Spring 2012

When the trivial is nontrivial

William Capecchi

Thomas Q. Sibley
College of Saint Benedict/Saint John's University, tsibley@csbsju.edu

Abelian Groups with Only Trivial Multiplications

William Capecchi
University of Wisconsin
Thomas Q. Sibley
St. John's University

Any abelian group $(G,+)$ with identity 0 can be made into a ring by defining the trivial multiplication $a * b = 0$. Surprisingly, there are nontrivial abelian groups for which this is the only possible way to define a ring. We start by showing that $\mathbb{Q}/\mathbb{Z}$, the quotient group of the rationals modulo the integers, is such a group. We find other such groups and search for criteria characterizing groups that can have no nontrivial multiplication.

Example 1. Let $(\mathbb{Q},+)$ be the rationals under addition and $(\mathbb{Z},+)$ be the subgroup of integers. We can think of the quotient group $\mathbb{Q}/\mathbb{Z}$ as rational points around a circle, as in Figure 1. Any $\frac{a}{b}+\mathbb{Z}$ in $\mathbb{Q}/\mathbb{Z}$ with $b>0$ has order b, provided $\frac{a}{b}$ is in reduced form. That is, with the usual notation for repeated addition, $b(\frac{a}{b}+\mathbb{Z}) = 0+\mathbb{Z}$. For simplicity, shorten $\frac{a}{b}+\mathbb{Z}$ to $\frac{a}{b}$. We show that distributivity completely limits what multiplication can be defined on $\mathbb{Q}/\mathbb{Z}$. Let $*$ be any multiplication that makes $\mathbb{Q}/\mathbb{Z}$ a ring. As before, for $\frac{a}{b} \in \mathbb{Q}/\mathbb{Z}$ with $b \in \mathbb{N}$, $b(\frac{a}{b}) = 0$. Also, for any $\frac{c}{d} \in \mathbb{Q}/\mathbb{Z}$, we have $\frac{c}{d} = b(\frac{c}{bd})$. Then, using distributivity, $\frac{a}{b} * \frac{c}{d} = \frac{a}{b} * b(\frac{c}{bd}) = b(\frac{a}{b} * \frac{c}{bd}) = (b\frac{a}{b}) * \frac{c}{d} = 0$.

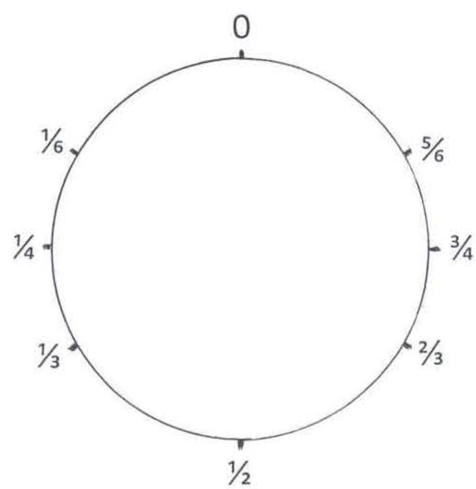

Figure 1.

The preceding argument used two properties of $\mathbb{Q}/\mathbb{Z}$. First of all, every element is of finite order. Secondly, for every $n \in \mathbb{N}$ and every element x, there is an element y such that adding y to itself n times gives $n(y) = x$. This last property appears sufficiently often in the study of infinite groups to merit a definition. (See [4, 180].)

Definition. A group $(G,+)$ is *divisible* iff for all $x \in G$ and for all $n \in \mathbb{N}$, there is $y \in G$ such that $n(y) = x$.

The rationals and reals are divisible. However, they have elements of infinite order and of course have familiar nontrivial multiplications. At the other extreme, nontrivial finite abelian groups have only elements of finite order, but they can't be divisible. However, as we'll see after Theorem 1, every nontrivial finite abelian group can have a nontrivial multiplication. So neither of the conditions above (finite order of each element and divisibility) are sufficient separately to force multiplication to be trivial. However, a direct modification of the argument in Example 1 shows that together these two properties suffice.

Theorem 1. If G is a divisible abelian group all of whose elements have finite order, then the only multiplication on G that gives a ring is the trivial multiplication.

Proof. Let $g, h \in G$, where $(G,+)$ is a divisible abelian group and every element is of finite order. Let $*$ be any binary operation such that $(G,+,*)$ is a ring. Suppose the order of g is n. By divisibility of G there is $j \in G$ such that $nj = h$. By distributivity and elementary ring properties $g * h = g * (nj) = n(g * j) = (ng) * j = 0 * j = 0$. Hence $*$ is the trivial multiplication.

