TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 279, Number 1, September 1983

COHOMOLOGY DETECTS FAILURES OF THE AXIOM OF CHOICE

BY

ANDREAS BLASS[1]

ABSTRACT. We propose that failures of the axiom of choice, that is, surjective functions admitting no sections, can be reasonably classified by means of invariants borrowed from algebraic topology. We show that cohomology, when defined so that its usual exactness properties hold even in the absence of the axiom of choice, is adequate for detecting failures of this axiom in the following sense. If a set X, viewed as a discrete space, has trivial first cohomology for all coefficient groups, then every X-indexed family of nonempty sets has a choice function. We also obtain related results when the coefficient groups are required to be abelian or well-orderable. In particular, we show that, if all discrete spaces have trivial first cohomology for all abelian coefficient groups, then the axiom of choice holds.

Introduction. The axiom of choice, in one of its many equivalent forms, asserts that, for any surjective function p, from a set Y onto a set X, there exists a section, i.e., a map $s\colon X \to Y$ with $p \circ s = \mathrm{id}_X$. A formally similar concept, the existence (or, more often, nonexistence) of continuous sections for continuous surjections, is one of the central concerns of algebraic topology, and topologists have created an impressive arsenal of sophisticated tools for analyzing it. It therefore seems reasonable to try to use these tools to describe the ways in which the axiom of choice can fail. The sets and functions that are relevant to the axiom of choice can be viewed as topological spaces and continuous functions, and thus brought formally within the domain of algebraic topology, by simply giving all of the sets the discrete topology.

An obvious difficulty with this project is that the homotopy, homology, and cohomology groups of discrete spaces all vanish, under the usual definitions, in all positive dimensions, whether or not the axiom of choice holds. One can circumvent this difficulty by using more exotic invariants, such as K-theory, but we shall adopt a more radical approach. We shall argue, in §1, that the usual definitions of cohomology are appropriate only in the presence of the axiom of choice; in its absence they fail to satisfy some simple exactness conditions. We therefore propose to adopt a definition of cohomology due to Giraud [3] which has the expected exactness properties even if the axiom of choice is false. With this definition, or indeed with any definition having a certain (rather tiny) amount of exactness, we can at least make a start on the project of using cohomology to describe failures of the axiom of

Received by the editors October 7, 1981 and, in revised form, September 15, 1982.
1980 *Mathematics Subject Classification.* Primary 03E25, 55N99.
Key words and phrases. Axiom of choice, cohomology, torsor, permutation model.
[1]Partially supported by NSF grant MCS 8101560.

©1983 American Mathematical Society
0002-9947/82/0000-0939/$04.50

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

choice. Our main theorem asserts that, if the first cohomology of every discrete space vanishes, for all coefficient groups, then the axiom of choice holds; in other words, cohomology (in dimension 1) is adequate for detecting failures of choice. This theorem improves a result of Diaconescu [**1**], who obtained the same conclusion from the assumption that both the first and second cohomology of a discrete space vanish for all (not necessarily constant) systems of coefficient groups.

After proving the main theorem, in §2, we devote the remaining sections to similar theorems in which the coefficient groups are subject to additional requirements, specifically abelianness and well-orderability.

The results in this paper, showing that cohomology detects failures of the axiom of choice, lend support to the hope that cohomology could be used to describe or classify such failures. Further support can be found in some calculations of cohomology of specific sets in certain models of set theory where choice fails; see §6 for an example. But the problem of giving a useful cohomological description of failures of choice remains open.

In the later sections of this paper, we shall need to consider some weakened forms of the axiom of choice, which we define and briefly discuss now to avoid interruptions later. For each positive integer n, we let $AC(n)$ be the statement that every surjection $p\colon Y \to X$ whose fibers $Y_x = p^{-1}\{x\}$ all have exactly n elements admits a section, in other words, that we can choose from n-element sets. Similarly, $AC(\text{finite})$ asserts the existence of sections for all surjections with finite fibers. The meaning of $AC(< n)$, $AC(\leqslant n)$, etc. should now be clear. AC, without any parenthetical restriction, is the full axiom of choice. Note that $AC(< n)$ and $AC(n)$ together imply $AC(\leqslant n)$, for each of the two hypotheses provides a partial section defined on the appropriate part of X, and the union of these partial sections is then a complete section. By induction, we conclude that $AC(\leqslant n)$ follows from (and is therefore equivalent to) the conjunction of $AC(2), AC(3), \ldots, AC(n)$. However, if $AC(n)$ holds for all finite n, we cannot conclude that $AC(\text{finite})$ holds. Although the hypothesis guarantees the existence of partial sections over each appropriate part $\{x \in X \mid Y_x$ has n elements$\}$ of X, we cannot select such a partial section for each n without invoking the axiom of choice. Of course, we do not need the full strength of AC; we need only $N - AC$, which asserts that every surjection to the set N of positive integers has a section, i.e., that we can make countably many choices. We use the notations $X - AC$, $X - AC(n)$, etc. similarly, for any set X. For more information about these weak axioms of choice, including, for example, a model of set theory where $AC(\text{finite})$ fails while every $AC(n)$ holds, see Jech's book [**5**], and the work of Truss [**7**].

