomials in x_1 whose coefficients are symmetric functions in the $x_1, \ldots, x_5$. For example, $x_2 + \ldots + x_4 = a_1 - x_1$; one would explicitly verify the other cases in the same manner.

Artin

1. There is a bijective correspondence between the subgroups of G(E/F) and the intermediate fields of E/F by the **Main Theorem of Galois Theory**.

2. It is immediate from the definitions that $G(E/F(x_\mu)) = \Im_\mu$.

3. By (1) and (2), it follows at once that $F(x_\mu)$ is the unique fixed field of $\Im_\mu$ in E.

4. By definition, any element of E that is invariant under all the automorphisms in $\Im_\mu$ is in the fixed field of $\Im_\mu$, namely $F(x_\mu)$.

5. But the elements of the field $F(x_\mu)$ are, by definition, polynomials in the root x_μ with coefficients in F.

I think the most immediate intuition here is that the modern proof identifies the *proper context* for thinking about the rational functions under consideration: with the conceptual resources of Artin's approach in hand, we can 'see' 'what' they 'really' are—they are just the elements in the fixed field of the inertia group $\mathfrak{I}_{\mu}$; after this, the result is immediate. In particular, it is striking that no symbolic computations are required.

Thus, the high-level feature most directly relevant here is the fact that $F(x_{\mu})$ is the unique fixed field of $\mathfrak{I}_{\mu}$ in E. Once this fact is established, the rest of the proof consists of two trivial applications of the definitions constitutive of Artin's approach. This crucial fact, in turn, is a direct consequence of the **Main Theorem** and the definition of Galois group. Thus, we may now say, the 'point' is not that there are certain relations between the symmetric functions (noted in Step 4 in Abel's proof), but the fact that any v in E with the stipulated property is in the fixed field of the group $\mathfrak{I}_{\mu}$.

Let us now compare the two proofs of the second part of **Theorem 6*a***:

Abel

4. Suppose that $v = v(x_1)$ is a polynomial in x_1 whose coefficients are symmetric functions in the $x_1, \ldots, x_5$.

5. Suppose that $v(x_1)$ has fewer than five distinct values under the permutations in **S**, and let $v(x_1), \ldots, v(x_5)$ be these values; that is, the $v(x_1), \ldots, v(x_5)$ only differ in that the variable is different in each.

6. Since there are fewer than 5 distinct values, we have $v(x_1) = v(x_m)$ for some m, and so, without loss of generality, we may suppose that $v(x_2) = v(x_1)$.

7. Now apply the four *transpositions* (x_2, x_μ) in **S** that exchange (x_2, x_μ), $\mu = 2, ..., 5$, to $v(x_1)$. Since these transpositions do not affect x_1 and since the coefficients are symmetric, we obtain $v(x_2) = v(x_1) = v(x_3) = v(x_4) = v(x_5)$. That is, v is symmetric.

Artin

6. Any element v of E of this form belongs to the field $F(x_\mu)$. There are two options only: if the element v is in F, it is (by definition) fixed by G(E/F); if the element v is not in F, the root x_μ appears in it and hence, it has 5 distinct conjugates under the action of G(E/F).

The same remarks can be made about the difference between the second parts of the proofs as about the first: the 'point' is not that the transpositions have a certain effect on v but rather that the structure of the extension E/F has certain high-level features. The essential features here are that any element v of E of the required form is in the field $F(x_\mu)$ and that we know how the Galois group acts on this field: the images of any one root are just the other roots; this determines how the Galois group acts on any element of $F(x_\mu)$.

Let us now compare the two proofs of **Theorem 6**.

Abel

1. Let $v_1, ..., v_5 \in$ E be the five distinct conjugates of $v = v_1$, and let $v_1, ..., v_\eta$ be the conjugates of v_1 one obtains by applying all the permutations in **S** that fix x_1, call it $\mathfrak{I}_1$. Then the expression

$$v_1 + v_2 + ... + v_\eta \qquad (*)$$

is clearly invariant under the permutations in $\mathfrak{I}_1$, since $\mathfrak{I}_1$ just permutes the $v_1, ..., v_\eta$ among themselves. So we can apply **Theorem 6*a*** which says that any such expression is a polynomial in x_1 with symmetric coefficients, which is what we want; call this expression $\varphi(x_1)$. So we want to show that v itself has this form.

2. The proof now proceeds by considering each of the five options one at a time. Some of the options lead to a contradiction, in others we can show that v has the required form.

Artin

1. The Galois group G(E/F) is the symmetric group $\mathbf{S}_5$ on five letters.

2. The five inertia groups $\mathfrak{I}_\mu$ of the five solutions are the only subgroups of $\mathbf{S}_5$ of index 5.

3. By the **Main Theorem of Galois Theory** it follows at once that the 5 fields $F(x_\mu)$ are the only extension fields of F of degree 5.

4. It is (just about) immediate from the definitions that any element v in E with five distinct conjugates generates an extension field $F(v)$ of F of degree 5.

5. Thus, $F(v) = F(x_\mu)$ for some x_μ. Hence, any v with five distinct conjugates can be expressed as a polynomial in x_μ with coefficients in F, as required.

Here the intuitions felt already in the case of **Theorem 6*a*** are even stronger: Abel does not manage to extract any feature that would be as directly relevant to inferring the required expression as the one in which Artin's proof culminates, namely the fact that $F(v) = F(x_\mu)$. Here we see very concretely what kind of a difference the availability of the field- and group-theoretic concepts makes: we just cannot articulate the said essential fact, never mind prove it, without those concepts; hence, we are forced to consider each of the individual possibilities for the 'explicit' expression for v the way Abel does. Given that my definition of directness of relevance was tailored to accommodate this very example, this is just the verdict it yields.

Comments

(1) Note that it is irrelevant from the point of view of my analysis that we would have to carry out further group-theoretic arguments, ones involving symbolic computations, in order to establish the claim in Artin's Step 2. The point is that there is a way to 'summarize' the result of those arguments in a way that can be fed directly into the conceptual framework of the proof as a whole.

(2) While I cannot argue for this here, I think it is clear that the differences we have seen between the two proofs of **Theorem 6*a*** and **Theorem 6** are just the sort of differences mathematicians would regard as differences in the degree to which the proofs 'get at' the 'essential' features of the mathematical situation.

4.5 SUMMARY

We have seen that Artin's resources allow him to maintain excellent cognitive control at all three levels on which we have considered his proof, including the local level. We have seen that there are five basic types of failures in the control Abel's resources allow over his proof. First, it is not clear whether Abel has actually managed to identify a target range for the process as a whole. Second, Abel's conceptual resources do not, for the most part, allow him to adopt a proper organizing representation in the sense required by my definition; hence, the representations that play the role of epistemic scaffoldings are not erected around organizing representations. Third, Abel's epistemic scaffolding in **Stage 3** is much less connected than Artin's. Fourth, there is little manipulation guidance, particularly when the proof is considered at the local level. Finally, Abel is much less successful than Artin in extracting features directly relevant to the aims that arise in the course of his process, most strikingly including the aim of the proof as a whole.

