Walker's cancellation theorem

Robert Lubarsky and Fred Richman
Florida Atlantic University

22 August 2012

Abstract

Walker's cancellation theorem says that if $B \oplus \mathbf{Z}$ is isomorphic to $C \oplus \mathbf{Z}$ in the category of abelian groups, then B is isomorphic to C. We construct an example in a diagram category of abelian groups where the theorem fails. As a consequence, the original theorem does not have a constructive proof even if B and C are subgroups of the free abelian group on two generators. Both of these results contrast with a group whose endomorphism ring has stable range one, which allows a constructive proof of cancellation and also a proof in any diagram category.

1 Cancellation

An object G in an additive category is **cancellable** if whenever $B \oplus G$ is isomorphic to $C \oplus G$, then B is isomorphic to C. Elbert Walker, in his dissertation [7], and P. M. Cohn in [3], independently answered a question of Irving Kaplansky by showing that finitely generated abelian groups are cancellable in the category of abelian groups. The most interesting case is that of $\mathbf{Z}$, the additive group of integers. That's because finitely generated groups are direct sums of copies of $\mathbf{Z}$ and of cyclic groups of prime power order, and a cyclic group of prime power order has a local endomorphism ring, hence is cancellable by a theorem of Azumaya [2].

It is somewhat anomalous that $\mathbf{Z}$ is cancellable. A rank-one torsion-free group A is cancellable if and only if $A \cong \mathbf{Z}$ or the endomorphism ring of A has stable range one [1, Theorem 8.12],[4]. (A ring R has **stable range**

one if whenever $aR + bR = R$, then $a + bR$ contains a unit of R.) Thus for rank-one torsion-free groups, the endomorphism ring tells the whole story—except for $\mathbf{Z}$. It turns out that an object is cancellable if its endomorphism ring has stable range one. The proof of this in [6, Theorem 4.4] is constructive and works for any abelian category. It is also true, [6], that semilocal rings have stable range one, so Azumaya's theorem is a special case of this. In fact, that the endomorphism ring of A has stable range one is equivalent to A being substitutable, a stronger condition than cancellation [6, Theorem 4.4]. We say that A is **substitutable** if any two summands a group, with complements that are isomorphic to A, have a common complement. The group $\mathbf{Z}$ is not substitutable: Consider the subgroups of $\mathbf{Z}^2$ generated by $(1,0)$, $(0,1)$, $(7,3)$, and $(5,2)$. The first and second, and the third and fourth, are complementary summands. The second and fourth do not have a common complement because that would require (a,b) with $a = \pm 1$ and $2a - 5b = \pm 1$.

In this paper we will investigate whether $\mathbf{Z}$ is cancellable in the (abelian) category $\mathcal{D}_T(\mathbf{Ab})$ of diagrams of abelian groups based on a fixed finite poset T with a least element. There is a natural embedding of $\mathbf{Ab}$ into $\mathcal{D}_T(\mathbf{Ab})$ given by taking a group into the constant diagram on T with identity maps between the groups on the nodes. In particular, we can identify the group of integers as an object of $\mathcal{D}_T(\mathbf{Ab})$. As the endomorphism ring of any group G is the same as that of its avatar in $\mathcal{D}_T(\mathbf{Ab})$, a substitutable group is substitutable viewed as an object in $\mathcal{D}_T(\mathbf{Ab})$. However it turns out that $\mathbf{Z}$ is not cancellable in $\mathcal{D}_T(\mathbf{Ab})$ where T is the linearly ordered set $\{0,1,2\}$.

This result has repercussions for the constructive theory of abelian groups. Because of it, we can conclude that Walker's theorem does not admit a constructive proof. In fact, it is not even provable when B and C are restricted to be subgroups of $\mathbf{Z}^2$. It was the question of whether Walker's theorem had a constructive proof that initiated our investigation. You can think of a constructive proof as being a proof within the context of intuitionistic logic. Such proofs are normally constructive in the usual informal sense. Most any proof of Azumaya's theorem is constructive, so a constructive proof of the cancellability of $\mathbf{Z}$ would show that you can cancel finite direct sums of finite and infinite cyclic groups.

As any homomorphism from an abelian group onto $\mathbf{Z}$ splits, Walker's theorem can be phrased as follows: If A is an abelian group, and $f, g : A \to \mathbf{Z}$ are epimorphisms, then $\ker f \cong \ker g$. The following theorem gets us part way to a proof of Walker's theorem.