1. Cohomology. We indicated in the introduction that the usual definitions of cohomology, by which we mean singular or Čech or simplicial or de Rham cohomology, are inappropriate for our purposes and in fact lack some of the expected exactness properties of cohomology when the axiom of choice fails. Specifically, let $0 \to A \to B \to C \to 0$ be a short exact sequence, and let X be an arbitrary set, viewed as a discrete space. Then any of the cohomology theories listed

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

above will make $H^0(X, A) = A^X$ and similarly for B and C. (In the case of de Rham cohomology, we assume that A, B, C are real vector spaces.) Since H^1 is trivial for X, the long cohomology sequence contains the segment $B^X \to C^X \to 0$. Exactness would require that every function from X to C lifts to B, a requirement that is easily seen to involve the axiom of choice. In fact, standard techniques for producing models of set theory without choice make it easy to produce situations where the required lifting does not exist and so the long sequence is not exact. Thus, if one wants to do cohomology theory without assuming the axiom of choice, one must choose between having long exact sequences and having trivial cohomology for discrete spaces. In this paper, I choose the former and analyze the failure of the latter. The other option may also be useful, perhaps for geometrical purposes such as measuring genuinely topological obstructions to liftings, as opposed to set-theoretical obstructions due to the failure of choice. But the focus in this paper is precisely on these set-theoretical obstructions. (Irrelevant exercise: Formulate the definition of Čech cohomology for general spaces so that it makes sense without the axiom of choice. The difficulty lies in passing from a cover to a refinement without being able to choose, for each set in the refinement, a superset in the original cover.)

Giraud [**3**] introduced a definition of cohomology (in the very general context of cohomology of sites with coefficients in a sheaf of groups) which, when specialized to topological spaces, agrees with Čech cohomology provided the axiom of choice holds, but which, even in the absence of choice, yields long exact sequences. These properties of Giraud cohomology indicate that it will serve our purposes, and they, along with other results in [**3**] (for example the description in terms of derived functors) seem to support the thesis that Giraud's definition is the correct one when the axiom of choice is not available.

We shall not need Giraud's definition for arbitrary topological spaces (much less for the situation treated in [**3**]) but only for discrete spaces, henceforth to be identified with their underlying sets. Furthermore, we shall need cohomology only in dimension 1. Let X be a set and let G be a group. A *G-torsor* over X is a set T equipped with a projection p onto X and a right action of G, written $(t, g) \to tg$, such that, in addition to the axioms for a group action (namely $(tg)h = t(gh)$ and $t1 = t$), the following hold. First $p(tg) = p(t)$ for all $t \in T$ and $g \in G$, and second, if $p(t) = p(u)$ then there is a unique $g \in G$ with $tg = u$. (In other words, G acts sharply transitively on the fibers of p.) Two G-torsors T and T' are *isomorphic* if there is a bijection $f\colon T \to T'$ commuting with the projections and G-actions ($p'(f(t)) = p(t)$ and $f(t)g = f(tg)$). $H^1(X, G)$ is the set of isomorphism classes of G-torsors over X.

In any G-torsor T over X, each of the fibers $T_x = p^{-1}\{x\}$ is in one-to-one correspondence with G. Indeed, if t is any element of T_x, then $g \mapsto tg$ is such a correspondence. If the axiom of choice holds, then there is a section s of p, selecting one element $s(x)$ from each fiber T_x and enabling us to define an isomorphism to T from the torsor $X \times G$ (with projection $(x, g) \mapsto x$ and action $((x, g), h) \mapsto (x, gh)$) by applying the preceding sentence in every fiber: $(x, g) \mapsto s(x)g$. Thus, the axiom of choice implies that $H^1(X, G)$ is trivial, i.e., consists of just one element. The same

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

argument shows that any torsor that has a section (meaning a section of p) is trivial (meaning isomorphic to $X \times G$); the converse is obvious, since $X \times G$ has sections, for example $x \mapsto (x, 1)$, and isomorphisms preserve them. Thus, to say that a torsor is trivial is just to say that it has a section, and to say that $H^1(X, G)$ is trivial is to say that all G-torsors over X have sections.

Readers who are willing to accept Giraud's definition of H^1 (for discrete spaces) can proceed directly to §2. For readers who, like the referees of an earlier version of this paper, find this definition too complex or esoteric to be of interest, we indicate that, whenever one of our theorems uses "$H^1(X, G)$ is trivial" as a hypothesis, it is permissible to interpret H^1 as referring, not specifically to Giraud cohomology, but to *any* cohomology theory possessing certain minimal exactness properties, to be specified below. The reason for this is that, if such a theory has $H^1(X, G)$ trivial, then so does Giraud's. In some of our proofs, however (specifically proof B of the main Theorem 1 and the proof of the lemma on which all of §3 is based), one could easily work directly with exactness properties and avoid torsors altogether; we have refrained from doing so in the interest of simplicity.