The group with one element can only have the trivial multiplication. However, all other finite abelian groups have nontrivial multiplications: Let G be any finite abelian group with more than one element. By the Fundamental Theorem of Finite Abelian Groups, G is the direct product of cyclic groups with more than one element. (See [3, 217].) Turn each cyclic group with n elements into the ring $\mathbb{Z}_n$. Then the direct product of these rings has a nontrivial multiplication and the additive group is isomorphic to G.

Two questions arise naturally: Are there other groups that share these two properties? Are these properties necessary to force trivial multiplication? Example 2 and Theorem 2 partially answer the first question and Example 4 answers the second one.

Example 2. Let $\mathbb{Q}_2/\mathbb{Z} = \{\frac{a}{2^i} : i \in \mathbb{N},\ 0 \le a < 2^i\}$. This is a subgroup of $\mathbb{Q}/\mathbb{Z}$, so every element is of finite order. We show it is divisible. Let $\frac{a}{2^i} \in \mathbb{Q}_2/\mathbb{Z}$ and $n \in \mathbb{N}$. Then we can write $n = 2^k j$, where j is an odd positive integer and k is a nonnegative integer. First of all, $2^k(\frac{a}{2^i 2^k}) = \frac{a}{2^i}$. Now j is relatively prime to 2^i and $H = \{\frac{a}{2^{i+k}} \ :\ 0 \le a < 2^{i+k}\}$ is a finite cyclic group with 2^{i+k} elements. Hence, the mapping $\phi : H \to H$ given by $\phi(\frac{a}{2^{i+k}}) = \frac{aj}{2^{i+k}}$ is an automorphism of H. (See [3, 131].) Thus there is some $\frac{b}{2^{i+k}} \in H$ such that $j(\frac{b}{2^{i+k}}) = \frac{a}{2^{i+k}}$. Hence, $n(\frac{b}{2^{i+k}}) = 2^k j(\frac{b}{2^{i+k}}) = 2^k(\frac{a}{2^{i+k}}) = \frac{a}{2^i}$. By Theorem 1, only the trivial multiplication makes $\mathbb{Q}_2/\mathbb{Z}$ into a ring.

We can modify Example 2 to permit any set of primes to appear as factors in the denominator, as long as any primes that appear in the denominator can be raised to any positive exponent. That is, suppose P is any nonempty set of prime numbers, finite or infinite, and let $\mathbb{Q}_P/\mathbb{Z} = \{\frac{a}{b} : 0 \le a < b$ and there are finitely many primes $p_i \in P$ and nonnegative integers k_i such that $b = \prod_{i=1}^{n} p_i^{k_i}\}$. Then $\mathbb{Q}_P/\mathbb{Z}$ is a divisible subgroup of $\mathbb{Q}/\mathbb{Z}$. (For q a prime, $\mathbb{Q}_q/\mathbb{Z}$ is also written $\sigma(q^\infty)$ and is called the *q-primary component* of $\mathbb{Q}/\mathbb{Z}$. See [4, 179 - 183].)

The next example illustrates that we need unlimited exponents for divisible subgroups of $\mathbb{Q}/\mathbb{Z}$.

Example 3. Let $\mathbb{Q}_{SF}/\mathbb{Z} = \{\frac{a}{b} : 0 \le a < b$ and b is a square free integer$\}$. Again, this set forms an infinite subgroup of $\mathbb{Q}/\mathbb{Z}$ and all elements have finite order. The requirement of the denominator being square free means that no prime can have a higher power than 1 in the denominator. This means $\mathbb{Q}_{SF}/\mathbb{Z}$ is not divisible: 2 is in $\mathbb{N}$ and $\frac{1}{2} \in \mathbb{Q}_{SF}/\mathbb{Z}$, but the only solutions in $\mathbb{Q}/\mathbb{Z}$ to $2(\frac{a}{b}) = \frac{1}{2}$ are $\frac{1}{4}$ and $\frac{3}{4}$, neither of which are in $\mathbb{Q}_{SF}/\mathbb{Z}$.

