FORMAL PROOFS AND REFUTATIONS

A DISSERTATION

SUBMITTED TO THE DEPARTMENT OF PHILOSOPHY

AND THE COMMITTEE ON GRADUATE STUDIES

OF STANFORD UNIVERSITY

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

Jesse Alama
June, 2009

I certify that I have read this dissertation and that, in my opinion, it is fully adequate in scope and quality as a dissertation for the degree of Doctor of Philosophy.

(Grigori Mints) Principal Adviser

I certify that I have read this dissertation and that, in my opinion, it is fully adequate in scope and quality as a dissertation for the degree of Doctor of Philosophy.

(Solomon Feferman)

I certify that I have read this dissertation and that, in my opinion, it is fully adequate in scope and quality as a dissertation for the degree of Doctor of Philosophy.

(Johan van Benthem)

I certify that I have read this dissertation and that, in my opinion, it is fully adequate in scope and quality as a dissertation for the degree of Doctor of Philosophy.

(Jeremy Avigad)

Approved for the Stanford University Committee on Graduate Studies.

Abstract

Two questions drive the dissertation:

- *What can one discover in a formal mathematical theory?*
- *What more do we know of a mathematical theorem when it has been formally proved than that it is provable?*

These questions spring from the provocative philosophy of mathematics of Imre Lakatos. They are tackled in two ways: by evaluating the philosophical foundations of Lakatos's work, and by studying contemporary work in formal mathematics, specifically formal proof checking technology.

The dissertation has a technical part and a philosophical part. The first part considers some philosophical problems raised (or brought into focus) by formal mathematical proofs. The second, technical part attempts to answer mathematical questions raised in the first part. The bridge between the two is a formal proof of a famous mathematical result known as *Euler's polyhedron formula*, whose history Lakatos has reconstructed and which serves as the central example for his philosophy of mathematics. The aim of the dissertation is to explore some of the philosophical problems suggested by such formalization efforts.

The argument of the dissertation has three components. In the first component, I explain how Lakatos's philosophy of mathematics poses a challenge to formal proof checking technology. The second component is to respond to the challenge by formalizing Euler's polyhedron formula. Finally, the third component evaluates the technical, formal proof response.

The dissertation is timely because, owing to developments in logic and computing in the last half-century, the concept of a formal proof, which used to be at best a model of mathematical argumentation, has become more concrete and practical. It has now become possible to actually formalize significant mathematical proofs. These contemporary developments are a source of problems for a philosophy of mathematics that is sensitive to mathematical practice. This movement within the philosophy of mathematics is to no small degree inspired by Lakatos's work. The time is ripe for returning to some of the basic philosophical problems that Lakatos and other philosophers pointed to long ago, and to examine new problems that come from the development of what might be called *proof technology*, tools for helping mathematicians construct and evaluate proofs.

In chapter 1, I lay out some of the main questions and problems about formal proofs and explain how they are related to central issues within mainstream philosophy, particularly epistemology and philosophy of science. The development of formal proof technology is based on classical 19th and 20th century results in mathematical logic but depends crucially on computers. Chapter 1 also surveys the variety of uses of computers in mathematical practice and discusses the variety of philosophical problems they pose.

The next step in the discussion of formal proofs will be a critical evaluation of the philosophy of mathematics of Imre Lakatos. His *Proofs and Refutations* (1963) attacks formalist philosophies of mathematics. Since much proof technology is to some extent based on or requires a certain formalist view of mathematics, the question naturally arises how Lakatos's philosophy bears on these developments. Chapter 2 addresses these concerns. I focus also on some epistemological problems suggested by formal proofs, such as the question of defining *rigor* and the problem of whether and how one improves one's justification for a mathematical claim through formalization of a proof of it.

The cornerstone of Lakatos's *Proofs and Refutations* is a history of a particular mathematical theorem known as *Euler's polyhedron formula*, which is a certain geometrical-combinatorial claim with a rather colorful history. I have formalized a proof of this mathematical result; chapter 3 contains a discussion of the proof and its formalization.

Thanks to the work carried out in chapter 3, Euler's polyhedron formula (understood in a certain abstract or combinatorial way that is explained in chapter 3) is shown to be a first-order consequence a certain first-order theory of sets. Because of the peculiarities of the particular proof technology with which the formal proof was carried out, the theory of sets that is used is much stronger than what is intuitively required for Euler's theorem. A natural proof-theoretic question thereby arises: can one do better? Are the strong assumptions really necessary? In chapter 4, I identify a weaker theory in which to carry out a formal proof Euler's formula. Also discussed are some formal problems about expressibility problems for combinatorial polyhedra, and related issues.

In chapter 5, I return to some of the issues that Lakatos raised in connection with formal proofs in light of the formal work that is carried out in chapter 3. This work provides some resources for taking on the two questions that were initially asked. I show that Lakatos's philosophy, its strong reservations against 'formalism' notwithstanding, applies quite naturally to formal mathematics.

Acknowledgements

First of all, my advisor, Grisha Mints, has been supportive and caring throughout my graduate education. I am thankful for my relationship with him, and for the opportunities he gave me throughout my time at Stanford.

My dissertation committee has also been quite helpful. I thank Sol Feferman, Johan van Benthem, and Jeremy Avigad for their support in helping me to grow from a student to a scholar.

I would also like to thank those who contributed by giving advice, criticism, and support. My family has been especially important in providing a steady base for me. In addition, the following people have all played their roles, small and large (in no particular order): Tomohiro Hoshi, Tobey Scharding, Paolo Mancosu, Marc Pauly, Krista Lawlor, Ulrich Kohlenbach, Branko Grünbaum, Lauren Hartzell, Valeria de Paiva, Darko Sarenac, Quayshawn Spencer, Alan Woods, Herman Geuvers, Audrey Yap, Heidi Dolamore, Jip Veldman, Boris Moroz, Fernando Ferreira, Henk Barendregt, Alexei Angelides, Bas Spitters, Patrick Girard, Elizabeth Coppock, Freek Wiedijk, Maria Taylor, David Fernandez, Stephen Simpson, Marvin Greenberg, Lanier Anderson, Michael Friedman, Robert Solovay, Tyler Greene, Peter Koepke, Conor Mayo-Wilson, Michael Beeson, Henry Towsner, Alistair Isaac, Mark Crimmins, Eric Pacuit.

I am grateful for all of you.

Contents

1 Introduction

Mathematics can be distinguished from other intellectual disciplines by its argumentative practices: only the most rigorous arguments—proofs—are allowed. Indeed, one might characterize mathematics as *the discipline whose claims to knowledge require proof*; an argument is mathematical to the extent that it is a proof. Within the study of argumentation, one ought to be especially interested in proofs, since they are perhaps the most sophisticated and rigorous arguments that we can produce.

But a proof is not merely any convincing argument; examples of bad convincing arguments are only too easy to find. What distinguishes mathematical proofs from other kinds of arguments? *What is a proof?* The question is quite broad, and of course hardly new.

The central theme of this dissertation is the concept of a *formal proof*, an argument executed according to the rules of a precisely specified mechanism. Depending on one's views, this study will be either one of contrasts (emphasizing the ways in which formal proofs differ from non-formal proofs) or of similarities (one sees non-formal proofs as more or less straightforward approximations of formal proofs).

Yet the dissertation is not merely a comparison of formal and non-formal proofs. I hope to show how questions about formal proofs touch on some central issues in mainstream philosophy. In this respect, the philosophy of Imre Lakatos animates the whole dissertation. Lakatos's major work, *Proofs and Refutations* [1], arising from his own dissertation, is a refreshing critique of certain approaches to the philosophy of mathematics which emphasize formal over non-formal proofs. Lakatos is not an enemy of formal proofs as such, but in his work he critiques philosophies of mathematics that hold that formal proofs ought to be somehow privileged, either philosophically or methodologically, over non-formal proofs. Lakatos' work engages deftly with the history of mathematics, but it does not shy away from some of the enduring questions of philosophy.

Two questions spur on the work:

- *What can one discover in a formal theory?*
- *What more do we know of a mathematical theorem when it has been formally proved than that it is provable?*

The structure of the dissertation will be as follows. There are two parts: a philosophical part and a technical part. The bridge between the two parts will be the central example of Lakatos's *Proofs and Refutations*: Euler's polyhedron formula. The first part will consider some philosophical problems raised (or brought into focus) by formal proofs. The second part is technical and attempts to answer mathematical questions raised in the first half.

In chapter 1, we will discuss some of the main questions and problems about formal proofs and show how they are related to central issues within mainstream philosophy.

By definition, a formal proof is a construction that is carried out according to the rules of a rigorously specified language and proof system. We lay down rules for what counts as a *deduction*: the statements appearing in it must be formulas within some specific formal language, and the steps in the deduction must be justified by appealing to certain mechanical rules. In general, the rules of inference in a proof system capture, or correspond to, only the particularly simple kinds of inferences that one might carry out in non-formal contexts. Thus, when formalizing a non-formal argument, invariably one ends up with a rather more detailed and considerably longer result compared with what one started with. For this reason, and the fact that the rules of inference are generally mechanical rules that can be implemented on a computer, the questions arising from the study of formal proofs generally goes hand-in-hand with questions arising from the use of computers. We shall also discuss these issues in chapter 1.

The next step in our discussion of formal proofs will be toward the philosophy of Imre Lakatos, who was already mentioned. Lakatos is remembered in philosophy of science for his work on what he called the methodology of scientific research programs, but he got his career started in earnest as a philosopher of mathematics. His *Proofs and Refutations* was a literary *tour de force*, attacking what he called formalist or Euclidean philosophies of mathematics according to which mathematics is best understood as a structure consisting of axioms at the top and theorems at the bottom, with a "truth-value injection" making all the theorems indubitably true. Lakatos's work is multi-faceted, but the concept of proof is the central hub from which everything else radiates. In chapter 2, we discuss how Lakatos' "dialectical" philosophy of mathematics bears on the subject of formal proofs and what we can learn from it. We will see how Lakatos's thought poses a challenge for the formalists.

Chapter 3 takes off where the chapter 2 left off, which was a discussion of Euler's polyhedron formula, the mathematical theorem that forms the cornerstone of Lakatos's *Proofs and Refutations*. The questions that shall occupy us in chapter 3 have to do with the problem of giving a formal proof of Euler's polyhedron formula. Other mathematical examples would likely have illustrated the same points, but the study of Euler's polyhedron formula in particular is motivated by the desire to engage with Lakatos's text as much as possible on the formal, mathematical side. Chapter 3, then, will be a discussion of a formal proof of Euler's polyhedron formula. We will describe what it means to formalize the theorem and we will compare it in detail with the informal proof on which it is based. (The actual formal text can be found in Appendix 1.)

Thanks to the work described in chapter 3, we have that Euler's polyhedron formula (understood in a certain combinatorial sense) is a first-order consequence of Tarski-Grothendieck set theory (TG). This theory of sets is quite strong in comparison to more familiar systems such as Zermelo-Fraenkel set theory (ZF). It is even much stronger than ZF together with the axiom of choice (the system ZFC): TG is an extension of ZFC together with an axiom that asserts the existence of arbitrarily large strongly inaccessible cardinal numbers. But clearly Euler's polyhedron formula does not require a theory as strong as TG for its proof. If we formalize Euler's formula as a certain arithmetical-combinatorial statement, then it seems plausible that Euler's formula could be proved in a theory far weaker than TG. In chapter 4, we shall identify a weaker theory in which to carry out a proof Euler's formula. We shall also discuss a number of metamathematical problems brought about polyhedra, specifically concerning expressibility of various properties in certain formal languages.

Finally, in chapter 5, we will step back and reflect on what has been accomplished by formalizing so many proofs and how we can use them to respond to Lakatos's challenge, which is set forth in chapter 2. By studying formal proofs of non-trivial mathematical theorems, what more can we say about the difference between formal and non-formal proofs?

The dissertation does not take any sides on the debate between formalists and non-formalists in the philosophy of mathematics, nor does it advocate any particular position for or against formal proofs. The dissertation is rather undertaken with a more neutral point of view in mind. Indeed, we hope that one of the main lessons of the dissertation is that whatever gulf does exist between those who favor and those who oppose formal proofs is not as wide as meets the eye.

2 Formal Proofs in Mathematics

2.1 Introduction

Our discussion begins with a survey of the development of what I call **formal proof technology**: tools for the production, recording, and evaluation of mathematical proofs. Such technology, and its mathematical and philosophical significance, constitutes the central theme of the work. In this chapter we will learn about the growth and development of formal proof technology to set the stage for a more sustained critical discussion, based on the philosophy of mathematics of Imre Lakatos. Lakatos's philosophy will be the subject of later chapters; the purpose of this chapter is to set the stage for a philosophical engagement with Lakatos based on modern formal proof technology.

2.2 Formal Proof Technology: Three Strands

The history of what I am calling formal proof technology can be seen as a bundle of three strands in the history of logic.

The first strand concerns early technical developments in mathematical logic in the late 19th and early 20th centuries. A landmark result in the subject that is of interest here is the **completeness theorem** for first-order logic, which demonstrated to us that it is possible to lay down axioms and rules of inference in such a way that (first-order) logical consequence implies provability from these rules and axioms.[1] Thus, at least in the case of first-order logic, one can give formal proofs to establish any logical consequence.

By inspection of the rules and axioms for the traditional proof formalisms—natural deduction, Hilbert-style systems, tableaus, and sequent calculi—it seems clear that they deliver a concept of a gap-free proof, that is, one all of whose logical details are explicitly stated. If one further identifies (if only as a first approximation) the concept of mathematical consequence with first-order logical consequence, then the completeness theorem tells us that any mathematical consequence can be given by a gap-free formal proof. In principle, then, one can rely on formal proof (in first-order logic) to establish any (first-order) logical consequence.

The second strand in the history of logic that I wish to emphasize is the formalization of mathematical knowledge. The idea is to express mathematical propositions in precisely specified formal languages. Major actors in this direction are Peano, Frege, and Russell and Whitehead. Peano, for example, was interested in the symbolic aspects of mathematics and indeed catalogued some of the notations of mathematics that existed at his time, and even invented new notations [2][2], such as $\in$ (for set membership), $\cap$ (for set intersection), and $\cup$ (for set union). Frege designed a notation—a concept script, or Begriffsschrift—to lay out the content of mathematical propositions and proof. Although logicians did not adopt Frege's notation, his contributions to logic were independent of his notation and proved to be fundamental. Russell and Whitehead, in their monumental *Principia Mathematica*, aimed to formally represent a small but central part of mathematical knowledge.

Project such as Peano's, Frege's, and Russell and Whitehead's, although they did not advance far into the reaches of mathematical knowledge, made it plausible that everyday mathematics—its concepts, propositions, and proofs—could be given in a totally formal way.

The third thread in the history of mathematical logic that is important for our purposes is the use of computers, especially in formalized mathematics. Such use is possible because of the finitist nature of the languages and proof systems that have been developed. More precisely, the problem of deciding whether a sequence of symbols (in some specified alphabet or pool of possible symbols) constitutes a well-formed formula is supposed to be decidable. Likewise, the problem of whether a figure is a deduction should be decidable. Such a representation is quite natural for formalized mathematics: for this to be a real possibility for humans, it should be possible to determine, in a finite amount of time (which is all any of us have) to say whether a string of symbols is a statement of a deduction. (If this were not the case, results like the completeness theorem would lose their significance for 'human-level' formalization.)

Indeed, the use of computers as tools for the recording, evaluating, and production of (formalized) mathematical proofs occurred quite early in the history of the computer.[3] For example, H. Wang, already in the 1950's (before modern-day computers were even a decade old), worked on the problem of generating formalizations of proofs taken from *Principia Mathematica*. Early work on implementing decisions procedures for certain axiomatized theories such as Davis's implementation [3] of a decision procedure for Presburger arithmetic, and on propositional satisfiability, were implemented early in the history of the computer.

But experience with formal proofs shows that they can become quite large and unmanageable.[4] A skeptical attitude toward formal proofs would then be quite justified; putting aside questions of what kind of knowledge one could gain from carrying out formal proofs, one can reasonably ask whether formal proofs are really accessible to us. Can one really give a surveyable, accessible proof of a non-trivial mathematical result?

Putting together these three strands in the history of mathematical logic we can see the ingredients for the development of modern formal proof technology. In the next section, we shall survey some of the results of the growth of this technology.

2.3 Early Growth of Formal Proof Technology

Concerning the problem of representing and evaluating mathematical proofs, J. McCarthy also figures into this early history, in his proposal (expressed, naturally, in LISP) for a program to check mathematical proofs [4]. One of the earliest sustained efforts in this direction is the AUTOMATH project [5] by N. G. de Bruijn, begun in the late 1960's. A major result of the AUTOMATH project was a formalization [6] of E. Landau's *Grundlagen der Analysis* in their framework. The MIZAR project, a proof representation and proof checking system, began in the early 1970's and remains active today; it is thus likely the oldest proof checking system that enjoys an active community of formalizers and developers. (MIZAR also enjoys one of the largest collections of formalized mathematical knowledge.)

The 1970's also witnessed the creation of the the Boyer-Moore theorem prover [7] (which has since developed in the modern ACL2 system [8]).

The roots of formal mathematics can be clearly seen in the work of Leibniz, who imagined a calculus of reasoning (*calculus ratiocinator*) with which one could *calculate* whether any given argument is correct [9]. Formal mathematics also takes inspiration from Frege's idea of a *gap-free proof*, a mathematical argument whose every logical step is spelled out explicitly. In the 20th century David Hilbert, Kurt Gödel, Gerhard Gentzen, and others forged a new path, which gave rise to proof theory. Hilbert called for the formalization of mathematics as one component of the research tradition that now bears his name (*Hilbert's program*) [10]. Thanks to his completeness theorem, Gödel shows us that, if we restrict ourselves to first-order logic, then every valid argument can in principle be articulated as a gap-free proof. The exciting new subject of proof theory took on a new dimension with the advent of computers: these early results in logic assured us of the possibility of carrying out mathematics formally, but to realize the ideal—to move from 'theoretical' proof theory to what might be called concrete proof theory—required the assistance of computers. Formal mathematics builds on the fundamental contributions of mathematical logic, as well as insight gained into programming languages and system design, to construct computer systems that help us to carry out mathematical reasoning.

To formalize a piece of mathematical knowledge (*e.g.*, a theorem, a definition, or a proof) is to capture it using a formal language. A formalization starts with a pre-existing mathematical text and reconstructs it within a formal language.

But formalization is not mere reconstruction. The product of a formalization is a reconstruction of *the complete logical structure* of a piece of mathematical knowledge. The word 'complete' is used to emphasize that all logical details are to be given; the argument is expressed so candidly and explicitly that its validity can be mechanically checked. One might view the computer as a highly skeptical participant in a mathematical conversation: it accepts only those steps of the argument that are logically given in detail; it requires us to be careful with out definitions and with the statements of results. And since it does not accept appeals to intuition, common sense reasoning, and other conversational moves on which we typically rely when presenting an argument to another human, the result of such a human-computer interaction is an argument whose logical structure is apparent and in whose validity we can have considerable confidence.

To craft a formal proof so that its validity can be mechanically checked, one must invest a considerable amount of energy to bring to light the logical and mathematical details of an informal proof that are often left implicit and unstated. Some of this uncovered knowledge is, to be sure, of a routine nature and is not necessarily notable. Yet often one uncovers interesting mathematical (or metamathematical) details that one might not have come across had one not formalized.

One does not need to view formal and informal mathematics as in competition with each other. Formal mathematics is to informal (or standard, normal) mathematics as implementations of algorithms are to algorithms. There is, of course, considerable value in algorithm design, and methods of solving problems. An informal argument is like pseudocode for a computer program, whereas a formal argument is like an implementation. One designs programming languages with which to express algorithms, and then of course on has to implement algorithms in particular programming languages for it to do anything.

The analogy between informal arguments and pseudocode also helps to explain the value of formal mathematics. One gains a different insight into an algorithm when one implements it; one understands the solution to a problem in one way in terms of pseudocode, and one sees other aspects when implementing it. Avigad, for example, has considered this issue [11–13] in detail. Implementation of algorithms is important because we want computers to carry out certain tasks for us; formalizing mathematics is important because we want to understand fully the justificatory structure of an (informal) mathematical proof.

2.4 Contemporary Developments in Formal Proof Technology

A number of major mathematical results have been given formal proofs in modern proof representation and proof checking systems. These include:

- Gödel's first incompleteness theorem [14],
- The Jordan curve theorem [15–16],
- The four color theorem [17],
- The prime number theorem [18].

This is but a sample of the 'named' theorems that have been proved formally.[5] The body of unnamed theorems, lemmas, definitions and proofs that have been formalized is very large indeed. These results show that formalization is generally possible, and often tractable. Of course, if one were to try to carry out these formal proofs by hand, the possibility of error (not to mention the likelihood that such projects would even be justified or completed) would be very high. It is only with the help of computers that these projects are possible.

2.4.1 The QED Project

In the 1990's, interest in formal mathematics grew and led to an international attempt, called the QED Project, to unify efforts. The participants drafted a 'manifesto' [20] so as to take a common stand toward the problem of formalizing mathematical knowledge. The goals of the project are:

1. to help mathematicians cope with the explosion in mathematical knowledge,
2. to help development of highly complex IT systems by facilitating the use of formal techniques,
3. to help in mathematical education,
4. to provide a cultural monument to "the fundamental reality of truth",
5. to help preserve mathematics from corruption,
6. to help reduce the 'noise level' of published mathematics,
7. to help make mathematics more coherent,
8. to add to the body of explicitly formulated mathematics, and
9. to help improve the low level of self-consciousness in mathematics.

The method to achieve these goals is through the design and implementation of large-scale systems for dealing with formal mathematics.

J. Harrison, a major figure in the field that I am calling formal proof technology, places his hopes for the field in two points [21]:

- Supplementing, or even partly replacing, the process of peer review for mainstream mathematical papers with an objective and mechanizable criterion for the correctness of proofs.
- Extending rigorous proof from pure mathematics to the verification of computer systems (programs, hardware systems, protocols, etc.), a process that presently relies largely on testing.

Harrison's second goal clearly aligns with the second goal of the QED Manifesto, but Harrison's first goal represents an objective that does not appear in the QED Manifesto (although perhaps it can be seen spread across some of the items, such as 6 and 7). It seems plausible to extend the QED Manifesto to include Harrison's goal.[6]

The aims of the QED Project are significant and its success would be a major contribution. Interest in the project, however, seems to have crested in the mid-90's. Although it is not clear that widespread interest in the project (or any related project) remains, the goals of the QED Project seem to have survived in any number of systems, such as MIZAR [22], HOL LIGHT [23], COQ [24], etc.

2.5 Digression: Computers in Mathematics

Since formal proofs are generally rather large constructions that cannot easily be completely handled with traditional 'small scale' tools such as pencil and paper, when working with formal proofs one typically relies on a computer. The computer stores the data and allows the formalizer to organize and manipulate it in ways that are not practically possible otherwise. The computer also takes charge of evaluating formal arguments. Such tasks could in principle be carried out by the human formalizer; the computer is, after all, applying computable functions. Because formalization does not, as a matter of definition, involve the use of computers or other new tools, we can disentangle from our discussion the question of *the purpose or value of formalization* and *the role of computers in mathematical practice*. This section is devoted to the latter question.

The main subject of the dissertation is computer-checked formal proofs. We are engaged in computer-checked formal proofs when we give to a computer a formal argument d, expressed in a formal language, and expect that the computer will check whether d is a proof. This is clearly but one of the many ways in which computers are used in mathematics. The inquiry begins with a survey of how computers are used in mathematics; the first step is to delimit the enterprise of *computer-checked formal proofs* from the other kinds of uses of computers in mathematics. The goal is to isolate the philosophical issues that pertain to computer-checked formal proofs from those which arise because of other uses. Of course, some issues are the same (does one trust a machine?); but some are bound to be different (e.g., some have claimed that computers are helping to change our concept of proof, but it seems clear that the enterprise of computer-checked formal proofs is based on adherence to a traditional view of proof).

Producing formal proofs is but one way in which computers are used by mathematicians to assist them with their proofs. Notable examples of computer-assisted proofs that are not computer-checked formal proofs include the Appel-Haken solution [25] of the four-color problem and the results of so-called experimental mathematics [26–27]. But since the aim of computer-checked formal proofs is to produce genuinely formal proofs, they can complement other uses of computers. Indeed, one way of justifying the enterprise of computer-checked formal proofs is to point out that they can be used to 'rein in' other kinds of computer-assisted mathematics by bringing them more in line with a classical formal conception of proof.

Let us discuss these examples (the Appel-Haken proof of the four-color theorem and experimental mathematics) in more detail.

The four-color theorem asserts that one needs only four colors so that one can assign different colors to countries on a map in such a way that neighboring countries do not get the same color. The problem was posed in 1852. Finally, in 1976, Kenneth Appel and Wolfgang Haken announced a solution. A key part of their proof involved the use of a computer to check a very large number of cases into which they had decomposed the problem; the calculation took more than 1200 hours (50 days). According to the philosopher T. Tymoczko, the Appel-Haken work was a new kind of mathematical proof [28]. Tymoczko claimed that the Appel-Haken solution to the four-color problem was a new kind of proof because it was non-surveyable, and introduced fallible, empirical elements into mathematical knowledge, which one might regard as *a priori* and certain.

Putting aside the question of whether Tymoczko is right about the Appel-Haken solution to the four-color problem, it is not clear that his claims about non-surveyable and fallible aspects of mathematical knowledge apply to computer-checked formal proofs. For, these proofs are, by design, surveyable: a human formalizer crafts the proof; the computer's role is to check the formalizer's text for validity. Appel and Haken could not feasibly check all the details of the manifold cases into which they divided their problem; a human formalizer, however, did check all (or nearly all) the details in the proof that they constructed.

As for fallibility and the use of empirical methods, again it is not clear that these features, which (we can assume for the sake of discussion) make sense for the Appel-Haken proof, apply in the case of computer-checked formal proofs. These proofs are constructed according to the norms of formal logic; the results of these proofs are deductions in the strict sense of the term. The warrant that formal proofs provide for mathematical knowledge therefore seems to admit very little room for fallibility or 'empirical elements'. It seems clear that fallibility and empirical elements enter into formal proofs to no greater degree than they already do in ordinary mathematical practice.

Independently, it is worth pointing out that Tymoczko's claims about the use of computers in mathematics—that computers introduce hitherto unknown features of mathematical justification and knowledge—is not universally agreed upon. Tymoczko's claim that computers present a kind of inscrutable source of justification may not be tenable [29], and the idea that computer provide a new kind of justification (as opposed to, say, providing just a faster way to carry out what we ourselves could do in principle) is also debatable [30].

So much for Tymoczko's well-known philosophy about the use of computers in mathematics. Another prominent source for arguments about how computers are changing mathematical practice centers on what is called *experimental mathematics*. There may not be any strong unifying theme for this subject, but as a first approach the idea behind experimental mathematics is that the computer is regarded as a kind of laboratory for carrying out mathematical experiments. A characteristic feature of some of the results of experimental mathematics is that one is able to obtain, after some computation, a result which, though possibly false, is true with extremely high margins of confidence. Or, in the laboratory, one finds patterns which suggest generalizations and further experimentation.

The characterization thus far is, of course, rather coarse, but it suffices for our discussion. The question in front of us is whether this kind of work justifies the claim that the nature of mathematical proof is changing.

Indeed, it seems clear that experimental mathematics is not fundamentally changing the face of mathematical proof. After discussing some examples in experimental mathematics which render various results true with extremely high probabilities, Borwein and Bailey, champions of the experimental approach to mathematics, concede that extensive computations do not amount to rigorous proofs. However, they write that 'in many cases computations constitute very strong evidence, evidence that it at least as compelling as some of the more complex formal proofs in the literature' [31]. They go on to write:

> Independent checks and extremely high numerical confidence levels still do not constitute formal proofs of correctness. Even so, one can argue that many computational results are as reliable, if not more so, than a highly complicated piece of human mathematics. For example, perhaps only 50 or 100 people alive can, given enough time, digest *all* of Andrew Wiles'

> extraordinarily sophisticated proof of Fermat's Last Theorem. If there is even a one percent chance that each has overlooked the same subtle error (and they may be psychologically predisposed to do so, given the numerous earlier results that Wiles' result relies on), then we must conclude that computational results are in many cases actually *more* secure than the proof of Fermat's Last Theorem. [31]

They then align their work with Thomas Kuhn's *Structure of Scientific Revolutions* [32] and assert that, thanks to developments with the computer, a paradigm shift is taking place or about to take place.[7] They assert that

> We acknowledge that the experimental approach to mathematics that we propose will be difficult for some people in the field to swallow. Many may still insist that mathematics is all about formal proof, and from their viewpoint, computations have no place in mathematics. But in our view, mathematics is not ultimately about formal proof; it is instead about secure mathematical knowledge.

Both kinds of uses of computers (large computations which are in principle completely correct, and computations which in principle warrant at most high confidence in a result) suggest that what's being counted as a proof in contemporary mathematics does not seem to adhere to the traditional view. Sociologist Donald MacKenzie has drawn attention to the divisions among some mathematicians engendered by the computer. MacKenzie writes

> For some, to put one's trust in the results of computer analysis is to violate the very essence of mathematics as an activity in which one's own human, personal understanding is central. To others, using a computer is no different in principle from using pencil and paper, which is of course universally accepted. . . . Those who find the assistance of the computer natural, typically see it as *more* reliable than the human mathematician. [34]

Such a sociological divide is quite interesting, but again it should be emphasized that the different reactions that one can have to mathematical proofs in which computers have played some role are at the same time differences in conceptions of proof.

We mention now, finally, an on-going (at the time of writing) episode in the history of mathematics that involves computers and controversy about proof. The example is Hales's solution of the Kepler conjecture. This conjecture, roughly speaking, asserts that the densest packing of spheres in space is the hexagonal pattern that we see in markets and grocery stores.[8] Like the four-color theorem, the Kepler conjecture was an open problem for many years before it was solved: Kepler posed the problem in 1611, but it wasn't solved until 1998.[9] And like the Appel-Haken solution to the four-color theorem, Hales's 1998 proof involved a tremendous amount of computer resources: several gigabytes of data were required. However, unlike the Appel-Haken solution, Hales's use of the computer did not amount merely to a very large calculation. The computer was used, for example, to even get an initial decomposition of the problem [36]. Interestingly, after Hales submitted his work to the *Annals of Mathematics*, the editors wrote back, four years later, saying that they were 99% certain that his arguments were correct. The missing 1% came from the failure to certify the correctness of the computer programs that Hales had used in his argument. Hales's paper was eventually published, but the episode led the editors of the *Annals of Mathematics* to revise their policy [37] on computer-assisted proofs. Hales is now engaged in a project [38] to give a formal proof (expressed in a formal, artificial language) of his result. Thus, he has moved to computer-checked formal proofs from an originally 'unorthodox' position. Although it may take a long time to finish the project (Hales estimates it may take 20 man-years), at the end the result will likely be the largest amount of mathematics that has even been formalized.

2.6 Formal Proof Technology: A Philosophical Error?

We have surveyed some of the historical features of what I am calling formal proof technology (tools for the production, evaluation, and storage of mathematical proofs). Obviously, all of these results take for granted, or require, a certain formal approach to mathematical knowledge. To carry out proofs in these systems require, in addition to mathematical skill, a facility with formal logic.

There seems to be a consensus that the limitations of proof checking are merely technical. Although at present proof representation and proof checking systems—formal proof technology—forms a rather small (and arguably insignificant) part of contemporary mathematical practice, the consensus among the developers of such systems, and among those outside it who are nonetheless interested in proof checking, is that the only gaps in the field are technical, the only problems one of engineering and not philosophy.

Limitations of engineering notwithstanding, is it not possible that these systems—which apparently require a kind of formal, modern view of mathematics—somehow not giving us what we want out of mathematical proof? Are they based on a philosophically erroneous view of mathematics? The gains in rigor that formal proof technology can deliver is undeniable, but at what philosophical cost does this progress come? In the next chapter we shall investigate a famous critique of such 'formalist' philosophies of mathematics, Imre Lakatos. We shall see that Lakatos presents a compelling challenge to the approach to mathematics that formal proof technology takes for granted.

3 A Lakatosian Challenge

3.1 Introduction

Mathematics provides a variety of knowledge that most plausibly qualifies for superlative epistemological qualities such as *certainty*, *indubitability*, *a priority*, *infallibility*, and so forth. One of the main questions in the philosophy of mathematics is to account for this: to explain how it is that mathematical knowledge has these properties (or, if they do not, to account for the appearance that they do). One way to explain the superlative features of mathematical knowledge is to point to the methodology by which mathematical truths are justified: the standard for claims to mathematical knowledge is *proof*. The epistemological features of mathematics can be explained by its standard for justification.

The Hungarian philosopher Imre Lakatos responded to claims like these in his famous *Proofs and Refutations* [1]. Written as a dialogue, *Proofs and Refutations* argues that

> Informal, quasi-empirical, mathematics does not grow through a monotonous increase in the number of indubitably established theorems but through the incessant improvement of guesses by speculation and criticism, by the logic of proofs and refutations.

Formalism for Lakatos is "the school of mathematical philosophy which tends to identify mathematics with its formal axiomatic abstraction (and the philosophy of mathematics with metamathematics)". A serious problem, for Lakatos, is that formalism disconnects mathematical knowledge from its history. Moreover, Lakatos argues that mathematical knowledge does *not* have the superlative epistemological features that we commonly assume that it has. Invoking Kant, Lakatos writes:

> The history of mathematics, lacking the guidance of philosophy, has become *blind*, while the philosophy of mathematics, turning its back on the most intriguing phenomena in the history of mathematics, has become *empty*.

For Lakatos, the formalist holds that mathematical theorems and proofs are more or less certain things from their birth. Mathematical statements are either unknown or irrefutably known with certainty. For Lakatos's formalist, *knowledge* and *certain knowledge* amount to the same thing (at least in the case of mathematics).

Proofs and Refutations is intended as the beginnings of a serious critique of formalism; Lakatos even believes that by looking at the history of mathematics we can show fairly conclusively that formalism is inadequate:

> The history of mathematics and the logic of mathematical discovery cannot be developed with the criticism and ultimate rejection of formalism.

In other words, the history of mathematics shows that formalism is not a viable philosophy of mathematics.

This chapter presents Lakatos's philosophy of mathematics as a challenge for formal proof technology, as explained in chapter 1; the challenge is taken up in chapter 3, and in chapter 5 we shall evaluate the Lakatos's philosophy in greater detail.

Lakatos's philosophy involves more substance than what will be discussed here. I am focusing on his philosophy insofar as it applies to formal proof technology. Consequently, I neglect a discussion of, say, concept formation, ancient history of mathematics, pedagogical aspects of mathematics, and so forth, all of which are discussed in detail by Lakatos. Such aspects of Lakatos's philosophy are philosophically rich, but they do not bear directly on the project contained here.

3.1.1 Digression: the problem of interpreting *Proofs and Refutations*

Before getting into the details of Lakatos's philosophy, we should be clear on how to make sense of *Proofs and Refutations*. Because it is largely written as a dialogue, we have to be careful about claims like "Lakatos said X" or "Lakatos holds that p". The reason is that it is not clear which character (or characters) in the dialogue are taking Lakatos's position. The situation is similar to that of Plato's dialogues, but, in a way, with *Proofs and Refutations* we are in a worse position: whereas (the character) Socrates plays the lead role in most of the Platonic dialogues, no analogous character in *Proofs and Refutations* can be found. The scene of the Lakatos's dialogue is a classroom of students and a teacher. One might be tempted to assert that Teacher is Lakatos; but that's not obvious, and in any case the role of Teacher is often just to summarize what has been said and to keep the discussion on track (as a real teacher does); Teacher generally does not offer significant new points; that is done by the students.

Unlike the Platonic dialogues, *Proofs and Refutations* opens with an expository introduction in which Lakatos introduces his work. The many footnotes in the text take place outside the dialogue. And, unlike the Platonic dialogues, where at times a character holds forth, stating and arguing for a position in detail, such passages are rare in Lakatos's text. Thus it often seems that we are not really arguing with Lakatos directly, but rather with our own informed guesses about what he might be saying.

However, all is not hopeless. As in the Platonic dialogues, we can reasonably infer what Lakatos thinks by the questions and problems that are raised in the dialogue, and the responses and solutions that are given. We need to live with the fact that some questions are not answered definitively.

Thus, although there is room for debate about the precise statement of Lakatos's philosophy of mathematics, we can be fairly sure which issues Lakatos thinks are important, even if we can't discern a clear *position* that Lakatos takes on them. And even in those places where we are not certain what Lakatos himself thought, we can take *Proofs and Refutations* as an "authorless" source of ideas constituting the beginnings of a philosophy of mathematics.

Before proceeding, it is worthwhile to pause to comment on the style of Lakatos's philosophy. The quotes already given should make it clear that Lakatos takes a strong stand against 'formalists' and emphatically holds that they are getting something wrong about the history and philosophy of mathematics. One can criticize Lakatos for failing to seriously characterize the formalist position. That he takes issue with *some* position in the philosophy of mathematics is clear enough; what is less clear is precisely what he is attacking, or whether anyone robustly holds the 'formalist' view that he is eager to refute. Putting aside for the moment the tension between history and philosophy, it seems clear that any serious philosophy of mathematics should be able to account to some extent for the growth and development of mathematics. Lakatos seems to be rather uncharitable here when he casts a wide net to capture all those 'formalists' who flagrantly ignore the history of mathematics.

Even though Lakatos takes rather strong and occasionally uncharitable positions toward his philosophical rivals, that should not lead us to dismiss him outright. Lakatos is as original as he is combative. His views do deserve to be taken seriously. In Lakatos one sees a challenge to modern formal proof technology. This chapter sets the stage for the challenge by, first, surveying Lakatos's philosophy of mathematics and, second, by posing the terms of the debate. In the next chapter, we will see in detail a formal proof of the mathematical theorem known as Euler's polyhedron formula (EPF), whose history Lakatos traces in *Proofs and Refutations*.

3.2 Main Features of Lakatos's Philosophy of Mathematics

The heart of Lakatos's philosophy of mathematics is that mathematical theorems are defeasible and subject to refutations not unlike claims in empirical sciences. The main idea is to extend Popper's critical philosophy of science to mathematics. For Popper, roughly speaking, universal scientific claims cannot be confirmed, but only refuted. Lakatos wants to extend this idea from natural science (where Popper's claim seems quite credible) to mathematics (to which Popper himself did not venture to apply his ideas). Mathematical theorems are not irrefutably true statements, but *conjectures*: one cannot know that a theorem will not be refuted.

To illustrate this thesis, Lakatos appealed to the history of Euler's polyhedron formula, which asserts that for a polyhedron p we have $V - E + F = 2$, where V, E, and F are, respectively, the number of vertices, edges, and faces of p. He showed how Euler's theorem and the concepts involved in it evolved through proofs, counterexamples and proofs modified in light of the counterexamples, thereby illustrating the fallibility of mathematics.

In addition to his view that mathematical knowledge is fallible, one of the Lakatos's central contributions to the discussion of proof in the philosophy of mathematics is his characterization of the concept of mathematical proof. As we shall see, his definition plays a crucial role in his discussion and helps us to understand a good deal of Lakatos's philosophy.

Lakatos's definition occurs near the beginning of the text:

> TEACHER: I propose to retain the time-honoured technical term 'proof' for a *thought-experiment*—or *'quasi-experiment'—which suggests a decomposition of the original conjecture into subconjectures or lemmas*, thus *embedding it* in a possibly quite distant body of knowledge.

Thus, for Lakatos, a proof is a kind of experiment that we can perform; to justify the conclusion of the experiment, we appeal to some previously accepted mathematical knowledge. Such a characterization of proof may be appealing. Notice, though, that it lacks (at least at this early stage of the text) of any relation between proof and truth, between the 'decomposition' and validity. Later in the dialogue, we find:

> LAMBDA: The proof is only a stage of the mathematician's work which has to be followed by proof-analysis and refutations and concluded by the rigorous theorem.

Thus, proof is not the end (as we might normally think) but rather the beginning of a theorem.

With this definition of proof, Lakatos is able to say that a mathematical statement can be both proved and refuted. This sounds oxymoronic but it is crucial to Lakatos's fallibilist philosophy of mathematics, in which proofs do not guarantee the truth of the statement being proved but instead invite us to search for counterexamples.

3.2.1 The method of proofs and refutations

To understand the heuristic development of informal proofs, Lakatos proposes four rules according to which one can improve mathematical knowledge. Before stating the rules, though, we must study two terms: *local counterexample* and *global counterexample*.

The context in which the local and global counterexamples occur is in the study of proofs. Suppose that we are studying a mathematical statement A whose logical form is $\forall x\varphi(x)$, and we find (somehow) a mathematical object a for which $\neg\varphi(a)$. Such an object shows that the statement A is refuted, and is called a *global counterexample*. Global counterexamples are what we normally think of as counterexamples: mathematical objects that show some universal statement to be false.[1] For example, the number 2 is a global counterexample to the statement "every even natural number is the sum of two primes", because 2 is the smallest prime number.

To say whether a mathematical object is a global counterexample does not require any reference to the proof of that statement. A *local counterexample*, by contrast, is a property not of a statement but of a proof of the statement. To understand proof, though, we should turn to Lakatos, who understands the term *proof* as a method of decomposition. Suppose that we have decomposed the proof of a statement A into a number of statements $A_1, A_2, \ldots, A_n$. Suppose that the logical form of, say, A_k is universal: A_k is $\forall x\varphi(x)$ for some statement $\varphi(x)$. If we have a mathematical object a for which $\neg\varphi(a)$, Lakatos calls that a is a *local counterexample* to the original statement A that we are trying to prove. Thus the definition of a local counterexample refers both to a statement and to a proof of it, regarded as a sequence of other statements.

Now that we are familiar with the terms *local* and *global counterexample*, we are ready to study the official statement of the method of proofs and refutations:

> LAMBDA: Let me state [the] main aspects [of the method of proofs and refutations] in three heuristic rules: *Rule 1. If you have a conjecture, set out to prove it and to refute it. Inspect the proof carefully to prepare a list of non-trivial lemmas (proof-analysis); find counterexamples both to the conjecture (global counterexamples) and to the suspect lemmas (local counterexamples).*
>
> *Rule 2. If you have a global counterexample discard the conjecture, add to your proof-analysis a suitable lemma that will be refuted by the counterexample, and replace the discarded conjecture by an*

improved one that incorporates that lemma as a condition. Do not allow a refutation to be dismissed as a monster. Try to make all 'hidden lemmas' explicit.

Rule 3. If you have a local counterexample, check to see whether it is not also a global counterexample. If it is, you can easily apply Rule 2.

Later in the dialogue, a fourth rule is added:

Rule 4. If you have a counterexample which is local but not global, try to improve your proof analysis by replacing the refuted lemma by an unfalsified one.

3.2.2 Lakatos on proof (continued)

Lakatos's characterization of the concept of mathematical proof does have some merits. For example, Lakatos's definition of proof allows us to understand statements such as

> Wiles's proof of Fermat's Last Theorem was incorrect.

and questions like

> What's wrong with Euler's proof of his polyhedron formula?

at face value. Although the statement and the question make sense, they might appear to be self-contradictory if by 'proof' we understand a deductively valid argument. Lakatos's definition allows us to make sense of these statements by dropping (at least initially) any connection between mathematical proof and error-free or valid argument. Wiles's proof and Euler's proof are thought experiments; they may admit counterexamples, but we can revise their proofs (though experiments) to deal with them. This sounds reasonable; Lakatos captures part of our everyday use of the term 'proof'.

How might a proof be incorrect? A proof could be incorrect if

- its conclusion is not true, or
- one of the steps in the proof is not valid (the assumptions in play at the step could be true while the conclusion of the step is false).

The idea, then, is that mathematical proofs are a certain kind of valid argument. To then say that a proof is 'incorrect' is to contradict oneself.

How can we make sense of the philosophical knots that we have gotten into? There are two approaches. We could insist that statements such as 'Euler's proof of his polyhedron formula is incorrect' make sense and drop the condition that a mathematical proof is a deductively valid argument. Another response is to retain the property that mathematical proofs are deductively valid arguments and say, in response to situations like those described above, that there was just some error:

> Wiles's believed that his argument for Fermat's Last Theorem was a proof, but his judgment was incorrect.

These two avenues for response show that two different views of mathematical proof are available:

- One view emphasizes the ideal of proof as a deductively valid, (in principle) error-free argument; let us call this the 'deductivist' view.
- The other view demurs from the 'deductivist' view. An argument can be a proof and yet fail to be logically valid.

The second view merely dissents from the first view. Expanding on the second view, one might say that, for the non-deductivist, proof is just what mathematicians *do*. They are interested, of course, in getting arguments right. But what matters more than correctness or deductive validity is the invention of new mathematical concepts and methods, the fruitful application and combination of previously accepted mathematical knowledge. Another way of making sense of the second alternative is to say that proofs are, in some essential way, *social* entities. (This is the approach taken by, for example, de Millo, Lipton and Perlis [39].) These considerations thus favor a Lakatos-like understanding of 'proof'.

We thus appreciate Lakatos's stance toward proof. By admitting multiple conceptions of the concept, the problem arises to explain the relationship between them. We are not taking the position that mathematical proofs are *not* (ideally) deductively valid arguments.

Although Lakatos's definition of proof can help us to make sense of our everyday use of the term, there remains the burden of accounting for the argumentative structure of mathematical arguments and their relation to mathematical truth. The non-deductivist needs to explain why mathematical argumentation differs from other kinds of arguments in science and everyday life. Mathematical arguments certainly appear to be deductively valid, and the mathematician apparently strives for deductive validity in his proofs.

In fact, Lakatos recognizes this issue and does account for it. To see that, we need to investigate Lakatos's conception of mathematical rigor. Tracing the history of Euler's formula (which, we are to assume, is but one concrete example that Lakatos develops to illustrate a more general claim about mathematics), we see that the proofs evolve. The goal of the development is a rigorous theorem, which Lakatos calls the **principle of retransmission of falsity** holds, namely that all global counterexamples be local. That is, any counterexample to the theorem should be a counterexample to some step in the proof of the theorem (purported falsity 'transmits' from the theorem to some part of its proof):

> LAMBDA: A proof-analysis is 'rigorous' or 'valid' and the corresponding mathematical theorem true if, and only if, there is no 'third-type' counterexample to it.

(The third-type counterexamples are those that are global—they refute the theorem at hand—but not local—they do not falsify any step of the proof.) To make sense of this, we need to explain Lakatos's distinction between *proof* and *proof analysis*. Lakatos's conception of proof has already been discussed. Roughly speaking, **proof analysis** is the production of what we might normally call the proof: the list of 'lemmas' into which the proof (thought experiment) was decomposed. We are doing proof analysis when we study the precise conditions under which the moves taken in the proof can be made, or are correct.[2]

3.2.3 Digression: Lakatos and Pólya

The mathematician G. Pólya, in a number of works [40–42], studies mathematical discovery and heuristic and thus touches on many of the same issues that Lakatos discusses. Indeed, it was Pólya himself who suggested to Lakatos to focus on the example of Euler's polyhedron formula. Lakatos places his own work in the context of Pólya's:

> This paper (i.e., [43]) should be seen against the background of Pólya's revival of mathematical heuristic, and of Popper's critical philosophy.

Lakatos translated Pólya's classic *How to Solve It* [44] from English to Hungarian.

Lakatos explains his own work as being an extension of Pólya's:

> The phase of *conjecturing* and *testing* in the case of $V - E + F = 2$ is discussed in Pólya. Pólya stopped here, and does not deal with the phase of *proving*—though of course he points out the need for a heuristic of 'problems to prove'. Our discussion starts where Pólya stops.

In *Proofs and Refutations*, Lakatos starts with a more or less completely specified proof of Euler's polyhedron formula, presented to the students by TEACHER, and the ensuing critical discussion about the proof takes off from there. For Lakatos, the 'dialectical' nature of mathematics, its fallibility, and its relation to epistemology and philosophy of science are central, whereas Pólya does not discuss these issues.

At the same time, the spheres of interest of Lakatos and Pólya overlap. Concerning the practice of not stopping at a proof but rather searching further for counterexamples, Lakatos cites Pólya as giving an early description:

> This standard pattern [of lemma incorporation] is essentially the one described in the classic of Pólya and Szegő: 'One should scrutinise each proof to see if one has in fact made use of all the assumptions; one should try to get the same consequence from fewer assumptions. . . and one should not be satisfied until counterexamples show that one has arrived at the boundary of the possibilities.'

Moreover, in discussing the different responses (monster barring, exception barring, monster adjustment) that one can take in the course of a proof and purported counterexamples to it, Lakatos again cites Pólya as:

> Monsterbarring in defense of the theorem is an important pattern in informal mathematics: 'What is wrong with the examples in which Euler's formula fails? Which geometrical conditions, rendering more precise the meanings of F, V, and E, would ensure the validity of Euler's formula?' (Pólya [40], I, Exercise 29.) The cylinder is given in Exercise 24. The answer is: '...an edge...should terminate in corners'. Pólya formulates this generally: 'The situation, not infrequent in mathematical research is this: A theorem has already been formulated but we have to give a more precise meaning to the terms in which it is formulated in order to render it strictly correct'.

In the preface to the paperback version of *Proofs and Refutations* Lakatos also thanks Pólya (and van der Waerden) for helping him to improve the discussion of the so-called exception barring method.

We thus see that Lakatos and Pólya certainly agree on many points (and arguably Pólya is the source of some of Lakatos's ideas). Nonetheless, it is also clear that Lakatos intended his work to be a contribution to the philosophy of mathematics, specifically its epistemology, whereas Pólya was concerned more practically with the education and training of the mathematical mind.

3.3 Summary of Lakatos scholarship

Proofs and Refutations has its origins in Lakatos's Ph.D. dissertation [45]. It was written between 1956 and 1960. The dialogue portion of the dissertation was extracted, modified, and serialized in four parts in the *British Journal for the Philosophy of Science* [43]. Apart from *Proofs and Refutations*, the only other work on the philosophy of mathematics that Lakatos published in his lifetime was *Infinite regress and the foundations of mathematics* [46]. When he died in 1976, Lakatos left behind a number of unfinished essays on the subject [47–49]. After *Proofs and Refutations*, Lakatos focused on the philosophy of science (he is famous for his debates with Kuhn and Feyerabend) rather than on the philosophy of mathematics.

After his death, Lakatos's students E. Zahar and J. Worrall prepared a new edition [1] of *Proofs and Refutations*, making it available in book form. The book also includes two other essays by Lakatos as appendices. Available as a book, *Proofs and Refutations* became more widely known; most scholarship on Lakatos thus begins then.

Zahar and Worrall added a handful of editor's footnotes to Lakatos's text. These editorial footnotes largely seek to temper some of Lakatos's claims against, for example, the 'rigorists' who have tried to make mathematical arguments ever more rigorous in the hope of achieving more certain knowledge. In addition to the editorial footnotes, Zahar and Worrall actually extend Lakatos's dialogue, adding at the end some discussion on proof checking.

Zahar and Worrall have been criticized for their editorial additions. The consensus seems to be that Zahar and Worrall miss Lakatos's point. Davis and Hersh [50], for example, are critical of the additions, saying that Zahar and Worral's claims about mechanical proof checking go against the grain of Lakatos's entire project. Bloor [51] says that Zahar and Worrall have "discharged their duty oddly" by qualifying Lakatos's remarks as they did. Larvor [52] also takes Zahar and Worrall to task for their editorial additions.

Lakatos's work has been reviewed by a number of famous philosophers. Quine [53], for example, reviewed it favorably (though briefly). Quine writes:

> The geometry is fascinating, but the purpose is philosophical. Lakatos is opposing the formalists' conception of mathematical proofs, which represents them as effectively testable and, once tested, incontrovertible. He is opposing the notion, so central to logical positivism, that mathematics and natural science are methodologically unlike.

In conclusion, Quine says:

> Lakatos does not in the end deny the feasibility of full formalistic rigour in mathematical proof, but he makes an eloquent and conclusive case for preferring the heuristic style of conjecture and refutation in mathematical treatises and textbooks.

(In *Proofs and Refutations* Lakatos takes aim at Quine, offering him up as an example of those who apparently have nothing to say about mathematical discovery. That Quine reviewed Lakatos's work positively might be odd, given that Lakatos seems to lump Quine in with the 'formalists' whom Lakatos is eager to attack.)

Not everyone has been so taken with Lakatos's work. Feferman [54], for example, while acknowledging the impressiveness of *Proofs and Refutations*, is nonetheless critical of it in several respects. He thinks that Lakatos's philosophy is too narrow and doesn't go far enough. Lakatos's philosophy focuses too much, for example, on claims of the form "All A's are B's" to the exclusion of claims having different logical forms, such as existential claims ('There is an odd perfect number') or singular propositions such as "$\sqrt{2}$ is irrational". Feferman points out that Lakatos's philosophy does not account for other ways in which mathematical knowledge grows, especially at higher conceptual levels instead of at the level of particular proofs. Examples of this kind of development that Feferman cites is the development of linear algebra, group theory, and topology. These theories arise through conceptual unification (he calls such developments "internal organizational, foundational moves"). Feferman also asks "What constitutes improvement in a proof?", "Is there no end to guessing?", and "What constitutes an initial proof? Where does it come from?" He argues that Lakatos either provides no answers or gives inadequate answers to these questions. Concerning the question of what counts as an improvement of a proof, Feferman's response that we do have informal criteria for this property is similar Sherry's view [55], who likewise argues that informal proofs can provide an answer to Feferman's question.

A number of scholars have been impressed by *Proofs and Refutations* to try to bring more prominence to the issues that Lakatos raises. But although Lakatos's *Proofs and Refutations* is an inspiring, rich, work, it is troubled. A Lakatos scholar, Brendan Larvor, writes:

> The fate of *Proofs and Refutations* is [...] paradoxical. Widely praised, it has enjoyed very little serious scholarly attention. This is perhaps because, unlike [...] Kuhn's scientific revolutions, *Proofs and Refutations* does not offer a simple logical scheme for philosophers to apply more or less mechanically to the history of any given discipline. *Proofs and Refutations* is, perhaps, too complex and ambiguous to be the first of a genre. [52]

If *Proofs and Refutations* is so troubled, then, what are we to make of Lakatos's project? According to Larvor, the legacy of Lakatos should not be an obsession with counterexamples and fallibility but rather in the "inner life" of mathematics [56]. A Lakatosian program, for Larvor, should be based on a sensitivity to the history of mathematics, an appreciation for the dynamics of its concepts and standards, and its relation with other fields.

Recent writers have been returning to Lakatos not so much because they wish to criticize or extend his work, but to be inspired by it and treat it as the beginnings of a new 'practice'-oriented philosophy of mathematics. This is the sentiment of the famous introduction [57] to a volume [58] on the history and philsophy of mathematics, in which the authors single out what they call the 'Maverick Tradition' in the philosophy of mathematics, of which Lakatos is a central figure. More terms have been coined to try to self-identify a new approach to the philosophy of mathematics, such as 'phenomenological':

> The phenomenological philosopher of mathematics starts by look at mathematics, and only then asks, and tries to answer, philosophical questions about the discipline. While the name 'phenomenological' has not always been used in describing this sort of philosophical approach to mathematics, papers advocating the phenomenological method so understood have been around at least since Lakatos's influential study, *Proofs and Refutations*. ([59], p. 3)

Others in the so-called phenomenological tradition include Rav [60–61], Corfield [62], Leng [59], and Hersh, who has written many papers [50, 63–69] on the 'practice'-based philosophy of mathematics.

What is new about the phenomenological/practice-oriented approach to the philosophy of mathematics? There is much less of an emphasis on ontological or metaphysical questions in mathematics (such as “Are mathematical objects real?” and “What are numbers?”). The attitude toward foundational questions (such as “What set-theoretic axioms suffice to formally reconstruct mathematics?” and “What is computability?”), which tends to favor formalism, is hostile (e.g., Lakatos, Rav) or at least demurring (e.g., Leng, Corfield). New questions raised by the ‘maverick’ tradition include “How does (informal) mathematics grow?”, “What are the main features of (informal) mathematical proof?”, “How do mathematical concepts evolve?”; other questions are “How are computers changing mathematical practice?”, “To what extent is mathematical knowledge founded on contingent social practices?”

The ‘maverick’ tradition does not necessary eschew traditional questions in the philosophy of mathematics; indeed, some of the older questions take on new aspects. For example, Kant’s main transcendental question [70] is “How is pure mathematics possible?” For Kant, mathematical knowledge is synthetic and a priori; the central question for him is to say how such knowledge is possible. In light of the increased prominence of social aspects of knowledge, one can re-ask Kant’s question: if our knowledge of mathematics depends, at least in part, on a community of mathematicians who maintain a body of knowledge, then how can such knowledge be a priori? It has been argued that formal mathematics seeks to undermine the strong social component of mathematical verification [39]. It seems, though, that rather than undermining or supplanting, the goal of formal mathematics is to enhance and support traditional mathematical work. This argument is made explicitly by Shankar [14], an early proponent of formal mathematics. (A recent expository article by Friedman [71] discusses in more detail the current situation in formal mathematics; Harrison [72] discusses some more of the background history of the subject.)

Another twist to the question arises in connection with computers in mathematics: can we have a priori mathematical knowledge on the basis of calculations/computations carried out by computer? Burge, for example, advocates [73–74] a theory of the a priori according to which testimony (such as a computer's testimony) preserves a priority. That the 'maverick' tradition is asking important questions is evidenced by the fact that 'mainstream' philosophers (such as Burge) are taking their questions seriously. But we digress.

Although many have been impressed by Lakatos, not all agree on how to interpret his work; nor is there widespread agreement that Lakatos is right on many of his central claims. Lakatos takes pains to exhibit mathematics as fallible, in the same (or a related) sense in which natural science is fallible. This means that mathematical propositions are essentially defeasible; they are conjectures, and they are in principle revisable. That natural science is fallible is a basic assumption in the philosophy of science; it is far less clear, and perhaps implausible, to extend fallibility to mathematics. But this is just what Lakatos does. What are the so-called potential falsifiers? What are the objects or phenomena which can show mathematical claims to be false? For Lakatos, *proofs* are akin to tests; proofs can show claims to be false. But this analogy is likely mistaken, and needs to be reinterpreted to make sense in mathematics [75]. And not everyone is happy to regard mathematics as fallible. See section **3.5** for a more thorough discussion of Lakatos's skepticism.

So much for a review of the literature on Lakatos. In the remainder of the chapter I describe my own interpretation of Lakatos in connection with formal proofs.

3.4 Some Basic Philosophical Issues in Lakatos's Work

Although Lakatos is regarded as a source or inspiration for a new approach to the philosophy of mathematics (the 'maverick' or 'phenomenological' approach), Lakatos does not avoid issues and questions in classical philosophy of mathematics. Nor can Lakatos avoid some of the main questions which 'foundationalist' philosophers ask.[3] There are at least three main philosophical worries that run through Lakatos's text:

- How can we claim to have knowledge a priori if our methods and concepts by which we come to have that knowledge are not fixed?
- What is fallible knowledge?
- How can we justify mathematical knowledge?

These are major questions in epistemology, and Lakatos deserves credit for bringing them up in the context of mathematics, where we might be a bit too quick (Lakatos would say *dogmatic*) to dismiss them, or diminish their importance.

Concerning the last question, Lakatos might reject it as ill-posed: he would say that to justify mathematical knowledge is to prove that it is true, which would establish it with certainty. But to say that a claim is justified is not to say that it is certainly true; it just means that we have adequate *reasons* to believe that it is true. Our reasons might not in fact be adequate; and even if they are, the claim that is justified might be false.

Lakatos is interested throughout *Proofs and Refutations* in justification, on what we might call the *justificatory structure* of mathematical arguments. Lakatos emphasizes that proofs in ordinary mathematics are *informal*, which are a source of interesting philosophical issues:

> The subject matter of metamathematics is an abstraction of mathematics in which mathematical theories are replaced by formal systems, proofs by certain sequence of well-formed formulae, definitions by 'abbreviatory devices' which are 'theoretically dispensable' but 'typographically convenient'. This abstraction was devised by Hilbert to provide a powerful technique for approaching some of the problems of the methodology of mathematics. At the same time there are problems which fall outside the range of metamathematical abstractions. Among these are all problems relating to the informal (*inhaltliche*) mathematics and to its growth, and all problems relating to the situational logic of mathematical problem solving.

To accomplish his historically informed project, Lakatos traces the history of Euler's polyhedron formula (EPF) and shows that, although the theorem was proved, it was also refuted, and then reproved, and re-refuted.

Lakatos does more than simply point out that mathematical knowledge evolves, or that mathematicians make mistakes (which goes without saying). Lakatos makes the more specific claim that mathematical knowledge (or at least some of it) grows through what he calls the *method of proofs and refutations* (MPR), as we discussed earlier. We shall look at the precise statement of MPR later, but for now we can understand it as the claim that mathematical claims may be both proved and refuted, and that proofs are improved by dealing with the refutations.[4]

We must also distinguish claims about the history of mathematics from claims about the nature of mathematics. Thus we must separate claims like *the history of Euler's polyhedron formula illustrates the method of proofs and refutations* from questions about what mathematical knowledge is like once we've reached the end of the method of proofs and refutations.

3.5 Lakatos and Mathematical Skepticism

Is Lakatos a skeptic about mathematics? If so, what kind of skeptic is he?

Certainly the tenor of Lakatos's work suggests that he is a skeptic about mathematics, in the sense that the central aim of his project is to limit our claims to mathematical knowledge, or to qualify the kind of knowledge produced by mathematical proofs. Let us approach the question by examining passages in *Proofs and Refutations* in which Lakatos explicitly advocates an apparently skeptical view:

> TEACHER: I hope that now all of you see that proofs, even though they may not *prove*, certainly do help to *improve* our conjecture. [. . .]

Using the Pólya's distinction between problems to find (in which the aim is to discover a mathematical object, such as a number or a figure, that satisfies certain conditions) and problems to prove (in which the aim is to demonstrate that a claim is true or false), Lakatos again reiterates his apparently skeptical view:

> ALPHA: It is wrong to assert that 'the aim of a "problem to prove" is to show conclusively that a certain clearly stated assertion is true, or else to show that it is false'. The *real* aim of a 'problem to prove' should be to *improve*—in fact, perfect—the original, *'naive' conjecture* into a genuine '*theorem*'.

Also, in a footnote, Lakatos writes:

> About 1800 the *rigour of proof* (crystal-clear thought experiment or construction) was contrasted with muddled argument and inductive generalisation. This was what Euler meant by '*rigida demonstratio*', and Kant's idea of infallible mathematics too was based on this concept. It was also thought that one proves what one has set out to prove. It did not occur to anybody that the verbal articulation of a thought-experiment involves any real difficulty. [. . .] The proof or thought-experiment carried full conviction without any deductive pattern or 'logical' structure.

The dialogue continues with ALPHA expanding on his comments:

> ALPHA: Our naive conjecture was 'All polyhedra are Eulerian'.
>
> The monsterbarring method defends the naive conjecture by reinterpreting its terms in such a way that at the end we have a *monsterbarring theorem*: 'All polyhedra are Eulerian'. But the identity of the linguistic expressions of the naive conjecture and the monsterbarring theorem hides, behind surreptitious changes in the meaning of terms, an essential improvement.
>
> The exception-barring method introduced an element which is really extraneous to the argument: convexity. The *exception-barring theorem* was: 'All convex polyhedra are Eulerian'.
>
> The lemma-incorporating method relies on the argument—i.e. on the proof—and on nothing else. It virtually *summed up the proof in the lemma-incorporating theorem*: 'All simple polyhedra with simply-connected faces are Eulerian'.
>
> This shows that (now I am using the term 'proving' in the traditional sense) *one does not prove what one sets out to prove*. Therefore no proof should conclude with the words: '*Quod erat demonstrandum.*'

Scholarship on Lakatos and contributions to the philosophy of mathematics that are inspired by Lakatos emphasize, to some extent, his focus on *mistakes* in mathematical argumentation. A recent contribution to Lakatos scholarship begins by saying that the 19th century was "a time of error for mathematics: not trivial oversights or amateurish confusions but fundamental mistakes in the understanding of mathematical concepts and the formulation of mathematical proofs” [77]. P. Davis defines the ‘authenticity’ of a mathematical proof and asserts that this property is established ‘by verifying that a sequence of transformations of atomic strings is legitimate’ [78]. He goes on to argue, based on a discussion of long calculations, that ‘the authenticity of a mathematical proof is not absolute, but only probabilistic’. A consequence:

> Proofs cannot be too long, else their probabilities go down and they baffle the checking process. To put it another way: all really deep theorems are false (or at best unproved or unprovable). All true theorems are trivial.

(It is not clear how philosophically sustainable this position really is.) P. Ernest, in his review of [55] (which will be discussed soon), writes that

> Fallibilism claims that mathematical knowledge (and truth) are relative, contingent, historical constructs. Absolute judgements with regard to truth/falsity and correctness/incorrectness cannot be made. The criteria and definitions involved vary with time, context, and never attain a final state. We can be pretty sure of some results, but the possibility of future revision or rejection cannot be eliminated. The source of this position is the early work of Lakatos.