Nevertheless, Abel's control over his proof of the unsolvability of the quintic is hardly a total failure. We would do well to remind ourselves, accordingly, that Abel's epistemic resources do not afford him control over any of the processes that one might naturally want to pursue in this same vicinity. One obvious failure of this kind is that Abel has nothing to say about the solvability of special polynomials—his resources are simply not suited to reasoning about their solvability at all. It is a consequence of this that he has nothing to say about the various geometrical construction problems that Galois can address quite easily. And, of course, if we allow ourselves to look beyond issues having directly to do with polynomials and solvability, it is clear that the resources in Artin’s approach afford us control over vast stretches of theory whereas Abel’s resources really only provide control over the one proof we have examined here.

5.0 CONCLUSION

I started with the idea that there is a substantial analytical challenge pertaining to the character of modern mathematics: to explicate just what the remarkable success of modern mathematics as a science consists in. I contended that we do not currently have the philosophical resources for tackling this challenge; in particular, it does not seem realistic to think that this success could consist simply in the acquisition of more mathematical knowledge. I took it that the best way to come up with such resources is to conduct mathematical case studies. Since mathematicians feel that 20th century mathematics has been much more successful as a science than 19th century mathematics, the obvious strategy was to compare two *prima facie* successful approaches to the same mathematical problem: one approach characteristic of 20th century mathematics, another characteristic of 19th century mathematics. If both approaches can solve the problem, we can set aside the issue of acquiring more knowledge, and hope to be able to isolate other features of the 20th century approach that render it epistemically superior to the 19th century one.

In my case study, I compared two approaches to what used to be a central problem in one of the central areas of mathematics, the solvability of polynomial equations by radicals; the 19th century approach was due to Abel, the 20th century one to Artin. The resources in each approach allowed us to prove that there is no general formula for a solution by radicals for equations of degree 5 or higher. I broke each proof down to three stages. The principal task of the first stage in each one was to identify a general criterion for solvability by radicals; that of the second was to develop theoretical tools for determining whether a given general polynomial satisfies that criterion; and, finally, the principal task of the third stage was to employ those tools to show that the general equation of degree 5 does not satisfy the criterion for solvability by radicals.

My analysis of the epistemic difference between the two proofs began by distinguishing epistemic resources and epistemic processes. Agent's epistemic resources were the ambient background of concepts, methods of acquiring knowledge, and bits of knowledge with which she will pursue particular epistemic aims. An epistemic process, then, was a sequence of applying those resources in order to pursue some such aim. The two paradigmatic types of epistemic processes in mathematics were, of course, searching for a proof of a putative theorem and reading a proof of an established theorem. The basic idea was that the character of one's epistemic standing with respect to an epistemic process depends on the epistemic resources one has at the outset of the process and, indeed, on the resources one manages to acquire in the course of that process.

My basic suggestion was that there is a particular kind of epistemic standing that deserves to be singled out in our philosophical analysis of the nature of the scientific success of modern mathematics: cognitive control. I motivated my characterization of cognitive control by noting that there are three basic types of epistemic challenges we need to be able to negotiate in typical mathematical epistemic processes: identify a terrain of facts to be examined, find a theoretically productive way of representing that terrain, and examine the appropriate locations in that terrain so as to extract features thereof that are directly relevant to answering the question driving the process. The basic idea was that, depending on one's epistemic resources, one may or may not be able to negotiate these challenges in a *rationally orchestrated* manner.

Thus, I proposed a characterization of cognitive control that comprised four interrelated components: an agent has cognitive control over an epistemic process to the extent to which she has managed to *identify a target range*, construct an *organizing representation* of her target range, erect an *epistemic scaffolding* for representing epistemically possible facts in that range; and the extent to which, in virtue of having those representations, she enjoys *aim*, *location*, and *manipulation guidance* in the course of *locating* and *extracting* features of the target range that are *directly relevant* to answering her question. I emphasized that when an agent has cognitive control, her epistemic standing has two central features: on the one hand, she can start with a panoptic overview of the epistemic terrain relevant to her aim and, given that overview, she is able to gradually home in on the appropriate features of that terrain. On the other hand, she is able to approach the question driving the process in an organized manner: she has a determinate scaffolding of facts into which she can plug further facts as they are discovered, and in virtue of that scaffolding, she enjoys guidance at each stage in the process.

I emphasized, further, that when an agent has cognitive control, she achieves the epistemic accomplishment required by each of the four components, at least in part, in virtue of having achieved the accomplishments required by the earlier components in the characterization; thus, the four components constitute a cumulative sequence. I argued, indeed, that even though the components are heterogeneous among themselves, they constitute a unitary kind of epistemic standing with respect to the epistemic process.

I went on to discuss the four components of cognitive control in the context of our mathematical case study. I argued that each one allows us to capture an important aspect of the pre-theoretically felt difference in the epistemic power of the two approaches to solvability by radicals. I argued, in particular, that we enjoy significantly better cognitive control over the process of reading Artin's proof of the unsolvability of the quintic than we do over the process of reading Abel's proof.

The two most significant differences between the processes of Abel and Artin turned out to be, first, that Artin can construct a more theoretically useful organizing representation and more theoretically useful epistemic scaffolding for his proof overall, the third stage in particular, and, second, that Artin is much more successful in locating and extracting features directly relevant to addressing the issue of solvability by radicals. As our pre-philosophical intuitions would have us expect, these differences stem from the fact that Artin has available to him a much richer stock of concepts than Abel. In particular, we saw that the modern field- and group-theoretic concepts played a central role in making possible the acquisition of cognitive control in Artin's epistemic process. Abel, in contrast, was forced to work mostly with explicit symbolic expressions for things like roots of polynomials and, in particular, rational functions of the roots of the general polynomial of degree 5. The principal failures of cognitive control in Abel's process can be traced back to the fact that there are certain ranges of facts and objects of which he simply cannot construct conceptually constituted representations. Thus, we found that he is often forced to respond to theoretically crucial facts indirectly, whereas Artin is able to articulate those facts explicitly and respond to them directly.

We saw, nevertheless, that the resources of Abel's approach make it possible to enjoy fairly good cognitive control over the process of reading his proof. Thus, we noted on a number of occasions that Artin's resources make it possible to acquire excellent cognitive control over wide ranges of mathematical epistemic processes, whereas Abel's resources do not.

It seems very likely that it would not be possible to characterize the difference in the epistemic standing we enjoy over the two proofs without *some* notion like cognitive control. For it is hard to see how we could characterize the epistemic accomplishments that mark the two approaches apart without appealing to something like target ranges, organizing representations, epistemic scaffoldings, guidance, and directness of relevance. What makes Artin's approach epistemically superior to Abel's is not *just* that he has more and more 'appropriate' concepts than Abel; it is not *just* that he is able to construct representations of more and more 'relevant' ranges of facts and objects; it is not *just* that he is in a better position to make rational decisions about how to proceed at each stage in the epistemic process; I think that the analysis of our case study shows as much. Further, it is hard to see how we could properly characterize the epistemic superiority of Artin's approach without recognizing that the accomplishments that constitute his proof are related in an intimate way. Indeed, what makes Artin's epistemic standing superior to Abel's is not *just* that he has all the various individual components of cognitive control in play. The superiority of his epistemic standing consists, first and foremost, in the circumstance that his epistemic resources, especially conceptual resources, allow him to *orient* his epistemic process from the start in such a way that the process as a whole constitutes an organic progression in which the components of cognitive control emerge each in its appropriate time and place from the ones preceding it.