In order to specify the exactness requirements on a cohomology theory that it must satisfy in order for our theorems to be applicable, we begin by recalling some facts about H^0 with nonconstant coefficients. If $G = (G_x)_{x \in X}$ is a family indexed by a (discrete) set X, then $H^0(X, G) = \prod_{x \in X} G_x$ is the set of functions on X whose value at x lies in G_x for each x. Note that this makes sense even if the G_x are not groups but merely sets. Of course then H^0 is not a group either; in general, H^0 inherits whatever algebraic structure the G_x carry. For our cohomology theories we require that $H^1(X, G)$ be (at least) a pointed set, that is, a set with a specified element, whenever G is a group. (We need H^1 only for constant coefficients.) The exactness requirement is that, if $\mathbf{H} = (H_x)_{x \in X}$ is a system of groups, each having G as a subgroup, and if $\mathbf{H}/G = (H_x/G)_{x \in X}$ is the associated system of left-coset spaces then

$$H^0(X, \mathbf{H}) \to H^0(X, \mathbf{H}/G) \xrightarrow{d} H^1(X, G)$$

is an exact sequence (of pointed sets), i.e., an element of $H^0(X, \mathbf{H}/G)$ maps to the distinguished element of $H^1(X, G)$ if and only if it is the image of an element of $H^0(X, \mathbf{H})$ under the map of H^0 induced by the projection from $\mathbf{H}$ to $\mathbf{H}/G$. Note that no properties of the connecting map d, other than its existence and the exactness requirement, are assumed.

To justify our claim that any such cohomology theory can be used in place of Giraud's in the hypotheses of our theorems, we show that the triviality of $H^1(X, G)$ for such a theory implies the triviality of all G-torsors on X. Assume that $H^1(X, G)$ is trivial, that H^1 has the exactness property above, and that T is a G-torsor on X. We define a system $\mathbf{H}$ of groups by letting H_x be the group generated by the disjoint union of G and T_x subject to relations of the following two sorts:

(a) for any two elements of G, their product is as computed in G;

(b) for any $g \in G$ and $t \in T_x$, the product tg is as computed in T.

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

The obvious map from G to H_x is a homomorphism by (a) and it is easily seen to be one-to-one. (In fact, for each x, H_x is the free product of G with the infinite cyclic group generated by any element of T_x, but this identification cannot be done for all x simultaneously since we do not know that we can choose elements from all the T_x simultaneously.) The relations (b) guarantee that T_x is, for each x, a left coset of G in H_x. The function that assigns to each $x \in X$ this coset T_x is thus an element of $H^0(X, \mathbf{H}/G)$. Since $H^1(X, G)$ is trivial, exactness requires that this element lifts to an element s of $H^0(X, \mathbf{H})$. But such an element is a function assigning to each $x \in X$ an element of the coset T_x in H_x. It is therefore a section of T, so T is trivial, as required.

Notice that the preceding argument used only half of the exactness assumption (kernel included in image) so we could, if we were so inclined, weaken our hypotheses on cohomology theories by dropping the other half of exactness.

It should also be pointed out that, when (as in §§3 and 5) we deal with abelian coefficient groups, we no longer need to consider nongroup coefficients in H^0; it suffices to assume exactness (as above) when G and all the H_x are abelian groups (so the H_x/G are also abelian groups). To see this, simply repeat the preceding argument using abelian groups everywhere. This means in particular that the elements of G will commute with those of T_x in H_x, so H_x is now the direct (rather than free) product of G with an infinite cyclic group.

2. Trivial cohomology implies choice. This section is devoted to the proof of the main result stated in the introduction.

THEOREM 1. *Let X be a set such that $H^1(X, G)$ is trivial for all groups G. Then every surjection to X admits a section, i.e., $X - AC$ holds.*

COROLLARY. *The axiom of choice is equivalent to the assertion that $H^1(X, G)$ is trivial for all discrete spaces X and all groups G.*

We shall give two proofs of Theorem 1, because they admit generalizations in different directions. The first proof is similar in some respects to Diaconescu's earlier proof [**1**] of the axiom of choice from the assumption that $H^1(X, G)$ and $H^2(X, G)$ are trivial for all discrete spaces X and all systems of groups G.

PROOF A. We must show that every surjection $p\colon Y \to X$ has a section. We do this first for the special case that all the fibers $Y_x = p^{-1}\{x\}$ have the same size; that is, we assume that there is a nonempty set S admitting bijections to every fiber. (If we could put a group structure on S, and if we could choose, for each $x \in X$, a sharply transitive action of S on Y_x, then Y would be an S-torsor and the hypothesis about $H^1(X, S)$ would yield the desired conclusion. Unfortunately, there seems to be no way to make S a group or choose appropriate actions on the fibers without AC.) Let G be the group of all permutations of S, and, for each $x \in X$, let T_x be the set of bijections $t\colon S \to Y_x$. Let G act on T_x by composition: $tg = t \circ g$. T_x is nonempty, by the hypothesis of the special case under consideration, and, for any t and u in T_x, there is a unique $g \in G$ with $u = tg$, namely $g = t^{-1} \circ u$. Therefore, the union T of the sets T_x, equipped with the action of G in each T_x and with the obvious projection

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

to X (sending T_x to x), is a G-torsor over X. By hypothesis, it has a section s, i.e., a function assigning to each $x \in X$ a bijection $s(x)\colon S \to Y_x$. Then, for any $a \in S$, the function $x \mapsto s(x)(a)$ is a section of p. This completes the proof of the special case.

