Philosophers' Imprint

volume 000, no. 00
october 23, 2014

THE UNSOLVABILITY OF THE QUINTIC: A CASE STUDY IN ABSTRACT MATHEMATICAL EXPLANATION

Christopher Pincock

The Ohio State University

Abstract

This paper identifies one way that a mathematical proof can be more explanatory than another proof. This is by invoking a more abstract kind of entity than the topic of the theorem. These abstract mathematical explanations are identified via an investigation of a canonical instance of modern mathematics: the Galois theory proof that there is no general solution in radicals for fifth-degree polynomial equations. I claim that abstract explanations are best seen as describing a special sort of dependence relation between distinct mathematical domains. This case study highlights the importance of the conceptual, as opposed to computational, turn of much of modern mathematics, as recently emphasized by Tappenden and Avigad. The approach adopted here is contrasted with alternative proposals by Steiner and Kitcher.

1. Introduction

Despite being usually overlooked by philosophical discussions of explanation, mathematical practice is often guided by the distinction between more and less explanatory proofs of a theorem. While all proofs from accepted assumptions are said to show that the theorem is true, it is only an explanatory proof that also shows why the theorem is true ([22]). However, philosophers have yet to offer a satisfying, positive account of explanatory proof. In this paper I use a case study to elucidate one kind of explanatory proof. The case is the canonical application of what is known as Galois theory: the proof that there is no general solution in radicals for the quintic (fifth-degree polynomial equations). There is considerable evidence that practitioners consider this proof to be more explanatory than its predecessors. As I will show below, Galois theory is a central instance of the more abstract, conceptual approach to mathematics that is sometimes known as modern mathematics. Thus it illustrates a more general change in the character of mathematics in the nineteenth and early twentieth centuries. The Galois theory proof is often judged to be more explanatory than an earlier proof of the same theorem by Abel from 1824. As Stewart has recently put it, “Not only does it [Galois’s ideas as articulated in Galois theory] prove that the general quintic has no radical solutions, it also explains why the general quadratic, cubic and quartic do have radical solutions and tells us roughly what they look like" ([27], p. 116). In a sympathetic discussion of Abel’s work, Pesic seems to agree. He says “What is new in Galois is a turn toward abstraction in an essentially modern way, leading to a complete understanding of solvability, which Abel lacked" ([23], pp. 108-109). Liebeck, writing in the recent *Princeton Companion to Mathematics*, concurs: “Galois . . . built an entirely new theory of equations that not only explained the nonexistence of formulas but laid the foundation for a whole edifice of algebra and number theory known as *Galois theory*, a major area of modern-day research" ([20], p. 709).

Identifying this apparent consensus among mathematicians and historians of mathematics is merely the first step in developing a philosophical account of explanatory proof. In this paper I will proceed cautiously and set aside the strong claim that there is only one kind of explanatory proof. Instead, I will allow that there might be many ways to arrive at an explanatory proof. My focus, then, is on a restricted class of explanatory proofs that I will call abstract mathematical explanations. These explanations will share some core features of the Galois theory proof. In particular, an abstract mathematical explanation will explain by appeal to an entity that is more abstract than the subject-matter or topic of the theorem. In terms of the notion of purity of methods recently explored by Detlefsen and Arana, abstract mathematical explanations are decidedly impure ([9]). Other mathematical explanations may turn out to be pure or to explain by other means. This paper will be successful if I can identify what is special about abstract explanations and their explanatory power.

To focus our attention on this restricted class of cases we can consider two recent papers. In “The Riemannian Background to Frege’s Philosophy" Tappenden argues that it is wrong to find a unified trend towards the “rigorization of analysis" in the nineteenth century. Instead, Tappenden demonstrates how there were actually two distinct trends that can be associated with Riemann and Weierstrass. Focusing on their different treatments of complex analysis, Tappenden argues that

> Riemann’s approach treated functions as given *independently* of their modes of representation. Riemann’s techniques systematically exploited indirect function–existence arguments that need not correspond to any formula. Weierstrass dealt with explicitly given representations of functions. (Weierstrass: ‘The whole point is the representation of a function’.) ([29], p. 107)

This *conceptual* approach of Riemann rejected the *computational* approach of Weierstrass. The same contrast is central to Avigad’s “Methodology and metaphysics in the development of Dedekind’s theory of ideals", although Avigad develops it in terms of the differences between Dedekind and Kronecker. He quotes Dedekind who said:

> Even if there were such a theory, based on calculation, it still would not be of the highest degree of perfection, in my opinion. It is preferable, as in the modern theory of functions, to seek proofs based immediately on fundamental characteristics, rather than on calculation, and indeed to construct the theory in such a way that it is able to predict the results of calculation ([2], p. 166).

Avidgad points out that the phrase “the modern theory of functions" is a reference to Riemann. He goes on to suggest that “localizing and minimizing the role of representations and calculations" illustrates “tendencies that have become hallmarks of modern mathematics" ([2], p. 181). As I will present it, the explanatory benefits of Galois theory correspond precisely with the conceptual approach that Tappenden and Avigad find in Riemann and Dedekind. This is not surprising as Dedekind was a major contributor to the articulation of Galois theory in its contemporary form.

Ideally, I would here present not only Galois theory but also its historical and conceptual links to the developments in complex analysis and algebraic number theory discussed by Tappenden and Avigad. As this is not feasible I restrict my discussion to this one application of Galois theory. This narrow focus on the proof of the unsolvability of the quintic has some benefits. To start, the initial problem and its eventual solution can be appreciated without extensive training in advanced mathematics. In the next section I will outline the mathematical details that are necessary for our philosophical discussions. A further benefit is that the two most thorough proposals for what constitutes a mathematical explanation grant that our Galois theory proof is an explanatory proof.[1] This makes it relatively easy to criticize these proposals for their failure to appreciate what is crucial to abstract explanations. As we will see, Steiner and Kitcher do not appreciate the significance of the conceptual turn of modern mathematics. This means that their approaches are fundamentally ill-equipped to handle an explanatory proof that they themselves grant is explanatory. After seeing the limitations of these approaches, I will turn to a positive account of abstract explanation.

While no comprehensive account is presented, I claim that the Galois theory proof is an explanatory proof because it invokes a special sort of ontological dependence between distinct mathematical domains. The evidence for this sort of dependence is the novel and informative classification of entities that is at the heart of the proof. As I will illustrate, the proof effects an exhaustive division of a given mathematical domain by appeal to the properties of objects drawn from a new and more abstract domain. These are the core features of what I will call an abstract explanation. It will become clear that abstract explanations function in a way that goes beyond the presence of any computational procedure.[2] An interesting aspect of abstract explanations is that they tend to change our conception of a given mathematical domain. However, in many cases, this change does not amount to a wholesale shift in our ontological commitments. Instead, we are left with two distinct mathematical domains where one domain is judged to illuminate the other.

1. It is also mentioned in passing in [19], p. 322.
2. This does not mean that these proofs fail to include any computation. The point is that the explanatory power of the proof is not determined by these procedures. I am grateful to an anonymous referee for emphasizing this point.

2. An explanatory proof

The general problem that I will discuss is the solvability of polynomial equations of the form

$$a_n t^n + \ldots + a_1 t + a_0 = 0 \tag{1}$$

n reflects the *degree* of the equation. The a_i in this equation are the *coefficients* of the equation. In all the cases that I will discuss here the coefficients are drawn from the rationals $\mathbb{Q}$ or the real numbers $\mathbb{R}$. A solution to this equation will provide an exhaustive list of the values for t that make the equation come out true. These are the *roots* of the equation. It is not too difficult to find equations where the roots lie outside the domain from which the coefficients are drawn. For example, using only coefficients from $\mathbb{Q}$, here is a polynomial whose roots are not in $\mathbb{Q}$:

$$t^2 - 2 = 0 \tag{2}$$

Analogously, using only coefficients from $\mathbb{R}$, here is a polynomial whose roots are not in $\mathbb{R}$:

$$t^2 + 1 = 0 \tag{3}$$

One might hope for a domain where the roots to any polynomial with coefficients drawn from that domain will have a solution in that domain. This domain exists and is the domain of the complex numbers $\mathbb{C}$. Each complex number is of the form $a + bi$, where a and b are real numbers and $i = \sqrt{-1}$. The Fundamental Theorem of Algebra ensures that any polynomial equation with coefficients from $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$ has roots in domain $\mathbb{C}$. In fact, when we account for the multiplicities of roots, there are exactly n roots for a polynomial equation of degree n.