I would like to suggest that we can apply the theoretical tools developed in this essay to analyze the epistemic accomplishments of modern mathematics quite generally. Of course I am not in a position to argue for this here, but further case studies strongly suggest that the epistemic significance of many of the principal accomplishments of modern mathematics is that they make it possible to acquire and maintain cognitive control over wide ranges of epistemic processes.

The project of this essay has been to propose an analysis of what the epistemic success of modern mathematics *consists in*. There is now an obvious sequel to this project: we would like to identify some of the principal *types* of epistemic resources that make improvements in cognitive control possible, and a philosophically illuminating *explanation* of how they do it. We have seen that a central part of this further project will have to be a diagnosis of the cognitive contribution of mathematical *concepts*. This is hardly surprising: perhaps the most common pre-theoretical intuition about modern mathematics is that its epistemic power derives, somehow or other, from the power of its concepts. Now one of the central features of much of modern mathematics is the pervasive employment of concepts of *relational structures* and of *morphisms* between such structures. I have not had the occasion to explore this theme here, but it seems to me that this emphasis on structure makes deep and wide-ranging contributions to the availability of cognitive control in mathematical reasoning. Thus, in future work I intend to focus on the contributions concepts of relational structures, and concepts associated with them, make to the availability of cognitive control.

The principal intra-theoretical challenge for my future work will be to refine the characterizations of the individual components of cognitive control. It seems to me that *target range*, *organizing representation* and *scaffolding* are about right; it seems likely that *guidance* is about right, though no doubt more work is needed here as well. Thus, *extracting features directly relevant* and *directness of relevance* itself seem to be the ones most in need of refinement. This refinement will have to involve a careful analysis of the notion of *high-level feature* of a range of mathematical facts. For the contribution of concepts of relational structures often appears to be that they make it possible to articulate epistemically crucial high-level features of our target ranges. Hence, an analysis of the notion of high-level feature, and an explanation of how concepts of relational structures make high-level features cognitively available to us, will both be central to understanding the epistemic contributions of the structural concepts and, as such, the epistemic power of modern mathematics.

APPENDIX A

DEFINITIONS OF GROUP, RING, FIELD AND VECTOR SPACE

Definition *A group* (G, ×) *is a nonempty set* G, *together with a binary operation* × *on* G, *which satisfies the following conditions*:

(1) (*Associativity*) *For any* x, y, z *in* G, $x \times (y \times z) = (x \times y) \times z$.

(2) (*Identity*) *There is an element* e *in* G *such that* $x \times e = e \times x = x$ *for all* x *in* G.

(3) (*Inverses*) *For any* x *in* G, *there is* y *in* G *such that* $x \times y = y \times x = e$.

Definition *An abelian group* (A, +) *is a group such that for any* x, y *in* A, $x + y = y + x$.

Definition *A ring* (R, +, ×) *is a nonempty set* R, *together with binary operations* + *and* ×, *which satisfy the following conditions*:

(1) (R, +) *is an abelian group*.

(2) *The operation* × *is associative*.

(3) *There is an element* e *in* R *such that* $s \times e = e \times s = s$ *for all* s *in* R.

(4) *The operation* × *distributes over* +; *for any* r, s, t *in* R,

$$r \times (s + t) = (r \times s) + (r \times t) \text{ and } (s + t) \times r = (s \times r) + (t \times r)$$

Definition *A field is a ring* (F, +, ×) *that satisfies the following conditions*:

(1) *For any* r, s *in* F, $r \times s = s \times r$.

(2) *For any* s *in* F *with* $s \neq 0$, *there is an element* t *in* F *such that* $s \times t = t \times s = e$, *where* $t \neq 0$, *and* 0 *is the identity element for* + *in* F.

Definition *A vector space* V *over a field* K *is an abelian group*, *together with a map*

$$(x, v) \rightarrow xv$$

of K × V → V *which satisfies the following conditions*:

(1) *If* e *is the identity element for* × *in* K, *then* $ev = v$ *for all* v *in* V.

(2) *For any* c *in* K *and* v, w *in* V, $c(v + w) = cv + cw$.

(3) *For any* x, y *in* K *and* v *in* V, $(x + y)v = xv + yv$.

(4) *For any* x, y *in* K *and* v *in* V, $(x \times y)v = x(yv)$.

APPENDIX B

TRANSLATION OF RADLOFF [1998]

ABEL'S IMPOSSIBILITY PROOF IN LIGHT OF MODERN GALOIS THEORY

Ivo Radloff
Bayreuth

In 1826 N. H. Abel published *Proof of the Impossibility of an Algebraic Solution of the General Equation Whose Degree is Greater than Four* in the first volume of Crelle's Journal. He begins with the words

> ...if I am not mistaken, then the question: *Is it possible in general to solve equations whose degree is greater than four*, has not yet been answered in a fully satisfactory manner. The aim of this treatise is to settle this question.

Up until now there has been no discussion in the literature as to whether Abel's proof, which Gauss called "an atrocity," is in fact conclusive.

In the following paper, we shall reformulate Abel's proof, which is nowadays understood only with a great difficulty, in modern terminology on the one hand, and reconstruct his heavily computational way of proceeding in the context of modern Galois theory on the other. In the end we will be able to determine whether Abel's proof is correct with its mode of presentation taken into consideration.

I

Abel called the first section "*Concerning the General Form of Algebraic Functions*." Here he is dealing with elementary properties of ring and field extensions of **Q**. Abel begins with the fact that **C** is algebraically closed, which Gauss had proved in his 1799 doctoral dissertation, without further comment.

In what follows, let K be an extension field of **Q**. Given a solution r of the equation

$$x^p - \mathrm{A},$$

Abel gives a proof analogous to the modern one of the fact that each v in K(r) can be written in the form

$$v = q_0 + q_1\, r + \ldots + q_{p-1}\, r^{p-1} \qquad (1)$$

for some q_0, …, q^{p-1} in K—that is, K[r] = K(r). He later goes on to note the consequence that each v in K(r) – K can be written in the form

$$v = q_0 + r + \ldots + q_{p-1}.r^{p-1} \qquad (2)$$

That is, one can take $q_1 = 1$. If v is not in K, then at least one q_μ with $0 < \mu < p$ in (1) is nonzero. One only needs to define $r' = q_\mu\, r^\mu$, so we have K[r] = K[r'], and r' is a zero of the equation $x^p - q_\mu^{\,p}\, \mathrm{A}^\mu$ in K[x]. A simple calculation shows that v itself can in fact be expressed as in (2).

II

The most important part of this section, called *Properties of Algebraic Functions that satisfy a given equation*, is **Theorem 1**.

In the opening of *A Treatise on…* ([2], pp. 29-54), Abel defines the concept *irreducible equation* over a given field K and proves the well-known fact that

> *if a polynomial is irreducible over a given K and has a common solution with a polynomial in* K[x], *then it is a factor of that polynomial*.

It follows that each polynomial in K[x] can be expressed uniquely as a product of finitely many irreducible factors. While Abel does not state either of these facts explicitly here, he uses them in several places.

Proposition 1 *If* K *contains any primitive p-th root of unity* (*and hence all*), *then the equation*

$$x^p - \mathrm{A} \in \mathrm{K}[x] \qquad (3)$$

is either irreducible over K, *or else all of its roots lie in* K.