We finish the proof by reducing the general case to the special one. So let $p\colon Y \to X$ be an arbitrary surjection. Define S to be the set of all finite sequences of elements of Y; for each $x \in X$, define U_x to be the set of those sequences in S that begin with an element of Y_x. Clearly, $U_x \subseteq S$, and, just as clearly, S can be mapped one-to-one into U_x by fixing an element of Y_x and adjoining it at the beginning of every sequence in S. By the Schröder-Bernstein theorem (which fortunately is provable without AC; see [**5**, p. 23]), each U_x is in one-to-one correspondence with S. So, by the special case that has already been proved, there is a function s assigning to each $x \in X$ a sequence in U_x. By assigning to each x the first element of this sequence $s(x)$, we obtain a section for p. □

The second proof of Theorem 1 is a slight variation of a technique I used (in 1976, unpublished) to eliminate the H^2 hypothesis from Diaconescu's theorem; I failed to notice then that only a slight variation was needed to reduce the hypothesis from "systems of groups" to "groups".

PROOF B. Let $p\colon Y \to X$ be given, and let F be the free group generated by Y. Thus, an element of F is a word, a finite formal product of elements of Y and their formal inverses, which is reduced in the sense that no element of Y occurs adjacent to its own inverse; words are multiplied by concatenating them and canceling until a reduced word is obtained. For any word w and any element $x \in X$, we let $E(w, x)$ be the number of $y \in Y_x$ occurring in w minus the number of inverses of such y's (counted with multiplicity); it is the total exponent of elements of Y_x in w. (A more modern definition is that $E(-, x)$ is the unique homomorphism from F to the additive group of integers that sends each element of Y_x to 1 and each element of $Y - Y_x$ to 0.) We define

$$G = \{w \in F \mid \text{for all } z \in X,\ E(w, z) = 0\}$$

and, for each $x \in X$,

$$T_x = \{w \in F \mid \text{for all } z \in X - \{x\},\ E(w, z) = 0 \text{ but } E(w, x) = 1\}.$$

Thus, G is a (normal) subgroup of F, and each T_x is a coset of G. The right action of G on each T_x, by multiplication in F, is sharply transitive, and each T_x is nonempty (containing the words y of length 1 for $y \in Y_x$). So $\bigcup_{x \in X} T_x$ (with the projection sending T_x to x) is a G-torsor over X. By hypothesis, it has a section s. For each $x \in X$, $s(x)$ is a word in which, since $E(s(x), x) = 1$, at least one $y \in Y_x$ occurs. Let $s'(x)$ be the first such y, first in the ordering of the word $s(x)$. Then s' is a section of p. □

3. Abelian groups. Since coefficient groups in algebraic topology are usually taken to be abelian (partly because then H^1 admits a natural group structure), and since both proofs of Theorem 1 relied on the use of nonabelian groups, it seems natural to ask whether Theorem 1 remains true if one assumes only that $H^1(X, G)$ is trivial for all abelian groups G. I do not know the answer to the question, but I conjecture that

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

it is negative. Nevertheless, the corollary to Theorem 1 does remain true when only abelian groups are considered (Theorem 3 below). The following lemma isolates the main step in the proofs of this theorem and of another adaptation (Theorem 2) of Theorem 1 to the abelian situation.

LEMMA. *Assume that X is a set such that $H^1(X, G)$ is trivial for all abelian groups G. Let $p\colon Y \to X$ be a surjection each of whose fibers has at least two elements. Then there is a function σ assigning to each $x \in X$ a nonempty finite proper subset $\sigma(x)$ of $p^{-1}\{x\}$.*

PROOF. Proceed as in Proof B of Theorem 1, using the free abelian group F_{ab} on Y in place of the free group. The only difference between F_{ab} and F is that words differing only in the order of factors count as the same word in F_{ab}. The proof works exactly as before up to and including the existence of the function s. But s' cannot be defined as before, since there is no longer any order within the word $s(x)$ that would allow us to pick out one of the appropriate y's. Instead, we take them all, defining

$$\sigma(x) = \{y \in Y_x \mid \text{the total exponent of } y \text{ in } s(x) \text{ is positive}\}.$$

(Total exponent includes negative contributions from y^{-1}.) Since the sum of these total exponents for all $y \in Y_x$ if $E(s(x), x) = 1$, we see that $\sigma(x)$ cannot be empty (lest $E(s(x), x) \leqslant 0$) and cannot be all of Y_x either (lest $E(s(x), x) \geqslant 2$ because Y_x has at least two elements). And $\sigma(x)$ is finite, because words are finite. □

THEOREM 2. *Let X be a set such that $H^1(X, G)$ is trivial for all abelian G. Then, for all positive integers n, $X - AC(n)$ holds, i.e., every n-to-one map onto X has a section.*