Mathematicians were not content to prove that the roots for each polynomial equation exist, but also wished to figure out how the roots for each equation related to the properties of that equation. By the end of the sixteenth century considerable progress on this problem had been made. For $n = 2, 3, 4$, there were formulae that allowed one to calculate the roots given only the coefficients of the polynomial.[3] An early success is the quadratic formula for second degree polynomials $a_2t^2 + a_1t + a_0 = 0$:

$$t = \frac{-a_1 \pm \sqrt{a_1^2 - 4a_2a_0}}{2a_2} \tag{4}$$

The quadratic formula allows us to conclude that the roots of (2) are $\pm\sqrt{2}$, while the roots of (3) are $\pm i$. Similar formulae were eventually obtained for polynomial equations of degree 3 and 4. What each formula had in common was that it started with numbers drawn from the domain of the coefficients and applied only the operations of addition, subtraction, multiplication, division and $\sqrt[b]{a}$. $\sqrt[b]{a}$ actually involves a series of operations that generalize the usual square root operation. $\sqrt[3]{a}$ is the cubic root operation that outputs a number that, when cubed, yields the number we started with: $\sqrt[3]{8} = 2$. $\sqrt[3]{a}$ appears in the formula for third degree equations, while each fourth degree equation can be solved by an elaborate reduction to a related third degree equation.

Let us say that a particular polynomial equation is *solvable by radicals* if there is a formula involving only the domain of the coefficients and the operations of addition, subtraction, multiplication, division and $\sqrt[b]{a}$. Then the success at obtaining the above formulae for $n = 2, 3, 4$ shows that every polynomial of degree 2, 3 or 4 is solvable by radicals. I will use "$R(n)$" to abbreviate the claim that every polynomial of degree n is solvable by radicals. Then we have shown that

3. I will ignore the $n = 1$ case as it is easily solved by the formula $t = -a_0/a_1$.

(A) if $n = 2, 3, 4$, then $R(n)$

But towards the end of the eighteenth century, there were some indications that (A) could not be extended when n is 5 or greater. To start, the methods used to obtain the formulae when $n = 2, 3, 4$ failed to provide a formula when $n = 5$. This, of course, did not prove that $R(n)$ failed when $n \geq 5$, but the continued efforts of mathematicians to prove $R(5)$ were unsuccessful.

Eventually mathematicians came to believe that

(B) $R(n)$ iff $n = 2, 3, 4$

The historical sequence of events is complicated, but can be summarized as follows. Lagrange, in a paper from 1770-71, collected together the different algorithms for solving equations of degree 2, 3 and 4. This unified treatment allowed Lagrange to show that these methods could not be extended in a straightforward manner to the case of the quintic.[4] Lagrange focused on the different expressions that could be formed from the unknown roots of an equation using operations like addition and square root. Some of these expressions retained their value as the roots were permuted. Considering these expressions helped Lagrange isolate which formulae would take one closer to determining the unknown roots. Abel, in 1824, built on this focus on the permutations of the roots to develop a proof that when $n > 4$ a contradiction resulted from the assumption that there was a formula sufficient to calculate the unknown roots. So, combined with the previously determined formulae for $n = 2, 3, 4$, Abel succeeded in proving (B).[5]

This is not the end of the story, however. For while Abel succeeded in proving (B), there is a clear sense in which this proof was not a good

4. [15], §2, [32], ch. II.1.
5. See [23] for a helpful overview of Abel's achievements. Ruffini is an interesting figure intermediate between Lagrange and Abel. In 1799 Ruffini claimed to have refuted $R(5)$. But his proof placed special restrictions on the radicals involved. Following Stewart, one can say that Ruffini showed that not every quintic is solvable by *Ruffini* radicals ([26], p. 96). Abel's proof showed that this restriction was unnecessary.

one. It is widely believed that a better proof of (B) was offered by Galois in 1831. Exactly what Galois accomplished is a delicate historical matter as his work is hard to understand and Galois' premature death prevented him from making any further clarifications. Beginning with Liouville's publication of Galois' major works in 1846, much of the rest of the nineteenth century is marked by a gradual assimilation and extension of Galois' ideas. Thus it would be wrong to say that Galois was the lone inventor of Galois theory. Significant contributions were made by Serret, Jordan, H. Weber and Dedekind. Kiernan, in his history of Galois theory, claims that it is only with Artin in 1938 that the contemporary understanding of Galois theory was obtained ([15], p. 145). While this may be an exaggeration, I will present the proof from the contemporary perspective found in Stewart's *Galois Theory* textbook ([26]). This will allow a more accessible presentation of the Galois theory proof of the unsolvability of the quintic. I hope to pursue in future work the historical subtleties that are glossed over here.[6]

Two innovations are central to the Galois theory proof. The first innovation concerns how we are to think about the property of a polynomial equation being solvable by radicals. Up to now we have considered the problem in terms of an equation with coefficients drawn from a domain like $\mathbb{Q}$. Then the problem is how to calculate the roots of this equation on the assumption that the roots will lie in $\mathbb{C}$ even if they are not in $\mathbb{Q}$. We first change our conception of the problem by introducing the notions of a field and a field extension. A *field* is a domain with operations $+$ and $\times$ defined on the members of the domain so that they obey the usual properties of commutativity and associativity.[7] In addition, we assume that every member of the domain has a multiplicative inverse: if $a \in F$, then there is an $a^{-1} \in F$ such that $a \times a^{-1} = 1$, where 1 is the unit of the field F. Both $\mathbb{Q}$ and $\mathbb{C}$ are fields, but there are many fields lying between $\mathbb{Q}$ and $\mathbb{C}$ in the following sense of "between": adding elements to $\mathbb{Q}$ from $\mathbb{C}$ and rounding out the domain to make the enlarged domain a field can lead to a field that is distinct from $\mathbb{C}$. For example, adding $\sqrt{2}$ to $\mathbb{Q}$ enlarges the domain, and we obtain a new field whose members can all be represented as

$$a + b\sqrt{2} \tag{5}$$

where a and b are drawn from $\mathbb{Q}$. This is one example of a *field extension* of $\mathbb{Q}$. A name to refer to this field extension is $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$.

The second major innovation is to consider the *field automorphisms* of a field extension. An automorphism is a one-one, onto mapping from a domain into that very domain. A field automorphism takes the members of a field and permutes them in such a way that its operations are preserved under the permutation. For a field extension like $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$ what we are interested in are automorphisms that take each member of the original field to itself, but that may permute objects in $\mathbb{Q}(\sqrt{2})$ which are not in $\mathbb{Q}$. In this case, it turns out that there are only two field automorphisms. First, there is the identity automorphism I that takes each number to itself, so in particular it takes $\sqrt{2}$ to $\sqrt{2}$. But there is also a field automorphism T that takes $\sqrt{2}$ to $-\sqrt{2}$. It also takes $-\sqrt{2}$ to $\sqrt{2}$. It permutes the two numbers. As all the members of $\mathbb{Q}(\sqrt{2})$ can be represented as $a + b\sqrt{2}$, knowing what the automorphism does with $\sqrt{2}$ is sufficient to determine what it does to any member of $\mathbb{Q}(\sqrt{2})$.

Now we are in a position to appreciate the genius of the Galois theory approach. For each field extension, there is a collection of field automorphisms. These automorphisms themselves form a group. A group is a domain with a single operation $\cdot$ defined on it obeying the three following conditions: the operation is associative, there is an identity element e and there is an inverse for each element in the group. We get a group from our two field automorphisms I, T if the group operation is the composition of two automorphisms. So, in this case, the group of field automorphisms turns out to be isomorphic to a group known as S_2. This is the permutation group of two objects. It itself has 2 members that can be represented as: I: $1 \mapsto 1, 2 \mapsto 2$, T:

6. See especially [31], part I, §1, ch. 4 and [24].
7. It also must be the case that $a(b+c) = ab + ac$. See [26], pp. 164-165 for the full definition.