Proof. Suppose that r is a solution of (3) that does not lie in K. Let $m(x)$ in K[x] be the minimal polynomial of r over K, of degree μ, so that $0 < \mu < p + 1$ and

$$m(x) \text{ divides } x^p - \mathrm{A}. \qquad (4)$$

Since r is not in K, $\mu > 1$; hence, there is another root of (3) that is a solution of $m(x)$. Each such root is known to be of the form αr, with α a *primitive p-th root of unity* in K. But if r and αr are both solutions of $m(x)$, then the polynomial

$$m(\alpha x) - \alpha^{\mu} m(x) \in \mathrm{K}[x]$$

of degree $\mu - 1$ has r as a solution and hence, given the irreducibility of $m(x)$, must be the zero polynomial (because of degree considerations). Thus, $m(0) - \alpha^{\mu}m(0) = 0$. But since $m(x)$ is irreducible over K, $m(0)$ must be different from zero, so that $\alpha^{\mu} = 1$. But this is not the case for $\mu < p$. Thus we have $\mu = p$ and (3) is the minimal polynomial of r over K. **QED**

> "*If a polynomial equation is algebraically solvable, then one can always express the solution in such a form that all the algebraic functions, out of which it is composed, can be expressed as rational functions of the solutions of the given equation.*"

Theorem 1 *Let* L *be a radical extension of* K*, so that* K *contains a primitive root of unity from* L/K *for each exponent.*[37] *If* $f(x)$ *is a polynomial in* K[x] *whose splitting field* E *is contained in* L*, then* E *itself is a radical extension of* K.

Proof. The splitting field E of $f(x)$ is contained in the radical extension L/K, so that

$$K = K_0 \subset K_1 \subset ... \subset K_{\eta - 1} \subset K_\eta = L \quad (5)$$

and each $K_{\mu+1}$, $\mu = 0, ..., \eta - 1$ is obtained by adjoining to K_μ a root r_μ of the polynomial

$$x\text{^}(p_\mu) - A_\mu \in K_\mu[x], \qquad (6)$$

with r_μ not in K_μ for some prime p_μ. By assumption, each polynomial in (6) is irreducible over K_μ. Abel now shows that for any μ, $E \cap K_{\mu+1}$ is a radical extension of $E \cap K_\mu$ of degree p_μ, or else is equal to $E \cap K_\mu$:

In case the two fields are not equal, pick any v in $E \cap K_{\mu+1}$ that is not in $E \cap K_\mu$. As Abel shows by using elementary methods, v is algebraic over K, and all the zeroes of the minimal polynomial $\varphi(x)$ of v over K are contained in E (since E/K is Galois).

[37] When L/K is defined as in (5), the exponent of L/K is the degree of the pure equation (6).

For short, let $r = r_\mu$, $A = A_\mu$, and $p = p_\mu$. Since $v \in E \cap K_{\mu+1} - E \cap K_\mu$, by (2), there is a polynomial

$$\psi(x) = q_0 + x + q_2.x^2 + ... + q_{p-1}.x^{p-1} \in K_\mu[x], \qquad (7)$$

so that $v = y_1 = \psi(r)$.

Abel next shows that r and each q_ν are contained in E: given a primitive p-th root of unity $\alpha \in K$ and let $y_\nu = \psi(\alpha^{\nu-1}r)$ for $\nu = 1, ..., p$. Then $r, \alpha r, ..., \alpha^{p-1}r$ are all the solutions of (6) and since $\varphi(y_1) = 0$ ($y_1 = v$), r is a solution of $\varphi(\psi(x)) \in K_\mu[x]$ and (6). Given the irreducibility of (6) over K_μ, we have $\varphi(\psi(\alpha^\nu r)) = \varphi(y_\nu) = 0$ for all $\alpha^\nu r$ ($\nu = 1, ..., p$); that is, all the y_ν are zeroes of $\varphi(x)$, and hence contained in E. Since the sum of all p-th roots of unity is zero, an easy calculation shows that,

$$q_\nu.r^\nu = 1/p\,(y_1 + \alpha^{-\nu}y_2 + \alpha^{-2\nu}y_3 + ... + \alpha^{-(p-1)\nu}y_p) \in E, \qquad (q_1 = 1) \qquad (8)$$

For $\nu = 1$, it follows that $r \in E$. Since $r \neq 0$, it follows that $q_\nu \in E$ for each ν.

Since $A = r^p \in E$, (6) is a polynomial in $(E \cap K_\mu)[x]$, and is obviously irreducible. Thus, $(E \cap K_\mu)(r)$ is a radical extension of $E \cap K_\mu$. Now, $\psi(x) \in (E \cap K_\mu)[x]$ (since $q_\nu \in E$), that is $v = \psi(r) \in (E \cap K_\mu)(r)$. Since the choice of v was arbitrary, it follows that

$$(E \cap K_{\mu+1}) \subseteq (E \cap K_\mu)(r).$$[38]

Conversely, certainly $(E \cap K_\mu)(r) \subseteq E(r) = E$ and $K_\mu(r) \subseteq K_{\mu+1}$. Thus, we have

$$E \cap K_{\mu+1} = (E \cap K_\mu)(r) \qquad \text{and} \qquad r^p \in E \cap K_\mu.$$

[38] If K, K' are subfields of **C**, and if $M \subseteq \mathbf{C}$, then in general $(K \cap K')(M) \neq K(M) \cap K'(M)$.

What this shows is that, when the equality is not strict, $E \cap K_{\mu+1}$ is a radical extension of $E \cap K_\mu$ of degree $p = p_\mu$. Since we have

$$K = K_0 \subset (K_1 \cap E) \subset ... \subset (K_{\eta-1} \cap E) \subset (K_\eta \cap E) = E,$$

we have shown that E is a radical extension of K. **QED**

The following **Lemma** follows from the proof of **Theorem 1**: if in the situation of **Proposition 1**, $x^p - A$ is *irreducible* over K and $v \in K(r) - K$, the minimal polynomial of v over K has p distinct solutions $y_1, \ldots, y_p$, so that

$$r = (1/p)(y_1 + \alpha^{p-1}y_2 + \ldots + \alpha y_p) \qquad (9)$$

The fact that the solutions are distinct follows from the irreducibility of $x^p - A$.

Regarding Theorem 1. Since the normal closure of L over K is a radical extension of K of the same exponent, L/K is a Galois extension. For each K_μ in (5) we set $N_\mu = \mathrm{Gal}(L/K_\mu)$, so that $N_{\mu+1}$ is a normal subgroup of N_μ, and

$$N_\mu/N_{\mu+1} \approx \mathrm{Gal}(K_{\mu+1}/K_\mu)$$

is a *cyclic group* of prime order p_μ; that is, G(L/K) is solvable. Let

$$\pi\text{: } \mathrm{Gal}(L/K) \to \mathrm{Gal}(E/K)$$

be the surjective restriction homomorphism. For each K_μ, L/K_μ is Galois, that is, the fixed field of N_μ in L is K_μ. If we now put $H_\mu = \pi N_\mu$, then $H_{\mu+1}$ is normal in H_μ and the fixed field of H_μ in E is $E \cap K_\mu$, whence $H_\mu = \mathrm{Gal}(E/E \cap K_\mu)$. Further, we have the induced surjective homomorphism

$$\pi_{\mu:}\ N_\mu/N_{\mu+1} \rightarrow H_\mu/H_{\mu+1}.$$

Accordingly, $H_\mu/H_{\mu+1}$ is either a cyclic group of order p, or else 1. Since $H_{\mu+1}$ is normal in H_μ, the extension $E \cap K_{\mu+1}/E \cap K_\mu$ is Galois and

$$H_\mu/H_{\mu+1} \approx \mathrm{Gal}(E \cap K_{\mu+1}/E \cap K_\mu).$$

That is, $E \cap K_{\mu+1}/E \cap K_\mu$ is either a cyclic extension of degree p_μ, or else it is trivial.