PROOF. We use induction on n, the case $n = 1$ being trivial. So assume $n \geqslant 2$ and $X - AC(k)$ holds for all $k < n$; we saw in the introduction that $X - AC(< n)$ also holds. Given any n-to-one map $p\colon Y \to X$, let σ be as in the lemma, and apply $X - AC(< n)$ to $p'\colon Y' \to X$, where p' is the restriction of p to $Y' = \bigcup_{x \in X} \sigma(x)$. □

Recall from the introduction that the conclusion of Theorem 2 does not imply $X - AC$(finite). It would also be incorrect to "prove" $X - AC$(finite) as follows: "Given finite nonempty sets Y_x for all $x \in X$, choose the unique element from any Y_x of cardinality 1 and apply the lemma to reduce the other Y_x's to proper nonempty subsets $\sigma(x)$. Again choose the unique element from any $\sigma(x)$ of cardinality 1, and apply the lemma to the rest. Continue in this fashion. Each Y_x, being finite, will eventually be reduced to a single element, which will serve as the chosen element of Y_x." The error in this argument is that, in iteratively applying the lemma, we need to choose an appropriate σ at each stage, which we can not do without AC (or at least the axiom of dependent choice). Apparently, the following is the best we can do.

COROLLARY. *Assume $H^1(X, G)$ is trivial for all abelian G, and assume either $X - AC$(finite) or $N - AC$, where N is the set of positive integers. Then $X - AC$ holds.*

PROOF. If we have $X - AC$(finite) then, given any $p\colon Y \to X$ with fibers of size at least 2, we first use the lemma to obtain $Y' = \bigcup_{x \in X} \sigma(x)$ with finite nonempty fibers, and then we use $X - AC$(finite) to obtain a section of $p \restriction Y'$. (If some fibers

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

Y_x have size only 1, add another element to apply the preceding argument, but at the end redefine the section to take the original element of Y_x, rather than the new one, as its value.) If we have $N - AC$ then, as pointed out in §1, we can obtain $X - AC$(finite) from the conclusion of Theorem 2. □

If we are willing to use the cohomology assumption for one X to obtain sections over a different X, then the situation improves greatly.

THEOREM 3. *Assume $H^1(X, G)$ is trivial for all sets X and all abelian groups G. Then the axiom of choice is true.*

PROOF. As usual, let a surjection p: $Y \to X$ be given; we seek a section. Let X' be the set of all subsets of Y that have at least two elements, let

$$Y' = \{(y, A) \mid y \in A \text{ and } A \in X'\},$$

and let p': $Y' \to X'$ map each (y, A) to A. Then the fiber Y'_A over any $A \in X'$ is in canonical one-to-one correspondence with A (with (y, A) corresponding to y), so it has at least two elements by definition of X'. By the lemma, applied with X' in place of X, there is a σ' assigning to every $A \in X'$ a nonempty finite proper subset of Y'_A. Via the correspondence mentioned a few lines ago, we get a function σ assigning to each $A \in X'$ a nonempty finite proper subset of itself. Now, given any nonempty $B \subseteq X$, we apply σ to it as often as possible, i.e., we form $B, \sigma(B), \sigma^2(B), \ldots$, where each term is defined if and only if the preceding one had at least two elements. Each term except possibly the first is finite and nonempty. If $\sigma(B)$ has n elements, then the sequence terminates after at most $n + 1$ terms, so there is always a last term. The only way a term can be the last is to have only one element. Call this element $f(B)$. Now $x \mapsto f(Y_x)$ is a section of p. □

Note that this proof is essentially a patching of the incorrect argument discussed after Theorem 2. The infinite sequence of choices of σ's in that argument has been replaced by a single σ, but at the cost of applying the lemma to X' instead of X. So we do not get a "local" result (hypothesis for one X, conclusion for the same X) like Theorem 1 but only a global result (hypothesis for all X, conclusion for all X) like its corollary. (Warning: "local" is stronger than "global", the opposite of the usual situation in topology.) Note further that X' depends not on X, but on Y, so to get $X - AC$ for one X we used the triviality of $H^1(X', G)$ for arbitrarily large X'. This situation could be improved by (a) applying the lemma first to reduce Y to a Y' with finite fibers and (b) defining X' to consist, not of all $\geqslant 2$-element subsets of Y, but only of those that lie in a single fiber; then X' would be only "slightly larger" than X in the sense of having a finite-to-one map $X' \to X$.

4. Well-ordered groups. All of the preceding proofs involve constructing sections for p: $Y \to X$ using the triviality of cohomology with coefficients in a group G that involves a good part of the complexity of Y. In this section, we consider what happens if we prohibit G from being too complex by requiring it to be well-orderable. (This means the underlying set is well orderable; there is no connection between the well-ordering and the group operation.) In rather vague terms, we are

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

trying to detect failures of the axiom of choice by means of a cohomology that does not involve such failures (via non-well-orderable G) in its very definition.

The hypothesis that $H^1(X, G)$ is trivial for all well-orderable G and all sets X does not imply the axiom of choice. That is, we do not get even the sort of global result that we had for abelian groups. To see this, observe that each fiber of any G-torsor is in one-to-one correspondence with G and is therefore well orderable. Thus, triviality of $H^1(X, G)$ follows immediately from AC(well-orderable), which is known to be strictly weaker than AC; see [**5**, p. 82]. Therefore, the best that we could hope for would be to derive AC(well-orderable) from this triviality hypothesis (or the corresponding local result). In fact, we get less, but we do get it locally.