$1 \mapsto 2, 2 \mapsto 1$. So, we see that $I \cdot I = I$ and $T \cdot T = I$.

An understandable reaction to the observation that the field automorphisms of a field extension form a group is to ask what this has to do with whether or not a polynomial is solvable by radicals. The final piece of the puzzle is to notice that the roots of an equation can be used to determine a field extension. To see how, look back at (2). The roots of this polynomial are $\pm\sqrt{2}$ and they lie outside of $\mathbb{Q}$. But now consider $\mathbb{Q}(\sqrt{2}) : \mathbb{Q}$. The roots are in this field extension because we added $\sqrt{2}$ to $\mathbb{Q}$ and so have obtained a field that has both $\pm\sqrt{2}$. It turns out that whether or not an equation is solvable by radicals in our original sense is determined by what field extensions of this sort there are. The case of the most relevance is when we take our starting field like $\mathbb{Q}$ and generate a series of field extensions where at each stage we add a single object. We will say that a field extension is a *radical extension* if each object that we add has the following feature: if α_i is added at stage i, then for some number b, α_i^b is already in the field at stage $i-1$. In our example, the starting stage 0 field is $\mathbb{Q}$ and $\sqrt{2}$ is added at stage 1 to obtain $\mathbb{Q}(\sqrt{2})$. This is a radical extension because $(\sqrt{2})^2$ is in the stage 0 field. More generally, the quadratic formula tells us that adding $\sqrt{a_1^2 - 4a_2a_0}$ is sufficient to obtain a field that contains the roots of the equation. Such an extension will always be a radical extension as $a_0, a_1, a_2 \in \mathbb{Q}$ guarantees that $(\sqrt{a_1^2 - 4a_2a_0})^2 \in \mathbb{Q}$.

This suggests that an equation is solvable by radicals just in case there is a radical extension of $\mathbb{Q}$ that includes the roots of the equation. We have recast the original problem, then, in terms of the existence of a certain sort of field extension. A surprising fact is that we can use the group of field automorphisms of a specified field extension to determine whether or not that field extension is a radical extension. For the quintic, there are some equations that we can determine do not involve a radical extension of $\mathbb{Q}$. Suppose the roots are $t_1, \ldots, t_5$. Then the field extension we are interested in is $\mathbb{Q}(t_1, \ldots, t_5) : \mathbb{Q}$.[8] As all field extensions have an associated group of field automorphisms, we can then consider that group, known as the *Galois group*. In some cases we can show that the group is S_5.[9] This is the group of permutations of five objects. It has $5! = 120$ elements. We can then examine the subgroups of S_5 and show that these subgroups correspond to field extensions $\mathbb{Q}(t_1, \ldots, t_5) : M$. In each case, M is an *intermediate* field obtained by adding a finite number of objects to $\mathbb{Q}$ so that M is contained in $\mathbb{Q}(t_1, \ldots, t_5)$. It is remarkable that even though the collection of all these intermediate fields is extremely hard to get a handle on directly, the link between the field extension, the intermediate fields, the Galois group and its subgroups provides the necessary traction. The basic idea is that a subgroup of the Galois group of a field extension will leave more objects fixed than the entire Galois group, which fixes $\mathbb{Q}$. So, we can gain valuable information about the intermediate fields by looking at the subgroups of the Galois group.

The most difficult step in the proof is to show that a field extension whose Galois group is S_5 is not a radical extension. So, these fifth degree equations are equations that are not solvable by radicals. Galois theory isolates a property of these groups that is a necessary and sufficient condition for the associated field extension to be a radical extension. This property of groups is called "solvability". This allows one to show that whenever n is 5 or greater, there is a Galois group for some polynomial equation that is not solvable. The key is to show that there must be a group that is isomorphic to S_n. Somewhat surprisingly, the crucial property that all these S_n groups have in common, when $n \geq 5$, is that they have a subgroup A_n that is not the size of a prime number. The size of each S_n group is $n!$ and the size of each subgroup A_n is $n!/2$. If $n \geq 5$, then $n!/2$ is not prime. In some sense, this is the ultimate reason that (B) holds. The size of these subgroups is important because for a group to be solvable we require a sequence of subgroups of a special kind ("normal") leading from the whole group S_n to 1. If S_n is part of such a sequence, then so is A_n. But when $n \geq 5$,

8. Or more carefully, we are interested in a field extension $\Sigma : \mathbb{Q}$, where Σ contains $\mathbb{Q}(t_1, \ldots, t_5)$.

9. See [26], §15.2.

we can show that the A_n sequence is not of the special kind. This is because both (i) none of the A_n have the right sort of subgroup, so they are "simple" and (ii) none of the A_n are of size p, for some prime p.[10]

The Galois theory proof illustrates the distinction between conceptual and computational mathematics. The proof depends on the existence of a Galois group for each polynomial equation, but the crucial features of this group cannot be readily computed from the known coefficients of the equation. Instead, the important properties of the Galois group are determined by the unknown roots of the equation. So, at least at a basic level, we can only know that a given polynomial equation is unsolvable by radicals if we already know what the roots of the equation are like! This shift in the setting for the problem was already clear in Galois' own work and may be the source of the critical reactions that it received. For example, Poisson, writing as a referee for a paper by Galois called "On the Conditions of Solvability of Equations by Radicals", complained that

> [The memoir] does not contain, as [its] title promised, the condition of solvability of equations by radicals ... one could not derive from it any good way of deciding whether a given equation of prime degree is solvable or not by radicals (given at [27], p. 106).

10. See [26], pp. 146-148.

The condition for solvability is not given in computational terms, but only in novel conceptual terms involving a group. This suffices to show that unsolvable polynomials exist, but leaves their coefficients a mystery. There is evidence that Galois himself appreciated the radical change in approach found in his work. He exhorts "future mathematicians" to "go to the roots of these calculations! Group the operations. Classify them according to their complexities rather than appearances."[11] Summarizing this shift with reference to Galois and Jordan, Gray notes the "expression of a preference for structural conceptual answers over computational ones" ([11], p. 236).[12] Gray concludes that this preference has epistemic significance for nineteenth century mathematics: "the new conceptual and aesthetic criteria have often achieved paramount position at the level of explanation, overthrowing mere calculation as the best criteria for truth" ([11], p. 239). It remains for us to consider what sort of explanation the Galois theory proof could provide.

My proposal is that the Galois theory proof explains because there is a special sort of dependence relation between facts about groups and facts about polynomial equations. This suggestion is a generalization of Salmon's ontic conception of explanation to those cases where causal relations no longer apply. As Koslicki has recently put the point, "an explanation, when successful, captures or represents (...) an underlying real-world relation of dependence of some sort which obtains among the phenomena cited in the explanation in question" ([17], p. 212). In our case the phenomenon is the distribution of solvability properties among polynomial equations. The explanation picks out the right groups and the appropriate group-theoretic property and shows how these facts are responsible for the features of the equations. This

11. Given at [15], p. 92. See also [32], pp. 102-104.
12. A footnote here states that Dedekind was the "leading German exponent of this point of view ... while the more algorithmic point of view, emphasizing explicit permutations, was kept alive by Kronecker". That is, even within Galois theory itself, the conceptual versus computational battle was waged. See [15], pp. 125-133 for some further discussion.

proposal gives rise to a number of additional questions about the metaphysics and epistemology of these dependence relations. I will return to some of these questions after a discussion of the alternative theories offered by Steiner and Kitcher. Even at this preliminary stage, one can argue that their accounts are unable to accommodate our Galois theory case.

3. Steiner and Kitcher

Galois theory is presented in Steiner's "Mathematical Explanation" as a potential counterexample to Steiner's own proposal for what is required for a mathematical explanation in pure mathematics. Steiner first argues that the abstraction or generality of a proof is not the key to its explanatory power. Instead, "an *explanatory proof* depends on a characterizing property of something mentioned in the theorem: if we 'deform' the proof, substituting the characterizing property of a related entity, we get a related theorem" ([25], p. 147). A characterizing property uniquely picks out the object from some contextually specified family of objects. But merely picking out the object by this sort of property is not sufficient: "One must be able to generate new, related proofs by varying the property and reasoning again" ([25], p. 151, fn. 12). So, a "*generalizable* proof" is explanatory, where the generalizability of the proof depends on its being a member of a collection of proofs that are connected by the deformations of a characterizing property. We can see Steiner as offering a further refinement of our ontological dependence proposal. For Steiner, dependencies require that a family of proofs result from transforming a characterizing property of an entity mentioned in the original theorem.