R. Hersh also repeats Lakatos’s emphasis on mistakes: enumerating some neglected aspects of mathematics, we find:

> Mathematical knowledge is fallible. Like science, mathematics can advance by making mistakes and then correcting and recorrecting them. (This “fallibilism” is brilliantly argued in Lakatos’s *Proofs and Refutations*.) [66]

To be sure, some who work on Lakatos do not entirely accept the Lakatos’s apparent skepticism. D. Sherry, for example, takes issue with Lakatos’s ‘fallibilist’ philosophy:

> That mathematicians are fallible is hardly news. More newsworthy is the thesis that mathematics itself is fallible. Fallibilists believe that long standing communities of mathematicians

> have been or can be in error about cherished results. They point to the historical record as evidence of the 'fallible, corrigible, tentative and evolving' nature of mathematics (Tymoczko, 1986, p. 21). *Prima facie* it is difficult to deny propositions like '7+5=12'. Even so, the fallibilist claims there are propositions thought to have been established only to have been overturned in the progress of mathematics. Frequently mentioned is Euler's conjecture that the vertices and faces of a polyhedron outnumber its edges by 2. Crowe (1988) is typical: 'Euler's claim was repeatedly falsified' (p. 264). But our epigraph warrants caution, and, in fact, standard historical cases fail to support the thesis that mathematics is fallible, corrigible or tentative; they serve only as evidence that mathematics is evolving. Errors implicating an entire community of mathematicians do not exist in any but a philosophically problematic sense.

Sherry argues [55] that case-studies such as Lakatos's history of Euler's polyhedron formula show at best that mathematics is evolving, not that it is fallible. T. Koetsier [79] argues similarly. M. Leng criticizes those who, taken with Lakatos's case-study, do not "[take] pains to provide further examples which show mathematics to be fallible in any philosophically interesting sense" [59].

Moreover, it is not at all clear that a sensitivity to the history of mathematics demands that one give up on the epistemological unique features of mathematical knowledge. Lakatos is eager to show that mathematical knowledge is 'fallible' and 'quasi-empirical', but the argument for that simply seems to be that in the history of mathematics one can perceive clear mistakes being committed by mathematicians. Such observations should give us pause and back away from simple-minded dogmatism about mathematical knowledge and concede at least some sense in which mathematical knowledge is fallible. That is, if the only evidence for fallibilism in mathematics is the sparse existence of 'mistakes' (even by great mathematicians), then the fallibilism we obtain is not yet philosophically substantial. Lakatos seems to want point to something deeper than just the existence of errors, but it is not yet clear precisely how that is to be accomplished. These epistemological issues will be discussed later in the chapter.

Despite the overall tenor of Lakatos's work, one should not be too quick to ascribe to Lakatos a simple kind of skepticism. The reason for his skepticism about mathematical knowledge is not that humans make mistakes. In the introduction to *Proofs and Refutations*, Lakatos places his work in the context of a long-standing discussion:

> For more than two thousand years there has been an argument between *dogmatists* and *sceptics*. The dogmatists hold that—by the power of our human intellect and/or senses—we can attain truth and know that we have attained it. The sceptics on the other hand either hold that we cannot attain the truth at all (unless with the help of mystical experience), or that we cannot know if we can attain it or that we have attained it. In this great debate, in which arguments are time and again brought up to date, mathematics has been the proud fortress of dogmatism. [. . .] Most sceptics resigned themselves to the impregnability of this stronghold of dogmatist philosophy. A challenge is now overdue.

Lakatos does indeed challenge the *dogmatist* stronghold, and thus is apparently taking up the skeptical banner. There are two reasons, though, to refrain from putting Lakatos squarely in the skeptical camp.

First, by invoking a very old debate between two named parties, it would seem that Lakatos is trying to distance himself from both of the parties and thus position himself as trying to transcend the apparently intractable fight. This reminds us of Kant's attempt to try to go beyond the old fights between the rationalists and the empiricists. (At the same time, it is acknowledged that Lakatos does, at the end of the passage, seem to take the side of the skeptics.)

The second reason to hesitate to brand Lakatos a skeptic, or at least to qualify his skepticism, is to examine whether his philosophy is successful at establishing skepticism on his own terms. Thanks to *Proofs and Refutations*, can we conclude that

- we cannot attain mathematical truth, or
- we cannot know if we can attain mathematical truth, or
- we cannot know if we have attained mathematical truth?

It is not clear that any of these are clearly present in Lakatos's philosophy. To be sure, concerning, say, claim (1), this is apparently consistent with Lakatos's philosophy, especially in what Lakatos calls 'mature theories'.

> TEACHER: The theorem does not *always* differ from the naive conjecture. We do not necessarily improve by proving. Proofs improve when the proof-idea discovers unexpected aspects of the naive conjecture which then appear in the theorem. But in *mature* theories this might not be the case. It is certainly the case in young, *growing* theories. This intertwining of discovery and justification, of improving and proving is primarily characteristic of the latter.

In mature mathematical theories, then, some kind of stability is achieved. Proofs carried out in such theories may not reveal any unexpected elements, so that proofs can come to an end. Of course, Lakatos does not say that *truth* is attained or that we *know* that truth is attained, but this is perhaps as close as Lakatos will come to allowing that.

3.5.1 Fallibilism in mathematics

I would submit that another troublesome problem for those who would champion a Lakatosian philosophy of mathematics is, first of all, to articulate a *fallibilist* epistemology that, second, acknowledges that there is something special about mathematical knowledge. Even if mathematical knowledge turns out to be fallible in some robust sense—which is *not* based merely on the (inevitable) presence of 'mistakes'—one would want a satisfying account of why mathematical knowledge is (or appears to be) so epistemically privileged.

One problem, in the first place, is to even say what fallible *knowledge* is. Some work has already been done in this direction. One of the first problems is to even say what fallibilist knowledge *is*. Following the traditional analysis of knowledge as justified true belief, to say that something is known fallibly involves us, at least initially, in a problem: if p is known fallibly, then, roughly speaking, p could have been false. But in the case of mathematical knowledge, which is supposed to be necessary, it could not be false. Thus, if p is a piece of mathematical knowledge, then it cannot be known *fallibly*, because it could not be false. Some early work by S. Haack, for example, articulates the problem.

> When it comes to the question of whether we are fallible, not only with respect to our ordinary, empirical beliefs, but also with respect to our mathematical beliefs, Peirce's confident anti-dogmatism seems to falter. Peirce believes that the truths of mathematics are necessary. And he seems to suspect that the necessity of mathematical truths somehow precludes the possibility of our being mistaken in our mathematical beliefs; for when he claims that fallibilism does extend even to mathematics he is tempted to compromise his commitment to the necessity of mathematical truths, and to hint that mathematical inference is, after all, only probable, and when, elsewhere he stresses the necessary character of mathematical truths, he also hints that we are fallible only with respect to our factual beliefs.

In Haack's brief summary of Peirce's philosophy we can perhaps see an example of what Lakatos was referring to when he mentions how the skeptics 'resigned themselves to the impregnability of this stronghold of dogmatist epistemology' (that is, mathematics). She goes on to survey some senses of 'fallibilism' that might have given rise to Peirce's waffling, and she relates her discussion to Lakatos's fallibilist philosophy of mathematics. B. Reed also lays out the problem: although fallibilism seems to be a plausible feature of our knowledge, it is not incompatible with the existence of necessary truths (e.g., mathematical truths); the puzzle is to explain such fallible knowledge.

3.6 A Lakatosian Challenge

An interest or even a defense of formal proofs does not imply that there are not problems in the philosophy of mathematics that cannot be well understood as questions about formal proofs. If this is the kind of philosophy of mathematics against which Lakatos was reacting, then surely Lakatos is in the right.

But *Proofs and Refutations* cannot help but being a work about proofs, and therefore at least in part about the structure of justification in mathematics. One of the central questions of *Proofs and Refutations* is: what is the structure of justification in informal mathematics as contrasted with formal mathematics? As a response, Lakatos advances (or rather: describes) the method of proofs and refutations (MPR). If I have been successful, I will have argued that MPR is characteristic of mathematical proof no matter whether formal or informal.

4 A Formal Proof of Euler's Polyhedron Formula

4.1 Introduction

In this chapter I discus a formalization of Euler's polyhedron formula, which asserts for a polyhedron p that

$$V - E + F = 2,$$

where V, E, and F are, respectively, the numbers of vertices, edges, and faces of p.

Section **4.2** is a brief survey of the history of Euler's formula, and justifies the choice of the particular informal proof, due to Poincaré, that was singled out for formalization.[1] Section **4.3** sketches Poincaré's linear algebraic proof, as presented by Lakatos. Section **4.4** is devoted to the formalization itself. Finally, I reflect on some of problems related to the formalization in section **4.5** and close with some suggestions for further avenues of research in section **4.6**.

4.2 A Brief History of Euler's Polyhedron Formula

Lakatos's history [1] of Euler's polyhedron formula is an entertaining discussion of some of the historical twists and philosophical problems surrounding the result. Indeed, a motivation for carrying out the formalization described here was to study Lakatos's philosophy of mathematics.

Euler first discussed his formula in a 1750 letter to Christian Goldbach:

> Recently it occurred to me to determine the general properties of solids bounded by plane faces, because there is no doubt that general theorems should be found for them, just as for plane rectilinear figures, whose properties are: (1) that in every plane figure the number of sides is equal to the number of angles, and (2) that the sum of all the angles is equal to twice as many right angles as there are sides, less four. Whereas for plane figures only sides and angles need to be considered, for the case of solids more parts must be taken into account. [80]

Euler does not use the term *polyhedra* but rather 'solids bounded by plane faces'. He goes on to enumerate some interesting propositions about polyhedra such as:

> 6. In every solid enclosed by plane faces the aggregate of the number of faces and the number of solid angles exceeds by two the number of edges, or $F + V = E + 2$.[2]

and

> 11. The sum of all plane angles is equal to four times as many right angles as there are solid angles, less eight, that is $4V - 8$ right angles.[3]

Euler expresses surprise that he has not been able to find a precedent for these relations:

> I find it surprising that these general results in solid geometry have not been previously noted by anyone, so far as I am aware;[4] and furthermore, that the important ones, Theorems 6 and 11, are so difficult that I have not yet been able to prove them in a satisfactory way.

It was not long before Euler presented his results publicly [84]. Like the letter to Goldbach, Euler's paper was programmatic: he was trying to encourage the study of three-dimensional solids as an extension of planar geometry. The 'most difficult' propositions he mentioned to Goldbach were discussed in detail, though he acknowledges that his presentation does not constitute a proof. Indeed, in the preface to his paper Euler qualifies his work thus:

> I for one have to admit that I have not yet been able to devise a strict proof of this theorem. As however the truth of it has been established in so many cases, there can be no doubt that it holds good for any solid. Thus the proposition seems to be satisfactorily demonstrated.

Euler was not satisfied with the unfinished state of his theorem and continued working with polyhedra. Eventually he did find a satisfactory proof [85].

Perhaps because of its simplicity and elegance, many other mathematicians studied the polyhedron formula and tried to give new proofs of Euler's polyhedron formula. Cauchy, for example, connected the study of polyhedra to planar graphs: project a polyhedron onto a plane, triangulate it, and take away one triangle at a time in a way that preserves χ until only a triangle remains; we obtain the desired result $\chi = 2$ by noting that the projection with which we started 'removes' a face from the polyhedron (which effectively sends one of the polyhedron's faces onto an unbounded planar region). Unlike Euler, whose conception of polyhedra was that of solid (which one can slice, as with a knife), Cauchy apparently viewed polyhedra as wireframes.

Poincaré provided a new conception of polyhedra based on incidence matrices with which he gave his own proof [86–87] of Euler's formula.[5] Poincaré's abstract, combinatorial conception of polyhedra makes no mention of points in $\mathbf{R}^3$, nor does it come from projecting polyhedra onto a plane. Poincaré's approach even allows for polyhedra of arbitrary dimension; the general result[6] states that

$$\sum_{k=0}^{d-1}(-1)^k N_k = 1 + (-1)^{d+1},$$

where the integer d is the dimension of p and N_k is the number of k-polytopes of p. The classical three-dimensional version stated by Euler is obtained by setting $d := 3$. The familiar property of a polygon that the number of vertices is equal to the number of edges is obtained by putting $d := 2$. (And a 1-dimensional polyhedron is just a line segment with its two endpoints, which also falls out of the general Euler relation by putting $d := 1$.)

So far no definition of polyhedron has been given, nor has any restriction been imposed on the domain of validity of Euler's relation. It is a commonplace that one has to be careful with how one defines one's terms, and the term 'polyhedron' is no exception. Grünbaum writes:

> The 'Original Sin' in the theory of polyhedra goes back to Euclid, and through Kepler, Poinsot, Cauchy, and many others . . . in that at each stage, the writers failed to define what are the 'polyhedra'. [88]

In addition to defining polyhedra, it is a further task to specify the domain of validity for Euler's relation to hold; it turns out that around the time of Cauchy's proof in the early 19th century, it started to become clear to mathematicians that Euler's polyhedron formula does not hold for all polyhedra. In 1811, for example, L'Hullier described 'exceptions' to

Euler's polyhedron formula, classifying them into three kinds. Research on polyhedra in the 19th century gradually revealed that for Euler's relation to hold one should focus on the property of being a homology sphere.

Poincaré's definition, on which the formalization to be described is based, is probably the simplest to describe. Following Poincaré, a polyhedron is characterized by a list of *incidence matrices*, which can be understood as functions f from a cartesian product $A \times B$ of sets A and B to $\{0, 1\}$, where $f(a, b) = 1$ is understood as 'a is incident with b' and $f(a, b) = 0$ is understood as 'a is not incident with b'. Thus to specify a polyhedron of dimension $d + 1$, one just gives d incidence matrices. Let us call such a structure an *abstract* or *combinatorial polyhedron*.

4.3 Poincaré's Proof of Euler's Polyhedron Formula

As part of his algebraic topological program, Poincaré gave a new proof of Euler's polyhedron formula. This section sketches Poincaré's proof; for a more detailed discussion, consult Lakatos [1] (chapter 2) or Coxeter [89] (chapter 9).

Later I discuss the relationship between the concepts of polyhedron and the crucial condition of being a homology sphere as they are defined by Lakatos and in alternative definitions. The advanced reader should note before proceeding that the definitions of polyhedron and being a homology sphere employed in Lakatos's proof and which are about to be disucssed are *not* the same as the concepts that come out of other (perhaps more familiar) approaches to polyhedra. The polyhedra that we shall consider here lack a good deal of geometric content; they are essentially combinatorial structures.

In Poincaré's framework (as presented by Lakatos), a (three-dimensional) polyhedron is determined by five pieces of data:

- A set of vertices (the 0-polytopes),
- A set of edges (the 1-polytopes),
- A set of faces (the 2-polytopes),

- An incidence matrix that says which vertices belong to which edges, and
- An incidence matrix that says which edges belong to which faces.[7]

Conventionally there is also a 3-polytope, namely the whole polyhedron p, and there is a (derived) incidence matrix declaring that all faces are incident with p. Symmetrically, there is a single (-1)-polytope and we declare that is incident with each vertex.

More generally, a d-dimensional polyhedron is characterized by a pair $(\mathcal{F}, \mathcal{I})$ ($\mathcal{F}$ for 'faces', $\mathcal{I}$ for 'incidences') of finite sequences, where

- $d = \operatorname{len} \mathcal{F}$,
- $\operatorname{len} \mathcal{F} > 0$,
- $\operatorname{len} \mathcal{I} = \operatorname{len} \mathcal{F} - 1$,
- For $0 \leq n < \operatorname{len} \mathcal{F}$, we have that $\mathcal{F}_n$ is a non-empty finite set (the set of k-polytopes of p), and
- For $0 \leq n < \operatorname{len} \mathcal{I}$, we have that $\mathcal{I}_n$ is an incidence matrix for $\mathcal{F}_n$ and $\mathcal{F}_{n+1}$.

In the more general setting we again have the stipulation that there is one d-dimensional polytope, namely p, that is incident with all $(d-1)$-polytopes; also, there is the stipulation that there is a -1-dimensional polytope that is incident with all 0-polytopes.

Theorem 1 *For every simply connected polyhedron p of dimension $d > 0$, we have*

$$\sum_{k=0}^{d-1} N_k = 1 + (-1)^{d+1},$$

where d is the dimension of p and N_k is the number of polytopes of p of dimension k.

For a polyhedron p and an integer k, let the k-chains of p be the powerset of the set of k-polytopes of p. The k-chains of p naturally form a vector space over the two-element field F_2, where vector addition is represented by symmetric difference; call this space C_k. The relation between C_k and polyhedra can be seen in the fact that the dimension of C_k is precisely N_k, the number of k-polytopes of p. (Reason: the singleton subsets of $\mathcal{F}_k$ are a basis for C_k.) The boundary $\partial_k c$ of a k-chain c is the $(k-1)$-chain

$$\{x \in \mathcal{F}_{k-1} \colon x \text{ is incident with an odd number of } k\text{-polytopes of } c\}.$$

In other words, a $(k-1)$-polytope x belongs to the boundary of a k-chain c iff

$$\sum_{y \in c} \mathcal{I}_{k-1}(x, y) = 1,$$

where the sum is taken modulo 2. The boundary operation ∂_k is a linear transformation from C_k to C_{k-1}. It turns out that the k-chains c whose boundary is empty (all $(k-1)$-polytopes are incident with c an even number of times) form a subspace, Z_k, of C_k. Such k-chains are called k-circuits (sometimes also called k-cycles). Another important subspace of the k-chain space C_k consists of those k-chains that are the boundary of a $(k+1)$-chain; for lack of a better name, let B_k (for 'bounding') denote this subspace.

The property of being a homology sphere is the property that $B_k = Z_k$, that the k-circuits are the bounding k-chains. The inclusion $B_k \subseteq Z_k$ says that $\partial_{k+1}\partial_k \equiv 0$. The reverse inclusion intuitively says that the only way something can be a cycle is if it 'traverses' a 'face'. This fails in cases where, for example, a face has a hole in it (one can go around the boundary of the inner hole, but there's no face that one is traversing).

We are now ready to prove Theorem 1.

Proof. If p is a homology sphere, then

$$Z_k = B_k,$$

so that

$$\dim Z_k = \dim B_k.$$

Since $N_k = \dim C_k$, we have by the rank+nullity theorem that

$$N_k = \dim C_k = \dim B_{k-1} + \dim Z_k = \dim B_{k-1} + \dim B_k.$$

Thus

$$\sum_{k=0}^{d-1} (-1)^k N_k = \sum_{k=0}^{d-1} (-1)^k (\dim B_{k-1} + \dim B_k) = \dim B_{-1} + (-1)^{d-1} \dim B_{d-1}.$$

The last equation follows because of the hypothesis the p is a homology sphere. Now $\dim B_{-1} = 1$, since B_{-1} is a two-element vector space (it contains the empty chain as well as the singleton chain containing the unique -1-polytope). And $\dim B_{d-1} = 1$ for the same reason: it contains the empty chain as well as the 'full' chain containing all the $(d-1)$-polytopes, so that it has at least two elements; if c is a $(d-1)$-chain different from the 'full' $(d-1)$-chain and the empty chain, then it is not in the range of ∂_d, since by stipulation *all* $(d-1)$-polytopes are incident to the unique d-polytope p. The proof is complete. □

4.4 The Formalization

This section describes the formalization of Poincaré's proof of Euler's polyhedron formula that was carried out in the MIZAR system.

MIZAR is based on classical first-order logic with equality and Tarski-Grothendieck set theory, a strong theory of sets that is equivalent to the Zermelo-Fraenkel theory together with an axiom asserting the existence of arbitrarily large inaccessible cardinals.

Among the many candidate systems (*e.g.*, ISABELLE, HOL LIGHT, COQ) with which the formalization could have been carried out, MIZAR was selected because of its familiar logical foundations (first-order set theory), its everyday knowledge representation language (dependent types, structures, flexible notation for functions and predicates), its standard proof language (a kind of natural deduction), and its large library of formalized mathematical knowledge on which one can build.[8] But it must be admitted that the choice of MIZAR over the other candidates was somewhat arbitrary. Nonetheless, it seems plausible that, if one were to compare the formalization in MIZAR under discussion with a formalization of the same proof in some other system, one would find considerable overlap.[9]

4.4.1 Main formalizations

One often finds when formalizing that, in addition to the logical and mathematical details in a formal proof that must be supplied, one must also formalize various kinds of 'background' knowledge. And one often finds that the simplest mathematical facts are (apparently) missing from the library of formalized mathematics[10]. Like Euler writing to Goldbach, one might be surprised that 'these general results have not been previously noted by anyone'.[11] The formalization of Poincaré's proof of Euler's polyhedron formula in MIZAR was no exception to this phenomenon. But this is understandable; just as libraries of implemented algorithms for various programming languages do not eliminate the need for programmers to adjust them to their specific problems, so too do general mathematical facts in a formal library require further specification before they can be applied.

The contribution naturally divided into three MIZAR 'articles' (collections of definitions, theorems). They were:

- `RANKNULL`: The rank+nullity theorem [91];
- `BSPACE`: The vector space of subsets of a set based on symmetric difference [92]; and
- `POLYFORM`: Euler's polyhedron formula [93].

I now briefly discuss some notable features of these formalizations.

4.4.1.1 The rank+nullity theorem

The rank+nullity theorem states that if T is a linear transformation from a finite-dimensional vector space V to a finite-dimensional space W, then

$$\dim V = \dim \operatorname{im} T + \dim \ker T.$$

I was able to straightforwardly formalize a standard proof [94] of the result, but some formal groundwork had to be laid for that to be possible.

Much basic linear algebra has already been formalized in MIZAR; there are a number of theorems and definitions concerning subspaces [95], linear combinations [96], dimensions of vector spaces [97] and linear spans of sets of vectors [98]. But some of the linear algebraic facts involved in a proof of the rank+nullity theorem were unavailable and had to be formalized. To carry out the formalization, I defined:

1. the image and kernel of a linear transformation, and the fact that these form subspaces of the domain and range of a linear transformation;
2. the restriction of a linear combination to a set of vectors; and
3. the image and inverse image of a linear combination under a linear transformation.

The first item is straightforward, but the second and third items may require some explanation. In MIZAR, a linear combination is represented as a function from a vector space to the field of scalars whose carrier (the set of vectors not mapped to zero) is finite.[12] The restriction of a linear combination l on a vector space V to a subset X of V is thus naturally represented by the function

$$\lambda v \in V. \begin{cases} l(v) & \text{if } v \in X \\ 0_V & \text{otherwise} \end{cases}.$$

Suppose that T is a linear transformation from a vector space V to a vector space W, both over a field F, and that l is a linear combination of vectors in V. Thus l represents the linear combination

$$a_1 v_1 + \cdots + a_n v_n,$$

where n is a natural number, $a_k \in F$ and $v_k \in V$ and $a_k \neq 0_F$ $(1 \leq k \leq n)$. Since T is a linear transformation, we ought to have

$$T(a_1 v_1 + \cdots + a_n v_n) = a_1 T(v_1) + \cdots + a_n T(v_n).$$

Thus, it is natural to define the image of l under T to be the MIZAR-linear combination

$$\lambda w \in W. \begin{cases} l(T^{-1}(\{w\})) & \text{if } w \in \operatorname{im} T \\ 0_F & \text{otherwise} \end{cases}.$$

The problem with this definition is that it works only if T is injective. We are supposed to define the image of any linear transformation T on any linear combination l, so we need to allow for the possibility that some of the $T(v_i)$'s are equal. A definition that gets around this problem is

$$T(l) := \lambda w \in W. \sum l(T^{-1}(w)).$$

This definition allows us to add together the coefficients, given by l, of those vectors in V that are identified by T. It is interesting to note how the formal definition of the image of a linear combination under a linear transformation differs from the informal (or semi-formal) notation above. This case provides an interesting example of a formal analysis of informal notation.

The inverse image operation also deserves to be mentioned. Suppose that X is a subset of a vector space V, that T is a linear transformation from V to W, and that l is a linear combination of $T(X)$ (that is, that l is a function from W to F with finite support whose value is 0_F outside of $T(X)$). This is a precise way of saying that l looks like

$$b_1 T(v_1) + \cdots + b_n T(v_n),$$

for some natural number n and $v_k \in X$. We want to say that the inverse image of l is the linear combination

$$b_1 v_1 + \cdots + b_n v_n.$$

This is correct, but only on the assumption that the vectors $T(v_1), \ldots, T(v_n)$ are distinct. One way to ensure this is by requiring that $T|X$ is one-to-one, and that is in fact what I did when defining the inverse image operation in MIZAR and suited the formalization task at hand. As it stands, the inverse image operation in MIZAR is a partial operation. The restriction of injectivity of the restriction is, however, not entirely unnecessary and it would be valuable to extend the formalization to account for the general case.

4.4.1.2 The vector space of subsets of a set based on symmetric difference

Another result needed for a formalization of Poincaré's proof of Euler's polyhedron formula is the fact that the power set of a set forms a vector space over the two-element field F_2. Vector addition is symmetric difference, and scalar multiplication is defined by

$$0 \cdot x := \emptyset, 1 \cdot x := x.$$

This fact is to be standard, but I was unable to find any conventional name for this space. For lack of a better notation, let $B(X)$ (for 'Boole') be the vector space of subsets of X based on symmetric difference.

Approximately half of the article BSPACE is devoted to proving that $B(X)$ is indeed a vector space. The other half is devoted to some facts about the linear algebraic features of the family of singleton subsets of X, namely that

- they are a linearly independent set of vectors, and
- if X is finite, then they span $B(X)$.[13]

4.4.1.3 Polyhedra

Perhaps surprisingly, the formalization of Poincaré's proof was rather straightforward. The highlight of the article is the generalized Euler polyhedron formula, as well as special cases for one-, two-, and three-dimensional polyhedra. The statement of the main theorem, in the MIZAR syntax, is

```
p is homology-sphere implies p is eulerian;
```

where of course p has type polyhedron. The term 'Eulerian' is a neologism that means that a polyhedron satisfies Euler's relation; it appears in Lakatos [1]. The definitions of the two properties are

```
p is homology-sphere
 means
for k being Integer
 holds k-circuits(p) = k-bounding-chains(p);
```

and

```
p is eulerian
 means
Sum (alternating-proper-f-vector(p))
  = 1 + (-1)|^(dim(p)+1);
```

(The f-vector of a polyhedron p is the sequence of natural numbers

$$s := N_{-1}, N_0, N_1, \ldots, N_d,$$

where $d = \dim p$ and N_k is the number of polytopes of dimension k. (It could also be reasonably defined as a bi-infinite sequence indexed by the integers containing the terms displayed above with all other terms being 0.) The terminology is standard [99], but to ease the formalization two related neologisms were coined: *proper f-vector* and *alternating proper f-vector*. By definition deleting the first and last terms of s gives the proper f-vector of p; alternating the signs of the sequence yields the alternating proper f-vector of p.) I also proved a lemma on telescoping sums that apparently did not exist in the MIZAR library:

```
for a,b,s being FinSequence of INT
 st len s > 0 &
    len a = len s & len b = len s &
    (for n being Nat st 1 <= n & n <= len s
      holds s.n = a.n + b.n) &
    (for k being Nat st 1 <= k & k < len s
      holds b.k = -(a.(k+1)))
 holds Sum s = (a.1) + (b.(len s))
```

The lemma is a formalization of the claim that if s, a, and b are are sequences of integers, all of the same length n, and if $s = a + b$ but $b_k = -a_{k+1}$, then $\sum s = a_1 + b_n$. In Poincaré's proof, thanks to the property of being a homology sphere, the sum on the left-hand side of the Euler relation turns out to be telescoping in this way.

4.5 Discussion

4.5.1 Definition of polyhedron and being a homology sphere

Lakatos's presentation of Poincaré's proof of Euler's polyheron formula differs from Poincaré's own presentation, and his definitions differ from the definition of polyhedron and the property of being a homology sphere that grew out of Poincaré's work.

The polyhedra that Lakatos considers have very little geometric content; they are essentially combinatorial structures. They are essentially structures for a three-sorted first-order language L with sorts for vertices, edges, and faces, together with two binary relations for the incidence relations. (One could equally well consider a single binary relation, taken as the union of the two relations in Lakatos's definition.) Perhaps a better term for these structures would be something like 'pre-polyhedron'; a 'polyhedron' would then be a structure for L that satisfies the property that $\partial_k \partial_{k+1} \equiv 0$. A better label for what Lakatos is defscribing would be perhaps 'abstract polyhedra'. One could then object and say that Lakatos has not proved Euler's formula for *polyhedra*, but rather just for *abstract polyhedra*. Following this line of thought, one could object to the claim that Lakatos (in the guise of the character Epsilon) has given a proof of Euler's polyhedron formula; from this it follows that the formalization described above is not a formal proof of Euler's polyhedron formula. In the following subsection a more geometrically contentful definition of polyhedron—which flows from Poincaré's original work—will be described. From that perspective we will be able to better understand Lakatos's abstract/combinatorial definition.

4.5.1.1 Algebraic topological definition of polyhedron

The material in this section is based largely on a standard treatment (by L. S. Pontryagin) of algebraic topology [100]. We shall eventually define a geometrically contentful concept of polyhedron, then abstract polyhedron. The latter, though lacking some geometric content, has more structure than Lakatos's polyhedra.

Definition 1 *A* **simplex** *of dimension d is the convex hull of an affinely independent set of $d-1$ points in a real linear space.*

Intuitively, then, a simplex is a generalization of a tetrahedron; it is supposed to be the simplest kind of geometrical arrangement.

Definition 2 *A* **complex** *is a finite set K of simplexes of a finite-dimensional real linear space such that*

1. *If A is in K, then every face of A is also in K, and*
2. *Every two simplexes in K are properly situated.*

We then define:

Definition 3 *A* **polyhedron** *is the union of the simplexes in a complex.*

Polyhedra as thus defined clearly have considerable geometric content. Their points are contained in a (finite-dimensional) real linear space, whereas Lakatos's polyhedra are mere combinatorial objects. We can abstract away from the analytic character and position of the parts of a polyhedra as just defined to get the concept of an *abstract complex*.

Definition 4 *An* **abstract complex** *is a subset $\mathcal{K}$ of the powerset $\mathcal{P}(X)$ of a finite set X such that*

1. *Every singleton subset of X is a member of K, and*
2. *If A is in $\mathcal{K}$, then every non-empty subset of A is also in $\mathcal{K}$.*

As a simple example, we have that for any finite set X, the set $\mathcal{P}X - \{emptyset, X\}$ is an abstract complex.

We can also see in this example why it is natural to include both $\emptyset$ and the set of all vertices of an abstract polyhedron as belonging to it. We obtain $\emptyset$ by relaxing the second condition in 4 to say that if A is in $\mathcal{K}$, then every subset of A is also in $\mathcal{K}$ (not just the non-empty subsets of A). And allowing the set of all vertices of $\mathcal{K}$ to be a member of K both conditions in the definition are maintained. The dimension of the new abstract simplex $\emptyset$ is naturally -1, and the dimension of the set of vertices of $\mathcal{K}$ is naturally $\dim \mathcal{K} + 1$. Let us define this new concept.

Definition 5 *A* **extended abstract complex** *with vertices X is a subset of $\mathcal{P}X$ such that*

1. *Every singleton subset of X is a member of $\mathcal{K}$,*
2. *If A is in $\mathcal{K}$, then every subset of A is also in $\mathcal{K}$, and*
3. *X is in $\mathcal{K}$.*

Clearly, from an abstract complex $\mathcal{K}$ with vertices X we produce an extended abstract complex $\mathcal{K}'$ with vertices X: $\mathcal{K}' = \mathcal{K} \cup \{\emptyset, X\}$.

It is with the help of abstract complexes that we can understand Lakatos's definition of polyhedra. Pointryagin uses the term **abstract simplex** to mean a member of an abstract complex. If we use the term 'polytope' instead, we start using Lakatos's terminology. Given an abstract complex $\mathcal{K}$, we can define a binary relation R on $\mathcal{K}$ by the rule

$$R(a,b) \quad \text{iff} \quad \text{there exists a vertex } x \text{ of } \mathcal{K} \text{ such that } a \cup \{x\} = b$$

R holds between abstract simplexes a and b of $\mathcal{K}$ just in case b is exactly one vertex larger than a.

Using this relation, we can convert an abstract complex $\mathcal{K}$ into a Lakatos polyhedron p in a natural way: the k-polytopes of p are precisely the abstract simplexes of $\mathcal{K}$ of cardinality $k+1$, and the incidence matrices of p are just the restrictions of the induced relation R to the k and the $(k+1)$-polytopes of p.

This transformation process also works for extended abstract complexes. Note that, when applied to extended abstract complexes, we get that $\emptyset$, the unique -1-dimensional abstract simplex, is incident with every 0-dimensional abstract simplex. We also get that the set X of vertices (assumed to be among the abstract simplexes of an extended abstract complex) is incident with every abstract simplex of the form $X - \{a\}$ $(a \in X)$. This is precisely what Lakatos asks us to postulate.

Let us denote by $P(\mathcal{K})$ the Lakatos polyhedron that is obtained from an (extended) abstract complex $\mathcal{K}$ in this way. To verify that $P(\mathcal{K}$ is really a Laktos polyhedron, we must check that $\partial_k \circ \partial \equiv 0$.

Theorem 2 *For every extended abstract complex $\mathcal{K}$ with vertices X, we have that $P(\mathcal{K})$ is a Lakatos polyhedron, i.e., $P(\mathcal{K})$ satisfies the condition that $\partial_k \circ \partial_{k+1} \equiv 0$, for every $0 < k \leq \dim \mathcal{K}$.*

Proof. First, we shall give a set-theoretic characterization of the boundary operator on the $P(\mathcal{K})$'s. Using that characterization we shall show that $\partial\partial \equiv \emptyset$.

The boundary $\partial_k(a)$ of a k-polytope a is simple to describe: it is $\{a - \{x\} : x \in a\}$. This just reflects condition (2) in the definition of extended abstract complexes.

The description of $\partial_k(C)$ for k-chains C is somewhat more complex. This reflects the fact that the k-polytopes in the k-chain C can share elements. We need to keep track of the parity of incidences.

Indeed, we have the following characterization: $A \in \partial_k(C)$ iff there exists a vertex x and an element c of C such that $A = c - \{x\}$ and $x \in \Delta(c)$. Here $\Delta(c)$ is understood as a generalized symmetric difference operator defined on collection of sets:

$$\Delta(Y) := \{y \in \bigcup Y : |\{Z \in Y : y \in Z\}| \text{ is odd}\}.$$

Given this characterization, we have that $A \in \partial_k\partial_{k+1}(C)$ iff there exists a vertex x and an element d of $\partial_{k+1}(C)$ such that $A = c - \{x\}$ and $x \in \Delta(\partial_k(C))$. But the condition that $x \in \Delta(\partial_{k+1}(C))$, is impossible. For

$$x \in \Delta(\partial_{k+1}(C))$$

iff

$$|\{B \in \partial_k(C) : x \in B\}| \text{ is odd},$$

which holds, by definition of ∂, iff

$$|\{B : \exists c \exists y (c \in C \wedge y \in X \wedge B = c - \{b\} \wedge y \in \Delta(c) \wedge y \in B\}| \text{ is odd}.$$

But note that the condition that B is supposed to satisfy is contradictory: $B = c - \{v\}$, so B excludes v, but the last condition asserts that y is in B. So the comprehended set is empty, so its cardinality is certainly not odd. □

Thus the incidence structure $P(\mathcal{K})$ is indeed a Lakatos polyhedron.

The Lakatos polyhedra that we obtain in this way from (extended) abstract complexes are a special subclass of the class of all Lakatos polyhedra. The main feature of $P(\mathcal{K})$ is that *a $(k+1)$-polytope is incident only with $k+1$ k-polytopes.* This property is not shared by all Lakatos polyhedra.

The reader may be familiar with another definition of 'polyhedron' in algebraic topology as the set of points of a complex. In such a setting one has chains and a boundary operator. The approach taken here is rather more general than the approach taken in algebraic topology in terms of complexes because the polyhedra of this approach are more abstract; they lack a good deal of geometrical content that's contained in the definition of complex (even abstract complex). The main difference is that, with complexes (even abstract complexes), one has that the boundary operator satisfies $\partial_k \partial_{k+1} \equiv 0$. However, in the approach taken here, the boundary operator is *not* nilpotent. (See § **6.2.2.3** for a simple counterexample.) One needs to build nilpotency in as an assumption on the class of 'polyhedra structures' considered here.

In the approach to polyhedra taken here, there are -1- and $(\dim p)$-dimensional polytopes, even though those don't appear in the usual definition of the term 'polyhedra', and don't necessarily arise in the algebraic topological approach. These objects are conventions.

Another important difference between the approach to polyhedra in algebraic topology and the approach here is that here there is no apparent discussion of an *orientation* of the vertices of a polyhedron.[14] This is related to the fact that the vector spaces that we are considering are over the two-element field F_2. One can prove in the algebraic topological setting that, if one considers coefficients for chains as coming from F_2, then orientation indeed plays no role (because positvely and negatively oriented polytopes are the same thing, as $+a = -a$ over F_2.).

4.5.1.2 Simple connectedness and homology spheres

The definition of simple connectedness employed in Lakatos is somewhat at odds with current mathematical terminology. Recall that a Lakatos polyhedron p is called simply connected if it satisfies $B_k \subseteq Z_k$ for every set integer k.

Another approach is the following. Let X be a topological space. X is called **path connected** if for any two points p and q in X, there exists a continuous function f from the real interval $[0,1]$ to X such that $f(0) = p$ and $f(1) = q$. Let S^1 be the unit circle in $\mathbf{R}^2$ (i.e., all pairs (x,y) of real numbers satisfying $x^2 + y^2 = 1$), and let D^2 be the unit disk (i.e., the set of all pairs (x,y) of real numbers such that $x^2 + y^2 \leq 1$).

Definition 6 *A topological space X is simply connected if it is path connected and every continuous function f from S^1 to X can be extended to a continuous function from D^2 to X.*

This definition clearly differs from Lakatos's. First of all, it applies to topological spaces, so it is not obvious that it can be modified in a straightforward way to Lakatos polyhedra. There is, however, a relation, given by the following fact:

Theorem 3 *Every two-dimensional manifold M for which $H_1(M, F_2)$ is trivial is simply connected.*

$H_1(M, F_2)$ is the so-called first homology group of the manifold M, which is by definition $Z_1(M, F_2)/B_1(M, F_2)$, where

- $Z_1(M, F_2)$ is the group of 1-chains (over F_2) of M whose boundary is 0, and
- $B_1(M, F_2)$ is the group of 1-chains (over F_2) of M that are the boundary of some 2-chain.

The definition makes sense because, in this setting, we have that $\partial\partial \equiv 0$, i.e., $B_r \subseteq Z_r$, as a basic theorem. To say that $H_1(M, F_2)$ is trivial just means that $B_r = Z_r$. Lakatos thus takes the property 'the first homology group is trivial' as his defnition of simple connectedness. From this it follows (by a result known as the universal coefficient theorem [101]) that $H_1(M, F_2)$ is the trivial group.

However, for every $n \geq 4$ there exist compact smooth manifolds of dimension n for which $H_1(M, \mathbb{Z}/)$ is trivial, but which are nonetheless not simply connected. Poincaré also found an example that works in dimension three.

The examples show that 'simply connected' is a minsomer. The terminology is appropriate for polyhedra of dimension at most 2 (i.e., two-dimensional surface sitting in $\mathbf{R}^3$), but that is so only because of a classification theorem for 2-manifolds. A better word for what the property that Lakatos calls 'simply connected' would be 'homologous to a sphere', or 'homology sphere'. This is the terminology that I've adopted.

4.5.2 A proof-theoretic question

The result of the formalization is that Euler's polyhedron formula (understood à la Poincaré) is a first-order logical consequence of the axioms of Tarski-Grothendieck set theory (TG). But it should be clear that the full strength of TG set is not *required* for Poincaré's proof; it would be quite surprising if Poincaré's proof of Euler's polyhedron formula required the existence of arbitrarily large inaccessible cardinals. After all, following Poincaré, polyhedra are conceived as certain combinatorial structures that, presumably, could be completely captured in an arithmetical theory. And thanks to the level of detail in the formal proof of Euler's polyhedron formula, one has a clear basis with which to prove Euler's polyhedron formula in a weaker theory than TG.

The characteristic axiom of TG asserts: for every set N there exists a set M such that

- $N \in M$,
- M is closed under taking subsets,
- M is closed under the powerset operation, and
- if $X \subseteq M$ and $X \not\sim M$, then $X \in M$.

Such a set M might be called a universe containing N; accordingly, let us call this principle the *universe axiom.* Some important consequences of the universe axiom (none of which are axioms of TG) are:

- The existence of an infinite set,
- The axiom of choice, and
- Powerset.

When one inspects the deduction underlying the MIZAR proof of Euler's polyhedron formula, one can trace the argument through each of the three principles mentioned above. Since each of these three principles are consequences of the universe axiom (together, of course, with other axioms of TG), we see that the MIZAR proof of Euler's polyhedron formula uses the universe axiom. But in MIZAR this is to be expected. Indeed, the proof of *every* theorem in the MIZAR mathematical library that involves natural numbers uses the universe axiom by way of the existence of an infinite set (obtained by applying the universe axiom to $\emptyset$).

It may be somewhat surprising that the axiom of choice appears in the proof of Euler's polyhedron formula. To be clear, what is claimed is not that Euler's polyhedron formula ineliminably *depends* on the axiom of choice in the way that, say, the well-ordering principle does. Instead, what is claimed is that there is a deduction of Euler's polyhedron formula that *uses* choice. The use occurs in the proof of the rank+nullity theorem theorem. The proof proceeds by starting with a linear transformation T from a finite-dimensional vector space V to a finite-dimensional vector space W. The first step is to choose a basis A for $\ker T$; one then extends A to a basis B for all of V and, finally, one shows that $T(B - A)$ is a basis of $\operatorname{im} T$. In the actual MIZAR proof of the rank+nullity theorem, the justification for the first step (choosing a basis for $\ker T$) appeals to the theorem [98] that every vector space has a basis.[15]

But clearly the principle that every vector space has a basis (which, perhaps surprisingly, is equivalent over ZF [102] to the axiom of choice) is stronger than what is required for the purpose of proving the rank+nullity theorem, which after all deals with only finite-dimensional vector spaces.[16] And for finite-dimensional vector spaces, it is clear that we can produce a basis through an iterative search procedure whose formalization requires only arithmetical principles.

Some custom software (building on Josef Urban's work [104]) for computing dependency relations in MIZAR texts provides evidence that the *only* way that the universe axiom is used is by way of the three principles mentioned above (infinity, choice, powerset). This in turn is evidence that, from the provability judgment $TG \vdash$ EPF we have the improved judgment $ZFC \vdash$ EPF, where 'EPF' is the Poincaré/combinatorial formalization of Euler's polyhedron formula.[17]

Applying 'Schoenfield's trick' to the Poincaré/combinatorial understanding of Euler's polyhedron formula, from the judgment $ZFC \vdash$ EPF we can drop choice and conclude that $ZF \vdash$ EPF. We have thus moved from the heights of TG to the more modest realm of ZF by studying the MIZAR deduction of Euler's polyhedron formula; we have established a new provability judgment without actually producing a new deduction.

One can continue the process of trying to further weaken the theory with which proof is carried out. It seems plausible that one can get away without having a *set* of natural numbers. That is, it seems plausible that one can eschew the axiom of infinity and deal with the natural numbers not as a set but as a proper class. Accepting that for the moment, we see, using the equivalence of ZF − Infinity and Peano Arithmetic (PA), that Poincaré's proof of Euler's polyhedron formula can be carried out in PA.

Based on some initial studies, it appears that a formalization of Poincaré's proof can be carried out in the theory $I\Delta_0(\exp)$, a first-order arithmetical theory in a language with addition, multiplication, ordering, and exponentiation with an induction scheme for Δ_0-formulas (which are permitted to contain exponentiation) [105]. It also appears that some kind of exponentiation is required. In the next chapter, we shall take up these issues in somewhat more detail.

4.5.3 Streamlining the formalization

At the time of writing, no mechanism for binders (apart from the quantifiers ∀ and ∃) has been implemented in the MIZAR language. (Wiedijk has a proposal [106] for this as-yet-unimplemented feature.) For example, the definition of the so-called incidence sequence $I_{x,c}$ generated by a $(k-1)$-polytope x and a k-chain c. Using one common notation for sequences [107], $I_{x,c}$ can be defined as

$$\langle v@P_{k,n} \cdot [x \in P_{k,n}] \colon 1 \leq n \leq N_{p,k} \rangle,$$

The bracket notation '[$x \in P_{k,n}$]', from Knuth [108], denotes 1 or 0 according as the relation does or does not hold.[18] The actual MIZAR definition is somewhat more complicated:

```
incidence-sequence(x,v) -> FinSequence of F2
 means
((k-1)-polytopes(p) is empty implies it = <*>{}) &
((k-1)-polytopes(p) is non empty implies
 len it = num-polytopes(p,k) &
 for n being Nat
  st 1 <= n & n <= num-polytopes(p,k)
  holds
  it.n =
   (v@(n-th-polytope(p,k)))*incidence-value(x,n-th-polytope(p,k)));
```

A binder syntax would simplify this definition. It would also help to simplify the examples involving linear combinations that have already been discussed (in light of the fact that in MIZAR linear combinations are represented as functions). Even if these examples are unconvincing, it should be clear that, in general, notations for sequences, functions (λ-abstraction), relations, and other mathematical objects would help to streamline the MIZAR language and make it even more attractive as a formal language for mathematics than it already is.

4.6 Conclusion and Further Work

Poincaré's abstract, combinatorial conception of polyhedra facilitated formalization because the definition could be easily captured using MIZAR structures. Following Poincaré, the messy details are largely suppressed; one just formalizes the definition of being a homology sphere and carries out the linear algebraic proof. Whether one regards this as a problem or a feature of Poincaré's approach is left for the reader to decide. A further challenge for formal mathematics would be to treat Euler's proof of his relation, involving 'concrete' or 'real' polyhedra. One could start with the relatively easy case of convex polyhedra (with which Euler was arguably working [109], even though his definition apparently permits non-convex polyhedra). It would be especially interesting to take on Euler's argument because of the subtle flaws that it was found to contain. The main problem was that Euler did not specify just how to carry out the slicing procedure. One can see, by inspecting simple examples, that one must be careful about the vertex about which the slicing procedure is done, because for some polyhedra and some choices of the vertex, Euler's method can lead to strange results:

> It is not at all obvious that this slicing procedure can always be carried out, and it may give rise to 'degenerate' polyhedra for which the meaning of the formula is ambiguous. [110]

Samelson [111] has repaired this gap in Euler's proof. Are there any others?

As mentioned earlier, for the purposes of the formalization is was not necessary to define in full generality the notion of the inverse $T^{-1}(l)$ of a linear combination l under a linear transformation T. It would be valuable for future formalizations in MIZAR of linear algebra to deal with the full generality of inverse images.

The property of a polyhedron satisfying $\partial\partial \equiv 0$ is part of the definition of being a homology sphere. This property is equivalent to the inclusion $B_k \subseteq Z_k$, which says that boundaries are circuits. One might regard this not as the *definition* of the property of being a homology sphere, but rather as part of the definition of polyhedron; one would then define the property of being a homology sphere as the converse inclusion $Z_k \subseteq B_k$ (circuits are boundaries). For future formalizations using combinatorial polyhedra in MIZAR, it may be valuable (if not necessary) to carry out this rearrangement.

A further step would be to give a formal proof of Steinitz's theorem relating convex 'analytic' polyhedra (whose points are in $\mathbf{R}^3$) to planar graphs [99, 112–113].

5 Metamathematical Problems about Polyhedra

5.1 Introduction

This chapter digresses from our main thread, which focuses on Lakatos's philosophy of mathematics; the next chapter takes up that thread again. Here we discuss some metamathematical problems that naturally arise when considering polyhedra as abstract structures. The topics treated are:

- expressibility problems concerning polyhedra (model theory, specifically finite model theory),
- formal theories of polyhedra, and
- a proof-theoretic question about Lakatos's proof of Euler's polyhedron formula (proof theory, more specifically bounded arithmetic).

Although this chapter digresses from the main philosophical thrust of the dissertation, the problems discussed here nonetheless relate to Lakatos's philosophy of mathematics insofar as they illustrate how, when certain mathematical problems are considered entirely formally, we can obtain interesting results that might not have occurred had we not treated them formally. Lakatos himself points out [48] the possibility that new informal metamathematical problems may arise through the formalization of informal mathematical theories. This chapter is a contribution in that spirit.

5.2 Expressibility Problems for Combinatorial Polyhedra

This section takes up the problem of formally expressing certain properties of combinatorial polyhedra, by which we understand polyhedra considered as incidence structures (as opposed to certain kind of spatial figures or regions).

To ensure a uniform treatment, let us define the following language:

Definition 7 *The first-order signature π consists of three unary relation symbols V, E, and F, and one binary relation symbol I.*

First-order structures for the signature π can be regarded as graphs whose nodes are colored in one of three 'colors' (V, E, or F).

What properties of polyhedra can be express using π? Can one express, for example, that a polyhedron is eulerian, i.e., that a finite π-structure A satisfies the property that $|V^A| - |E^A| + |F^A| = 2$? What about the property of being a homology sphere? What about the property that $\partial \circ \partial \equiv \emptyset$? And can we express that an π-structure comes from a convex three-dimensional polyhedron?

The answer to most of these questions is 'no', especially in the case of first-order logic. Some of the aforementioned properties, however, can be captured using certain extensions of first-order logic, which we shall see.

Note that the aforementioned properties properties are straightforwardly computable: if one is given a finite π-structure A, one can compute in a finite amount of time whether A is eulerian, whether it satisfies the property that $\partial \circ \partial \equiv \emptyset$, whether it 'comes from' a convex polyhedron. (The latter is not immediately obvious; one needs to appeal to a basic result known as Steinitz's theorem for that. Steinitz's theorem will be discussed later.) Indeed, it seems clear that one can compute these properties in time polynomial in the cardinality $|A|$ of the structure A, assuming that one can test in constant time whether an element satisfies the predicates V, E, or F. Thus, by Fagin's theorem [114], which says, roughly, that existential second-order logic captures the complexity class NP, all these properties of finite π-structures can be captured in existential second-order logic. Our investigation seeks to place these properties in rather weaker extensions of first-order logic than full existential second-order logic.

5.2.1 Being a homology sphere

The property of being a homology sphere, recall, is that every cycle is a boundary: the only way of being for a k-chain to 'go all the way around' is for it to go around *something*.

The most interesting case for us of the property of being a homology sphere is that, for every 1-cycle c, there exists a 2-chain d such that $\partial_2(d) = c$. For this property we have the following result.

Theorem 4 *The property of being a homology sphere is not expressible by a first-order sentence in π.*

Proof. The proof uses Hanf locality. Suppose to the contrary that there exists a sentence γ of π such that, for every finite π-structure A, we have

$$A \models \gamma \quad \text{iff} \quad A \text{ is a homology sphere}$$

Let d be the Hanf locality degree of γ. Consider now the two families of structures A_k and B_k, defined as follows:

- Both A and B are loop-free undirected graphs, so that R is interpreted as an irreflexive symmetric relation;
- A is a single ring;
- B is a double ring (annulus) consisting of an outer ring and an inner ring;
- A bounds a single face; it is the only face of A;
- B, considered as an annulus, has one face in the region between the two rings; that is the only face of B;
- $|V^A| = |V^B| = 4k$;
- the inner ring and the outer ring of A have $2d$ vertices;

The structure B is such that the boundary of the inner ring is empty, but it does not bound any face (i.e., the inner ring is not the boundary of the unique face of B). Let f be a bijection from A to B that sends the face of A to the face of B, the edges of A to the edges of B, and the vertices of A to the vertices of B. We have set up the structures in such a way that the d-neighborhoods of any element a in A and the corresponding element $f(a)$ in B are essentially the same:

- if a is the unique face of A, then $f(a)$ is the unique face of B; a is incident with $4k$ edges and $4k$ vertices, and so is $f(a)$, so their $d < 4k$ neighborhoods are essentially the same;
- if a is an edge of A and x is in the d-neighborhood of a, then x is either the face of A (in which case $f(x)$ is the unique face of B); if x is an edge of A, the it is one of the $d < 2k$ edges around a, but there are precisely the same number of edges around $f(a)$ in B; and likewise in the case where x is a vertex of A;
- if a is a vertex of A, then by reasoning as in the previous item we can argue that the d-neighborhood of a is essentially the same as the d-neighborhood of $f(a)$.

□

5.2.2 Eulerianness

Definition 8 *A π-structure A is called* **eulerian** *if it satisfies the equation*

$$|V^A| - |E^A| + |F^A| = 2.$$

Question: is this property expressible in π? If not, in what extensions of first-order logic *can* it be expressed? These questions shall occupy us in this section.

Restricting attention first of all to first-order logic, the answer to our question is 'no'.

Theorem 5 *There is no first-order sentence ϕ of the signature π such that for all finite π-structures A, we have*

$$A \vDash \phi \quad \textit{iff} \quad A \textit{ is eulerian}$$

.

Proof. By the (negative) corollary to the Ehrenfeucht-Fraïssé theorem, it suffices to produce a sequence (A_n, B_n) of pairs of finite π-structures such that, for all $k \geq 0$,

- A_k is eulerian,
- B_k is not eulerian, but
- $A_k \equiv_k B_k$.

Our structures will be defined as follows:

1. The domains of A_k and B_k will both be the disjoint unions of the interpretations of the relation symbols V, E, and F;
2. $V^{A_k} = V^{B_k}$ is a set of k elements;
3. $E^{A_k} = E^{B_k}$ is a set of $2k$ elements;
4. F^{A_k} is a set of $k+2$ elements;
5. F^{B_k} is a set of $k+3$ elements;
6. $I^{A_k} = I^{B_k} = \emptyset$.

By 1–4, A_k is eulerian ($k - 2k + (k+2) = 2$); and by 1–3 and 5, B_k is not eulerian ($k - 2k + (k+3) = 3$).

It remains to show that $A_k \equiv_k B_k$. To define a winning strategy for duplicator in the length k Ehrenfeucht-Fraïssé game based on A_k and B_k, note that we can set up a simple one-to-one correspondence between V^{A_k} and V^{B_k} and E^{A_k} and E^{B_k}. The only potential trouble for duplicator occurs in the F parts of the two structures, where there in fact is some difference that could be detected.

We need not specify a correspondence between the F's in A_k and B_k; it should be clear that whatever element spoiler chooses, if it is an E element, then there are enough E elements in the other structure for duplicator to respond. In other words, a winning strategy for duplicator is simply to respond to spoiler's chosen element by choosing *any* element in the other structure of the same kind (i.e., if spoiler chooses a V, the duplicator responds with an arbitrarily chosen V, etc.). $\square$

5.2.2.1 Extending the result: euler characteristic and general-dimensional polyhedra

We can extend the result further by introducing the notion of an euler characteristic—which will show that there is nothing special about the constant 2 in the key equation $V - E + F = 2$—and by permitting polyhedra of arbitrary (finite) dimensions, thereby showing that there is nothing special about dimension 3 polyhedra.

Definition 9 *The* **euler characteristic** $\chi(A)$ *for a finite* π*-structure* A *is the integer*

$$\chi(A) := |V^A| - |E^A| + |F^A|.$$

The main theorem shows that the property of having euler characteristic 2 is not expressible by a first-order sentence (of the signature π).

Theorem 6 *For every integer* k*, the property of finite* π*-structures of having euler characteristic* k *is not expressible by a first-order sentence of* π*.*

Proof. Given an integer k, 'normalize' the equation $V - E + F = k$ by adding E to both sides and adding k to both sides if k is negative. We are thus dealing with the property $V + F = E + k$, or $V + F + (-k) = E$, if k is negative.

Define a sequence (A_n, B_n) of finite π-structures such that, for all $n \geq 0$,

- A_n has euler characteristic k,
- B_n does not have euler characteristic k, but
- $A_n \equiv_n B_n$.

The description of the game (and the winning strategy) uses the 'normalized' equation. Thus, if we wanted to show that the property of having euler characteristic equal to -9, note that we are dealing with the equation $V + F + 9 = E$. Now consider the sequence structures $(A_{k,-9}, B_{k,-9})$ $(k \geq 0)$ defined as

1. The domains of $A_{k,-9}$ and $B_{k,-9}$ will both be the disjoint unions of the interpretations of the relation symbols V, E, and F;
2. $V^{A_{k,-9}} = V^{B_{k,-9}}$ is a set of k elements;
3. $E^{A_{k,-9}}$ is a set of $2k + 9$ elements;
4. $E^{B_{k,-9}}$ is a set of $2k + 10$ elements;
5. $F^{A_{k,-9}} = F^{B_{k,-9}}$ is a set of k elements;
6. $I^{A_{k,-9}} = I^{B_{k,-9}} = \emptyset$.

It is clear that duplicator has a winning strategy in the length k Ehrenfeucht-Fraïssé game based on $A_{k,-9}$ and $B_{k,-9}$; the description of the winning strategy follows the same outline as we have in the case where we considered π-structures whose euler characteristics were 2. □

Thus, as one might have expected, there is nothing special about the constant 2. Moreover, there is nothing special about the dimension 3.

Definition 10 *For a positive natural number d, let π_d be a signature with d unary relation symbols P_0, P_1, ..., P_{d-1}.*

Intuitively, π_d gives us a language for talking about d-dimensional combinatorial polyhedra. (The letter 'P' in the names of the unary predicates stands for 'polytope'. P_k is intended to denote the set of k-dimensional polytopes.) The 'polyhedral' signature π that we have been using is the special case $d = 3$. There is a natural extension of the notion of euler characteristic from three-dimensional polyhedra to polyhedra of any positive dimension.

Definition 11 *The* **euler characteristic** *for a finite π_d-structure A is the alternating sum*

$$\sum_{k=0}^{d-1} (-1)^k |P_k^A|.$$

(This coheres with the case of $d = 3$, where the euler characteristic was defined as the alternating sum $V - E + F$.)

The definition comes from Schläfli's generalization of Euler's polyhedron formula to polyhedra of arbitrary dimension[1]. The alternating sum can be motivated by observing that

- a polyhedron of dimension 1 is a line segment, and thus has two vertices, whence $V = 2$;
- a polyhedron of dimension 2 is a polygon, and thus has an equal number of vertices and edges, whence $V = E$, i.e., $V - E = 0$;
- a polyhedron of dimension 3 satisfies Euler's relation, whence $V - E + F = 2$.

As the dimension of the polyhedra increases, the right-hand side of the equation oscillates between 2 and 0. Also, the left-hand side starts with a positive term counting the number of polytopes of lowest dimension (0, or vertices) and alternates in sign as polytopes of increasing dimension are considered.

Theorem 7 *For every natural number $d \geq 2$, and every integer k, the property of finite π_d-structures of having euler characteristic k is not expressible by a first-order sentence (of the signature π_d).*

Before getting into the proof, let us pause to explain why the condition that d be at least 2 is necessary. We cannot claim that the result holds for $d = 1$, because we *do* have expressibility results in that case, at least for non-negative euler characteristics. For example, in the case of $d = 1$, we *can* express that the euler characteristic of a π_1-structure is 2:

$$\exists x \exists y (P_0(x) \wedge P_0(y) \wedge x \neq y).$$

Clearly for every natural number n we can write a first-order formula in the signature π_1 saying that there are exactly n vertices, which, in this trivial low-dimensional case, is the property of the euler characteristic being equal to n. Of course, we cannot write a first-order formula saying that there negatively many vertices.

Proof. An easy generalization of the case $d = 3$. For example, if $d = 4$ and $k = 42$, consider the structures (A_n, B_n) $(n \geq 0)$ defined as:

1. the domains of $A_{n,4,42}$ and $B_{n,4,42}$ will both be the disjoint unions of the interpretations of the relation symbols P_0, P_1, P_2, and P_3;
2. $P_0^{A_{n,4,42}} = P_0^{B_{n,4,42}}$ is a set of k elements;
3. $P_1^{A_{n,4,42}} = P_1^{B_{n,4,42}}$ is a set of k elements;
4. $P_2^{A_{n,4,42}}$ is a set of $k + 42$ elements;
5. $P_2^{B_{n,4,42}}$ is a set of $k + 43$ elements;
6. $P_3^{A_{n,4,42}} = P_4^{B_{n,4,42}}$ is a set of k elements;
7. $I^{A_{n,4,42}} = I^{B_{n,4,42}} = \emptyset$.

By design, the euler characteristic of $A_{n,4,42}$ is 42, but that of $B_{n,4,42}$ is 43. The only potentially detectable difference between the two structures is in the P_2 part; but there are enough such elements to ensure that $A_{n,4,42} \equiv_n B_{n,4,42}$ by simply responding arbitrarily to whatever move spoiler makes (provided, of course, the duplicator responds to a P_0 move by choosing a P_0 element, etc.). □

The general-dimensional approach has among its consequences a familiar result from finite model theory:

Corollary 1 *There does not exist a first-order sentence ϕ, in a signature using two unary predicate symbols R and S (together with equality), which is such that*

$$A \vDash \phi \quad \textit{iff} \quad |R^A| = |S^A|.$$

Proof. In the previous theorem, put $d = 2$ and $k = 0$. □

In the proofs of the preceding theorems on eulerianness and euler characteristics, we have used Ehrenfeucht-Fraïssé games. One would reasonably wonder whether more sophisticated tools, such as Hanf locality, might have led to these results more efficiently. The answer is that such tools might very well apply in these cases, but one initial obstacle to applying them is that the properties here are 'cardinal' properties, that is, they are defined as relations holding among the cardinalities of the various parts of the structures involved. We described structures in which duplicator can win, but the structures had different cardinalities: one structure was always bigger than the other by one. However, when applying Hanf locality, one must take care that the structures involved have the *same* cardinality. This consideration is presented not as a decisive obstacle to using Hanf locality for establishing non-expressibility of cardinality properties such as eulerianness (or any other euler characteristic). If that is right, then the cardinal properties here seem to be 'basic' in some sense.

5.2.2.2 Monadic second-order logic

We have seen that eulerianness cannot be captured in first-order logic by a sentence in our 'polyhedron language' π; what about for extensions of first-order logic? In this section we consider monadic second-order logic, which extends first-order logic by permitting set quantifiers. Can eulerianness be expressed with monadic second-order logic?

The answer is, once again, 'no'.

Theorem 8 *Eulerianness is not expressible as a sentence of π in monadic second-order logic.*

The proof uses the modification of Ehrenfeucht-Fraïssé games that are suitable for monadic second-order logic.[2] For these games for monadic second-order logic, we have an expressibility result analogous to what we had for first-order logic. We shall use the notation $A \equiv_k^{\mathrm{MSO}} B$ to indicate that duplicator has a winning strategy in the length k monadic second-order logic Ehrenfeucht-Fraïssé game based on the structures A and B.

Theorem 9 *A property P of finite structures (over a relational signature π) is expressible in monadic second-order logic iff there exists a natural number n such that for every two π-structures A and B, if A has property P and $A \equiv_k^{MSO} B$, then B has property P.*

For a proof, see Libkin [114].

As before, we are interested in applying this result to prove non-expressibility.

Proof. A sequence (C_k, D_k) of pairs structures that work for the monadic second-order case is closely related to the sequence of pairs of structures that worked for the proof in the first-order case. Interestingly, thanks to the increased expressive power of monadic second-order logic, duplicator needs more 'room' to carry out his 'deception' of spoiler. Define $C_k := A_{2k}$ and $D_k := B_{2k+1}$. Note that for C_k we have

$$V^{C_k} - E^{C_k} + F^{C_k} \quad = \quad (2k+1) - 4k + (2k+1) \quad = \quad 2,$$

whereas for D_k we have

$$V^{D_k} - E^{D_k} + F^{D_k} \quad = \quad (2k+1) - 4k + (2k+2) \quad = \quad 3.$$

Thus C_k is eulerian but D_k is not. We need to argue that $C_k \equiv_k^{\mathrm{MSO}} D_k$.