THEOREM 4. *If $H^1(X, G)$ is trivial for all well-orderable G, or indeed only for all countable G, then $X - AC(\text{finite})$ is true.*

PROOF. Let G be the group of those permutations of the set N of positive integers that move only finitely many integers. So G is countable (hence well orderable). Given a surjection $p\colon Y \to X$ with finite fibers, define, for each $x \in X$, T_x = set of bijections $t\colon N \to Y_x \cup \{k+1, k+2, \dots\}$ such that $t(n) = n$ for all but finitely many $n \in N$, where k is the number of elements of Y_x. Thus, T_x is essentially like G except that, in the range (but not the domain) of any of its elements, the k members of Y_x replace the first k members of N. G acts on T_x by right composition, $tg = t \circ g$, and it is easy to see (as in Proof A of Theorem 1) that $\bigcup_{x \in X} T_x$, with the obvious projection, is a G-torsor over X. By hypothesis, it has a section s. For each $x \in X$, $s(x)\colon N \to Y_x \cup \{k+1, k+2, \dots\}$ may be viewed as an enumeration (by positive integers) of $Y_x \cup \{k+1, k+2, \dots\}$; let $s'(x)$ be the first member of Y_x in this enumeration. Then s' is a section of p. □

The clauses about moving only finitely many integers, in the definition of G and T_x, were needed because the group of all permutations of N might not be well orderable. If we assume that well-ordered sets have well-orderable permutation groups, then the preceding proof, with transfinite ordinals in place of integers, would yield $X - AC$(well-orderable) from the hypothesis that $H^1(X, G)$ is trivial for all well-orderable G.

5. Abelian well-ordered groups. In this section we weaken the cohomological triviality assumption still further, by requiring the coefficient group to be both abelian and well orderable. We begin with a local result; the bound of 4 here cannot be improved, as we shall see in the next section.

THEOREM 5. *Assume $H^1(X, G)$ is trivial for all abelian well-orderable groups G. Then $X - AC(\leqslant 4)$ holds.*

PROOF. As remarked in the introduction, it suffices to prove $X - AC(n)$ for $n = 2, 3, 4$.

First observe that, in Proof A of Theorem 1, in the special case where all the Y_x's had the same cardinality, if that cardinality happened to be 2, then the group used in that proof, the group of permutations of a two-element set, is abelian and well orderable. So the present hypotheses yield $X - AC(2)$.

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

$X - AC(3)$ is harder, because the group of permutations of a three-element set is not abelian. If each Y_x consisted of three elements *with a specified cyclic ordering*, then we could carry through essentially the same argument as before, putting bijections into G or T_x only if they respect the given cyclic orderings on the Y_x's and some fixed cyclic ordering on $S = \{1, 2, 3\}$. Then G is the cyclic group of order three, hence abelian and well orderable, so we get a section and proceed as before. Unfortunately, the three-element sets Y_x need not be equipped with specified cyclic orderings; each Y_x has two possible cyclic orderings and, to make the preceding argument work, we must specify one of the two. But we can do this, since we have already proved $X - AC(2)$.

Experts in cohomology[2] will have noticed that this proof of $X - AC(3)$ is simply an application of the fragment

$$H^1(X, C_3) \to H^1(X, S_3) \to H^1(X, C_2)$$

of the long exact cohomology sequence for the inclusion of the cyclic group C_3 in the symmetric group S_3; the two outside terms are trivial by hypothesis, so the middle term is trivial too. They will also have noticed that the same idea yields the triviality of $H^1(X, G)$ for any solvable well-orderable group G, in particular for S_4, so that $X - AC(4)$ holds.

But in fact this cohomological argument is superfluous, since $X - AC(4)$ follows combinatorially from $X - AC(2)$ and $X - AC(3)$. Indeed, given an X-indexed family of four-element sets, observe that each one can be partitioned into two two-element subsets in exactly three ways. Choose one such partition for each of the four-element sets, by $X - AC(3)$. Then use $X - AC(2)$ twice, first to choose one of the two pieces in each chosen partition, and then to choose one of the two elements in each chosen piece. This yields a choice function for the original family. □

It should be pointed out, in connection with the last part of this proof, that Tarski [**5**, p. 107] has shown that $AC(2)$ implies $AC(4)$. However, this implication does not localize; for example, $N - AC(2)$ does not imply $N - AC(4)$. It should also be pointed out that the derivability of $X - AC(4)$ from $X - AC(2)$ and $X - AC(3)$ is a very special case of (a slight modification of) a result of Gauntt [**2**]. For more on the implications between various $AC(n)$'s, see [**2, 5, 6, 7**].

Before proceeding, we isolate for future use a fact that was used (for $n = 3$) in the preceding proof. If we are given an n-to-one map $p\colon Y \to X$ and, in each fiber, a cyclic ordering, then we can get a section for p from the assumption that $H^1(X, C_n)$ is trivial, where C_n is the (abelian well-orderable) cyclic group of order n.