Furthermore, we can define nontrivial multiplications on $\mathbb{Q}_{SF}/\mathbb{Z}$. For example, for reduced fractions define $\frac{a}{b} * \frac{c}{d} = \left\{ \begin{array}{cc} \frac{1}{2} & \text{if both } b \text{ and } d \text{ are even} \\ 0 & \text{otherwise} \end{array} \right\}$. We prove that $(\mathbb{Q}_{SF}/\mathbb{Z}, +, *)$ is a ring. For associativity, note that the product of three fractions is 0, unless all three denominators are even. For distributivity we need to consider $(\frac{a}{b} * \frac{c}{d}) + (\frac{a}{b} * \frac{e}{f})$ and $\frac{a}{b} * (\frac{c}{d} + \frac{e}{f})$. When b is odd, both terms are 0. Thus we suppose b is even. If both d and f are odd, the denominator of $\frac{c}{d} + \frac{e}{f}$ is also odd and so both terms are again 0. Next let, say, d be odd and f be even. Then $(\frac{a}{b} * \frac{c}{d}) + (\frac{a}{b} * \frac{e}{f}) = 0 + \frac{1}{2} = \frac{1}{2}$. Also, e must be odd for $\frac{e}{f}$ to be reduced. Hence $\frac{c}{d} + \frac{e}{f}$ will have an odd numerator and even denominator. This means that $\frac{a}{b} * (\frac{c}{d} + \frac{e}{f}) = \frac{1}{2}$ as well. Finally, suppose that both d and f are even. Then $(\frac{a}{b} * \frac{c}{d}) + (\frac{a}{b} * \frac{e}{f}) = \frac{1}{2} + \frac{1}{2} = 0$. Furthermore, c and e are odd since the fractions are reduced. Because both d and f have exactly one factor of 2 in them, the common denominator for $\frac{c}{d} + \frac{e}{f}$ has just one factor of 2. Hence in adding them, each denominator will be multiplied by an odd number to get the common denominator. Thus the two new numerators will be odd and their sum even. Then the reduced sum has an odd denominator and $\frac{a}{b} * (\frac{c}{d} + \frac{e}{f}) = 0$. This finishes showing distributivity and so $(\mathbb{Q}_{SF}/\mathbb{Z}, +, *)$ is a ring with nontrivial multiplication.

The next theorem uses familiar algebra constructions to find groups that have only trivial multiplication and are somewhat more general than subgroups of $\mathbb{Q}/\mathbb{Z}$.

Theorem 2. The direct product and homomorphic images of divisible abelian groups whose elements are all of finite order have only the trivial multiplication.

Proof. Suppose G and H are divisible abelian groups all of whose elements are of finite order. Let $(g,h) \in G \oplus H$, their direct product. The order of (g,h) is the least common multiple of the orders of g and h and so is finite. For $n \in \mathbb{N}$, by the divisibility of G and H, there are elements $g' \in G$ and $h' \in H$ such that $ng' = g$ and $nh' = h$. Then $n(g',h') = (g,h)$, showing $G \times H$ is divisible. By Theorem 1, the only multiplication on $G \times H$ is trivial.

Now suppose that $\phi : G \to K$ is a homomorphism from G onto a group K. Since G is abelian and ϕ is onto, K is abelian. Let $k \in K$. By onto there is $g \in G$ such that $\phi(g) = k$. The order of g is finite, say $|g| = n$. Then $nk = n\phi(g) = \phi(ng) = \phi(0) = 0$. Thus k has finite order. Now let $s \in \mathbb{N}$. By divisibility of G, there is some $g' \in G$ such that $sg' = g$. Then $s\phi(g') = \phi(sg') = \phi(g) = k$. So $\phi(g')$ fulfills the definition for K to be divisible. By Theorem 1, the only multiplication on K is trivial.

Surprisingly neither of the conditions in Theorem 1 is necessary, as Example 4 shows:

Example 4. Let $\mathbb{Q}_{SF} = \{\frac{a}{b} : b \text{ is square free}\}$. Note that this group is not divisible since, for example, $\frac{1}{2}$ can't be "divided in half": In $\mathbb{Q}$, if $x + x = \frac{1}{2}$, then $x = \frac{1}{4}$, which is not in $\mathbb{Q}_{SF}$. Also, every nonzero element of $\mathbb{Q}_{SF}$ is of infinite order. Nevertheless, the only multiplication on $\mathbb{Q}_{SF}$ is the trivial multiplication.

Proof. Suppose $*$ is a binary operation that makes $(\mathbb{Q}_{SF}, +, *)$ a ring. For a contradiction, suppose for some nonzero $\frac{a}{b}$ and $\frac{c}{d}$ in $\mathbb{Q}_{SF}$, their product $\frac{a}{b} * \frac{c}{d} = \frac{s}{t}$ is nonzero. Then by distributivity $\frac{s}{t} = \frac{a}{b} * \frac{c}{d} = a(\frac{1}{b}) * c(\frac{1}{d}) = ac(\frac{1}{b} * \frac{1}{d})$. Thus $\frac{1}{b} * \frac{1}{d} = \frac{s}{act}$ and so $1 * 1 = \frac{bds}{act}$, which isn't 0. For ease, write $1 * 1 = \frac{x}{y}$. For every prime p, $\frac{x}{y} = 1 * 1 = (p\frac{1}{p}) * (p\frac{1}{p}) = p^2(\frac{1}{p} * \frac{1}{p})$ and so $\frac{1}{p} * \frac{1}{p}$ is not zero. Furthermore since $\frac{1}{p} * \frac{1}{p}$ is in $\mathbb{Q}_{SF}$, it has at most one factor of p in its denominator. Thus x must have a factor of p in it. However, this would be true for every prime p, which would make x infinite, a contradiction. Hence, the multiplication must be trivial.