III

The title of this paragraph *Concerning the number of distinct values a function of several quantities can take when the quantities are permuted among themselves* is word-for-word translation from French of the title an article by Cauchy which Abel himself cites.

In modern terms, in this paragraph Abel studied the intermediate fields of the splitting field of the general 5-th degree polynomial. While Abel formulated **Theorem 2** and **Theorem 6** for an arbitrary degree n, we will concentrate on the case $n = 5$.

The context makes it clear that Abel understood the notion of *general polynomial* as follows:

Definition 1 Let k be a subfield of **C** and $E = k(x_1, \ldots, x_5)$ the field of rational functions in five variables. Further, let $a_1, \ldots, a_5$ be the elementary symmetric polynomials in these variables, so that E is the splitting field of the polynomial

$$f(X) = X^5 + a_1 X^4 + a_2 X^3 + a_3 X^2 + a_4 X + a_5 \in K[X]$$

where $K = k(a_1, \ldots, a_5)$. Then we will call $f(x)$ *the general 5-th degree polynomial*. The symmetric group S_5 can be identified with the permutation group of $x_1, \ldots, x_5$.

As Abel shows in two particular cases, E = K[x_1, …, x_5]. In what follows, the elements of E will be viewed as polynomials in x_1, …, x_5 with coefficients in K.

In the modern definition of the general polynomial of 5th degree, the a_1, …, a_5 are defined as variables over k, and one then shows that the situation in **Definition 1** obtains. The extension E/K is Galois, and we have

$$\text{Gal}(E/K) \approx S_5. \qquad (11)$$

These groups will be identified in what follows. Abel, too, treats the permutations in S_5 as if they were K-automorphisms of E without further comment.[39] If one polynomial in E is mapped to another by a permutation in S_5, they are called *conjugates* (over K). The minimal polynomial of such a polynomial means minimal polynomial over K.

If a polynomial is invariant under all permutations in S_5, it is called *symmetric*. A polynomial that is invariant under (at least) all permutations in A_5 is called *alternating*. In what follows, Abel makes frequent use of **The Main Theorem of Symmetric Functions** (MSF), which Waring had proved already in 1762.

> "*The number of distinct values a polynomial in n quantities can take under all the possible permutations of these quantities is a factor in the product* 1.2. … *n*."

This Theorem, which Abel describes as "well-known," goes by the name *Lagrange's Theorem*, for one finds it already in Article 97 of Lagrange's *Reflections*… from the year 1771:

Theorem 2 (Lagrange) *The number of conjugates of a polynomial v in E is a factor of*

[39] Abel makes a definite distinction between what used to be called *permutations* and *substitutions*.

the order of $S_5 = 5!$.

In its group-theoretic formulation, **Theorem 2** says that the order of any subgroup of S_5 divides the order of the group itself. The **Main Theorem of Galois Theory** implies that the number of conjugates of v is equal to the index of Gal(E/K(v)) in S_5. The proof of **Theorem 2** is elementary and will not be reproduced here.

> "*It is* […] *impossible to find a function in* 5 *quantities that has* 3 *or* 4 *distinct values. The proof of this Theorem is contained in a treatise by Cauchy*…"

Cauchy notes in his article that this Theorem is a generalization of a result due to Ruffini from 1804. Abel proves a more general version of **Theorem 3** which we will, for the sake of clarity, only consider in the special case $n = 5$. The proof we will present, however, does come directly from Abel.

Theorem 3 (Ruffini) *A polynomial in E with fewer than 5 conjugates is either alternating or symmetric*.

Modern Proof. One knows from *Bertrand's Theorem* that for $n \neq 4$, the group S_n has no subgroup with index $2 < m < 5$. But the number of conjugates of v in E is precisely the index of Gal(E/K(v)) in S_n.

Proof. Let v in E be a polynomial with m conjugates with $m < 5$. Thus, v is invariant under any permutation S of degree 5. For, since $m < 5$, at least two of the polynomials

$$v, \quad Sv, \quad S^2v, \quad S^3v, \quad S^4v \qquad\qquad (12)$$

are equal, with $S^{\mu}v = S^{\mu'}v$ with $\mu \neq \mu'$ mod 5. Thus, v is invariant under $S^{\mu - \mu'}$ and any power thereof. Since 5 is a prime, there is some ν such that $\nu(\mu - \mu') \equiv 1$ mod 5. Hence, v is in fact invariant under $S = S^{\nu(\mu - \mu')}$, as claimed.

A straightforward calculation shows that any 3-cycle in S_5 can be expressed as a product of two permutations of degree 5. Hence, v is invariant under any 3-cycle. But it is well-known that the 3-cycles generate the alternating group A_5. Thus, v is alternating. It follows that v is alternating or symmetric. **QED**

In light of **Theorem 3**, Abel now investigates polynomials $v \in E$ with 2 or 5 conjugates. It turns out that the splitting fields K(v) are already known in these cases.

> "Each function in five quantities that has exactly two distinct values
>
> can be expressed in the form $p + q\rho$, where p and q are symmetric functions
>
> and $\rho = (x_1 - x_2)(x_1 - x_3) \ldots (x_4 - x_5)$."

Theorem 4 *Each polynomial with fewer than five distinct conjugates is contained in* K[ρ], *where* ρ^2 *denotes the discriminant of* $f(x)$.

Modern Proof. In its group-theoretic formulation, **Theorem 4** states that A_5 is the unique subgroup of S_5 with index 2. The **Main Theorem of Galois Theory** then implies that the fixed field of A_5 is the unique subfield of E with degree = 2 over K, and since ρ is alternating but not symmetric, the fixed field in E of A_5 is K[ρ].

Proof. Since the solutions of $f(x)$ are *distinct*, we have $\rho \neq 0$. Clearly, ρ is alternating and ρ^2 is symmetric. Given **Theorem 3**, a polynomial v_1 in E with fewer than 5 conjugates is either alternating or symmetric. In the symmetric case, certainly v_1 is in K[ρ]. In the alternating case, let v_2 be the distinct conjugate of v_1. Then both $t = v_1 + v_2$ and $t_1 = \rho(v_1 - v_2)$ are symmetric and hence, by **MSF**, belong to K. Thus, v_1 is in K[ρ], since

$$v_1 = p + q\rho \text{ with } p = t/2,\ q = t_1/2\rho^2 \in \mathrm{K}.$$

QED

Theorem 5 *For a given zero x_μ of $f(x)$, let $\Im_\mu$ be the group of all permutations in* S_5 *that fix x_μ.*

A polynomial v in E *is invariant under all permutations in $\Im_\mu$ precisely when v belongs to* K[x_μ]. *Further, any v in* K[x_μ] *either has* 5 *conjugates or else is symmetric*.