If we do not insist on a local result, Theorem 5 can be improved as follows.

THEOREM 6. *Assume $H^1(X, G)$ is trivial for all sets X and all abelian well-orderable groups, or indeed just all finite cyclic groups, G. Then $AC(n)$ holds for all positive integers n.*

---

[2] Nonexperts can skip this paragraph without losing the thread of the proof.

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

PROOF. We proceed by induction on n, the case $n = 1$ being trivial. Suppose $n \geq 2$ and we have $AC(k)$ for all $k < n$, so we have $AC(< n)$. Let an n-to-one map p: $Y \to X$ be given. For each $y \in Y$, the set

$$\{y' \in Y \mid p(y) = p(y') \text{ but } y \neq y'\}$$

of other points in the same fiber has $n - 1$ elements, so, by induction hypothesis, let f be a function assigning to each $y \in Y$ a different point $f(y)$ in the same fiber. Noting that, for each $x \in X$, f maps Y_x into itself, we partition X into three parts as follows:

$$X_1 = \{x \in X \mid f \text{ restricted to } Y_x \text{ is not a permutation of } Y_x\};$$

$$X_2 = \{x \in X \mid f \text{ restricted to } Y_x \text{ is a permutation consisting of at least two disjoint cycles}\};$$

$$X_3 = \{x \in X \mid f \text{ restricted to } Y_x \text{ is a cyclic permutation of } Y_x\}.$$

We intend to find partial sections s_i $(i = 1, 2, 3)$ for p with domain X_i; then $s_1 \cup s_2 \cup s_3$ is the required section of p.

For $x \in X_1$, f cannot map Y_x onto itself, as a surjection from a finite set to itself is a permutation. So $f(Y_x)$ has size between 1 and $n - 1$ (inclusive). Apply $AC(< n)$ to obtain a choice function for the sets $f(Y_x)$, $x \in X_1$; it is also a section of p over X_1.

For $x \in X_2$, let Z_x be the set of cycles of f in Y_x. Since each cycle has at least two elements (as $f(y) \neq y$), Z_x has fewer than n elements. By $AC(< n)$ we can select one element of Z_x, i.e., one cycle in Y_x, for each $x \in X_2$. The selected cycles have fewer than n elements, by definition of X_2. So a second application of $AC(< n)$ selects an element from each of these cycles and thus provides our desired sections s_2.

For X_3, f provides cyclic orderings of all the fibers, so, by the remark preceding the theorem, the triviality of $H^1(X, C_n)$ provides the required s_3. □

COROLLARY. *If $H^1(X, G)$ is trivial for all sets X and all abelian well-orderable groups G, and if $N - AC$ holds, then so does AC(finite).* □

6. Permutation models. In this section, we assume familiarity with permutation models (or Fraenkel-Mostowski-Specker models) of set theory with atoms (or urelements); see [**5**, Chapter 4]. We use them to make a comment about the results of §4 and to show that Theorem 5 is optimal. We also use them to give an example relevant to the broader project of using nontrivial cohomology to describe failures of the axiom of choice.

In any permutation model, the group of all permutations of a well-ordered set can itself be well ordered. (See [**5**, p. 135] for the corresponding fact about power sets; the result for permutation groups can be deduced from this or proved in a similar manner.) Therefore the remark at the end of §4 is applicable, and we obtain the following improvement, for permutation models, of Theorem 4.

THEOREM 7. *In permutation models, the triviality of $H^1(X, G)$ for all well-orderable G is equivalent to $X - AC$(well-orderable).*

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

It should be noted that the corresponding global result can also be deduced directly from (the global form of) Theorem 4, because P. Howard has shown [**4**] that in permutation models AC(finite) implies AC(well-orderable).

Our final theorem shows that the bound of 4 in Theorem 5 is optimal.

THEOREM 8. *There is a permutation model in which $H^1(N, G)$ is trivial for all abelian well-orderable groups G but $N - AC(5)$ is false.*

PROOF. We use a variant, introduced by Mostowski [**6**], of the second Fraenkel model [**5**, Chapter 4]. Begin with a countably infinite set A of atoms, partitioned into countably many subsets F_n ($n \in N$) of five elements each. Let Γ be the group of those permutations π of A such that π maps each F_n onto itself and is an even permutation of F_n. Thus, Γ is (isomorphic to) the direct product of denumerably many copies Γ_n of the alternating group on five objects, where Γ_n permutes F_n while fixing all the other F_k's pointwise. For each finite subset E of N, let $\hat{E}$ be the subgroup of Γ fixing F_n pointwise for all $n \in E$, i.e., the product of the Γ_n's for $n \notin E$. Let $\mathfrak{F}$ be the filter of subgroups of Γ generated by the groups $\hat{E}$, and let M be the permutation model determined by A, Γ, and the normal filter $\mathfrak{F}$. It is easy to check that M contains A and the projection $A \to N$ that sends each F_n to n, but M does not contain any section for this projection. So $N - AC(5)$ is false in M.