To define a winning strategy for duplicator, proceed as follows. If duplicator make a point move (i.e., selects an element of one of the structures), then duplicator is to respond in the same way as was done in the previously described first-order Ehrenfeucht-Fraïssé game. If spoiler makes a set move (i.e., chooses a subset of one of the structures), then duplicator is to respond in the following way:

- If spoiler chose $\emptyset$ in either structure, respond with $\emptyset$;
- If spoiler chose a singleton subset $\{x\}$ of either structure, respond with the singleton subset $\{y\}$, where y corresponds to x in the first-order Ehrenfeucht-Fraïssé game described above;
- If spoiler makes a set move that contains elements satisfying V or E, then respond with a set move containing the corresponding elements in the other structure satisfying V or E. The idea is that since the V and E parts of the two structures C_k and D_k are 'identical', duplicator can easily respond to any move that takes place in those 'parts' of the structures;
- If spoiler makes a set move X in D_k (where $|F^{D_k}|$ is exactly one larger than $|F^{C_k}|$, then respond with a set Y in C_k in the following way:
  - If $|X \cap F^{D_k}| \leq k$, then for Y choose a subset of C_k such that $|Y \cap F^{C_k}| = |X \cap F^{D_k}|$;

  - If $|X \cap F^{D_k}| > k$, then for Y choose a subset of C_k such that $|Y \cap F^{C_k}| + 1 = |X \cap F^{D_k}|$.
- If spoiler makes a set move X in C_k, then respond with a set Y in D_k in the following way (exactly analogous to the previous case):
  - If $|X \cap F^{C_k}| \leq k$, then for Y choose a subset of D_k such that $|Y \cap F^{D_k}| = |X \cap F^{C_k}|$;
  - If $|X \cap F^{C_k}| > k$, then for Y choose a subset of D_k such that $|Y \cap F^{D_k}| = |X \cap F^{C_k}| + 1$.

To get a sense of how this strategy works, let us consider some possible set moves that spoiler could make that might lead to a loss for duplicator, and how duplicator can respond to them. If spoiler chooses, say, *all* the F's in C_k, the duplicator needs to respond by choosing all the F's in D_k, and vice versa. For if duplicator responds by choosing a proper subset X of the F's, then spoiler can choose an F in the complement of X, and duplicator loses. From below, we can consider what happens if spoiler chooses a small subset of the F's in one of the structures, say an unordered pair. Duplicator needs to respond (assuming that we are dealing with the trivial cases where k is 0, 1, or 2) by choosing an unordered pair in the other structure; otherwise, spoiler can discover a difference in the cardinalities of these two sets in three moves. Thus, from below, duplicator needs to respond by choosing sets with the same cardinality as spoilers sets. From above, we know that, since the cardinality of the F's in the two structures is not the same, there must come a point when duplicator cannot always respond by choosing a set with exactly the same cardinality. In the last two moves above, we choose cardinality k as the transition point: for sets of cardinality at most k, duplicator responds by choosing sets with precisely the same cardinality as spoiler's sets; after k, duplicator responds to spoiler's 'large' set moves by responding with another 'large' set whose size differs by exactly one. By playing this way only for 'large' sets (cardinality greater than k), spoiler cannot tell—in k moves—that there is a difference between the two structures. □

As we had in the case of first-order logic, the result extends to arbitrary euler characteristics and arbitrary dimensions (at least two).

Theorem 10 *For each integer k, the property of finite π-structure of having euler characteristic k is not expressible by a monadic second-order sentence of the signature π.*

Proof. Uses the same (sequence of) structures that worked when we were concerned with first-order logic in the case of arbitrary euler characteristics, but 'doubled' as we just saw in the previous proof. (Such doubling—increasing the size of the structures involved to give duplicator more 'room'—appears to be necessary.) □

5.2.2.3 Expressibility using an equicardinality generalized quantifier

The investigation of expressibility of eulerianness has so far been negative; neither first-order logic nor monadic second-order logic were able to capture this property in a single sentence. The discussion now turns in a more positive direction.

This section concerns an extension of first-order logic obtained by adding a new quantifier for *equicardinality*. Syntactically, the quantifier binds one variable and two formulas $\alpha(x)$ and $\beta(x)$. Formally, it is characterized as follows:

Definition 12 *Let A be a first-order structure, x a variable, α and β two formulas, and let s be a variable assignment for A. Define*

$$A \vDash \textsc{eq-card}\, x(\alpha, \beta) \quad \textit{iff} \quad |\{a \in A\colon A \vDash \alpha[s(x|a)]\}| = |\{a \in A\colon A \vDash \beta[s(x|a)]\}|$$

.

Using such a quantifier, it turns our that we can express eulerianness. But we first place a condition on our structures:

Definition 13 *A π-structure A is called* **partitioned** *if its domain is the disjoint union of the interpretations in A of the unary predicates V, E, and F.*

The condition of being partitioned ensures that every element is one of the three kinds (intuitively, every element is either a vertex, an edge, or a face), and that no element is of two (or more) kinds. Note that the class of partitioned structures is elementary: it is axiomatized by the π-sentence

$$\forall x[V(x) \vee E(x) \vee F(x)] \wedge \begin{bmatrix} V(x) \rightarrow \neg E(x) \wedge \neg F(x) \\ \wedge \\ E(x) \rightarrow \neg V(x) \wedge \neg F(x) \\ \wedge \\ F(x) \rightarrow \neg V(x) \wedge \neg E(x) \end{bmatrix}.$$

Theorem 11 *For each integer k, the property of finite partitioned π-structures having euler characteristic k is expressible by a sentence of first-order logic with a generalized quantifier for equicardinality.*

Proof. The proof goes by example. To warm up, consider the case $k = 0$. Claim: the formula

$$\phi_0 := \text{EQ-CARD}_x(E(x), V(x) \vee F(x)).$$

works. A finite partitioned first-order structure A whose domain is the satisfies ϕ_0 iff the $|V^A| + |F^A| = |E^A|$, i.e., $|V|^A - |E|^A + |F|^A = 0$. This is essentially read off from the satisfaction conditions for the equicardinality quantifier and the definition of being partitioned.

Now consider the case $k = 1$. To say that a finite π-structure has euler characteristic 1 means that $V - E + F = 1$, i.e., $V + F = E + 1$, so that there is (exactly) one more vertex-or-face element than there are edges. We can express this using the equicardinality quantifier as

$$\phi_1 := \exists x([V(x) \vee F(x)] \wedge \text{EQ-CARD}_y(E(y), [V(y) \vee F(y)] \wedge y \neq x)).$$

A finite partitioned first-order structure A satisfies ϕ_1 iff the euler characteristic of A is 1.

If $k = -1$, we have to express the property $V - E + F = -1$, or $V + F + 1 = E$. A formula ϕ_{-1} that works for $k = -1$ looks like ϕ_1. ☐

The condition of the structures as being partitioned is essential: if we drop this condition and allow elements satisfy none of these predicates V, E, and F, or more than one of them, then our expressibility results fail. For a counterexample, consider a structure A with one point, satisfying both V and F. The euler characteristic of A is 2, but the formula ϕ_0 above, using the equal cardinality quantifier, is false in this structure (the cardinality of the set of elements that satisfy $V(x) \vee F(x)$ is 1, but the cardinality of the set of elements that satisfy $E(x)$ is 0).

It is not clear that there exists a formula using the equicardinality quantifier that will work in the class of *all* structures, as opposed to the class of partitioned structures. One approach toward expressing this class of structures would be to use the principle of inclusion-exclusion[3], well known from elementary combinatorics. We leave this as an open question.

5.2.2.4 Expressibility in dyadic existential second-order logic

Theorem 12 *For each integer k, the property of finite partitioned π-structures of having euler characteristic k is expressible by a sentence of (dyadic) existential second-order logic.*

Proof. By example. Consider $k = 0$, and look at the sentence

$$\exists R([R \text{ is a one-to-one functional}] \wedge [\operatorname{dom} R = V \cup F] \wedge [\operatorname{ran} R = E]).$$

The formula expresses that there exists a bijective relation whose domain is the union of the vertices and faces (assumed to be disjoint) and whose range is the set of edges. The conditions written in text (that R is one-to-one, that R is functional, etc) can all be expressed as first-order sentences using R as a parameter. This clearly works.

For other k's, we can use the same idea as we used when using the equicardinality quantifier. For example, for $k = 3$, we can capture the class of partitioned π-structures whose euler characteristic is 3 with the help of the sentence:

$$\exists R \exists x \exists y \exists z \left(\begin{array}{c} x \neq y \wedge y \neq z \wedge z \neq x \\ \wedge \\ [R \text{ is a one-to-one functional relation}] \\ \wedge \\ [\operatorname{dom} R = (V \cup F) - \{x, y, z\}] \\ \wedge \\ [\operatorname{ran} R = E] \end{array} \right).$$

In other words, $V - E + F = 3$ holds iff $V + F = E + 3$, which, for finite partitioned π-structures, means that there are exactly 3 vertex-or-face elements more than there are edge elements. The relation R enforces this. □

5.2.3 Convexity

We now investigate the problem of expressing convexity: can we write down a sentence γ of π such that a finite π-structure A satisfies γ iff A is isomorphic to the incidence structure of a convex three-dimensional polyhedron? The answer seems to be 'no', in light of Steinitz's theorem [115]:

Theorem 13 *A graph g is isomorphic to the 1-skeleton of a three-dimensional convex polyhedron p iff g is planar and 3-connected.*

The 1-skeleton of a three-dimensional polyhedron is obtained by looking at only the vertices and edges (the 'skeleton'), ignoring the faces. A graph is said to be **3-connected** if there is no pair of vertices whose removal disconnects the graph.

We now formulate a conjecture:

Conjecture 1 *The property of being isomorphic to the incidence structure of a convex three-dimensional polyhedron is not expressible by a first-order sentence in π.*

The properties of planarity and 3-connectedness are each known to be not expressible in a first-order language for graphs with just an incidence relation, and likewise for both a representation of graphs with both vertices and edges as objects. It would thus appear, in light of Steinitz's result and its connection with properties that are known to be not expressible in a language for graphs, that convexity (that is, being isomorphic to the incidence structure of a convex three-dimensional polytope) is likewise not expressible in our language.

The reason for hesitation in concluding that Steinitz's theorem gives us a new undefinability result, and for calling this a conjecture rather than a theorem, is that our language, π, is richer than just a pure language for graphs. We have a unary predicate for faces, but the previous undefinability results dealt with languages in which, at most, there were predicates for vertices and edges. It seems plausible, but not obvious, that convexity is not expressible in π. Private correspondence with B. Grünbaum, an expert in polyhedra, graph theory, and Steinitz's theorem, has made it clear that Steinitz's result immediately applies to our richer language.

5.3 Formal Theories of Polyhedra

In this section we catalog a handful of various theories of polyhedra. None of these theories are due to me. Nonetheless, it is valuable to list them because they provide an interesting testbed for a formal investigation of polyhedra.

5.3.1 Steinitz-Rademacher polyhedral complexes

The first theory that we shall discuss is due to Steinitz and Rademacher [116].

Definition 14 *A* **polyhedral complex** *is a π-structure that satisfies the following conditions:*

- *I is symmetric,*
- *No two elements from the sets V, E, and F are incident (i.e., $\forall x \forall y(\neg I(x,y))$, and the same goes for the sets E and F), and*
- *If v, e and f are such that $v \in V$, $e \in E$, $f \in F$, $I(v,e)$ and $I(e,f)$, then $I(v,f)$.*
- *Every edge is incident with two vertices,*
- *Every edge is incident with two faces,*
- *For every vertex v and every face f such that v is incident with f, there are exactly two edges incident with both v and f, and*
- *Every vertex and every face is incident to at least one other element.*

It is clear that the axioms for structural and polyhedral complexes can be straightforwardly formalized using a first-order language with three unary relation symbols V, E, and F and one binary relation symbol I.

The smallest polyhedral complex has cardinality six: there are two vertices, two edges, and two faces. To visualize this structure, imagine a circle cut in half by a diameter; the endpoints of the diameter are the two vertices; the two arcs of the circle cut by the diameter are the two edges; and the space between the diameter and the two arcs are the two faces. One can verify this claim using a first-order model generation program (such as MACE 4) and verifying that there are no polyhedral complexes of size 1, 2, 3, 4, or 5; and that one of the models of size 6 corresponds to the description just given. (One can even verify that this structure is, up to isomorphism, the *only* polyhedral complex of size 6.)

5.3.1.1 Digression: expressibility of eulerianness in the class of polyhedral complexes

Earlier we saw that the property of being an eulerian polyhedron is not expressible in first-order logic, in a signature π with unary predicate symbols V, E, and F, and one binary predicate symbol I for incidence. We used Ehrenfeucht-Fraïssé games to establish that result, by defining a sequence (A_k, B_k) of pairs of structures such that

- A_k is eulerian,
- B_k is not eulerian, but
- $A_k \equiv_k B_k$.

The incidence relation in the structures A_k and B_k was defined to be empty. The geometric content of the non-expressibility result, then, is perhaps questionable. Although the theorem shows that eulerianness is not expressible in the class of all π-structures, one might wish to re-ask the question, this time restricting attention to π-structures that have some geometric content. Polyhedral complexes form such a class. Our question is: is eulerianness expressible by a first-order π-sentence in the class of polyhedral complexes? That is, does there exist a π-sentence ϕ such that, for all polyhedral complexes A, we have

$$A \vDash \phi \quad \text{iff} \quad A \text{ is eulerian?}$$

The answer is 'no'. We can use Ehrenfeucht-Fraïssé games once again to establish this result. The argument in this case, however, is more difficult; we can no longer use the structures A_k and B_k, because they had no geometric content. To establish the negative result, it suffices to find a sequence (C_k, D_k) of pairs of polyhedral complexes such that, for all $k \geq 0$,

- C_k is eulerian,
- D_k is not eulerian, but
- $C_k \equiv_k D_k$.

It turns out that the following structures work: C_k is a tower of 2^k consisting of copies of $(2^k + 2)$-gons; D_k is a disjoint union of two copies of C_k. (The '+2' is to ensure that the number of vertices in the polygons is at least 3, even when $k = 0$.) To see that these structures are such that, for all k, we have $C_k \equiv D_k$, see the argument in section 4.3.6 for the proof that the class of Grünbaum polyhedra is not elementary. The argument shows at the same time that the class of Grünbaum polyhedra is not elementary, as well as showing that eulerianness is not first-order expressible in the class of polyhedral complexes, because the structures C_k are both Grünbaum polyhedra and polyhedral complexes, and the structures D_k are neither Grünbaum polyhedra nor eulerian.

5.3.2 Extensional theory

The theory of polyhedral complexes permits different edges to share the same endpoints. That is, polyhedral complexes permit so-called **multi-edges**. We may wish to investigate polyhedral complexes in which this is not the case, that is, polyhedral complexes that satisfy the laws

$$\forall e_1 \forall e_2 (\forall v (R(v, e_1) \leftrightarrow R(v, e_2)) \rightarrow e_1 = e_2).$$

and

$$\forall f_1 \forall f_2 (\forall e (R(e, f_1) \leftrightarrow R(e, f_2)) \rightarrow f_1 = f_2).$$

This reminds us of the axiom of extensionality for sets, so we may call the polyhedral complexes that satisfy this additional principle **extensional polyhedral complexes**.

The polyhedral complex of cardinality 6 is not an extensional polyhedral complex (its two edges are both incident with its two vertices). Its smallest model seems to be the tetrahedron, of cardinality 14 (four vertices, six edges, four faces). As before, one can verify this claim using a first-order model generation program such as MACE 4.

5.3.3 Simplicial polyhedral complexes

One can obtain a further refinement of Steinitz-Rademacher polyhedral complexes by focusing on *simplicial* polyhedral complexes, which, roughly speaking, are the polyhedral complexes that are maximally triangulated.

Definition 15 *A* **simplicial polyhedral complex** *is a polyhedral complex that satisfies the property:*

- *Every face is a triangle (i.e., for every face f there exists exactly three edges that are incident with it).*

One might ask whether the non-expressibility results that we had before, especially concerning eulerianness, still hold even in the case of simplicial polyhedral complexes. The answer appears to be ‘no’, but this remains an open problem. (The reason for suspecting that the answer is ‘no’ is that it seems that one can triangulate the polygons that were used in the non-expressibility of eulerianness relative to the class of all polyhedral complexes.)

5.3.4 Digression: infinite models

The existence of infinite models of the first-order theories treated previously follows by the compactness theorem for first-order logic, since there exist models of arbitrary finite cardinality. What is an ‘infinite’ model of these theories? As it stands, from the application of compactness alone all we can infer is that there exists a polyhedron structure *at least one of whose sorts is infinite.*

In fact, one can see that there exist infinite polyhedron structures that have:

- infinitely many vertices, but finitely many edges and finitely many faces (‘refinement’ of, say, a tetrahedron obtained by inserting in new vertices on the edges);
- infinitely many vertices, infinitely many edges, and infinitely many faces (tessellations)

However, if a polyhedron structure has infinitely many edges, then it must have infinitely many vertices as well; and if it has infinitely many edges, then it has infinitely many faces, too.

An interesting problem associated with such polyhedra would be to classify them. One basic question that one might ask: are the two kinds of infinite polyhedra (‘refinements’ and tessellations) the only kinds of infinite models?

5.3.5 Digression: logical complexity

The theories considered above, with the exception of Grünbaum’s, can be expressed in a straightforward way using the first-order language π. (Proofs that some of Grünbaum’s axioms cannot be expressed in π will appear in the next section.) Thus, for each of the theories, we are dealing with an axiomatizable class of structures. In fact, they are all elementary classes. One basic question that can be asked about these classes of structures are the complexities of the formulas required to express them. Besides being of intrinsic interest, such complexity problems are important as preparatory questions for investigations using automated deduction tools. As stated, the theories involve a number of existential quantifiers; when these theories are thus put into clausal form, numerous Skolem functions arise, which complicates the search process.

For example: can the Steinitz-Rademacher theory of polyhedral complexes be axiomatized by a π_1 formula, that is, one whose prenex normal form has a prefix of only universal quantifiers?

We can see that the answer to this question is 'no'. If the class $\mathcal{C}$ of polyhedral complexes were axiomatized by a π_1 formula ϕ, then, by downward preservation of π_1 formulas, $\mathcal{C}$ would be closed under taking substructures. But evidently it is not. For the smallest polyhedral complex has two vertices, two edges, and two faces. This polyhedral complex has many proper substructures, but none of them can also be polyhedral complexes, by minimality.

Indeed, a naive inspection of the axioms suggests that the class of polyhedral complexes is a π_3 class, i.e., axiomatized by a formula whose prenex normal form has the quantifier prefix $\forall\exists\forall$. The second block of universal quantifiers ensures uniqueness of some of the objects introduced by the existential quantifiers. Indeed, this seems to be the sharpest result that can be given, but no proof is given here. We leave it here as an open problem that the class of polyhedral complexes is not axiomatized by a π_1 sentence.

5.3.6 Grünbaum's polyhedron theory

B. Grünbaum has proposed a theory of polyhedra as well [115]. His axioms are:

1. Every edge is incident with precisely two vertices and two faces;
2. If a vertex and a face are incident there are exactly two distinct edges that are incident with both;
3. For each face (vertex) the vertices (faces) and edges incident with it form a simple circuit of length at least 3;
4. If two edges are incident with the same two vertices (faces), then the four faces (vertices) incident with the two edges are distinct;
5. Each pair of faces (vertices) is connected through a finite chain of incident edges and vertices.

It is clear that axioms 1, 2, and 4 of Grünbaum's theory can be captured in a first-order language. Axiom 3, on the other hand, asserts that the vertices and edges that are incident with a face have the structure of a cycle. (And, dually, the axiom asserts that the faces and edges incident with a vertex likewise form a cycle.) We shall see later that this property is not first-order expressible. Axiom 5 asserts that the set of faces and the set of vertices are connected: any vertex can be reached from any other vertex, and likewise for faces. This property also turns out to be not expressible in first-order logic, as we will see later.

Returning to Grünbaum's theory, we have already remarked (but not yet proved) that the class of Grünbaum polyhedra is not elementary (with respect to the signature π). The heart of the matter is to consider the two axioms of Grünbaum's theory that are not first-order expressible, namely

- For each face, the vertices and edges incident with it form a simple circuit whose length is at least 3, and likewise for vertices; and
- Any two vertices are connected, as are any two faces.

Let us state the main result about Grünbaum polyhedra.

Theorem 14 *There is no first-order sentence ϕ of π such that, for every finite π-structure A, we have that*

$$A \vDash X \quad \textit{iff} \quad A \textit{ is a Grünbaum polyhedron}$$

Proof. We use Ehrenfeucht-Fraïssé games. Consider the sequences of π-structures (A_k, B_k), for $k \geq 0$, defined as follows:

- A_k is a convex polyhedron that has 2^k+2 vertices (to ensure that we have a polygon even when $k = 0$) arranged as a regular polygon about the origin (of $\mathbf{R}^3$) in the xy-plane, with 2^k regular 2^k-gons stacked on top, each shrinking in diameter but still centered about the origin, capped off with a single vertex at the top. This construction is repeated below the polygon in the xy-plane as well.
- B_k is the disjoint union of two copies of A_k.

The interpretation of vertex, edge, and face for these two structures is clear. Of course, B_k is not a Grünbaum polyhedron because it fails to satisfy the requirement of connectivity. Nonetheless, we shall show that $A_k \equiv_k B_k$, that is, duplicator has a winning strategy in the k-round Ehrenfeucht-Fraïssé game based on A_k and B_k. The idea is that, although B_k consists of two disjoint convex polyhedra, it it has enough structure to 'simulate' the single convex polyhedron A_k. □

5.3.7 Lakatos polyhedra

In chapter 2 of *Proofs and Refutations* Lakatos offers a theory of polyhedra, too. He attributes the conception/definition to Poincaré. For Lakatos a polyhedron is a structure of vertices, edges, and faces arranged in such a way that $\partial_k \circ \partial_{k+1} \equiv \emptyset$ for all integers k, where ∂_k is the boundary operator on the set of k-chains (the values of ∂_k are $(k-1)$-chains). The definition of Lakatos polyhedra requires several preliminary definitions (the definition of k-chain, the extremal chain cases, the k-boundary operator). Lakatos's definition of polyhedra is the broadest of all the conceptions we have seen so far because it admits a great variety of mathematical objects as polyhedra that might not normally be considered as polyhedra. For example, a single edge with two vertices—no faces—is a Lakatos polyhedron, but is neither a Grünbaum polyhedron nor is it a polyhedral complex in the Steinitz-Rademacher sense. Moreover, because of the arithmetic involved in the definition it seems unlikely that one could even define Lakatos polyhedra in a first-order way. We shall see in the next section that that is so.

5.3.7.1 Digression: Lakatos polyhedra and polyhedral complexes

How do polyhedral complexes relate to Lakatos polyhedra? Both can be understood as first-order structures of a certain kind. Is it true that all Lakatos polyhedra are polyhedral complexes? Are all polyhedral complexes Lakatos polyhedra?

First of all, it is not true that every Lakatos polyhedron is a polyhedral complex. The condition that $\partial\partial \equiv \emptyset$ is very weak; structures can satisfy that condition without satisfying the axioms for polyhedral complexes. For example, consider the Lakatos 'polyhedron' consisting of exactly one vertex, one edge, and one face, but with an empty incidence relation. It is, trivially, a Lakatos polyhedron. Such a Lakatos polyhedron, considered as a first-order structure, is not a polyhedral complex: there is only one vertex (there should be at least two), there is only one face (there should be at least two), and there is only one edge (there should be at least two).

The more interesting question is whether every polyhedral complex is a Lakatos polyhedron. Indeed, this is the case.

Theorem 15 *Every polyhedral complex is a Lakatos polyhedron.*

Proof. There are only a few cases to consider: we have to check

1. $\partial_0\partial_1$,
2. $\partial_1\partial_2$,
3. $\partial_2\partial_3$.

For other values of k (namely $k < 0$ and $k > 3$), the desired equation holds trivially. The most interesting case to consider is **2**. We shall treat this case first, and turn to **1** and **3** later.

Proof that $\partial_1 \circ \partial_2 \equiv \emptyset$. We have to show that for every 2-chain c, we have $\partial_1(\partial_2(C)) = \emptyset$. Thus, let $C = \{f_1, f_2, \ldots, f_n\}$ for some $n \geq 0$. The set $\partial_2(C)$ is a 1-chain that contains those edges that are incident with an odd number of faces of C. But, by **?**, an edge e can be incident with either 0, 1, or 2 faces; it cannot be incident with three or more faces. Thus, if an edge belongs to $\partial_2(C)$, it is incident with *exactly one* face of C.

Now suppose, toward a contradiction, that a vertex v belongs to $\partial_1(\partial_2(C))$. Thus v is incident with an odd number of elements of $\partial_2(C)$. We shall show that this is impossible.

The argument proceeds by considering a slight reformulation of the problem. Taking the neighborhood $N(v)$ of a vertex v (i.e., the set of edges and faces with which v is incident), we can imagine a finite 'wheel' of which v is the central hub; the edges with which v is incident are the 'spokes' of the wheel. The gaps between two spokes correspond to the faces to which v is incident. Now, the 2-chain C gives rise to a coloring of the circular sectors between spokes: a face be either in C or not, so it can be regarded as colored or not. Call an edge *balanced* if it is adjacent to one colored and one uncolored face.

In fact, the neighborhood of a vertex of a polyhedral complex is a union of disjoint cycles; thus, there may be more than one 'wheel' for which v is the 'hub'. We shall now show that, within such a cycle, there are an even number of balanced edges. This shows that there cannot be an odd number of balanced edges, i.e., that v cannot be incident with an odd number of members of $\partial_2(C)$.

To see that every wheel must have an even number of balanced spokes, proceed by cases. Either there are no balanced spokes (so that the claim s true), or there does exist at least one balanced spoke. In the latter case, choose a balanced spoke s_1 and move clockwise among the spokes. We need to specify the 'partner' s_1' for s_1. For s_1', let it be the next balanced spoke of the wheel in the enumeration of all spokes following s_1 in clockwise order.

We cannot have that $s_1' = s_1$ by the definition of what it means to be a balanced spoke (the colors of the faces adjacent to s_1 are opposite). Either there are no more balanced spokes in the clockwise enumeration or there are such spokes; in the latter case let s_2 be the next spoke after s_1', and proceed as before to find the 'partner' s_2' for s_2. As before, $s_2' \neq s_2$.

We can see that, by induction, there must be an even number of finite spokes for any wheel for which v is a 'hub'. This shows that the condition $v \in \partial_1(\partial_2(C)$, i.e., that v is incident with an odd number of elements of $\partial_2(C)$, is impossible for any 2-chain C.

Turning now to case **1**, we have to show that it is not the case, for a 1-chain C, that ε, the unique -1-polytope, belongs to $\partial_0(\partial_1(C))$. Since, by convention, ε is incident with every 0-polytope, we just have to show that $\partial_1(C)$ cannot have odd cardinality.

The argument in this case is somewhat more complex. Divide the vertices in $\partial_1(C)$ into equivalence classes using the reachability relation $R(u, v)$, defined as

$$R(u, v) \leftrightarrow u = v \vee \text{there exists a path from } u \text{ to } v.$$

We shall show that each equivalence class has even cardinality. This will imply that $\partial_1(C)$ itself has even cardinality (since it is the union of finite many sets of even cardinality).

To show that each equivalence class of vertices under the reachability relation has even cardinality, note first of all that no equivalence class can have cardinality 1. So each equivalence class has cardinality at least 2.

Within an equivalence class there may be cycles. Indeed, the whole equivalence class may be a cycle. But we can safely ignore the cycles: each vertex in a cycle is incident with two edges, so it need not concern us. If we disregard cycles, then, we can prove that the equivalence class has an even number of vertices as follows. Since we are ignoring cycles, there must be two 'extreme' vertices u and v in the sense that u is 'leftmost' and v is 'rightmost'. Pair u with v and continue. We are left with either zero vertices, or at least 2 (there cannot be exactly one). In the former case we are done; in the latter case we can repeat the 'trimming' construction to decrease the number of vertices by 2. We have thus produced a construction that shows that each equivalence class has an even number of elements in it.

Turning finally to the last case, **3**, note that if C is the empty 3-chain, then $\partial_2(\partial_3(C)) = \emptyset$, so we need only consider the case where $C = \{p\}$, where p is the 'whole' polyhedron, which is by convention incident with every 2-polytope. Thus $\partial_3(\{p\})$ is the set of all 2-polytopes, and the hypothesis that an edge e is in $\partial_2(\partial_3(\{p\})$ amounts to saying that e is incident with an odd number of faces. But that's impossible: edges are incident with two faces.

□

5.3.7.2 Digression: the value of a formal proof of Euler's polyhedron formula for Lakatos polyhedra

Because they lack so much geometric content, one could argue that the formalization of Euler's polyhedron formula for Lakatos polyhedra is not as interesting as it would be for, say, polyhedral or simplicial complexes. There is a grain of truth to this; we want to learn something about polyhedra, in the intuitive sense of the term; instead, we have a proof that is about an apparently purely combinatorial structure. The only geometric content that Lakatos polyhedra can claim to have is that they are assumed to satisfy the condition '$\partial\partial = 0$'. This condition rules out some 'polyhedra', to be sure, but at the same time the sole condition does allow for structures that clearly have nothing to do with polyhedra in the intuitive sense of the term.

Their lack of geometric content notwithstanding, the fact that we have a proof of Euler's polyhedron formula for Lakatos polyhedra shows that the conditions

- $B_k \subseteq Z_k$,
- $Z_k \subseteq B_k$

are sufficient for Euler's polyhedron formula. The fact that there are Lakatos polyhedra that satisfy these conditions but which do not have any clear geometric meaning is, to some extent, a strength of the abstract approach rather than a weakness. If we were to focus on only geometric polyhedra, we might have missed the fact that these above conditions are the ones ‘responsible’ for Euler’s polyhedron formula.

5.3.7.3 Non-elementarity of the class of Lakatos polyhedra

The property of a polyhedron structure A that $\partial_k(\partial_{k+1}(c)) \equiv 0$ for every $(k+1)$-chain c and every integer k, is not expressible in our polyhedron language π.

Before embarking on the argument, recall that, as we saw before, every polyhedral complex satisfies the property that $\partial_k \circ \partial_{k+1} \equiv \emptyset$, so in the class of polyhedral complexes any logically true formula (e.g., $\forall x(V(x) \vee \neg V(x))$) suffices for us. And since the class of polyhedral complexes is elementary (take the conjunction of its finitely many axioms), our problem seems to be solved.

But this is clearly not what we are after. We want to find a sentence ϕ in the polyhedron language π such that for all finite π-structures A, we have

$$A \vDash \phi \quad \text{iff} \quad \text{for all integers } k \text{ and all } (k+1)\text{-chains } c \text{ of } A, \text{ we have } \partial_k(\partial_{k+1}(c)) = \emptyset$$

The conjunction of the axioms for polyhedral complexes solves only half of the problem: it gives us the left-to-right implication, but not the right-to-left direction. That this is so can be seen by considering π-structures for which the ‘$\partial \circ \partial \equiv \emptyset$’ property holds but which are not polyhedral complexes. Indeed, any π-structure A for which the incidence relation I^A is empty trivially satisfies the desired property because all boundaries are empty. But no polyhedral complex can have an empty incidence relation.[4] Thus we cannot take the conjunction of the axioms for polyhedral complexes as a solution to our problem.

Since our language π does not have predicate or function symbols for sets, and since the property in question quantifies over sets, it seems unlikely that our desired query is expressible in π. To make the problem more tractable, then, we refine the query to a special case: can we define the property that $\partial_1(\partial_2(\{f\}) = \emptyset$ for every face f (i.e., for every object that satisfies the predicate F)? That is, can we define the property that the boundary of the boundary of a face is empty?

Since $\partial_2(\{f\})$ is just the set of edges incident with the face f, we are to check whether

$$\exists v \exists f (|\{e \colon V(v) \wedge E(e) \wedge F(f) \wedge I(v,e) \wedge I(e,f)\}| \text{ is odd})$$

holds in a polyhedron structure. This property expresses the existence of a counterexample to the universal claim that for every face f we have $\partial_1(\partial_2(\{f\})) = \emptyset$.

Because it involves parity, this property resembles others for which inexpressibility results are known, such as testing (using only equality) whether a finite first-order structure has even or odd cardinality, or testing whether the extension of a unary predicate symbol in first-order structure has even or odd cardinality [114]. Our problem fits a more general pattern: *can we test whether a certain definable set of elements in a structure has even cardinality?*

Theorem 16 *There does not exist a first-order sentence in the signature π such that, for all finite π-structures A, we have*

$$A \vDash \phi \quad \textit{iff} \quad \textit{for every face } f \textit{ of } A, \textit{ we have } \partial_1(\partial_2(\{f\})) = \emptyset$$

Proof. We shall use Hanf locality. Suppose that, to the contrary, the property in question were expressible as a π-sentence ϕ, and suppose that the Hanf locality rank of ϕ is d. Let A and B be the π-structures defined as follows:

- Both A and B have exactly one face;
- A has $2d+1$ vertices, all incident with the unique face of A,
- B has $2d+2$ vertices, all incident with the unique face of B,
- All edges of A are incident with the unique face of A,
- All edges of B are incident with the unique face of B,
- The edges and vertices of A form K_{2d+1}, the complete graph on $2d+1$ vertices,
- The edges and vertices of A form K_{2d+2}, the complete graph on $2d+2$ vertices.

In both A and B, we have that $\partial_2(\{f\})$ is the set of all edges of A and B, respectively, where f is understood as the unique face of the structures. The d-neighborhoods of any element of A and B are the same (enough vertices and edges were chosen to ensure that

A and B are similar enough in this respect). But every vertex of A is incident with an even number of edges, and every vertex of B is incident with an odd number of edges. Thus, in A, we have a face f such that $\partial_1(\partial_2(f)) \neq \emptyset$, but in B for every face f we have $\partial_1(\partial_2(f)) = \emptyset$. □

5.4 Proving Euler's Polyhedron Formula in Weaker Theories

5.4.1 Introduction

This section of the chapter is devoted to the problem of formalizing Poincaré's proof of Euler's polyhedron formula in 'weaker theories'. Here, weaker means: weaker than Tarski-Grothendieck set theory. Thanks to the formalization described in the previous chapter, we know that there exists a first-order deduction from the axioms of Tarski-Grothendieck set theory whose conclusion is a (formalization of) Euler's polyhedron formula.

But this formalization result should sit uncomfortably with us. Tarski-Grothendieck set theory (TG) is a very strong extension of Zermelo-Fraenkel set theory (ZF): the characteristic axiom of TG implies the existence of arbitrarily large inaccessible cardinals; the existence of even one such cardinal is unprovable in ZF.[5] On the other hand, the concept of polyhedron employed in Poincaré's proof is entirely combinatorial, based as it is on finite sets and finite relations on these sets. Moreover, the vector spaces that arise in the course of the proof are *finite* (and hence finite-dimensional). It thus should be quite plausible that the full strength of TG is not required to formalize Poincaré's proof. Our question in this section is: Our question is:

Question 1 *What is the weakest mathematical theory in which we can carry out Poincaré's proof of Euler's polyhedron formula?*

We shall see that there are a number of natural candidates theories in which Poincaré's proof, each weaker than the next. The main result is:

Theorem 17 *Poincaré's proof of Euler's polyhedron formula can be formally proved in $I\Delta_0(exp)$,*

which is a certain weak theory of arithmetic that will be defined later.

To be able to even state Euler's theorem, we need to ensure that we can adequately represent the concept of a polyhedron, an incidence matrix, and enough of the linear algebra that goes into the proof of the rank-nullity theorem. However, the project is largely a study of how much of the linear algebra on which Poincaré's proof is based goes through in formal systems weaker than TG.

5.4.2 First refinement

We wish to prove that we can carry out Poincaré's proof of EPF in a theory weaker than TG.

One place to focus is on the places in the argument where the methods do not strike us being obviously formalizable in a theory weaker than TG. The first such step in the argument is the application of the rank+nullity theorem.

Theorem 18 *For every linear transformation T from a finite-dimensional vector space V to a finite-dimensional vector space W, we have*

$$\dim V = \dim \operatorname{im} T + \dim \ker T.$$

The proof is not difficult, and we will not give it in full detail here. It suffices to point out the parts of the argument that are most noteworthy from the perspective of a formalization in weak theories occur at the very beginning. Following a standard proof, the argument proceeds as follows:

Proof. Let A be a basis for $\ker T$, and let B be a basis for V that extends B. Now show that $T(B - A)$ is a basis for $\operatorname{im} T$. □

The problem is the first and the second step. The most natural explanation for these two steps is that we have used the fact that

Every vector space has a basis

and the fact that

Every linearly independent set can be extended to a basis.

Note:

- These two theorems are equivalent to each other. To see that the second implies the first, note that $\emptyset$ is a linearly independent set. To prove the second from the first, let X be a linearly independent set of vectors; we have to show that there exists a basis A such that $X \subseteq A$. Consider $L(V - L(X))$, the linear span of the "complement" of X in V. This is a subspace of V, and so has a basis by the first theorem; call it B. Claim: $X \cup B$ is a basis of all of V. Proof: that it spans the space is obvious; we just need to prove independence. Suppose that we have

$$a_1 v_1 + \cdots + a_n v_n = 0,$$

  where all the v_j's are in $X \cup B$. If all are actually in X or all are in B, then we obtain the desired result, since X and B are linearly independent. So suppose that some of the v_j's are in X, and some are in B. Separate them by writing

$$b_{i_1} v_{i_1} + \cdots + b_{i_m} v_{i_m} = c_{j_1} v_{j_1} + \cdots + c_{j_n} v_{j_{n-m}},$$

  where the i's and j's exhaust $[1, n]$ and the b_i's and c_j's exhaust $[a_1, \ldots, a_n]$, and all v_i's are in X and all v_j's are in B. Since $L(V - L(X)) \cap L(X) = \{0\}$, we obtain the desired result.
- The first theorem is known to be equivalent (over ZF) to AC [102]. Thus, by the preceding result, we have two equivalents of AC.

These observations suggest that the rank+nullity theorem in full generality is actually quite a strong statement. Of course, we do not have a proof that the rank+nullity theorem is in fact equivalent to such strong set theoretical results. When we stepped back from the proof of the rank+nullity theorem and isolated the statements that did not seem to be formalizable in a weak theory, we found statements that were equivalent to the axiom of choice. If we want to see whether our result can go through in, say, ZF − Infinity—where choice does not (in general) hold—we must try to give a more careful analysis. Can we do better?

Indeed, we can. We isolated the statements "every vector space has a basis" and "every linearly independent set can be extended to a basis". But these statements are stronger than what we need for the purposes of formalizing Poincaré's proof of Euler's polyhedron formula because for that proof we need only that they hold for every *finite-dimensional* vector space. (The only vector spaces that arise in the proof are finite, and hence finite-dimensional.) In other words, what we need are

1. Every *finite-dimensional* vector space has a basis, and
2. Every linearly independent set of vectors from a *finite-dimensional vector space* can be extended to a basis.

Statement (1) now is trivially true, since to say that a vector space is finite-dimensional is to say that there exists a basis for it that is finite. Statement (2) is more interesting. It seems likely that statement (2) can be proved in ZF − Infinity.

Even more refinement is possible. We applied the rank+nullity theorem for only *finite* vector spaces, namely, the k-chain spaces C_k and the k-circuit and k-bounding chain subspaces Z_k and B_k. Thus, all we need are the principles:

- Every *finite* vector space has a basis.
- Every linearly independent set of vectors from a *finite* vector space can be extended to a basis.

From the perspective of strong set theories such as ZFCand TG, this process of refinement is redundant, since much more general linear algebraic facts hold in those broad settings. However, the process of refinement now makes it clear that we might be able to get just what we need in theories much weaker than ZFCand TG.

But *even more* refinement is possible, if all we are looking for is a weak theory in which to carry out *only* Poincaré's proof, without necessarily setting for ourselves the goal of proving a good deal of linear algebra to also be proved in that weak theory. Thus, all we need is

- For every integer k, there exists a basis for $\ker \partial_k$ that can be extended to a basis for C_k.

Although it is sufficient to show that this claim can be proved in ZF − Infinity, doing so would be somewhat unsatisfactory. Presumable, more linear algebra can be carried out in ZF − Infinitythan just this specific fact. It would be more satisfying if we could show that one of the broader claims can be formalized in ZF − Infinity. Since the most general claim implies all more specific claims (and presumably, this implication holds in ZF − Infinity), we will first attempt to prove the following claim:

Claim 1 *In ZF − Infinity, we have that for every finite-dimensional vector space V and every linearly independent subset X of V, there exists a basis A of V such that $X \subseteq A$.*

A standard argument for this claim goes as follows.

Proof. Let V be a finite-dimensional vector space, and let X be a linearly independent subset of V. Define $X_0 := X$. If $L(X_0) = V$, then X_0 is a basis for V and we are done. Otherwise, there exists a vector v_1 in V such that $v_1 \notin L(X_0)$. Put $X_1 := X_0 \cup \{v_1\}$. Then $X_0 \subset X_1$ and X_1 is linearly independent. If $L(X_1) = V$, then X_1 is a basis and we are done. Otherwise, there exists a vector v_2 in V such that $v_2 \notin L(X_1)$. Put $X_2 := X_1 \cup \{v_2\}$. Then $X_1 \subset X_2$, and X_2 is linearly independent. We repeat the process until we reach a basis, i.e., a linearly independent set X_n for which $L(X_n) = V$. □

Our task is to show that the preceding argument can indeed by formalized in ZF − Infinity. Let us begin with the following (slightly) more formal version of the preceding proof.

Proof. Let V be a finite-dimensional vector space, and let X be a linearly independent subset of V. Let B be a basis for V (given by the condition that V is finite-dimensional). Consider the predicate $P[k]$ defined as

> For all linearly independent subsets Y of V,
> if $|B| - |Y| = k$, then there exists a basis A of V
> such that $X \subseteq A$.

The desired claim we are after is implied by $\forall n P[n]$, so it makes sense to prove this by induction.

Base Case. If $|B| - |Y| = 0$, then Y is a basis for V, and we are done.

Inductive Step. Assume $P[k]$, and that $|B| - |Y| = k + 1$. Since Y is a linearly independent subset of V, we have $|Y| \leq |B|$. Thus, there exists a vector b in B such that $b \notin L(Y)$; otherwise Y would be spanning, and we would have $|B| - |Y| = 0$, since all bases have the same cardinality. Then $Y \cup \{b\}$ is a linearly independent, and $|B| - |Y \cup \{b\}| = k$. Now apply the inductive hypothesis. $\square$

We shall use this result throughout the rest of this section.

5.4.3 Formalizing Poincaré's proof in $\mathbf{ACA}_0$

It is known [103] that the claim "every countable vector space over a countable field has a basis" is equivalent over $\mathbf{RCA}_0$ to $\mathbf{ACA}_0$. Assuming then that the only step in Poincaré's proof of EPF that does obviously go through in $\mathbf{ACA}_0$, we have the following theorem:

Theorem 19 *Poincaré's proof of EPF can be formalized in* $\mathbf{ACA}_0$.

We would like to continue to weaken the system in which we are carrying out the proofs even more. Can we get Poincaré's proof to go through even in $\mathbf{RCA}_0$? It seems that it is possible; we do not need the full generality of "every countable vector space over a countable field has a basis". Rather, we can get by with a much weaker result: all we need is that any *finite* field over F_2 has a basis. The restriction to F_2 is probably not important, so we formulate the following problem:

Problem 1 *Show that* $\mathbf{RCA}_0$ *proves that every finite vector space over a finite field has a basis.*

To see whether this is possible, let's try to see whether the argument in [103] goes through in $\mathbf{RCA}_0$.

To begin with, we need to concept of a field. Of course, we shall just mimic in our arithmetical theory the usual definition.

$$\mathbf{field}(x) \equiv \left[\begin{array}{c} \mathrm{Seq}(x) \wedge \mathrm{lh}(x) = 5 \\ \wedge \\ (x)_1 \in (x)_0 \wedge (x)_2 \in (x)_1 \\ \wedge \\ \text{binary-operation-on}((x)_3, (x)_0) \wedge \text{binary-operation-on}((x)_4, (x)_0) \\ \wedge \\ \langle (x)_3 \text{ is associative and commutative, with } (x)_1 \text{ as its left zero} \rangle \\ \wedge \\ \langle (x)_4 \text{ is associative and commutative, with } (x)_2 \text{ as its left zero} \rangle \\ \wedge \\ \left[\begin{array}{c} \forall a(a \in (x)_0 \to \forall b(b \in (x)_0 \to \forall c(c \in (x)_0 \\ \to \\ \left(\begin{array}{c} \text{app-bin-op}((x)_4, a, \text{app-bin-op}((x)_3, b, c)) \\ = \\ \text{app-bin-op}((x)_3, \text{app-bin-op}((x)_4, a, b), \text{app-bin-op}((x)_4, a, c)) \end{array}\right))) \end{array}\right] \end{array}\right]$$

Here app-bin-op(f, a, b) is the value of the binary operation f on arguments a and b (in that order), which of course are assumed to belong to the domain of f. We've omitted saying explicitly what formula we mean when we write "$(x)_3$ is associative" (for example); using app-bin-op it is clear what is intended.

The definition of vector spaces follows a similar pattern.

Given a vector space V, we define a function f as follows:

$$f(-1) := \emptyset$$
$$f(n+1) := \begin{cases} f(n) \cup \{n+1\} & \text{if } n+1 \in L_V(f(n)) \\ f(n) & \text{otherwise} \end{cases} .$$

Claim 2 $f(n) \subset f(n+1)$ *for all* n.

This is obvious from the definition of f.

Claim 3 $f(|V|+1)$ *spans* V.

Proof. The more specific claim is true: for all n, if $n \in V$, then $n \in L_V(f(n))$. This is clear from the definition of f. □

Claim 4 $f(|V|+1)$ *is linearly independent.*

Proof. If $f(|V|+1)$ were linearly dependent, then there would be a vector v of $f(|V|+1)$ such that $v \in L(|V|)$; this follows by **2**. But that is impossible, again by inspecting the definition of f. □

The result of these claims is that $f(|V|+1)$ *is a basis of* V. We've thus proved that every finite vector space has a basis.

It seems that the proof does not require any induction, apart from that necessary to introduce the concept of ordered pair, finite sequence, the cardinality operator on finite sets, and the property of belonging to the linear span of a set of vectors, and to prove the handful of properties that we need in the proof. However, the existence of the function f *does* require induction; this can be done in $I\Sigma_1$, as proved in [105].

5.4.3.1 Refined argument

The idea behind the function f above seems simple enough, but let's look at the details to convince ourselves that the function really will do the trick. Let us look into the parts of the definition of f that need to be accounted for:

- Taking singletons;
- Taking unions;
- Projecting onto the 0-th component of V;
- Testing membership; and
- Calculating the linear span of V.

Let us take these in turn.

Following Hájek and Pudlák, as well as Rose [118], let's make sure that the function f really is primitive recursive.

We shall use the relation

$$x \in y \quad \text{iff} \quad \text{the } x\text{'th bit in the binary representation of } y \text{ is } 1.$$

In terms of this representation of sets, it is clear that the definition of f above is primitive recursive: we need only recall that the component operations in its definition—successor, membership, and union—are primitive recursive. For details, see Rose [118]

5.4.4 Arithmetic

Euler's formula involves integers and not just natural numbers. To do that, we introduce, in a standard way, a new unary predicate symbol $N(x)$, to be interpreted as "x is a natural number", in the usual way using equivalence classes of differences $m - n$. We then define addition, multiplication, and subtraction. The result is then that the natural numbers have been extended to the ring of integers.

Poincaré's proof makes uses of a basic theorem on telescoping sequences: for all finite sequences a and b of integers of length $n + 1$, we have

$$\sum_{k=0}^{n} (-1)^k (a_k + a_{k+1}) = a_0 + (-1)^n a_n.$$

This can be proved by induction on n using the above equation as the inductive formula.

1. The singleton $\{x\}$ of x is represented by 2^x. This is clearly a primitive recursive function of x.

2. The union of x and y turns out to be their sum $x + y$.

3. The function $(s)_k$, projecting onto the k-th component of the sequence s, is clearly primitive recursive.

4. Testing membership. This is dealt with by noting the function $M(x, y)$, the characteristic function of the relation $x \in y$, is primitive recursive.

5. Calculating the linear span of a set of elements. This item requires more care.

Following the development [96] of the theory of linear combinations in MIZAR, let us say that linear combination on a vector space is a function L from (carrier of) V to the (carrier of) field of V. For our purposes, we modify the definition slightly and declare that a linear combination is is a function from a subset of (the carrier of) V to (the carrier of) the field of V. In [96] they naturally require that the *carrier* of L—the set of elements v of V such that $L(v) \neq 0_V$—is finite. In our case, though, since all sets are finite, we do not need to add this additional condition.

Formally, for a vector space V, we define the relation $\mathrm{LC}(V, L, X)$ to be the property:

$$X \subseteq (V)_0 \wedge \mathrm{FunctionOf}(L, X, (V)_3) \wedge \forall x (x \in (V)_0 \wedge x \notin X \to L(x) = 0_{\mathrm{field}(V)}),$$

where, recall, $(V)_0$ is the carrier of V and $(V)_3$ is the carrier of the field of V.

We now define the sum of a linear combination L over a vector space V.

$$\mathrm{Sum}_V(L) := \begin{cases} 0_V & \text{if } L = \emptyset \\ (L(h(L,V)) \cdot_V h(L,V)) +_V \mathrm{Sum}_V(L - \{\langle h(L,V) \rangle\} & \end{cases},$$

where $h(L, V)$ is the auxiliary function

$$h(L, V) := \mu k (k \in \mathrm{dom}(L)).$$

We can now define the property of a vector v in a V being a linear combination of some subset X of V:

$$L_V(X, v) := \exists X \exists L (\mathrm{LC}(V, L, X) \wedge \mathrm{Sum}_V(L) = v)$$

The problem is how to bound L and X. A natural bound for X, since it is a subset of V, is just V itself; but for L, we need to consider all linear combinations, so the bound is $|V|^{|X|}$.

5.4.5 Geometry

It remains to formally define, in arithmetic, the concepts involved in the statement of Euler's polyhedron formula. We begin with the notion of an incidence matrix.

$$\textbf{incidence-matrix}(I,X,Y) \leftrightarrow \begin{bmatrix} \mathrm{Seq}(I) \\ \wedge \\ \forall x(x \in X \to \forall y(y \in Y \to \exists! k(k < \mathrm{lh}(I) \wedge \exists e(e < 2 \wedge \langle\langle x,y\rangle e\rangle \in I)))) \end{bmatrix}$$

Then, following [93], we say that a polyhedron is a certain kind of pair, consisting of polytope sets and incidence matrices:

$$\textbf{polyhedron}(p) \leftrightarrow \begin{bmatrix} \mathrm{Seq}(x) \wedge \mathrm{lh}(x) = 2 \\ \wedge \\ \mathrm{Seq}((x)_0) \wedge \mathrm{Seq}((x)_1) \\ \wedge \\ \mathrm{lh}((x)_1 + 1 = \mathrm{lh}((x)_0) \\ \wedge \\ \forall n(n < \mathrm{lh}((x)_1) \to \text{incidence-matrix}((x)_1)_k, ((x)_0)_k, ((x)_0)_{k+1}) \end{bmatrix}$$

5.4.6 Final refinement

Now we would like to explore an even more refined result by replacing "PRA" in Theorem 2 with a weaker theory.

Theorem 20 *Poincaré's proof of EPF can be formalized in* $I\Delta_0(exp)$.

This should now seems plausible; the length of the computation required for computing the basis of a vector space are all bounded by a polynomial (the size the underlying space). As the Δ_0-definable functions of $\mathrm{I}\Delta_0(\mathrm{exp})$ are those that are bounded by finite iterations of the exponential function [119], it should be clear that the proof can be carried out in $\mathrm{I}\Delta_0(\mathrm{exp})$.

5.5 Conclusion and Future Work

In this section we have explored a number of problems that arise naturally when polyhedra are considered from a formal perspective. The main problems to be attacked are 'axiomatizing' polyhedra in the sense of giving formal theories whose models are polyhedra and polyhedra-like objects, posing definability problems, and investigating the proof-theoretic strength of principles such as Euler's polyhedron formula. Many of the approaches discussed here are preliminary; we have not yet identified deep problems, results, or methods. Nonetheless, it seems clear that there are a number of paths to be explored further.

We have thus seen a number of expressibility and non-expressibility results for various logics, always focused on the property of eulerianness. This project could be continued in a number of ways. In a later section we shall see how they can be extended to certain elementary classes of structures that have some geometric content. At present, though, we leave a number of open problems:

- Ordered structures. In finite model theory, one often restricts attention to structures that are *linearly ordered*. The idea is that one has at hand a binary relation $<$ that can be assumed to be a linear order (although one does not assume anything about how the elements of a structure are ordered, in particular). Above, we did not consider ordered structures; our structures were unordered. We formulate two conjectures about the possibility of extending our results to the ordered setting:

  Conjecture 2 *Over ordered structures, eulerianness is not expressible by a first-order sentence of the three-dimensional signature π_3; moreover, generalized eulerianness is not expressible by a first-order sentence of the general-dimensional signatures π_d.*

  On the other hand, we do have a positive conjecture.

  Conjecture 3 *Over ordered structures, eulerianness* is *expressible by a monadic second-order sentence in the signature π_3.*

The suspicion is that the problem of expressing eulerianness over ordered structures is similar to the problem of expressing even cardinality, which is known to be not expressible in monadic second-order logic over unordered structures, but which *is* expressible in monadic second-order logic over ordered structures. Some initial explorations of this problem lead us to suspect that eulerianness and the property of having even cardinality are sufficiently closely related that the positive result for evenness might also hold for eulerianness.

- Another way to add geometric content to the results would be to require *connectedness* to the incidence relation. As we shall see later, we are able to establish non-expressibility results for certain axiomatized classes of structures using Ehrenfeucht-Fraïssé games and sequences of pairs (A_n, B_n) of structures such that, for every n, A_n satisfies the property in question B_n does not, but $A_n \equiv_n B_n$. It is not entirely satisfying that the incidence relation in the structures B_n is not connected (in fact, B_n is a disjoint union of two copies of A_n). It would be valuable to investigating expressibility in the context of connected structures (i.e., structures in which the incidence relation is connected). It is conceivable that properties that are not expressible become expressible when restricting one can assume that the structures one is working with are connected.
- We have focused attention on only a handful of possible extensions of first-order logic: monadic second-order logic, dyadic second order logic, and first-order logic with an equicardinality quantifier. Further exploration with logics for counting [114] would be valuable.

6 Responding to the Lakatosian Challenge

6.1 Introduction

In this chapter we come to the task of evaluating the formal work, described in chapter 3, of a formal proof of Euler's polyhedron formula as a response to Lakatos's challenge, as laid out in chapter 2.

The main difficulty, as I see it, is that Lakatos emphasizes the development of informal proofs without recognizing or stating that his interests are not entirely disjoint from those of the 'formalists' he's attacking. The formalization described in chapter 3 provides a good test case to evaluate Lakatos's claims about the growth of mathematical knowledge. I shall argue that Lakatos has cast his net rather too wide, that when he criticizes formalists he ends up undermining his own claims about the growth of mathematical knowledge.

In this chapter three responses to Lakatos are carried out. In section 2, I argue that

What I would like to advance here is the view that Lakatos's views actually are strengthened and reinforced thanks to the development of formal proofs. Although he apparently sets his sights squarely on formal proofs, hoping to show how very different they are from everyday informal proofs, I submit that Lakatos would be engaging in "friendly fire", that is, harming his own case. I argue here that the central idea of *Proofs and Refutations*, the method of proofs and refutations, applies to the development of formal proofs as well as it does to informal proofs.

Let us recall the statement of the method of proofs and refutations:

> *Rule 1.* If you have a conjecture, set out to prove it and to refute it. Inspect the proof carefully to prepare a list of non-trivial lemmas (proof-analysis); find counterexamples both to the conjecture and to the suspect lemmas.
>
> *Rule 2.* If you have a global counterexample discard your conjecture, add to your proof-analysis a suitable lemma that will be refuted by the counterexample, and replace the discarded conjecture by an improved one that incorporates that lemmas as a condition. Do not allow a refutation to be dismissed as a monster. Try to make all 'hidden lemmas' explicit.

> *Rule 3.* If you have a local counterexample, check to see whether it is not also a global counterexample. If it is, you can easily apply Rule 2.

Lakatos allows that by following the method of proofs and refutations, we can improve proofs to the point where a kind of stability is reached. The stability characterizes mature mathematical theories; the "intertwining of discovery and justification, of improving and proving is primarily characteristic of [young, growing theories]." By allowing that theorems in mature mathematical theories enjoy a certain stability, his view that all theorems are conjectures becomes less plausible. If, at least in some cases, we can refine a proof into a valid argument, then why hold that all theorems are *conjectures*? With formal proofs, one can see the idea of proof analysis—making explicit the background assumptions and knowledge that are invoked in a proof—taken, in a sense, to its limit. The very method that Lakatos describes is the force that drives a proof toward a valid argument.

'Conjecture', then, is perhaps the wrong word. To say of a proposition that it is a conjecture is to imply that we could in principle resolve the question of whether the proposition is true. But for Lakatos, the claim that mathematical propositions are, as it were, *permanently conjectural* seems to suggest that, no matter how good our justification is for the truth or falsity of the proposition in question, it will remain a conjecture. Nothing we can do can transform the epistemic status of a proposition from conjecture to non-conjecture.

6.2 What Can One Discover in a Formalized Mathematical Theory?

The problem of discovery is to explain how knowledge comes to be known. This chapter concerns a special case: *What can one discover in a formalized mathematical theory?* The question was taken up by Lakatos in his famous *Proofs and Refutations* [1]. One of Lakatos's central tasks in this book is to develop a logic of discovery, rules for characterizing the growth of mathematical knowledge. He carries out his task impressively for *informal* mathematics, but Lakatos gives a pessimistic answer to the analogous question for *formal* mathematics. In this chapter I argue for for a rather more optimistic outlook.

The problem of discovery in mathematics can be distinguished, at least at first blush, from the more general problem of discovery in science. The difference is methodological: mathematics differs from other sciences insofar as it is wholly deductive; the only acceptable justifications in mathematics are *proofs*. We can sharpen the discussion by appealing to the special character of mathematical proofs. Developments in logic in the 19th and 20th centuries has given us the concept of a *formal proof*, a representation of a mathematical proof laid down in accordance with strict rules of inference and linguistic rigidity. The ideal of formal proof is powerful; one might even go so far as to characterize mathematical proof as in-principle-formalizable arguments [120]. Logician have studied formal proofs in various settings and have given us *deductive systems*, such as Hilbert- or Frege-style systems, natural deduction systems, sequent calculi. Thanks to soundness and completeness results for these various deductive systems, in principle any valid argument can be formally represented in them.

But would a formal *gap-free* proof have any value? Our study begins when, in *Proofs and Refutations*, Lakatos takes aim at those who, in his view, overemphasize the formal nature of mathematics. The question that shall concern us in this paper can be seen in one of *Proofs and Refutations*'s trenchant passages:

> According to formalists, mathematics is identical with formalized mathematics. But what can one *discover* in a formalized theory? Two sorts of things. *First*, one can discover the solution to problems which a suitably programmed Turing machine could solve in a finite time (such as: is a certain alleged proof a proof or not?). No mathematician is interested in following out the dreary mechanical 'method' prescribed by such decision procedures. *Secondly*, one can discover the solutions to problems (such as: is a certain formula in a non-decidable theory a theorem or not?), where one can be guided by only by the 'method' of 'unregimented insight and good fortune'.

Lakatos's response is, in part, polemical. He uses the concept of discovery as a foil against the 'formalists' who would identify mathematics with formalized mathematics. Evidently, then, for Lakatos the prospects for discovery in formal mathematics are rather bleak. The first possible discovery available in a formalized mathematical theory (that a certain combinatorial figure is a deduction) is impractical ('no mathematician is interested in following out the dreary mechanical 'method' prescribed by such decision procedures'. The second kind of discovery (that a formula is provable), in the words of Quine[1], arises apparently at random; the search for a proof is apparently random and is in any case driven by factors (insight, luck) that cannot be explained in terms the formal theory at hand.

Having satisfactorily exposed the comedy of formal mathematics, Lakatos goes on to motivate his work thus:

> Now this bleak alternative between the rationalism of a machine and the irrationalism of blind guessing does not hold for live mathematics: an investigation of *informal* mathematics will yield a rich situational logic for working mathematicians, a situational logic which is neither mechanical nor irrational, but which cannot be recognized and still less, stimulated, by the formalist philosophy.

Polemics aside, the thesis of this paper is that Lakatos's view on the kinds of discoveries that can be had in formalized mathematical theories is too narrow. Modern formalization enterprises, in which one constructs formal proofs of mathematical theorems, give us, I submit, a wider view of discovery in formalized mathematical theories. It is not that Lakatos is wrong to draw attention to the development of informal mathematics. This is a genuinely interesting subject that poses many worthy problems to the philosophy and history of mathematics. Instead, this paper makes the case that the prospects for discovery in formal mathematics are wider than Lakatos imagined.

Although I shall argue that discovery does occur in formal mathematics, to avoid potential misunderstanding we should be clear on how I am using the term 'discovery'. The discoveries that I will describe are, to be sure, quite modest. They are not on a par with the discovery that the Earth revolves around the sun, Einstein's discovery of relativity theory, or Mendeleev's discovery of the table of the elements. Even restricting attention to mathematics, the discoveries that we will see are more humble than the discovery of irrational numbers, of the consistency of non-Euclidean geometry, or Gödel's incompleteness theorem. Nonetheless, the term 'discovery' is apt because, thanks to formalization, we can improve our knowledge. *Something was unknown before the formalization that was known afterward.*

This paper is but one piece in a project to re-assess Lakatos's philosophical project. Nonetheless, Lakatos offers fresh insights into the philosophy of mathematics and his thought deserves to be taken seriously.

Although this paper disagrees with Lakatos's claim about the kinds of discoveries that can arise in formal mathematics, I believe that the results of formal mathematics, rather than contradicting Lakatos, actually support his conclusions. Indeed, one could argue that developments in formal mathematics *illustrate* Lakatos's philosophy. But Lakatos's broader philosophy is the subject for another discussion; this paper is not an overall assessment of Lakatos's project in *Proofs and Refutations*, but rather a concentrated study of his views on discovery in formal mathematics.

The heart of my argument rests on three case studies taken from my own work [91–93] in formal mathematics. The next couple of sections discuss Lakatos's answers in detail and some of the technical and technological background for my response to Lakatos. Section **6.2.2** contains the three case studies in formal mathematics. Using those case studies, section **4.5** argues that in both of them discoveries can be found.

6.2.1 Lakatos's answer

Before moving on the specific case studies, it may be worthwhile to reflect on Lakatos's answer to his question about what can be discovered in a formal mathematical theory. To reiterate, the thesis of this paper is not that Lakatos's answer is incorrect, but rather that it is too narrow.

Lakatos's interest in *Proofs and Refutations* is on the development of mathematics. His 'speedy philosophising' notwithstanding [76], his philosophy is refreshing because it offers up a number of issues that do not normally arise in traditional philosophy of mathematics. One of the main challenges in evaluating *Proofs and Refutations* is: what is Lakatos's point? Worrall, an editor of Lakatos's works, offers two views on this matter:

> Lakatos sometimes described himself as extending Popper's fallibilist-falsificationist view of science into the field of mathematics, and there are even hints of Lakatos's Hegelian past in some of the claims about the autonomous development of mathematics. An alternative view, however, is that the main significance of his work is to cast light simply, though importantly, on the development of mathematics—on how mathematical truth is arrived at—and that it has nothing distinctive to say about the epistemological status of mathematical truths once they have been arrived at. But even if this alternative view is correct, there is a good of undoubtedly epistemological significance in some of the particular issues raised (for example, what he calls the problem of translation highlighting issues about how the formal systems, within which effectively infallible proof can be achieved, relate to the informal mathematics said to be captured by those formal systems). [122]

There have been a number of discussions [123–126] concerning the extent to which Lakatos was trying to extend to mathematics Popper's philosophy of science, and whether he was (or could be) successful. What concerns us here is the second alternative to which Worrall points. Even adopting the view that Lakatos is just trying to get us to pay attention to the development of mathematics, we still need to decide whether Lakatos's apparent antipathy toward 'formalism' is justified. Is it really true that the possibilities for discovery in formal mathematics are as poor as Lakatos makes them out to be?

To some extent, Lakatos's pessimistic assessment of the opportunities for discovery in formal mathematical theories is justified. It certainly would be just a dreary exercise to check, for example, whether a sequence of first-order formulas that looks like

$$\forall x \forall y(xy = yx), \forall x \forall y \forall z(x(y+z) = xy + xz), \langle \textit{many omitted axioms} \rangle, \ldots,$$
$$\ldots, \langle \textit{many omitted proof steps} \rangle, \forall n(\exists k(2k = n) \rightarrow (\exists k \exists y[y = n+1 \wedge y+1 = 2k]))$$

is a deduction in Peano Arithmetic of the familiar result that if n is an even natural number then $n+1$ is odd. (The consequent in the matrix of the final term of the sequence can be understood as: odd$(n+1)$, where odd(x) is understood as: $\exists k(2 \cdot k = x+1)$.[2] Doing so would require pattern matching: one would have to check, of each term in the sequence, whether (i) it is an axiom (pattern-matching against the axioms and the axiom scheme of induction), or (ii) it is an application of the inference rule modus ponens. Surely the effort to carry out this exercise greatly exceeds whatever payoff might be attained.

