On Groups That Are Isomorphic to a Proper Subgroup

SHAUN FALLAT
CHI-KWONG LI
DAVID LUTZER
DAVID STANFORD
College of William and Mary
Williamsburg, VA 23187-8795

Introduction When is a group isomorphic to a proper subgroup of itself? Clearly, no finite group can have this property, but what about $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$, the familiar additive groups of integers, rational, real, and complex numbers? What about $\mathbb{R}^n$, the additive group of n-dimensional vectors? What about the multiplicative groups of non-zero rational, real, or complex numbers? What about the multiplicative group $T = \{z \in \mathbb{C} : |z| = 1\}$ of complex numbers with modulus one? What about your own favorite infinite group from the first modern algebra class?

These easily stated questions are very special cases of an important problem in group theory (namely to determine whether or not two groups are isomorphic) and can be the basis for classroom discussion in an introductory modern algebra course as soon as the notions of group, subgroup, and isomorphism have been introduced. Further, such questions can be posed again as new algebraic constructions (e.g., product groups and quotient groups) are introduced, and they have analogues for the other familiar algebraic structures (rings, fields) often found in undergraduate modern algebra. In addition, the isomorphic subgroup question provides a valuable way to get students to think about the familiar groups $\mathbb{Z}, \mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ in a non-trivial context. Finally, the question can be the basis for open-ended student projects in such a course.

Textbooks develop standard techniques for showing that two groups are *not* isomorphic. Perhaps one is cyclic and the other is not. Perhaps the groups have different cardinalities. Perhaps the two groups have a different number of elements of some order k. On the other hand, for students in an introductory course, showing that two groups *are* isomorphic usually means constructing a specific isomorphism. As a result, many of the examples of isomorphic groups given in introductory courses are transparently isomorphic.

The goal of this note is to illustrate how the proper subgroup question can be used in an introductory course, and to show how ideas from linear algebra can be used in an introductory modern algebra course to exhibit non-transparently isomorphic groups. We will answer the questions posed in the opening paragraph, and suggest further projects that might be of interest to students. We do not claim novelty for the results below, nor do we give the most general statements or the best possible proofs of the results. (An elegant classical reference for related material is [2].)

Some easy examples Clearly, if a group G is isomorphic to a proper subgroup of itself, then $|G|$, the cardinality of G, must be infinite. However, being infinite is not enough, because easy examples show that some infinite groups are, and others are not, isomorphic to proper subgroups of themselves.

EXAMPLE 1. The additive group $\mathbb{Z}$ of all integers is isomorphic to the subgroup of even integers under the isomorphism $f(x) = 2 * x$.

EXAMPLE 2. The additive group $\mathbb{Q}$ of all rational numbers is *not* isomorphic to a proper subgroup of itself because every homomorphism $f:\mathbb{Q}\to\mathbb{Q}$ has the form $f(x)=f(1)*x$, so that that every isomorphism from $\mathbb{Q}$ into $\mathbb{Q}$ is actually an isomorphism onto $\mathbb{Q}$.

QUESTION 1. What about the direct sum group $\mathbb{Q}\oplus\mathbb{Q}$? Is it isomorphic to a proper subgroup of itself? What about $\mathbb{Q}\oplus\mathbb{Z}$? (The answers are "No" and "Yes," respectively.)

QUESTION 2. What about the quotient group $\mathbb{Q}/\mathbb{Z}$? It is not isomorphic to a proper subgroup of itself because if g is an isomorphism from $\mathbb{Q}/\mathbb{Z}$ into itself and if $A(k)=\{x\in\mathbb{Q}/\mathbb{Z}: x \text{ has order } k\}$, then $g[A(k)]\subseteq A(k)$. But then, $A(k)$ being finite and g being one-to-one, we have $g[A(k)]=A(k)$. Because $\mathbb{Q}/\mathbb{Z}=\bigcup\{A(k): k\geq 1\}$, g must be onto.

Next we show that some familiar multiplicative groups provide many different examples of groups that are isomorphic to proper subgroups of themselves. We consider the multiplicative groups $\mathbb{Q}^+,\mathbb{Q}^*,\mathbb{R}^+,\mathbb{R}^*$ consisting, respectively, of all positive rationals, non-zero rationals, positive reals, and non-zero reals.

PROPOSITION 1. *The multiplicative groups $\mathbb{Q}^+$, $\mathbb{Q}^*$, $\mathbb{R}^+$, and $\mathbb{R}^*$ are all isomorphic to proper subgroups of themselves.*

Proof. Define $f:\mathbb{Q}^*\to\mathbb{Q}^*$ by $f(x)=x^3$. This f is an isomorphism from $\mathbb{Q}^*$ onto a proper subgroup of itself, and when restricted to $\mathbb{Q}^+$, f provides an isomorphism from $\mathbb{Q}^+$ onto a proper subgroup of itself. Next, the function $g(x)=e^x$ is an isomorphism from the additive group $\mathbb{R}$ onto the multiplicative group $\mathbb{R}^+$. Hence, by Theorem 1 (to follow), we have that $\mathbb{R}^+$ is isomorphic to a proper subgroup of itself. Because the multiplicative group $\mathbb{R}^*$ is the internal direct sum of $\mathbb{R}^+$ and the two element group $T_0=\{-1,1\}$ with its usual multiplication, we see that $\mathbb{R}^*$ is isomorphic to a proper subgroup of itself. (See also Exercise 1, below.)