Theorem 1 *Let A be an abelian group and $f, g : A \to \mathbf{Z}$ be epimorphisms. Then $f(\ker g) = g(\ker f)$ so that*

$$\frac{\ker g}{\ker f \cap \ker g} \cong f(\ker g) = g(\ker f) \cong \frac{\ker f}{\ker f \cap \ker g}$$

Proof. Consider the image I of the map $A \to \mathbf{Z} \oplus \mathbf{Z}$ induced by f and g. As f and g are epimorphisms, I is a subdirect product. Note that $f(\ker g) = I \cap (\mathbf{Z} \oplus 0)$ when the latter is viewed as a subgroup of $\mathbf{Z}$, and similarly $g(\ker f) = I \cap (0 \oplus \mathbf{Z})$. To finish the proof we show that if $(x, 0) \in I$, then $(0, x) \in I$. As I is a subdirect product, there exists $n \in \mathbf{Z}$ such that $(n, 1) \in I$. Thus $(0, x) = x(n, 1) - n(x, 0) \in I$. ■

Thus we get the desired isomorphism $\ker f \cong \ker g$ if $\ker f \cap \ker g = 0$ or if $f(\ker g)$ is projective. Classically, every subgroup of $\mathbf{Z}$ is projective, so this constitutes a classical proof. Indeed, it is a classical proof that in the category of modules over a Dedekind domain D, the module D is cancellable [5].

2 The example

Our example lives in the category $\mathcal{D}_T(\mathbf{Ab})$ of diagrams of abelian groups based on the linearly ordered set $T = \{0, 1, 2\}$. The example shows that you can't cancel $\mathbf{Z}$ in $\mathcal{D}_T(\mathbf{Ab})$.

The groups on the nodes will be subgroups $A_0 \subset A_1 \subset A_2 = \mathbf{Z}^3$ defined by generators:

$$A_0 = \begin{matrix} (1,3,0) \\ (3,1,0) \end{matrix} \quad A_1 = \begin{matrix} (1,0,-24) \\ (0,1,8) \\ (0,0,64) \end{matrix} \quad A_2 = \begin{matrix} (1,0,0) \\ (0,1,0) \\ (0,0,1) \end{matrix}$$

Note that $(0,8,0), (8,0,0) \in A_0$. The maps between these groups are inclusions. Define the maps $f, g : \mathbf{Z}^3 \to \mathbf{Z}$ by $f(a,b,c) = a$ and $g(a,b,c) = b$. The maps f and g each induce maps from these three groups into $\mathbf{Z}$ which give two maps from the diagram into the constant diagram $\mathbf{Z}$. We denote the kernel of the map f restricted to A_i by $\ker_i f$ and similarly for g. These kernels admit the following generators:

$$\ker_0 f = (0,8,0) \quad \ker_1 f = \begin{matrix} (0,1,8) \\ (0,0,64) \end{matrix} \quad \ker_2 f = \begin{matrix} (0,1,0) \\ (0,0,1) \end{matrix}$$

$$\ker_0 g = (8,0,0) \quad \ker_1 g = \begin{matrix}(1,0,-24)\\(0,0,64)\end{matrix} \quad \ker_2 g = \begin{matrix}(1,0,0)\\(0,0,1)\end{matrix}$$

The diagrams $B = \ker f$ and $C = \ker g$ are clearly each embeddable in the diagram $\mathbf{Z} \oplus \mathbf{Z}$. That $B \oplus \mathbf{Z}$ is isomorphic to $C \oplus \mathbf{Z}$ follows from the fact that the diagram A can be written as an internal direct sum $B \oplus \mathbf{Z}$ and also as an internal direct sum $C \oplus \mathbf{Z}$. The generator of $\mathbf{Z}$ in the first case is the element $(1,3,0)$, in the second case $(3,1,0)$.

Theorem 2 *There is no isomorphism between* $\ker f$ *and* $\ker g$ *in* $\mathcal{D}_T(\mathbf{Ab})$.

Proof. Suppose we had an isomorphism $\varphi : \ker f \to \ker g$. Looking at the isomorphisms at 0 and 2, there exist $e, e' = \pm 1$ and $x \in \mathbf{Z}$ so that

$$\varphi(0,8,0) = (8e,0,0) \text{ and } \varphi(0,0,1) = (x,0,e')$$

Thus $\varphi(0,1,8) = (e+8x, 0, 8e')$. For $(e+8x,0,8e')$ to be in $\ker_1 g$, we must have $8e'+24(e+8x)$ divisible by 64. But $8e'+24(e+8x)$ is equal to $8e'+24e$ modulo 64, and this is not divisible by 64. ■

The following result shows that we can't get an example that is a subobject of the diagram $\mathbf{Z}^n$ using the linearly ordered set $T = \{0,1\}$.