An objection (ascribed to Feferman) is that the Galois theory proof is explanatory even though it does not fit into Steiner's account. Steiner first argues that his account can make sense of the Galois theory proof of (B). This is because he takes it to involve "the general polynomial equation" of degree n, which is uniquely characterized by a Galois group. However, Steiner grants that problems arise when we turn to particular equations because now many different equations share the same Galois group. As Steiner puts it, "an arbitrary equation with rational coefficients has not a unique Galois group, in the sense that no other equation has it (though it is, of course, the only Galois group of the equation)" ([25], p. 149). More generally, "the contemporary style is to study domain X by assigning a counterpart in domain Y to each object in X" ([25], pp. 149-150). Steiner responds by weakening his account to allow partial characterization: "The Galois group of E characterizes it in that the properties of the group tell us much about E" ([25], p. 150). However, as Steiner recognizes, he must do more to deflect this objection. He must also link this partial characterization of E in terms of its Galois group to an appropriate collection of proofs. It is here that I believe the limitations of Steiner's approach to mathematical explanation become clear. All Steiner says is "'Deforming' a proof in Galois theory produces results linking a new Galois group to any equation with that group – but we still must look for equations *having* the group (an unsolved problem in general)" ([25], p. 150). What he seems to have in mind is that we can move from the proof that (B) to the proof that some equations with Galois groups besides S_5 are solvable or unsolvable based on the appropriate features of these new groups. This fits with our earlier interpretation that Steiner's notion of dependence requires the existence of an appropriate family of proofs. The problem with this proposal is that the explanatory power of the Galois theory proof of (B) does not hinge on the existence of this family of proofs. As Steiner notes, there is no effective means to move to a new Galois group and determine the polynomial equations associated with it. So there is no family of proofs that can be generated along the lines that Steiner requires. I conclude that this sort of explanatory proof is explanatory in its own right. Whatever dependence relations it describes are not relations that require the existence of a family of proofs.

This sort of objection to Steiner is not a new one. In their thorough analysis of Steiner's account, Hafner and Mancosu develop a counterexample based on an explanation offered by Pringsheim for a test on the convergence of series of the form Σa_n. The test involves a sequence (B_n) that is arbitrary. For this reason, "one couldn't base any proof on a characterizing property of (B_n) ...Consequently, Steiner's account renders [Pringsheim's proof] non-explanatory because it fails to satisfy a necessary condition for explanatoriness" ([12], p. 230). Of course, Steiner might reply that this particular proof is not explanatory, but this response runs up squarely against Pringsheim's own claim that his proof is explanatory ([12], p. 229). An advantage of considering the Galois theory proof of (B) is that Steiner grants that our proof is explanatory, so we have the means to overcome this potential standoff. The problem that Hafner and Mancosu point to is that a proof may be explanatory because it depends on an arbitrary object of some kind. Our Galois theory proof involves a new kind of entity beyond those mentioned in the theorem. The appeal to this sort of entity is explanatory even when there is no method of deforming the proof. Both sorts of explanations are missed by Steiner.

A second influential account of mathematical explanation has been developed by Kitcher. He claims that a given argument or proof is explanatory if it appears in the collection of arguments or proofs that best unifies the domain K of the theory. Ultimately, Kitcher's goal is to define causal and other dependence relations in terms of the explanations that are found at an ideal "end of science" ([16], §8.3). The key tool for this task is the notion of the explanatory store for some accepted claims K at some stage of science. The explanatory store over K, $E(K)$, is a special collection of schematic argument patterns (with associated filling instructions) that is sufficient to derive all of K ([16], p. 432). There are many subtleties to Kitcher's approach, but for our purposes he can be seen as making one decisive error. Kitcher ignores the crucial shift from the computational to the conceptual so he has problems with Galois theory. In the case of the Galois theory proof of (B), there is little reason to think that adding the proof improves the explanatory store. That is, the proof is not part of the most unified family of proofs of the sort envisioned by Kitcher. If so, then Kitcher has no positive account of the widely accepted judgment that the Galois theory proof is indeed explanatory.

In his brief discussion of this case, Kitcher begins with Lagrange's work on the methods of solving polynomials of degrees 2, 3 and 4. He claims that

> After Galois, we have a criterion for the expressibility of roots as rational functions of coefficients, to wit the solvability of the Galois group of the equation, and we can see just why this applies in the four special cases. Nonexplanatory special derivations *give way* to an explanatory proof drawn from a general theory about the properties of classes of equations ([16], pp. 425-426, emphasis added).

The key to appreciating the problems for Kitcher's account is to distinguish some different explanatory questions. The known answers to these questions correspond to different members of K. At its most concrete, we have (i) particular claims about the roots of particular polynomial equations. Two examples are "The roots of (2) are $\pm\sqrt{2}$" and "The roots of (3) are $\pm i$". Beyond these explicitly solved polynomials, we have members of K that claim (ii) that a particular equation is solvable by radicals. Moving further in the direction of abstraction, there are claims that (iii) all equations of some fixed degree are solvable by radicals. Then we have the claim (A) which appears to cover the "four special cases" Kitcher mentions ($1 \leq n \leq 4$). In addition there is the claim (B). Prior to Galois or anything approaching Galois theory mathematicians had available the formulae for degrees 2, 3 and 4. Lagrange and Abel then added a unified treatment in terms of permutations and Abel's proof of (B). Now it seems clear that the formulae for degrees 2, 3 and 4 by themselves provide a highly unified explanatory store for all claims of type (i), (ii) and (iii). Kitcher's criteria generate three schematic arguments with precise filling instructions that specify how the roots are to be determined using the appropriate formula. An additional general argument is needed to prove (A). This very argument was extended by Abel when he provided the materials necessary to prove (B). So four schematic argument patterns are sufficient for this K.

To evaluate Kitcher's approach we must see how things are changed with the Galois theory proof of (B). Despite what Kitcher suggests, the Galois theory proof of (B) does not supplant the three schematic arguments that are used to derive claims of type (i), (ii) and (iii). For while it is true that “we have a criterion for the expressibility of roots as rational functions of coefficients" and “we can see just why this applies in the four special cases", this insight does not remove the need for the formulae if we wish to account for the specific roots of particular equations. These derivations using the formulae do not “give way" to the Galois theory proof of (B). The formulae are still needed to derive some members of *K*. The only improvement that I can see in terms of Kitcher’s framework is that (B) is proven directly, without an appeal to the proof of (A) via the formulae for degrees 2, 3 and 4. So, the best that can be said for the addition of Galois theory with respect to these claims is that it reduces the number of argument schema by one. But even this gain seems somewhat illusory. A simple recasting of the explanatory store over *K* prior to Galois theory could present Abel’s proof of (B) as a single argument, which includes (A) as a lemma. The basic problem is that what has changed with Galois theory is not the number of argument schema used to unify our beliefs *K*, but the character of this collection of beliefs. I aim to analyze this change in character in terms of the objective dependence relations mentioned above. Kitcher’s attempt to dispense with these relations by appeal to his notion of unification is not successful.

Tappenden has put the main objection succinctly in his discussion of Kitcher: “successfully identifying unifying generalities is assessed not by counting the total number of patterns but rather by the quality of the patterns themselves: Are they the *right* ones (are they deep or fruitful or revealing or whatever?)" ([28], p. 169). Hafner and Mancosu make a related criticism based on a theorem about polynomials on real closed fields. A decision procedure exists that establishes the result for each polynomial, but mathematicians criticize the use of such a procedure as less explanatory than some alternative methods. However, the decision procedure leads to an explanatory store with a single argument schema, whereas the alternative methods must invoke more than one argument schema: “Kitcher’s model ends up positing as the best systematization one which in practice does not enjoy the properties of explanatoriness that Kitcher’s model would seem to bestow upon it" ([13], p. 166).[13] All this strongly suggests that we must look beyond Kitcher if we are to make sense of the value of abstract explanations like the Galois theory proof of (B).