It is natural to wonder whether the groups in Proposition 1 are really different. They are. Cardinality arguments show that the rational and real groups in Proposition 1 are distinct. To distinguish between $\mathbb{Q}^+$ and $\mathbb{Q}^*$, ask how many solutions the equation $x^2=1$ has in each group. The same question distinguishes between $\mathbb{R}^+$ and $\mathbb{R}^*$. Compare this with Proposition 4, below.

More complicated examples and $\mathbb{Q}$-linearity Certain groups are able to carry more than just group structure. For example, the additive groups $\mathbb{R}$, $\mathbb{C}$, and $\mathbb{R}^n$ are also vector spaces over the field $\mathbb{Q}$, and group homomorphisms of these groups are easily seen to be $\mathbb{Q}$-linear mappings as well. Those facts allow students to use some of the ideas that they encountered in their first linear algebra course, namely the notions of spanning sets, bases, and dimension. Of course, one must now deal with vector spaces that are infinite dimensional over $\mathbb{Q}$, and one must distinguish between finite, countable, and uncountable dimensional spaces. That added complication allows students to review the finite-dimensional proofs they encountered in linear algebra, to see whether basis theory still works in more general spaces. By mimicking the finite-dimensional proofs, and using the observation that the $\mathbb{Q}$-linear span of an infinite set S has cardinality $|\mathbb{Q}|*|S|=|S|$, strong students would be able to prove:

PROPOSITION 2. *Two vector spaces V and W over the field $\mathbb{Q}$ are $\mathbb{Q}$-linearly isomorphic if and only if V and W have bases over $\mathbb{Q}$ of the same cardinality.*

There is a second result that is useful in exploiting the $\mathbb{Q}$-linear structure of certain groups, but one that is rarely mentioned in introductory textbooks, probably because it depends on what Halmos called "transfinite trickery" [1, p. 13].

PROPOSITION 3. *Any linearly independent set in any vector space V is contained in a basis for V. In particular, there is a basis B for the $\mathbb{Q}$-vector space $\mathbb{R}$ with $1 \in B$.*

Undergraduates have no problem understanding the statement of Proposition 3. Our experience suggests that most are willing to accept the statement without insisting on a proof. For the others, Proposition 3 could be the basis for an outside reading project on Zorn's lemma. Students who know that $\mathbb{Q}$ is countable while $\mathbb{R}$ is not will be able to prove that the basis B for $\mathbb{R}$ over $\mathbb{Q}$ is infinite, a fact that we need below. Using Propositions 2 and 3, one can prove:

THEOREM 1. *The additive group $\mathbb{R}$ is isomorphic to a proper subgroup of itself.*

Proof. Using Proposition 3 choose any basis B for $\mathbb{R}$ over $\mathbb{Q}$. Then B is infinite. Choose distinct $b(1), b(2), \ldots$ in B and define $s: B \to B$ by $s(b(n)) = b(n+1)$ and $s(b) = b$ if $b \in B - \{b(n): n \geq 1\}$. Then extend s over $\mathbb{R}$ in a $\mathbb{Q}$-linear way. The resulting $\mathbb{Q}$-vector space isomorphism is the required group isomorphism from $\mathbb{R}$ onto a proper subgroup of itself.

Students might be tempted to think that additional examples of groups that are isomorphic to proper subgroups could be obtained from other familiar groups such as $\mathbb{R}^n$ and $\mathbb{C}$. Such examples do exist, but they are not *new* examples because Proposition 2 yields:

PROPOSITION 4. *Each of the additive groups $\mathbb{R}^n, \mathbb{C}^n, \mathbb{R}[X] = \{p(X): p$ is a polynomial with coefficients in $\mathbb{R}\}$, and $\mathbb{C}[X] = \{p(X): p$ is a polynomial with coefficients in $\mathbb{C}\}$ is isomorphic to the additive group $\mathbb{R}$.*

Proof. Starting with a basis B for $\mathbb{R}$ over $\mathbb{Q}$, one can show that each of these groups is a $\mathbb{Q}$-vector space with a basis of cardinality $|B|$. Now apply Proposition 2 to conclude that the groups listed in this proposition are $\mathbb{Q}$-linearly isomorphic, and hence group isomorphic.

A slightly less familiar but very important group is the multiplicative group $T = \{z \in \mathbb{C}: |z| = 1\}$, where $|z|$ denotes the usual absolute value of the complex number z. In a moment we will need to know that the function $h(x) = e^{2\pi i x}$ induces a group isomorphism from $\mathbb{R}/\mathbb{Z}$ onto T.