Modern Proof. By the **Main Theorem of Galois Theory**, Gal(E/K[x_μ]) = $\Im_\mu$, and therefore K[x_μ] is the fixed field of $\Im_\mu$.

Proof. Without loss of generality, let $x_\mu = x_1$. Each polynomial v in E invariant under the permutations in $\Im_1$ is symmetric in the zeroes x_2, …, x_5 and, by the **MSF**, such v can be expressed as a polynomial in x_1 over K and in the symmetric polynomials in x_2, …, x_5. The latter, however, are contained in K[x_1] (for example, $x_2 + \ldots + x_4 = a_1 - x_1$). Thus, v is in K[x_1]. The verification is trivial.

Let now $v = v(x_1) \in$ K[x_1]. Then $v(x_1)$, ..., $v(x_5)$ are the conjugates of $v(x_1)$, and suppose, WLOG, that $v(x_2) = v(x_1)$, so one obtains by applying the four transpositions (x_2, x_μ), $\mu = 2, ..., 5$, that v is symmetric. **QED**

“*Each rational function of five quantities that has five distinct values, is of the form*

$$r_0 + r_1 x + r_2 x^2 + r_3 x^3 + r_4 x^4,$$

where r_0, ..., r_4 are symmetric functions and x is any one of the five quantities.”

Theorem 6 *If a polynomial $v \in$ E has exactly five distinct conjugates, then* $\mathrm{K}(v) = \mathrm{K}(x_\mu)$ *for any solution x_μ of $f(x)$*.

Modern Proof. If $n \neq 6$, the n subgroups $\Im_\mu$ are the only subgroups of S_n of index n. From the **Main Theorem of Galois Theory** it follows that if $n \neq 6$, the n fields $\mathrm{K}[x_\mu]$ are the only extension fields of K of degree n. Thus, $\mathrm{K}(v) = \mathrm{K}(x_\mu)$.

Proof. Let v_1, ..., $v_5 \in$ E be the five distinct conjugates of $v = v_1$, and let v_1, ..., v_μ be the conjugates one obtains by applying all the permutations from $\Im_1$. Then by **Theorem 5**,

$$v_1 + v_2 + ... + v_\eta = \varphi(x_1) \in \mathrm{K}[x_1] \qquad (13)$$

for some $\varphi(x) \in \mathrm{K}[x]$. Consider the possible values η can take:

1. $\eta = 5$. Pick m large enough so that none of the polynomials v_1, ..., v_η is divisible by the powers x_1^m, ..., x_5^m. The polynomial $x_1^m v_1 \in$ E can have at most 25 distinct conjugates. Given that $\eta = 5$, if one applies all the permutations from $\Im_1$ on $x_1^m v_1$, one obtains the polynomials

$$x_1^m v_1, \quad x_1^m v_2, \quad x_1^m v_3, \quad x_1^m v_4, \quad x_1^m v_5.$$

If one now applies to these polynomials the five transpositions $T_\mu = (x_1, x_\mu)$ for $\mu = 1, ..., 5$, given the bijectivity of T_μ, one obtains the 25 polynomials $x_\mu{}^m v_\nu$, with $\nu = 1, ..., 5$, which, given the choice of m, are pairwise distinct. Thus $x_1{}^m v_1$ has 25 distinct conjugates, which is impossible by **Theorem 2**. So, $\eta = 5$ cannot occur.

2. $\eta = 1$. In this case, $v_1 = \varphi(x_1) \in K[x_1]$ and the **Theorem** follows.

3. $\eta = 4$. In this case, $v_5 + \varphi(x_1)$ is symmetric and hence in K. Hence, $v_5 \in K[x_1]$ and so one obtains v_1 from v_5 by applying some permutation, whence $v_1 \in K[x_\nu]$ for some x_ν.

4. $\eta = 2$. Abel rules out this case by solving a system of equations by considering a large number of subcases. But this case can also be handled more easily by using Abel's own methods: to begin with, there is at least one $S \in S_5$ of order 5, so that after suitably renaming them,

$$v_1, \quad v_2 = Sv_1, \quad v_3 = S^2v_1, \quad v_4 = S^3v_1, \quad v_5 = S^4v_1$$

are precisely the 5 distinct conjugates of v_1, for otherwise it would follow as in the proof of **Theorem 3**, that v_1 is either alternating or symmetric.[40] As Cauchy shows in *Sur le Nombre des Valeurs…*, S is 5-cycle. One can thereby further show that $x_{\nu+1} = S^\nu x_1$, for $\nu = 1, ..., 4$. By applying S to (13), one obtains

$$v_1 + v_2 = \varphi(x_1)$$

$$v_2 + v_3 = \varphi(x_2)$$

[40] v_2 is fixed by (13).

$$\ldots \qquad (14)$$

$$v_5 + v_1 = \varphi(x_5)$$

By eliminating $v_2, \ldots, v_5$ in this system, one obtains

$$v_1 = \Sigma - \varphi(x_2) - \varphi(x_4), \qquad (15)$$

where 2Σ = sum over all $\varphi(x_v)$. As a symmetric function, Σ is in K. Now $\varphi(x_2)$ cannot be symmetric, for otherwise $\varphi(x_4)$ would also be symmetric and hence, finally, v_1, which is not the case. Thus, by **Theorem 5**, $\varphi(x_2)$ has 5 conjugates. But then, by applying a suitable transposition, one shows that the right-hand side of (15) would have to have more than two conjugates under the permutations from $\mathfrak{I}_1$. Hence, $\eta = 2$ does not occur.

5. $\eta = 3$. In this case Σ = the symmetric sum over all the v_ν. Thus, $\Sigma = v_4 + v_5 + \varphi(x_1)$; hence, $v_4 + v_5 = \psi(x_1)$ for some $\psi(x) \in$ K$[x]$. By replacing v_4 with v_1 and v_5 with v_2, one obtains a contradiction in a manner analogous with case 4.

In sum, $v \in$ K(x_μ) for some zero x_μ of $f(x)$. If v is not symmetric and since a field extension of prime degree cannot contain a proper intermediate field, we actually have K(v) = K(x_μ) (Abel proves this last step by using elementary methods). **QED**

> "*If a function of several quantities has m distinct values, one can always find an equation of degree m whose coefficients are symmetric functions, and have these values as solutions; it is, however, impossible to find an equation of this form, but of lower degree, that has one or more of these values as solution*."

Theorem 7 *Two polynomials in E are conjugates if and only if they are solutions of the same minimal polynomial. Thus, the number of conjugates of a polynomial is the number* *of solutions of its minimal polynomial.*

The proof is analogous to the modern one and will not be presented here.

IV

Abel's treatise concludes with this paragraph and the *Proof of the Impossibility of the general Solution of the Fifth Degree Equation*:

Theorem 8 *The general polynomial of fifth degree is not solvable by radicals.*

Modern Proof. In group theoretic terms, **Theorem 8** says that S_5 is not solvable. In order to present Abel's reasoning more clearly, in this paragraph we will present his proof also in group-theoretic terms, so that the modern translations of the results in the previous paragraph may be employed more easily.