No one wants to go through the task of verifying whether a sequence of formulas is a deduction. But no one has to: early results of proof theory, especially the completeness theorem for first-order logic, show that we can give a complete proof system for first-order logic that is also decidable: we can just compute whether a sequence of formulas is a deduction. Such dreariness can safely be left to a computer. Lakatos points out that checking an informal proof, in contrast to that of a formal proof, can involve quite a lot of mathematical ingenuity. The triviality of checking proofs (in, say, first-order logic), when compared to the complexity of checking an informal proof, shows that the two are clearly quite different. The comparison is supposed to be a blow for 'formalism'. But what 'formalist' would deny the difference between formal and informal proofs?

I mentioned earlier that the problem of checking formal proofs can be safely left to computers. This should be contrasted with the result that the validity problem for first-order logic is undecidable; there is no computable function that, given a formula in an arbitrary first-order language, can decide whether the formula is provable. Thus, if a mathematician wants to construct a formal proof of some theorem, in general he has to do some work; he has to *discover* the formal proof.

This leads us to discuss Lakatos's second kind of discovery. Imagine we are dealing with an undecidable theory: given a formula in the language of the theory, we cannot simply execute a computer program to decide whether it is a theorem. We can fumble around, trying to discover a deduction of the formula from the axioms of theory. Logic alone doesn't specify how we should organize our search for a deduction.[3] Perhaps we will get lucky and stumble upon a deduction of the formula; we would thereby discover (but only by chance) that it is a theorem.

Moreover, it can be significant if, after investing much energy into designing a formal proof, one discovers that, contrary to expectations, it is invalid. The fact that a certain step in a purported proof is invalid can come as a surprise; it spurs one to discover the reasons for the invalidity, which may lead to new mathematical insight.[4] This kind of discovery will be illustrated in the examples.

In the next section I discuss the two case studies that are used to give my own answer to Lakatos's question.

6.2.2 Examples

This section is devoted to two case studies of discovery in formal mathematics. The next section is devoted to the problem of understanding the kinds of discoveries that are discussed in this section. These examples came from my efforts to construct a formal proof of a theorem that Lakatos himself studies, namely Euler's polyhedron formula, discussed in detail in chapter 3.

Before getting into the details, it is worth mentioning that these examples are rather typical in formal mathematics. Although the case studies to be described arose in the course of a formalization of a specific mathematical proof, the issues these examples raise can be found throughout formal mathematics.

6.2.2.1 Example 1: The image of a linear combination under a linear transformation

The example that I wish to discuss concerns the problem of specifying the image of a so-called linear combination under a linear transformation. Roughly speaking, a *linear combination* is a sum of vectors:

$$a_1 \cdot v_1 + a_2 \cdot v_2 + \cdots + a_n \cdot v_n \tag{6.1}$$

It is said that a formula like **6.1** is a *linear combination of* $v_1, v_2, \ldots, v_n$. The simplest non-trivial example of a linear combination is the sum $u + v$ of two vectors u and v; another is the sum $2 \cdot u + v$; another is $\frac{1}{2} \cdot u + \frac{2}{3}v$. A more clever example of a linear combination of u and v is just u (the coefficient of v is 0); an even more clever example is just 0 (the coefficient of both vectors is 0). (This example shows that the zero vector of A is a linear combination of any set of vectors.) There is nothing special about adding together two vectors; $u + v + w$ is a linear combination of u, v and w (each of whose coefficients is 1); so is $\frac{1}{2} \cdot u + \frac{2}{3} \cdot v + \frac{3}{4} \cdot w$. Being clever again, we see that $u + v$ is also a linear combination of u, v, and w. (More generally, every linear combination of u and v is a linear combination of u, v, and w.)

If we apply a linear transformation T to a linear combination $a_1 \cdot v_1 + a_2 \cdot v_2 + \cdots + a_n \cdot v_n$, we should get

$$T(a_1 \cdot v_1 + a_2 \cdot v_2 + \cdots + a_n \cdot v_n) = a_1 \cdot T(v_1) + a_2 \cdot T(v_2) + \cdots + a_n \cdot T(v_n)$$

(To rigorously prove this one uses mathematical induction together with the associativity of vector addition.) Thus the image of a linear combination of $v_1, v_2, \ldots, v_n$ is a linear combination of $T(v_1), T(v_2), \ldots, T(v_n)$.

All this seems to be correct, but we still haven't said precisely what a linear combination is; no definition has been given except 'a sum of scalar multiples of some vectors'. A linear combination is not a *kind* of vector (note that every vector is automatically a linear combination of itself), nor is it a property of sets or sequences of vectors. What is it, exactly?

Two approaches to defining linear combinations suggest themselves. One could say that a linear combination is not really an *object* of linear algebra but a *form*. To make the idea of form precise, imagine that we are dealing with a many-sorted language for linear algebra. There are two sorts: one for vectors, another for scalars. In this language, we could define linear combinations as *terms*; any term is a linear combination. If we add a new unary function symbol T to the language, we could then prove, by induction on n, that $T(a_1 \cdot v_1 + a_2 \cdot v_2 + \cdots + a_n \cdot v_n) = a_1 \cdot T(v_1) + a_2 \cdot T(v_2) + \cdots + a_n \cdot T(v_n)$. The problem would then be solved, though it would have the possibly unwanted feature of requiring a mix of language and metalanguage.

Another approach is to define linear combinations as first-order objects rather than as linguistic forms. One could say that a linear combination of vectors $v_1, v_2, \ldots, v_n$ is a certain kind of function l from A to k. The idea is that an equation $l(v) = a$ is to be interpreted as: the coefficient of v is a. Thus the sum $u + v$ of u and v would be represented as the function from A to k that sends u and v to 1 and every other vector in A to 0.

Linear combinations are supposed to represent *finite* sums of vectors: infinite sums such as

$$a_1 \cdot v_1 + a_2 \cdot v_2 \cdot + \cdots$$

are not generally regarded as linear combinations, at least not without further assumptions on the vector space (one would want some notation of *limit* or *order* with which one could distinguish those infinite sums that converge to a vector and and those that diverge and do not represent any vector). As it stands, though, our definition of linear combination does not rule out infinite sums. We need to add a technical condition to our definition.

Definition 16 *A* **linear combination** *is a function from A to k* with finite support, *that is, a function l from A to k such that the set*

$$\{v \in V : l(v) \neq 0\}$$

is finite.[5]

In other words, a linear combination is a function that can take on only finitely many non-zero values.

We still have not defined the notion of the application of a linear transformation to a linear combination. A linear transformation is a certain kind of function from one vector space to another. Note that under **Definition 6.1** is *not* a vector. Strictly speaking it is meaningless to apply a linear transformation to a linear combination: a linear combination is a function from A to k, and linear transformation is a function from A to B, so they cannot be composed in the usual set-theoretic sense. How to combine these to get a linear combination on B, i.e., a function from B to k?

To help make our way to an appropriate definition, let us invent the notation '@' and let '$T@l$' denote the application of a linear transformation T to a linear combination l. Intuitively, $T@l$ is a linear combination of vectors in B (the image space of T), so it should be a certain kind of function from B to k. What function? How does the function depend on the data T and l?

To calculate $T@l$ for a vector w in B, first find $T^{-1}(\{w\})$, the set of those vectors v in A that are mapped to w. There may be zero, one, or many such vectors. Add together the $l(v)$'s that one obtains with v's in $T^{-1}(\{w\})$. The result is the vector we want. We can concisely capture this algorithm with λ-notation:

$$T@l := \lambda w \in W. \sum l(T^{-1}(\{w\}))$$

Note that the definition neatly deals with the special case where the set $T^{-1}(\{w\})$ is empty, because the sum of an empty set of elements of k is 0. This agrees with what we had before, but we now do not need to single out this special case in our definition.

There is one potential problem with our definition: what if $T^{-1}(\{w\})$ is infinite? The sum of a finite set of members of k makes sense because of the assumption on associativity and commutativity of $+$; the sum of an infinite subset of a field does not, in general, make sense. The problem is overcome by recalling that, by definition, a linear combination has *finitely* many non-zero values. Thus, $l(T^{-1}(\{w\}))$ is finite *even if* $T^{-1}(\{w\})$ *is infinite*. There can be only finitely many non-zero values of T (i.e., non-0 values); if $T^{-1}(\{w\})$ is infinite, then 'almost all' values of T on elements of this set must be 0_f.

The potential difficulty with our definition of $T@l$ has been explained. The revised definition is in fact how the notion of the image of a linear combination under a linear transformation is defined in the MIZAR proof-checking system [91].[6]

6.2.2.2 Example 2: A counterexample to a 'natural' linear algebraic lemma

The second example is also linear algebraic. All technical terms are defined in the appendix. It involves a basic theorem of linear algebra known as the *rank+nullity theorem.*

Theorem 21 *If T is a linear transformation from a finite-dimensional vector space A to a vector space B, then* $\dim V = \dim \operatorname{im} T + \dim \ker T$.

(The numbers $\dim \operatorname{im} T$ and $\dim \ker T$ are often called the *rank* and the *nullity* of T, respectively, whence the name of the theorem.) A proof of the theorem is simple enough:

Proof. ⓪ Let k be a field, let A and B be vector spaces over k, and let T be a linear transformation from A to B. ① Let A be a basis for $\ker T$, and let B be a basis for A that extends A. ② Put $C := T(B - A)$, and put $D := L(C)$. ③ We have $|C| = |B - A|$. ④ We have that $D = \operatorname{im} T$. ⑤ The inclusion $D \subset \operatorname{im} T$ is obvious. ⑥ To prove the reverse inclusion, let $v = T(u)$ be an element of $\operatorname{im} T$. ⑦ Since $u \notin L(A)$, we have $u \in L(B - A)$. ⑧ Thus, C spans B, and the proof is complete. □

It is not necessary to understand this argument in detail. The informal proof discussed above seems to be perfectly correct; indeed, one can formalize statements 1–8 and mechanically verify that the argument is valid; one then needs to give justifications for each of the steps. However, it turns out that statement 7 simply cannot be proved; it is not a logical consequence of the assumptions in play at that stage. A counterexample: let $A := \mathbf{R}^2$ (the real plane), $X := \{(0,1)\}$, $Y := A \cup \{(1,0)\}$, $x := (7,5)$ shows that statement cannot be proved.

The problem was solved by realizing that the proof had to proceed along slightly different lines than those sketched above. Eventually, a correct proof was formalized. What is important about this example is that the error was discovered through formalization. Only by decomposing the proof of the above theorem into sufficiently fine-grained steps did the error become apparent.

The first example concerns linear algebra. I wanted to formally state and prove the statement: "if $A \subseteq B$, where A and B are subsets of a vector space V over a field F, and if $x \in L(B)$ but $x \notin L(A)$, then $x \in L(B - A)$". This one of the lemmas into which I decomposed one of the main theorems leading up to EPF. Using my proof checking system, I had checked the my list of lemmas into which I had decomposed the main theorem did indeed logically imply the main theorem. So all I had to do was give a proof of that theorem. The expression of the formula in the particular proof formalism that I was using looks like this:

```
for F being Field,
    V being VectSp of F,
    A,B being Subset of V,
    x being Element of V
  st A c= B &
     not x is Element of Lin A &
     x is Element of Lin B
  holds
    x is Element of Lin (B \ A)
```

The main theorem that I was trying to prove was an important theorem in linear algebra known as the rank+nullity theorem. The formal expression of that theorem looks like this:

```
for F being Field,
    V,W being finite-dimensional VectSp of F,
    T being linear-transformation of V,W
  holds
    dim V = rank(T) + nullity(T)
```

(You can see clearly why this might be called the rank+nullity theorem.)

The outline of the proof of the the rank+nullity theorem that I had in mind, which I intended to formalize, goes as follows:

⑨ Let F be a field, let V and W be vector spaces over F, and let T be a linear transformation from V to W. ⑩ Let A be a basis for $\ker T$, and let B be a basis for V that extends A. ⑪ Put $C := T(B - A)$, and put $D := L(C)$. ⑫ We have $|C| = |B - A|$. ⑬ We have that $D = \operatorname{im} T$. ⑭ The inclusion $D \subset \operatorname{im} T$ is obvious. ⑮ To prove the reverse inclusion, let $v = T(u)$ be an element of $\operatorname{im} T$. ⑯ Since $u \notin L(A)$, we have $u \in L(B - A)$. ⑰ Thus, C spans W, and the proof is complete.

It is not necessary to understand linear algebra to see that I had decomposed the proof fairly finely, and that sentence 7 corresponds to the statement given just above.

The problem is that statement 7 is simply not true. After trying to get the proof to go through (i.e., to have the proof certified as valid by the proof checking system), I realized to my chagrin that it is false. The example where $V := R^2$ (the plane), $A := \{(0,1)\}$, $B := A \cup \{(1,0)\}$, $x := (7,5)$ (for example) shows that my statements is false.

But this counterexample was local, not global. So I had to apply Rule 4: I had to modify my decomposition of the rank+nullity theorem to get around the problem ("replace the refuted lemma by an unfalsified one"). I therefore had to try out a different proof of the rank+nullity theorem.

This was an example where I had a local but not global counterexample. Global counterexamples can also arise when working with formal proofs. The following example came up in my formalization of EPF.

```
for F being Field,
    V being VectSp of F,
    A being Subset of V,
    l being Linear_Combination of A,
    x being Element of V,
    p being FinSequence of V,
    a being Element of F
  st rng p = Carrier l &
     p is one-to-one &
     a <> 0.F
  holds Sum ((l ++* (x,a)) (#) p)
        = Sum (l (#) p) - (l.x)*x + a*x
```

What all that means is not important. What's important is that I believed that the statement was true and that I could give a proof of it. In fact, as in the preceding example, I had provided a proof that was almost correct (i.e., there were very few errors reported by the proof checking program).

It's also important to note that my statement was false, and that became clear where I was trying to fix the errors reported by the proof checker. It turned out that there was an assumption that I neglected to include; the correct statement of the problem is

```
theorem
for F being Field,
    V being VectSp of F,
    A being Subset of V,
    l being Linear_Combination of A,
    x being Element of V,
    p being FinSequence of V,
    a being Element of F
  st rng p = Carrier l &
     p is one-to-one &
     a <> 0.F &
     x in Carrier l
  holds Sum ((l +* (x,a)) (#) p)
        = Sum (l (#) p) - (l.x)*x + a*x
```

The additional assumption posed no problem, because the theorem of which the current theorem was a lemma actually did have that assumption. So passing the assumption along from the main theorem's hypothesis to the local lemma's hypotheses was unproblematic. What's the difference between what I did and " If you have a global counterexample discard the conjecture, add to your proof-analysis a suitable lemma that will be refuted by the counterexample, and replace the discarded conjecture by an improved one that incorporates that lemma as a condition. Do not allow a refutation to be dismissed as a monster. Try to make all 'hidden lemmas' explicit." But that's just Rule 2 of the method of proofs and refutations!

These two examples[7] are offered to illustrate how the development of formal proofs can follow the method of proofs and refutations (MPR). Insofar as Lakatos intends MPR to be a characteristic feature of informal mathematics, he seems to be narrowing his philosophy too much. It seems to me that what Lakatos is doing is focusing on the *development* of informal mathematics as a response to claims about the *status* of formal mathematics. But if he had looked at the *development* of formal mathematics, he might have found an "ally among the enemies" in the guise of modern formal mathematics.

6.2.2.3 Example 3: A condition on polyhedra

My formalization [93] of a proof of Euler's polyhedron formula is based on Lakatos's presentation of Poincaré's proof; it is contained in chapter 2 of *Proofs and Refutations*. Lakatos's purpose is to allow one of the characters of his dialogue to give a 'final' proof of Euler's formula. My formalization follows that discussion. I gave a definition of polyhedron and described the condition (what Lakatos calls simple connectedness, but which is better referred to as being a homology sphere) that is sufficient for a polyhedron to satisfy Euler's relation ($V - E + F = 2$). The formal proof was nearly complete until a gap was uncovered: and essential condition was missed!

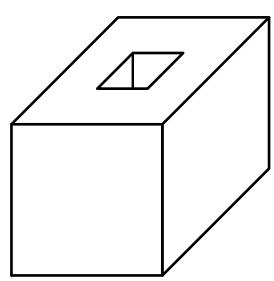
It turned out that there was a rather crucial part of the argument that was overlooked. In his discussion of Poincaré's proof, we find this exchange:

> GAMMA: I think that the boundary of a decent k-chain should be closed. For instance I could not possibly accept as a polyhedron a cube with the top missing; and I could not possibly accept as a polygon a square with an edge missing. Can you prove, that the boundary of any k-chain is closed?
>
> EPSILON: Can I prove that the boundary of the boundary of any k-chain is zero?
>
> GAMMA: That is it.
>
> EPSILON: No, I cannot. This is indubitably true. It is an axiom. There is no need to prove it.

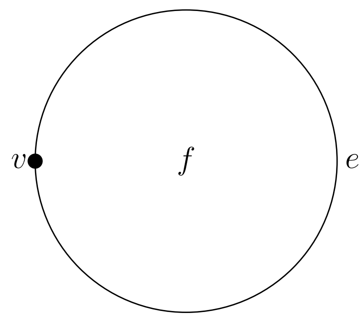
Lakatos is right that this principle must be an 'axiom' in some form. The significance of this passage was revealed to me *thanks to* the formalization.

To appreciate the significance of the missing condition, we need to lay down terminology for polyhedra. A polyhedron, for the purposes of the proof that I formalized, is given by three sets (of vertices, edges, and faces), and two so-called incidence matrices: one that says which vertices are incident with which edges, and another that says which edges are incident with which faces. To make the terminology uniform, for an integer k we say that a k-chain is a subset of the set of k-polytopes, where a k-polytope is supposed to be one of the basic elements of dimension k. (Thus a 0-polytope is a vertex, a 1-polytope is an edge, and a 2-polytope is a face.) For each integer k one can define a boundary operation, denoted ∂_k, whose domain is the set of k-chains and whose range is included in the set of $(k-1)$-chains. (Thus the boundary of an edge, a 1-chain, is a set of vertices, i.e., a 0-chain; the boundary of a face, a 2-chain, is a set of edges, i.e., a 1-chain.) Among the k-chains we can distinguish those that *go all the way around*, such as the edges of a polygon. Such k-chains are, appropriately enough, called k-circuits (also known as k-cycles). And some k-chains can be obtained by applying the boundary operation on a $(k+1)$-chain; such k-chains are called *bounding*.

Using this terminology, Lakatos lays down a condition on polyhedra that is standardly referred to as *simple connectedness*: a polyhedron p is simply connected if every k-circuit is bounding. (Again, this is Lakatos's terminology; a better term, and one that is actually used in the formal proof, is being a homology sphere.) In other words, the only way one can 'go around' is if one goes around *something*. Such is the case with polygons, for example: the reason why the set of edges of a polygon forms a circuit is that the edges 'traverse' a face. A failure of simple connectedness arises when one permits faces of polyhedra to have *holes* in them. Imagine a cube with hole in the top face: one can going around the perimeter of the hole, but one is not going around a face.



At one step in the proof it seemed that what was necessary is the converse to simple connectedness: every k-circuit is a boundary. Indeed, this feeling that something was missing, first suggested by the proof checker, turns out to be well founded: a counterexample to Euler's formula can be found if one does not assume this extra condition. Take the example of a circle (only one face in this polyhedron), whose perimeter is the only edge, which contains precisely one vertex.



More formally, the incidence matrices that characterize this polyhedron are: $\{(v, e)\}$ to represent the incidences between the vertices and the edges and $\{(e, f)\}$ to represent the incidences between the edges and the faces. Yet in this case, the boundary of the 2-polytope f is the 1-chain $\{e\}$, whose boundary is $\{v\}$. Euler's formula is false, because $V - E + F$ for this polyhedron is 1. Yet it is simply connected! (The condition that every circuit is a boundary is satisfied because there are no non-trivial circuits at all.)

6.2.3 Two Discoveries

The case studies of the two examples above illustrate that there are (at least) two kinds of discoveries to be had in formal mathematical theories. In the first example, we saw how, by formalizing the mathematical concept of a linear transformation as we did, we faced the problem of defining the notion of the application of a linear transformation to a linear combination. The second example we considered had to do with logical gaps that were exposed thanks to the requirement of strict formality. We discuss these two examples in more detail in the following two subsections.

6.2.3.1 First discovery: analysis of informal notation

The lesson that I take away from the formal work involved in defining the notion of the application of a linear transformation to a linear combination is an appreciation for how flexible our (informal or semi-formal) mathematical notation can be. In some cases, it is straightforward to formalize a mathematical concept, notation, theorem, or definition. In other cases, as this example shows, the problem of coming up with an adequate formalization itself requires some mathematical insight. Furthermore, once a decision is made concerning how to formally represent an informal mathematical notion, certain derived obligations arise, such as the obligation to prove that the $l(T^{-1}(\{w\}))$ is a finite subset of k. Arguably, the formalization has taught us something about our notation. When we write that

$$T(a_1 \cdot v_1 + a_2 \cdot v_2 + \cdots + a_n \cdot v_n) = a_1 \cdot T(v_1) + a_2 \cdot T(v_2) + \cdots + a_n \cdot T(v_n),$$

there does seem to be an implicit assumption that the $T(v_k)$'s are different. But *the informal notation gets it right.* If, say, $n = 3$ and $T(v_1) = T(v_2)$, then

$$a_1 \cdot T(v_1) + a_2 \cdot T(v_2) + a_3 \cdot T(v_3) = (a_1 + a_2) \cdot T(v_1) + a_3 \cdot T(v_3),$$

which falls out of our formal definition. The definition of $T@l$ also shows us that there is more to our informal notation than meets the eye. Who would have guessed that to formalize the apparently simple property of linear transformations would, formally, involve inverses and sums of subsets of k, and that we would further have to justify our notation by proving that no infinite sums arise?

This example challenges Lakatos's answer to his question ('What can one discover in a formal mathematical theory?'). By working in a formal mathematical theory, we 'force the issue' of the definitions of our terms. In the formal development of linear algebra, we would be forced eventually to say what linear combinations are, and to say what it means to apply a linear transformation to a linear combination. To meet this formal challenge, we had to engage in mathematical work that led to an unexpected result. Our discovery of the definition of the application of a linear transformation to a linear combination surely wins no awards for mathematical ingenuity, nor does it break new mathematical ground. Nonetheless, the unexpected features of the definition (unbounded sums, inverses) suggest that there is a bit more to the notion of linear combination than meets the eye. And we found that out through formalization.

6.2.3.2 Second discovery: gaps

In the second and third examples above, we saw that, thanks to the requirement of strict formality, we were able to spot a gap in a proof that might have been overlooked. What is claimed is not that formalization is the only way that the problem could have been discovered. If that were the case, then it would be necessary to describe the precise formalism that was used in considerably more detail. But (thankfully) that is unnecessary; the result is not ineliminably tied to the particular formalism that was used. What I claim is something rather more modest: thanks to formalization, an error that might have gone undetected was brought clearly to light.

The examples involving logical gaps leads into the broader epistemological question of how formal proofs can in any sense be epistemically 'superior' to non-formal proofs. Is there any philosophical justification for the enterprise of computer-checked formal proofs? One could take a skeptical view toward mathematical proof and hold that *only* completely formal proofs deserve to be called (genuine) proofs. Yet in the history of formal mathematics, one has to acknowledge the paucity of genuinely *interesting* logical gaps that have been exposed. The skeptical justification, which doubt the validity of virtually every proof in mathematics and regards all proofs are informal and (potentially) rife with logical gaps, is untenable. The failure to uncover *interesting* gaps—oversights, ambiguities, or errors that, once exposed, would alter the views of the working mathematician—is not to be taken lightly [55, 59, 130]. One might say that a formalized proof of a theorem gives us better grounds to believe the theorem than were available before the proof was formalized, but at present it seems to be an open philosophical challenge to say why this should be so, while acknowledging the rarity of interesting gaps [13].

6.2.4 Comments

We thus see the potential for formal mathematics to be a source for mathematical discoveries, rather than as an obstacle.

These thoughts are echoed by G. Gonthier, who designed a formal proof of the famous four-color theorem, which was discussed previously. He clearly lays out his motivation for his work:

> While we tackled this project mainly to explore the capabilities of a modern formal proof system—at first, to benchmark speed—we were pleasantly surprised to uncover new and rather elegant nuggets of mathematics in the process. In hindsight this might have been expected: to produce a formal proof one must make explicit every single logical step of a proof; this both provides new insight in the structure of the proof, and forces one to use this insight to discover every possible symmetry, simplification, and generalization, if only to cope with the sheer amount of imposed detail. . . . Perhaps this is the most promising aspect of formal proof: it is not merely a method to make absolutely sure we have not made a mistake in a proof, but also a tool that shows us and compels us to understand why a proof works. [131]

Gonthier thus sees the formalizer's burden—arguments be specified in more or less complete logical detail—not as an obstacle but as a potential source of innovation. The formalizer is spurred to try to discover refinements to the argument under consideration so as to make the formalization more tractable. Thus formalization provides, to some extent, a means of discovery.

Gonthier identifies at least two sources for potential innovation that come from formalization. In a formal proof:

- one must seek symmetries, simplifications, and generalizations to help make the formalization more tractable; and
- one cannot appeal to visual reasoning, nor to unformalized results.

Although Gonthier is a passionate and convincing advocate for the value of formalization, we should note that his conclusions are not necessarily the case for all formalizations. Although interesting discoveries are potentially at hand in any non-trivial formalization effort, innovation might not occur for two reasons.

First, the argument that Gonthier formalized was a rather substantial one (and has a complex history, too). It is not clear—and practice with proof-checking systems suggests—that we cannot expect interesting discoveries to routinely arise from the formalization of smaller or more straightforward proofs.

Second, Gonthier himself is a talented mathematician whose skills at programming and logic are clearly quite advanced. Had a mathematician with lesser skills taken on the same problem (to give a formal proof of the four color theorem), the discoveries that Gonthier made might not have arisen. The potential for discovery does not lie solely in the tools (the proof checker), nor in the proof to be formalized, but in the way that the formalizer uses his tools in his formalization.

6.3 Further Worries

6.3.1 The problem of translation

One question that often arises in response to formal proofs of mathematical theorems is: are we sure that the definitions of the concepts involved in the proof are accurately represented in the formalization? The worry is that if we have not accurately formalized our concepts, then the value of the formal proof is diminished, if it is meaningful at all.

Lakatos raises the problem of translation in connection with Poincaré's proof of EPF. The problem is, roughly: *how do we know that the terms in Poincaré's proof have the same meaning as the terms outside of Poincaré's proof?* We are interested in polyhedra, in some more-or-less intuitive sense; does Poincaré's proof show us that polyhedra, in our more-or-less intuitive sense, satisfy Euler's formula?

The problem of translation comes up just after Epsilon has finished giving his (Poincaré's) proof of EPF:

> Alpha: Before you do let me raise a second question about your proof, or rather about the finality and certainty that you claim for it. Is the polyhedron in fact a model of your vector-algebraic structure? Are you sure that your translation of 'polyhedron' into vector theory was a *true* translation?
>
> Epsilon: I have already said that it is true. If something startles you that is no reason for doubting it. 'I am following the great school of mathematicians who, in virtue of a series of startling definitions, have saved mathematics from the sceptics, and provided a rigid demonstration of its propositions.'
>
> Teacher: I indeed think that this method of translation is the heart of the matter of the certainty and finality of Epsilon's proof. I think we should call it *translation-procedure.*

Epsilon/Poincaré modeled polyhedra with the help of incidence matrices, from which various vector spaces were defined. Alpha asks whether what Epsilon has done is a true "translation" of the intuitive concept of polyhedron into a linear algebraic framework. Later in the dialogue, Alpha again states the problem:

> Alpha: But you [Epsilon] lose something which is much more important. You have to restrict your Euclidean programme to theories with perfectly known concepts, and when you want to pull theories with vague concepts into the scope of this programme, you cannot do this by your translational technique: as you said, you do not translate, rather you create new meaning. But even if you tried to *translate* the old meaning, some essential aspects of the original vague concept may get lost in this translation. The new clear concept may not serve for the solution of the problem for which the old concept was meant to serve. If you regard your translations as infallible, or, if you consciously scrap the old meaning, both these extremes will yield the same result: you may push out the original problem into the limbo of the history of thought—which in fact you do not want to do. So if you calm down, you have to admit that definition must have a touch of modified essentialism: it must preserve some relevant aspects of the old meaning, it must transfer relevant elements of meaning from left to right.

The worry is that some essential aspects of the intuitive concept of polyhedron may get lost. I take it that an 'essential' loss here means such a modification of the intuitive concept that can no longer confidently state that the mathematical theorem is about what we intended it to be about.

Does the problem of translation apply to formal proofs? At first glance it would appear that the problem applies to a greater degree to formal proofs as it does to informal proofs (such as Poincaré's): formal proofs are written in a non-natural language, with which we are less familiar, so we lack standards for what counts as an adequate expression in the non-natural language of our intuitive concepts.

One way of putting the problem of translation is that there can be different translations of one and the same informal statement into a more formal language; the translations are different because they imply different statements.

But does that really arise in the case of formal proofs? I would urge that they do not; it seems to me that there are often unproblematic translations from informal to formal language. For example: translate "a polyhedron is determined by three sets V, E, and F consisting of its vertices, edges, and faces" as

```
definition
  mode polyhedron
means
  ex V begin set, E begin set, F being set st it = [V,E,F];
```

Here "`ex`" means "exists" and "`st`" means "such that"; the notation "`[V,E,F]`" refers to the ordered triple of the three sets V, E, and F. (That V, E and F are translated as sets is given by the `being set` construction.) The `it` is an indexical; we are defining the type `polyhedron` by a formula with one free variable, called `it`.

This snippet of MIZAR code is an unproblematic translation of the expression "a polyhedron is determined by three sets V, E, and F". Somewhat more formally, this statement is understood as: "to say that something is a polyhedron is to say that there exist three sets

V, E, and F that determine the polyhedron". If one doubts that ordered triples adequately determine their data, one should be swayed by the following facts in the MML:

```
definition
  let X1, X2, X3 be set;
  func [:X1,X2,X3:] -> set
         equals
       [:[:X1,X2:],X3:];
```

and the formal theorem

```
for X1,X2,Y1,Y2 being set
  st [:X1,Y1:] = [:X2,Y2:]
  holds X1 = X2 & Y1 = Y2;
```

It is perhaps not always so simple for formal proofs. But I submit that the problem of translation, insofar as it applies between informal and formal proofs, is largely unproblematic. Experience shows that formal proofs and informal proofs are already fairly close to one another; whatever essential content that has been lost has been lost at an earlier stage in the development of the theorem and proof.

As for the problem of translation for informal proofs, we may respond by pointing out that, at least in the case of Euler's formula, the objection that Poincaré's polyhedra are simply too abstract to count as genuine polyhedra, is not unique to Lakatos. Indeed, mathematicians themselves—even those who are quite sympathetic to formal proofs—are sensitive to the issue.

One response to the problem of Poincaré's polyhedra is given by Steinitz's theorem which shows how to relate abstract polyhedra to analytic ones, i.e., ones with which we are more familiar. Steinitz's theorem is discussed in chapter 4; here is a brief restatement of the result. Let $G(P)$ be the graph determined by the vertices and edges of a convex polytope P. It is not difficult to show that $G(P)$ is planar and 3-connected (i.e., no removal of two vertices disconnects the graph) for every 3-polytope P. Steinitz's theorem is eseentialy the converse:

Theorem 22 *A graph C is isomorphic to the graph $G(P)$ of a 3-polytope P iff C is planar and 3-connected.*

For a proof, see Barnette and Grünbaum [132]. The theorem relates combinatorial structures arising from polyhedra to the polyhedra themselves.

Thus, the mathematical community themselves wondered what the connection was between abstract polyhedra and our intuitive geometric concept of polyhedra. The problem of translation may be a problem, but it is not an obstacle that we cannot address.

In the latter part of *Proofs and Refutations*, after EPSILON/ presents Poincaré's proof of Euler's polyhedron formula, some other characters ask whether we can be confident that we have now proved Euler's formula.

> ALPHA: Is the polyhedron in fact a model of your vector-algebraic structure? Are you sure that your translation of 'polyhedron' into vector theory was a *true* translation?
>
> EPSILON: I have already said that it is true. If something startles you that is no reason for doubting it. 'I am following the great school of mathematicians who, in virtue of a series of startling definitions, have saved mathematics from the sceptics, and provided a rigid demonstration of its propositions.'
>
> TEACHER: I indeed think that this method of translation is the heart of the matter of the certainty and finality of Epsilon's proof. I think we should call it *translation-procedure*.

The problem here is that Poincaré's/Epsilon's proof of Euler's formula involved a particular definition of the concept of polyhedron as a certain kind of combinatorial structure. Earlier in the discussion of Poincaré's/Epsilon's proof there was a question of whether the definition is appropriate:

> GAMMA: I am a bit puzzled by your definition of polyhedra. In the first place, as you bother to define the notion of a polyhedron at all, I conclude that you do not consider it to be perfectly well known. But then where do you take your definition from? You defined the obscure concept of polyhedron in terms of the 'perfectly known' concepts of faces, edges, and vertices. But your definition—namely that the polyhedron is a set of vertices, plus a set of edges, plus a set of faces,

> plus an incidence matrix, obviously fails to capture the intuitive notion of a polyhedron. It implies, for instance, that any polygon is a polyhedron, as is, say, a polygon with a free edge standing out of it.

Gamma is right that Poincaré's/Epsilon's definition of polyhedron that is advanced at this stage of the proof is clearly too broad; *any* set of vertices, edges, and faces, arranged in any way, falls under Epsilon's combinatorial definition. One could take Gamma's worry farther and note that, at this stage, Euler's polyhedron formula is surely invalid. Consider, for example, a 'polyhedron' with no vertices, no edges, and no faces. Such a degenerate structure falls under the combinatorial definition so far, but it falsifies the formula ($0 - 0 + 0 = 0$, not 2).

Some kind of condition needs to be imposed on combinatorial polyhedra. And indeed, a condition is eventually added: the combinatorial polyhedron must be simply connected. A good deal of discussion in chapter 2 of *Proofs and Refutations* is devoted to understanding this condition on polyhedra. Epsilon does lay down a definition, but to appreciate its geometrical significance, a number of examples are considered.

In Lakatos's words, the question is whether combinatorial polyhedra are a good model of polyhedra. The problem seems to be that there are two realms of mathematical objects, or two concepts: *combinatorial polyhedra* and *polyhedra*. The former concept is clearly defined in the language of set theory; the latter is not so well defined, but there are any number of uncontroversial examples. For *combinatorial polyhedra* we can lay down a rigorously defined condition, simple connectedness, and rigorously prove that all simply-connected combinatorial polyhedra are Eulerian. For (pre-theoretical) *polyhedra* we apparently lack a proof. The problem of translation can be stated as: *can we transfer the knowledge that we get from the Epsilon's proof for combinatorial polyhedra to non-combinatorial polyhedra?* Or: even if we grant the most secure knowledge of one realm of objects, can we conclude that we have the same kind of knowledge for another realm of objects?

It would seem that, initially, the intention behind asking the question is to be skeptical about claims to mathematical knowledge. At least for some mathematical domains—such as the study of polyhedra, where the objects are apparently richly structured than we might initially take them to be—the best the mathematician can do is to lay down certain definitions of his concepts and rigorously prove properties of whatever objects satisfy those definitions. His proof may even be specified to the highest level of logical detail, as is th case with computer-checked formal proofs. But at the end of the day, when he has finished his proof, the mathematician has only his proof. He cannot move from the claim

> I know with certainty that this argument is valid

to

> I know with certainty the proposition proved is true

because he does not know that the definitions employed in his proof are correct.

This reminds us of the usual distinction between validity and soundness of arguments. The validity of an argument can be determined by the data given in the argument itself. The soundness of the argument, on the other hand, cannot in general be determined from the data of the argument. Some external knowledge seems to be required.

Lakatos may ultimately be right; it may be that, philosophically, there are limits on what we can know about mathematical concepts. Yet although this may seem to be correct in the case of polyhedra, for other mathematical structures knowledge suffers less from the problem of translation. Let us consider two examples.

First, let us consider the natural numbers. Like polyhedra, these are mathematical objects about which we have much intuition. We can give a formal proof in, say, Peano Arithmetic that 4 is an even number, a formal proof of the statement $\exists k((1+1)\cdot k = 1+(1+(1+1)))$. Does this show that 4 is an even number? If we agree that the number 4 is accurately expressed in the language of Peano Arithmetic by the term '$1 + (1 + (1 + 1))$', and if we agree that the concept of evenness of an number a is accurately expressed in the language of

Peano Arithmetic by the existential formula '$\exists k \ulcorner 2 \urcorner \cdot k = \ulcorner a \urcorner$', if the number 2 is accurately captured by '$1+1$', and if we agree that the axioms of Peano Arithmetic express valid laws of arithmetic, then we can be confidently claim that d gives us justification that 4 is an even number.

We can see that the validity of our deduction d can be established by looking only at the deduction itself. No knowledge of arithmetic needed to see that the figure d is in fact a deduction. However, we have to admit that to infer from the deduction that 4 is an even number requires more than the deduction itself. Our knowledge that 4 is an even number is grounded not merely by the deduction d. We have to set up coordination principles between our non-formal concepts and certain formal expressions. And those coordination principles (such as: 'the number 4 is accurately expressed by the term $1+(1+(1+1))$') can be true or false, and the truth or falsity is not given by d. Although we can have certain knowledge that d is a deduction, our knowledge that the proposition we intended to prove is in fact proved is mediated by the coordination principles. That is: the certainty of the 'deductionhood' of d does not imply that we know with certainty that 4 is an even number.

To be clear, this example was chosen not to mock Lakatos's philosophy. The example was *not* chosen to show that, in fact, we can have certain knowledge that our coordination principles are correct—and thus Lakatos is wrong. In the case of natural numbers, it seems fairly clear that we *can* have irrefragable confidence (or something near enough) in the correctness of our coordination principles: the term $1 + (1 + (1 + 1))$ *is* an adequate formalization of the number 4; the formula $\exists k((1+1) \cdot k = \ulcorner a \urcorner)$ *is* an adequate formalization of the property of the number a being even. This is not dogmatic table-thumping. It is consistent with Lakatos's philosophy that we can have certain or near-certain knowledge of the correctness of our coordination principles. Lakatos is not a skeptic who wishes to deny that we can have mathematical knowledge of the highest epistemological nature. Rather, the more modest lesson to take away from this example is that *the quality of our formally proved mathematical knowledge is limited by the quality of our coordination principles.*

The second example that I wish to consider is algebraic. A *group* is a mathematical structure equipped with a binary function that is associative, has a left and right identity, and left and right inverses. These properties can be straightforwardly formalized using the language of first-order logic.[8] One simple theorem about groups is Lagrange's theorem: for a finite groups, the order of a subgroup of a group G always divides the cardinality of G. One can give a formal proof of this fact (as has been done in, for example, the MIZAR system [133]). In the case of groups and other similarly-defined algebraic structures, the possibility of uncertainty is considerably reduced. The coordination principle that allows to infer from a formal proof of Lagrange's theorem that the property it expresses lies almost exclusively in the *convention* that the concept of a group just *is* any structure that satisfies the group axioms. Other coordination principles are at play as well: since the proof involves some arithmetic, a formal proof of Lagrange's theorem needs to have formalizations for the relevant arithmetical concepts and theorems.

The purpose of these two examples is to contrast the example of Euler's polyhedron formula from other mathematical results. For polyhedra, the status of our coordination principles is more contentious than they are in the case of arithmetic and algebraic structures such as groups, which admit a definition by convention. Again, the lesson to take away from these examples is not that Lakatos is wrong. Lakatos is not intended to be a skeptic who insists that through formal proof we cannot have any mathematical knowledge. Rather, these examples are chosen to help us to understand Lakatos's point that the soundness of our formal proofs depends not only on the proofs themselves but also on coordination principles that relate the formal expressions to informal concepts. In some cases, these coordination principles can be very good, apparently irrefragable. In other cases, such as polyhedra, they can be more controversial.

6.3.1.1 Aside: Comparing Lakatos's problem of translation with Quine's problem of the indeterminacy of translation

In *Word and Object* [134] and later works [135–136], Quine posed a problem that is apparently related to the problem that Lakatos raises. Quine called it the **indeterminacy**

of translation. The words suggest that Quine and Lakatos are dealing with a similar problem. But the two problems are quite different.

Quine's problem involves a thought experiment of 'radical translation', where a 'field linguist' in the jungle is trying to communicate with natives whose language he does not understand. Radical translation is an interpersonal situation, and the resulting indeterminacy is a critique of meaning. The problem problem is intersubjective and linguistic; it has to do with the problem of communication between people whose native languages differ. Lakatos's problem of translation is not inherently linguistic, nor is it a problem of intersubjectivity.

We can further distinguish indeterminacy of translation from the problem, well known the philosophy of science, of underdetermination of theory by date: Contrasting these two problems, Quine writes:

> If translators disagree on the translation of a Jungle sentence but no behavior on the part of the Jungle people could bear on the disagreement, then there is simply no fact of the matter. In the case of natural science, on the other hand, there is a fact of the matter, even if all possible observations are insufficient to reveal it uniquely. [136]

Contrasted with Quine's problem of the indeterminacy of translation, Lakatos's problem of translation is (apparently) not interpersonal, nor is it (inherently) linguistic. Rather, it seems to be a problem about mathematical *concepts*.

Lakatos's point seems to be that to express our mathematical arguments (and hence, to formalize them), we must take an stand toward the salient mathematical concepts. We thus are not proving anything about a mathematical *concept* (or concepts), but rather about some *articulation/conception* of them.

6.4 Conclusion

By 'forcing the issues' of (1) exactly how mathematical concepts are formally represented, and of (2) the precise structure of a mathematical proof, it would seem that the formal viewpoint behind modern proof-checking enterprises, far from standing in opposition to Lakatos, actually *support* his philosophy of mathematics. Lakatos is interested in the development of mathematical concepts and proofs.

7 Conclusion

The project described here was an engagement with the philosophy of mathematics of Imre Lakatos. The main task was to present Lakatos as offering a challenge to those who work with (what I have called) modern formal proof technology. There, formal proofs are, of course, the central object of study to the extent that they are actually constructed. Lakatos, on the other hand, is generally quite negative about such proofs and their value for philosophy of mathematics, arguing specifically that they have little to say about the growth of mathematics, and mathematical discovery.

If I have responded well to Lakatos's challenge, then I have successfully argued that, first of all, that Lakatos's central insight into the methodology of mathematics—what he calls the method of proofs and refutations—applies as well to formal mathematics as it does to informal mathematics. Moreover, I hope to have mitigated Lakatos's skepticism about the methodology of mathematics by arguing that the view of mathematical knowledge as *conjectural* is not well supported.

If, as Worrall suggests [122], the aim of *Proofs and Refutations* is to call attention to merely call attention to the growth and history of mathematics without offering any distinctive new view about the epistemology of mathematics, then the strength of the argument is considerably mitigated. Surely no one can object to an expansion of the scope of the philosophy of mathematics to include such case studies as Lakatos's. Relatedly, if all Lakatos is arguing is that it is a mistake to *identify* the philosophy of mathematics with metamathematics, then again there is little room for disagreement. Feferman put it well when he concedes that 'logic as it stands fails to give a direct account either of the historical growth of mathematics or the day-to-day experience of its practitioners' [54]. If that is Lakatos's main point, then again there seems to be little room for disagreement. And if Lakatos is just trying to get us to all be a little more modest about our proofs and to prefer the heuristic presentation of mathematics in the classroom, then this seems to be a laudable goal and I think we can all support it.

Assuming, then, that Lakatos is in fact trying to develop some new epistemological features of mathematical knowledge, then more room is available in which to carry out the discussion. My hope is to have contributed to Lakatos scholarship by bringing him 'up to date' with developments in modern formal proof technology that Lakatos could only imagine. I aimed to take up the tenor Lakatos's new insights into the philosophy of mathematics while, at the same time, taking issue with some of the places where he overreaches. The work is written in the hope that it would take Lakatos on in his own terms; I hope to have avoided the charge of belonging to the camp of 'dogmatists' that Lakatos describes in the introduction to *Proofs and Refutations*, as those who simply simply take mathematical knowledge to be uncriticizable, infallible, deserving of our immediate assent, or any other heavy-handed epistemological feature.

At the same time, Lakatos might charge me with taking up the 'dogmatist' line of thought because I question the extent to which his skeptical view applies. It is not clear, for example, that Lakatos has given an argument that *mathematical knowledge is not a priori* or that *mathematical proofs do not provide a priori justifications*. It is consistent with Lakatos's view that *mathematical knowledge differs from 'everyday' knowledge of the world*, and that *even if mathematical knowledge is fallible, the character of its fallibility differs from that of other kind of knowledge*, and, relatedly, *mathematical proofs are justify knowledge in rather special way*.

I have also discussed a handful of problems as they arise from the combinatorial treatment of polyhedra. The problems there are (meta)mathematical. A number of problems remain in this direction.

The project contained here suggests a number of fruitful directions for further research. They are, mainly, philosophical approaches; they focus, moreover, primarily on the epistemology of mathematics. Lakatos has inspired research in the philosophy of mathematics on several fronts that promise to shed new light and help us to better appreciate one of the oldest and arguable epistemically most interesting aspects of human intellectual life.

A Endnotes

A.1 Chapter 2: Formal Proofs in Mathematics

1 Historically, it was Hilbert and Bernays who gave completeness as an open problem in their *Grundzüge der theoretischen Logik*. By adapting a result of Skolem, Gödel was able to solve the problem.

2 Peano remained active in the project of formalization for years. As a side note, Peano was clearly quite interested in language more generally: he designed his own language—Latino sine Flexione (Latin without inflections)—in which his book was written. (The citation [2] is to to the French translation.)

3 What follows is a discussion of notable events in the 20th century. But arguably this presents far too modern of a point of view; already, in the imaginings of thinkers from long ago, such as Leibniz, we see the idea of computers being used in connection with proofs as they are used today.

4 Work by (for example) Orevkov gives a sense in which formal proofs (in some proof formalisms) can be so large as to be practically impossible to completely survey. What we have in mind here is something more mundane that Orevkov-style results: that the problem of producing formal proofs can result in deductions that are much larger than the informal proofs from which they come.

5 A list of 100 interesting mathematical theorems, and their status as formalized or unformalized (and, if formalized, in which of the many contemporary proof checking systems) is maintained [19] by F. Wiedijk.

6 Harrison is not the only one to articulate this goal for an ideal proof system: one can hear this goal in informal conversation among those who are active in the subject.

7 Another work connecting Kuhn and Lakatos, not motivated by experimental mathematics, is [33].

8 In more mathematical terms, the Kepler conjecture states that the density of a packing of congruent spheres in R^3 is not greater than $\pi/\sqrt{18}$.

9 Another famous long-standing problem in mathematics, Fermat's Last Theorem, was stated around 1637 [35], and solved by Andrew Wiles in 1995 (after Wiles's 1993 proof was found to be flawed). The difference between the time when the problem was solved and when it was posed for Fermat's last theorem and the Kepler conjecture are, respectively, 358 and 387 years.

A.2 Chapter 3: A Lakatosian Challenge

1 Feferman has criticized Lakatos for focusing on mathematical statements that have only a universal form $\forall x \varphi(x)$, but many mathematical statements do not have such a form, such as "$\sqrt{2}$ is irrational" and "there are exactly two integers that divide all other integers". The logical form of a great many of the statements of mathematics is, however, universal.

2 At one point Lakatos simply says that the proof analysis of a proof just is the list of 'lemmas' coming from the proof: the character Kappa criticizes the way that Teacher is responding to the critique that the students are giving of Teacher's initial proof of Euler's polyhedron formula:

> Kappa: You improved the proof-analysis, i.e. the list of lemmas; but the thought-experiment which you called 'the proof' has disappeared.

Nonetheless, Lakatos places more weight on the idea of proof analysis as an activity of investigating the conditions under which the moves carried out in the proof can be made, or are correct. This can lead to a refinement of the list of lemmas.

3 It seems to me that one issue that classical philosophy of mathematics addresses and which Lakatos does not are metaphysical and ontological questions about mathematical objects. But one reviewer has noted [76] an interesting metaphysical corollary of Lakatos's case study of Euler's formula: "In the beginning Euler's theorem was false; in the end it is true because we have come to formulate a concept of polyhedron that makes it true. The theorem has been 'analytified'. Yet making it true by convention was not matter of fiat but the product of refined analysis. This doctrine of analytification has unsettling consequences. The Platonist cannot welcome a view which makes the truth of the proposition in the end something embedded in

the canons of mathematical language, where the ideas are stripped of their dignity. They are no longer what makes mathematics true, nor the subject matter of mathematics. Yet the nominalist is equally disconcerted, for even if we end up with truth by convention, the convention seems to be organising a 'reality' that has nothing to do with words."

4 Again, we shall see later what MPR amounts to, but for now, to ward off any misunderstanding, Lakatos is not saying that strict deductions of a universal claim $\forall x\varphi(x)$ and crystal-clear counterexample $\neg\varphi(a)$, in which there is no equivocation of the terms in the two claims, are simultaneously allowed. That, of course, would be irrational. As one might expect Lakatos is using the words "proof" and "refutation" in a special sense related to but different from our usual use of the words. We can see that "proof" doesn't mean something like "deduction in Fitch" and counterexample means something like "configuration in Tarski's World/ showing a universal statement to be false". Fitch and Tarski's World/ are dealing with a concept of proof as formal deduction, and counterexample as object in a structure for which a negation holds, following Tarski's definition of truth. For these concepts we have the soundness and completeness theorem, which imply that logical validity coincides with provability. Thus, if a statement is proved in this sense, then, by the soundness theorem, if is impossible to give a counterexample.

A.3 Chapter 4: A Formal Proof of Euler's Polyhedron Formula

1 Many results could be called 'Euler's formula'; Euler was a prolific mathematician who made fundamental contributions to any number of areas of mathematics. A result arguably more famous than the polyhedron formula that could be the referent of 'Euler's formula' is the famous relation $e^{ix} = \cos x + i \sin x$, one of whose special cases is the remarkable $e^{i\pi} + 1 = 0$. In this paper, 'Euler's formula' is short for 'Euler's polyhedron formula'.

2 Euler's text has been modified to bring it into line with the notation used in this paper: he did not use the conventional English abbreviations 'V', 'E', and 'F'.

3 Euler proved that proposition 6 is equivalent to proposition 11. This is an interesting equivalence because one statement has a combinatorial flavor, while the other has an analytic flavor. Proposition 11 can be seen in the famous Gauss-Bonnet formula [81].

4 Unknown to Euler, Descartes had actually given a proof of Proposition 11 [82]. This result of Descartes's, seems to have been missing at Euler's time; it was rediscovered in the 19th century, long after Euler's death [83].

5 Poincaré was interested more broadly in the new subject of topology, of which he was one of the earliest explorers; his new proof of Euler's polyhedron formula was but one element in his wider topological program.

6 Poincaré was not the first to generalize Euler's polyhedron formula to higher dimensions; that was done by L'Hullier.

7 In fact, Poincaré used a single incidence matrix to represent a polyhedron. The matrix is a block matrix, two of whose blocks are just the zero matrix, expressing the fact that vertices are not (strictly speaking) incident with faces but only with edges.

8 At the time the formalization began, no formal proof of Euler's formula was known. But independently, another formal proof has been carried out in the coq system [90].

9 It would be interesting to discover cases where one *learns* something different about a proof (and not about the different systems or the different logics on which they are built) when formalizing it in one system as compared with what one learns from another formalization of the same proof.

10 There are two kinds of missing knowledge: well-known (perhaps named) mathematical results can be contrasted with details that, in an less formal context, are left tacit.

11 And, conversely, often one discovers that mathematical knowledge that was previously thought to be unformalized does in fact exist in the library. At one point I thought that he had a *proof* that the mizar library did not contain a formalization of the fact that $\{0, 1\}$ can be regarded as a two-element field. This turned out to be mistaken.

12 This is a case where a representation of a mathematical object contains more information than meets the eye. When represented this way, linear combinations tacitly build in the commutativity of vector addition.

$u + v$ is represented by a function f that sends u and v to 1 and every other vector to 0. The same function f also represents $v + u$.

13 The condition of finiteness is necessary because linear combinations must be finite; if X is infinite no finite set of singletons can span X.

14 In fact, if one inspects the formal proof one sees that polytope sets are assumed to be ordered. However, it is still the case that orientation plays no role in this development: the ordering is assumed to make certain definitions simpler; an unordered approach would have worked just as well.

15 In the MML version 4.110.1033, released September 9, 2008, the exact MIZAR item is `VECTSP_7:def 3`. Every type in MIZAR must be provably non-empty. Interestingly, the theorem that every vector space has a basis appears not as a MIZAR theorem *per se*, but rather as the justification for the non-emptiness of the type `Basis of V`, where V itself has the dependent type `VectSp of F`, where, finally, F has type `Field`. The proof of the non-emptiness of the `Basis` type appeals to the theorem that every linearly independent subset of a vector space can be extended to a linearly independent spanning set, *i.e.*, a basis.

16 Simpson has shown that the principle 'Every vector space has a basis' is equivalent, over the second-order arithmetical theory RCA_0 (for 'recursive comprehension axiom'), to the principle of arithmetical comprehension [103].

17 The custom code is not yet complete; certain features of the MIZAR system are not yet accounted for, such as so-called registrations and the implicit uses of Hilbert's ε-operator. Thus it is possible that some important dependency relations are not being taken into account with the present version of the software.

18 Perhaps even this notation could be implemented in MIZAR, but its logical properties are peculiar and would be a challenge to formally specify.

A.4 Chapter 5: Metamathematical Problems about Polyhedra

1 For more information about Schläfli's work, see Coxeter [89].

2 The games proceed as before, but with a new kind of move: not only can the players choose elements of structures, but also subsets. Spoiler chooses one of the structures and either a subset or an element of it; duplicator chooses from the other structure either a subset or an element of it, corresponding to the kind of move that spoiler made. Duplicator wins the game after k turns if the structures, with the chosen elements and chosen subsets, are partially isomorphic. See Libkin [114], chapter 7.

3 This is the principle which, in its simplest form, states that $|A \cup B| = |A| + |B| - |A \cap B|$. This involves only two terms; for more terms, the principle becomes more complicated.

4 The argument is simple: since every element of a polyhedral complex satisfies exactly one of V, E, or F, there must be at least one vertex, at least one edge, or at least one face. In the first and the third case, axiom **?** ensures that there is some other element to which the element is incident. And if there is an edge, then, by **?**, there are vertices with which the edge is incident.

5 That can be seen because one can prove that if there is an inaccessible cardinal κ (and if ZF is consistent), then V_κ is a model of ZF. If ZF were to prove the existence of an inaccessible cardinal, then it would prove its own consistency. See Kunen [117] for more details.

A.5 Chapter 6: Responding to the Lakatosian Challenge

1 "This reflects the characteristic mathematical situation: the mathematician hits upon his proof by unregimented insight and good fortune, but afterwards other mathematicians can check his proof." [121] Lakatos upbraids Quine for this statement, accusing him of equivocating on the meaning of 'mathematics' by using the word in both its formal and informal ('ordinary') senses. Lakatos points out that "often the checking of an *ordinary* proof is a very delicate enterprise, and to hit on a 'mistake' requires as much insight and luck as to hit on a proof".

2 Oddness could have been formalized differently. We could have said: n is odd iff there exists a natural number k such that $2 \cdot k + 1 = n$. With this definition of oddness, the proof that if n is even then $n + 1$ is

odd does not require any number-theoretic axioms: by definition, there exists a natural number k such that $2 \cdot k = n$; adding one to both sides gives $2 \cdot k + 1 = n + 1$ (which follows by an axiom for equality), so that $n + 1$ is odd. Summary: the k that witnesses the evenness of n also witnesses the oddness of $k + 1$. In other words, the evenness of n (first-order) logically implies the oddness of $n + 1$. The exercise becomes more involved if one uses the definition of oddness given in the text, for then the evenness of n does *not* logically imply the oddness of $n + 1$; to prove that $n + 1$ is odd one must appeal to some non-logical number-theoretic axioms.

3 The statement that logic alone doesn't specify how we should organize a search for a deduction is correct enough as it stands, but there is considerable interest within the automated reasoning community on developing heuristics for how this search can be carried out. [127]. The community has been somewhat successful; they can claim to have discovered a formal proof of a theorem (the solution to the so-called Robbins conjecture) that no human had found. [128–129]

4 It is somewhat peculiar that Lakatos didn't highlight this potential value of formal proofs. After all, one reason for the failure of a sequence of formulas to be a deduction is that the theorem to be proved suffers from a so-called *global counterexample*, or perhaps the problem is rather more isolated (*local counterexample*). This echoes a point made by Feferman. [54]

5 The function l that represents the simple linear combination $u + v$ also represents $v + u$. More generally, if l represents $a_1 \cdot v_1 + a_2 \cdot v_2 + \cdots + a_n \cdot v_n$, then l also represents any permutation of the terms. Thus, our choice of representation for linear combinations tacitly builds in the commutativity of vector addition.

6 And in fact, to justify the definition in the MIZAR system, one has to prove that the definition does make sense by showing that the application of l to $T^{-1}(\{w\})$ is finite.

7 These examples follow the pattern of Feferman's "logical analysis" scheme [54].

8 There are a variety of possible axiomatizations of group theory. One can formulate the axioms using a constant symbol for the identity, or not; one can require that the identity be both left and right, or just right (in which case one has to assume that one can cancel on the left).

B A MIZAR Proof of Euler's Polyhedron Formula

This appendix contains the formal text, expressed in the MIZAR language, of a proof of Euler's polyhedron formula. The formal work is laid out in three stages:

1. First, a formal proof the rank+nullity theorem (which is the main linear algebraic result in Poincaré's proof);
2. Second, a formal development of the construction of a vector space based on the powerset of a set;
3. Finally, a formal development of Poincaré's proof.

The three stages build on each other. Moreover, the work does not take place *ex nihilo*; the proof makes extensive use of much mathematical knowledge that has already been formalized in the MIZAR Mathematical Library.

The software with which one can verify these proofs can be downloaded from the MIZAR homepage [22].