Consider $\mathbb{C}^*$, the multiplicative group of all non-zero complex numbers. This group is not isomorphic to any of the groups considered above (namely, the multiplicative groups $\mathbb{Q}^+$, $\mathbb{Q}^*$, $\mathbb{R}^+$, $\mathbb{R}^*$, and the additive groups listed in Proposition 4) because it contains two elements of order three (i.e., nontrivial solutions of the equation $x^3 = 1$) while none of the other groups has this property. Is $\mathbb{C}^*$ isomorphic to a proper subgroup of itself? The answer is "yes." The most elementary proof that we know uses the linear algebra tools from the previous section as a start, and then makes careful use of the isomorphism theorems for groups. In this case, one can give a concrete example of a proper subgroup of $\mathbb{C}^*$ to which $\mathbb{C}^*$ is isomorphic, and the result is somewhat counter-intuitive.

THEOREM 2. *The multiplicative groups $\mathbb{C}^*$ and T are isomorphic.*

Proof. Using Proposition 3, choose a basis B for $\mathbb{R}$ as a $\mathbb{Q}$-vector space, with $1 \in B$. Because B is infinite, we can write $B = B_1 \cup B_2$ where $B_1 \cap B_2 = \emptyset$, $|B_i| = |B|$ and

$1 \in B_1$. For each $b \in B$ let Q_b be the $\mathbb{Q}$-vector space $\{q * b : q \in \mathbb{Q}\}$. Then Proposition 2 yields an isomorphism f from the $\mathbb{Q}$-vector space $\mathbb{R}$ onto $(\oplus\{Q_b : b \in B_1\}) \oplus (\oplus\{Q_b : b \in B_2\})$ that sends the number $1 \in \mathbb{R}$ to the vector $1 \in Q_1 \subset R_1$ where $R_i = \oplus\{Q_b : b \in B_i\}$. By Proposition 2, each R_i is $\mathbb{Q}$-linearly isomorphic to $\mathbb{R}$.

Now think of the $\mathbb{Q}$-vector spaces above as additive groups. Then f is a group isomorphism from $\mathbb{R}$ onto $R_1 \oplus R_2$, and $(R_2, +)$ is group isomorphic to $(\mathbb{R}^+, *)$ under the exponential function. Writing $Z_1 = f[\mathbb{Z}]$ and writing $\cong$ to denote group isomorphism, we have $\mathbb{R}/\mathbb{Z} \cong R_1/Z_1 \oplus R_2 \cong (T, *) \oplus (\mathbb{R}^+, *)$. But the usual polar representation of non-zero complex numbers establishes a group isomorphism between $T \oplus (\mathbb{R}^+, *)$ and $\mathbb{C}^*$. Thus $T \cong \mathbb{R}/\mathbb{Z} \cong T \oplus \mathbb{R}^+ \cong \mathbb{C}^*$, as claimed.

More exercises for undergraduates The ideas in this paper can be the basis for exploration projects in a first modern algebra course. In this section, we give a few examples of questions that an instructor might pose at various stages of the course.

EXERCISE 1. *Direct sums and proper subgroups.* Suppose G and H are groups, one of which is isomorphic to a proper subgroup of itself. Then so is $G \oplus H$. What about the converse? If $G \oplus H$ is isomorphic to a proper subgroup of itself, must the same be true of one of G and H?

EXERCISE 2. *Which groups are $\mathbb{Q}$-linear spaces?* The central idea in our paper is that many familiar groups are, in fact, $\mathbb{Q}$-linear vector spaces. Characterize all Abelian groups that are $\mathbb{Q}$-linear vector spaces.

EXERCISE 3. *Counting morphisms.* How many group homomorphisms exist from the additive group $\mathbb{Q}$ into itself? From the additive group $\mathbb{R}$ into itself? From the multiplicative groups considered in Section 3 into themselves? How many group isomorphisms exist in each case?

EXERCISE 4. *Fields and subfields.* Which fields are field isomorphic to proper subfields of themselves? One can show that the usual fields $\mathbb{Q}$ and $\mathbb{R}$ are *not* isomorphic to proper subfields of themselves, but that there are fields lying between $\mathbb{Q}$ and $\mathbb{R}$ that are isomorphic to proper subfields of themselves. One approach is to prove that the identity function is the only field isomorphism from either $\mathbb{Q}$ or $\mathbb{R}$ into itself. One can also show that the usual field $\mathbb{C}$ of complex numbers is isomorphic to a proper subfield of itself. In addition, unlike the situation for $\mathbb{Q}$ and $\mathbb{R}$, there are many field automorphisms of $\mathbb{C}$. See [3] for an elegant discussion.

EXERCISE 5. *Quotient groups.* When is a group G isomorphic to a non-trivial quotient group of itself? (By a "nontrivial quotient group of G" we mean a quotient group G/H where $|H| > 1$.)

REFERENCES

1. P. Halmos, *Finite Dimensional Vector Spaces*, D. Van Nostrand, New York, NY, 1958.
2. I. Kaplansky, *Infinite Abelian Groups*, University of Michigan Press, Ann Arbor, MI, 1954.
3. P. Yale, Automorphisms of the complex numbers, this MAGAZINE 39 (1966), 135–141.