13. See also [13], pp. 157-158 where Kitcher’s remarks about Galois are noted.

4. Abstract dependence

What is distinctive about a conceptual approach to a mathematical problem is that it picks out a new kind of entity whose features are central to the solution of the problem. When the features of this kind of entity can be shown to be crucial to the proof of the theorem in question, then practitioners often conclude that they have found an explanatory proof. The features that I have emphasized in the Galois theory proof are the way that the new entity permits the determination of a necessary and sufficient condition for the central property mentioned in the theorem. As I will put it, we obtain a novel and informative classification of polynomial equations. The equations that are solvable by radicals are precisely those whose Galois group is solvable. Recall that the solvability of a group is tied to its decomposition into subgroups. This seemed to have nothing to do with polynomial equations, but the proof makes the link manifest.

There are two different questions about explanatory proofs that must be answered by any acceptable theory of mathematical explanation. First, what makes a given proof explanatory?[14] This question is answered by pointing out the sort of thing that explanations are. It is what might be thought of as the metaphysical question for explanation. Second, how do practitioners comes to know that they have an explanation? On most theories of explanation, what makes something an explanation can depart from the evidence that scientists and mathematicians have at their disposal. Someone might think they have an explanatory proof and turn out to be wrong because their evidence was not conclusive. This epistemic question about explanation is often much more difficult to answer than the metaphysical question. Delicate judgments based on expertise may be involved in determining that something actually fits the metaphysical theory of explanation.

As noted above, I aim to defend an ontic theory of mathematical explanation. In a case like the Galois theory proof, what makes the proof explanatory is that it describes a dependence relation that obtains between the groups and the polynomial equations. What makes a given polynomial equation solvable, we should say, is that its Galois group is solvable. It is difficult to analyze what this dependence comes to in simpler terms. For example, we cannot say that the dependence is cashed out in modal terms. Whatever is true in mathematics is arguably metaphysically necessary. So, we cannot say that if the group S_5 had been solvable, then some polynomial equation would have been solvable. If S_5 actually fails to solvable, then it must fail to be solvable. Philosophers such as Kit Fine and Koslicki have pursued a different strategy tied to the essence of a thing (or kind of thing).[15] What it is for a thing to be lightning is for that thing to be composed of electrons. It is part of the essence of lightning, we could say, for it to be made up of electrons. This kind of essential dependence between lightning and electrons cannot be reduced to modal relations between the two. Nevertheless, it seems to be a genuine relation that we should accept as part of our theory of the world. However, even this well-worn path does not seem suited to the dependence relation that obtains between a group and a polynomial equation. A polynomial equation is not composed of the group. Indeed, it does not seem to be part of the essence of either entity that it be related to the other. This situation presents us, then, with a difficult choice. One option is to posit a new kind of dependence relation that can obtain in the absence of any essential composition relation. This is the option that I will pursue here. Another option (that I do not explore here) would be to question the ontic approach to explanation and explore some alternative.

It would be premature to propose a theory of a new sort of dependence relation on the basis of one case. Instead, I will only outline a theory and argue that it can be made consistent with this case.[16] The theory is inspired by Frege and Detlefsen's insightful discussion

14. I here ignore the question of what makes one explanatory proof more or less explanatory than another explanatory proof.

15. For a helpful survey of this growing literature, see [6].

16. In the next section I will also argue that this theory can be made consistent with another case discussed by Steiner. I am grateful to an anonymous referee for pressing me for more of the metaphysical details of this relation.

of some problems that Frege runs into ([8]).[17] Frege's interest in the distinction between explanatory and non-explanatory proofs is clear in the opening sections of his *Foundations of Arithmetic*. He says, for example, "The aim of proof is, in fact, not merely to place the truth of a proposition beyond all doubt, but also to afford us insight into the dependence of truths upon one another" ([10], §2). Frege's logicism includes the claim that all the truths of arithmetic ultimately depend on the truths of logic. Detlefsen analyzes this notion of dependence or grounding in terms of the "*whole* or *complete* source of truth" ([8], p. 115, fn. 6). This leads him to conclude that "*uniqueness* seems to be a necessary feature of grounding" as "It simply cannot be that p's truth both arises (wholly) from g and also (wholly) from g'; rather the one excludes the other" ([8], pp. 104-105). But if grounds for p are unique, then a proof that yields p need not only involve some sufficient conditions for the truth of p. It must also be the case "that a ground for a proposition is, in some sense, a necessary condition for it" ([8], p. 105). That is, p and its total grounds q must be so tightly linked that no other truths besides q stand in this special grounding relationship to p. q is responsible for the truth of p in this strong sense.

Detlefsen goes on to argue that these demanding conditions cannot be met with the tools that Frege had at his disposal. In particular, the "global conception of logic" ([8], p. 106) that Frege deploys is not sensitive enough to isolate the grounds of the truths of arithmetic. It would take us too far afield to summarize this objection to Frege's project. Instead, I will propose an alternate route to obtain the tight link between a truth and its grounds. The heart of this proposal is the existence of biconditionals that link facts of type X to facts of type Y. Schematically, I will represent a fact of type X with constituent x using "$X_i(x)$", where "i" is an index used to distinguish that fact from another fact of that type. In special cases it turns out that (i) for any x, y, given $R(x,y)$, $(X_i(x) \leftrightarrow Y_j(y))$. That is, for a suitably constrained set of facts of type X and type Y, once the R relation obtains between two appropriate objects, facts of those sorts are paired up in the following sense. One such fact obtains just in case a fact of the other type obtains. This suggests that an objective dependence relation obtains between facts of type X and facts of type Y. Clearly, when all the R relations are in place, the X fact is sufficient for the Y fact to obtain. But there is also a sense in which the X fact is necessary for the Y to obtain. That is the force of the biconditional.

Still, the truth of this sort of biconditional is not enough to establish a grounding or explanatory relationship. For there might be other biconditionals of just that sort linking facts of these types to facts of some other type Z. Consider, for example, (ii) for any x, z, given $S(x,z)$, $(X_i(x) \leftrightarrow Z_k(z))$ and (iii) for any z, y, given $T(z,y)$, $(Z_k(x) \leftrightarrow Y_j(y))$. If facts are individuated in an appropriately fine-grained way, we can have mathematical cases where (i), (ii) and (iii) all obtain. How, then, should we single out one of these biconditionals as the one that reflects a grounding relationship? And which side of the biconditional is grounding or explaining, and which side is being grounded or explained? It is here that logical or formal tools must give way to assumptions about the facts themselves and their relationships. Here is a proposal. First, suppose that we wish to fix the explanatory grounds of facts of type Y with constituents y. I will say that each collection of type X facts that are mentioned in the true biconditionals of form (i) noted above constitute some *potential* explanatory grounds for the Y facts. To choose between these potential grounds I invoke a notion of abstractness. That is, one object can be more abstract than another. The explanatory grounds will be given by facts of type X whose constituents x are *more* abstract than y but *less* abstract than objects z drawn from any other potential explanatory grounds.[18] So, the idea is that the unique

17. See also [5]. Another important figure for these debates is Bolzano, but I lack the space to engage with his work here. See especially [21] and [4].

18. An alternative route to securing uniqueness would be to choose potential explanatory grounds whose constituents are the most abstract. I cannot compare these two options here.

explanatory grounds for facts of type Y are the least more abstract domain of facts where an appropriate biconditional obtains.[19]

For this proposal to work, objects must be partially ordered by their abstractness. To clarify this ordering, I draw on the broadly structuralist thought that some objects can have other objects as instances. When a has b as an instance, I say that a is more abstract than b. The instantiation relation here is irreflexive, asymmetric and transitive. Perhaps the clearest case of what I have in mind is the type-token relationship. A letter type like “E" has particular inscriptions as its instances. So, in the stipulated sense, that type is more abstract than its tokens. Part of what it is for certain objects to be the objects that they are is that they can stand in these instantiation relations to other objects. When b is an instance of a, b has all of a's properties of a given sort, but some additional properties as well. The tokens of “E" have all of the type's shape properties, and also additional properties such as spatial locations. Some of the type's properties fail to carry over to its tokens, such as the type's failure to have a spatial location. Nevertheless, we can explain features of the token by appeal to the type. Another example is offered by the view that distinguishes between the universal version of some quality and the particularized version of that quality as it is realized in a given substance. On this view, the universal humanity has Socrates' humanity as an instance. Accordingly, I would say that the universal is more abstract.