Theorem 3 *Let* $T = \{0,1\}$. *In the category* $\mathcal{D}_T(\mathbf{Ab})$, *if* A *and* B *are subobjects of* $\mathbf{Z}^n$, *and* $A \oplus \mathbf{Z}$ *is isomorphic to* $B \oplus \mathbf{Z}$, *then* A *is isomorphic to* B.

Proof. Write $A \subseteq \mathbf{Z}^n$ as $A_0 \subseteq A_1$. As A_1 is a finite-rank free abelian group, the situation $A_0 \subseteq A_1$ can be represented by an integer matrix whose rows generate A_0. Using elementary row and column operations, we can diagonalize this matrix so that each entry on the diagonal divides the next (Smith normal form). Thus A is isomorphic to B exactly when the ranks of the free abelian groups A_1 and B_1 are equal, and $A_1/A_0 \cong B_1/B_0$. If $C = A \oplus \mathbf{Z}$ is isomorphic to $D = B \oplus \mathbf{Z}$, then the rank of $C_1 = A_1 \oplus \mathbf{Z}$ is equal to the rank of $D_1 = B_1 \oplus \mathbf{Z}$, so the rank of A_1 is equal to the rank of B_1, and $A_1/A_0 \cong C_1/C_0 \cong D_1/D_0 \cong B_1/B_0$, so A is isomorphic to B. ■

This theorem leaves open the question of whether there is an counterexample of this sort using the poset that looks like a "V".

3 The Brouwerian counterexample

A Brouwerian example is an object depending on a finite family of propositions. The idea is that if a certain statement holds about that object, then some relation holds among the propositions. Thus a Brouwerian example is piece of *reverse mathematics*: the derivation of a propositional formula from a mathematical statement. For example, there may be just one proposition P and if the statement holds for that object, then $P \vee \neg P$ holds. Thus from the general truth of the statement we could derive the law of excluded middle, from which we would conclude that the statement does not admit a constructive proof. Our Brouwerian counterexample to Walker's theorem is based on the diagram of groups of the previous section.

Let P and Q be propositions. Let

$$A = \left\{ x \in \mathbf{Z}^3 : x \in A_0 \text{ or } P \wedge x \in A_1 \text{ or } P \wedge Q \right\}$$

where A_0 and A_1 are defined in the preceding section. The maps $f, g : \mathbf{Z}^3 \to \mathbf{Z}$ are defined as before by $f(a, b, c) = a$ and $g(a, b, c) = b$.

Note that A is a discrete group (any two elements are either equal or distinct) as it is a subgroup of the discrete group $\mathbf{Z}^3$.

Theorem 4 *The groups* $\ker f$ *and* $\ker g$ *are isomorphic if and only if* $P \vee P \Rightarrow (Q \vee \neg Q)$*.*

Proof. As before, we denote $A_i \cap \ker f$ by $\ker_i f$.

If P holds, then the isomorphism is induced by $\varphi(0, 1, 0) = (1, 0, -32)$ and $\varphi(0, 0, 1) = (0, 0, 1)$. Suppose $P \Rightarrow (Q \vee \neg Q)$ holds. Define φ on $\ker_0 f$ by $\varphi(0, 8, 0) = (0, 0, 8)$. That's all we have to do unless we are given x that is not in $\ker_0 f$. If $x \in \ker_2 f$, and $x \notin \ker_0 f$, then P holds, hence either Q or $\neg Q$ holds. If Q holds, then the isomorphism is induced by $\varphi(0, 1, 0) = (1, 0, 0)$ and $\varphi(0, 0, 1) = (0, 0, 1)$. If $\neg Q$ holds, the isomorphism is induced by $\varphi(0, 1, 8) = (3, 0, -8)$ and $\varphi(0, 8, 0) = (8, 0, 0)$.

Conversely, suppose φ is an isomorphism. If $\varphi(0, 8, 0) \neq (\pm 8, 0, 0)$, then P holds, so we may assume that $\varphi(0, 8, 0) = (8, 0, 0)$. To show that $P \Rightarrow Q \vee \neg Q$, suppose P holds. If $\varphi(\ker_1 f) \neq \ker_1 g$, then Q holds. If $\varphi(\ker_1 f) = \ker_1 g$, then Q cannot hold because that would give an isomorphism in the diagram category contrary to Theorem 2. ∎

So if we could find a constructive proof that $\ker f$ and $\ker g$ were isomorphic, then we would have a constructive proof of the propositional form

$$P \vee P \Rightarrow (Q \vee \neg Q).$$

That means that this form would be a theorem in the intuitionistic propositional calculus. But then by the disjunction property, either P is a theorem, which it is not, or $P \Rightarrow (Q \vee \neg Q)$ is a theorem. In the latter case, substituting $\top$ for P gives $Q \vee \neg Q$, the law of excluded middle, which is not a theorem.