Abel's proof can be divided into two auxiliary propositions.

Proposition 2 *If* K *contains a primitive p-th root of unity* α *for a prime p, and if r* $\in$ E *is a solution of the equation*

$$x^p - \mathrm{A} \in \mathrm{K}[x], \qquad (16)$$

but not symmetric, then p = 2 *and* K(r) = K[ρ]. *Thus,* K[ρ] *is the only radical extension of K contained in E.*

This Proposition says, strengthening **Theorem 4**, that A_5 is the only normal subgroup of S_5 with prime index.

Proof. By **Proposition 1**, the polynomial x^p – A is irreducible over K. By **Theorem 7**, the p is the number of conjugates of r, and so by **Theorem 2**, p divides 5!.

By **Theorem 3**, either $p = 2$ or $p = 5$. But if $p = 5$, we then have $K(x_1) = K(r)$ by **Theorem 6**. By (9) we would further have

$$r = 1/5(x_1 + \alpha^4 x_2 + \alpha^3 x_3 + \alpha^2 x_2 + \alpha x_5).$$

The right-hand side has 120 = 5! distinct conjugates, a contradiction. Hence, $p = 2$ and by **Theorem 4**, $K(r) = K[\rho]$. **QED**

Group Theoretic. Since S_5 has no subgroup of index $2 < m < 5$ by Bertrand's Theorem, the index of a normal subgroup N of S_5 with a prime index would have to be = 2 or = 5. The isotropy group $\mathfrak{I}_\mu$ from **Theorem 5** is the only subgroup of S_5 of index 5, but it is not normal. Hence, $p = 2$. On the other hand, since A_5 is the only normal subgroup of S_5 of index 2, we must have $N = A_5$.

Proposition 3 *If* K *contains a primitive root of unity for each prime p, then there is no proper radical extension of* K[ρ] *contained in* E.

In modern terms, this says that A_5 has no normal subgroup of prime index and as such, is not solvable.

Proof. Suppose that $L(r) \neq L = K[\rho]$ is a radical extension, so that r is a solution of

$$x^p - A \in L[x] \qquad (17)$$

with p a prime. Then r is not in L, and by **Proposition 2**, (17) is irreducible over L. On the other hand, A is not in K, for otherwise by **Proposition 2** we would have $L(r) = K(r) = L$. Hence, A is alternating but not symmetric.

Abel now shows that the polynomial

$$(x^p - A)(x^p - A') \in K[x]$$

which is contained in K[x] by **MSF**, is the minimal polynomial of r over K, so that A' is the unique conjugate of A. The proof is elementary, and will not be reproduced here. Thus, by **Theorem 7**, r has 2p distinct conjugates. Hence, by **Theorem 3**, $p \neq 2$.

Now consider the case $p = 5$. If r' is a solution of $x^p - A' \in L[x]$, then r' is a conjugate of r, so $r' \in E$. Hence, the polynomial $x^p - A.A' \in K[x]$ is not irreducible over K, with $r.r' \in E$ a solution, for by **Proposition 2** we would have $2p = 2$, a contradiction. So, by **Proposition 1**, $x^p - A$ splits into linear factors over K, and in particular we have

$$\gamma = r.r' \in K.$$

Now let $\mu = 1, ..., p$ and let α be a primitive p-th root of unity α

$$v_\mu = \alpha^\mu.r + \alpha^{-\mu}.r' = \alpha^\mu.r + \gamma/\alpha^\mu.r \in K(r) \qquad (18)$$

By applying *Newton's Formula* one obtains easily

$$\varphi(x) = (x - v_1)(x - v_2)...(x - v_p) \in K[x].$$

By the irreducibility of (17) over K and by the irreducibility of the p-th [...]polynomial over **Q** (proved by Gauss in 341 of the *Discquisitiones*) it follows that $\varphi(x)$ is irreducible over K (obviously $v_1, ..., v_p$ is a complete system in E of conjugate over K).

If $\varphi(x)$ is irreducible over K, by **Theorem 7**, v_1 has p distinct conjugates, so that by **Theorem 2**, p divides 5!. By **Theorem 3**, $p = 3$ cannot occur and since we have just excluded $p = 2$, we must have $p = 5$.

Hence, by **Theorem 6**, $K(v_1) = K(x_1)$ for the solution x_1 of $f(x)$. Since $v_1 \in K(r)$, $x_1 \in K[\rho](r)$. If x_1 has more than two conjugates, x_1 is not in K[ρ]. Hence by (9), we have

$$r = 1/5(x_1 + \alpha^4 x_2 + \alpha^3 x_3 + \alpha^2 x_4 + \alpha x_5)$$

Hence, r has $5! = 120$ conjugates (that is, r is a primitive element of E/K). But, above we saw that r must have $2.p = 10$ conjugates. Hence, $p \neq 5$. **QED**

Group Theoretic. If N is a normal subgroup of A_5 of prime index p, then $[S_5 : N] = 2.p$. Since S_5 contains no subgroup of index $2 < m < 5$ (by the remark following **Theorem 3**), we have $p \neq 2$. Now ..., then each 3-cycle can be written as a product of two such permutations. Hence, there is at least one S in A_5 of order 2 with S not in N. If H is a the subgroup generated by S, then N.H is a subgroup of A_5 of order 2.[N], that is,

$$[S_5 : N.H] = p \text{ divides } [S_5].$$

Since $p = 3$ cannot occur by Bertrand's theorem, $p = 5$. But then $N.H = \mathfrak{I}_\mu$ for some x_μ. But since $\mathfrak{I}_\mu$ is not contained in A_5, $p = 5$ cannot occur. Hence, A_5 is not solvable.

Proof of **Theorem 8** Suppose that the general equation of 5th degree is solvable by radicals. Then it is also solvable over the extension of K one obtains by adjoining all the roots of unity in K. Hence, we can suppose that K contains all the roots of unity. By **Theorem 1**, E is therefore itself a radical extension of K of the form

$$K = K_0 \subset K_1 \subset \ldots \subset K_{\eta-1} \subset K_\eta = E,$$

where $K_{\mu+1}$ for $\mu = 0, \ldots, \eta - 1$ is obtained by adjoining a solution of $x^p - A \in K_\mu[x]$ to K_μ for some A, some p.

Since $f(x)$ is by **Theorem 7** irreducible over K, then $K \neq E$, and hence $\eta \neq 0$. By **Proposition 2**, $K_1 = K[\rho]$. Since each element of $K[\rho]$ has just two conjugates, we cannot have $E = K_1$. Hence, $\eta > 1$. By **Proposition 3**, E contains no proper radical extension of $K[\rho]$ and hence, $f(x)$ is not solvable. **QED**

Abel's proof of **Theorem 8** is entirely conclusive, once some critical places in the extensive proofs of **Theorems 1** and **6** and **Proposition 2**, are filled in. The problem with these proofs stems principally from the fact that Abel sets out to investigate the statements (concerning the degrees of minimal polynomials) only relative to the ground field K and not also relative to extension fields L of K.

Abel published two further treatises on the question of solvability of polynomials; from neither one does one get the impression that Abel would have been moving towards the sort of general theory which Galois obtained a few years later.