B.1 The rank+nullity theorem

```
:: The Rank+Nullity Theorem
::  by Jesse Alama
::
:: Received July 31, 2007
:: Copyright (c) 2007 Association of Mizar Users

environ

 vocabularies RANKNULL, VECTSP_1, MATRLIN, VECTSP10, VECTSP_9, RLVECT_3,
      RLSUB_1, FUNCT_1, FINSET_1, SUBSET_1, BOOLE, CARD_1, RELAT_1, RLVECT_1,
      RLVECT_2, INCSP_1, RLSUB_2, FINSEQ_1, QC_LANG1, FUNCT_2, TARSKI, ARYTM_1,
      FUNCOP_1, LOPBAN_1, SEQ_1, FINSEQ_4, FUNCT_4, CAT_1, COMPLEX1, TDGROUP,
      ARYTM, GROUP_1;
 notations TARSKI, XBOOLE_0, SUBSET_1, DOMAIN_1, RELAT_1, RELSET_1, FUNCT_1,
      NAT_1, NUMBERS, FUNCOP_1, PARTFUN1, FUNCT_2, FUNCT_4, XCMPLX_0, XXREAL_0,
      CARD_1, FINSET_1, FINSEQ_1, FINSEQOP, STRUCT_0, RLVECT_1, RLVECT_2,
      VECTSP_1, FUNCT_7, VECTSP_4, VECTSP_5, VECTSP_6, VECTSP_7, MOD_2,
      MATRLIN, VECTSP_9, LOPBAN_1;
 constructors NAT_1, FINSEQOP, HAHNBAN, VECTSP_6, VECTSP_7, MOD_2, VECTSP_9,
      REALSET1, RLVECT_2, WELLORD2, LOPBAN_1, VECTSP_5, FUNCT_7, FUNCT_4,
      XXREAL_0, MATRLIN;
 registrations RELAT_1, FUNCT_1, FUNCT_2, STRUCT_0, CARD_1, FINSET_1, FRAENKEL,
      VECTSP_9, XBOOLE_0, VECTSP_7, MATRLIN, FUNCOP_1, ORDINAL1, XREAL_0,
      SUBSET_1, VECTSP_1;
```

```
 requirements BOOLE, SUBSET, NUMERALS, ARITHM;
 definitions TARSKI, RELAT_1, FUNCT_1, FINSEQ_1, VECTSP_4, VECTSP_6, XBOOLE_0,
      RLVECT_1, STRUCT_0, MOD_2, MATRLIN, FUNCOP_1, LOPBAN_1, FUNCT_2;
 theorems TARSKI, ZFMISC_1, RELAT_1, FINSET_1, FINSEQ_1, FUNCT_1, VECTSP_7,
      VECTSP_9, CARD_2, XBOOLE_1, FUNCT_2, SUBSET_1, XBOOLE_0, VECTSP_1,
      RLVECT_1, VECTSP_4, VECTSP_6, STRUCT_0, RLVECT_2, MOD_2, MATRLIN, CARD_1,
      FUNCOP_1, VECTSP_5, FUNCT_7, FINSEQ_2, FUNCT_4, ENUMSET1, ORDINAL1,
      PARTFUN1;
 schemes CLASSES1;

begin

theorem Th1:
  for f,g being Function
  st g is one-to-one & f|(rng g) is one-to-one & rng g c= dom f
  holds f*g is one-to-one
proof
  let f,g be Function such that
A1: g is one-to-one and
A2: f|(rng g) is one-to-one and
A3: rng g c= dom f;
  set h = f*g;
A4: dom h = dom g
  proof
    thus dom h c= dom g
    proof
      let x be set such that
A5:   x in dom h;
      thus thesis by A5,FUNCT_1:21;
    end;
    thus dom g c= dom h
    proof
      let x be set such that
A6:   x in dom g;
      g.x in rng g by A6,FUNCT_1:12;
      hence thesis by A3,A6,FUNCT_1:21;
    end;
  end;
  for x1,x2 being set st x1 in dom h & x2 in dom h & h.x1 = h.x2 holds x1 = x2
  proof
    let x1,x2 be set such that
A7: x1 in dom h and
A8: x2 in dom h and
A9: h.x1 = h.x2;
A10: h.x1 = f.(g.x1) by A7,FUNCT_1:22;
A11: h.x2 = f.(g.x2) by A8,FUNCT_1:22;
A12: g.x2 in rng g by A4,A8,FUNCT_1:12;
A13: f.(g.x1) = (f|(rng g)).(g.x1) by A4,A7,FUNCT_1:12,72;
A14: f.(g.x2) = (f|(rng g)).(g.x2) by A4,A8,FUNCT_1:12,72;
    dom (f|(rng g)) = rng g by A3,RELAT_1:91;
    then
A15: g.x1 in dom (f|(rng g)) by A4,A7,FUNCT_1:12;
    g.x2 in dom (f|(rng g)) by A3,A12,RELAT_1:91;
    then g.x1 = g.x2 by A2,A9,A10,A11,A13,A14,A15,FUNCT_1:def 8;
    hence thesis by A1,A4,A7,A8,FUNCT_1:def 8;
  end;
  hence thesis by FUNCT_1:def 8;
end;

:: If a function is one-to-one on a set X, then it is one-to-one on
:: any subset of X.

theorem Th2:
  for f being Function, X,Y being set st X c= Y & f|Y is one-to-one
  holds f|X is one-to-one
proof
  let f be Function, X,Y be set such that
A1: X c= Y and
A2: f|Y is one-to-one;
```

```
  f|X = (f|Y)|X by A1,RELAT_1:103;
  hence thesis by A2,FUNCT_1:84;
end;

theorem Th3:
  for V being 1-sorted, X,Y being Subset of V
  holds X meets Y iff ex v being Element of V st v in X & v in Y
proof
  let V be 1-sorted, X,Y be Subset of V;
  X meets Y implies ex v being Element of V st v in X & v in Y
  proof
    assume X meets Y;
    then consider z being set such that
A1: z in X and
A2: z in Y by XBOOLE_0:3;
    reconsider v = z as Element of V by A1;
    take v;
    thus thesis by A1,A2;
  end;
  hence thesis by XBOOLE_0:3;
end;

reserve F for Field,
  V,W for VectSp of F;

registration
  let F be Field, V be finite-dimensional VectSp of F;
  cluster finite Basis of V;
  existence
  proof
    consider A being finite Subset of V such that
A1: A is Basis of V by MATRLIN:def 3;
    reconsider A as Basis of V by A1;
    take A;
    thus thesis;
  end;
end;

registration
  let F be Field, V,W be VectSp of F;
  cluster linear Function of V,W;
  existence
  proof
    set f = FuncZero ([#]V,W);
    reconsider f as Function of V,W;
A1: f is linear
    proof
      thus for x,y being Vector of V holds f.(x+y) = (f.x)+(f.y)
      proof
        let x,y be Vector of V;
A2:     f.(x+y) = 0.W by FUNCOP_1:13;
A3:     f.x = 0.W by FUNCOP_1:13;
        f.y = 0.W by FUNCOP_1:13;
        hence thesis by A2,A3,RLVECT_1:def 7;
      end;
      thus for a being Element of F, x being Element of V
      holds f.(a*x) = a*(f.x)
      proof
        let a be Element of F, x be Element of V;
A4:     f.(a*x) = 0.W by FUNCOP_1:13;
        f.x = 0.W by FUNCOP_1:13;
        hence thesis by A4,VECTSP_1:59;
      end;
    end;
    take f;
    thus thesis by A1;
  end;
end;
```

```
theorem Th4:
  [#]V is finite implies V is finite-dimensional
proof
  assume
A1: [#]V is finite;
  consider B being Basis of V;
  reconsider B as finite Subset of V by A1;
  take B;
  thus thesis;
end;
theorem
  for V being finite-dimensional VectSp of F st card ([#]V) = 1
  holds dim V = 0
proof
  let V be finite-dimensional VectSp of F such that
A1: card ([#]V) = 1;
  [#]V = {0.V}
  proof
    consider y being set such that
A2: [#]V = {y} by A1,CARD_2:60;
    thus thesis by A2,TARSKI:def 1;
  end;
  then (Omega).V = (0).V by VECTSP_4:def 3;
  hence thesis by VECTSP_9:33;
end;
theorem
  card ([#]V) = 2 implies dim V = 1
proof
  assume
A1: card ([#]V) = 2;
A3: [#]V is finite by A1;
  reconsider C = [#]V as finite set by A1;
A4: card ([#]V) = card (C);
  reconsider V as finite-dimensional VectSp of F by A3,Th4;
  ex v being Vector of V st v <> 0.V & (Omega).V = Lin ({v})
  proof
    consider x,y being set such that
A5: x <> y and
A6: [#]V = {x,y} by A1,A4,CARD_2:79;
    per cases by A6,TARSKI:def 2;
    suppose
A7:   x = 0.V;
      reconsider y as Element of V by A6,TARSKI:def 2;
      reconsider x as Element of V by A7;
      set L = Lin ({y});
A8:   for v being Element of V holds v in (Omega).V iff v in L
      proof
        let v be Element of V;
        v in (Omega).V implies v in L
        proof
          assume v in (Omega).V;
A9:       y in {y} by TARSKI:def 1;
A10:      0.L in L by STRUCT_0:def 5;
          per cases by A6,TARSKI:def 2;
          suppose v = x;
            hence thesis by A7,A10,VECTSP_4:def 2;
          end;
          suppose v = y;
            hence thesis by A9,VECTSP_7:13;
          end;
        end;
        hence thesis by STRUCT_0:def 5;
      end;
      take y;
      thus thesis by A5,A7,A8,VECTSP_4:38;
    end;
```

```
    suppose
A11:  y = 0.V;
      then reconsider y as Element of V;
      reconsider x as Element of V by A6,TARSKI:def 2;
      set L = Lin ({x});
A12:  for v being Element of V holds v in (Omega).V iff v in L
      proof
        let v be Element of V;
        v in (Omega).V implies v in L
        proof
          assume v in (Omega).V;
A13:      x in {x} by TARSKI:def 1;
A14:      0.L in L by STRUCT_0:def 5;
          per cases by A6,TARSKI:def 2;
          suppose v = y;
            hence thesis by A11,A14,VECTSP_4:def 2;
          end;
          suppose v = x;
            hence thesis by A13,VECTSP_7:13;
          end;
        end;
        hence thesis by STRUCT_0:def 5;
      end;
      take x;
      thus thesis by A5,A11,A12,VECTSP_4:38;
    end;
  end;
  hence thesis by VECTSP_9:34;
end;

begin :: Basic facts of linear transformations

definition
  let F be Field, V,W be VectSp of F;
  mode linear-transformation of V,W is linear Function of V,W;
end;

reserve T for linear-transformation of V,W;

theorem Th7:
  for V, W being non empty 1-sorted, T being Function of V,W holds
  dom T = [#]V & rng T c= [#]W
proof
  let V, W be non empty 1-sorted, T be Function of V,W;
  T is Element of Funcs([#]V,[#]W) by FUNCT_2:11;
  hence thesis by FUNCT_2:169;
end;

theorem Th8:
  for x,y being Element of V holds T.x - T.y = T.(x - y)
proof
  let x,y be Element of V;
A1: T.(x - y) = T.x + T.(-y) by MOD_2:def 5;
A2: -y = (-1.F)*y by VECTSP_1:59;
  T.((-1.F)*y) = (-1.F)*(T.y) by MOD_2:def 5;
  hence thesis by A1,A2,VECTSP_1:59;
end;

theorem Th9:
  T.(0.V) = 0.W
proof
  0.V = (0.F)*(0.V) by VECTSP_1:59;
  then T.(0.V) = (0.F)*T.(0.V) by MOD_2:def 5
    .= 0.W by VECTSP_1:59;
  hence thesis;
end;

definition
  let F be Field, V,W be VectSp of F, T be linear-transformation of V,W;
  func ker T -> strict Subspace of V means
  :Def1:
  [#]it = { u where u is Element of V : T.u = 0.W };
```

```
  existence
  proof
    set K = { u where u is Element of V : T.u = 0.W };
    K c= [#]V
    proof
      let x be set such that
A1:   x in K;
      consider u being Element of V such that
A2:   u = x and T.u = 0.W by A1;
      thus thesis by A2;
    end;
    then reconsider K as Subset of V;
A3: for v being Element of V st v in K holds T.v = 0.W
    proof
      let v be Element of V such that
A4:   v in K;
      consider u being Element of V such that
A5:   u = v and
A6:   T.u = 0.W by A4;
      thus thesis by A5,A6;
    end;
    K <> {} & K is linearly-closed
    proof
      T.(0.V) = 0.W by Th9;
      then 0.V in K;
      hence K <> {};
      thus K is linearly-closed
      proof
A7:     now
          let u,v be Element of V such that
A8:       u in K and
A9:       v in K;
A10:      T.u = 0.W by A3,A8;
          T.v = 0.W by A3,A9;
          then T.(u+v) = 0.W + 0.W by A10,MOD_2:def 5
            .= 0.W by RLVECT_1:def 7;
          hence u+v in K;
        end;
        now
          let u be Element of V, a be Element of F such that
A11:      u in K;
          T.u = 0.W by A3,A11;
          then T.(a*u) = a*(0.W) by MOD_2:def 5
            .= 0.W by VECTSP_1:59;
          hence a*u in K;
        end;
        then for a being Element of F, u being Element of V st u in K
        holds a*u in K;
        hence thesis by A7,VECTSP_4:def 1;
      end;
    end;
    then consider W being strict Subspace of V such that
A12: K = the carrier of W by VECTSP_4:42;
    take W;
    thus thesis by A12;
  end;
  uniqueness by VECTSP_4:37;
end;

theorem Th10:
  for x being Element of V holds x in ker T iff T.x = 0.W
proof
  let x be Element of V;
  thus x in ker T implies T.x = 0.W
  proof
    assume x in ker T;
    then
```

```
A1: x in [#]ker T by STRUCT_0:def 5;
    [#]ker T = { u where u is Element of V : T.u = 0.W } by Def1;
    then consider u being Element of V such that
A2: u = x and
A3: T.u = 0.W by A1;
    thus thesis by A2,A3;
  end;
  assume T.x = 0.W;
  then x in { u where u is Element of V : T.u = 0.W };
  then x in [#]ker T by Def1;
  hence thesis by STRUCT_0:def 5;
end;
definition
  let V,W be non empty 1-sorted, T be Function of V,W, X be Subset of V;
  redefine func T .: X -> Subset of W;
  coherence
  proof
A1: rng T c= [#]W by Th7;
    T .: X c= rng T by RELAT_1:144;
    hence thesis by A1,XBOOLE_1:1;
  end;
end;
definition
  let F be Field, V,W be VectSp of F, T be linear-transformation of V,W;
  func im T -> strict Subspace of W means
  :Def2:
  [#]it = T .: [#]V;
  existence
  proof
    reconsider U = T .: [#]V as Subset of W;
A1: for u being Element of W holds
    u in U iff ex v being Element of V st T.v = u
    proof
      let u be Element of W;
      thus u in U implies ex v being Element of V st T.v = u
      proof
        assume u in U;
        then consider x being set such that x in dom T and
A2:     x in [#]V and
A3:     u = T.x by FUNCT_1:def 12;
        reconsider x as Element of V by A2;
        take x;
        thus thesis by A3;
      end;
      thus (ex v being Element of V st T.v = u) implies u in U
      proof
        given v being Element of V such that
A4:     T.v = u;
        v in [#]V;
        then v in dom T by Th7;
        hence thesis by A4,FUNCT_1:def 12;
      end;
    end;
    U <> {} & U is linearly-closed
    proof
      thus U <> {}
      proof
        T.(0.V) = 0.W by Th9;
        hence thesis by A1;
      end;
      thus U is linearly-closed
      proof
A5:     now
          let u,v be Element of W such that
A6:       u in U and
A7:       v in U;
```

```
          consider x being Element of V such that
A8:       T.x = u by A1,A6;
          consider y being Element of V such that
A9:       T.y = v by A1,A7;
          u+v = T.(x+y) by A8,A9,MOD_2:def 5;
          hence u+v in U by A1;
        end;
        now
          let a be Element of F, w be Element of W such that
A10:      w in U;
          consider v being Element of V such that
A11:      T.v = w by A1,A10;
          T.(a*v) = a*w by A11,MOD_2:def 5;
          hence a*w in U by A1;
        end;
        hence thesis by A5,VECTSP_4:def 1;
      end;
    end;
    then consider A being strict Subspace of W such that
A12: U = the carrier of A by VECTSP_4:42;
    take A;
    thus thesis by A12;
  end;
  uniqueness by VECTSP_4:37;
end;
theorem
  0.V in ker T
proof
  T.(0.V) = 0.W
  proof
    0.V = (0.F)*(0.V) by VECTSP_1:59;
    then T.(0.V) = (0.F)*T.(0.V) by MOD_2:def 5
      .= 0.W by VECTSP_1:59;
    hence thesis;
  end;
  hence thesis by Th10;
end;
theorem Th12:
  for X being Subset of V holds T .: X is Subset of im T
proof
  let X be Subset of V;
  [#](im T) = T .: [#]V by Def2;
  hence thesis by RELAT_1:156;
end;
theorem Th13:
  for y being Element of W
  holds y in im T iff ex x being Element of V st y = T.x
proof
  let y be Element of W;
A1: y in im T implies ex x being Element of V st y = T.x
  proof
    assume y in im T;
    then reconsider y as Element of im T by STRUCT_0:def 5;
    [#](im T) = T .: [#]V by Def2;
    then consider x being set such that x in dom T and
A2: x in [#]V and
A3: y = T.x by FUNCT_1:def 12;
    reconsider x as Element of V by A2;
    take x;
    thus thesis by A3;
  end;
  (ex x being Element of V st y = T.x) implies y in im T
  proof
    assume ex x being Element of V st y = T.x;
    then consider x being Element of V such that
A4: y = T.x;
```

```
    dom T = [#]V by Th7;
    then y in T .: [#]V by A4,FUNCT_1:def 12;
    then y in [#](im T) by Def2;
    hence thesis by STRUCT_0:def 5;
  end;
  hence thesis by A1;
end;

theorem
  for x being Element of ker T holds T.x = 0.W
proof
  let x be Element of ker T;
  reconsider y = x as Element of V by VECTSP_4:18;
  y in ker T by STRUCT_0:def 5;
  hence thesis by Th10;
end;

theorem Th15:
  T is one-to-one implies ker T = (0).V
proof
  assume
A1: T is one-to-one;
  reconsider Z = (0).V as Subspace of ker T by VECTSP_4:50;
  for v being Element of ker T holds v in Z
  proof
    let v be Element of ker T;
    assume
A2: not v in Z;
A3: T.(0.V) = 0.W by Th9;
A4: not v = 0.V by A2,VECTSP_4:46;
A5: v in ker T by STRUCT_0:def 5;
    reconsider v as Element of V by VECTSP_4:18;
A6: T.v = 0.W by A5,Th10;
    dom T = [#]V by Th7;
    hence thesis by A1,A3,A4,A6,FUNCT_1:def 8;
  end;
  hence thesis by VECTSP_4:40;
end;

theorem Th16:
  for V being finite-dimensional VectSp of F holds dim ((0).V) = 0
proof
  let V be finite-dimensional VectSp of F;
  (Omega).((0).V) = (0).((0).V) by VECTSP_4:47;
  hence thesis by VECTSP_9:33;
end;

theorem Th17:
  for x,y being Element of V st T.x = T.y holds x - y in ker T
proof
  let x,y be Element of V such that
A1: T.x = T.y;
  T.(x - y) = T.x - T.y by Th8
    .= 0.W by A1,VECTSP_1:66;
  hence thesis by Th10;
end;

theorem Th18:
  for A being Subset of V, x,y being Element of V st x - y in Lin A
  holds x in Lin (A \/ {y})
proof
  let A be Subset of V, x,y be Element of V such that
A1: x - y in Lin A;
  y in {y} by TARSKI:def 1;
  then
A2: y in Lin ({y}) by VECTSP_7:13;
A3: (x - y) + y = x - (y - y) by RLVECT_1:43
    .= x - 0.V by VECTSP_1:66
    .= x by RLVECT_1:26;
  Lin (A \/ {y}) = (Lin A) + (Lin {y}) by VECTSP_7:20;
```

```
  hence thesis by A1,A2,A3,VECTSP_5:5;
end;

begin :: Some basic facts about linearly independent subsets and linear
      :: combinations

theorem Th19:
  for X being Subset of V st V is Subspace of W holds X is Subset of W
proof
  let X be Subset of V;
  assume V is Subspace of W;
  then
A1: [#]V c= [#]W by VECTSP_4:def 2;
  X c= [#]W
  proof
    let x be set such that
A2: x in X;
    x in [#]V by A2;
    hence thesis by A1;
  end;
  hence thesis;
end;

:: A linearly independent set is a basis of its linear span.

theorem Th20:
  for A being Subset of V st A is linearly-independent
  holds A is Basis of Lin A
proof
  let A be Subset of V such that
A1: A is linearly-independent;
  A c= [#](Lin A)
  proof
    let x be set such that
A2: x in A;
    reconsider x as Element of V by A2;
    x in Lin A by A2,VECTSP_7:13;
    hence thesis by STRUCT_0:def 5;
  end;
  then reconsider B = A as Subset of Lin A;
A3: B is linearly-independent by A1,VECTSP_9:16;
  Lin B = Lin A by VECTSP_9:21;
  hence thesis by A3,VECTSP_7:def 3;
end;

:: Adjoining an element x to A that is already in its linear span
:: results in a linearly dependent set.

theorem Th21:
  for A being Subset of V, x being Element of V st x in Lin A & not x in A
  holds A \/ {x} is linearly-dependent
proof
  let A be Subset of V, x be Element of V such that
A1: x in Lin A and
A2: not x in A;
  per cases;
  suppose A is linearly-independent;
    then reconsider A' = A as Basis of Lin A by Th20;
    x in [#](Lin A) by A1,STRUCT_0:def 5;
    then reconsider X = {x} as Subset of Lin A by SUBSET_1:63;
A3: X misses A'
    proof
      assume X meets A';
      then consider y being set such that
A4:   y in X and
A5:   y in A' by XBOOLE_0:3;
      thus contradiction by A2,A4,A5,TARSKI:def 1;
    end;
    reconsider B = A' \/ X as Subset of Lin A;
A6: B is linearly-dependent by A3,VECTSP_9:19;
    thus thesis by A6,VECTSP_9:16;
```

```
  end;
  suppose
A7: A is linearly-dependent;
    thus thesis by A7,VECTSP_7:2,XBOOLE_1:7;
  end;
end;

theorem Th22:
  for A being Subset of V, B being Basis of V st A is Basis of ker T & A c= B
  holds T|(B \ A) is one-to-one
proof
  let A be Subset of V, B be Basis of V such that
A1: A is Basis of ker T and
A2: A c= B;
  set f = T|(B \ A);
  let x1,x2 be set such that
A3: x1 in dom f and
A4: x2 in dom f and
A5: f.x1 = f.x2 and
A6: x1 <> x2;
A7: dom T = [#]V by Th7;
  reconsider x1 as Element of V by A3;
  reconsider x2 as Element of V by A4;
  reconsider A' = A as Subset of V;
A8: x1 in B \ A by A3,A7,RELAT_1:91;
A9: x2 in B \ A by A4,A7,RELAT_1:91;
A10: f.x1 = T.x1 by A8,FUNCT_1:72;
  f.x2 = T.x2 by A9,FUNCT_1:72;
  then
A11: x1 - x2 in ker T by A5,A10,Th17;
  reconsider A as Basis of ker T by A1;
  ker T = Lin A by VECTSP_7:def 3;
  then x1 - x2 in Lin A' by A11,VECTSP_9:21;
  then
A12: x1 in Lin (A' \/ {x2}) by Th18;
A13: (A' \/ {x2}) \/ {x1} = A' \/ {x1,x2}
  proof
    {x2} \/ {x1} = {x1,x2} by ENUMSET1:41;
    hence thesis by XBOOLE_1:4;
  end;
A14: not x1 in (A' \/ {x2})
  proof
    assume
A15: x1 in A' \/ {x2};
    per cases by A15,XBOOLE_0:def 3;
    suppose x1 in A';
      hence contradiction by A8,XBOOLE_0:def 5;
    end;
    suppose x1 in {x2};
      hence contradiction by A6,TARSKI:def 1;
    end;
  end;
A16: A' \/ {x1,x2} c= B
  proof
    {x1,x2} c= B
    proof
      let z be set such that
A17:  z in {x1,x2};
      per cases by A17,TARSKI:def 2;
      suppose z = x1;
        hence thesis by A8,XBOOLE_0:def 5;
      end;
      suppose z = x2;
        hence thesis by A9,XBOOLE_0:def 5;
      end;
    end;
    hence thesis by A2,XBOOLE_1:8;
```

```
  end;
  B is linearly-independent by VECTSP_7:def 3;
  hence thesis by A12,A13,A14,A16,Th21,VECTSP_7:2;
end;
theorem
  for A being Subset of V, l being Linear_Combination of A,
  x being Element of V, a being Element of F
  holds l ++* (x,a) is Linear_Combination of A \/ {x}
proof
  let A be Subset of V, l be Linear_Combination of A, x be Element of V,
  a be Element of F;
  set m = l ++* (x,a);
  m is Element of Funcs ([#]V,[#]F)
  proof
A1: dom m = [#]V
    proof
A2:   dom l = [#]V by FUNCT_2:169;
      then
A3:   m = l +* (x .--> a) by FUNCT_7:def 3;
A4:   dom (x .--> a) = {x} by FUNCOP_1:19;
      dom m = (dom l) \/ (dom (x .--> a)) by A3,FUNCT_4:def 1;
      hence thesis by A2,A4,XBOOLE_1:12;
    end;
    rng m c= [#]F
    proof
      let y be set such that
A5:   y in rng m;
      consider x' being set such that
A6:   x' in dom m and
A7:   m.x' = y by A5,FUNCT_1:def 5;
A8:   x' in dom l by A1,A6,FUNCT_2:169;
      per cases;
      suppose x' = x;
        then m.x' = a by A8,FUNCT_7:33;
        hence thesis by A7;
      end;
      suppose x' <> x;
        then
A9:     m.x' = l.x' by FUNCT_7:34;
A10:    l.x' in rng l by A8,FUNCT_1:12;
        rng l c= [#]F by FUNCT_2:169;
        hence thesis by A7,A9,A10;
      end;
    end;
    hence thesis by A1,FUNCT_2:def 2;
  end;
  then reconsider m as Element of Funcs ([#]V,[#]F);
  set T = Carrier l \/ {x};
  for v being Element of V st not v in T holds m.v = 0.F
  proof
    let v be Element of V such that
A11: not v in T;
A12: not v in Carrier l by A11,XBOOLE_0:def 3;
    not v in {x} by A11,XBOOLE_0:def 3;
    then v <> x by TARSKI:def 1;
    then m.v = l.v by FUNCT_7:34;
    hence thesis by A12;
  end;
  then reconsider m as Linear_Combination of V by VECTSP_6:def 4;
A13: Carrier m c= T
  proof
    let y be set such that
A14: y in Carrier m;
    consider z being Element of V such that
A15: y = z and
A16: m.z <> 0.F by A14;
```

```
    per cases;
    suppose
A17:  z = x;
A18:  x in {x} by TARSKI:def 1;
      {x} c= T by XBOOLE_1:7;
      hence thesis by A15,A17,A18;
    end;
    suppose z <> x;
      then m.z = l.z by FUNCT_7:34;
      then
A19:  z in Carrier l by A16;
      Carrier l c= T by XBOOLE_1:7;
      hence thesis by A15,A19;
    end;
  end;
  T c= A \/ {x}
  proof
    Carrier l c= A by VECTSP_6:def 7;
    hence thesis by XBOOLE_1:9;
  end;
  then Carrier m c= A \/ {x} by A13,XBOOLE_1:1;
  hence thesis by VECTSP_6:def 7;
end;
definition
  let V be 1-sorted, X be Subset of V;
  func V \ X -> Subset of V equals
  [#]V \ X;
  coherence;
end;
definition
  let F be Field, V be VectSp of F, l be Linear_Combination of V,
  X be Subset of V;
  redefine func l .: X -> Subset of F;
  coherence
  proof
    l .: X c= [#]F;
    hence thesis;
  end;
end;
reserve l for Linear_Combination of V;
registration
  let F be Field, V be VectSp of F;
  cluster linearly-dependent Subset of V;
  existence
  proof
    reconsider S = {0.V} as Subset of V;
A1: 0.V in S by TARSKI:def 1;
    take S;
    thus thesis by A1,VECTSP_7:3;
  end;
end;
:: Restricting a linear combination to a given set
definition
  let F be Field, V be VectSp of F, l be Linear_Combination of V,
  A be Subset of V;
  func l!A -> Linear_Combination of A equals
  (l|A) +* ((V \ A) --> 0.F);
  coherence
  proof
    set f = (l|A) +* ((V \ A) --> 0.F);
A1: dom f = dom (l|A) \/ dom ((V \ A) --> 0.F) by FUNCT_4:def 1;
    dom l = [#]V by FUNCT_2:169;
    then
A2: dom (l|A) = A by RELAT_1:91;
A3: dom ((V \ A) --> 0.F) = V \ A by FUNCOP_1:19;
```

```
A4: A \/ ([#]V \ A) = [#]V by XBOOLE_1:45;
A5: dom f = [#]V by A1,A2,A3,XBOOLE_1:45;
    rng f c= [#]F
    proof
      let y be set such that
A6:   y in rng f;
      consider x being set such that
A7:   x in dom f and
A8:   y = f.x by A6,FUNCT_1:def 5;
      reconsider x as Element of V by A1,A2,A3,A7,XBOOLE_1:45;
      per cases by A4,XBOOLE_0:def 3;
      suppose
A9:     x in A;
        then not x in dom ((V \ A) --> 0.F) by XBOOLE_0:def 5;
        then
A10:    f.x = (l|A).x by FUNCT_4:12;
        (l|A).x = l.x by A9,FUNCT_1:72;
        hence thesis by A8,A10;
      end;
      suppose
A11:    x in V \ A;
        then x in dom ((V \ A) --> 0.F) by FUNCOP_1:19;
        then f.x = ((V \ A) --> 0.F).x by FUNCT_4:14
          .= 0.F by A11,FUNCOP_1:13;
        hence thesis by A8;
      end;
    end;
    then reconsider f as Element of Funcs([#]V,[#]F) by A5,FUNCT_2:def 2;
    ex T being finite Subset of V st
    for v being Element of V st not v in T holds f.v = 0.F
    proof
      set C = Carrier l;
      set D = { v where v is Element of V : f.v <> 0.F };
      D is Subset of V
      proof
        D c= [#]V
        proof
          let x be set such that
A12:      x in D;
          consider v being Element of V such that
A13:      x = v and f.v <> 0.F by A12;
          thus thesis by A13;
        end;
        hence thesis;
      end;
      then reconsider D as Subset of V;
      D c= C
      proof
        let x be set such that
A14:    x in D;
        consider v being Element of V such that
A15:    x = v and
A16:    f.v <> 0.F by A14;
A17:    dom ((V \ A) --> 0.F) = V \ A by FUNCOP_1:19;
A18:    now
          assume
A19:      v in V \ A;
          then f.v = ((V \ A) --> 0.F).v by A1,A5,A17,FUNCT_4:def 1
            .= 0.F by A19,FUNCOP_1:13;
          hence contradiction by A16;
        end;
        then not v in dom ((V \ A) --> 0.F);
        then
A20:    f.v = (l|A).v by FUNCT_4:12;
        v in A by A18,XBOOLE_0:def 5;
        then (l|A).v = l.v by FUNCT_1:72;
```

```
        hence thesis by A15,A16,A20;
      end;
      then reconsider D as finite Subset of V;
      take D;
      thus thesis;
    end;
    then reconsider f as Linear_Combination of V by VECTSP_6:def 4;
    Carrier f c= A
    proof
      let x be set such that
A21:  x in Carrier f;
      reconsider x as Element of V by A21;
A22:  f.x <> 0.F by A21,VECTSP_6:20;
      now
        assume not x in A;
        then
A23:    x in V \ A by XBOOLE_0:def 5;
        then x in dom (l|A) \/ (dom ((V \ A) --> 0.F)) by A3,XBOOLE_0:def 3;
        then f.x = ((V \ A) --> 0.F).x by A3,A23,FUNCT_4:def 1;
        hence contradiction by A22,A23,FUNCOP_1:13;
      end;
      hence thesis;
    end;
    hence thesis by VECTSP_6:def 7;
  end;
end;
theorem Th24:
  l = l!Carrier l
proof
  set f = l|(Carrier l);
  set g = (V \ Carrier l) --> 0.F;
  set m = f +* g;
A1: dom l = [#]V by FUNCT_2:169;
  then
A2: dom f = Carrier l by RELAT_1:91;
A3: dom g = V \ (Carrier l) by FUNCOP_1:19;
  then
A4: (dom f) \/ (dom g) = [#]V by A2,XBOOLE_1:45;
  then
A5: dom l = dom m by A1,FUNCT_4:def 1;
  for x being set st x in dom l holds l.x = m.x
  proof
    let x be set such that
A6: x in dom l;
    reconsider x as Element of V by A6;
    per cases;
    suppose
A7:   x in Carrier l;
      then not x in dom g by XBOOLE_0:def 5;
      then m.x = f.x by A4,FUNCT_4:def 1;
      hence thesis by A7,FUNCT_1:72;
    end;
    suppose
A8:   not x in Carrier l;
      then
A9:   x in V \ (Carrier l) by XBOOLE_0:def 5;
      then
A10:  m.x = g.x by A3,A4,FUNCT_4:def 1;
      g.x = 0.F by A9,FUNCOP_1:13;
      hence thesis by A8,A10;
    end;
  end;
  hence thesis by A5,FUNCT_1:def 17;
end;
```

```
Lm1: for X being Subset of V holds l .: X is finite
proof
  let X be Subset of V;
A1: l = l!(Carrier l) by Th24;
A2: rng (l|Carrier l) is finite
  proof
    rng (l|Carrier l) = l .: Carrier l by RELAT_1:148;
    hence thesis;
  end;
  rng ((V \ (Carrier l)) --> 0.F) c= {0.F}
  proof
    set f = ((V \ (Carrier l)) --> 0.F);
    per cases;
    suppose V \ (Carrier l) = {};
      then f = {};
      hence thesis by RELAT_1:60,XBOOLE_1:2;
    end;
    suppose V \ (Carrier l) <> {};
      hence thesis by FUNCOP_1:14;
    end;
  end;
  then rng ((V \ (Carrier l)) --> 0.F) is finite;
  then (rng (l|Carrier l)) \/ rng ((V \ (Carrier l)) --> 0.F) is finite
  by A2;
  then rng l is finite by A1,FINSET_1:13,FUNCT_4:18;
  hence thesis by FINSET_1:13,RELAT_1:144;
end;
theorem Th25:
  for A being Subset of V, v being Element of V st v in A holds (l!A).v = l.v
proof
  let A be Subset of V, v be Element of V such that
A1: v in A;
  not v in V \ A by A1,XBOOLE_0:def 5;
  then
A2: not v in dom ((V \ A) --> 0.F);
  dom (l!A) = [#]V by FUNCT_2:169;
  then (dom (l|A)) \/ (dom ((V \ A) --> 0.F)) = [#]V by FUNCT_4:def 1;
  then (l!A).v = (l|A).v by A2,FUNCT_4:def 1
    .= l.v by A1,FUNCT_1:72;
  hence thesis;
end;
theorem Th26:
  for A being Subset of V, v being Element of V st not v in A
  holds (l!A).v = 0.F
proof
  let A be Subset of V, v be Element of V such that
A1: not v in A;
A2: dom ((V \ A) --> 0.F) = V \ A by FUNCOP_1:19;
A3: dom (l!A) = (dom (l|A)) \/ (dom ((V \ A) --> 0.F)) by FUNCT_4:def 1;
A4: dom (l!A) = [#]V by FUNCT_2:169;
A5: v in V \ A by A1,XBOOLE_0:def 5;
  then (l!A).v = ((V \ A) --> 0.F).v by A2,A3,A4,FUNCT_4:def 1
    .= 0.F by A5,FUNCOP_1:13;
  hence thesis;
end;
theorem Th27:
  for A,B being Subset of V, l being Linear_Combination of B st A c= B
  holds l = (l!A) + (l!(B\A))
proof
  let A,B be Subset of V, l be Linear_Combination of B such that
A1: A c= B;
  set r = (l!A) + (l!(B\A));
  let v be Element of V;
A2: (v in B) implies (v in A or v in B \ A)
  proof
    assume
```

```
A3: v in B;
    B = A \/ (B \ A) by A1,XBOOLE_1:45;
    hence thesis by A3,XBOOLE_0:def 3;
  end;
  per cases by A2;
  suppose
A4: v in A;
    then not v in B \ A by XBOOLE_0:def 5;
    then
A5: (l!(B\A)).v = 0.F by Th26;
    (l!A).v = l.v by A4,Th25;
    then r.v = l.v + 0.F by A5,VECTSP_6:def 11
      .= l.v by RLVECT_1:10;
    hence l.v = r.v;
  end;
  suppose
A6: v in B\A;
    then not v in A by XBOOLE_0:def 5;
    then
A7: (l!A).v = 0.F by Th26;
    (l!(B\A)).v = l.v by A6,Th25;
    then r.v = 0.F + l.v by A7,VECTSP_6:def 11
      .= l.v by RLVECT_1:10;
    hence l.v = r.v;
  end;
  suppose
A8: not v in B;
    then
A9: not v in B\A by XBOOLE_0:def 5;
    not v in A by A1,A8;
    then
A10: (l!A).v = 0.F by Th26;
A11: (l!(B\A)).v = 0.F by A9,Th26;
    Carrier l c= B by VECTSP_6:def 7;
    then
A12: not v in Carrier l by A8;
    r.v = 0.F + 0.F by A10,A11,VECTSP_6:def 11
      .= 0.F by RLVECT_1:10;
    hence l.v = r.v by A12;
  end;
end;

registration
  let F be Field, V be VectSp of F, l be Linear_Combination of V,
  X be Subset of V;
  cluster l .: X -> finite;
  coherence by Lm1;
end;

definition
  let V,W be non empty 1-sorted, T be Function of V,W, X be Subset of W;
  redefine func T"X -> Subset of V;
  coherence
  proof
    dom T = [#]V by Th7;
    hence thesis by RELAT_1:167;
  end;
end;

theorem Th28:
  for X being Subset of V st X misses Carrier l holds l .: X c= {0.F}
proof
  let X be Subset of V such that
A1: X misses Carrier l;
  set M = l .: X;
  let y be set such that
A2: y in M;
  consider x being set such that
A3: x in dom l and
```

```
A4: x in X and
A5: y = l.x by A2,FUNCT_1:def 12;
  reconsider x as Element of V by A3;
  now
    assume l.x <> 0.F;
    then x in Carrier l;
    then x in (Carrier l) /\ X by A4,XBOOLE_0:def 4;
    hence contradiction by A1,XBOOLE_0:def 7;
  end;
  hence thesis by A5,TARSKI:def 1;
end;
:: The image of a linear combination under a linear transformation:
::
::   T(a1*v1 + a2*v2 + ... + an*vn)
::     =  a1*T(v1) + a2*T(v2) + ... + an*T(vn).
::
:: Linear combinations are represented as functions from the space to
:: the underlying field having finite support, so to define a new
:: linear combination it is enough to say what its values are for the
:: elements of W and to prove that its support is finite.
::
:: The only difficulty is that some values T(vi) and T(vj) may be
:: equal.  In this case, the new linear combination should be the sum
:: of the coefficients ai and aj, i.e., l(vi) and l(vj).
definition
  let F be Field, V,W be VectSp of F, l be Linear_Combination of V,
  T be linear-transformation of V,W;
  func T@l -> Linear_Combination of W means
  :Def5:
  for w being Element of W holds it.w = Sum (l .: (T"{w}));
  existence
  proof
    defpred P[set,set] means
    ex w being Element of W st $1 = w & $2 = Sum (l .: (T"{w}));
A2: for x being set st x in [#]W holds ex y being set st P[x,y]
    proof
      let x be set such that
A3:   x in [#]W;
      reconsider x as Element of W by A3;
      take Sum (l .: (T"{x}));
      thus thesis;
    end;
    consider f being Function such that
A4: dom f = [#]W and
A5: for x being set st x in [#]W holds P[x,f.x] from CLASSES1:sch 1(A2);
A6: for w being Element of W holds f.w = Sum (l .: (T"{w}))
    proof
      let w be Element of W;
      consider w' being Element of W such that
A7:   w = w' and
A8:   f.w = Sum (l .: (T"{w'})) by A5;
      thus thesis by A7,A8;
    end;
    rng f c= [#]F
    proof
      let y be set such that
A9:   y in rng f;
      consider x being set such that
A10:  x in dom f and
A11:  f.x = y by A9,FUNCT_1:def 5;
      consider w being Element of W such that x = w and
A12:  f.x = Sum (l .: (T"{w})) by A4,A5,A10;
      thus thesis by A11,A12;
    end;
    then reconsider f as Element of Funcs([#]W,[#]F) by A4,FUNCT_2:def 2;
    ex T being finite Subset of W
```

```
    st for w being Element of W st not w in T holds f.w = 0.F
    proof
      set C = Carrier l;
      reconsider TC = T .: C as Subset of W;
      set X = { w where w is Element of W : f.w <> 0.F };
      X is Subset of W
      proof
        X c= [#]W
        proof
          let x be set such that
A13:      x in X;
          consider w being Element of W such that
A14:      x = w and f.w <> 0.F by A13;
          thus thesis by A14;
        end;
        hence thesis;
      end;
      then reconsider X as Subset of W;
      X c= TC
      proof
        let x be set such that
A15:    x in X;
        consider w being Element of W such that
A16:    x = w and
A17:    f.w <> 0.F by A15;
        T"{w} meets Carrier l
        proof
          assume
A18:      T"{w} misses Carrier l;
          then
A19:      l .: T"{w} c= {0.F} by Th28;
          Sum (l .: T"{w}) = 0.F
          proof
            per cases;
            suppose l .: T"{w} = {}F;
              hence thesis by RLVECT_2:14;
            end;
            suppose
A20:          l .: T"{w} <> {}F;
              l .: T"{w} = {0.F}
              proof
                thus l .: T"{w} c= {0.F} by A18,Th28;
                thus {0.F} c= l .: T"{w}
                proof
                  let y be set such that
A21:              y in {0.F};
A22:              y = 0.F by A21,TARSKI:def 1;
                  consider z being set such that
A23:              z in l .: T"{w} by A20,XBOOLE_0:def 1;
                  thus thesis by A19,A22,A23,TARSKI:def 1;
                end;
              end;
              hence thesis by RLVECT_2:15;
            end;
          end;
          hence contradiction by A6,A17;
        end;
        then consider y being set such that
A24:    y in T"{w} and
A25:    y in Carrier l by XBOOLE_0:3;
        reconsider y as Element of V by A25;
A26:    dom T = [#]V by Th7;
        T.y in {w} by A24,FUNCT_1:def 13;
        then T.y = w by TARSKI:def 1;
        hence thesis by A16,A25,A26,FUNCT_1:def 12;
      end;
```

```
      then reconsider X as finite Subset of W;
      take X;
      thus thesis;
    end;
    then reconsider f as Linear_Combination of W by VECTSP_6:def 4;
A27: for w being Element of W holds f.w = Sum (l .: (T"{w}))
    proof
      let w be Element of W;
      consider w' being Element of W such that
A28:  w = w' and
A29:  f.w = Sum (l .: (T"{w'})) by A5;
      thus thesis by A28,A29;
    end;
    take f;
    thus thesis by A27;
  end;
  uniqueness
  proof
    let f,g be Linear_Combination of W such that
A30: for w being Element of W holds f.w = Sum (l .: (T"{w})) and
A31: for w being Element of W holds g.w = Sum (l .: (T"{w}));
A32: dom f = [#]W by FUNCT_2:169;
A33: dom g = [#]W by FUNCT_2:169;
    for x being set st x in dom f holds f.x = g.x
    proof
      let x be set such that
A34:  x in dom f;
      reconsider x as Element of W by A34;
      f.x = Sum (l .: (T"{x})) by A30;
      hence thesis by A31;
    end;
    hence thesis by A32,A33,FUNCT_1:def 17;
  end;
end;

theorem Th29:
  T@l is Linear_Combination of T .: (Carrier l)
proof
  Carrier (T@l) c= T .: (Carrier l)
  proof
    let w be set such that
A1: w in Carrier (T@l);
    reconsider w as Element of W by A1;
A2: (T@l).w <> 0.F by A1,VECTSP_6:20;
    now
      assume
A3:   T"{w} misses Carrier l;
      then
A4:   l .: T"{w} c= {0.F} by Th28;
      Sum (l .: T"{w}) = 0.F
      proof
        per cases;
        suppose l .: T"{w} = {}F;
          hence thesis by RLVECT_2:14;
        end;
        suppose
A5:       l .: T"{w} <> {}F;
          l .: T"{w} = {0.F}
          proof
            thus l .: T"{w} c= {0.F} by A3,Th28;
            thus {0.F} c= l .: T"{w}
            proof
              let y be set such that
A6:           y in {0.F};
A7:           y = 0.F by A6,TARSKI:def 1;
              consider z being set such that
A8:           z in l .: T"{w} by A5,XBOOLE_0:def 1;
```

```
              thus thesis by A4,A7,A8,TARSKI:def 1;
            end;
          end;
          hence thesis by RLVECT_2:15;
        end;
      end;
      hence contradiction by A2,Def5;
    end;
    then consider x being set such that
A9: x in T"{w} and
A10: x in Carrier l by XBOOLE_0:3;
A11: x in dom T by A9,FUNCT_1:def 13;
A12: T.x in {w} by A9,FUNCT_1:def 13;
    reconsider x as Element of V by A9;
    T.x = w by A12,TARSKI:def 1;
    hence thesis by A10,A11,FUNCT_1:def 12;
  end;
  hence thesis by VECTSP_6:def 7;
end;

theorem Th30:
  Carrier (T@l) c= T .: (Carrier l)
proof
  T@l is Linear_Combination of T .: (Carrier l) by Th29;
  hence thesis by VECTSP_6:def 7;
end;

theorem Th31:
  for l,m being Linear_Combination of V st (Carrier l) misses (Carrier m)
  holds Carrier (l + m) = (Carrier l) \/ (Carrier m)
proof
  let l,m be Linear_Combination of V such that
A1: (Carrier l) misses (Carrier m);
  thus Carrier (l+m) c= (Carrier l) \/ (Carrier m) by VECTSP_6:51;
  thus (Carrier l) \/ (Carrier m) c= Carrier (l+m)
  proof
    let v be set such that
A2: v in (Carrier l) \/ (Carrier m);
    per cases by A2,XBOOLE_0:def 3;
    suppose
A3:   v in Carrier l;
      then reconsider v as Element of V;
A4:   (l+m).v = (l.v) + (m.v) by VECTSP_6:def 11;
A5:   l.v <> 0.F by A3,VECTSP_6:20;
      not v in Carrier m by A1,A2,A3,XBOOLE_0:5;
      then m.v = 0.F;
      then (l+m).v = l.v by A4,RLVECT_1:10;
      hence thesis by A5;
    end;
    suppose
A6:   v in Carrier m;
      then reconsider v as Element of V;
A7:   (l+m).v = (l.v) + (m.v) by VECTSP_6:def 11;
A8:   m.v <> 0.F by A6,VECTSP_6:20;
      not v in Carrier l by A1,A2,A6,XBOOLE_0:5;
      then l.v = 0.F;
      then (l+m).v = m.v by A7,RLVECT_1:10;
      hence thesis by A8;
    end;
  end;
end;

theorem Th32:
  for l,m being Linear_Combination of V st (Carrier l) misses (Carrier m)
  holds Carrier (l - m) = (Carrier l) \/ (Carrier m)
proof
  let l,m be Linear_Combination of V such that
A1: (Carrier l) misses (Carrier m);
  Carrier (-m) = Carrier m by VECTSP_6:69;
```

```
  hence thesis by A1,Th31;
end;

theorem Th33:
  for A,B being Subset of V st A c= B & B is Basis of V
  holds V is_the_direct_sum_of Lin A, Lin (B \ A)
proof
  let A,B be Subset of V such that
A1: A c= B and
A2: B is Basis of V;
A3: (Omega).V = (Lin A) + (Lin (B \ A))
  proof
    set U = (Lin A) + (Lin (B \ A));
    [#]U = [#]V
    proof
      thus [#]U c= [#]V by VECTSP_4:def 2;
      thus [#]V c= [#]U
      proof
        let v be set such that
A4:     v in [#]V;
        reconsider v as Element of V by A4;
        v in Lin B by A2,VECTSP_9:14;
        then consider l being Linear_Combination of B such that
A5:     v = Sum l by VECTSP_7:12;
        set m = l!A;
        set n = l!(B\A);
A6:     l = m + n by A1,Th27;
        ex v1,v2 being Element of V
        st v1 in Lin A & v2 in Lin (B \ A) & v = v1 + v2
        proof
          take Sum m, Sum n;
          thus thesis by A5,A6,VECTSP_6:77,VECTSP_7:12;
        end;
        then v in (Lin A) + (Lin (B \ A)) by VECTSP_5:5;
        hence thesis by STRUCT_0:def 5;
      end;
    end;
    hence thesis by VECTSP_4:37;
  end;
  (Lin A) /\ (Lin (B \ A)) = (0).V
  proof
    set U = (Lin A) /\ (Lin (B \ A));
    reconsider W = (0).V as strict Subspace of U by VECTSP_4:50;
    for v being Element of U holds v in W
    proof
      let v be Element of U;
A7:   v in U by STRUCT_0:def 5;
      then
A8:   v in Lin A by VECTSP_5:7;
A9:   v in Lin (B \ A) by A7,VECTSP_5:7;
      consider l being Linear_Combination of A such that
A10:  v = Sum l by A8,VECTSP_7:12;
      consider m being Linear_Combination of B \ A such that
A11:  v = Sum m by A9,VECTSP_7:12;
A12:  0.V = (Sum l) - (Sum m) by A10,A11,VECTSP_1:66
        .= Sum (l - m) by VECTSP_6:80;
A13:  Carrier (l - m) c= (Carrier l) \/ (Carrier m) by VECTSP_6:74;
A14:  Carrier l c= A by VECTSP_6:def 7;
A15:  Carrier m c= B \ A by VECTSP_6:def 7;
A16:  A \/ (B \ A) = B by A1,XBOOLE_1:45;
      (Carrier l) \/ (Carrier m) c= A \/ (B \ A) by A14,A15,XBOOLE_1:13;
      then Carrier (l - m) c= B by A13,A16,XBOOLE_1:1;
      then reconsider n = l - m as Linear_Combination of B by VECTSP_6:def 7;
      B is linearly-independent by A2,VECTSP_7:def 3;
      then
A17:  Carrier n = {} by A12,VECTSP_7:def 1;
      A misses (B \ A) by XBOOLE_1:79;
```

```
      then Carrier n = (Carrier l) \/ (Carrier m) by A14,A15,Th32,XBOOLE_1:64;
      then Carrier l = {} by A17;
      then l = ZeroLC(V) by VECTSP_6:def 6;
      then Sum l = 0.V by VECTSP_6:41;
      hence thesis by A10,VECTSP_4:46;
    end;
    hence thesis by VECTSP_4:40;
  end;
  hence thesis by A3,VECTSP_5:def 4;
end;

theorem Th34:
  for A being Subset of V, l being Linear_Combination of A,
  v being Element of V st T|A is one-to-one & v in A
  holds ex X being Subset of V st X misses A & T"{T.v} = {v} \/ X
proof
  let A be Subset of V, l be Linear_Combination of A,
  v be Element of V such that
A1: T|A is one-to-one and
A2: v in A;
  set X = T"{T.v} \ {v};
A3: {v} c= T"{T.v}
  proof
    let x be set such that
A4: x in {v};
A5: x = v by A4,TARSKI:def 1;
A6: dom T = [#]V by Th7;
    T.v in {T.v} by TARSKI:def 1;
    hence thesis by A5,A6,FUNCT_1:def 13;
  end;
A7: X misses A
  proof
    assume X meets A;
    then consider x being set such that
A8: x in X and
A9: x in A by XBOOLE_0:3;
A10: x in T"{T.v} by A8,XBOOLE_0:def 5;
    not x in {v} by A8,XBOOLE_0:def 5;
    then
A11: x <> v by TARSKI:def 1;
    T.x in {T.v} by A10,FUNCT_1:def 13;
    then
A12: T.x = T.v by TARSKI:def 1;
    T.x = (T|A).x by A9,FUNCT_1:72;
    then
A13: (T|A).v = (T|A).x by A2,A12,FUNCT_1:72;
    dom T = [#]V by Th7;
    then dom (T|A) = A by RELAT_1:91;
    hence thesis by A1,A2,A9,A11,A13,FUNCT_1:def 8;
  end;
  take X;
  thus thesis by A3,A7,XBOOLE_1:45;
end;

theorem Th35:
  for X being Subset of V st X misses Carrier l & X <> {} holds l .: X = {0.F}
proof
  let X be Subset of V such that
A1: X misses Carrier l and
A2: X <> {};
A3: l .: X c= {0.F} by A1,Th28;
  dom l = [#]V by FUNCT_2:169;
  then l .: X <> {} by A2,RELAT_1:152;
  hence thesis by A3,ZFMISC_1:39;
end;

theorem Th36:
  for w being Element of W st w in Carrier (T@l) holds T"{w} meets Carrier l
proof
```

```
  let w be Element of W such that
A1: w in Carrier (T@l);
A2: (T@l).w <> 0.F by A1,VECTSP_6:20;
  assume
A3: T"{w} misses Carrier l;
  per cases;
  suppose T"{w} = {};
    then Sum (l .: T"{w}) = Sum ({}F) by RELAT_1:149
      .= 0.F by RLVECT_2:14;
    hence thesis by A2,Def5;
  end;
  suppose T"{w} <> {};
    then l .: T"{w} = {0.F} by A3,Th35;
    then Sum (l .: T"{w}) = 0.F by RLVECT_2:15;
    hence thesis by A2,Def5;
  end;
end;

theorem Th37:
  for v being Element of V st T|(Carrier l) is one-to-one & v in Carrier l
  holds (T@l).(T.v) = l.v
proof
  let v be Element of V such that
A1: T|(Carrier l) is one-to-one and
A2: v in Carrier l;
  consider X being Subset of V such that
A3: X misses Carrier l and
A4: T"{T.v} = {v} \/ X by A1,A2,Th34;
  per cases;
  suppose
A5: X = {};
A6: dom l = [#]V by FUNCT_2:169;
    l .: {v} = Im (l,v)
      .= {l.v} by A6,FUNCT_1:117;
    then Sum (l .: T"{T.v}) = l.v by A4,A5,RLVECT_2:15;
    hence thesis by Def5;
  end;
  suppose
A7: X <> {};
A8: l .: T"{T.v} = (l .: {v}) \/ (l .: X) by A4,RELAT_1:153;
A9: dom l = [#]V by FUNCT_2:169;
A10: l .: {v} = Im (l,v)
      .= {l.v} by A9,FUNCT_1:117;
A11: l .: X = {0.F}
    proof
A12:  {0.F} c= l .: X
      proof
        let x be set such that
A13:    x in {0.F};
A14:    x = 0.F by A13,TARSKI:def 1;
        consider y being set such that
A15:    y in X by A7,XBOOLE_0:def 1;
A16:    now
          assume y in Carrier l;
          then y in (Carrier l) /\ X by A15,XBOOLE_0:def 4;
          hence contradiction by A3,XBOOLE_0:def 7;
        end;
        reconsider y as Element of V by A15;
        l.y = x by A14,A16;
        hence thesis by A9,A15,FUNCT_1:def 12;
      end;
      l .: X c= {0.F}
      proof
        let y be set such that
A17:    y in l .: X;
        consider x being set such that
A18:    x in dom l and
```

```
A19:    x in X and
A20:    y = l.x by A17,FUNCT_1:def 12;
A21:    now
          assume x in Carrier l;
          then x in (Carrier l) /\ X by A19,XBOOLE_0:def 4;
          hence contradiction by A3,XBOOLE_0:def 7;
        end;
        reconsider x as Element of V by A18;
        l.x = 0.F by A21;
        hence thesis by A20,TARSKI:def 1;
      end;
      hence thesis by A12,XBOOLE_0:def 10;
    end;
    l .: X misses l .: {v}
    proof
A22:  dom l = [#]V by FUNCT_2:169;
A23:  l .: {v} = Im (l,v)
        .= {l.v} by A22,FUNCT_1:117;
      assume l .: X meets l .: {v};
      then consider x being set such that
A24:  x in l .: X and
A25:  x in l .: {v} by XBOOLE_0:3;
A26:  x = 0.F by A11,A24,TARSKI:def 1;
      x = l.v by A23,A25,TARSKI:def 1;
      hence thesis by A2,A26,VECTSP_6:20;
    end;
    then Sum (l .: T"{T.v}) = (Sum (l .: {v})) + (Sum (l .: X)) by A8,
RLVECT_2:18
      .= l.v + (Sum ({0.F})) by A10,A11,RLVECT_2:15
      .= l.v + 0.F by RLVECT_2:15
      .= l.v by RLVECT_1:10;
    hence thesis by Def5;
  end;
end;
theorem Th38:
  for G being FinSequence of V
  st rng G = Carrier l & T|(Carrier l) is one-to-one
  holds T*(l (#) G) = (T@l) (#) (T*G)
proof
  let G be FinSequence of V such that
A1: rng G = Carrier l and
A2: T|(Carrier l) is one-to-one;
  reconsider L = T*(l (#) G) as FinSequence of W;
  reconsider R = (T@l) (#) (T*G) as FinSequence of W;
A3: len L = len (l (#) G) by FINSEQ_2:37
    .= len G by VECTSP_6:def 8;
A4: len R = len (T*G) by VECTSP_6:def 8
    .= len G by FINSEQ_2:37;
  for k being Nat st 1 <= k & k <= len L holds L.k = R.k
  proof
    let k be Nat such that
A5: 1 <= k and
A6: k <= len L;
    len (l (#) G) = len G by VECTSP_6:def 8;
    then
A7: dom (l (#) G) = Seg len G by FINSEQ_1:def 3;
    k in NAT by ORDINAL1:def 13;
    then
A8: k in dom (l (#) G) by A3,A5,A6,A7;
    then
A9: k in dom G by A7,FINSEQ_1:def 3;
    then
A10: G.k in rng G by FUNCT_1:12;
    reconsider gk = G/.k as Element of V;
A11: (l (#) G).k = (l.gk)*gk by A8,VECTSP_6:def 8;
A12: G.k = G/.k by A9,PARTFUN1:def 8;
```

```
    then reconsider Gk = G.k as Element of V;
    (T*G).k = T.Gk by A9,FUNCT_1:23;
    then reconsider TGk = (T*G).k as Element of W;
A13: L.k = T.((l.gk)*gk) by A8,A11,FUNCT_1:23
      .= (l.gk)*(T.gk) by MOD_2:def 5
      .= (l.Gk)*TGk by A9,A12,FUNCT_1:23;
A14: dom R = Seg len G by A4,FINSEQ_1:def 3;
    dom T = [#]V by Th7;
    then dom (T*G) = dom G by A1,RELAT_1:46;
    then
A15: (T*G)/.k = (T*G).k by A9,PARTFUN1:def 8;
    (T@l).((T*G).k) = l.(G.k)
    proof
      (T*G).k = T.(G.k) by A9,FUNCT_1:23;
      hence thesis by A1,A2,A10,Th37;
    end;
    hence thesis by A7,A8,A13,A14,A15,VECTSP_6:def 8;
  end;
  hence thesis by A3,A4,FINSEQ_1:18;
end;
theorem Th39:
  T|(Carrier l) is one-to-one implies T .: (Carrier l) = Carrier (T@l)
proof
  assume
A1: T|(Carrier l) is one-to-one;
A2: Carrier (T@l) c= T .: (Carrier l) by Th30;
  T .: (Carrier l) c= Carrier (T@l)
  proof
    let w be set such that
A3: w in T .: (Carrier l);
    consider v being set such that
A4: v in dom T and
A5: v in Carrier l and
A6: T.v = w by A3,FUNCT_1:def 12;
    reconsider v as Element of V by A4;
A7: (T@l).(T.v) = l.v by A1,A5,Th37;
    l.v <> 0.F by A5,VECTSP_6:20;
    hence thesis by A6,A7;
  end;
  hence thesis by A2,XBOOLE_0:def 10;
end;
theorem Th40:
  for A being Subset of V, B being Basis of V,
  l being Linear_Combination of B \ A st A is Basis of ker T & A c= B
  holds T.(Sum l) = Sum (T@l)
proof
  let A be Subset of V, B be Basis of V,
  l be Linear_Combination of B \ A such that
A1: A is Basis of ker T and
A2: A c= B;
  consider G being FinSequence of V such that
A3: G is one-to-one and
A4: rng G = Carrier l and
A5: Sum l = Sum (l (#) G) by VECTSP_6:def 9;
  set H = T*G;
  reconsider H as FinSequence of W;
A6: T|(B \ A) is one-to-one by A1,A2,Th22;
  Carrier l c= B \ A by VECTSP_6:def 7;
  then
A7: (T|(B \ A))|(Carrier l) = T|(Carrier l) by RELAT_1:103;
  then
A8: T|(Carrier l) is one-to-one by A6,FUNCT_1:84;
  dom T = [#]V by Th7;
  then
A9: H is one-to-one by A3,A4,A6,A7,Th1,FUNCT_1:84;
A10: rng H = T .: (Carrier l) by A4,RELAT_1:160
```

```
      .= Carrier (T@l) by A8,Th39;
A11: T*(l (#) G) = (T@l) (#) H by A4,A8,Th38;
  Sum (T@l) = Sum ((T@l) (#) H) by A9,A10,VECTSP_6:def 9;
  hence thesis by A5,A11,MATRLIN:20;
end;

theorem Th41:
  for X being Subset of V st X is linearly-dependent
  holds ex l being Linear_Combination of X st Carrier l <> {} & Sum l = 0.V
proof
  let X be Subset of V such that
A1: X is linearly-dependent;
  not (for l being Linear_Combination of X st Sum l = 0.V
  holds Carrier l = {}) by A1,VECTSP_7:def 1;
  hence thesis;
end;

:: "Pulling back" a linear combination from the image space of a
:: linear transformation to the base space.

definition
  let F be Field, V,W be VectSp of F, X be Subset of V,
  T be linear-transformation of V,W, l be Linear_Combination of T .: X;
  assume
A1: T|X is one-to-one;
  func T#l -> Linear_Combination of X equals
  :Def6:
  (l*T) +* ((V \ X) --> 0.F);
  coherence
  proof
    set f = (l*T) +* ((V \ X) --> 0.F);
    dom l = [#]W by FUNCT_2:169;
    then rng T c= dom l by Th7;
    then
A2: dom (l*T) = dom T by RELAT_1:46;
A3: dom ((V \ X) --> 0.F) = [#]V \ X by FUNCOP_1:19;
A4: dom T = [#]V by Th7;
    [#]V \/ ([#]V \ X) = [#]V by XBOOLE_1:12;
    then
A5: dom f = [#]V by A2,A3,A4,FUNCT_4:def 1;
A6: rng f c= rng (l*T) \/ rng ((V \ X) --> 0.F) by FUNCT_4:18;
A7: rng (l*T) c= rng l by RELAT_1:45;
    rng ((V \ X) --> 0.F) c= {0.F} by FUNCOP_1:19;
    then
A8: rng ((V \ X) --> 0.F) c= [#]F by XBOOLE_1:1;
    rng l c= [#]F by FUNCT_2:169;
    then rng (l*T) c= [#]F by A7,XBOOLE_1:1;
    then rng (l*T) \/ rng ((V \ X) --> 0.F) c= [#]F by A8,XBOOLE_1:8;
    then rng f c= [#]F by A6,XBOOLE_1:1;
    then reconsider f as Element of Funcs ([#]V,[#]F) by A5,FUNCT_2:def 2;
    ex T being finite Subset of V st
    for v being Element of V st not v in T holds f.v = 0.F
    proof
      set C = { v where v is Element of V : f.v <> 0.F };
      C c= [#]V
      proof
        let x be set such that
A9:     x in C;
        consider v being Element of V such that
A10:    v = x and f.v <> 0.F by A9;
        thus thesis by A10;
      end;
      then reconsider C as Subset of V;
      C is finite
      proof
        card C c= card Carrier l
        proof
          ex g being Function
          st g is one-to-one & dom g = C & rng g c= Carrier l
```

```
          proof
            set S = (T"(Carrier l)) /\ X;
            set g = T|S;
A11:        S = C
            proof
A12:          S c= C
              proof
                let x be set such that
A13:            x in S;
A14:            x in X by A13,XBOOLE_0:def 4;
A15:            x in T"(Carrier l) by A13,XBOOLE_0:def 4;
                then
A16:            x in dom T by FUNCT_1:def 13;
A17:            T.x in Carrier l by A15,FUNCT_1:def 13;
                reconsider x as Element of V by A13;
                not x in dom ((V \ X) --> 0.F) by A14,XBOOLE_0:def 5;
                then
A18:            f.x = (l*T).x by FUNCT_4:12;
A19:            (l*T).x = l.(T.x) by A16,FUNCT_1:23;
                l.(T.x) <> 0.F by A17,VECTSP_6:20;
                hence thesis by A18,A19;
              end;
              C c= S
              proof
                let x be set such that
A20:            x in C;
                consider v being Element of V such that
A21:            v = x and
A22:            f.v <> 0.F by A20;
                reconsider x as Element of V by A21;
A23:            now
                  assume not x in X;
                  then
A24:              x in V \ X by XBOOLE_0:def 5;
                  then x in dom ((V \ X) --> 0.F) by FUNCOP_1:19;
                  then f.x = ((V \ X) --> 0.F).x by FUNCT_4:14;
                  hence contradiction by A21,A22,A24,FUNCOP_1:13;
                end;
                x in T"(Carrier l)
                proof
A25:              dom T = [#]V by Th7;
                  T.x in Carrier l
                  proof
                    not x in V \ X by A23,XBOOLE_0:def 5;
                    then
A26:                f.x = (l*T).x by A3,FUNCT_4:12;
                    (l*T).x = l.(T.x) by A25,FUNCT_1:23;
                    hence thesis by A21,A22,A26;
                  end;
                  hence thesis by A25,FUNCT_1:def 13;
                end;
                hence thesis by A23,XBOOLE_0:def 4;
              end;
              hence thesis by A12,XBOOLE_0:def 10;
            end;
A27:        dom g = S
            proof
              dom T = [#]V by Th7;
              hence thesis by RELAT_1:91;
            end;
A28:        rng g c= Carrier l
            proof
              let y be set such that
A29:          y in rng g;
              consider x being set such that
A30:          x in dom g and
```

```
A31:          y = g.x by A29,FUNCT_1:def 5;
              x in T"(Carrier l) by A27,A30,XBOOLE_0:def 4;
              then T.x in Carrier l by FUNCT_1:def 13;
              hence thesis by A27,A30,A31,FUNCT_1:72;
            end;
            take g;
            thus thesis by A1,A11,A27,A28,Th2,XBOOLE_1:17;
          end;
          hence thesis by CARD_1:26;
        end;
        hence thesis;
      end;
      then reconsider C as finite Subset of V;
      take C;
      thus thesis;
    end;
    then reconsider f as Linear_Combination of V by VECTSP_6:def 4;
    Carrier f c= X
    proof
      let x be set such that
A32:  x in Carrier f;
      reconsider x as Element of V by A32;
      now
        assume not x in X;
        then
A33:    x in V \ X by XBOOLE_0:def 5;
        then f.x = ((V \ X) --> 0.F).x by A3,FUNCT_4:14
          .= 0.F by A33,FUNCOP_1:13;
        hence contradiction by A32,VECTSP_6:20;
      end;
      hence thesis;
    end;
    hence thesis by VECTSP_6:def 7;
  end;
end;

theorem Th42:
  for X being Subset of V, l being Linear_Combination of T .: X,
  v being Element of V st v in X & T|X is one-to-one holds (T#l).v = l.(T.v)
proof
  let X be Subset of V, l be Linear_Combination of T .: X,
  v be Element of V such that
A1: v in X and
A2: T|X is one-to-one;
A3: not v in dom ((V \ X) --> 0.F) by A1,XBOOLE_0:def 5;
  T#l = (l*T) +* ((V \ X) --> 0.F) by A2,Def6;
  then
A4: (T#l).v = (l*T).v by A3,FUNCT_4:12;
  dom T = [#]V by Th7;
  hence thesis by A4,FUNCT_1:23;
end;

:: # is a right inverse of @

theorem Th43:
  for X being Subset of V, l being Linear_Combination of T .: X
  st T|X is one-to-one holds T@(T#l) = l
proof
  let X be Subset of V, l be Linear_Combination of T .: X such that
A1: T|X is one-to-one;
  set m = T@(T#l);
  let w be Element of W;
  per cases;
  suppose
A2: w in Carrier l;
    then
A3: l.w <> 0.F by VECTSP_6:20;
    Carrier l c= T .: X by VECTSP_6:def 7;
    then consider v being set such that
```

```
A4: v in dom T and
A5: v in X and
A6: w = T.v by A2,FUNCT_1:def 12;
    reconsider v as Element of V by A4;
    consider B being Subset of V such that
A7: B misses X and
A8: T"{T.v} = {v} \/ B by A1,A5,Th34;
A9: dom (T#l) = [#]V by FUNCT_2:169;
A10: (T#l).v = l.(T.v) by A1,A5,Th42;
A11: (T#l) .: {v} = Im (T#l,v)
      .= {(T#l).v} by A9,FUNCT_1:117;
A12: m.w = Sum ((T#l) .: T"{T.v}) by A6,Def5
      .= Sum ({l.(T.v)} \/ ((T#l) .: B)) by A8,A10,A11,RELAT_1:153;
    per cases;
    suppose B = {};
      then m.w = Sum ({l.(T.v)} \/ {}F) by A12,RELAT_1:149
        .= l.w by A6,RLVECT_2:15;
      hence thesis;
    end;
    suppose
A13:  B <> {};
      Carrier (T#l) c= X by VECTSP_6:def 7;
      then B misses Carrier (T#l) by A7,XBOOLE_1:63;
      then m.w = Sum ({l.(T.v)} \/ {0.F}) by A12,A13,Th35
        .= Sum ({l.(T.v)}) + Sum ({0.F}) by A3,A6,RLVECT_2:18,ZFMISC_1:17
        .= l.(T.v) + Sum ({0.F}) by RLVECT_2:15
        .= l.(T.v) + 0.F by RLVECT_2:15
        .= l.w by A6,RLVECT_1:10;
      hence thesis;
    end;
  end;
  suppose
A14: not w in Carrier l;
    then
A15: l.w = 0.F;
    now
      assume
A16:  m.w <> 0.F;
      then w in Carrier m;
      then T"{w} meets Carrier (T#l) by Th36;
      then consider v being Element of V such that
A17:  v in T"{w} and
A18:  v in Carrier (T#l) by Th3;
      T.v in {w} by A17,FUNCT_1:def 13;
      then
A19:  T.v = w by TARSKI:def 1;
A20:  Carrier (T#l) c= X by VECTSP_6:def 7;
      then T|(Carrier (T#l)) is one-to-one by A1,Th2;
      then m.w = (T#l).v by A18,A19,Th37
        .= 0.F by A1,A15,A18,A19,A20,Th42;
      hence contradiction by A16;
    end;
    hence thesis by A14;
  end;
end;
begin :: The rank+nullity theorem
definition
  let F be Field, V,W be finite-dimensional VectSp of F,
  T be linear-transformation of V,W;
  func rank(T) -> Nat equals
  dim (im T);
  coherence;
  func nullity(T) -> Nat equals
```

```
  dim (ker T);
  coherence;
end;
theorem Th44:
  for V,W being finite-dimensional VectSp of F,
  T being linear-transformation of V,W holds dim V = rank(T) + nullity(T)
proof
  let V,W be finite-dimensional VectSp of F,
  T be linear-transformation of V,W;
  consider A being finite Basis of ker T;
  reconsider A' = A as Subset of V by Th19;
  consider B being Basis of V such that
A1: A c= B by VECTSP_9:17;
  reconsider B as finite Subset of V by VECTSP_9:24;
  reconsider X = B \ A' as finite Subset of B by XBOOLE_1:36;
  reconsider X as finite Subset of V;
A2: B = A \/ X by A1,XBOOLE_1:45;
  reconsider C = T .: X as finite Subset of W;
  reconsider A as finite Basis of ker T;
  reconsider B as finite Basis of V;
A3: T|X is one-to-one by A1,Th22;
A4: X c= dom (T|X)
  proof
    dom T = [#]V by Th7;
    hence thesis by RELAT_1:91;
  end;
A5: card C = card X
  proof
    X,(T|X) .: X are_equipotent by A3,A4,CARD_1:60;
    then X,C are_equipotent by RELAT_1:162;
    hence thesis by CARD_1:21;
  end;
A6: C is linearly-independent
  proof
    assume C is linearly-dependent;
    then consider l being Linear_Combination of C such that
A7: Carrier l <> {} and
A8: Sum l = 0.W by Th41;
    ex m being Linear_Combination of X st l = T@m
    proof
      reconsider l' = l as Linear_Combination of T .: X;
      set m = T#(l');
      take m;
      thus thesis by A3,Th43;
    end;
    then consider m being Linear_Combination of B \ A' such that
A9: l = T@m;
    T.(Sum m) = 0.W by A1,A8,A9,Th40;
    then Sum m in ker T by Th10;
    then Sum m in Lin A by VECTSP_7:def 3;
    then Sum m in Lin A' by VECTSP_9:21;
    then consider n being Linear_Combination of A' such that
A10: Sum m = Sum n by VECTSP_7:12;
    (Sum m) - (Sum n) = 0.V by A10,VECTSP_1:66;
    then
A11: Sum (m - n) = 0.V by VECTSP_6:80;
A12: Carrier (m - n) c= (Carrier m) \/ (Carrier n) by VECTSP_6:74;
A13: Carrier m c= B \ A' by VECTSP_6:def 7;
A14: Carrier n c= A by VECTSP_6:def 7;
A15: (B \ A') \/ A' = B by A1,XBOOLE_1:45;
    (Carrier m) \/ (Carrier n) c= (B \ A') \/ A by A13,A14,XBOOLE_1:13;
    then Carrier (m - n) c= B by A12,A15,XBOOLE_1:1;
    then reconsider o = m - n as Linear_Combination of B by VECTSP_6:def 7;
    B is linearly-independent by VECTSP_7:def 3;
    then
A16: Carrier o = {} by A11,VECTSP_7:def 1;
```

```
    A' misses B \ A' by XBOOLE_1:79;
    then Carrier (m - n) = (Carrier m) \/ (Carrier n) by A13,A14,Th32,
XBOOLE_1:64;
    then Carrier m = {} by A16;
    then T .: (Carrier m) = {} by RELAT_1:149;
    hence thesis by A7,A9,Th30,XBOOLE_1:3;
  end;
  reconsider C as finite Subset of im T by Th12;
  reconsider L = Lin C as strict Subspace of im T;
  for v being Element of im T holds v in L
  proof
    let v be Element of im T;
A17: v in im T by STRUCT_0:def 5;
    reconsider v' = v as Element of W by VECTSP_4:18;
    consider u being Element of V such that
A18: T.u = v' by A17,Th13;
    reconsider A' = A as Subset of V by Th19;
    V is_the_direct_sum_of Lin A', Lin (B \ A') by A1,Th33;
    then
A19: (Omega).V = (Lin A') + (Lin (B \ A')) by VECTSP_5:def 4;
    u in (Omega).V by STRUCT_0:def 5;
    then consider u1, u2 being Element of V such that
A20: u1 in Lin A' and
A21: u2 in Lin (B \ A') and
A22: u = u1 + u2 by A19,VECTSP_5:5;
A23: T.u = T.u1 + T.u2 by A22,MOD_2:def 5;
    Lin A = ker T by VECTSP_7:def 3;
    then u1 in ker T by A20,VECTSP_9:21;
    then T.u1 = 0.W by Th10;
    then
A24: T.u = T.u2 by A23,RLVECT_1:10;
    consider l being Linear_Combination of B \ A' such that
A25: u2 = Sum l by A21,VECTSP_7:12;
A26: T@l is Linear_Combination of T .: (Carrier l) by Th29;
A27: Carrier l c= B \ A' by VECTSP_6:def 7;
    reconsider C' = C as Subset of W;
    reconsider m = T@l as Linear_Combination of C' by A26,A27,RELAT_1:156
,VECTSP_6:25;
    ex m being Linear_Combination of C' st v = Sum m
    proof
      take m;
      thus thesis by A1,A18,A24,A25,Th40;
    end;
    then v in Lin C' by VECTSP_7:12;
    hence thesis by VECTSP_9:21;
  end;
  then
A28: Lin C = im T by VECTSP_4:40;
  reconsider C as linearly-independent Subset of im T by A6,VECTSP_9:16;
  reconsider C as finite Basis of im T by A28,VECTSP_7:def 3;
A29: nullity T = card A by VECTSP_9:def 2;
A30: rank T = card C by VECTSP_9:def 2;
  dim V = card B by VECTSP_9:def 2
    .= rank T + nullity T by A2,A5,A29,A30,CARD_2:53,XBOOLE_1:79;
  hence thesis;
end;

theorem
  for V,W being finite-dimensional VectSp of F,
  T being linear-transformation of V,W st T is one-to-one holds dim V = rank T
proof
  let V,W be finite-dimensional VectSp of F,
  T be linear-transformation of V,W such that
A1: T is one-to-one;
  ker T = (0).V by A1,Th15;
  then
A2: nullity(T) = 0 by Th16;
```

```
  dim V = rank(T) + nullity(T) by Th44
    .= rank(T) by A2;
  hence thesis;
end;
```