The diagram example of the preceding section can itself be thought of as an object in a model of intuitionistic abelian group theory, and in this way directly shows that Walker's theorem does not admit a constructive proof, even for subgroups of $\mathbf{Z}^2$.

4 Canceling Z with respect to subgroups of Q

We have seen that we can't cancel $\mathbf{Z}$ with respect to certain subgroups of $\mathbf{Z} \oplus \mathbf{Z}$. It is natural to ask what the situation is with respect to subgroups of $\mathbf{Z}$. We give a constructive proof of the following theorem.

Theorem 5 *Let B be an abelian group such that every nontrivial homomorphism from B to $\mathbf{Z}$ is one-to-one. If f is a homomorphism from $B \oplus \mathbf{Z}$ onto $\mathbf{Z}$, then $\ker f$ is isomorphic to mB for some positive integer m. Hence if B is torsion free, then $\ker f$ is isomorphic to B.*

Proof. Let $s = f(0,1)$ and f_1 the restriction of f to B. As f is onto, we have $f_1(B) + s\mathbf{Z} = \mathbf{Z}$. If $s = 0$, then f maps B isomorphically onto $\mathbf{Z}$, and $0 \oplus \mathbf{Z}$ is $\ker f$, in which case we can set $m = 1$. So we may suppose that $s > 0$. We will show that $\ker f$ is isomorphic to sB.

When is (b,n) in $\ker f$? As $f(b,n) = f_1(b) + sn$, we see that a necessary and sufficient condition is that $f_1(b) \in s\mathbf{Z}$ and $n = -f_1(b)/s$. Thus $\ker f$ is isomorphic to $f_1^{-1}(s\mathbf{Z})$. As $f_1(B) + s\mathbf{Z} = \mathbf{Z}$, and $f_1(B)$ and $s\mathbf{Z}$ are ideals of $\mathbf{Z}$, it follows that $f_1(B) \cap s\mathbf{Z} = f_1(B)\, s\mathbf{Z} = s f_1(B)$. Thus

$$f_1^{-1}(s\mathbf{Z}) = f_1^{-1}(f_1(B) \cap s\mathbf{Z}) = f_1^{-1}(s f_1(B))$$

Clearly $f_1^{-1}(sf_1(B)) \supseteq sB$. Conversely, if $f_1(b) \in sf_1(B) = f_1(sB)$, then $f_1(b) = f_1(sb')$ so $b = sb' \in sB$. ■

Note that any torsion-free group B of rank at most one satisfies the hypothesis of the theorem. Also any group with no nontrival maps into $\mathbf{Z}$. Classically, this latter condition simply says that B has no proper $\mathbf{Z}$ summands.

What other groups B allow cancellation of $\mathbf{Z}$? It suffices that B be finitely generated. To see this, look at Theorem 1. If $\ker f$ is finitely generated, then $g(\ker f)$ is a finitely generated subgroup of $\mathbf{Z}$, hence is projective. From this argument it suffices that any image of B in $\mathbf{Z}$ be finitely generated. Notice that subgroups of $\mathbf{Z}$ need not have this property.

What about a direct sum of two groups that allow cancellation of $\mathbf{Z}$, such as a direct sum of two subgroups of $\mathbf{Z}$?

References

[1] Arnold, David M., *Finite rank torsion free abelian groups and rings*, Lecture Notes in Mathematics **931**, Springer, 1982.

[2] Azumaya, Goro, Corrections and supplementaries to my paper concerning Krull-Remak-Schmidt's theorem, *Nagoya Math. J.*, **1** (1950), 117–124.

[3] Cohn, Paul M., The complement of a finitely generated direct summand of an abelian group, *Proc. Amer. Math. Soc.*, **7** (1956), 520–521.

[4] Fuchs, Laszlo and Frans Loonstra, On the cancellation of modules in direct sums over Dedekind domains, *Indag. Math.* **33** (1971), 163–169.

[5] Hsü, Chin-shui, Theorems on direct sums of modules, *Proc. Amer. Math. Soc.*, **13** (1962), 540–542

[6] Lam, Tsit Yuen, *A crash course on stable range, cancellation, substitution, and exchange*, math.berkeley.edu/~lam/ohio.ps

[7] Walker, Elbert A., Cancellation in direct sums of groups, *Proc. Amer. Math. Soc.*, **7** (1956) 898–902.