It remains to be shown how this theory of abstract dependence can be made consistent with our Galois theory case. To reconstruct the proof in a way that fits into this theory, I note first that the proof links facts about groups to facts about polynomial equations. But we cannot say that polynomial equations are instances of groups. Each polynomial equation gives rise to a field extension, and each field extension determines a collection of automorphisms. I claim that each collection of automorphisms is an instance of a group. So, in our stipulated sense, groups like S_5 are more abstract than the associated collection of field automorphisms. To be a group, on this view, just is to satisfy the group axioms. S_5, a particular group, just is the abstract structure that involves the group operation taking its inputs to the required output in the right way. The collection of field automorphisms has all these group-theoretic properties, but has additional properties linked to the elements being automorphisms of that specific field extension.

I claim that the Galois theory proof makes an appeal to entities that are more abstract than the entities involved in the theorem. Each Galois group is more abstract than the collection of automorphisms of a field extension, and the theorem is about these field extensions. It remains to show that the proof involves the right sort of biconditional between facts of the appropriate sort. As I emphasized in my discussion of the proof, there is a necessary and sufficient condition for each polynomial equation to be solvable by radicals. This is that the associated group be solvable. Let $R(x, y)$ be the relation that obtains just in case x is the Galois group of polynomial equation y. The fact that x is a solvable group will be abbreviated as $X_i(x)$, where i is the index for that fact, as above. The fact that y is a polynomial equation that is solvable by radicals will be abbreviated by $Y_j(y)$. The key to the proof is the claim that, for suitably delimited facts X_i, Y_j, for all x, y, given $R(x, y)$, $(X_i(x) \leftrightarrow Y_j(y))$. In words: whenever x is the Galois group of polynomial equation y, x is a solvable group if and only if y is solvable by radicals.

The main difficulty in showing that our theory makes the Galois theory proof explanatory is that there still might be an appropriate biconditional involving a kind of object that is more abstract than the collections of field automorphisms and yet less abstract than groups. This involves controversial issues about mathematical existence. It is surely possible to define a problematic intermediate entity. But the theory just articulated requires that if the proof is explanatory, then no such entities will exist. Here we see the gap between the requirements of a theory of the abstract dependence relation and our knowledge

19. I will say that a domain of facts X is more abstract than a domain of facts Y when each X_i has a constituent that is more abstract than any constituent of a Y fact.

that these dependence facts actually obtain. I hope it is clear what the theory is, and what it requires to certify this proof as an explanatory proof. The epistemic matters are subtle, and I turn to them now.

The formulation of the Galois theory proof involves the discovery of a novel and informative classification of solvable polynomial equations. It would be a mistake to say that this feature is part of what makes the equations depend on the groups. For this feature is clearly tied to the particular epistemic situation of a community of mathematicians. The dependence relation we are trying to characterize is thought to be mind-independent, in line with other kinds of ontic explanations. What we should say, then, is that when a proof provides a novel and informative classification of the topic of the theorem, then this is evidence of an underlying dependence relation. This is the first step towards filling in the epistemological side of an account of explanatory proof. It is a small step, though, as it is not yet clear how this sort of classification could be evidence for an abstract dependence relation.

What is needed is a more general discussion of the prospects for some sort of inference to the best explanation in these sorts of cases. The possibility of this kind of inference has been noted by Mancosu (drawing on Feferman). Mancosu presents, but does not endorse, the following kind of argument:

> 1. There are scattered results (...) which call for an explanation.
> 2. Such an explanation is obtained by appealing to more abstract entities (...).
> 3. We thus have good reason to postulate such abstract entities and to believe in their existence ([22], p. 139).

What is in question in our case is not the existence of groups. Instead, we take the explanation to require that there be some dependence relation between groups and field extensions. Part of the evidence that this relation obtains is the goodness of the explanation that would result if it did obtain. Inference to the best explanation is a controversial mode of inference in science. But if suitably clarified, it seems like it is well-suited to fill out the epistemology of our abstract dependence relations.

Another strategy is to revisit the comparative judgments that mathematicians have made throughout history. This should provide additional materials for a theory of how we come to know that one proof is more explanatory than another. And if an explanatory proof describes objective dependence relations, then this historical investigation will inform an epistemic account of how we come to know about these relations. The basic idea is that a proof that exploits genuine abstract dependence relations will exhibit a range of desirable features. We can then infer that the relation obtains when we observe these desirable features.

An intriguing philosophical analysis of the contrast at the heart of our case is given in Keränen's dissertation *Cognitive Control in Mathematics* ([14]).[20] Keränen discusses what he calls the "cognitive control" achieved by Artin's version of the Galois theory proof. The starting point for the discussion is Abel's proof of the same theorem. We can use Keränen's investigations to inform an epistemology of dependence relations.[21] In particular, Keränen emphasizes the difference between an informed engagement with Abel's and Artin's proofs. While both proofs are successful, reflection on the two proofs indicates that Abel exhibits a lesser degree of cognitive control than Artin. Keränen develops a rich vocabulary to analyze what this comes to, but the basic idea is that Artin structures his proof around concepts and results that guide the reader towards the result. By contrast, the concepts and results that Abel deploys leave the reader unsure about the next step and the proof's overall chances of success.

Two of the notions that Keränen deploys in his analysis of cognitive control are epistemic option and epistemic guidance. Given the fixed aim of proving some particular theorem, two mathematicians

20. I am grateful to Douglas Marshall for emphasizing the importance of this dissertation for my project. It appears that Keränen has not yet published any of these ideas in a more accessible form.

21. Keränen expresses nominalist sympathies, so he is unlikely to accept our notion of abstract dependence ([14], p. 77).

may still have wildly different epistemic options. These options are the ways to attempt the proof that are left open by the agent's background knowledge and representational abilities ([14], p. 140). An agent may have a better or worse representation of their epistemic options. In particular, one mathematician may have a surveyable representation of how to proceed to prove a theorem, while another mathematician may not be able to survey their options. A superior representation of epistemic options affords a mathematician a higher degree of epistemic guidance. This guidance is something a reader of the proof can detect and use to assess the overall level of cognitive control. Keränen argues that the conceptual approach exhibited by Artin contributed to the high level of epistemic guidance that is manifest in his proof. By contrast, Abel's impoverished conceptual resources led him to focus on symbolic manipulations and computations that decreased the level of epistemic guidance shown in his proof.

What Keränen offers, then, is a range of features that can be used to distinguish proofs of the same theorem. His notion of cognitive control is interesting in its own right, but it could also inform an epistemology for dependence relations. The key additional element needed to make this link is the idea that a proof exhibits cognitive control because it is highly likely to be exploiting some objective dependence relation between the mathematical domains being discussed. This is an idea that seems to be reflected in the informal remarks of some mathematicians. For example, we began with Dedekind's remark that "It is preferable, as in the modern theory of functions, to seek proofs based immediately on fundamental characteristics, rather than on calculation, and indeed to construct the theory in such a way that it is able to predict the results of calculation." One way to take this is in epistemic terms: if we can predict and control the results of calculations, then this is evidence that we have found the fundamental characteristics of the problem. But whether or not this idea can be cashed out in convincing terms must be reserved for future work.

From this perspective, the accounts offered by Steiner and Kitcher confuse the evidence for having found an explanatory proof with what makes a proof explanatory. When a proof is generalizable, then that is evidence that there is an underlying dependence relation, but the generalizability is not what makes the dependence relation obtain. Analogously, when a proof is part of an appropriately unified explanatory store, in Kitcher's sense, that is also evidence that a dependence relation obtains. But we do not need to follow Kitcher and attempt to define the dependence relation in terms of the existence of some explanatory store.[22]

22. This approach could also allow for negative indications of dependence. For example, Baker has argued that "other things being equal – disjunctiveness is negatively correlated with explanatoriness in the context of proof" ([3], p. 148). See also [19] for a similar conclusion. In our terms, a highly disjunctive proof is defeasible evidence that the proof is not exploiting genuine dependence relations.