[*Section omitted.*]

References

[1] Abel, N.H. *Oeuvres complètes de N.H. Abel mathématicien*, Sylow L., Lie S. (Eds.), Christian (1881)

[2] Abel, N.H., Galois E. *Über die algebraische Auflösung der Gleichungen von N.H. Abel und Evariste Galois*, Maser H. (Ed.), Berlin (1889)

[3] Cauchy, A.L. *Sur le Nombre des Valeurs qu'une Fonction peut acquérir…*, Journal de l'Ecole Polytechnique, Vol. 17, (1815), 1-29

[4] Cauchy, A.L. *Sur les Fonction qui ne peuvent obtenir que deux valeurs égales…*, Journal de l'Ecole Polytechnique, Vol. 17, (1815), 29-112

[5] Galois, E. *Ecrits et mémoires mathématiques d'Evariste Galois*, J-P. Azra, R. Bourgne (Eds.), Paris: Gauthier-Villars (1962)

[6] Gauss, C.F. *Untersuchungen über höhere Arithmetik* (Disquisitiones Arithmeticae), Maser, H. (Ed.), Berlin (1889)

[7] Huppert, B. *Endlich Gruppen*, Vol. 1., Berlin-Heidelberg-New York: Springer-Verlag (1967)

[8] Könisberger, L. *Berichtigung eines Satzes von Abel, die Darstellung der algebraichen Functionen betreffend*, Math.Ann. I, (1869), 168-169

[9] Lagrange, J.L. *Réflexions sur la résolution algébrique des équations*, in *Werken*, Paris: Gauthier-Villars (1869), Vol. 3, 204-421

BIBLIOGRAPHY

1. Artin, Emil: 1942, *Galois Theory*. Notre Dame Mathematical Lectures, Number 2. Notre Dame: Notre Dame University Press.

2. Avigad, Jeremy: 2003: "Number theory and elementary arithmetic". *Philosophia Mathematica* (3), Vol. 11, 257-284.

3. Avigad, Jeremy: 2005: "Mathematical method and proof". To appear in *Synthese*.

4. Avigad, Jeremy: 2005: "Methodology and metaphysics in the development of Dedekind's theory of ideals". Unpublished.

5. Cooper, Neil: 1994, "The Epistemology of Understanding." *Inquiry* 38, 205-15.

6. Corfield, David: 2003, *Towards a philosophy of real mathematics*. Cambridge: Cambridge University Press.

7. Ebbinghaus, H.-D., H. Hermes, F. Hirzebruch, M. Koecher, K. Mainzer, J. Neukirch, A. Prestel, and R. Remmert: 1990, *Numbers*. Vol. 123 of *Graduate Texts in Mathematics*. New York: Springer-Verlag. With an introduction by K. Lamotke, Translated from the second German edition by H. L. S. Orde, Translation edited and with a preface by J. H. Ewing.

8. Edwards, Harold: 1992, "Mathematical Ideas, Ideals, and Ideology." *Mathematical Intelligencer*, Vol. 14, No. 2, 6-19.

9. Fenrick, Maureen: 1992, *Introduction to the Galois Correspondence*. Boston: Birkhäuser.

10. Gauss, Carl Friedrich: 1801, *Disquisitiones Arithmeticae*. Leipzig: G. Fleischer.

11. Goldman, J. R.: 1998, The Queen of Mathematics: a historically motivated guide to number theory. Wellesley, MA: A K Peters Ltd.

12. Gray, Jeremy: 1992, "The nineteenth-century revolution in mathematical ontology." In *Revolutions in mathematics*. Oxford Sci. Publ. New York: Oxford Univ. Press, 226-248.

13. Grillet, Pierre Antoine: 1999, *Algebra*. New York: Wiley-Interscience.

14. Hamilton, William R.: 1839, "On the Argument of Abel". *Transactions of the Royal Irish Academy* 18, 171-259.

15. Hamilton, William R.: 1841, "Investigations Respecting Equations of the Fifth Degree". *Proceedings of the Royal Irish Academy* 1, 76-80.

16. Kiernan, B. Melvin: 1971, "The Development of Galois Theory from Lagrange to Artin." *Archive for History of Exact Science* 8, 40-154.

17. Leon, Uri: 1983, "Structuring Mathematical Proofs." *American Mathematical Monthly*, Vol. 90, Issue 3, 174-185.

18. McDowell, John: 1994, *Mind and World*. Cambridge: Harvard University Press.

19. Mac Lane, Saunders: 1996, "Structure in Mathematics." *Philosophia Mathematica* (3), Vol. 4, 174-183.

20. Mancosu, Paolo: 2001, "Mathematical Explanation: Problems and Prospects." *Topoi* 20, 97-117.

21. Manders, Kenneth: "The Euclidean Diagram." Unpublished.

22. Marquis, Jean-Pierre: 1997, "Abstract Mathematical Tools and Machines for Mathematics." *Philosophia Mathematica* (3), Vol. 5, 250-272.

23. Österman, Bernt: 2001, "Is There a General Sense of Understanding?" *Acta Philosophica Fennica* 69, 27-41.

24. Pesic, Peter: 2004, *Abel's Proof: An Essay on the Sources and Meaning of Mathematical Unsolvability*. Cambridge, MA: MIT Press.

25. Radloff, Ivo: 1996, *Originalwerke Abels und Galois' im Spiegel der modernen Mathematik*. Diplomarbeit, Phillips-Universität Marburg.

26. Radloff, Ivo: 1998, "Abels Unmöglichkeitsbeweis im Spiegel der modernen Galoistheorie." *Mathematische Semesterberichte* 45, 127-139.

27. Radloff, Ivo: 2001, "Évariste Galois: Principles and Applications." Unpublished.

28. Serre, Jean-Pierre: *Représentations lineaires des groupes finis*. Paris: Hermann 1971. Translated from the second French edition by Leonard L. Scott as *Linear Representations of Finite Groups*. 1977. New York: Springer-Verlag.

29. Stein, Howard: 1988, "Logos, *Logic*, and Logistiké: *Some Philosophical Remarks on Nineteenth-Century Transformation of Mathematics*". W. Aspray and P. Kitcher (eds.), *History and Philosophy of Modern Mathematics*. University of Minnesota Press, 238-259.

30. Steiner, Mark: 1978, "Mathematical Explanation". *Philosophical Studies* 34, 133-151.

31. Tappenden, Jamie: 1995, "Extending Knowledge and 'Fruitful Concepts': Fregean Themes in the Foundations of Mathematics." *Noûs*, 427-467.

32. Thurston, William: 1994, “On Proof and Progress in Mathematics.” *Bulletin of the American Mathematical Society*, 30, number 2, April 1994, 161-177.

33. Tymoczko, Thomas (ed.): 1998, *New Directions in the Philosophy of Mathematics*. Princeton: Princeton University Press.

34. Van Bendegem, Jean Paul: 1988, “Non-Formal Properties of Real Mathematical Proofs,” in A. Fine and J. Leplin (eds.), *PSA 1988: Proceedings of the 1988 Biennial Meeting of the Philosophy of Science Association Volume One*.

35. Wussing, H.: 1984, *The genesis of the abstract group concept: a contribution to the history of the origin of abstract group theory*. Cambridge, MA: MIT Press. Translated from German by Abe Shenitzer and Hardy Grant.