B.2 The vector space of subsets of a set based on symmetric difference

Note: there is a discrepency between the intended title of this section and the title of the corresponding MIZAR article. As of April 15, 2009, the official title of this article in the MIZAR Mathematical Library is 'The vector space of subsets of a set based on disjoint union'. The editors of the MIZAR Mathematical Library have accepted my request to change 'disjoint union' to 'symmetric difference', but the current edition of the library does not yet reflect that change.

```
:: The Vector Space of Subsets of a Set Based on Disjoint Union
::  by Jesse Alama
::
:: Received October 9, 2007
:: Copyright (c) 2007 Association of Mizar Users
environ
 vocabularies FINSET_1, BSPACE, FUNCT_1, CARD_1, SUBSET_1, TARSKI, BOOLE,
      RELAT_1, NAT_1, GROUP_1, FINSEQ_1, FINSEQ_2, QC_LANG1, BINOP_1, VECTSP_1,
      RLVECT_1, RLVECT_3, RLVECT_2, SEQ_1, FINSEQ_4, FUNCT_4, ORDINAL2,
      MATRLIN, VECTSP_9, INT_3, REALSET1, ARYTM;
 notations TARSKI, XBOOLE_0, ZFMISC_1, SUBSET_1, RELAT_1, DOMAIN_1, RELSET_1,
      FUNCT_1, NUMBERS, NAT_1, INT_1, PARTFUN1, FUNCT_2, BINOP_1, FUNCT_7,
      XXREAL_0, CARD_1, FINSET_1, FINSEQ_1, FINSEQOP, CARD_2, REALSET1,
      STRUCT_0, ALGSTR_0, GROUP_1, RLVECT_1, VECTSP_1, VECTSP_6, VECTSP_7,
      MATRLIN, VECTSP_9, INT_3, RANKNULL;
 constructors NAT_1, FINSEQOP, HAHNBAN, VECTSP_7, VECTSP_9, REALSET1, WELLORD2,
      NAT_D, FUNCT_7, BINOP_1, CARD_2, RANKNULL, INT_3, GR_CY_1, XXREAL_0,
      MATRLIN;
 registrations RELAT_1, STRUCT_0, CARD_1, FINSET_1, FINSEQ_1, REALSET1,
      SUBSET_1, XBOOLE_0, VECTSP_1, ORDINAL1, XREAL_0, INT_1, VECTSP_7;
 requirements NUMERALS, BOOLE, ARITHM, SUBSET, REAL;
 definitions TARSKI, FUNCT_1, FINSEQ_1, CARD_1, VECTSP_6, XBOOLE_0, VECTSP_1,
      RLVECT_1, STRUCT_0, FINSEQ_2, BINOP_1, INT_3, ALGSTR_0;
 theorems TARSKI, ZFMISC_1, FINSEQ_1, FUNCT_1, VECTSP_7, CARD_2, XBOOLE_1,
      FUNCT_2, SUBSET_1, XBOOLE_0, VECTSP_1, RLVECT_1, VECTSP_4, VECTSP_6,
      STRUCT_0, CARD_1, FUNCOP_1, FUNCT_7, FINSEQ_2, NAT_1, WELLORD2, RANKNULL,
      MATRIX_3, INT_2, INT_3, GR_CY_1, NAT_D, REALSET1, ORDINAL1, PARTFUN1,
      FINSEQ_3, MATRLIN;
 schemes FINSEQ_1, FINSET_1, BINOP_1, FINSEQ_2, CLASSES1;
begin
definition
  let S be 1-sorted;
  func <*>S -> FinSequence of S equals
  <*>([#]S);
  coherence;
end;
:: exactly as in FINSEQ_2
reserve S for 1-sorted,
  d for Element of S,
  i for Element of NAT,
  p for FinSequence,
  b,X for set;
:: copied from FINSEQ_2:13
```

```
theorem
  for p being FinSequence of S st i in dom p holds p.i in S
proof
  let p be FinSequence of S;
  assume i in dom p;
  hence p.i in the carrier of S by FINSEQ_2:13;
end;

:: copied from FINSEQ_2:14

theorem
  (for i being Nat st i in dom p holds p.i in S) implies p is FinSequence of S
proof
  assume
A1: for i being Nat st i in dom p holds p.i in S;
  for i being Nat st i in dom p holds p.i in the carrier of S
  proof
    let i be Nat;
    assume i in dom p;
    then p.i in S by A1;
    hence thesis by STRUCT_0:def 5;
  end;
  hence thesis by FINSEQ_2:14;
end;

scheme IndSeqS{S() -> 1-sorted, P[set]}:
  for p being FinSequence of S() holds P[p]
provided
A1: P[<*> S()]
and
A2: for p being FinSequence of S() for x being Element of S()
st P[p] holds P[p^<*x*>]
proof
A3: P[<*>the carrier of S()] by A1;
  thus for p being FinSequence of the carrier of S() holds P[p]
  from FINSEQ_2:sch 2(A3,A2);
end;

begin :: The two-element field Z_2

definition
  func Z_2 -> Field equals
  INT.Ring(2);
  coherence by INT_2:44,INT_3:22;
end;

theorem
  [#]Z_2 = {0,1} by CARD_1:88;

theorem
  for a being Element of Z_2 holds a = 0 or a = 1 by CARD_1:88,TARSKI:def 2;

theorem Th5:
  0.Z_2 = 0 by FUNCT_7:def 1,GR_CY_1:12;

theorem Th6:
  1.Z_2 = 1 by INT_3:24;

theorem Th7:
  1.Z_2 + 1.Z_2 = 0.Z_2
proof
  1.Z_2 + 1.Z_2 = (1+1) mod 2 by Th6,GR_CY_1:def 5
    .= 0 by NAT_D:25;
  hence thesis by FUNCT_7:def 1;
end;

theorem
  for x being Element of Z_2 holds x = 0.Z_2 iff x <> 1.Z_2
  by Th5,Th6,CARD_1:88,TARSKI:def 2;

begin :: Set-theoretical Preliminaries

definition
  let X,x be set;
  func X@x -> Element of Z_2 equals
  :Def3:
  1.Z_2 if x in X otherwise 0.Z_2;
```

```
  coherence;
  consistency;
end;
theorem
  for X,x being set holds X@x = 1.Z_2 iff x in X by Def3;
theorem
  for X,x being set holds X@x = 0.Z_2 iff not x in X by Def3;
theorem
  for X,x being set holds X@x <> 0.Z_2 iff X@x = 1.Z_2
  by Th5,Th6,CARD_1:88,TARSKI:def 2;
theorem
  for X,x,y being set holds X@x = X@y iff (x in X iff y in X)
proof
  let X,x,y be set;
  thus X@x = X@y implies (x in X iff y in X)
  proof
    assume
A1: X@x = X@y;
    thus x in X implies y in X
    proof
      assume x in X;
      then X@x = 1.Z_2 by Def3;
      hence thesis by A1,Def3;
    end;
    assume y in X;
    then X@y = 1.Z_2 by Def3;
    hence thesis by A1,Def3;
  end;
  assume
A2: x in X iff y in X;
  per cases by Th5,Th6,CARD_1:88,TARSKI:def 2;
  suppose X@x = 0.Z_2;
    hence thesis by A2,Def3;
  end;
  suppose X@x = 1.Z_2;
    hence thesis by A2,Def3;
  end;
end;
theorem
  for X,Y,x being set holds X@x = Y@x iff (x in X iff x in Y)
proof
  let X,Y,x be set;
  thus X@x = Y@x implies (x in X iff x in Y)
  proof
    assume
A1: X@x = Y@x;
    thus x in X implies x in Y
    proof
      assume x in X;
      then X@x = 1.Z_2 by Def3;
      hence thesis by A1,Def3;
    end;
    assume x in Y;
    then Y@x = 1.Z_2 by Def3;
    hence thesis by A1,Def3;
  end;
  thus (x in X iff x in Y) implies X@x = Y@x
  proof
    assume
A2: x in X iff x in Y;
    per cases by Th5,Th6,CARD_1:88,TARSKI:def 2;
    suppose X@x = 0.Z_2;
      hence thesis by A2,Def3;
    end;
    suppose X@x = 1.Z_2;
```

```
      hence thesis by A2,Def3;
    end;
  end;
end;

theorem
  for x being set holds {}@x = 0.Z_2 by Def3;

theorem Th15:
  for X being set, u,v being Subset of X, x being Element of X
  holds (u \+\ v)@x = u@x + v@x
proof
  let X be set, u,v be Subset of X, x be Element of X;
  per cases;
  suppose
A1: x in u \+\ v;
    then
A2: (u \+\ v)@x = 1.Z_2 by Def3;
    per cases;
    suppose
A3:   x in u;
      then
A4:   not x in v by A1,XBOOLE_0:1;
A5:   u@x = 1.Z_2 by A3,Def3;
      v@x = 0.Z_2 by A4,Def3;
      hence thesis by A2,A5,RLVECT_1:10;
    end;
    suppose
A6:   not x in u;
      then
A7:   x in v by A1,XBOOLE_0:1;
A8:   u@x = 0.Z_2 by A6,Def3;
      v@x = 1.Z_2 by A7,Def3;
      hence thesis by A2,A8,RLVECT_1:10;
    end;
  end;
  suppose
A9: not x in u \+\ v;
    then
A10: (u \+\ v)@x = 0.Z_2 by Def3;
    per cases;
    suppose
A11:  x in u;
      then
A12:  x in v by A9,XBOOLE_0:1;
      u@x = 1.Z_2 by A11,Def3;
      hence thesis by A10,A12,Def3,Th7;
    end;
    suppose
A13:  not x in u;
      then
A14:  not x in v by A9,XBOOLE_0:1;
A15:  u@x = 0.Z_2 by A13,Def3;
      v@x = 0.Z_2 by A14,Def3;
      hence thesis by A10,A15,RLVECT_1:10;
    end;
  end;
end;

theorem
  for X,Y being set holds X = Y iff for x being set holds X@x = Y@x
proof
  let X,Y be set;
  thus X = Y implies for x being set holds X@x = Y@x;
  thus (for x being set holds X@x = Y@x) implies X = Y
  proof
    assume
A1: for x being set holds X@x = Y@x;
    thus X c= Y
```

```
    proof
      let y be set such that
A2:   y in X;
      X@y = 1.Z_2 by A2,Def3;
      then Y@y = 1.Z_2 by A1;
      hence thesis by Def3;
    end;
    let y be set such that
A3: y in Y;
    Y@y = 1.Z_2 by A3,Def3;
    then X@y = 1.Z_2 by A1;
    hence thesis by Def3;
  end;
end;
begin :: The Boolean Bector Space of Subsets of a Set
definition
  let X be set, a be Element of Z_2, c be Subset of X;
  func a \*\ c -> Subset of X equals
  :Def4:
  c if a = 1.Z_2, {}X if a = 0.Z_2;
  consistency;
  coherence;
end;
definition
  let X be set;
  func bspace-sum(X) -> BinOp of bool X means
  :Def5:
  for c,d being Subset of X
  holds it.(c,d) = c \+\ d;
  existence
  proof
    defpred P[set,set,set] means
    ex a,b being Subset of X st $1 = a & $2 = b & $3 = a \+\ b;
A1: for x,y being set st x in bool X & y in bool X ex z being set
    st z in bool X & P[x,y,z]
    proof
      let x,y be set such that
A2:   x in bool X and
A3:   y in bool X;
      reconsider x,y as Subset of X by A2,A3;
      set z = x \+\ y;
      take z;
      thus thesis;
    end;
    consider f being Function of [:bool X,bool X:],bool X such that
A4: for x,y being set st x in bool X & y in bool X
    holds P[x,y,f.(x,y)] from BINOP_1:sch 1(A1);
    reconsider f as BinOp of bool X;
A5: for c,d being Subset of X holds f.(c,d) = c \+\ d
    proof
      let c,d be Subset of X;
      consider a,b being Subset of X such that
A6:   c = a and
A7:   d = b and
A8:   f.(c,d) = a \+\ b by A4;
      thus thesis by A6,A7,A8;
    end;
    take f;
    thus thesis by A5;
  end;
  uniqueness
  proof
    let f,g be BinOp of bool X such that
A9: for c,d being Subset of X holds f.(c,d) = c \+\ d and
A10: for c,d being Subset of X holds g.(c,d) = c \+\ d;
    dom f = [:bool X,bool X:] by FUNCT_2:def 1;
```

```
    then
A11: dom f = dom g by FUNCT_2:def 1;
    for x being set st x in dom f holds f.x = g.x
    proof
      let x be set such that
A12:  x in dom f;
      consider y,z being set such that
A13:  y in bool X and
A14:  z in bool X and
A15:  x = [y,z] by A12,ZFMISC_1:def 2;
      reconsider y as Subset of X by A13;
      reconsider z as Subset of X by A14;
      f.(y,z) = y \+\ z & g.(y,z) = y \+\ z by A9,A10;
      hence thesis by A15;
    end;
    hence thesis by A11,FUNCT_1:9;
  end;
end;

theorem Th17:
  for a being Element of Z_2, c,d being Subset of X
  holds a \*\ (c \+\ d) = (a \*\ c) \+\ (a \*\ d)
proof
  let a be Element of Z_2, c,d be Subset of X;
  per cases by Th5,Th6,CARD_1:88,TARSKI:def 2;
  suppose a = 0.Z_2;
    then a \*\ (c \+\ d) = {}X & a \*\ c = {}X & a \*\ d = {}X by Def4;
    hence thesis;
  end;
  suppose a = 1.Z_2;
    then a \*\ (c \+\ d) = c \+\ d & a \*\ c = c & a \*\ d = d by Def4;
    hence thesis;
  end;
end;

theorem Th18:
  for a,b being Element of Z_2, c being Subset of X
  holds (a+b) \*\ c = (a \*\ c) \+\ (b \*\ c)
proof
  let a,b be Element of Z_2, c be Subset of X;
  per cases by Th5,Th6,CARD_1:88,TARSKI:def 2;
  suppose
A1: a = 0.Z_2;
    then a \*\ c = {}X by Def4;
    hence thesis by A1,RLVECT_1:10;
  end;
  suppose
A2: a = 1.Z_2;
    per cases by Th5,Th6,CARD_1:88,TARSKI:def 2;
    suppose
A3:   b = 0.Z_2;
      then b \*\ c = {}X by Def4;
      hence thesis by A3,RLVECT_1:10;
    end;
    suppose
A4:   b = 1.Z_2;
      then
A5:   b \*\ c = c by Def4;
      c \+\ c = {}X by XBOOLE_1:92;
      hence thesis by A2,A4,A5,Def4,Th7;
    end;
  end;
end;

theorem
  for c being Subset of X holds (1.Z_2) \*\ c = c by Def4;

theorem Th20:
  for a,b being Element of Z_2, c being Subset of X
```

```
  holds a \*\ (b \*\ c) = (a*b) \*\ c
proof
  let a,b be Element of Z_2, c be Subset of X;
  per cases by Th5,Th6,CARD_1:88,TARSKI:def 2;
  suppose
A1: a = 0.Z_2;
    then
A2: a*b = 0.Z_2 by VECTSP_1:39;
    a \*\ (b \*\ c) = {}X by A1,Def4;
    hence thesis by A2,Def4;
  end;
  suppose
A3: a = 1.Z_2;
    then a \*\ (b \*\ c) = b \*\ c by Def4;
    hence thesis by A3,VECTSP_1:def 16;
  end;
end;

definition
  let X be set;
  func
  bspace-scalar-mult(X) -> Function of [:the carrier of Z_2,bool X:],bool X
  means
  :Def6:
  for a being Element of Z_2, c being Subset of X
  holds it.(a,c) = a \*\ c;
  existence
  proof
    defpred P[set,set,set] means ex a being Element of Z_2,
    c being Subset of X st $1 = a & $2 = c & $3 = a \*\ c;
A1: for x,y being set st x in the carrier of Z_2 & y in bool X ex z being set
    st z in bool X & P[x,y,z]
    proof
      let x,y be set such that
A2:   x in the carrier of Z_2 and
A3:   y in bool X;
      reconsider x as Element of Z_2 by A2;
      reconsider y as Subset of X by A3;
      set z = x \*\ y;
      take z;
      thus thesis;
    end;
    consider f being Function of [:the carrier of Z_2,bool X:],bool X such that
A4: for x,y being set st x in the carrier of Z_2 & y in bool X
    holds P[x,y,f.(x,y)] from BINOP_1:sch 1(A1);
A5: for a being Element of Z_2, c being Subset of X holds f.(a,c) = a \*\ c
    proof
      let a be Element of Z_2, c be Subset of X;
      consider a' being Element of Z_2, c' being Subset of X such that
A6:   a = a' and
A7:   c = c' and
A8:   f.(a,c) = a' \*\ c' by A4;
      thus thesis by A6,A7,A8;
    end;
    take f;
    thus thesis by A5;
  end;
  uniqueness
  proof
    let f,g be Function of [:the carrier of Z_2,bool X:],bool X such that
A9: for a being Element of Z_2, c being Subset of X
    holds f.(a,c) = a \*\ c and
A10: for a being Element of Z_2, c being Subset of X holds g.(a,c) = a \*\ c;
    dom f = [:the carrier of Z_2,bool X:] by FUNCT_2:def 1;
    then
A11: dom f = dom g by FUNCT_2:def 1;
    for x being set st x in dom f holds f.x = g.x
```

```
      proof
        let x be set such that
A12:  x in dom f;
        consider y,z being set such that
A13:  y in the carrier of Z_2 and
A14:  z in bool X and
A15:  x = [y,z] by A12,ZFMISC_1:def 2;
        reconsider y as Element of Z_2 by A13;
        reconsider z as Subset of X by A14;
        f.(y,z) = y \*\ z & g.(y,z) = y \*\ z by A9,A10;
        hence thesis by A15;
      end;
      hence thesis by A11,FUNCT_1:9;
    end;
end;
definition
  let X be set;
  func bspace(X) -> non empty VectSpStr over Z_2 equals
  VectSpStr (# bool X,
    bspace-sum(X), {}X, bspace-scalar-mult(X) #);
  coherence;
end;
Lm1: for a,b,c being Element of bspace(X), A,B,C being Subset of X
st a = A & b = B & c = C holds a+(b+c) = A \+\ (B \+\ C)
& (a+b)+c = (A \+\ B) \+\ C
proof
  let a,b,c be Element of bspace(X);
  let A,B,C be Subset of X;
  assume
A1: a = A & b = B & c = C;
  thus a+(b+c) = A \+\ (B \+\ C)
  proof
    b+c = B \+\ C by A1,Def5;
    hence thesis by A1,Def5;
  end;
  thus (a+b)+c = (A \+\ B) \+\ C
  proof
    a+b = A \+\ B by A1,Def5;
    hence thesis by A1,Def5;
  end;
end;
Lm2: for a,b being Element of Z_2, x,y being Element of bspace(X),
c,d being Subset of X st x = c & y = d holds (a*x)+(b*y)
= (a \*\ c) \+\ (b \*\ d) & a*(x+y) = a \*\ (c \+\ d) &
(a+b)*x = (a+b) \*\ c & (a*b)*x = (a*b) \*\ c & a*(b*x) = a \*\ (b \*\ c)
proof
  let a,b be Element of Z_2, x,y be Element of bspace(X), c,d be Subset of X
  such that
A1: x = c and
A2: y = d;
  thus (a*x)+(b*y) = (a \*\ c) \+\ (b \*\ d)
  proof
A3: a*x = a \*\ c by A1,Def6;
    b*y = b \*\ d by A2,Def6;
    hence thesis by A3,Def5;
  end;
  thus a*(x+y) = a \*\ (c \+\ d)
  proof
A4: x+y = c \+\ d by A1,A2,Def5;
    thus thesis by A4,Def6;
  end;
  thus (a+b)*x = (a+b) \*\ c by A1,Def6;
  thus (a*b)*x = (a*b) \*\ c by A1,Def6;
  thus a*(b*x) = a \*\ (b \*\ c)
  proof
```

```
      b*x = b \*\ c by A1,Def6;
      hence thesis by Def6;
    end;
  end;

  theorem Th21:
    bspace(X) is Abelian
  proof
    let x,y be Element of bspace(X);
    reconsider A = x, B = y as Subset of X;
    x+y = B \+\ A by Def5
      .= y+x by Def5;
    hence thesis;
  end;

  theorem Th22:
    bspace(X) is add-associative
  proof
    let x,y,z be Element of bspace(X);
    reconsider A = x, B = y, C = z as Subset of X;
    x+(y+z) = A \+\ (B \+\ C) by Lm1
      .= (A \+\ B) \+\ C by XBOOLE_1:91
      .= (x+y)+z by Lm1;
    hence thesis;
  end;

  theorem Th23:
    bspace(X) is right_zeroed
  proof
    let x be Element of bspace(X);
    reconsider A = x as Subset of X;
    reconsider Z = 0.bspace(X) as Subset of X;
    x+0.bspace(X) = A \+\ Z by Def5
      .= x;
    hence thesis;
  end;

  theorem Th24:
    bspace(X) is right_complementable
  proof
    let x be Element of bspace(X);
    reconsider A = x as Subset of X;
  A1: A \+\ A = {}X by XBOOLE_1:92;
    take x;
    thus thesis by A1,Def5;
  end;

  theorem Th25:
    for a being Element of Z_2, x,y being Element of bspace(X)
    holds a*(x+y) = (a*x)+(a*y)
  proof
    let a be Element of Z_2, x,y be Element of bspace(X);
    reconsider c = x, d = y as Subset of X;
    a*(x+y) = a \*\ (c \+\ d) by Lm2
      .= (a \*\ c) \+\ (a \*\ d) by Th17
      .= (a*x)+(a*y) by Lm2;
    hence thesis;
  end;

  theorem Th26:
    for a,b being Element of Z_2, x being Element of bspace(X)
    holds (a+b)*x = (a*x)+(b*x)
  proof
    let a,b be Element of Z_2, x be Element of bspace(X);
    reconsider c = x as Subset of X;
    (a+b)*x = (a+b) \*\ c by Lm2
      .= (a \*\ c) \+\ (b \*\ c) by Th18
      .= (a*x)+(b*x) by Lm2;
    hence thesis;
  end;
```

```
theorem Th27:
  for a,b being Element of Z_2, x being Element of bspace(X)
  holds (a*b)*x = a*(b*x)
proof
  let a,b be Element of Z_2, x be Element of bspace(X);
  reconsider c = x as Subset of X;
  (a*b)*x = (a*b) \*\ c by Lm2
    .= a \*\ (b \*\ c) by Th20
    .= a*(b*x) by Lm2;
  hence thesis;
end;

theorem Th28:
  for x being Element of bspace(X) holds (1_Z_2)*x = x
proof
  let x be Element of bspace(X);
  reconsider c = x as Subset of X;
  (1_Z_2)*x = (1_Z_2) \*\ c by Def6
    .= c by Def4;
  hence thesis;
end;

theorem Th29:
  bspace(X) is VectSp-like
proof
  let a,b be Element of Z_2, x,y be Element of bspace(X);
  thus a*(x+y) = (a*x)+(a*y) by Th25;
  thus (a+b)*x = (a*x)+(b*x) by Th26;
  thus (a*b)*x = a*(b*x) by Th27;
  thus (1.Z_2)*x = x by Th28;
end;

registration
  let X be set;
  cluster bspace(X) -> VectSp-like Abelian right_complementable
    add-associative right_zeroed;
  coherence by Th21,Th22,Th23,Th24,Th29;
end;

begin :: The Linear Independence and Linear Span of Singleton Subsets

definition
  let X be set;
  attr X is Singleton means
  :Def8:
  X is non empty trivial;
end;

registration
  cluster Singleton -> non empty trivial set;
  coherence by Def8;
  cluster non empty trivial -> Singleton set;
  coherence by Def8;
end;

definition
  let X be set, f be Subset of X;
  redefine attr f is Singleton means
  :Def9:
  ex x being set st x in X & f = {x};
  compatibility
  proof
    thus f is Singleton implies ex x being set st x in X & f = {x}
    proof
      assume f is Singleton;
      then f is non empty trivial;
      then consider x being set such that
A1:   f = {x} by REALSET1:def 4;
      take x;
      x in f by A1,TARSKI:def 1;
      hence x in X;
      thus thesis by A1;
```

```
    end;
    thus thesis;
  end;
end;
definition
  let X be set;
  func singletons(X) equals
  { f where f is Subset of X : f is Singleton };
  coherence;
end;
definition
  let X be set;
  redefine func singletons(X) -> Subset of bspace(X);
  coherence
  proof
    set S = singletons(X);
    S c= bool(X)
    proof
      let f be set such that
A1:   f in S;
      consider g being Subset of X such that
A2:   f = g and g is Singleton by A1;
      reconsider f as Subset of X by A2;
      f is Element of bool(X);
      hence thesis;
    end;
    hence thesis;
  end;
end;
registration
  let X be non empty set;
  cluster singletons(X) -> non empty;
  coherence
  proof
    consider x being Element of X;
    {x} in singletons(X);
    hence thesis;
  end;
end;
theorem Th30:
  for X being non empty set, f being Subset of X
  st f is Element of singletons(X) holds f is Singleton
proof
  let X be non empty set, f be Subset of X such that
A1: f is Element of singletons(X);
  f in singletons(X) by A1;
  then consider g being Subset of X such that
A2: g = f and
A3: g is Singleton;
  thus thesis by A2,A3;
end;
definition
  let F be Field, V be VectSp of F, l be Linear_Combination of V,
  x be Element of V;
  redefine func l.x -> Element of F;
  coherence
  proof
    l.x in [#]F;
    hence thesis;
  end;
end;
definition
  let X be non empty set, s be FinSequence of bspace(X), x be Element of X;
  func s@x -> FinSequence of Z_2 means
  :Def11:
```

```
  len it = len s
  & for j being Nat st 1 <= j & j <= len s holds it.j = (s.j)@x;
  existence
  proof
    deffunc F(set) = (s.$1)@x;
    consider p being FinSequence such that
A1: len p = len s and
A2: for k being Nat st k in dom p holds p.k = F(k) from FINSEQ_1:sch 2;
A3: for j being Nat st 1 <= j & j <= len s holds p.j = (s.j)@x
    proof
      let j be Nat such that
A4:   1 <= j and
A5:   j <= len s;
      j in dom p by A4,A5,A1,FINSEQ_3:27;
      hence thesis by A2;
    end;
    rng p c= the carrier of Z_2
    proof
      let y be set such that
A6:   y in rng p;
      consider a being set such that
A7:   a in dom p and
A8:   p.a = y by A6,FUNCT_1:def 5;
      p.a = (s.a)@x by A2,A7;
      hence thesis by A8;
    end;
    then reconsider p as FinSequence of Z_2 by FINSEQ_1:def 4;
    take p;
    thus thesis by A1,A3;
  end;
  uniqueness
  proof
    let f,g be FinSequence of Z_2 such that
A9: len f = len s & for j being Nat st 1 <= j & j <= len s
    holds f.j = (s.j)@x and
A10: len g = len s & for j being Nat st 1 <= j & j <= len s
    holds g.j = (s.j)@x;
    for k being Nat st 1 <= k & k <= len f holds f.k = g.k
    proof
      let k be Nat such that
A11:  1 <= k and
A12:  k <= len f;
      f.k = (s.k)@x & g.k = (s.k)@x by A9,A10,A11,A12;
      hence thesis;
    end;
    hence thesis by A9,A10,FINSEQ_1:18;
  end;
end;

theorem Th31:
  for X being non empty set, x being Element of X
  holds (<*>(bspace(X)))@x = <*>Z_2
proof
  let X be non empty set, x be Element of X;
  set V = bspace(X);
  set L = (<*>V)@x;
  len L = len <*>V by Def11
     .= 0;
  hence thesis;
end;

theorem Th32:
  for X being set, u,v being Element of bspace(X), x being Element of X
  holds (u + v)@x = u@x + v@x
proof
  let X be set, u,v be Element of bspace(X), x be Element of X;
  reconsider u' = u, v' = v as Subset of X;
  (u + v)@x = (u' \+\ v')@x by Def5
```

```
    .= (u'@x) + (v'@x) by Th15;
  hence thesis;
end;
theorem Th33:
  for X being non empty set, s being FinSequence of bspace(X),
  f being Element of bspace(X), x being Element of X
  holds (s ^ <*f*>)@x = (s@x) ^ <*f@x*>
proof
  let X be non empty set, s be FinSequence of bspace(X),
  f be Element of bspace(X), x be Element of X;
  set L = (s ^ <*f*>)@x;
  set R = (s@x) ^ <*f@x*>;
A1: len L = len (s ^ <*f*>) by Def11
    .= (len s) + (len <*f*>) by FINSEQ_1:35
    .= (len s) + 1 by FINSEQ_1:56;
A2: len ((s@x) ^ <*f@x*>) = (len (s@x)) + (len <*f@x*>) by FINSEQ_1:35
    .= (len s) + (len <*f@x*>) by Def11
    .= (len s) + 1 by FINSEQ_1:56;
  for k being Nat st 1 <= k & k <= len L holds L.k = R.k
  proof
    let k be Nat such that
A3: 1 <= k and
A4: k <= len L;
A5: k in NAT by ORDINAL1:def 13;
    per cases by A1,A4,NAT_1:8;
    suppose
A6:   k <= len s;
      k <= len (s ^ <*f*>) by A4,Def11;
      then
A7:   L.k = ((s ^ <*f*>).k)@x by A3,Def11;
      dom (s@x) = Seg (len (s@x)) by FINSEQ_1:def 3
        .= Seg (len s) by Def11;
      then k in dom (s@x) by A3,A5,A6;
      then
A8:   R.k = (s@x).k by FINSEQ_1:def 7
        .= (s.k)@x by A3,A6,Def11;
      dom s = Seg (len s) by FINSEQ_1:def 3;
      then k in dom s by A3,A5,A6;
      hence thesis by A7,A8,FINSEQ_1:def 7;
    end;
    suppose
A9:   k = len L;
A10:  k <= len (s ^ <*f*>) by A4,Def11;
A11:  len (s@x) = len s by Def11;
      dom (<*f@x*>) = {1} by FINSEQ_1:4,def 8;
      then 1 in dom (<*f@x*>) by TARSKI:def 1;
      then
A12:  R.k = <*f@x*>.1 by A1,A9,A11,FINSEQ_1:def 7
        .= f@x by FINSEQ_1:def 8;
      dom (<*f*>) = {1} by FINSEQ_1:4,def 8;
      then 1 in dom (<*f*>) by TARSKI:def 1;
      then (s ^ <*f*>).k = <*f*>.1 by A1,A9,FINSEQ_1:def 7
        .= f by FINSEQ_1:def 8;
      hence thesis by A3,A10,A12,Def11;
    end;
  end;
  hence thesis by A1,A2,FINSEQ_1:18;
end;
theorem Th34:
  for X being non empty set, s being FinSequence of bspace(X),
  x being Element of X holds (Sum s)@x = Sum (s@x)
proof
  let X be non empty set, s be FinSequence of bspace(X), x be Element of X;
  set V = bspace(X);
  defpred Q[FinSequence of V] means (Sum ($1))@x = Sum (($1)@x);
A1: Q[<*>V]
```

```
  proof
    set e = <*>V;
    reconsider z = 0.V as Subset of X;
A2: Sum e = 0.V by RLVECT_1:60;
A3: e@x = <*>Z_2 by Th31;
    z@x = 0.Z_2 by Def3;
    hence thesis by A2,A3,RLVECT_1:60;
  end;
A4: for p being FinSequence of V, f being Element of V st Q[p]
  holds Q[p ^ <*f*>]
  proof
    let p be FinSequence of V, f be Element of V such that
A5: Q[p];
    (Sum (p ^ <*f*>))@x = ((Sum p) + (Sum <*f*>))@x by RLVECT_1:58
      .= ((Sum p) + f)@x by RLVECT_1:61
      .= (Sum p)@x + f@x by Th32
      .= Sum (p@x) + Sum (<*f@x*>) by A5,RLVECT_1:61
      .= Sum (p@x ^ <*f@x*>) by RLVECT_1:58
      .= Sum ((p ^ <*f*>)@x) by Th33;
    hence thesis;
  end;
  for p being FinSequence of V holds Q[p] from IndSeqS(A1,A4);
  hence thesis;
end;

theorem Th35:
  for X being non empty set, l being Linear_Combination of bspace(X),
  x being Element of bspace(X) st x in Carrier l holds l.x = 1_Z_2
proof
  let X be non empty set, l be Linear_Combination of bspace(X),
  x be Element of bspace(X) such that
A1: x in Carrier l;
  l.x <> 0.Z_2 by A1,VECTSP_6:20;
  hence thesis by Th5,Th6,CARD_1:88,TARSKI:def 2;
end;

theorem Th36:
  singletons {} = {}
proof
  set X = {};
  assume singletons(X) <> {};
  then consider f being set such that
A1: f in singletons(X) by XBOOLE_0:def 1;
  consider g being Subset of X such that g = f and
A2: g is Singleton by A1;
  consider x being set such that
A3: x in X and g = {x} by A2;
  thus thesis by A3;
end;

theorem Th37:
  singletons(X) is linearly-independent
proof
  per cases;
  suppose
A1: X is empty;
    thus thesis by A1,Th36;
  end;
  suppose X is non empty;
    then reconsider X as non empty set;
    set V = bspace(X);
    set S = singletons(X);
    for l being Linear_Combination of S st Sum l = 0.V holds Carrier l = {}
    proof
      let l be Linear_Combination of S such that
A2:   Sum l = 0.V;
      set C = Carrier l;
      reconsider s = Sum l as Subset of X;
      assume C <> {};
```

```
      then consider f being Element of V such that
A3:   f in C by SUBSET_1:10;
      reconsider f as Subset of X;
      C c= S by VECTSP_6:def 7;
      then f is Singleton by A3,Th30;
      then consider x being set such that
A4:   x in X and
A5:   f = {x} by Def9;
      x in f by A5,TARSKI:def 1;
      then
A6:   f@x = 1.Z_2 by Def3;
      reconsider x as Element of X by A4;
A7:   s@x = 0.Z_2 by A2,Def3;
A8:   for g being Subset of X st g <> f & g in C holds g@x = 0.Z_2
      proof
        let g be Subset of X such that
A9:     g <> f and
A10:    g in C;
        C c= S by VECTSP_6:def 7;
        then g is Singleton by A10,Th30;
        then consider y being set such that
A11:    y in X and
A12:    g = {y} by Def9;
        reconsider y as Element of X by A11;
        now
          assume g@x <> 0.Z_2;
          then x in {y} by A12,Def3;
          hence contradiction by A5,A9,A12,TARSKI:def 1;
        end;
        hence thesis;
      end;
      reconsider g = f as Element of V;
      reconsider m = l!(C \ {g}) as Linear_Combination of C \ {g};
      reconsider n = l!{g} as Linear_Combination of {g};
      reconsider t = Sum m, u = Sum n as Subset of X;
A13:  l!(Carrier l) = l by RANKNULL:24;
A14:  {g} c= Carrier l by A3,ZFMISC_1:37;
      reconsider l as Linear_Combination of C by A13;
      l = n + m by A14,RANKNULL:27;
      then Sum l = (Sum m) + (Sum n) by VECTSP_6:77;
      then s = t \+\ u by Def5;
      then
A15:  s@x = t@x + u@x by Th15;
A16:  t@x = 0
      proof
A17:    for F being FinSequence of V st F is one-to-one & rng F = Carrier m
        holds (m (#) F)@x = (len F) |-> 0.Z_2
        proof
          let F be FinSequence of V such that F is one-to-one and
A18:      rng F = Carrier m;
          set L = (m (#) F)@x;
          set R = (len F) |-> 0.Z_2;
A19:      len (m (#) F) = len F by VECTSP_6:def 8;
          then
A20:      len L = len F by Def11;
          dom R = Seg (len F) by FUNCOP_1:19;
          then
A21:      len L = len R by A20,FINSEQ_1:def 3;
          for k being Nat st 1 <= k & k <= len L holds L.k = R.k
          proof
            let k be Nat such that
A22:        1 <= k and
A23:        k <= len L;
            len (m (#) F) = len F by VECTSP_6:def 8;
            then
A24:        dom (m (#) F) = Seg (len F) by FINSEQ_1:def 3;
```

```
A25:          k in NAT by ORDINAL1:def 13;
              then k in dom (m (#) F) by A20,A22,A23,A24;
              then
A26:          (m (#) F).k = m.(F/.k)*(F/.k) by VECTSP_6:def 8;
              dom F = Seg (len F) by FINSEQ_1:def 3;
              then
A27:          k in dom F by A20,A22,A23,A25;
              then
A28:          F/.k = F.k by PARTFUN1:def 8;
              then
A29:          F/.k in Carrier m by A18,A27,FUNCT_1:12;
              reconsider Fk = F/.k as Subset of X;
              m.(F/.k) = 1_Z_2 by A18,A27,A28,Th35,FUNCT_1:12;
              then
A30:          (m (#) F).k = Fk by A26,VECTSP_1:def 26;
A31:          Carrier m = C \ {f}
              proof
                thus Carrier m c= C \ {f} by VECTSP_6:def 7;
                thus C \ {f} c= Carrier m
                proof
                  let y be set such that
A32:              y in C \ {f};
A33:              y in C by A32,XBOOLE_0:def 5;
                  reconsider y as Element of V by A32;
                  now
                    assume
A34:                not y in Carrier m;
                    m.y = l.y by A32,RANKNULL:25;
                    then l.y = 0.Z_2 by A34;
                    hence contradiction by A33,VECTSP_6:20;
                  end;
                  hence thesis;
                end;
              end;
A35:          Fk <> f
              proof
                assume Fk = f;
                then not f in {f} by A29,A31,XBOOLE_0:def 5;
                hence contradiction by TARSKI:def 1;
              end;
A36:          Fk in C by A29,A31,XBOOLE_0:def 5;
A37:          L.k = ((m (#) F).k)@x by A19,A20,A22,A23,Def11
                .= 0.Z_2 by A8,A30,A35,A36;
              k in Seg (len F) by A20,A22,A23,A25;
              hence thesis by A37,FUNCOP_1:13;
            end;
            hence thesis by A21,FINSEQ_1:18;
          end;
          consider F being FinSequence of V such that
A38:      F is one-to-one and
A39:      rng F = Carrier m and
A40:      t = Sum (m (#) F) by VECTSP_6:def 9;
A41:      (Sum (m (#) F))@x = Sum ((m (#) F)@x) by Th34;
          (m (#) F)@x = (len F) |-> 0.Z_2 by A17,A38,A39;
          hence thesis by A40,A41,Th5,MATRIX_3:13;
        end;
        u = f
        proof
A42:      Sum n = (n.g)*g by VECTSP_6:43;
          g in {g} by TARSKI:def 1;
          then
A43:      n.g = l.g by RANKNULL:25;
          l.g <> 0.Z_2 by A3,VECTSP_6:20;
          then
A44:      l.g = 1_Z_2 by Th5,Th6,CARD_1:88,TARSKI:def 2;
          thus thesis by A42,A43,A44,VECTSP_1:def 26;
```

```
      end;
      hence thesis by A6,A7,A15,A16,Th5,RLVECT_1:10;
    end;
    hence thesis by VECTSP_7:def 1;
  end;
end;
theorem
  for f being Element of bspace(X) st (ex x being set st x in X & f = {x})
  holds f in singletons(X);
theorem Th39:
  for X being finite set, A being Subset of X
  ex l being Linear_Combination of singletons(X) st Sum l = A
proof
  let X be finite set, A be Subset of X;
  set V = bspace(X);
  set S = singletons(X);
  defpred P[set] means $1 is Subset of X
  implies ex l being Linear_Combination of S st Sum l = $1;
A1: A is finite;
A2: P[{}]
  proof
    assume {} is Subset of X;
    reconsider l = ZeroLC(V) as Linear_Combination of S by VECTSP_6:26;
A3: Sum l = 0.V by VECTSP_6:41;
    take l;
    thus thesis by A3;
  end;
A4: for x,B being set st x in A & B c= A & P[B] holds P[B \/ {x}]
  proof
    let x,B be set such that x in A and B c= A and
A5: P[B];
    assume
A6: B \/ {x} is Subset of X;
    then reconsider B as Subset of X by XBOOLE_1:11;
    consider l being Linear_Combination of S such that
A7: Sum l = B by A5;
    per cases;
    suppose
A8:   x in B;
      take l;
      thus thesis by A7,A8,ZFMISC_1:46;
    end;
    suppose
A9:   not x in B;
      reconsider f = {x} as Element of V by A6,XBOOLE_1:11;
      reconsider g = f as Subset of X;
      reconsider z = ZeroLC(V) as Linear_Combination of {}V by VECTSP_6:26;
      set m = z +* (f,1_Z_2);
      m is Linear_Combination of {}V \/ {f} by RANKNULL:23;
      then reconsider m = z +* (f,1_Z_2) as Linear_Combination of {f};
      dom z = [#]V by FUNCT_2:169;
      then
A10:  m.f = 1_Z_2 by FUNCT_7:33;
A11:  B misses {x} by A9,ZFMISC_1:56;
      f in S;
      then {f} c= S by ZFMISC_1:37;
      then m is Linear_Combination of S by VECTSP_6:25;
      then reconsider n = l + m as Linear_Combination of S by VECTSP_6:52;
A12:  Sum n = (Sum l) + (Sum m) by VECTSP_6:77
        .= (Sum l) + (m.f)*f by VECTSP_6:43
        .= (Sum l) + f by A10,VECTSP_1:def 26
        .= B \+\ g by A7,Def5
        .= (B \/ {x}) \ (B /\ {x}) by XBOOLE_1:101
        .= (B \/ {x}) \ {} by A11,XBOOLE_0:def 7
        .= B \/ {x};
      take n;
```

```
      thus thesis by A12;
    end;
  end;
  P[A] from FINSET_1:sch 2(A1,A2,A4);
  hence thesis;
end;

theorem Th40:
  for X being finite set holds Lin(singletons(X)) = bspace(X)
proof
  let X be finite set;
  set V = bspace(X);
  set S = singletons(X);
  for v being Element of V holds v in Lin(S)
  proof
    let v be Element of V;
    reconsider f = v as Subset of X;
    consider A being set such that
A1: A c= X and
A2: f = A;
    reconsider A as Subset of X by A1;
    consider l being Linear_Combination of S such that
A3: Sum l = A by Th39;
    thus thesis by A2,A3,VECTSP_7:12;
  end;
  hence thesis by VECTSP_4:40;
end;

theorem Th41:
  for X being finite set holds singletons(X) is Basis of bspace(X)
proof
  let X be finite set;
A1: singletons(X) is linearly-independent by Th37;
  Lin(singletons(X)) = bspace(X) by Th40;
  hence thesis by A1,VECTSP_7:def 3;
end;

registration
  let X be finite set;
  cluster singletons(X) -> finite;
  coherence;
end;

registration
  let X be finite set;
  cluster bspace(X) -> finite-dimensional;
  coherence
  proof
    set S = singletons(X);
A1: S is Basis of bspace(X) by Th41;
    thus thesis by A1,MATRLIN:def 3;
  end;
end;

theorem
  card (singletons X) = card X
proof
  defpred P[set,set] means $1 in X & $2 = {$1};
A2: for x being set st x in X holds ex y being set st P[x,y];
  consider f being Function such that
A3: dom f = X and
A4: for x being set st x in X holds P[x,f.x] from CLASSES1:sch 1(A2);
A5: f is one-to-one
  proof
    let x1,x2 be set such that
A6: x1 in dom f and
A7: x2 in dom f and
A8: f.x1 = f.x2;
A9: P[x1,f.x1] by A3,A4,A6;
    P[x2,f.x2] by A3,A4,A7;
```

```
    hence thesis by A8,A9,ZFMISC_1:6;
  end;
  rng f = singletons(X)
  proof
    thus rng f c= singletons(X)
    proof
      let y be set such that
A10:  y in rng f;
      consider x being set such that
A11:  x in dom f and
A12:  y = f.x by A10,FUNCT_1:def 5;
A13:  f.x = {x} by A3,A4,A11;
      then reconsider fx = f.x as Subset of X by A3,A11,ZFMISC_1:37;
      fx is Singleton by A13;
      hence thesis by A12;
    end;
    let y be set such that
A14: y in singletons(X);
    consider z being Subset of X such that
A15: y = z and
A16: z is Singleton by A14;
    reconsider y as Subset of X by A15;
    consider x being set such that
A17: x in X and
A18: y = {x} by A15,A16,Def9;
    reconsider x as Element of X by A17;
    y = f.x by A4,A17,A18;
    hence thesis by A3,A17,FUNCT_1:12;
  end;
  then X,singletons(X) are_equipotent by A3,A5,WELLORD2:def 4;
  hence thesis by CARD_1:21;
end;
theorem
  card [#](bspace X) = exp(2,card(X)) by CARD_2:44;
theorem
  dim bspace {} = 0
proof
  card [#]bspace {} = 1 by CARD_2:60,ZFMISC_1:1;
  hence thesis by RANKNULL:5;
end;
```