5. Improved setting

One interesting consequence of an abstract explanatory proof is the suggestion that the proof offers an improved setting for addressing the problem in question.[23] In our case, what initially seemed to be a well-defined problem concerning the solution of polynomial equations takes on a quite different flavor when approached via Galois theory. It is tempting to say that what mathematicians were talking about all along was groups of field automorphisms. This would be quite implausible, though. At least in those cases where we have an independently identified subject-matter like polynomial equations, the improved setting does not displace the original topic of the theorem. Instead, mathematicians learn the value of tackling these old problems in this new way. Our account of abstract mathematical explanation is able to handle this feature of the practice because the abstract dependence relations I have invoked do not require a wholesale reinterpretation. Y facts can abstractly depend on X facts while the X facts retain their autonomy. For example, to say that a polynomial equation is solvable by radicals does not require the mention of any facts involving groups.

To show the value of the notion of improved setting just outlined I will briefly consider a new case. This also provides a sort of test case for our account of abstract dependence. This case involves a proof that there are only five regular convex polyhedra. It is discussed by Steiner, who grants that it is an explanatory proof and who also insists that his "theory illuminates, aside from explanation, the notion of relevance in mathematics" ([25], p. 146). Unfortunately, Steiner distorts the case to some degree in order to make it fit into his account of mathematical explanation. But once it is presented in an undistorted way, it is possible to see how the link between explanation and improved setting works. The theorem in question is

(C) An object is a regular convex polyhedron if and only if it is a tetrahedron, octahedron, cube, icosahedron or dodecahedron.

23. See [30] for further discussion of some of these issues.

A regular convex polyhedron is a closed three-dimensional object whose faces all have the same number of edges, and whose edges all have the same length.[24] The original setting for the problem of the existence of regular convex polyhedra is Euclid's metric, solid geometry. Euclid offers a proof of (C) that involves the size of the angles which would be required for any sixth polyhedron.[25] As Steiner summarizes it, Euclid's proof involves the claims that "the sum of the angles around any vertex must be less than $360°$, that it takes three polygons to form a vertex, and that regular polygons of six or more sides require angles of $120°$ or more" ([25], p. 146). For example, suppose we considered a regular polyhedron composed of hexagons. Each vertex must connect at least three hexagons. A geometric calculation shows that the interior angles of a hexagon are each $120°$. So, each vertex must have a total angle of at least $360°$. But this violates the theorem that the total angle around any vertex is less than $360°$. Similar reasoning rules out a regular polyhedron made of polygons of any greater number of sides. Based on this proof it seems clear that the original setting for (C) involves metrical considerations about the size of angles, the length of sides, and so on.

Steiner relates a proof that suggests a more abstract, improved setting. This proof involves Euler's theorem that for any polyhedron that can be continuously transformed into a sphere,

$$V - E + F = 2 \tag{6}$$

Here V is the number of vertices, E is the number of edges and F is the number of faces.[26] As the notion of continuous transformation indicates, this theorem involves an abstraction away from the metrical

24. A convex polyhedron includes the lines that connect any two vertices. The challenges posed by non-convex polyhedra are central to [18], esp. §1.8.
25. *Elements*, book 13, prop. 18, remark.
26. Steiner does not give a reference for this proof, but my exposition follows [7], p. 240.

properties of a polyhedron and considers only its topological properties. So, in this sense, a sphere is more abstract than a polyhedron because many different polyhedra are topologically equivalent to a sphere. Euler's theorem and some additional assumptions about the relationship between V, E and F in a regular convex polyhedron are sufficient to prove (C). To start, we assume that a regular polyhedron is composed of polygons with n sides. Furthermore, we assume that at each vertex of such a polyhedron, r of the polygons meet. For example, a cube has $n = 4$ and $r = 3$. The first step of the proof is to express F and V in terms of E, n and r. Notice that the total number of edges is at most nF. But in fact every polygon shares an edge with exactly one other polygon so $nF = 2E$. Looking at r, we see that it tells us not only how many polygons meet at each vertex, but how many edges meet at each vertex. For example, with a cube, three squares meet at each vertex, and this requires that three edges meet at each vertex. So, the total number of edges is at most rV. But each edge has two vertices, so $rV = 2E$. This allows us to obtain,

$$F = \frac{2E}{n}, \; V = \frac{2E}{r} \tag{7}$$

Making the substitution into (6) yields

$$\frac{1}{n} + \frac{1}{r} = \frac{1}{E} + \frac{1}{2} \tag{8}$$

Of course, n, r and E are restricted to the positive integers. And we know that both n and r are at least three. Investigation of (8) subject to these conditions shows that the only admissible values of $\{n, r\}$ are $\{3,3\}$, $\{3,4\}$, $\{3,5\}$, $\{4,3\}$, $\{5,3\}$. To see why, notice that n and r cannot both be greater than 3. In such a case, the left hand side of (8) is at most $1/2$, while the right hand side of (8) must be greater than $1/2$. And if one of n or r is 3 and the other is greater than 5, then the left hand side of (8) is at most $1/2$. This violates the requirement that the right hand side of (8) is greater than $1/2$. So, an exhaustive list of the solutions of (8) is given by our list of the five values of $\{n, r\}$. These correspond to the tetrahedron, octahedron, icosahedron, cube and dodecahedron, respectively.

On my approach this proof of (C) is an abstract explanation. To see why notice that it involves a sphere. This is the entity whose features are used to isolate the possible regular polyhedra. We relate all potential regular polyhedra to the sphere using a topological transformation. This permits the application of (6). Using (6) and some additional assumptions about regular convex polyhedra, we are able to show that all and only the regular convex polyhedra have $n = 3, 4, 5$ and $r = 3, 4, 5$ such that the only combinations are the five given. That is, we use (6) and our understanding of n and r to specify a novel and informative classification of convex polyhedra (into regular and irregular). And once we find the admissible combinations of n and r, a simple calculation leads to the list provided by (C). So, this proof satisfies my conditions on being an abstract explanation. It should also be clear how this proof supports the conclusion that an improved setting for (C) is topological. We see that the calculations in terms of the angles that dominated Euclid's proof are besides the point.

It is less clear how this proof fits with the more tentative proposal for the details of the abstract dependence relation that I advanced in section 4. One problem is isolating an appropriate biconditional that links facts about spheres to facts about regular convex polyhedra. Let us start with a domain of facts X that each involve polyhedra x. Let the domain of facts Y involve only highly symmetric objects like circles and spheres of various dimensions. With x and y restricted in this way, we get biconditional (i): "Given that x is topologically equivalent to y, x is a convex polyhedron just in case y is a sphere". The proof proceeds by imposing the additional condition that the polyhedra be regular: (ii) "Given that x is topologically equivalent to y, x is a regular convex polyhedron just in case y is a sphere and x is formed by n-gons meeting r at a time at each vertex." This entails the theorem that (C) "x is a regular convex polyhedron just in case x is a tetrahedron, octahedron, cube, icosahedron or dodecahedron." This proof exhibits a few differences from the Galois theory case, but the basic pattern remains the same. We still have a domain of X facts that involve objects x, here polyhedra. There is also a domain of Y facts that involve objects y, now spheres. The $R(x, y)$ relation is just that x is topologically equivalent to y. On this analysis, the crucial biconditional is (i) and it has the required form "for any x, y, given $R(x, y)$, $(X_i(x) \leftrightarrow Y_j(y))$."

As with the Galois case, the more debatable issue concerns the relative abstractness of spheres and polyhedra. Are spheres really the least more abstract kind of object than convex polyhedra? We can certainly argue that spheres are more abstract than convex polyhedra. To be a convex polyhedron requires not only the topology of the sphere, but also additional metrical properties like having a face of some determinate area. This means that a given convex polyhedron has all the topological properties of a sphere, and some additional ones as well. It is harder to show that there are no objects that are more abstract than convex polyhedra and yet less abstract than spheres. Again, this involves difficult questions of mathematical existence. All that we have done is articulate a theory of abstract dependence and shown how it can be made consistent with this case. Additional work is needed to see if this is the best theory of abstract dependence and what alternatives might be available.