It remains to prove that $H^1(N, G)$ is trivial (in M) for all abelian well-ordered (in M) groups G. Suppose G is such a group and T is a G-torsor over N with projection p: $T \to N$ (all in M). Since G is well orderable in M, it is fixed pointwise by some group in the filter $\mathfrak{F}$. Also, since T, p, and the action of G on T are in M, they are invariant (not pointwise) under some groups in $\mathfrak{F}$. Intersecting these groups and using the definition of $\mathfrak{F}$, we find a finite set $E \subseteq N$ such that $\hat{E}$ fixes G pointwise and leaves T, p, and the action of G on T invariant.

Let $n \in N - E$ be arbitrary, and consider how Γ_n acts on a fiber T_x of T. As $\Gamma_n \subseteq \hat{E}$, each $\pi \in \Gamma_n$ leaves p invariant and (since it certainly fixes the integer x) therefore maps T_x into itself. Consider an arbitrary but fixed $t \in T_x$. Since G acts sharply transitively on T_x we have, for each $\pi \in \Gamma_n$, a unique $\bar{\pi} \in G$ such that $\pi(t) = t\bar{\pi}$. For any other element of T_x, say tg, we have, since π fixes the action and g,

$$\pi(tg) = \pi(t)\pi(g) = t\bar{\pi}g.$$

Thus, if σ is another element of Γ_n,

$$(\pi \circ \sigma)t = \pi(t\bar{\sigma}) = t\bar{\pi}\bar{\sigma}$$

which means $\overline{\pi\sigma} = \bar{\pi}\bar{\sigma}$. We have therefore defined a homomorphism, $\pi \mapsto \bar{\pi}$ from Γ_n into G. But G is abelian and Γ_n, being isomorphic to the alternating group on five objects, has no nontrivial homomorphisms to abelian groups. Therefore $\bar{\pi} = 1$ for all π, which means t is fixed by every $\pi \in \Gamma_n$. Since n was arbitrary in $N - E$, we infer that t is fixed by all those elements of $\hat{E}$ that have only finitely many nonidentity components, i.e., by the weak direct product of the Γ_n for $n \notin E$. Being in M, t is also fixed by $\hat{F}$ for some finite $F \subseteq N$, and it is trivial to check that $\hat{F}$ and the weak direct product just mentioned generate the full direct product $\hat{E}$. Thus, $\hat{E}$ fixes t.

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use

Finally, we use the fact that t was arbitrary in T (since x was arbitrary in N) to see that $\hat{E}$ fixes T pointwise. So T admits a well-ordering in M and therefore also admits a section for p. (In fact, any section of p in the real universe is in M since $\hat{E}$ fixes it.) □

We remark that a similar argument, with the alternating group on five elements changed to that on four elements (which has no subgroup of index two), shows that $N - AC(2)$ does not imply $N - AC(4)$.

Another similar argument, this time with the alternating group changed to the symmetric group on two elements, i.e., with the second Fraenkel model, shows that in this model $H^1(N, C_m)$ is trivial for all odd values of m, while $H^1(N, C_2)$ can be described as follows. Let S be the group of all finite subsets of N under symmetric difference, let S^N be the group of all functions from N to S, and let B be the subgroup of bounded functions, i.e., functions whose values all lie within some finite subset of N. Then $H^1(N, C_2)$ is canonically isomorphic to S^N/B. This large group, contrasted with the vanishing of $H^1(N, C_m)$ for m odd, can be viewed as representing, in some sense, the intuition that the failure of countable choice in the second Fraenkel model is "concentrated at the prime 2". Similar results are possible for variants of the second Fraenkel model such as those considered above, but the problem of doing similar calculations for other models and giving reasonable intuitive interpretations to the results remains open.

Our local results concerning $AC(n)$ under the hypothesis of trivial H^1 for abelian well-ordered G, namely that proving $AC(n)$ is trivial for $n = 1$, possible for $n = 2, 3, 4$, but impossible for larger n, are similar to the classical results on solvability of nth degree equations by radicals, not only in appearance but also in their essential reason, the solvability or unsolvability of the symmetric groups.

References

1. R. Diaconescu, *Non-abelian cohomology à la Giraud*, Kategorien, Tagungsbericht, Oberwolfach, June-July 1975.

2. R. J. Gauntt, *Some restricted versions of the axiom of choice*, Notices Amer. Math. Soc. **15** (1968), 351.

3. J. Giraud, *Cohomologie non abélienne*, Springer-Verlag, Berlin, Heidelberg and New York, 1971.

4. P. Howard, *Limitations of the Fraenkel-Mostowski method of independence proofs*, J. Symbolic Logic **38** (1973), 416–422.

5. T. Jech, *The axiom of choice*, North-Holland, Amsterdam, 1973.

6. A. Mostowski, *Axiom of choice for finite sets*, Fund. Math. **33** (1945), 137–168.

7. J. Truss, *Finite axioms of choice*, Ann. Math. Logic **6** (1973), 147–176.

Department of Mathematics, The University of Michigan, Ann Arbor, Michigan 48109

License or copyright restrictions may apply to redistribution; see http://www.ams.org/journal-terms-of-use