B.3 Euler's polyhedron formula

Note: there is a discrepency between the formal text to be presented and the discussion in the body of the dissertation, especially chapter 3. There, I distinguished the concept of 'simple connectedness' from the neologism 'being a homology sphere' (suggested to me by R. Solovay). The editors of the MIZAR Mathematical Library have approved my change from `simply-connected` to `homology-sphere`, but this change is not yet reflected in the edition of the library as it stands on April 15, 2009.

```
:: Euler's Polyhedron Formula
::  by Jesse Alama
::
:: Received October 9, 2007
:: Copyright (c) 2007 Association of Mizar Users
environ
```

```
 vocabularies FINSET_1, FUNCT_1, FUNCT_2, CARD_1, SUBSET_1, TARSKI, BOOLE,
      RELAT_1, ORDINAL2, VECTSP_1, VECTSP_9, INT_1, RLVECT_1, GROUP_1, ARYTM_1,
      FINSEQ_1, FINSEQ_2, QC_LANG1, RLSUB_1, BSPACE, RANKNULL, RLVECT_3,
      MATRLIN, FINSEQ_4, POLYFORM, VECTSP10, PRALG_1, MATRIX_2, POWER,
      FUNCOP_1, ARYTM, VALUED_0;
 notations TARSKI, XBOOLE_0, ENUMSET1, ZFMISC_1, SUBSET_1, RELAT_1, FUNCT_1,
      RELSET_1, PARTFUN1, FUNCT_2, BINOP_1, CARD_1, NUMBERS, FUNCOP_1,
      FINSET_1, XCMPLX_0, XXREAL_0, NAT_1, INT_1, CARD_2,
      VALUED_0, FINSEQ_1,
      FINSEQ_2, POWER, RVSUM_1, NEWTON, ABIAN, STRUCT_0, RLVECT_1, GROUP_1,
      VECTSP_1, VECTSP_4, VECTSP_5, VECTSP_7, FVSUM_1, GR_CY_1, MATRLIN,
      VECTSP_9, RANKNULL, BSPACE;
 constructors NAT_1, VECTSP_9, BINOP_1, REALSET1, FINSOP_1, XXREAL_0, FVSUM_1,
      WELLORD2, BSPACE, REAL_1, BINOP_2, RANKNULL, VECTSP_7, VECTSP_5, NEWTON,
      GR_CY_1, ABIAN, POWER, CARD_2, CARD_3;
 registrations FRAENKEL, FINSET_1, XBOOLE_0, FUNCT_1, FUNCT_2, RELAT_1,
      SUBSET_1, NAT_1, INT_1, VECTSP_1, STRUCT_0, FINSEQ_1, FINSEQ_2, CARD_1,
      MATRLIN, BSPACE, ORDINAL1, NEWTON, RVSUM_1, FUNCOP_1, POLYNOM1, ABIAN,
      XREAL_0, NUMBERS, JORDAN23, GOBRD13, XCMPLX_0, XXREAL_0, VALUED_0,
      PARTFUN1;
 requirements NUMERALS, BOOLE, ARITHM, SUBSET, REAL;
 definitions XBOOLE_0, BINOP_1, STRUCT_0, TARSKI, FVSUM_1, FINSEQ_1, BSPACE,
      RANKNULL, ALGSTR_0;
 theorems XBOOLE_0, FUNCT_1, RELAT_1, XBOOLE_1, TARSKI, ZFMISC_1, FUNCT_2,
      GROUP_1, RLVECT_1, VECTSP_1, FVSUM_1, FINSEQ_2, CARD_1, FINSEQ_1, NAT_1,
      FINSOP_1, VECTSP_4, BSPACE, RANKNULL, VECTSP_9, ORDINAL1, NEWTON,
      RVSUM_1, GR_CY_1, FUNCOP_1, XREAL_1, XXREAL_0, INT_1, JORDAN16, POWER,
      FIB_NUM2, NUMBERS, CARD_2, PRE_CIRC, FINSEQ_3, SUBSET_1, MOD_2, MATRIX_3,
      CALCUL_1, PARTFUN1, VALUED_0, RELSET_1;
 schemes FUNCT_2, FINSEQ_1, FINSEQ_2;
begin
theorem Th1:
  for X,c,d being set st (ex a,b being set st a <> b & X = {a,b}) & c in X &
  d in X & c <> d holds X = {c,d}
proof
  let X,c,d be set such that
A1: ex a,b being set st a <> b & X = {a,b} and
A2: c in X and
A3: d in X and
A4: c <> d;
  consider a,b being set such that a <> b and
A5: X = {a,b} by A1;
A6: {c,d} c= X by A2,A3,ZFMISC_1:38;
  X c= {c,d}
  proof
A7: c = a or c = b by A2,A5,TARSKI:def 2;
A8: d = a or d = b by A3,A5,TARSKI:def 2;
    let x be set such that
A9: x in X;
    per cases by A5,A9,TARSKI:def 2;
    suppose x = a;
      hence thesis by A4,A7,A8,TARSKI:def 2;
    end;
    suppose x = b;
      hence thesis by A4,A7,A8,TARSKI:def 2;
    end;
  end;
  hence thesis by A6,XBOOLE_0:def 10;
end;
theorem Th2:
  for f being Function st f is one-to-one holds card (dom f) = card (rng f)
proof
  let f be Function such that
A1: f is one-to-one;
A2: dom f, f .: (dom f) are_equipotent by A1,CARD_1:60;
  f .: (dom f) = rng f by RELAT_1:146;
```

```
  hence thesis by A2,CARD_1:21;
end;
begin :: Arithmetical Preliminaries
reserve n for Nat,
  k for Integer;
theorem Th3:
  1 <= k implies k is Nat
proof
  assume 1 <= k;
  then reconsider k as Element of NAT by INT_1:16;
  k is Nat;
  hence thesis;
end;
definition
  let a be Integer, b be Nat;
  redefine func a*b -> Element of INT;
  coherence by INT_1:def 2;
end;
theorem Th4:
  1 is odd
proof
  1 = (2*(0 qua Nat) qua Nat)+ 1;
  hence thesis;
end;
theorem Th5:
  2 is even
proof
  2 = 2*1;
  hence thesis;
end;
theorem Th6:
  3 is odd
proof
  3 = 2*1 + 1;
  hence thesis;
end;
theorem Th7:
  4 is even
proof
  4 = 2*2;
  hence thesis;
end;
theorem Th8:
  n is even implies (-1)|^n = 1
proof
  assume
A1: n is even;
  reconsider n as Element of NAT by ORDINAL1:def 13;
  (-1)|^n = (-1) to_power n by POWER:46;
  hence thesis by A1,FIB_NUM2:5;
end;
theorem Th9:
  n is odd implies (-1)|^n = -1
proof
  assume
A1: n is odd;
  reconsider n as Element of NAT by ORDINAL1:def 13;
  (-1)|^n = (-1) to_power n by POWER:46;
  hence thesis by A1,FIB_NUM2:3;
end;
theorem Th10:
  (-1) |^ n is Integer
proof
  per cases;
```

```
  suppose n is even;
    hence thesis by Th8;
  end;
  suppose n is odd;
    hence thesis by Th9;
  end;
end;

definition
  let a be Integer, n be Nat;
  redefine func a |^ n -> Element of INT;
  coherence
  proof
    consider b being Element of NAT such that
A1: a = b or a = -b by INT_1:8;
    per cases by A1;
    suppose a = b;
      then reconsider a as Element of NAT;
      reconsider s = a |^ n as Element of NAT by ORDINAL1:def 13;
      s in NAT;
      hence thesis by NUMBERS:17;
    end;
    suppose
A2:   a = -b;
A3:   -b = (-1)*b;
      reconsider bn = b |^ n as Element of NAT by ORDINAL1:def 13;
      (-1) |^n is Integer by Th10;
      then reconsider l = (-1) |^ n as Element of INT by INT_1:def 2;
      a |^ n = l*bn by A2,A3,NEWTON:12;
      hence thesis;
    end;
  end;
end;

Lm1: for x being Element of NAT st 0 < x holds 0 qua Nat+1 <= x by NAT_1:13;

theorem Th11:
  for p,q,r being FinSequence holds len (p ^ q) <= len (p ^ (q ^ r))
proof
  let p,q,r be FinSequence;
  len ((p ^ q) ^ r) = len (p ^ (q ^ r)) by FINSEQ_1:45;
  hence thesis by CALCUL_1:6;
end;

theorem Th12:
  1 < n + 2
proof
  0 < n + 1 implies 1 < n + 2
  proof
    assume 0 < n + 1;
    0 qua Nat + 1 = 1;
    hence thesis by XREAL_1:10;
  end;
  hence thesis;
end;

theorem Th13:
  (-1)|^2 = 1
proof
  (-1)|^2 = (-1)|^(1+1)
    .= ((-1)|^1)*((-1)|^1) by NEWTON:13
    .= ((-1)|^1)*(-1) by NEWTON:10
    .= (-1)*(-1) by NEWTON:10;
  hence thesis;
end;

theorem Th14:
  for n being Nat holds (-1)|^n = (-1)|^(n+2)
proof
  let n be Nat;
  (-1)|^(n+2) = ((-1)|^n)*((-1)|^2) by NEWTON:13
```

```
    .= (-1)|^n by Th13;
  hence thesis;
end;

begin :: Preliminaries on Finite Sequences

registration
  let f be FinSequence of INT, k be Nat;
  cluster f.k -> integer;
  coherence
  proof
    per cases;
    suppose k in dom f;
      then f.k = f/.k by PARTFUN1:def 8;
      hence thesis;
    end;
    suppose not k in dom f;
      hence thesis by FUNCT_1:def 4;
    end;
  end;
end;

:: A theorem on telescoping sequences of integers.

theorem Th15:
  for a,b,s being FinSequence of INT st len s > 0 & len a = len s &
  len b = len s & (for n being Nat st 1 <= n & n <= len s
  holds s.n = a.n + b.n) & (for k being Nat st 1 <= k & k < len s
  holds b.k = -(a.(k+1))) holds Sum s = (a.1) + (b.(len s))
proof
  let a,b,s be FinSequence of INT such that
A1: len s > 0 and
A2: len a = len s and
A3: len b = len s and
A4: for n being Nat st 1 <= n & n <= len s holds s.n = a.n + b.n and
A5: for k being Nat st 1 <= k & k < len s holds b.k = -(a.(k+1));
  defpred P[FinSequence of INT] means len $1 > 0 implies
  for a,b being FinSequence of INT st len a = len $1 & len b = len $1 &
  (for n being Nat st 1 <= n & n <= len $1 holds $1.n = a.n + b.n) &
  (for k being Nat st 1 <= k & k < len $1 holds b.k = -(a.(k+1)))
  holds Sum $1 = a.1 + b.(len $1);
A6: P[<*>INT];
A7: for p being FinSequence of INT, x being Element of INT st P[p]
  holds P[p^<*x*>]
  proof
    let p be FinSequence of INT, x be Element of INT such that
A8: P[p];
    set t = p ^ <*x*>;
    assume len t > 0; :: this is outright provable, of course
    let a,b be FinSequence of INT such that
A9: len a = len t and
A10: len b = len t and
A11: for n being Nat st 1 <= n & n <= len t holds t.n = a.n + b.n and
A12: for k being Nat st 1 <= k & k < len t holds b.k = -(a.(k+1));
A13: Sum t = (Sum p) + x by GR_CY_1:20;
    per cases;
    suppose
A14:  len p = 0;
      then p = {};
      then
A15:  Sum p = 0 by GR_CY_1:22;
A16:  t = <*x*>
      proof
        p = {} by A14;
        hence thesis by FINSEQ_1:47;
      end;
      then
A17:  len t = 1 by FINSEQ_1:56;
      reconsider egy = 1 as Nat;
```

```
      egy <= len t by A16,FINSEQ_1:56;
      then t.egy = a.egy + b.egy by A11;
      hence thesis by A13,A15,A16,A17,FINSEQ_1:57;
    end;
    suppose
A18:  len p > 0;
      set m = len p;
      set a' = a|m;
      set b' = b|m;
A19:  m <= len a & m <= len b by A9,A10,CALCUL_1:6;
      then
A20:  len a' = len p by FINSEQ_1:80;
A21:  len b' = len p by A19,FINSEQ_1:80;
A22:  for n being Nat st 1 <= n & n <= len p holds p.n = a'.n + b'.n
      proof
        let n be Nat such that
A23:    1 <= n and
A24:    n <= len p;
        len p <= len t by CALCUL_1:6;
        then
A25:    n <= len t by A24,XXREAL_0:2;
        dom p = Seg len p by FINSEQ_1:def 3;
        then
A26:    n in dom p by A23,A24,FINSEQ_1:3;
        reconsider n as Element of NAT by ORDINAL1:def 13;
        p.n = t.n by A26,FINSEQ_1:def 7
          .= a.n + b.n by A11,A23,A25
          .= a'.n + b.n by A24,FINSEQ_3:121
          .= a'.n + b'.n by A24,FINSEQ_3:121;
        hence thesis;
      end;
      for n being Nat st 1 <= n & n < len p holds b'.n = -(a'.(n+1))
      proof
        let n be Nat such that
A27:    1 <= n and
A28:    n < len p;
        reconsider n as Element of NAT by ORDINAL1:def 13;
A29:    b'.n = b.n by A28,FINSEQ_3:121;
A30:    n + 1 <= len p by A28,INT_1:20;
        len p <= len t by CALCUL_1:6;
        then
A31:    n < len t by A28,XXREAL_0:2;
        a'.(n+1) = a.(n+1) by A30,FINSEQ_3:121;
        hence thesis by A12,A27,A29,A31;
      end;
      then
A32:  Sum p = a'.1 + b'.(len p) by A8,A18,A20,A21,A22;
A33:  a'.1 = a.1
      proof
        reconsider egy = 1 as Element of NAT;
        0 qua Nat + 1 = 1;
        then egy <= len p by A18,INT_1:20;
        hence thesis by FINSEQ_3:121;
      end;
      x = -(b'.(len p)) + b.(len t)
      proof
A34:    len t = (len p) + 1
        proof
          len <*x*> = 1 by FINSEQ_1:56;
          hence thesis by FINSEQ_1:35;
        end;
A35:    1 <= len t
        proof
          0 qua Nat + 1 = 1;
          hence thesis by A34,XREAL_1:8;
        end;
```

```
A36:    a.(len t) = -(b'.(len p))
        proof
A37:      len p < len t
          proof
            0 qua Nat + len p = len p;
            hence thesis by A34,XREAL_1:8;
          end;
          1 <= len p by A18,Lm1;
          then
A38:      b.(len p) = -(a.(len p + 1)) by A12,A37;
          b.(len p) = b'.(len p) by FINSEQ_3:121;
          hence thesis by A34,A38;
        end;
        x = t.(len p + 1) by FINSEQ_1:59
          .= -(b'.(len p)) + b.(len t) by A11,A34,A35,A36;
        hence thesis;
      end;
      hence thesis by A13,A32,A33;
    end;
  end;
  for p being FinSequence of INT holds P[p] from FINSEQ_2:sch 2(A6,A7);
  hence thesis by A1,A2,A3,A4,A5;
end;

theorem Th16:
  for p,q,r being FinSequence holds
  len (p ^ q ^ r) = (len p) + (len q) + (len r)
proof
  let p,q,r be FinSequence;
  len (p ^ q ^ r) = (len (p ^ q)) + (len r) by FINSEQ_1:35
    .= ((len p) + (len q)) + (len r) by FINSEQ_1:35;
  hence thesis;
end;

theorem Th17:
  for x being set, p,q being FinSequence holds (<*x*> ^ p ^ q).1 = x
proof
  let x be set, p,q be FinSequence;
  <*x*> ^ p ^ q = <*x*> ^ (p ^ q) by FINSEQ_1:45;
  hence thesis by FINSEQ_1:58;
end;

theorem Th18:
  for x being set, p,q being FinSequence
  holds (p ^ q ^ <*x*>).((len p) + (len q) + 1) = x
proof
  let x be set, p,q be FinSequence;
  set s = p ^ q;
  (s ^ <*x*>).((len s) + 1) = x by FINSEQ_1:59;
  hence thesis by FINSEQ_1:35;
end;

theorem Th19:
  for p,q,r being FinSequence, k being Nat st len p < k & k <= len (p ^ q)
  holds (p ^ q ^ r).k = q.(k - (len p))
proof
  let p,q,r be FinSequence, k be Nat such that
A1: len p < k and
A2: k <= len (p ^ q);
  len (p ^ q) <= len (p ^ (q ^ r)) by Th11;
  then k <= len (p ^ (q ^ r)) by A2,XXREAL_0:2;
  then
A3: (p ^ (q ^ r)).k = (q ^ r).(k - (len p)) by A1,FINSEQ_1:37;
  set n = k - (len p);
  (len p) - (len p) = 0;
  then
A4: 0 < n by A1,XREAL_1:11;
  0 qua Nat + 1 = 1;
  then
```

```
A5: 1 <= n by A4,INT_1:20;
  then reconsider n as Nat by Th3;
A6: k <= (len p) + (len q) by A2,FINSEQ_1:35;
  n <= len q
  proof
    ((len p) + (len q)) - (len p) = len q;
    hence thesis by A6,XREAL_1:11;
  end;
  then n in Seg (len q) by A5,FINSEQ_1:3;
  then
A7: n in dom q by FINSEQ_1:def 3;
  reconsider n as Element of NAT by ORDINAL1:def 13;
  (q ^ r).n = q.n by A7,FINSEQ_1:def 7;
  hence thesis by A3,FINSEQ_1:45;
end;

definition
  let a be Integer;
  redefine func <*a*> -> FinSequence of INT;
  coherence
  proof
    set s = <*a*>;
A1: rng s = {a} by FINSEQ_1:55;
    a in INT by INT_1:def 2;
    then {a} c= INT by ZFMISC_1:37;
    hence thesis by A1,FINSEQ_1:def 4;
  end;
end;

definition
  let a,b be Integer;
  redefine func <*a,b*> -> FinSequence of INT;
  coherence
  proof
    set s = <*a,b*>;
A1: rng s = {a,b} by FINSEQ_2:147;
    {a,b} c= INT
    proof
      a in INT & b in INT by INT_1:def 2;
      hence thesis by ZFMISC_1:38;
    end;
    hence thesis by A1,FINSEQ_1:def 4;
  end;
end;

definition
  let a,b,c be Integer;
  redefine func <*a,b,c*> -> FinSequence of INT;
  coherence
  proof
    set s = <*a,b,c*>;
A1: rng s = {a,b,c} by FINSEQ_2:148;
    {a,b,c} c= INT
    proof
A2:   a in INT by INT_1:def 2;
A3:   b in INT by INT_1:def 2;
      c in INT by INT_1:def 2;
      hence thesis by A2,A3,JORDAN16:2;
    end;
    hence thesis by A1,FINSEQ_1:def 4;
  end;
end;

definition
  let p,q be FinSequence of INT;
  redefine func p ^ q -> FinSequence of INT;
  coherence by FINSEQ_1:96;
end;
```

```
theorem Th20:
  for p,q being FinSequence of INT holds Sum (p ^ q) = (Sum p) + (Sum q)
proof
  let p,q be FinSequence of INT;
A1: rng p c= REAL by NUMBERS:15,XBOOLE_1:1;
  rng q c= REAL by NUMBERS:15,XBOOLE_1:1;
  then reconsider p,q as real-valued FinSequence by A1,VALUED_0:def 3;
  Sum (p ^ q) = (Sum p) + (Sum q) by RVSUM_1:105;
  hence thesis;
end;

theorem Th21:
  for k being Integer, p being FinSequence of INT
  holds Sum (<*k*> ^ p) = k + (Sum p)
proof
  let k be Integer, p be FinSequence of INT;
  reconsider k as Element of INT by INT_1:def 2;
  Sum (<*k*> ^ p) = (Sum p) + (Sum <*k*>) by Th20
    .= Sum (p ^ <*k*>) by Th20
    .= k + (Sum p) by GR_CY_1:20;
  hence thesis;
end;

theorem Th22:
  for p,q,r being FinSequence of INT
  holds Sum (p ^ q ^ r) = (Sum p) + (Sum q) + (Sum r)
proof
  let p,q,r be FinSequence of INT;
  Sum (p ^ q ^ r) = (Sum (p ^ q)) + (Sum r) by Th20
    .= ((Sum p) + (Sum q)) + Sum r by Th20;
  hence thesis;
end;

theorem
  for a being Element of Z_2 holds Sum <*a*> = a by FINSOP_1:12;

begin :: Polyhedra and Incidence Matrices

:: An incidence matrix is a function that says of any two objects
:: (contained in some set) whether they are incidence to each other.

definition
  let X,Y be set;
  mode incidence-matrix of X,Y is Element of Funcs([:X,Y:],{0.Z_2,1.Z_2});
end;

theorem Th24:
  for X,Y being set holds [:X,Y:] --> 1.Z_2 is incidence-matrix of X,Y
proof
  let X,Y be set;
  set f = [:X,Y:] --> 1.Z_2;
A1: dom f = [:X,Y:] by FUNCOP_1:19;
A2: rng f c= {1.Z_2} by FUNCOP_1:19;
  {1.Z_2} c= {0.Z_2,1.Z_2} by ZFMISC_1:12;
  then rng f c= {0.Z_2,1.Z_2} by A2,XBOOLE_1:1;
  hence thesis by A1,FUNCT_2:def 2;
end;

:: A polyhedron (one might call it an abstract polyhedron) consists of
:: two pieces of data: a sequence of ordered sets, representing the
:: polytope sets (they are ordered for convenience's sake) and a
:: sequence of incidence matrices, which lays out the incidence
:: relation between the (k-1)-polytopes and the k-polytopes.

definition
  struct PolyhedronStr(# PolytopsF ->FinSequence-yielding FinSequence,
    IncidenceF ->Function-yielding FinSequence #);
end;

:: The following properties, 'polyhedron_1', 'polyhedron_2', and
:: 'polyhedron_3' are admittedly a bit contrived.  However, they ensure
:: that a PolyhedronStr is a polyhedron: that there is one more polytope set
:: than incidence matrix, that the incidience matrices are incidence matrices
```

```
:: of the right sets, and that each term of the polytope sequence is an
:: enumeration of the respective polytope set.

definition
  let p be PolyhedronStr;
  attr p is polyhedron_1 means
  :Def1:
  len the IncidenceF of p = len(the PolytopsF of p) - 1;
  attr p is polyhedron_2 means
  :Def2:
  for n being Nat
  st 1 <= n & n < len the PolytopsF of p holds (the IncidenceF of p).n
  is incidence-matrix of rng ((the PolytopsF of p).n),
  rng ((the PolytopsF of p).(n+1));
  attr p is polyhedron_3 means
  :Def3:
  for n being Nat
  st 1 <= n & n <= len the PolytopsF of p
  holds (the PolytopsF of p).n is non empty &
  (the PolytopsF of p).n is one-to-one;
end;

registration
  cluster polyhedron_1 polyhedron_2 polyhedron_3 PolyhedronStr;
  existence
  proof
    reconsider F = <*<*{}*>*> as FinSequence-yielding FinSequence;
    reconsider I = <*>{} as Function-yielding FinSequence;
    take p = PolyhedronStr(#F,I#);
A1: len F = 1 by FINSEQ_1:56;
    len I = 1-1;
    hence p is polyhedron_1 by A1,Def1;
    for n being Nat st 1 <= n & n < 1
    holds I.n is incidence-matrix of rng (F.n),rng (F.(n+1));
    hence p is polyhedron_2 by A1,Def2;
    let n be Nat such that
A2: 1 <= n and
A3: n <= len the PolytopsF of p;
    n = 1 by A1,A2,A3,XXREAL_0:1;
    hence thesis by FINSEQ_1:def 8;
  end;
end;

definition
  mode polyhedron is polyhedron_1 polyhedron_2 polyhedron_3 PolyhedronStr;
end;

reserve p for polyhedron,
  k for Integer,
  n for Nat;

:: The dimension dim(p) of a polyhedron p is just the number of
:: polytope sets that it has.

definition
  let p be polyhedron;
  func dim(p) -> Element of NAT equals

  len the PolytopsF of p;
  coherence;
end;

:: For integers k such that 0 <= k <= dim(p), the set of k-polytopes
:: is data already given by the polyhedron.  For k = dim(p), the set
:: is the singleton {p}, which seems clear enough.  For k = -1, it is
:: convenient to define the set of k-polytopes to be {{}}.  Doing this
:: ensures that, if p is simply connected, then any two vertices are
:: connected by a system of edges.
::
:: For k < -1 and k > dim(p), the set of k-polytopes of p is empty.

definition
  let p be polyhedron, k be Integer;
```

```
  func k-polytopes(p) -> finite set means
  :Def5:
  (k < -1 implies it = {}) &
  (k = -1 implies it = {{}}) & (-1 < k & k < dim(p) implies
  it = rng ((the PolytopsF of p).(k+1))) & (k = dim(p) implies it = {p}) &
  (k > dim(p) implies it = {});
  existence
  proof
    set F = the PolytopsF of p;
    per cases by XXREAL_0:1;
    suppose
A1:   k < -1;
      take {};
      thus thesis by A1;
    end;
    suppose
A2:   k = -1;
      take {{}};
      thus thesis by A2;
    end;
    suppose
A3:   -1 < k & k < dim(p);
      -1 + 1 = 0;
      then 0 <= k by A3,INT_1:20;
      then reconsider k as Element of NAT by INT_1:16;
      set n = k + 1;
      reconsider Fn = F.n as FinSequence;
      take rng Fn;
      thus thesis by A3;
    end;
    suppose
A4:   k = dim(p);
      take {p};
      thus thesis by A4;
    end;
    suppose
A5:   k > dim(p);
      take {};
      thus thesis by A5;
    end;
  end;
  uniqueness
  proof
    set F = the PolytopsF of p;
    let X,Y be finite set such that
A6: k < -1 implies X = {} and
A7: k = -1 implies X = {{}} and
A8: (-1 < k & k < dim(p)) implies X = rng (F.(k+1)) and
A9: k = dim(p) implies X = {p} and
A10: k > dim(p) implies X = {} and
A11: k < -1 implies Y = {} and
A12: k = -1 implies Y = {{}} and
A13: (-1 < k & k < dim(p)) implies Y = rng (F.(k+1)) and
A14: k = dim(p) implies Y = {p} and
A15: k > dim(p) implies Y = {};
    per cases by XXREAL_0:1;
    suppose k < -1;
      hence thesis by A6,A11;
    end;
    suppose k = -1;
      hence thesis by A7,A12;
    end;
    suppose -1 < k & k < dim(p);
      hence thesis by A8,A13;
    end;
    suppose k = dim(p);
```

```
      hence thesis by A9,A14;
    end;
    suppose k > dim(p);
      hence thesis by A10,A15;
    end;
  end;
end;

theorem Th25:
  -1 < k & k < dim(p) implies k + 1 is Nat & 1 <= k + 1 & k + 1 <= dim(p)
proof
  assume
A1: -1 < k;
  assume
A2: k < dim(p);
  -1 + 1 = 0;
  then
A3: 0 < k + 1 by A1,XREAL_1:8;
  then reconsider n = k + 1 as Element of NAT by INT_1:16;
A4: n is Nat;
  0 qua Nat + 1 = 1;
  hence thesis by A2,A3,A4,INT_1:20;
end;

theorem Th26:
  k-polytopes(p) is non empty iff (-1 <= k & k <= dim(p))
proof
  set X = k-polytopes(p);
  thus X is non empty implies -1 <= k & k <= dim(p) by Def5;
  thus -1 <= k & k <= dim(p) implies k-polytopes(p) is non empty
  proof
    assume
A1: -1 <= k;
    assume
A2: k <= dim(p);
    per cases by A1,A2,XXREAL_0:1;
    suppose k = -1;
      hence thesis by Def5;
    end;
    suppose
A3:   -1 < k & k < dim(p);
      set F = the PolytopsF of p;
A4:   k-polytopes(p) = rng (F.(k+1)) by A3,Def5;
      set n = k + 1;
A5:   1 <= n by A3,Th25;
A6:   n <= dim(p) by A3,Th25;
      reconsider n as Element of NAT by A5,INT_1:16;
      reconsider n as Nat;
      F.n is non empty & F.n is one-to-one by A5,A6,Def3;
      hence thesis by A4;
    end;
    suppose k = dim(p);
      then k-polytopes(p) = {p} by Def5;
      hence thesis;
    end;
  end;
end;

theorem Th27:
  k < dim(p) implies k - 1 < dim(p) by XREAL_1:148,XXREAL_0:2;

:: As we defined the set of k-polytopes for all integers k, we define
:: the an incidence matrix, eta(p,k), for any integer k.  Naturally,
:: for almost all k, this is the empty matrix (empty function).  The
:: two cases in which we extend the data already given by the
:: polyhedron itself is for k = 0 and k = dim(p).  For the latter, we
:: declare that the empty set (the unique -1-dimensional polytope) is
:: incident to all 0-polytopes. For the latter, we declare that every
```

```
:: (dim(p)-1)-polytope is incidence to p, the unique dim(p)-polytope
:: of p.
definition
  let p be polyhedron, k be Integer;
  func eta(p,k) -> incidence-matrix of (k-1)-polytopes(p),k-polytopes(p) means
  :Def6:
  (k < 0 implies it = {}) &
  (k = 0 implies it = [:{{}},0-polytopes(p):] --> 1.Z_2) &
  (0 < k & k < dim(p) implies it = (the IncidenceF of p).k) &
  (k = dim(p) implies it = [:(dim(p) - 1)-polytopes(p),{p}:] --> 1.Z_2) &
  (k > dim(p) implies it = {});
  existence
  proof
    per cases by XXREAL_0:1;
    suppose
A1:   k < 0;
      (k-1)-polytopes(p) = {}
      proof
        k - 1 < 0 qua Nat - 1 by A1,XREAL_1:11;
        hence thesis by Th26;
      end;
      then
A2:   [:(k-1)-polytopes(p),k-polytopes(p):] = {} by ZFMISC_1:113;
      set f = {};
      reconsider f as Function;
      reconsider f as
      Function of [:(k-1)-polytopes(p),k-polytopes(p):],{0.Z_2,1.Z_2}
      by A2,RELSET_1:25;
      reconsider f as
      Element of Funcs([:(k-1)-polytopes(p),k-polytopes(p):],{0.Z_2,1.Z_2})
      by FUNCT_2:11;
      take f;
      thus thesis by A1;
    end;
    suppose
A3:   k > dim(p);
      then k-polytopes(p) = {} by Th26;
      then
A4:   [:(k-1)-polytopes(p),k-polytopes(p):] = {} by ZFMISC_1:113;
      set f = {};
      reconsider f as Function;
      reconsider f as
      Function of [:(k-1)-polytopes(p),k-polytopes(p):],{0.Z_2,1.Z_2}
      by A4,RELSET_1:25;
      reconsider f as
      Element of Funcs([:(k-1)-polytopes(p),k-polytopes(p):],{0.Z_2,1.Z_2})
      by FUNCT_2:11;
      take f;
      thus thesis by A3;
    end;
    suppose
A5:   0 < k & k < dim(p);
      set F = the PolytopsF of p, I = the IncidenceF of p;
      0 qua Nat + 1 = 1;
      then
A6:   1 <= k by A5,INT_1:20;
      1 - 1 = 0;
      then -1 < k - 1 & k - 1 < dim(p) by A5,A6,Th27,XREAL_1:11;
      then
A7:   (k-1)-polytopes(p) = rng (F.((k-1)+1)) by Def5;
A8:   k-polytopes(p) = rng (F.(k+1)) by A5,Def5;
      reconsider k' = k as Nat by A6,Th3;
      reconsider Ik = I.k' as incidence-matrix of (k-1)-polytopes(p),
      k-polytopes(p) by A5,A6,A7,A8,Def2;
      take Ik;
      thus thesis by A5;
```

```
    end;
    suppose
A9:   k = 0;
      per cases;
      suppose
A10:    k = dim(p);
A11:    (k-1)-polytopes(p) = {{}} by A9,Def5;
        set f = [:{{}},{p}:] --> 1.Z_2;
        reconsider f as incidence-matrix of {{}},{p} by Th24;
        reconsider f as incidence-matrix of (k-1)-polytopes(p),
        k-polytopes(p) by A10,A11,Def5;
        take f;
        thus thesis by A9,A10,Def5;
      end;
      suppose
A12:    k <> dim(p);
        set f = [:{{}},0-polytopes(p):] --> 1.Z_2;
        reconsider f as incidence-matrix of {{}},0-polytopes(p) by Th24;
        reconsider f as incidence-matrix of (k-1)-polytopes(p),
        k-polytopes(p) by A9,Def5;
        take f;
        thus thesis by A9,A12;
      end;
    end;
    suppose
A13:  k = dim(p);
      per cases;
      suppose
A14:    k = 0;
        then
A15:    (k-1)-polytopes(p) = {{}} by Def5;
        set f = [:{{}},{p}:] --> 1.Z_2;
        reconsider f as incidence-matrix of {{}},{p} by Th24;
        reconsider f as incidence-matrix of (k-1)-polytopes(p),
        k-polytopes(p) by A13,A15,Def5;
        take f;
        thus thesis by A13,A14,Def5;
      end;
      suppose
A16:    k <> 0;
        set f = [:(dim(p) - 1)-polytopes(p),{p}:] --> 1.Z_2;
        reconsider f as incidence-matrix of (dim(p) - 1)-polytopes(p),{p}
        by Th24;
        reconsider f as incidence-matrix of (k-1)-polytopes(p),
        k-polytopes(p) by A13,Def5;
        take f;
        thus thesis by A13,A16;
      end;
    end;
  end;
  uniqueness
  proof
    set I = the IncidenceF of p;
    let s,t be incidence-matrix of (k-1)-polytopes(p),k-polytopes(p) such that
A17: (k < 0 implies s = {}) and
A18: (k = 0 implies s = [:{{}},0-polytopes(p):] --> 1.Z_2) and
A19: (0 < k & k < dim(p) implies s = I.k) and
A20: (k = dim(p) implies s = [:(dim(p) - 1)-polytopes(p),{p}:] --> 1.Z_2) and
A21: (k > dim(p) implies s = {}) and
A22: (k < 0 implies t = {}) and
A23: (k = 0 implies t = [:{{}},0-polytopes(p):] --> 1.Z_2) and
A24: (0 < k & k < dim(p) implies t = I.k) and
A25: (k = dim(p) implies t = [:(dim(p) - 1)-polytopes(p),{p}:] --> 1.Z_2) and
A26: (k > dim(p) implies t = {});
    per cases by XXREAL_0:1;
    suppose k < 0;
```

```
        hence thesis by A17,A22;
      end;
      suppose k = 0;
        hence thesis by A18,A23;
      end;
      suppose 0 < k & k < dim(p);
        hence thesis by A19,A24;
      end;
      suppose k = dim(p);
        hence thesis by A20,A25;
      end;
      suppose k > dim(p);
        hence thesis by A21,A26;
      end;
    end;
end;

definition
  let p be polyhedron, k be Integer;
  func k-polytope-seq(p) -> FinSequence means
  :Def7:
  (k < -1 implies it = <*>{}) & (k = -1 implies it = <*{}*>) &
  (-1 < k & k < dim(p) implies it = (the PolytopsF of p).(k+1)) &
  (k = dim(p) implies it = <*p*>) & (k > dim(p) implies it = <*>{});
  existence
  proof
    per cases by XXREAL_0:1;
    suppose
A1:   k < -1;
      take <*>{};
      thus thesis by A1;
    end;
    suppose
A2:   k = -1;
      take <*{}*>;
      thus thesis by A2;
    end;
    suppose
A3:   -1 < k & k < dim(p);
      set F = the PolytopsF of p;
      take F.(k+1);
      thus thesis by A3;
    end;
    suppose
A4:   k = dim(p);
      take <*p*>;
      thus thesis by A4;
    end;
    suppose
A5:   k > dim(p);
      take <*>{};
      thus thesis by A5;
    end;
  end;
  uniqueness
  proof
    set F = the PolytopsF of p;
    let s,t be FinSequence such that
A6: (k < -1 implies s = <*>{}) and
A7: (k = -1 implies s = <*{}*>) and
A8: (-1 < k & k < dim(p) implies s = F.(k+1)) and
A9: (k = dim(p) implies s = <*p*>) and
A10: (k > dim(p) implies s = <*>{}) and
A11: (k < -1 implies t = <*>{}) and
A12: (k = -1 implies t = <*{}*>) and
A13: (-1 < k & k < dim(p) implies t = F.(k+1)) and
A14: (k = dim(p) implies t = <*p*>) and
```

```
A15: (k > dim(p) implies t = <*>{});
    per cases by XXREAL_0:1;
    suppose k < -1;
      hence thesis by A6,A11;
    end;
    suppose k = -1;
      hence thesis by A7,A12;
    end;
    suppose -1 < k & k < dim(p);
      hence thesis by A8,A13;
    end;
    suppose k = dim(p);
      hence thesis by A9,A14;
    end;
    suppose k > dim(p);
      hence thesis by A10,A15;
    end;
  end;
end;
definition
  let p be polyhedron, k be Integer;
  func num-polytopes(p,k) -> Element of NAT equals
  card(k-polytopes(p));
  coherence;
end;
:: It will be convenient to use these in the cases of Euler's
:: polyhedron formula that interest us.
definition
  let p be polyhedron;
  func num-vertices(p) -> Element of NAT equals
  num-polytopes(p,0);
  correctness;
  func num-edges(p) -> Element of NAT equals
  num-polytopes(p,1);
  correctness;
  func num-faces(p) -> Element of NAT equals
  num-polytopes(p,2);
  correctness;
end;
theorem Th28:
  dom (k-polytope-seq(p)) = Seg (num-polytopes(p,k))
proof
  set F = the PolytopsF of p;
  per cases;
  suppose
A1: k < -1;
    then
A2: k-polytope-seq(p) = <*>{} by Def7;
    k-polytopes(p) = {} by A1,Def5;
    hence thesis by A2,FINSEQ_1:def 3;
  end;
  suppose
A3: -1 <= k & k <= dim(p);
    per cases by A3,XXREAL_0:1;
    suppose
A4:   k = -1;
      then
A5:   k-polytopes(p) = {{}} by Def5;
A6:   k-polytope-seq(p) = <*{}*> by A4,Def7;
A7:   num-polytopes(p,k) = 1 by A5,CARD_2:60;
      len (k-polytope-seq(p)) = 1 by A6,FINSEQ_1:56;
      hence thesis by A7,FINSEQ_1:def 3;
    end;
    suppose
A8:   -1 < k & k < dim(p);
```

```
      then
A9:   k-polytope-seq(p) = F.(k+1) by Def7;
A10:  k-polytopes(p) = rng (F.(k+1)) by A8,Def5;
      set n = k + 1;
      reconsider n as Nat by A8,Th25;
      reconsider Fn = F.n as FinSequence;
      1 <= n & n <= dim(p) by A8,Th25;
      then Fn is one-to-one by Def3;
      then num-polytopes(p,k) = card (dom Fn) by A10,Th2;
      then len Fn = num-polytopes(p,k) by PRE_CIRC:21;
      hence thesis by A9,FINSEQ_1:def 3;
    end;
    suppose
A11:  k = dim(p);
      then
A12:  k-polytopes(p) = {p} by Def5;
A13:  k-polytope-seq(p) = <*p*> by A11,Def7;
A14:  num-polytopes(p,k) = 1 by A12,CARD_2:60;
      len (k-polytope-seq(p)) = 1 by A13,FINSEQ_1:56;
      hence thesis by A14,FINSEQ_1:def 3;
    end;
  end;
  suppose
A15: k > dim(p);
    then
A16: k-polytope-seq(p) = <*>{} by Def7;
    k-polytopes(p) = {} by A15,Def5;
    hence thesis by A16,FINSEQ_1:def 3;
  end;
end;

theorem Th29:
  len (k-polytope-seq(p)) = num-polytopes(p,k)
proof
  dom (k-polytope-seq(p)) = Seg (num-polytopes(p,k)) by Th28;
  hence thesis by FINSEQ_1:def 3;
end;

theorem Th30:
  rng (k-polytope-seq(p)) = k-polytopes(p)
proof
  set F = the PolytopsF of p;
  per cases;
  suppose
A1: k < -1;
    then k-polytopes(p) = {} by Def5;
    hence thesis by A1,Def7,RELAT_1:60;
  end;
  suppose
A2: -1 <= k & k <= dim(p);
    per cases by A2,XXREAL_0:1;
    suppose
A3:   k = -1;
      then
A4:   k-polytopes(p) = {{}} by Def5;
      k-polytope-seq(p) = <*{}*> by A3,Def7;
      hence thesis by A4,FINSEQ_1:55;
    end;
    suppose
A5:   -1 < k & k < dim(p);
      then k-polytopes(p) = rng (F.(k+1)) by Def5;
      hence thesis by A5,Def7;
    end;
    suppose
A6:   k = dim(p);
      then
A7:   k-polytopes(p) = {p} by Def5;
      k-polytope-seq(p) = <*p*> by A6,Def7;
```

```
      hence thesis by A7,FINSEQ_1:55;
    end;
  end;
  suppose
A8: k > dim(p);
    then k-polytopes(p) = {} by Def5;
    hence thesis by A8,Def7,RELAT_1:60;
  end;
end;

theorem Th31:
  num-polytopes(p,-1) = 1
proof
  reconsider minusone = -1 as Integer;
  minusone-polytopes(p) = {{}} by Def5;
  hence thesis by CARD_1:50;
end;

theorem Th32:
  num-polytopes(p,dim(p)) = 1
proof
  dim(p)-polytopes(p) = {p} by Def5;
  hence thesis by CARD_1:50;
end;

:: The k-polytope sets aren't really sets: they're ordered sets
:: (finite sequences).
::
:: Since the k-polytope sets are empty for k < -1 and k > dim(p), we
:: have to put a condition on n and k for the definition to make
:: sense.

definition
  let p be polyhedron, k be Integer, n be Nat;
  assume
A1: 1 <= n & n <= num-polytopes(p,k) & -1 <= k & k <= dim(p);
  func n-th-polytope(p,k) -> Element of k-polytopes(p) equals
  :Def12:
  (k-polytope-seq(p)).n;
  coherence
  proof
    n in Seg num-polytopes(p,k) by A1,FINSEQ_1:3;
    then n in dom (k-polytope-seq(p)) by Th28;
    then (k-polytope-seq(p)).n in rng (k-polytope-seq(p)) by FUNCT_1:12;
    hence thesis by Th30;
  end;
end;

theorem Th33:
  -1 <= k & k <= dim(p) implies for x being Element of k-polytopes(p)
  ex n being Nat st x = n-th-polytope(p,k) & 1 <= n & n <= num-polytopes(p,k)
proof
  assume
A1: -1 <= k & k <= dim(p);
  let x be Element of k-polytopes(p);
  per cases by A1,XXREAL_0:1;
  suppose
A2: k = -1;
    then
A3: k-polytopes(p) = {{}} by Def5;
    then
A4: x = {} by TARSKI:def 1;
    reconsider n = 1 as Nat;
    k-polytope-seq(p) = <*{}*> by A2,Def7;
    then
A5: (k-polytope-seq(p)).n = {} by FINSEQ_1:def 8;
A6: n <= num-polytopes(p,k) by A3,CARD_1:50;
    take n;
    thus thesis by A1,A4,A5,A6,Def12;
  end;
```

```
  suppose
A7: k = dim(p);
    then
A8: k-polytopes(p) = {p} by Def5;
    then
A9: x = p by TARSKI:def 1;
    reconsider n = 1 as Nat;
A10: num-polytopes(p,k) = 1 by A8,CARD_1:50;
    k-polytope-seq(p) = <*p*> by A7,Def7;
    then
A11: (k-polytope-seq(p)).n = p by FINSEQ_1:def 8;
    take n;
    thus thesis by A1,A9,A10,A11,Def12;
  end;
  suppose
A12: -1 < k & k < dim(p);
    set F = the PolytopsF of p;
A13: k-polytopes(p) = rng (F.(k+1)) by A12,Def5;
A14: k-polytope-seq(p) = F.(k+1) by A12,Def7;
    then
A15: num-polytopes(p,k) = len (F.(k+1)) by Th29;
A16: -1 + 1 < k + 1 by A12,XREAL_1:8;
A17: k + 1 <= dim(p) by A12,INT_1:20;
A18: 0 qua Nat + 1 <= k + 1 by A16,INT_1:20;
    reconsider k' = k + 1 as Element of NAT by A16,INT_1:16;
    F.k' is non empty by A17,A18,Def3;
    then rng (F.k') is non empty;
    then consider m being set such that
A19: m in dom (F.k') and
A20: (F.k').m = x by A13,FUNCT_1:def 5;
    reconsider Fk' = F.k' as FinSequence;
A21: dom Fk' = Seg (len Fk') by FINSEQ_1:def 3;
    reconsider m as Element of NAT by A19;
A22: 1 <= m & m <= len Fk' by A19,A21,FINSEQ_1:3;
    take m;
    thus thesis by A12,A14,A15,A20,A22,Def12;
  end;
end;

theorem Th34:
  k-polytope-seq(p) is one-to-one
proof
  set s = k-polytope-seq(p);
  per cases by XXREAL_0:1;
  suppose k < -1;
    hence thesis by Def7;
  end;
  suppose k = -1;
    hence thesis by Def7;
  end;
  suppose
A1: -1 < k & k < dim(p);
    set F = the PolytopsF of p;
A2: s = F.(k+1) by A1,Def7;
A3: -1 + 1 < k + 1 by A1,XREAL_1:8;
    then reconsider m = k + 1 as Element of NAT by INT_1:16;
A4: 0 qua Nat + 1 <= m by A3,INT_1:20;
    m <= dim(p) by A1,INT_1:20;
    hence thesis by A2,A4,Def3;
  end;
  suppose k = dim(p);
    then s = <*p*> by Def7;
    hence thesis;
  end;
  suppose k > dim(p);
    hence thesis by Def7;
```

```
  end;
end;
theorem Th35:
  -1 <= k & k <= dim(p) implies for m,n being Nat
  st 1 <= n & n <= num-polytopes(p,k) & 1 <= m & m <= num-polytopes(p,k)
  & n-th-polytope(p,k) = m-th-polytope(p,k) holds m = n
proof
  assume
A1: -1 <= k & k <= dim(p);
  let m,n be Nat such that
A2: 1 <= n and
A3: n <= num-polytopes(p,k) and
A4: 1 <= m and
A5: m <= num-polytopes(p,k) and
A6: n-th-polytope(p,k) = m-th-polytope(p,k);
  set s = k-polytope-seq(p);
A7: n-th-polytope(p,k) = s.n by A1,A2,A3,Def12;
A8: m-th-polytope(p,k) = s.m by A1,A4,A5,Def12;
  n in Seg (num-polytopes(p,k)) by A2,A3,FINSEQ_1:3;
  then
A9: n in dom s by Th28;
  m in Seg (num-polytopes(p,k)) by A4,A5,FINSEQ_1:3;
  then
A10: m in dom s by Th28;
  s is one-to-one by Th34;
  hence thesis by A6,A7,A8,A9,A10,FUNCT_1:def 8;
end;
definition
  let p be polyhedron, k be Integer, x be Element of (k-1)-polytopes(p),
  y be Element of k-polytopes(p);
  assume
A1: 0 <= k & k <= dim(p);
  func incidence-value(x,y) -> Element of Z_2 equals
  :Def13:
  eta(p,k).(x,y);
  coherence
  proof
    set n = eta(p,k);
A2: dom n = [:(k-1)-polytopes(p),k-polytopes(p):] by FUNCT_2:169;
A3: (k-1)-polytopes(p) <> {}
    proof
      set m = k - 1;
      0 qua Nat - 1 = -1;
      then
A4:   -1 <= m by A1,XREAL_1:11;
      m <= dim(p) - (0 qua Nat) by A1,XREAL_1:15;
      hence thesis by A4,Th26;
    end;
    k-polytopes(p) <> {} by A1,Th26;
    then
A5: [x,y] in dom n by A2,A3,ZFMISC_1:106;
A6: rng n c= {0.Z_2,1.Z_2} by FUNCT_2:169;
    n.[x,y] in rng n by A5,FUNCT_1:12;
    hence thesis by A6,BSPACE:3,5,6;
  end;
end;
begin :: The Chain Spaces and their Subspaces.  Boundary of a k-chain.
::  The set of subsets of the k-polytopes naturally forms a vector
::  space over the field Z_2.  Addition is disjoint union, and scalar
::  multiplication is defined by the equations 1*x = x, 0*x = 0.
definition
  let p be polyhedron, k be Integer;
  func k-chain-space(p) -> finite-dimensional VectSp of Z_2 equals
  bspace(k-polytopes(p));
```

```
  coherence;
end;
theorem
  for x being Element of k-polytopes(p)
  holds (0.(k-chain-space(p)))@x = 0.Z_2 by BSPACE:14;
theorem Th37:
  num-polytopes(p,k) = dim (k-chain-space(p))
proof
A1: singletons(k-polytopes(p)) is Basis of k-chain-space(p) by BSPACE:41;
  set n = dim (k-chain-space(p));
  n = card (singletons(k-polytopes(p))) by A1,VECTSP_9:def 2;
  hence thesis by BSPACE:42;
end;
:: A k-chain is a set of k-polytopes.
definition
  let p be polyhedron, k be Integer;
  func k-chains(p) -> non empty finite set equals
  bool (k-polytopes(p));
  coherence;
end;
definition
  let p be polyhedron, k be Integer, x be Element of (k-1)-polytopes(p),
  v be Element of k-chain-space(p);
  func incidence-sequence(x,v) -> FinSequence of Z_2 means
  :Def16:
  ((k-1)-polytopes(p) is empty implies it = <*>{}) &
  ((k-1)-polytopes(p) is non empty implies len it = num-polytopes(p,k)
  & for n being Nat st 1 <= n & n <= num-polytopes(p,k) holds it.n =
  (v@(n-th-polytope(p,k)))*incidence-value(x,n-th-polytope(p,k)));
  existence
  proof
    per cases;
    suppose
A1:   (k-1)-polytopes(p) is empty;
      set s = <*>{};
      rng s c= the carrier of Z_2 by XBOOLE_1:2;
      then reconsider s as FinSequence of Z_2 by FINSEQ_1:def 4;
      take s;
      thus thesis by A1;
    end;
    suppose
A2:   (k-1)-polytopes(p) is non empty;
      deffunc F(Nat) =
      (v@($1-th-polytope(p,k)))*incidence-value(x,$1-th-polytope(p,k));
      consider s being FinSequence of Z_2 such that
A3:   len s = num-polytopes(p,k) and
A4:   for n being Nat st n in dom s
      holds s.n = F(n) from FINSEQ_2:sch 1;
A5: dom s = Seg num-polytopes(p,k) by A3,FINSEQ_1:def 3;
A6:   for n being Nat st 1 <= n & n <= num-polytopes(p,k) holds s.n =
      (v@(n-th-polytope(p,k)))*incidence-value(x,n-th-polytope(p,k))
      proof
        let n be Nat such that
A7:     1 <= n and
A8:     n <= num-polytopes(p,k);
A9:     n in Seg num-polytopes(p,k) by A7,A8,FINSEQ_1:3;
        thus thesis by A4,A9,A5;
      end;
      take s;
      thus thesis by A2,A3,A6;
    end;
  end;
  uniqueness
  proof
    let s,t be FinSequence of Z_2 such that
```

```
A10: (k-1)-polytopes(p) is empty implies s = <*>{} and
A11: (k-1)-polytopes(p) is non empty implies len(s) = num-polytopes(p,k) &
    (for n being Nat st 1 <= n & n <= num-polytopes(p,k) holds s.n =
    (v@(n-th-polytope(p,k)))*incidence-value(x,n-th-polytope(p,k))) and
A12: (k-1)-polytopes(p) is empty implies t = <*>{} and
A13: (k-1)-polytopes(p) is non empty implies len(t) = num-polytopes(p,k) &
    for n being Nat st 1 <= n & n <= num-polytopes(p,k) holds t.n =
    (v@(n-th-polytope(p,k)))*incidence-value(x,n-th-polytope(p,k));
    per cases;
    suppose (k-1)-polytopes(p) is empty;
      hence thesis by A10,A12;
    end;
    suppose
A14:  (k-1)-polytopes(p) is non empty;
      for n being Nat st 1 <= n & n <= len s holds s.n = t.n
      proof
        let n be Nat such that
A15:    1 <= n and
A16:    n <= len s;
        reconsider n as Nat;
        s.n = (v@(n-th-polytope(p,k)))*incidence-value(x,n-th-polytope(p,k))
        by A11,A14,A15,A16;
        hence thesis by A11,A13,A14,A15,A16;
      end;
      hence thesis by A11,A13,A14,FINSEQ_1:18;
    end;
  end;
end;

theorem Th38:
  for c,d being Element of k-chain-space(p), x being Element of k-polytopes(p)
  holds (c+d)@x = (c@x) + (d@x)
proof
  let c,d be Element of k-chain-space(p), x be Element of k-polytopes(p);
  c+d = c \+\ d by BSPACE:def 5;
  hence thesis by BSPACE:15;
end;

theorem Th39:
  for c,d being Element of k-chain-space(p),
  x being Element of (k-1)-polytopes(p) holds incidence-sequence(x,c+d)
  = incidence-sequence(x,c) + incidence-sequence(x,d)
proof
  let c,d be Element of k-chain-space(p), x be Element of (k-1)-polytopes(p);
  set n = num-polytopes(p,k);
  set l = incidence-sequence(x,c+d);
  set isc = incidence-sequence(x,c);
  set isd = incidence-sequence(x,d);
  set r = isc + isd;
  per cases;
  suppose
A1: (k-1)-polytopes(p) is empty;
    then
A2: isc = <*>(the carrier of Z_2) by Def16;
A3: isd = <*>(the carrier of Z_2) by A1,Def16;
    reconsider isc as Element of 0-tuples_on the carrier of Z_2
    by A2,FINSEQ_2:114;
    reconsider isd as Element of 0-tuples_on the carrier of Z_2
    by A3,FINSEQ_2:114;
    isc + isd is Element of 0-tuples_on the carrier of Z_2;
    then r = <*>(the carrier of Z_2) by FINSEQ_2:113;
    hence thesis by A1,Def16;
  end;
  suppose
A4: (k-1)-polytopes(p) is non empty;
A5: len(l) = n & len(r) = n
    proof
A6:   len isc = n by A4,Def16;
```

```
A7:   len isd = n by A4,Def16;
      reconsider isc as Element of n-tuples_on the carrier of Z_2
      by A6,FINSEQ_2:110;
      reconsider isd as Element of n-tuples_on the carrier of Z_2
      by A7,FINSEQ_2:110;
      reconsider s = isc + isd as Element of n-tuples_on the carrier of Z_2;
      len s = n by FINSEQ_2:109;
      hence thesis by A4,Def16;
    end;
    for n being Nat st 1 <= n & n <= len l holds l.n = r.n
    proof
      let m be Nat such that
A8:   1 <= m and
A9:   m <= len l;
      set a = m-th-polytope(p,k);
      set iva = incidence-value(x,a);
A10:  len l = n by A4,Def16;
      then
A11:  l.m = ((c+d)@a)*iva by A4,A8,A9,Def16;
A12:  isc.m = (c@a)*iva by A4,A8,A9,A10,Def16;
A13:  isd.m = (d@a)*iva by A4,A8,A9,A10,Def16;
A14:  dom r = Seg n by A5,FINSEQ_1:def 3;
A15:  len l = n by A4,Def16;
      m in NAT by ORDINAL1:def 13;
      then m in dom r by A8,A9,A14,A15;
      then r.m = (c@a)*iva + (d@a)*iva by A12,A13,FVSUM_1:21
        .= (c@a + d@a)*iva by VECTSP_1:def 12
        .= l.m by A11,Th38;
      hence thesis;
    end;
    hence thesis by A5,FINSEQ_1:18;
  end;
end;

theorem Th40:
  for c,d being Element of k-chain-space(p),
  x being Element of (k-1)-polytopes(p)
  holds Sum (incidence-sequence(x,c) + incidence-sequence(x,d))
  = (Sum incidence-sequence(x,c)) + (Sum incidence-sequence(x,d))
proof
  let c,d be Element of k-chain-space(p), x be Element of (k-1)-polytopes(p);
  set isc = incidence-sequence(x,c);
  set isd = incidence-sequence(x,d);
  per cases;
  suppose
A1: (k-1)-polytopes(p) is empty;
    then
A2: isc = <*>(the carrier of Z_2) by Def16;
A3: isd = <*>(the carrier of Z_2) by A1,Def16;
    reconsider isc as Element of 0-tuples_on the carrier of Z_2
    by A2,FINSEQ_2:114;
    reconsider isd as Element of 0-tuples_on the carrier of Z_2
    by A3,FINSEQ_2:114;
A4: Sum isc = 0.Z_2 by FVSUM_1:93;
A5: Sum isd = 0.Z_2 by FVSUM_1:93;
    reconsider s = isc + isd as Element of 0-tuples_on the carrier of Z_2;
    Sum s = 0.Z_2 by FVSUM_1:93;
    hence thesis by A4,A5,RLVECT_1:def 7;
  end;
  suppose
A6: (k-1)-polytopes(p) is non empty;
    reconsider n = num-polytopes(p,k) as Element of NAT;
A7: len isc = n by A6,Def16;
A8: len isd = n by A6,Def16;
    reconsider isc' = isc
    as Element of n-tuples_on the carrier of Z_2 by A7,FINSEQ_2:110;
    reconsider isd' = isd
```

```
    as Element of n-tuples_on the carrier of Z_2 by A8,FINSEQ_2:110;
    Sum (isc + isd) = Sum (isc' + isd')
      .= Sum (isc) + Sum (isd) by FVSUM_1:95;
    hence thesis;
  end;
end;
theorem Th41:
  for c,d being Element of k-chain-space(p),
  x being Element of (k-1)-polytopes(p) holds Sum incidence-sequence(x,c+d)
  = (Sum incidence-sequence(x,c)) + (Sum incidence-sequence(x,d))
proof
  let c,d be Element of k-chain-space(p), x be Element of (k-1)-polytopes(p);
  Sum incidence-sequence(x,c+d)
  = Sum (incidence-sequence(x,c) + incidence-sequence(x,d)) by Th39
    .= (Sum incidence-sequence(x,c)) + (Sum incidence-sequence(x,d)) by Th40;
  hence thesis;
end;
theorem Th42:
  for c being Element of k-chain-space(p), a being Element of Z_2,
  x being Element of k-polytopes(p) holds (a*c)@x = a*(c@x)
proof
  let c be Element of k-chain-space(p), a be Element of Z_2,
  x be Element of k-polytopes(p);
  per cases by BSPACE:8;
  suppose
A1: a = 0.Z_2;
    then
A2: a*(c@x) = 0.Z_2 by VECTSP_1:39;
    a*c = 0.(k-chain-space(p)) by A1,VECTSP_1:59;
    hence thesis by A2,BSPACE:14;
  end;
  suppose
A3: a = 1.Z_2;
    then a*(c@x) = c@x by VECTSP_1:def 16;
    hence thesis by A3,VECTSP_1:def 26;
  end;
end;
theorem Th43:
  for c being Element of k-chain-space(p), a being Element of Z_2,
  x being Element of (k-1)-polytopes(p)
  holds incidence-sequence(x,a*c) = a*incidence-sequence(x,c)
proof
  let c be Element of k-chain-space(p), a be Element of Z_2,
  x be Element of (k-1)-polytopes(p);
  set l = incidence-sequence(x,a*c);
  set isc = incidence-sequence(x,c);
  set r = a*isc;
  per cases;
  suppose
A1: (k-1)-polytopes(p) is empty;
    then isc = <*>(the carrier of Z_2) by Def16;
    then reconsider isc as Element of 0-tuples_on the carrier of Z_2
    by FINSEQ_2:114;
    a*isc is Element of 0-tuples_on the carrier of Z_2;
    then reconsider r as Element of 0-tuples_on the carrier of Z_2;
    r = <*>(the carrier of Z_2) by FINSEQ_2:113;
    hence thesis by A1,Def16;
  end;
  suppose
A2: (k-1)-polytopes(p) is non empty;
    set n = num-polytopes(p,k);
A3: len l = n & len r = n
    proof
      len isc = n by A2,Def16;
      then reconsider isc as Element of n-tuples_on the carrier of Z_2
      by FINSEQ_2:110;
```

```
      set r = a*isc;
      reconsider r as Element of n-tuples_on the carrier of Z_2;
      len r = n by FINSEQ_2:109;
      hence thesis by A2,Def16;
    end;
    for m being Nat st 1 <= m & m <= len l holds l.m = r.m
    proof
      let m be Nat such that
A4:   1 <= m and
A5:   m <= len l;
      set s = m-th-polytope(p,k);
      set ivs = incidence-value(x,s);
A6:   len l = n by A2,Def16;
      then
A7:   l.m = ((a*c)@s)*ivs by A2,A4,A5,Def16;
A8:   isc.m = (c@s)*ivs by A2,A4,A5,A6,Def16;
A9:   dom r = Seg n by A3,FINSEQ_1:def 3;
A10:  len l = n by A2,Def16;
      m in NAT by ORDINAL1:def 13;
      then m in Seg n by A4,A5,A10;
      then r.m = a*((c@s)*ivs) by A8,A9,FVSUM_1:62
        .= (a*(c@s))*ivs by GROUP_1:def 4
        .= l.m by A7,Th42;
      hence thesis;
    end;
    hence thesis by A3,FINSEQ_1:18;
  end;
end;

theorem Th44:
  for c,d being Element of k-chain-space(p)
  holds c = d iff for x being Element of k-polytopes(p) holds c@x = d@x
proof
  let c,d be Element of k-chain-space(p);
  thus c = d implies for x being Element of k-polytopes(p) holds c@x = d@x;
  thus (for x being Element of k-polytopes(p) holds c@x = d@x) implies c = d
  proof
    assume
A1: for x being Element of k-polytopes(p) holds c@x = d@x;
    thus c c= d
    proof
      let x be set such that
A2:   x in c;
      reconsider c as Subset of k-polytopes(p);
      reconsider x as Element of k-polytopes(p) by A2;
      c@x = 1.Z_2 by A2,BSPACE:def 3;
      then d@x = 1.Z_2 by A1;
      hence thesis by BSPACE:9;
    end;
    thus d c= c
    proof
      let x be set such that
A3:   x in d;
      reconsider d as Subset of k-polytopes(p);
      reconsider x as Element of k-polytopes(p) by A3;
      d@x = 1.Z_2 by A3,BSPACE:def 3;
      then c@x = 1.Z_2 by A1;
      hence thesis by BSPACE:9;
    end;
  end;
end;

theorem Th45:
  for c,d being Element of k-chain-space(p) holds c = d iff
  for x being Element of k-polytopes(p) holds x in c iff x in d
proof
  let c,d be Element of k-chain-space(p);
  thus c = d
```

```
  implies for x being Element of k-polytopes(p) holds x in c iff x in d;
  thus (for x being Element of k-polytopes(p) holds x in c iff x in d)
  implies c = d
  proof
    assume
A1: for x being Element of k-polytopes(p) holds x in c iff x in d;
    assume c <> d;
    then consider x being Element of k-polytopes(p) such that
A2: c@x <> d@x by Th44;
    not (x in c iff x in d) by A2,BSPACE:13;
    hence thesis by A1;
  end;
end;

scheme
  ChainEx { p() -> polyhedron, k() -> Integer,
  P[Element of k()-polytopes(p())] } : ex c being Subset of k()-polytopes(p())
  st for x being Element of k()-polytopes(p())
  holds x in c iff (P[x] & x in k()-polytopes(p()))
proof
  set c = { x where x is Element of k()-polytopes(p()) :
  P[x] & x in k()-polytopes(p()) };
  c c= k()-polytopes(p())
  proof
    let x be set such that
A1: x in c;
    consider y being Element of k()-polytopes(p()) such that
A2: x = y and P[y] and
A3: y in k()-polytopes(p()) by A1;
    thus thesis by A2,A3;
  end;
  then reconsider c as Subset of k()-polytopes(p());
A4: for x being Element of k()-polytopes(p()) holds
  x in c iff (P[x] & x in k()-polytopes(p()))
  proof
    let x be Element of k()-polytopes(p());
    thus x in c implies (P[x] & x in k()-polytopes(p()))
    proof
      assume x in c;
      then consider y being Element of k()-polytopes(p()) such that
A5:   y = x and
A6:   P[y] and
A7:   y in k()-polytopes(p());
      thus thesis by A5,A6,A7;
    end;
    thus (P[x] & x in k()-polytopes(p())) implies x in c;
  end;
  take c;
  thus thesis by A4;
end;

:: The boundary of a k-chain v is the (k-1)-chain consisting of the
:: (k-1)-polytopes that are on the "perimeter" of v.  Being on the
:: perimeter amounts the sum of the incidence sequence being non-zero,
:: i.e., being equal to 1.

definition
  let p be polyhedron, k be Integer, v be Element of k-chain-space(p);
  func Boundary(v) -> Element of (k-1)-chain-space(p) means
  :Def17:
  ((k-1)-polytopes(p) is empty implies it = 0.((k-1)-chain-space(p))) &
  ((k-1)-polytopes(p) is non empty implies
  for x being Element of (k-1)-polytopes(p)
  holds x in it iff Sum incidence-sequence(x,v) = 1.Z_2);
  existence
  proof
    per cases;
    suppose
A1:   (k-1)-polytopes(p) is empty;
```

```
      take 0.((k-1)-chain-space(p));
      thus thesis by A1;
    end;
    suppose
   (k-1)-polytopes(p) is non empty;
      defpred Q[Element of (k-1)-polytopes(p)] means
      Sum incidence-sequence($1,v) = 1.Z_2;
      consider c being Subset of (k-1)-polytopes(p) such that
A3:   for x being Element of (k-1)-polytopes(p)
      holds x in c iff (Q[x] & x in (k-1)-polytopes(p)) from ChainEx;
      reconsider c as Element of (k-1)-chain-space(p);
      take c;
      thus thesis by A3;
    end;
  end;
  uniqueness
  proof
    let c,d be Element of (k-1)-chain-space(p) such that
A4: (k-1)-polytopes(p) is empty implies c = 0.((k-1)-chain-space(p)) and
A5: (k-1)-polytopes(p) is non empty implies
    for x being Element of (k-1)-polytopes(p)
    holds x in c iff Sum incidence-sequence(x,v) = 1.Z_2 and
 (k-1)-polytopes(p) is empty implies d = 0.((k-1)-chain-space(p)) and
A7: (k-1)-polytopes(p) is non empty implies
    for x being Element of (k-1)-polytopes(p)
    holds x in d iff Sum incidence-sequence(x,v) = 1.Z_2;
    per cases;
    suppose (k-1)-polytopes(p) is empty;
      hence thesis by A4;
    end;
    suppose
A8:   (k-1)-polytopes(p) is non empty;
      for x being Element of (k-1)-polytopes(p) holds x in c iff x in d
      proof
        let x be Element of (k-1)-polytopes(p);
        thus x in c implies x in d
        proof
          assume x in c;
          then Sum incidence-sequence(x,v) = 1.Z_2 by A5;
          hence thesis by A7,A8;
        end;
        thus x in d implies x in c
        proof
          assume x in d;
          then Sum incidence-sequence(x,v) = 1.Z_2 by A7;
          hence thesis by A5,A8;
        end;
      end;
      hence thesis by Th45;
    end;
  end;
end;

theorem Th46:
  for c being Element of k-chain-space(p),
  x being Element of (k-1)-polytopes(p)
  holds (Boundary(c))@x = Sum incidence-sequence(x,c)
proof
  let c be Element of k-chain-space(p), x be Element of (k-1)-polytopes(p);
  set b = Boundary(c);
  per cases;
  suppose
A1: (k-1)-polytopes(p) is empty;
    then
A2: Boundary(c) = 0.((k-1)-chain-space(p));
    set iscx = incidence-sequence(x,c);
    iscx = <*>(the carrier of Z_2) by A1,Def16;
```

```
      then Sum iscx = 0.Z_2 by RLVECT_1:60;
      hence thesis by A2,BSPACE:14;
    end;
    suppose
A3: (k-1)-polytopes(p) is non empty;
      then
A4: x in b iff Sum incidence-sequence(x,c) = 1.Z_2 by Def17;
      per cases;
      suppose x in b;
        hence thesis by A4,BSPACE:def 3;
      end;
      suppose
A5:     not x in b;
        then Sum incidence-sequence(x,c) <> 1.Z_2 by A3,Def17;
        then Sum incidence-sequence(x,c) = 0.Z_2 by BSPACE:8;
        hence thesis by A5,BSPACE:def 3;
      end;
    end;
end;
:: Every dimension k has its own boundary operation.
definition
  let p be polyhedron, k be Integer;
  func k-boundary(p) -> Function of k-chain-space(p),(k-1)-chain-space(p)
  means
  :Def18:
  for c being Element of k-chain-space(p) holds it.c = Boundary(c);
  existence
  proof
    defpred Q[set,set] means
    ex c being Element of k-chain-space(p) st $1 = c & $2 = Boundary(c);
A1: for x being set st x in k-chains(p) holds
    ex y being set st y in (k-1)-chains(p) & Q[x,y]
    proof
      let x be set such that
A2:   x in k-chains(p);
      reconsider x as Element of k-chain-space(p) by A2;
      set b = Boundary(x);
      take b;
      thus thesis;
    end;
    consider f being Function of k-chains(p), (k-1)-chains(p) such that
A3: for x being set st x in k-chains(p) holds Q[x,f.x] from FUNCT_2:sch 1(A1);
    reconsider f as Function of k-chain-space(p),(k-1)-chain-space(p);
A4: for c being Element of k-chain-space(p) holds f.c = Boundary(c)
    proof
      let c be Element of k-chain-space(p);
      Q[c,f.c] by A3;
      hence thesis;
    end;
    take f;
    thus thesis by A4;
  end;
  uniqueness
  proof
    let f,g be Function of k-chain-space(p),(k-1)-chain-space(p) such that
A5: for c being Element of k-chain-space(p) holds f.c = Boundary(c) and
A6: for c being Element of k-chain-space(p) holds g.c = Boundary(c);
    dom f = [#](k-chain-space(p)) by FUNCT_2:def 1;
    then
A7: dom f = dom g by FUNCT_2:def 1;
    for x being set st x in dom f holds f.x = g.x
    proof
      let x be set such that
A8:   x in dom f;
      reconsider x as Element of k-chain-space(p) by A8;
      f.x = Boundary(x) by A5;
```

```
      hence thesis by A6;
    end;
    hence thesis by A7,FUNCT_1:9;
  end;
end;

theorem Th47:
  for c,d being Element of k-chain-space(p)
  holds Boundary(c+d) = Boundary(c) + Boundary(d)
proof
  let c,d be Element of k-chain-space(p);
  set bc = Boundary(c);
  set bd = Boundary(d);
  set s = c+d;
  set l = Boundary(s);
  set r = bc+bd;
  for x being Element of (k-1)-polytopes(p) holds l@x = r@x
  proof
    let x be Element of (k-1)-polytopes(p);
A1: l@x = Sum incidence-sequence(x,s) by Th46;
      set a = bc@x;
      set b = bd@x;
A2: r@x = a+b by Th38;
A3: a = Sum incidence-sequence(x,c) by Th46;
      b = Sum incidence-sequence(x,d) by Th46;
    hence thesis by A1,A2,A3,Th41;
  end;
  hence thesis by Th44;
end;

theorem Th48:
  for a being Element of Z_2, c being Element of k-chain-space(p)
  holds Boundary(a*c) = a*(Boundary(c))
proof
  let a be Element of Z_2, c be Element of k-chain-space(p);
  set lsm = a*c;
  set l = Boundary(lsm);
  set rb = Boundary(c);
  set r = a*rb;
  for x being Element of (k-1)-polytopes(p) holds l@x = r@x
  proof
    let x be Element of (k-1)-polytopes(p);
A1: l@x = Sum incidence-sequence(x,lsm) by Th46;
A2: rb@x = Sum incidence-sequence(x,c) by Th46;
      set b = rb@x;
A3: r@x = a*b by Th42;
    incidence-sequence(x,lsm) = a*incidence-sequence(x,c) by Th43;
    hence thesis by A1,A2,A3,FVSUM_1:92;
  end;
  hence thesis by Th44;
end;

:: As defined, the k-boundary operator gives rise to a linear
:: transformation.

theorem Th49:
  k-boundary(p) is
  linear-transformation of k-chain-space(p),(k-1)-chain-space(p)
proof
  set V = k-chain-space(p);
  set b = k-boundary(p);
A1: for x,y being Element of V holds b.(x+y) = (b.x) + (b.y)
  proof
    let x,y be Element of V;
    b.(x+y) = Boundary(x+y) by Def18
      .= Boundary(x) + Boundary(y) by Th47
      .= (b.x) + Boundary(y) by Def18
      .= (b.x) + (b.y) by Def18;
    hence thesis;
```

```
  end;
  for a being Element of Z_2, x being Element of V holds b.(a*x) = a*(b.x)
  proof
    let a be Element of Z_2, x be Element of V;
    b.(a*x) = Boundary(a*x) by Def18
      .= a*(Boundary(x)) by Th48
      .= a*(b.x) by Def18;
    hence thesis;
  end;
  hence thesis by A1,MOD_2:def 5;
end;

definition
  let p be polyhedron, k be Integer;
  redefine func k-boundary(p) -> linear-transformation of k-chain-space(p),
  (k-1)-chain-space(p);
  coherence by Th49;
end;

:: The term "circuit" is used in Lakatos.  (A more customary term is
:: "cycle".)

definition
  let p be polyhedron, k be Integer;
  func k-circuit-space(p) -> Subspace of k-chain-space(p) equals
  ker (k-boundary(p));
  coherence;
end;

definition
  let p be polyhedron, k be Integer;
  func k-circuits(p) -> non empty Subset of k-chains(p) equals
  [#](k-circuit-space(p));
  coherence by VECTSP_4:def 2;
end;

definition
  let p be polyhedron, k be Integer;
  func k-bounding-chain-space(p) -> Subspace of k-chain-space(p) equals
  im ((k+1)-boundary(p));
  coherence;
end;

definition
  let p be polyhedron, k be Integer;
  func k-bounding-chains(p) -> non empty Subset of k-chains(p) equals
  [#](k-bounding-chain-space(p));
  coherence by VECTSP_4:def 2;
end;

definition
  let p be polyhedron, k be Integer;
  func k-bounding-circuit-space(p) -> Subspace of k-chain-space(p) equals
  (k-bounding-chain-space(p)) /\ (k-circuit-space(p));
  coherence;
end;

definition
  let p be polyhedron, k be Integer;
  func k-bounding-circuits(p) -> non empty Subset of k-chains(p) equals
  [#](k-bounding-circuit-space(p));
  coherence by VECTSP_4:def 2;
end;

theorem
  dim (k-chain-space(p))
  = rank (k-boundary(p)) + nullity (k-boundary(p)) by RANKNULL:44;

begin :: Simply Connected and Eulerian Polyhedra

:: The property of being simply connected is that circuits are
:: bounding, and vice versa (any bounding chain is a circuit).

definition
  let p be polyhedron;
  attr p is simply-connected means
```

```
  :Def25:
  for k being Integer holds k-circuits(p) = k-bounding-chains(p);
end;

theorem Th51:
  p is simply-connected iff for n being Integer holds n-circuit-space(p)
  = n-bounding-chain-space(p)
proof
  defpred Q[polyhedron] means for n being Integer holds n-circuit-space($1)
  = n-bounding-chain-space($1);
  thus p is simply-connected implies Q[p]
  proof
    assume
A1: p is simply-connected;
    let n be Integer;
    n-circuits(p) = n-bounding-chains(p) by A1,Def25;
    hence thesis by VECTSP_4:37;
  end;
  thus Q[p] implies p is simply-connected
  proof
    assume
A2: Q[p];
    let n be Integer;
    thus thesis by A2;
  end;
end;

definition
  let p be polyhedron;
  func alternating-f-vector(p) -> FinSequence of INT means
  :Def26:
  len(it) = dim(p) + 2 & (for k being Nat st 1 <= k & k <= dim(p) + 2
  holds it.k = ((-1)|^k)*num-polytopes(p,k-2));
  existence
  proof
    deffunc F(Nat) = ((-1)|^$1)*num-polytopes(p,$1-2);
    consider s being FinSequence of INT such that
A1: len s = dim(p) + 2 and
A2: for j being Nat st j in dom s
    holds s.j = F(j) from FINSEQ_2:sch 1;
A3: dom s = Seg(dim(p) + 2)  by A1,FINSEQ_1:def 3;
A4: for j being Nat st 1 <= j & j <= dim(p) + 2
    holds s.j = ((-1)|^j)*num-polytopes(p,j-2)
    proof
      let j be Nat such that
A5:   1 <= j and
A6:   j <= dim(p) + 2;
A7:   j in Seg (dim(p) + 2) by A5,A6,FINSEQ_1:3;
      thus thesis by A2,A7,A3;
    end;
    take s;
    thus thesis by A1,A4;
  end;
  uniqueness
  proof
    let s,t be FinSequence of INT such that
A8: len(s) = dim(p) + 2 and
A9: for k being Nat st 1 <= k & k <= dim(p) + 2
    holds s.k = ((-1)|^k)*num-polytopes(p,k-2) and
A10: len(t) = dim(p) + 2 and
A11: for k being Nat st 1 <= k & k <= dim(p) + 2
    holds t.k = ((-1)|^k)*num-polytopes(p,k-2);
    for k being Nat st 1 <= k & k <= len s holds s.k = t.k
    proof
      let k be Nat such that
A12:  1 <= k and
A13:  k <= len s;
      reconsider k as Nat;
```

```
      s.k = ((-1)|^k)*num-polytopes(p,k-2) by A8,A9,A12,A13;
      hence thesis by A8,A11,A12,A13;
    end;
    hence thesis by A8,A10,FINSEQ_1:18;
  end;
end;

definition
  let p be polyhedron;
  func alternating-proper-f-vector(p) -> FinSequence of INT means
  :Def27:
  len(it) = dim(p) & (for k being Nat st 1 <= k & k <= dim(p)
  holds it.k = ((-1)|^(k+1))*num-polytopes(p,k-1));
  existence
  proof
    deffunc F(Nat) = ((-1)|^($1+1))*num-polytopes(p,$1-1);
    consider s being FinSequence of INT such that
A1: len s = dim(p) and
A2: for j being Nat st j in dom s holds s.j = F(j) from FINSEQ_2:sch 1;
A3: dom s = Seg dim p by A1,FINSEQ_1:def 3;
A4: for j being Nat st 1 <= j & j <= dim(p)
    holds s.j = ((-1)|^(j+1))*num-polytopes(p,j-1)
    proof
      let j be Nat such that
A5:   1 <= j and
A6:   j <= dim(p);
A7:   j in Seg dim(p) by A5,A6,FINSEQ_1:3;
      thus thesis by A2,A7,A3;
    end;
    take s;
    thus thesis by A1,A4;
  end;
  uniqueness
  proof
    let s,t be FinSequence of INT such that
A8: len(s) = dim(p) and
A9: for k being Nat st 1 <= k & k <= dim(p)
    holds s.k = ((-1)|^(k+1))*num-polytopes(p,k-1) and
A10: len(t) = dim(p) and
A11: for k being Nat st 1 <= k & k <= dim(p)
    holds t.k = ((-1)|^(k+1))*num-polytopes(p,k-1);
    for k being Nat st 1 <= k & k <= len s holds s.k = t.k
    proof
      let k be Nat such that
A12:  1 <= k and
A13:  k <= len s;
      reconsider k as Nat;
      s.k = ((-1)|^(k+1))*num-polytopes(p,k-1) by A8,A9,A12,A13;
      hence thesis by A8,A11,A12,A13;
    end;
    hence thesis by A8,A10,FINSEQ_1:18;
  end;
end;

definition
  let p be polyhedron;
  func alternating-semi-proper-f-vector(p) -> FinSequence of INT means
  :Def28:
  len(it) = dim(p) + 1 & (for k being Nat st 1 <= k & k <= dim(p) + 1
  holds it.k = ((-1)|^(k+1))*num-polytopes(p,k-1));
  existence
  proof
    deffunc F(Nat) = ((-1)|^($1+1))*num-polytopes(p,$1-1);
    consider s being FinSequence of INT such that
A1: len s = dim(p) + 1 and
A2: for j being Nat st j in dom s
    holds s.j = F(j) from FINSEQ_2:sch 1;
A3: dom s = Seg(dim(p) + 1)  by A1,FINSEQ_1:def 3;
```

```
A4: for j being Nat st 1 <= j & j <= dim(p) + 1
    holds s.j = ((-1)|^(j+1))*num-polytopes(p,j-1)
    proof
      let j be Nat such that
A5:   1 <= j and
A6:   j <= dim(p) + 1;
A7:   j in Seg (dim(p) + 1) by A5,A6,FINSEQ_1:3;
      thus thesis by A2,A7,A3;
    end;
    take s;
    thus thesis by A1,A4;
  end;
  uniqueness
  proof
    let s,t be FinSequence of INT such that
A8: len(s) = dim(p) + 1 and
A9: for k being Nat st 1 <= k & k <= dim(p) + 1
    holds s.k = ((-1)|^(k+1))*num-polytopes(p,k-1) and
A10: len(t) = dim(p) + 1 and
A11: for k being Nat st 1 <= k & k <= dim(p) + 1
    holds t.k = ((-1)|^(k+1))*num-polytopes(p,k-1);
    for k being Nat st 1 <= k & k <= len s holds s.k = t.k
    proof
      let k be Nat such that
A12:  1 <= k and
A13:  k <= len s;
      reconsider k as Nat;
      s.k = ((-1)|^(k+1))*num-polytopes(p,k-1) by A8,A9,A12,A13;
      hence thesis by A8,A11,A12,A13;
    end;
    hence thesis by A8,A10,FINSEQ_1:18;
  end;
end;

theorem Th52:
  1 <= n & n <= len (alternating-proper-f-vector(p))
  implies (alternating-proper-f-vector(p)).n
  = ((-1)|^(n+1))*(dim ((n-2)-bounding-chain-space(p)))
  + ((-1)|^(n+1))*(dim ((n-1)-circuit-space(p)))
proof
  set apcs = alternating-proper-f-vector(p);
  assume
A1: 1 <= n;
  assume n <= len apcs;
  then
A2: n <= dim(p) by Def27;
  set a = (-1)|^(n+1);
  apcs.n = a*num-polytopes(p,n-1) by A1,A2,Def27
    .= a*(dim ((n-1)-chain-space(p))) by Th37
    .= a*(rank ((n-1)-boundary p) + nullity ((n-1)-boundary p)) by RANKNULL:44
    .= (a*dim ((n-2)-bounding-chain-space(p)))
  + (a*dim ((n-1)-circuit-space(p)));
  hence thesis;
end;

:: The term "eulerian" comes from Lakatos.

definition
  let p be polyhedron;
  attr p is eulerian means
  :Def29:
  Sum (alternating-proper-f-vector(p)) = 1 + (-1)|^(dim(p)+1);
end;

theorem Th53:
  alternating-semi-proper-f-vector(p)
  = alternating-proper-f-vector(p) ^ <*(-1)|^(dim(p))*>
proof
  set d = dim(p);
```

```
  set aspcs = alternating-semi-proper-f-vector(p);
  set apcs = alternating-proper-f-vector(p);
  set r = apcs ^ <*(-1)|^(dim(p))*>;
A1: len aspcs = d + 1 by Def28;
  len r = (len apcs) + (len <*(-1)|^(dim(p))*>) by FINSEQ_1:35
    .= d + (len <*(-1)|^(dim(p))*>) by Def27
    .= d + 1 by FINSEQ_1:57;
  then
A2: len aspcs = len r by Def28;
  for n being Nat st 1 <= n & n <= len aspcs holds aspcs.n = r.n
  proof
    let n be Nat such that
A3: 1 <= n and
A4: n <= len aspcs;
    per cases by A1,A4,NAT_1:8;
    suppose
A5:   n <= d;
A6:   len apcs = d by Def27;
A7:   dom apcs = Seg (len apcs) by FINSEQ_1:def 3;
      n in NAT by ORDINAL1:def 13;
      then n in dom apcs by A3,A5,A6,A7;
      then r.n = apcs.n by FINSEQ_1:def 7
        .= ((-1)|^(n+1))*num-polytopes(p,n-1) by A3,A5,Def27;
      hence thesis by A1,A3,A4,Def28;
    end;
    suppose
A8:   n = d + 1;
      then
A9:   aspcs.n = ((-1)|^(n+1))*num-polytopes(p,n-1) by A3,Def28
        .= ((-1)|^(n+1))*1 by A8,Th32
        .= (-1)|^(n+1);
      n = (len apcs) + 1 by A8,Def27;
      then r.n = (-1)|^d by FINSEQ_1:59
        .= (-1)|^(d+2) by Th14;
      hence thesis by A8,A9;
    end;
  end;
  hence thesis by A2,FINSEQ_1:18;
end;

:: Another characterization of Eulerian polyhedra

definition
  let p be polyhedron;
  redefine attr p is eulerian means
  :Def30:
  Sum (alternating-semi-proper-f-vector(p)) = 1;
  compatibility
  proof
    set apcs = alternating-proper-f-vector(p);
    set aspcs = alternating-semi-proper-f-vector(p);
    aspcs = apcs ^ <*(-1)|^(dim(p))*> by Th53;
    then
A1: Sum aspcs = (Sum apcs) + (-1)|^(dim(p)) by GR_CY_1:20;
A2: p is eulerian implies Sum aspcs = 1
    proof
      assume p is eulerian;
      then Sum aspcs = 1 + (-1)|^(dim(p)+1) + (-1)|^(dim(p)) by A1,Def29
        .= 1 + (-1)*((-1)|^(dim(p))) + (-1)|^(dim(p)) by NEWTON:11
        .= 1;
      hence thesis;
    end;
    Sum aspcs = 1 implies p is eulerian
    proof
      assume Sum aspcs = 1;
      then Sum apcs = 1 + (-1)*((-1)|^(dim(p))) by A1
        .= 1 + (-1)|^(dim(p)+1) by NEWTON:11;
      hence thesis by Def29;
```

```
    end;
    hence thesis by A2;
  end;
end;

theorem Th54:
  alternating-f-vector(p) = <*-1*> ^ alternating-semi-proper-f-vector(p)
proof
  set acs = alternating-f-vector(p);
  set aspcs = alternating-semi-proper-f-vector(p);
  set d = dim(p);
  set r = <*-1*> ^ aspcs;
A1: len r = (len <*-1*>) + (len aspcs) by FINSEQ_1:35
    .= (len <*-1*>) + (d + 1) by Def28
    .= 1 + (d + 1) by FINSEQ_1:57
    .= d + 2;
  then
A2: len acs = len r by Def26;
  for n being Nat st 1 <= n & n <= len acs holds acs.n = r.n
  proof
    let n be Nat such that
A3: 1 <= n and
A4: n <= len acs;
A5: n <= d + 2 by A4,Def26;
    per cases by A3,XXREAL_0:1;
    suppose
A6:   n = 1;
      then acs.n = ((-1)|^1)*num-polytopes(p,1-2) by A5,Def26
        .= (-1)*num-polytopes(p,-1) by NEWTON:10
        .= (-1)*1 by Th31
        .= -1;
      hence thesis by A6,FINSEQ_1:58;
    end;
    suppose
A7:   n > 1;
      then
A8:   1 - 1 < n - 1 by XREAL_1:11;
      then reconsider m = n - 1 as Element of NAT by INT_1:16;
      0 < 0 qua Nat + m by A8;
      then
A9:   1 <= m by NAT_1:19;
      n - 1 <= (d + 2) - 1 by A5,XREAL_1:11;
      then
A10:  m <= d + 1;
A11:  r.n = aspcs.(n-1)
      proof
        len <*-1*> = 1 by FINSEQ_1:56;
        hence thesis by A1,A5,A7,FINSEQ_1:37;
      end;
      aspcs.m = ((-1)|^(m+1))*num-polytopes(p,m-1) by A9,A10,Def28
        .= ((-1)|^n)*(num-polytopes(p,n-2));
      hence thesis by A3,A5,A11,Def26;
    end;
  end;
  hence thesis by A2,FINSEQ_1:18;
end;

:: Yet another characterization of eulerian polyhedra

definition
  let p be polyhedron;
  redefine attr p is eulerian means
  :Def31:
  Sum (alternating-f-vector(p)) = 0;
  compatibility
  proof
    set acs = alternating-f-vector(p);
    set aspcs = alternating-semi-proper-f-vector(p);
    acs = <*-1*> ^ aspcs by Th54;
```

```
    then
A1: Sum acs = -1 + (Sum aspcs) by Th21;
      p is eulerian implies Sum acs = 0
    proof
      assume p is eulerian;
      then Sum acs = -1 + 1 by A1,Def30
        .= 0;
      hence thesis;
    end;
    hence thesis by A1,Def30;
  end;
end;

begin :: The Extremal Chain Spaces

theorem Th55:
  0-polytopes(p) is non empty
proof
  set d = dim(p);
  per cases;
  suppose d = 0;
    then 0-polytopes(p) = {p} by Def5;
    hence thesis;
  end;
  suppose d > 0;
    hence thesis by Th26;
  end;
end;

theorem Th56:
  card [#]((-1)-chain-space(p)) = 2
proof
  (-1)-polytopes(p) = {{}} by Def5;
  then card ((-1)-polytopes(p)) = 1 by CARD_1:50;
  then card [#]((-1)-chain-space(p)) = exp(2,1) by BSPACE:43
    .= 2 by CARD_2:40;
  hence thesis;
end;

theorem Th57:
  [#]((-1)-chain-space(p)) = { {}, {{}} }
proof
  (-1)-polytopes(p) = {{}} by Def5;
  hence thesis by ZFMISC_1:30;
end;

theorem Th58:
  for x being Element of k-polytopes(p), e being Element of (k-1)-polytopes(p)
  st k = 0 & e = {} holds incidence-value(e,x) = 1.Z_2
proof
  let x be Element of k-polytopes(p),
  e be Element of (k-1)-polytopes(p) such that
A1: k = 0 and
A2: e = {};
A3: 0 <= k & k <= dim(p) by A1;
A4: eta(p,k) = [:{{}},0-polytopes(p):] --> 1.Z_2 by A1,Def6;
A5: {} in {{}} by TARSKI:def 1;
  0-polytopes(p) is non empty by A3,Th26;
  then
A6: [{},x] in [:{{}},0-polytopes(p):] by A1,A5,ZFMISC_1:106;
  incidence-value(e,x) = eta(p,k).(e,x) by A3,Def13
    .= 1.Z_2 by A2,A4,A6,FUNCOP_1:13;
  hence thesis;
end;

theorem Th59:
  for k being Integer, x being Element of k-polytopes(p),
  v being Element of k-chain-space(p), e being Element of (k-1)-polytopes(p),
  n being Nat st k = 0 & v = {x} & e = {} & x = n-th-polytope(p,k)
  & 1 <= n & n <= num-polytopes(p,k) holds incidence-sequence(e,v).n = 1.Z_2
proof
```

```
  let k be Integer, x be Element of k-polytopes(p),
  v be Element of k-chain-space(p), e be Element of (k-1)-polytopes(p),
  n be Nat such that
A1: k = 0 and
A2: v = {x} and
A3: e = {} and
A4: x = n-th-polytope(p,k) and
A5: 1 <= n and
A6: n <= num-polytopes(p,k);
  set iseq = incidence-sequence(e,v);
A7: (k-1)-polytopes(p) is non empty by A1,Def5;
A8: x in v by A2,TARSKI:def 1;
  iseq.n = (v@x)*incidence-value(e,x) by A4,A5,A6,A7,Def16
    .= (1.Z_2)*incidence-value(e,x) by A8,BSPACE:def 3
    .= (1.Z_2)*(1.Z_2) by A1,A3,Th58
    .= 1.Z_2 by VECTSP_1:def 16;
  hence thesis;
end;

theorem Th60:
  for k being Integer, x being Element of k-polytopes(p),
  e being Element of (k-1)-polytopes(p), v being Element of k-chain-space(p),
  m,n being Nat st k = 0 & v = {x} & x = n-th-polytope(p,k) & 1 <= m &
  m <= num-polytopes(p,k) & 1 <= n & n <= num-polytopes(p,k) & m <> n
  holds incidence-sequence(e,v).m = 0.Z_2
proof
  let k be Integer, x be Element of k-polytopes(p),
  e be Element of (k-1)-polytopes(p), v be Element of k-chain-space(p),
  m,n be Nat such that
A1: k = 0 and
A2: v = {x} and
A3: x = n-th-polytope(p,k) and
A4: 1 <= m and
A5: m <= num-polytopes(p,k) and
A6: 1 <= n and
A7: n <= num-polytopes(p,k) and
A8: m <> n;
  set iseq = incidence-sequence(e,v);
  -1 <= k & k <= dim(p) by A1;
  then
A9: m-th-polytope(p,k) <> x by A3,A4,A5,A6,A7,A8,Th35;
  now
    assume v@(m-th-polytope(p,k)) = 1.Z_2;
    then m-th-polytope(p,k) in {x} by A2,BSPACE:9;
    hence contradiction by A9,TARSKI:def 1;
  end;
  then
A10: v@(m-th-polytope(p,k)) = 0.Z_2 by BSPACE:11;
  (k-1)-polytopes(p) is non empty by A1,Def5;
  then iseq.m = (0.Z_2)*(incidence-value(e,m-th-polytope(p,k)))
  by A4,A5,A10,Def16
    .= 0.Z_2 by VECTSP_1:39;
  hence thesis;
end;

theorem Th61:
  for k being Integer, x being Element of k-polytopes(p),
  v being Element of k-chain-space(p), e being Element of (k-1)-polytopes(p)
  st k = 0 & v = {x} & e = {} holds Sum incidence-sequence(e,v) = 1.Z_2
proof
  let k be Integer, x be Element of k-polytopes(p),
  v be Element of k-chain-space(p),
  e be Element of (k-1)-polytopes(p) such that
A1: k = 0 and
A2: v = {x} and
A3: e = {};
  set iseq = incidence-sequence(e,v);
  -1 <= k & k <= dim(p) by A1;
```

```
  then consider n being Nat such that
A4: x = n-th-polytope(p,k) and
A5: 1 <= n and
A6: n <= num-polytopes(p,k) by Th33;
  (k-1)-polytopes(p) is non empty by A1,Def5;
  then
A7: len iseq = num-polytopes(p,k) by Def16;
  dom iseq = Seg (len iseq) by FINSEQ_1:def 3;
  then
A8: n in dom iseq by A5,A6,A7,FINSEQ_1:3;
A9: iseq.n = 1.Z_2 by A1,A2,A3,A4,A5,A6,Th59;
  for m being Nat st m in dom iseq & m <> n holds iseq.m = 0.Z_2
  proof
    let m be Nat such that
A10: m in dom iseq and
A11: m <> n;
    m in Seg (len iseq) by A10,FINSEQ_1:def 3;
    then 1 <= m & m <= len iseq by FINSEQ_1:3;
    hence thesis by A1,A2,A4,A5,A6,A7,A11,Th60;
  end;
  hence thesis by A8,A9,MATRIX_3:14;
end;
theorem Th62:
  for x being Element of 0-polytopes(p) holds (0-boundary(p)).({x}) = {{}}
proof
  let x be Element of 0-polytopes(p);
  set T = 0-boundary(p);
  reconsider minusone = 0 qua Nat - 1 as Integer;
  0-polytopes(p) is non empty by Th55;
  then reconsider v = {x} as Subset of 0-polytopes(p) by ZFMISC_1:37;
  reconsider v as Element of 0-chain-space(p);
A1: T.v = Boundary(v) by Def18;
  reconsider bv = Boundary(v) as Element of minusone-chain-space(p);
A2: minusone-polytopes(p) is non empty by Def5;
  (0 qua Nat-1)-polytopes(p) = {{}} by Def5;
  then reconsider null = {} as
  Element of (0 qua Nat-1)-polytopes(p) by TARSKI:def 1;
  null in bv iff Sum incidence-sequence(null,v) = 1.Z_2 by A2,Def17;
  then
A3: {null} c= bv by Th61,ZFMISC_1:37;
  bv c= {null}
  proof
    let y be set such that
A4: y in bv;
A5: [#](minusone-chain-space(p)) = { {}, {{}} } by Th57;
    per cases by A5,TARSKI:def 2;
    suppose bv = {};
      hence thesis by A4;
    end;
    suppose bv = {{}};
      hence thesis by A4;
    end;
  end;
  hence thesis by A1,A3,XBOOLE_0:def 10;
end;
theorem Th63:
  k = -1 implies dim(k-bounding-chain-space(p)) = 1
proof
  assume
A1: k = -1;
  set T = 0-boundary(p);
  set V = k-bounding-chain-space(p);
  card [#]V = 2
  proof
A2: T.(0.(0-chain-space(p))) = 0.(k-chain-space(p)) by A1,RANKNULL:9
      .= {};
```

```
    0-polytopes(p) <> {} by Th55;
    then consider x being set such that
A3: x in 0-polytopes(p) by XBOOLE_0:def 1;
    reconsider x as Element of 0-polytopes(p) by A3;
    set v = {x};
A4: T.v = {{}} by Th62;
A5: dom T = [#](0-chain-space(p)) by RANKNULL:7;
    reconsider v as Subset of 0-polytopes(p) by A3,ZFMISC_1:37;
    reconsider v as Element of 0-chain-space(p);
A6: v in dom T by A5;
A7: {} in rng T by A2,A5,FUNCT_1:12;
    {{}} in rng T by A4,A6,FUNCT_1:12;
    then
A8: {{},{{}}} c= rng T by A7,ZFMISC_1:38;
    card {{},{{}}} = 2 by CARD_2:76;
    then
A9: 2 c= card rng T by A8,CARD_1:27;
A10: card rng T = card (T .: [#](0-chain-space(p))) by FUNCT_2:45
      .= card [#]V by A1,RANKNULL:def 2;
    [#]V c= [#](k-chain-space(p)) by VECTSP_4:def 2;
    then card [#]V c= card [#](k-chain-space(p)) by CARD_1:27;
    then card [#]V c= 2 by A1,Th56;
    hence thesis by A9,A10,XBOOLE_0:def 10;
  end;
  hence thesis by RANKNULL:6;
end;

theorem Th64:
  card [#](dim(p)-chain-space(p)) = 2
proof
  dim(p)-polytopes(p) = {p} by Def5;
  then card (dim(p)-polytopes(p)) = 1 by CARD_1:50;
  then card [#]((dim(p))-chain-space(p)) = exp(2,1) by BSPACE:43
    .= 2 by CARD_2:40;
  hence thesis;
end;

theorem Th65:
  {p} is Element of dim(p)-chain-space(p)
proof
  dim(p)-polytopes(p) = {p} by Def5;
  hence thesis by ZFMISC_1:def 1;
end;

theorem Th66:
  {p} in [#](dim(p)-chain-space(p))
proof
  {p} is Element of dim(p)-chain-space(p) by Th65;
  hence thesis;
end;

theorem Th67:
  (dim(p) - 1)-polytopes(p) is non empty
proof
  set n = dim(p) - 1;
A1: -1 <= n
  proof
    0 qua Nat - 1 = -1;
    hence thesis by XREAL_1:11;
  end;
  n <= dim(p) by XREAL_1:148;
  hence thesis by A1,Th26;
end;

registration
  let p be polyhedron;
  cluster (dim(p)-1)-polytopes(p) -> non empty;
  coherence by Th67;
end;
```

```
theorem Th68:
  [#](dim(p)-chain-space(p)) = { 0.(dim(p)-chain-space(p)), {p} }
proof
  set V = dim(p)-chain-space(p);
  set C = [#]V;
A1: card C = 2 by Th64;
  reconsider C as finite set;
  consider a,b being set such that
A2: a <> b and
A3: C = {a,b} by A1,CARD_2:79;
  {p} in C by Th66;
  hence thesis by A2,A3,Th1;
end;

theorem Th69:
  for x being Element of dim(p)-chain-space(p)
  holds x = 0.(dim(p)-chain-space(p)) or x = {p}
proof
  set V = dim(p)-chain-space(p);
  let x be Element of V;
  x in [#]V;
  then x in { 0.V, {p} } by Th68;
  hence thesis by TARSKI:def 2;
end;

theorem Th70:
  for x,y being Element of dim(p)-chain-space(p) st x <> y
  holds x = 0.(dim(p)-chain-space(p)) or y = 0.(dim(p)-chain-space(p))
proof
  set V = dim(p)-chain-space(p);
  let x,y be Element of V such that
A1: x <> y;
  assume
A2: x <> 0.V;
  assume
A3: y <> 0.V;
  x = {p} by A2,Th69;
  hence contradiction by A1,A3,Th69;
end;

theorem
  dim(p)-polytope-seq(p) = <*p*> by Def7;

theorem Th72:
  1-th-polytope(p,dim(p)) = p
proof
  reconsider egy = 1 as Nat;
A1: egy <= num-polytopes(p,dim(p)) by Th32;
  set s = dim(p)-polytope-seq(p);
A2: s = <*p*> by Def7;
  egy-th-polytope(p,dim(p)) = s.egy by A1,Def12
    .= p by A2,FINSEQ_1:57;
  hence thesis;
end;

theorem Th73:
  for c being Element of dim(p)-chain-space(p),
  x being Element of dim(p)-polytopes(p) st c = {p} holds c@x = 1.Z_2
proof
  let c be Element of dim(p)-chain-space(p),
  x be Element of dim(p)-polytopes(p) such that
A1: c = {p};
  dim(p)-polytopes(p) = {p} by Def5;
  hence thesis by A1,BSPACE:def 3;
end;

theorem Th74:
  for x being Element of (dim(p)-1)-polytopes(p),
  c being Element of dim(p)-polytopes(p) st c = p
  holds incidence-value(x,c) = 1.Z_2
proof
```

```
  let x be Element of (dim(p)-1)-polytopes(p),
  c be Element of dim(p)-polytopes(p) such that
A1: c = p;
  set f = [:(dim(p)-1)-polytopes(p),{p}:] --> 1.Z_2;
A2: eta(p,dim(p)) = f by Def6;
A3: dom f = [:(dim(p)-1)-polytopes(p),{p}:] by FUNCOP_1:19;
  c in {p} by A1,TARSKI:def 1;
  then [x,c] in dom f by A3,ZFMISC_1:106;
  then f.(x,c) in rng f by FUNCT_1:12;
  then f.(x,c) in {1.Z_2} by FUNCOP_1:14;
  then f.(x,c) = 1.Z_2 by TARSKI:def 1;
  hence thesis by A2,Def13;
end;

theorem Th75:
  for x being Element of (dim(p)-1)-polytopes(p),
  c being Element of dim(p)-chain-space(p) st c = {p}
  holds incidence-sequence(x,c) = <*1.Z_2*>
proof
  let x be Element of (dim(p)-1)-polytopes(p),
  c be Element of dim(p)-chain-space(p) such that
A1: c = {p};
  set iseq = incidence-sequence(x,c);
  num-polytopes(p,dim(p))= 1 by Th32;
  then
A2: len iseq = 1 by Def16;
  iseq.1 = 1.Z_2
  proof
    reconsider egy = 1 as Nat;
A3: egy <= num-polytopes(p,dim(p)) by Th32;
    set z = egy-th-polytope(p,dim(p));
A4: iseq.egy = (c@z)*(incidence-value(x,z)) by A3,Def16;
A5: c@z = 1.Z_2 by A1,Th73;
    incidence-value(x,z) = 1.Z_2 by Th72,Th74; :: !!!
    hence thesis by A4,A5,VECTSP_1:def 16;
  end;
  hence thesis by A2,FINSEQ_1:57;
end;

theorem Th76:
  for x being Element of (dim(p)-1)-polytopes(p),
  c being Element of dim(p)-chain-space(p) st c = {p}
  holds Sum incidence-sequence(x,c) = 1.Z_2
proof
  let x be Element of (dim(p)-1)-polytopes(p),
  c be Element of dim(p)-chain-space(p) such that
A1: c = {p};
  incidence-sequence(x,c) = <*1.Z_2*> by A1,Th75;
  hence thesis by FINSOP_1:12;
end;

:: The boundary operation applied to the unique non-zero vector of the
:: dim(p)-chain space gives the "top" vector of the (dim(p)-1)-chain
:: space.  In other words, every (dim(p)-1)-polytope is incidence to
:: the whole polyhedron.

theorem Th77:
  (dim(p)-boundary(p)).{p} = (dim(p)-1)-polytopes(p)
proof
  set T = dim(p)-boundary(p);
  set X = (dim(p)-1)-polytopes(p);
  reconsider c = {p} as Element of dim(p)-chain-space(p) by Th65;
  reconsider d = X as Element of (dim(p)-1)-chain-space(p) by ZFMISC_1:def 1;
  reconsider Tc = T.c as Element of (dim(p)-1)-chain-space(p);
  for x being Element of X holds x in Tc iff x in d
  proof
    let x be Element of X;
    thus x in Tc implies x in d;
    thus x in d implies x in Tc
```

```
      proof
        assume x in d;
        Sum incidence-sequence(x,c) = 1.Z_2 by Th76;
        then x in Boundary(c) by Def17;
        hence thesis by Def18;
      end;
    end;
    hence thesis by SUBSET_1:8;
  end;
  theorem Th78:
    dim(p)-boundary(p) is one-to-one
  proof
    set T = dim(p)-boundary(p);
    set U = (dim(p) - 1)-chain-space(p);
    set V = dim(p)-chain-space(p);
    set B = {p};
    assume not T is one-to-one;
    then consider x1,x2 being set such that
  A1: x1 in dom T and
  A2: x2 in dom T and
  A3: T.x1 = T.x2 and
  A4: x1 <> x2 by FUNCT_1:def 8;
    reconsider x1 as Element of V by A1;
    reconsider x2 as Element of V by A2;
    per cases by A4,Th70;
    suppose
  A5: x1 = 0.V;
      then
  A6: x2 = B by A4,Th69;
      T.x1 = 0.U by A5,RANKNULL:9;
      hence thesis by A3,A6,Th77;
    end;
    suppose
  A7: x2 = 0.V;
      then
  A8: x1 = B by A4,Th69;
      T.x2 = 0.U by A7,RANKNULL:9;
      hence thesis by A3,A8,Th77;
    end;
  end;
  theorem Th79:
    dim ((dim(p)-1)-bounding-chain-space(p)) = 1
  proof
    set d = dim(p);
    set T = d-boundary(p);
    set U = d-chain-space(p);
    set V = (d-1)-bounding-chain-space(p);
  A1: T is one-to-one by Th78;
  A2: card [#]V = card (T .: [#]U) by RANKNULL:def 2
      .= card (rng T) by FUNCT_2:45;
    card (dom T) = card [#]U by RANKNULL:7
      .= 2 by Th64;
    then card [#]V = 2 by A1,A2,Th2;
    hence thesis by RANKNULL:6;
  end;
  theorem Th80:
    p is simply-connected implies dim ((dim(p)-1)-circuit-space(p)) = 1
  proof
    assume
  A1: p is simply-connected;
    set d = dim(p);
    set U = (d-1)-bounding-chain-space(p);
    set V = (d-1)-circuit-space(p);
    U = V by A1,Th51;
    hence thesis by Th79;
  end;
```

```
theorem Th81:
  1 < n & n < dim(p) + 2 implies (alternating-f-vector(p)).n
  = (alternating-proper-f-vector(p)).(n-1)
proof
  assume
A1: 1 < n;
  assume
A2: n < dim(p) + 2;
  set acs = alternating-f-vector(p);
  set apcs = alternating-proper-f-vector(p);
A3: acs.n = ((-1)|^n)*num-polytopes(p,n-2) by A1,A2,Def26;
  0 <= n - 1
  proof
    1 - 1 = 0;
    hence thesis by A1,XREAL_1:15;
  end;
  then reconsider m = n - 1 as Element of NAT by INT_1:16;
  reconsider m as Nat;
A4: 1 <= m
  proof
A5: 2 <= n
    proof
      1 + 1 = 2;
      hence thesis by A1,INT_1:20;
    end;
    2 - 1 = 1;
    hence thesis by A5,XREAL_1:15;
  end;
  m <= dim(p)
  proof
    n < (dim(p) + 1) + 1 by A2;
    then n <= dim(p) + 1 by NAT_1:13;
    then n - 1 <= (dim(p) + 1) - 1 by XREAL_1:11;
    hence thesis;
  end;
  then apcs.m = ((-1)|^(m+1))*num-polytopes(p,m-1) by A4,Def27;
  hence thesis by A3;
end;

theorem Th82:
  alternating-f-vector(p)
  = <*-1*> ^ alternating-proper-f-vector(p) ^ <*(-1)|^(dim(p))*>
proof
  set acs = alternating-f-vector(p);
  set apcs = alternating-proper-f-vector(p);
  set r = <*-1*> ^ apcs ^ <*(-1)|^(dim(p))*>;
  set n = dim(p);
A1: len acs = n + 2 by Def26;
A2: len apcs = n by Def27;
A3: len r = (len <*-1*>) + (len apcs) + (len <*(-1)|^(dim(p))*>) by Th16;
A4: len <*-1*> = 1 by FINSEQ_1:56;
A5: len <*(-1)|^(dim(p))*> = 1 by FINSEQ_1:56;
  for k being Nat st 1 <= k & k <= len acs holds acs.k = r.k
  proof
    let k be Nat such that
A6: 1 <= k and
A7: k <= len acs;
    per cases by A1,A6,A7,XXREAL_0:1;
    suppose
A8:   k = 1;
A9:   1 <= n + 2 by Th12;
      reconsider o = 1 as Nat;
      o - 2 = -1;
      then
A10:  acs.o = ((-1)|^o)*num-polytopes(p,-1) by A9,Def26;
A11:  (-1)|^1 = -1 by Th4,Th9;
      num-polytopes(p,-1) = 1 by Th31;
```

```
        hence thesis by A8,A10,A11,Th17;
      end;
      suppose
A12:  k = n + 2;
        then 1 <= k by Th12;
        then
A13:  acs.k = ((-1)|^k)*num-polytopes(p,k-2) by A12,Def26;
A14:  r.k = (-1)|^k
        proof
          k = (len <*-1*> + len (apcs) + 1)
          proof
            len <*-1*> = 1 by FINSEQ_1:56;
            hence thesis by A2,A12;
          end;
          then r.k = (-1)|^(dim(p)) by Th18
            .= (-1)|^k by A12,Th14;
          hence thesis;
        end;
        num-polytopes(p,k-2) = 1 by A12,Th32;
        hence thesis by A13,A14;
      end;
      suppose
A15:  1 < k & k < n + 2;
        set m = k - 1;
A16:  len <*-1*> = 1 by FINSEQ_1:56;
        k <= len (<*-1*> ^ apcs)
        proof
A17:    len (<*-1*> ^ apcs) = (len <*-1*> + len apcs) by FINSEQ_1:35
            .= n + 1 by A2,FINSEQ_1:56;
A18:    k + 1 <= n + 2 by A15,INT_1:20;
A19:    (k + 1) - 1 = k;
          (n + 2) - 1 = n + 1;
          hence thesis by A17,A18,A19,XREAL_1:11;
        end;
        then r.k = apcs.m by A15,A16,Th19;
        hence thesis by A15,Th81;
      end;
    end;
    hence thesis by A1,A2,A3,A4,A5,FINSEQ_1:18;
end;

begin :: A Generalized Euler Relation and its 1-, 2-, and 3-dimensional Special Cases

theorem Th83:
  dim(p) is odd implies Sum (alternating-f-vector(p))
  = Sum (alternating-proper-f-vector(p)) - 2
proof
  assume
A1: dim(p) is odd;
  set acs = alternating-f-vector(p);
  set apcs = alternating-proper-f-vector(p);
A2: acs = <*-1*> ^ apcs ^ <*(-1)|^(dim(p))*> by Th82;
A3: (-1)|^(dim(p)) = -1 by A1,Th9;
  reconsider minusone = -1 as Integer;
  reconsider lastterm = (-1)|^(dim(p)) as Integer;
  Sum acs = (Sum <*minusone*>) + (Sum apcs) + (Sum <*lastterm*>) by A2,Th22
    .= (Sum <*minusone*>) + (Sum apcs) + (-1) by A3,RVSUM_1:103
    .= (-1) + (Sum apcs) + (-1) by RVSUM_1:103
    .= (Sum apcs) - 2;
  hence thesis;
end;

theorem Th84:
  dim(p) is even implies Sum (alternating-f-vector(p))
  = Sum (alternating-proper-f-vector(p))
proof
  assume
A1: dim(p) is even;
  set acs = alternating-f-vector(p);
```

```
  set apcs = alternating-proper-f-vector(p);
A2: acs = <*-1*> ^ apcs ^ <*(-1)|^(dim(p))*> by Th82;
A3: (-1)|^(dim(p)) = 1 by A1,Th8;
  reconsider minusone = -1 as Integer;
  reconsider lastterm = (-1)|^(dim(p)) as Integer;
  Sum acs = (Sum <*minusone*>) + (Sum apcs) + (Sum <*lastterm*>) by A2,Th22
    .= (Sum <*minusone*>) + (Sum apcs) + 1 by A3,RVSUM_1:103
    .= (-1) + (Sum apcs) + 1 by RVSUM_1:103
    .= Sum apcs;
  hence thesis;
end;

theorem Th85:
  dim(p) = 1 implies Sum alternating-proper-f-vector(p) = num-polytopes(p,0)
proof
  assume
A1: dim(p) = 1;
  set apcs = alternating-proper-f-vector(p);
A2: len apcs = 1 by A1,Def27;
  reconsider egy = 1 as Nat;
A3: apcs.egy = (-1)|^(egy+1)*num-polytopes(p,egy-1) by A1,Def27;
  (-1)|^(egy+1) = 1 by Th5,Th8;
  then apcs = <*num-polytopes(p,0)*> by A2,A3,FINSEQ_1:57;
  hence thesis by RVSUM_1:103;
end;

theorem Th86:
  dim(p) = 2 implies Sum alternating-proper-f-vector(p)
  = num-polytopes(p,0) - num-polytopes(p,1)
proof
  assume
A1: dim(p) = 2;
  set apcs = alternating-proper-f-vector(p);
A2: len apcs = 2 by A1,Def27;
  reconsider o = 1 as Nat;
  reconsider t = 2 as Nat;
A3: apcs.o = ((-1)|^(o+1))*num-polytopes(p,o-1) by A1,Def27;
A4: apcs.t = ((-1)|^(t+1))*num-polytopes(p,t-1) by A1,Def27;
A5: (-1)|^(o+1) = 1 by Th5,Th8;
A6: (-1)|^(t+1) = -1 by Th6,Th9;
  reconsider apcso = apcs.o as Integer;
  reconsider apcst = apcs.t as Integer;
A7: apcs = <*apcso,apcst*> by A2,FINSEQ_1:61;
  Sum apcs = apcso + apcst by A7,RVSUM_1:107
    .= num-polytopes(p,0) - num-polytopes(p,1) by A3,A4,A5,A6;
  hence thesis;
end;

theorem Th87:
  dim(p) = 3 implies Sum alternating-proper-f-vector(p)
  = num-polytopes(p,0) - num-polytopes(p,1) + num-polytopes(p,2)
proof
  assume
A1: dim(p) = 3;
  set apcs = alternating-proper-f-vector(p);
A2: len apcs = 3 by A1,Def27;
  reconsider o = 1 as Nat;
  reconsider tw = 2 as Nat;
  reconsider th = 3 as Nat;
  reconsider mo = -1 as Integer;
A3: (-1)|^(o+1) = 1 by Th5,Th8;
A4: (-1)|^(tw+1) = -1 by Th6,Th9;
A5: (-1)|^(th+1) = 1 by Th7,Th8;
A6: apcs.o = o*num-polytopes(p,o-1) by A1,A3,Def27;
A7: apcs.tw = mo*num-polytopes(p,tw-1) by A1,A4,Def27;
A8: apcs.th = o*num-polytopes(p,th-1) by A1,A5,Def27;
  reconsider apcson = apcs.o as Integer;
  reconsider apcstw = apcs.tw as Integer;
  reconsider apcsth = apcs.th as Integer;
```

```
A9: apcs = <*apcson,apcstw,apcsth*> by A2,FINSEQ_1:62;
  Sum apcs = apcson + apcstw + apcsth by A9,RVSUM_1:108
    .= num-polytopes(p,0)
  - num-polytopes(p,1) + num-polytopes(p,2) by A6,A7,A8;
  hence thesis;
end;

:: A trivial special case

theorem Th88:
  dim(p) = 0 implies p is eulerian
proof
  set d = dim(p);
  assume
A1: d = 0;
  set apcs = alternating-proper-f-vector(p);
  (-1)|^(d+1) = -1 by A1,NEWTON:10;
  then
A2: 1 + (-1)|^(d+1) = 0;
  len apcs = 0 by A1,Def27;
  then apcs = <*>INT;
  hence thesis by A2,Def29,GR_CY_1:22;
end;

theorem Th89:
  p is simply-connected implies p is eulerian
proof
  assume
A1: p is simply-connected;
  set apcs = alternating-proper-f-vector(p);
  per cases;
  suppose dim(p) = 0;
    hence thesis by Th88;
  end;
  suppose dim(p) > 0;
    then
A2: len apcs > 0 by Def27;

:: Split the alternating characteristic sequence into a sum of two
:: sequences, a and b
    deffunc A(Nat) = ((-1)|^($1+1))*(dim (($1-2)-bounding-chain-space(p)));
    deffunc B(Nat) = ((-1)|^($1+1))*(dim (($1-1)-circuit-space(p)));
    consider a being FinSequence such that
A3: len a = len apcs and
A4: for n being Nat st n in dom a holds a.n = A(n) from FINSEQ_1:sch 2;
    consider b being FinSequence such that
A5: len b = len apcs and
A6: for n being Nat st n in dom b holds b.n = B(n) from FINSEQ_1:sch 2;
    rng a c= INT & rng b c= INT
    proof
      thus rng a c= INT
      proof
        let y be set such that
A7:     y in rng a;
        consider x being set such that
A8:     x in dom a and
A9:     y = a.x by A7,FUNCT_1:def 5;
        reconsider x as Element of NAT by A8;
        a.x = ((-1)|^(x+1))*(dim ((x-2)-bounding-chain-space(p))) by A4,A8;
        hence thesis by A9;
      end;
      thus rng b c= INT
      proof
        let y be set such that
A10:    y in rng b;
        consider x being set such that
A11:    x in dom b and
A12:    y = b.x by A10,FUNCT_1:def 5;
        reconsider x as Element of NAT by A11;
```

```
        b.x = ((-1)|^(x+1))*(dim ((x-1)-circuit-space(p))) by A6,A11;
        hence thesis by A12;
      end;
    end;
    then reconsider a,b as FinSequence of INT by FINSEQ_1:def 4;
A13: for n being Nat st 1 <= n & n <= len apcs holds apcs.n = a.n + b.n
    proof
      let n be Nat such that
A14:  1 <= n and
A15:  n <= len apcs;
A16:  apcs.n = ((-1)|^(n+1))*(dim ((n-2)-bounding-chain-space(p)))
      + ((-1)|^(n+1))*(dim ((n-1)-circuit-space(p))) by A14,A15,Th52;
      reconsider n' = n as Element of NAT by ORDINAL1:def 13;
A17:  n' in dom b by A14,A15,FINSEQ_3:27,A5;
      n' in dom a by A14,A15,FINSEQ_3:27,A3;
      then a.n' = ((-1)|^(n'+1))*(dim ((n'-2)-bounding-chain-space(p))) by A4;
      hence thesis by A6,A16,A17;
    end;
:: Now we want to how that the alternating characterstic sequence is
:: a telescoping sum of the sequences a and b.  First, we establish
:: the necessary relation among the sequences a and b.
    for n being Nat st 1 <= n & n < len apcs holds b.n = -(a.(n+1))
    proof
      let n be Nat such that
A18:  1 <= n and
A19:  n < len apcs;
A20:  n in dom b by A18,A19,FINSEQ_3:27,A5;
      reconsider n as Element of NAT by ORDINAL1:def 13;
A21:  b.n = ((-1)|^(n+1))*(dim ((n-1)-circuit-space(p))) by A6,A20;
A22:  n + 1 <= len apcs by A19,INT_1:20;
      1 <= n + 1 by NAT_1:11;
      then n + 1 in dom a by A22,FINSEQ_3:27,A3;
      then a.(n+1) = A(n+1) by A4
        .= (((-1)|^(n+1))*((-1)|^1))*(dim ((n-1)-bounding-chain-space(p)))
      by NEWTON:13
        .= ((-1)|^(n+1))*(-1)*(dim ((n-1)-bounding-chain-space(p)))
      by NEWTON:10
        .= -((-1)|^(n+1))*(dim ((n-1)-bounding-chain-space(p)))
        .= -(b.n) by A1,A21,Th51;
      hence thesis;
    end;
    then
A23: Sum apcs = (a.1) + (b.(len apcs)) by A2,A3,A5,A13,Th15;
A24: a.1 = 1
    proof
      reconsider egy = 1 as Element of NAT;
      1 <= 0 qua Nat + 1;
      then egy <= len apcs by A2,NAT_1:13;
      then egy in dom a by FINSEQ_3:27,A3;
      then a.egy = ((-1)|^(1+1))*(dim ((egy-2)-bounding-chain-space(p))) by A4
        .= 1*(dim ((egy-2)-bounding-chain-space(p))) by Th5,Th8
        .= 1 by Th63;
      hence thesis;
    end;
    b.(len apcs) = (-1)|^(dim(p)+1)
    proof
      reconsider n = len apcs as Element of NAT;
A25:  n = dim(p) by Def27;
      0 qua Nat + 1 = 1;
      then 1 <= len apcs by A2,NAT_1:13;
      then n in dom b by FINSEQ_3:27,A5;
      then b.n = B(n) by A6
        .= ((-1)|^(n+1))*1 by A1,A25,Th80
        .= (-1)|^(n+1);
      hence thesis by Def27;
    end;
```

```
    hence thesis by A23,A24,Def29;
  end;
end;

:: Euler's Polyhedron Formula in One Dimension: simply-connected
:: 1-dimensional polyhedra are just line segments.

theorem
  p is simply-connected & dim(p) = 1 implies num-vertices(p) = 2
proof
  assume
A1: p is simply-connected;
  assume
A2: dim(p) = 1;
  set acs = alternating-f-vector(p);
  set apcs = alternating-proper-f-vector(p);
  p is eulerian by A1,Th89;
  then 0 = Sum acs by Def31
    .= Sum apcs - 2 by A2,Th4,Th83
    .= num-polytopes(p,0) - 2 by A2,Th85;
  hence thesis;
end;

:: Euler's Polyhedron Formula in Two Dimensions: polygons have exactly
:: as many vertices as edges.

theorem
  p is simply-connected & dim(p) = 2 implies num-vertices(p) = num-edges(p)
proof
  assume
A1: p is simply-connected;
  assume
A2: dim(p) = 2;
A3: p is eulerian by A1,Th89;
  set s = num-polytopes(p,0) - num-polytopes(p,1);
A4: s = Sum(alternating-proper-f-vector(p)) by A2,Th86;
  set c = alternating-f-vector(p);
  0 = Sum c by A3,Def31
    .= s by A2,A4,Th5,Th84;
  hence thesis;
end;

:: Euler's Polyhedron Formula in Three Dimensions: V - E + F = 2.

theorem
  p is simply-connected & dim(p) = 3
  implies num-vertices(p) - num-edges(p) + num-faces(p) = 2
proof
  assume
A1: p is simply-connected;
  assume
A2: dim(p) = 3;
A3: p is eulerian by A1,Th89;
  set s = num-polytopes(p,0) - num-polytopes(p,1) + num-polytopes(p,2);
A4: s = Sum(alternating-proper-f-vector(p)) by A2,Th87;
  set c = alternating-f-vector(p);
  0 = Sum c by A3,Def31
    .= s - 2 by A2,A4,Th6,Th83;
  hence thesis;
end;
```