Steiner is eager to classify this proof as an explanatory proof in his sense and, as we have seen, also claims that the proof shows what is relevant to the theorem. But he takes an additional step that I would reject. Recall that Steiner's explanatory proofs must involve a characteristic property of an entity mentioned in the theorem. This leads him to conclude that even though a sphere is not explicitly mentioned in the theorem, it really does involve a sphere:

> Euclid's theorem proceeds from a characterizing property of an entity (the sphere) not mentioned overtly in the theorem itself. The properties responsible for there being no more than five regular solids do not uniquely characterize regular solids, since 'deforming' the solids does not 'deform' the theorem. Rather they characterize a topological space, and for this reason we say that Euclid's theorem is 'really' topological in character, and that any geometrical proof is 'irrelevant' ([25], p. 147).

However, it seems too quick to conclude that an explanatory proof of (C) that mentions a sphere shows that (C) is itself about spheres or topological spaces. On any reasonable conception of "about", (C) is about polyhedra. What seems to be driving Steiner to his unwarranted conclusion is his assumption that the explanatory proof must turn on a feature of an entity mentioned in the theorem. I have rejected that assumption. I retain Steiner's idea that the explanatory proof indicates what is relevant to the truth of the theorem, but have preferred to cash this out in terms of a difference between the original setting and an improved setting. Sometimes an improved setting for a theorem involves entities beyond those mentioned in the theorem.[27]

27. See [1] for a nuanced discussion of another case where it seems best to allow for an improved setting that goes beyond what the theorem is about.

6. Conclusion

In this paper I have presented one kind of explanatory proof. This is the Galois-theory proof of the unsolvability of the quintic. The main evidence that this proof is explanatory came from the judgments of mathematicians like Stewart and Liebeck. However, these judgments do not indicate what makes this kind of proof explanatory. I emphasized the way that the Galois-theory proof affords a novel and informative classification of the polynomial equations that are solvable by radicals. This distinctive feature created problems for the accounts of explanatory proof offered by Steiner and Kitcher. It also suggested an alternative approach in terms of abstract dependence relations. However, both the metaphysics and the epistemology of these dependence relations remains to be clarified. Above all, what is needed are additional cases where the claims of mathematicians and historians can be used to inform a more nuanced account of explanatory proof. One consequence of having an explanatory proof is the judgment that a theorem has been placed in an improved setting. It is possible that further investigation of the complex interactions between explanatory considerations and this notion of improved setting could pave the way for a more philosophically satisfactory understanding of modern mathematics.

Acknowledgments. Two quite different versions of this paper were presented at the 2010 meeting of the Association for the Philosophy of Mathematical Practice (Brussels) and the 2011 meeting of the Midwest PhilMath Workshop (Notre Dame). I am grateful to both audiences for their constructive and insightful suggestions. In particular, this paper benefitted from the feedback and encouragement of Andrew Arana, William D'Alessandro, Jamie Tappenden, Ken Manders, Paolo Mancosu and Douglas Marshall. In addition, this paper was considerably revised in light of the critical comments of two anonymous referees for this journal. I would like to thank them for their help in improving the paper.

References

[1] Andrew Arana and Paolo Mancosu. On the relationship between plane and solid geometry. *Review of Symbolic Logic*, 5:294–353, 2012.

[2] Jeremy Avigad. Methodology and metaphysics in the development of Dedekind's theory of ideals. In J. Ferreirós and J. J. Gray, editors, *Architecture of Modern Mathematics: Essays in History and Philosophy*, pages 159–186. Oxford University Press, 2006.

[3] Alan Baker. Mathematical accidents and the end of explanation. In O. Bueno and Ø. Linnebo, editors, *New Waves in the Philosophy of Mathematics*, pages 137–159. Palgrave Macmillan, 2009.

[4] Arianna Betti. Explanation in metaphysics and Bolzano's theory of ground and consequence. *Logique et Analyse*, 211:281–316, 2010.

[5] Tyler Burge. Frege on knowing the foundation. *Mind*, 107:305–348, 1998.

[6] M. J. Clark and D. Liggins. Recent work on grounding. *Analysis*, 72:812–823, 2012.

[7] Richard Courant and Herbert Robbins. *What is Mathematics?* Oxford University Press, 1941.

[8] Michael Detlefsen. Fregean hierarchies and mathematical explanation. *International Studies in the Philosophy of Science*, 3:97–116, 1988.

[9] Michael Detlefsen and Andrew Arana. Purity of methods. *Philosophers' Imprint*, 11(2):1–20, 2011.

[10] Gottlob Frege. *The Foundations of Arithmetic*. J. L. Austin (Trans.). Northwestern University Press, Second edition, 1980.

[11] Jeremy Gray. The nineteenth century revolution in mathematical ontology. In Donald Gillies, editor, *Revolutions in Mathematics*, pages 226–248. Oxford University Press, 1992.

[12] J. Hafner and P. Mancosu. The varieties of mathematical explanation. In P. Mancosu, K. F. Jørgensen, and S. A. Pedersen, editors, *Visualization, Explanation and Reasoning Styles in Mathematics*, pages 215–250. Springer, 2005.

[13] Johannes Hafner and Paolo Mancosu. Beyond unification. In Paolo Mancosu, editor, *The Philosophy of Mathematical Practice*, pages 151–178. Oxford University Press, 2008.

[14] Jukka Keränen. *Cognitive Control in Mathematics*. PhD thesis, University of Pittsburgh, 2005.

[15] B. Melvin Kiernan. The development of Galois theory from Lagrange to Artin. *Archive for the History of Exact Sciences*, 8:40–154, 1971.

[16] Philip Kitcher. Explanatory unification and the causal structure of the world. In Philip Kitcher and Wesley Salmon, editors, *Scientific Explanation*, pages 410–505. University of Minnesota Press, 1989.

[17] Kathrin Koslicki. Varieties of ontological dependence. In F. Correia and B. Schnieder, editors, *Metaphysical Grounding: Understanding the Structure of Reality*, pages 186–213. Cambridge University Press, 2012.

[18] Imre Lakatos. *Proofs and Refutations: The Logic of Mathematical Discovery*. Cambridge University Press, 1976.

[19] Marc Lange. What are mathematical coincidences (and why does it matter)? *Mind*, 119:307–340, 2010.

[20] Martin W. Liebeck. The insolubility of the quintic. In T. Gowers, J. Barrow-Green, and I. Leader, editors, *Princeton Companion to Mathematics*, pages 708–710. Princeton University Press, 2008.

[21] Paolo Mancosu. Bolzano and Cournot on mathematical explanation. *Revue d'histoire des sciences*, 52:429–456, 1999.

[22] Paolo Mancosu. Mathematical explanation: Why it matters. In Paolo Mancosu, editor, *The Philosophy of Mathematical Practice*, pages 134–150. Oxford University Press, 2008.

[23] Peter Pesic. *Abel's Proof: An Essay on the Sources and Meaning of Mathematical Unsolvability*. MIT Press, 2004.

[24] E. Scholz. Die Enstehung der Galoistheorie. In E. Scholz, editor, *Geschichte der Algebra*, pages 365–398. Wissenschaftverlag, 1990.

[25] Mark Steiner. Mathematical explanation. *Philosophical Studies*, 34:135–151, 1978.

[26] Ian Stewart. *Galois Theory*. Chapman and Hall, third edition, 2004.

[27] Ian Stewart. *Why Beauty is Truth: A History of Symmetry*. Basic Books, 2007.

[28] Jamie Tappenden. Proof style and understanding in mathematics i: Visualization, unification and axiom choice. In P. Mancosu, K. F. Jørgensen, and S. A. Pedersen, editors, *Visualization, Explanation and Reasoning Styles in Mathematics*, pages 147–214. Springer, 2005.

[29] Jamie Tappenden. The Riemannian background to Frege's philosophy. In J. Ferreirós and J. J. Gray, editors, *Architecture of Modern Mathematics: Essays in History and Philosophy*, pages 97–132. Oxford University Press, 2006.

[30] Jamie Tappenden. Mathematical concepts: Fruitfulness and naturalness. In Paolo Mancosu, editor, *The Philosophy of Mathematical Practice*, pages 276–301. Oxford University Press, 2008.

[31] Jules Vuillemin. *La philosophie de l'algèbre*. Presses Universitaires de France, 1962.

[32] Hans Wussing. *The Genesis of the Abstract Group Concept*. Springer, 2007.