Since the group of Example 3 is the homomorphic image of the group in Example 4, the homomorphism part of Theorem 2 does not extend to groups whose only multiplication is trivial. A result from model theory answers the question of direct products of such groups in the affirmative.

Theorem 3. If G and H are abelian groups whose only multiplications are trivial, then $G \oplus H$ is an abelian group whose only multiplication is trivial.

Proof. We can write the condition that the only multiplication on $(G,+)$ is trivial as "For all binary operations $*$, if $*$ is associative and $*$ distributes over $+$, then for all $x,y \in G$, $x * y = 0$." Let A be the proposition "$*$ is associative," D be "$*$ distributes over $+$" and T be "for all $x,y \in G$, $x * y = 0$." This condition becomes "if A and D, then T," which is logically equivalent to "not A or not D or T." This is a Horn sentence. By Theorem 6.2.2 of [2, 328], this property is preserved under direct products.

It appears difficult to characterize completely those abelian groups whose only multiplication is trivial. A few theorems from [4, 175 - 192] providing a partial description of infinite abelian groups may point the way. Theorem 9.22 states "Every abelian group G can be imbedded in a divisible group." Theorem 9.13 states "Every divisible group D is the direct sum of copies of $\mathbb{Q}$ and of copies of [$\mathbb{Q}_p/\mathbb{Z}$, the primary components of $\mathbb{Q}/\mathbb{Z}$] (for various primes p)." Note that any element in a group isomorphic to $\mathbb{Q}_p/\mathbb{Z}$ has finite order, whereas every element in $\mathbb{Q}$, except the identity, has infinite order. The previous examples indicate divisibility interacts with elements of finite order and infinite order quite differently with regard to giving groups with only trivial multiplications. It appears that divisibility for elements of infinite order and non-divisibility for elements of finite order lead to nontrivial multiplications. However, one still needs to find such a multiplication, which Example 5 illustrates.

Example 5. The abelian, divisible group $\mathbb{R}/\mathbb{Z}$ has a nontrivial multiplication. While the factor corresponding to $\mathbb{Q}/\mathbb{Z}$ has only elements of finite order, for any irrational r the coset $r + \mathbb{Z}$ has infinite order in $\mathbb{R}/\mathbb{Z}$. Nevertheless, we still need to define a nontrivial multiplication and show it gives a ring. We consider $\mathbb{R}$ as a vector space over $\mathbb{Q}$. Using Zorn's Lemma, there is a basis for $\mathbb{R}$, called a Hamel basis. (See [4, 181 - 182].) Assume for ease that π is a basis vector. Then every $x \in \mathbb{R}$ can be written as a finite linear combination $x = a\pi + \sum$, where $\sum$ represents the remaining terms. For $a\pi + \sum + \mathbb{Z}$, $b\pi + \sum' + \mathbb{Z}$ in $\mathbb{R}/\mathbb{Z}$, define $(a\pi + \sum + \mathbb{Z}) * (b\pi + \sum' + \mathbb{Z}) = ab\pi + \mathbb{Z}$. For distributivity, let $a\pi + \sum + \mathbb{Z}$, $b\pi + \sum' + \mathbb{Z}$ and $c\pi + \sum'' + \mathbb{Z}$ be in $\mathbb{R}/\mathbb{Z}$. Then we have, for an appropriate finite linear combination $\sum^{\#}$,

$(a\pi + \sum + \mathbb{Z}) * (b\pi + \sum' + \mathbb{Z} \ + \ c\pi + \sum'' + \mathbb{Z}) = (a\pi + \sum + \mathbb{Z}) * ((b + \ c)\pi + \sum^{\#} + \mathbb{Z})$

$= a(b + c)\pi + \mathbb{Z} = (ab\pi + \mathbb{Z}) + (ac\pi + \mathbb{Z})$

$= (a\pi + \sum + \mathbb{Z}) * (b\pi + \sum' + \mathbb{Z}) + (a\pi + \sum + \mathbb{Z}) * (c\pi + \sum'' + \mathbb{Z})$.

Associativity is shown similarly.

References

1. W. Capecchi, "Circle groups and rings with trivial multiplication," St. John's University, 2009.

2. C. C. Chang and H. J. Keisler, *Model Theory*, New York: North-Holland, 1973.

3. J. A. Gallian, *Contemporary Abstract Algebra*, 6^{th} Ed., Boston: Houghton Mifflin, 2006.

4. J. J. Rotman, *The Theory of Groups: An Introduction*, Boston: Allyn and Bacon, 1965.