C References

[1] I. Lakatos, *Proofs and Refutations: The Logic of Mathematical Discovery*. (Cambridge University Press, 1976).

[2] G. Peano, *Formulaire de mathématique*. (Bocca frères, Ch. Clausen, Turin, 1895).

[3] M. Davis, *A program for Presburger's algorithm*, in *Proceedings of the Summer Institute of Symbolic Logic at Cornell University* (1957), p. 215.

[4] J. McCarthy, *Computer programs for checking mathematical proofs*, in *Proceedings of the Fifth Symposium in Pure Mathematics* (American Mathematical Society, 1961), pp. 219–227.

[5] N. de Bruijn, *A survey of the project* AUTOMATH, in *To H. B. Curry: Essays on Combinatory Logic, Lambda Calculus and Formalism*, edited by J. R. Hindley and J. P. Seldin (Academic Press, 1980).

[6] L. van Bentham-Jutting, *Checking Landau's Grundlagen in the* AUTOMATH *system* Tech. Rep. 83, Mathematisch Centrum, Amsterdam (1979).

[7] R. S. Boyer and J. S. Moore, *A Computational Logic*. (Academic Press, 1980).

[8] M. Kaufmann, P. Manolios, and J. S. Moore, *Computer-Aided Reasoning: An Approach*. (Kluwer Academic Publishers, 2000).

[9] G. W. Leibniz, *Dissertatio de arte combinatorica*, Ph.D. thesis, Universität Altdorf, (1666).

[10] R. Zach, *Hilbert's program*. In *Stanford Encyclopedia of Philosophy*, edited by E. N. Zalta (Fall 2003). Available online at http://plato.stanford.edu/archives/fall2003/entries/hilbert-program/.

[11] J. Avigad, *Computers in mathematical inquiry*. In [137] . Forthcoming.

[12] J. Avigad, *Understanding proofs*. In [137] . Forthcoming.

[13] J. Avigad, *Mathematical method and proof*, Synthese **153** (2006), 105–159.

[14] N. Shankar, *Metamathematics, Machines, and Gödel's Proof*, volume 38 of *Camridge Tracts in Theoretical Computer Science*. (Camridge University Press, 1994).

[15] A. Korniłowicz, *Jordan curve theorem*, Formalized Mathematics **13**(4) (2005), 481–491.

[16] T. C. Hales, *The Jordan Curve Theorem, formally and informally*, American Mathematical Monthly **114**(10) (2007), 882–894.

[17] G. Gonthier, *A computer-checked proof of the four-color theorem* Tech. Rep., Microsoft Research.

[18] J. Avigad, K. Donnelly, D. Gray, and P. Raff, *A formally verified proof of the prime number theorem*, ACM Transactions on Computational Logic **9**(1:2) (2007), 1–23.

[19] F. Wiedijk, *100 theorems*, Available online at http://www.cs.ru.nl/~freek/100/.

[20] *The QED Manifesto*, in *Automated Deduction - CADE 12* (Springer-Verlag, 1994), vol. 814 of *Lecture Notes in Artificial Intelligence*, pp. 238–251.

[21] J. Harrison, *Formal proof—theory and practice*, Notices of the American Mathematical Society **55**(11) (2008), 1395–1406.

[22] MIZAR, Available online at http://www.mizar.org.

[23] Hol Light, Available online at http://www.cl.cam.ac.uk/~jrh13/hol-light/.

[24] coq, Available online at http://coq.inria.fr/.

[25] K. Appel and W. Haken, *Every planar map is four-colorable*, Illinois Journal of Mathematics **21** (1977a), 439–567.

[26] J. Borwein and D. Bailey, *Mathematics by Experiment: Plausible Reasoning in the 21st Century*. (A. K. Peters, 2004).

[27] J. Borwein, D. Bailey, and R. Girgensohn, *Experimentation in Mathematics: Computational Paths to Discovery*. (A. K. Peters, 2004).

[28] T. Tymoczko, *The four-color problem and its philosphical significance*, The Journal of Philosophy **76**(2) (1979), 57–83.

[29] E. R. Swart, *The philosophical implications of the four-color problem*, The American Mathematical Monthly **87**(9) (1980), 697–707.

[30] M. Detlefsen, *The four-color theorem and mathematical proof*, The Journal of Philosophy **77**(12) (1980), 803.

[31] D. Bailey and J. Borwein, *Experimental mathematics: examples, methods and implications*, Notices of the American Mathematical Society **52** (2005), 502–514.

[32] T. S. Kuhn, *The Structure of Scientific Revolutions*. (University of Chicago Press, 1996), 3rd ed.

[33] E. Glas, *Kuhn, Lakatos, and the image of mathematics*, Philosophia Mathematica **3**(3) (1995), 225–247.

[34] D. MacKenzie, *Slaying the Kraken: The sociohistory of a mathematical proof*, Social Studies of Science **29**(1) (1999), 7–60.

[35] A. D. Aczel, *Fermat's Last Theorem*. (Four Walls Eight Windows, 1996).

[36] T. C. Hales, *An overview of the Kepler Conjecture* (2002a).

[37] Editors of the *Annals of Mathematics*, *Editors' statements* (2006).

[38] T. C. Hales, *The* flyspeck *project*, Available online at http://www.math.pitt.edu/~thales/flyspeck/.

[39] R. De Millo, R. J. Lipton, and A. J. Perlis, *Social processes and proofs of theorems and programs*, Communications of the ACM **22**(5) (1979), 271–280.

[40] G. Pólya, *Mathematics and Plausible Reasoning*. (Princeton University Press, 1954).

[41] G. Pólya, *Mathematics and Plausible Reasoning: Patterns of Plausible Inference*, volume 2. (Princeton University Press, 1968), 2ndnd ed.

[42] G. Pólya, *Mathematical Discovery: On Understanding, Learning and Teaching Problem Solving*. (John Wiley & Sons, 1981), Combined ed. Forward by Peter Hilton.

[43] I. Lakatos, *Proofs and refutations*, British Journal for the Philosophy of Science **14** (1963–1964), 1–25, 120–139, 221–245, 296–342. In four parts.

[44] G. Pólya, *How to Solve It: A New Aspect of Mathematical Method*. (Princeton University Press, 1948/1985), 2nd ed.

[45] I. Lakatos, *Essays in the Logic of Mathematical Discovery*, Ph.D. thesis, Cambridge University, (1961).

[46] I. Lakatos, *Infinite regress and the foundations of mathematics*, Supplementary Volume of the Proceedings of the Aristotelian Society **36** (1962), 155–184. With an erratum.
[47] I. Lakatos, *A renaissance of empiricism in the recent philosophy of mathematics?* In [138] . Comments on the discussion following Kalmár's presentation [139].
[48] I. Lakatos, *What does a mathematical proof prove?* (1998), Revised and Expanded ed., p. 153–162. [140]
[49] I. Lakatos, *Analysis-Synthesis—a Heuristic Starting Point of Research Programmes in Failed Attempts of Refutations* (1978). Volume 2 of [141]
[50] P. Davis and R. Hersh, *The Mathematical Experience.* (Cambridge University Press, 1980).
[51] D. Bloor, *Polyhedra and the abominations of Leviticus*, British Journal for the Philosophy of Science **11**(3) (1978), 245–272.
[52] B. Larvor, *Lakatos: An Introduction.* (Routledge, 1998).
[53] W. V. O. Quine, *Review of Proofs and Refutations*, British Journal for the Philosophy of Science **28** (1977), 81–82.
[54] S. Feferman, *The logic of mathematical discovery versus the logical structure of mathematics*, in *PSA: Proceedings of the Biennial Meeting of the Philosophy of Science Association* (1978), pp. 309–327.
[55] D. Sherry, *On mathematical error*, Studies in History and Philosophy of Science **28**(3) (1997), 393–416.
[56] B. Larvor, *What is dialectical philosophy of mathematics?*, Philosophia Mathematica **9**(3) (2001a), 212–229.
[57] P. Kitcher and W. Aspray, *An opinionated introduction.* In [58] , p. 3–57.
[58] W. Aspray and P. Kitcher (eds.), *History and Philosophy of Modern Mathematics* Number 11 in Minnesota Studies in the Philosophy of Science. (University of Minnesota Press, 1988).
[59] M. Leng, *Phenomenology and mathematical practice*, Philosophia Mathematica **10**(3) (2002), 3–25.
[60] Y. Rav, *Why do we prove theorems?*, Philosophia Mathematica **7**(1) (1999), 5–41.
[61] Y. Rav, *A critique of a formalist-mechanist version of the justification of arguments in mathematicians' proof practices*, Philosophia Mathematica **15**(3) (2007), 291–320.
[62] D. Corfield, *Towards a Philosophy of Real Mathematics.* (Cambridge University Press, 2003).
[63] R. Hersh, *Introducing Imre Lakatos*, Mathematical Intelligencer **1**(3) (1978), 148–151.
[64] P. J. Davis and R. Hersh, *Rhetoric and mathematics.* In *The Rhetoric of the Human Sciences: Language and Argument in Scholarship and Public Affairs*, edited by J. S. Nelson, A. Megill, and D. N. McCloskey (University of Wisconsin Press, 1987), p. 52–68.
[65] R. Hersh, *Mathematics has a front and a back*, Synthese **88** (1991b), 127–133.
[66] R. Hersh, *Fresh breezes in the philosophy of mathematics*, American Mathematical Monthly **102**(7) (1995), 589–594.

[67] R. Hersh, *Prove—once more and again*, Philosophia Mathematica **5**(2) (1997), 153–165.
[68] R. Hersh, *Some proposals for reviving the philosophy of mathematics.* In [140] , p. 10–28.
[69] R. Hersh (ed.), *18 Unconventional Essays on the Nature of Mathematics* (Springer, 2006).
[70] I. Kant, *Prolgomena to Any Future Metaphysics that will be Able to Come Forward as Science.* (Cambridge University Press, 1783/2004), Revised ed. Translation and introduction by Gary Hatfield, with selections from the *Critique of Pure Reason.*
[71] H. Friedman, *Adventures in the formalization of mathematics* (2006). Talk given at the Ohio State University Computer Science Colloquium, June 8, 2006.
[72] J. Harrison, *A short history of automated reasoning*, in *Algebraic Biology 2007*, edited by H. Anai, K. Horimoto, and T. Kutsia (Springer, 2007), vol. 4545 of *Lecture Notes in Computer Science*, pp. 334–349.
[73] T. Burge, *Content preservation*, The Philosophical Review **102**(4) (1993), 457–488.
[74] T. Burge, *Computer proof, apriori knowledge, and other minds*, Nôus **32** (1998), 1–37. Supplement: Philosophical Perspectives 12: Language, Mind and Ontology.
[75] H. Lehman, *An examination of Imre Lakatos' philosophy of mathematics*, Philosophical Forum **12** (1980), 33–48.
[76] I. Hacking, *Imre Lakatos' philosophy of science*, British Journal for the Philosophy of Science **30** (1979), 381–410.
[77] J. Kadvany, *Imre Lakatos and the Guises of Reason.* (Duke University Press, 2001).
[78] P. J. Davis, *Fidelity in mathematical discourse: Is one and one really two?*, American Mathematical Monthly **79**(3) (1972), 252–263.
[79] T. Koetsier, *Lakatos' Philosophy of Mathematics: A Historical Approach.* (North-Holland, 1991).
[80] A. P. Juskevich and E. Winter (eds.), *Leonhard Euler und Christian Goldbach: Briefwechsel 1729-1764* (Akademie-Verlag, Berlin, 1965).
[81] M. Spivak, *A Comprehensive Introduction to Differential Geometry.* (Publish or Perish, 1999), 3rd ed. (5 vols.)
[82] P. Hilton and J. Pedersen, *Descartes, Euler, Poincaré, Pólya—and polyhedra*, L'Enseignement Mathématique (IIe Série) **27**(3-4) (1981), 327–343.
[83] E. Sandifer, *How Euler did it: V, E and F (Part 2)*, MAA Online (2004b)
[84] L. Euler, *Elementa doctrinae solidorum*, Novi Commentarii Academiae Scientarum Petropolitanae **4** (1758a), 109–140.
[85] L. Euler, *Demonstratio nonnullarum insignium proprietatum quibus solida hedris planis inclusa sunt praedita*, Novi Commentarii Academiae Scientarum Petropolitanae **4** (1758b), 94–108.
[86] H. Poincaré, *Sur la généralisation d'un théorème d'Euler relatif aux polyèdres*, Comptes Rendus de Séances de l'Academie des Sciences **117** (1893), 144.
[87] H. Poincaré, *Complément à l'analysis situs*, Rendiconti del Circolo Matematico di Palermo **13** (1899), 285–343.

[88] B. Grünbaum, *Polyhedra with hollow faces*, NATO-ASI Series C Mathematical and Physical Sciences **440** (1994b), 43–70.
[89] H. S. M. Coxeter, *Regular Polytopes*. (Dover Publications, 1973).
[90] J.-F. Dufourd, *Polyhedra genus theorem and Euler formula: A hypermap-formalized intuitionistic proof*, Theoretical Computer Science **403**(2-3) (2008), 133–159.
[91] J. Alama, *The rank+nullity theorem*, Formalized Mathematics **15**(3) (2007), 137–142.
[92] J. Alama, *The vector space of subsets of a set based on symmetric difference*, Formalized Mathematics **16**(1) (2008), 1–6.
[93] J. Alama, *Euler's polyhedron formula*, Formalized Mathematics **16**(1) (2008), 7-19. In press.
[94] S. Lang, *Algebra*, volume 211 of *Graduate Texts in Mathematics*. (Springer, 2002).
[95] W. A. Trybulec, *Operations on subspaces in vector space*, Formalized Mathematics **1**(5) (1990), 871–876.
[96] W. Trybulec, *Linear combinations in a vector space*, Formalized Mathematics **1**(5) (1990), 877–882.
[97] M. Żynel, *The Steinitz theorem and the dimension of a vector space*, Formalized Mathematics **5**(3) (1996), 423–428.
[98] W. A. Trybulec, *Basis of vector space*, Formalized Mathematics **1**(5) (1990), 883–885.
[99] A. Brøndsted, *An Introduction to Convex Polytopes*. (Springer, 1983).
[100]
[101] E. H. Spanier, *Algebraic Topology*. (Springer-Verlag, 1968).
[102] A. Blass, *Existence of bases implies the axiom of choice*. In *Axiomatic Set Theory*, edited by J. E. Baumgartner, D. A. Martin, and S. Shelah , number 31 in Contemporary Mathematics Series (American Mathematical Society, 1984), p. 31–33.
[103] S. G. Simpson, *Subsystems of Second Order Arithmetic*. (Springer, 1999).
[104] J. Urban, *XML-izing* MIZAR*: Making semantic processing and presentation of* MML *easy*, in *MKM 2005: Mathematical Knowledge Management* (2005).
[105] P. Hájek and P. Pudlák, *Metamathematics of First-Order Arithmetic*. (Springer-Verlag, 1993).
[106] F. Wiedijk, *A proposed syntax for binders in* MIZAR. Available online at http://www.cs.ru.nl/~freek/mizar/binder.pdf.
[107] D. Gries and F. B. Schneider, *A Logical Approach to Discrete Math*. (Springer, 1993).
[108] D. D. Knuth, *Two notes on notation*, American Mathematical Monthly **99**(5) (1992), 403–422.
[109] C. Francese and D. Richeson, *The flaw in Euler's proof of his polyhedral formula*, American Mathematical Monthly **114** (2007), 286–296.
[110] N. L. Biggs, E. K. Lloyd, and R. J. Wilson, *Graph Theory: 1736-1936*. (Oxford University Press, 1976).
[111] H. Samelson, *In defense of Euler*, L'Enseignement Mathématique **42** (1996), 377–382.

[112] B. Grünbaum, *Convex Polytopes*, volume 221 of *Graduate Texts in Mathematics*. (Springer, 2003), 2nd ed.
[113] B. Lindström, *On the realization of convex polytopes, Euler's formula and Möbius functions*, Aequationes Mathematicae **6**(2-3) (1971), 235–240.
[114] L. Libkin, *Elements of Finite Model Theory*. (Springer-Verlag, 2004).
[115] B. Grünbaum, *Graphs of polyhedra; polyhedra as graphs*, Discrete Mathematics **307** (2007), 445–463.
[116] E. Steinitz and H. Rademacher, *Vorlesungen über die Theorie der Polyeder unter Einschluss der Elemente der Topologie*. (Springer, New York, 1976). Reprint of the original 1934 edition.
[117] K. Kunen, *Set Theory: An Introduction to Independence Proofs*. (North-Holland, 1980).
[118] H. E. Rose, *Subrecursion: Functions and Hierarchies*, volume 9 of *Oxford Logic Guides*. (Clarendon Press, Oxford, 1984).
[119] J. Avigad, *Number theory and elementary arithmetic*, Philosophia Mathematica **11** (2003), 257–284.
[120] J. Azzouni, *The derivation-indicator view of mathematical practice*, Philosophia Mathematica **12** (2004), 81–106.
[121] W. V. O. Quine, *Mathematical Logic*. (Harvard University Press, 1951), 2nd ed.
[122] J. Worrall, *Lakatos, Imre* (Macmillan Reference, 2006), 2nd ed., vol. 5, pp. 171–175.
[123] E. Glas, *The 'Popperian Programme' and mathematics. Part I: The fallibilist logic of mathematical discovery*, Studies in History and Philosophy of Science **32**(1) (2001a), 119–137.
[124] E. Glas, *The 'Popperian Programme' and mathematics. Part II: From quasi-empiricism to mathematical research programmes*, Studies in History and Philosophy of Science **32**(2) (2001b), 355–376.
[125] I. Grattan-Guinness, *Lakatos and the philosophy of mathematics and science. on popper's philosophy and its prospects*, British Journal for the Philosophy of Science **12**(3) (1979), 317–337. Review of [141].
[126] G. Currie, *Lakatos's philosophy of mathematics*, Synthese **42**(2) (1979), 335–351. Review of [1].
[127] F. Portoraro, *Automated reasoning*. In *Stanford Encyclopedia of Philosophy*, edited by E. N. Zalta (Fall 2008). Available online at http://plato.stanford.edu/archives/fall2008/entries/reasoning-automate%␣d/.
[128] W. McCune, *Solution of the Robbin's problem*, Journal of Automated Reasoning **19** (1997), 263–276.
[129] B. Fitelson, *Using Mathematica to understand the computer proof of the Robbins Conjecture*, Mathematica in Education and Research **7**(1) (1997), 17–26.
[130] D. Fallis, *Intentional gaps in mathematical proofs*, Synthese **134** (2003), 45–69.
[131] G. Gonthier, *Formal proof—the four-color theorem*, Notices of the American Mathematical Society **55**(11) (2008), 1382–1393.

[132] D. W. Barnette and B. Grünbaum, *On Steinitz's theorem concerning convex* 3-*polytopes and on some properties of planar graphs*, in *The Many Facets of Graph Theory: Conference Proceedings, Western Michigan University, Kalamazoo, Michigan, October 31-November 2, 1968.*, edited by G. Cartrand and S. F. Kapoor (Springer, 1968), pp. 27–40.

[133] W. A. Trybulec, *Subgroup and cosets of subgroups. lagrange theorem*, Formalized Mathematics **1**(5) (1990), 855–864.

[134] W. V. O. Quine, *Word and Object*. (MIT Press, 1964).

[135] W. V. O. Quine, *On the reasons for indeterminacy of translation*, Journal of Philosophy **67**(6) (1970), 178–183.

[136] W. V. O. Quine, *Indeterminacy of translation again*, Journal of Philosophy **84**(1) (1987), 5–10.

[137] P. Mancosu (ed.), *The Philosophy of Mathematical Practice*. Forthcoming.

[138] I. Lakatos, ed., *Problems in the Philosophy of Mathematics* (North-Holland, 1967).

[139] L. Kalmár, *Foundations of mathematics–whither now?* In [138] , pp. 187–194.

[140] T. Tymoczko (ed.), *New Directions in the Philosophy of Mathematics: An Anthology* (Princeton University Press, 1998), Revised and Expanded ed.

[141] I. Lakatos, *Mathematics, Science, and Epistemology: Philosophical Papers*, volume 2. (Cambridge University Press, 1978).