vulpeculiar musing 8: independent axioms in the definition of rings

vulpecule · 13 Aug 2026

https://functor.network/user/3486/entry/1928

It is a surprising fact, or at least a fact that surprised me when I learned it, that commutativity of addition is not actually a necessary imposition in the definition of a ring. In particular, any group with a monoid distributing over it is necessarily Abelian - in fact you don't even need associativity of multiplication, or even that the identity is two-sided.

To see this, consider that $(x+z)\cdot(y+u) = x(y+u)+z(y+u) = xy+xu+zy+zu$, but also $(x+z)\cdot(y+u) = (x+z)y+(x+z)u = xy+zy+xu+zu$, so clearly $xy+xu+zy+zu = xy+zy+xu+zu$. Then if we take $y = u = 1$, we get that $x+x+z+1 = x+z+x+1$, but cancellativity allows us to simply cancel out the outer terms and recover commutativity.

Each of these assumptions - two-sided cancellativity of addition, associativity of addition, two-sided distributivity, and one-sided multiplicative identity, are all necessary, and we can find counterexamples proving this.

- For one-sided cancellativity, simply consider a left- or right-zero band and the rule $0^2 = 0$; then any imposition of 1 being a left-, right-, or two-sided identity will all work.
- For nonassociativity, we can construct a unique multiplication by simply imposing $c^2 = b$ upon the additive quasigroup

$$\begin{array}{ccc} a & b & c \\ c & a & b \\ b & c & a \end{array}$$

- For multiplication without identity, simply consider the smallest non-Abelian group (S_3) with constant multiplication $xy = \mathrm{id}$.
- One-sided distributivity is harder, but there is a multiplication over D_8 that works; let's denote the identity as 0 and the single rotation as 1, the double rotation as 2, triple rotation as 3, and the reflection as σ, then this curious multiplication, with 1 as multiplicative

identity, works:

$$\begin{array}{cccccccc}
0 & 0 & 0 & 0 & \sigma & \sigma & \sigma & \sigma \\
0 & 1 & 2 & 3 & \sigma & \sigma+1 & 1+\sigma & \sigma+2 \\
0 & 2 & 0 & 2 & \sigma & \sigma+2 & \sigma+2 & \sigma \\
0 & 3 & 2 & 1 & \sigma & 1+\sigma & \sigma+1 & \sigma+2 \\
0 & \sigma & 0 & \sigma & \sigma & 0 & 0 & \sigma \\
0 & \sigma+1 & 0 & \sigma+1 & 0 & \sigma+1 & \sigma+1 & 0 \\
0 & 1+\sigma & 0 & 1+\sigma & 0 & 1+\sigma & 1+\sigma & 0 \\
0 & \sigma+2 & 0 & \sigma+2 & \sigma & 2 & 2 & \sigma
\end{array}$$

Thus, an independent axiomatization of rings would omit additive commutativity. In fact, this is an independent axiomatization:

- addition forms a (left or right) quasigroup (can be given quasi-equationally or equationally)
- addition is associative
- multiplication is associative
- multiplication has a two-sided identity
- multiplication distributes over addition on both sides

That this actually defines a ring is clear, given the fact that all associative quasigroups are groups alongside the above commutativity theorem, and we can exhibit independence by finding some counterexamples…

- A ring with non-quasigroup addition is easily exhibited by the two-element structure with addition given by $x + y = 0$
- A ring with nonassociative addition can be given by equipping the usual multiplicative monoid of $\mathbb{Z}_3$ with the addition of this commutative and idempotent quasigroup

  $$\begin{array}{ccc}
  a & c & b \\
  c & b & a \\
  b & a & c
  \end{array}$$

- A ring with nonassociative multiplication (a so-called “NA-ring”) can be given by equipping the ring $\mathbb{Z}_2^3$ with a new multiplication defined by $(x, y, z) \times (w, v, u) = (x \ominus w, y \ominus v, z \cdot u)$, where $\ominus$ is Boolean NAND and $\cdot$ is the usual multiplication of $\mathbb{Z}_2$, except for the special case $(x, x, x) = x$ defining the identity and absorbing elements.
- A ring without multiplicative identity (a rng) can be immediately given by equipping the Abelian group on two elements with a constant multiplication.
- Of course, a ring without distributivity is simply an arbitrary pair of an Abelian group and a monoid, and a nondistributive example is quickly given by Boolean NAND over $\mathbb{Z}_2$ again.

Now, the associativities are one thing, but two of the axioms are not really satisfactory due to being chiral. This leads us to the question of whether all of the axioms actually need two-sidedness to be explicitly imposed. Counterexemplifying this is not so hard:

- We can give V_4 a multiplication making it a rng with one-sided identity by simply taking the group identity to be multiplicatively absorbing, arbitrarily choosing two other elements to be left or right identities, and having the last element evaluate to 0 on the left or right.
- V_4 again admits monoidal multiplications distributing over it on only one side: pick an arbitrary nonidentity element to be the multiplicative identity, say the additive identity and another element are left or right absorbing, and define the remaining row or column by switching the absorbing elements and defining the final square to be the multiplicative identity.

Now, the final unsatisfactory thing is the quasigroup axiom, as the standard Birkhoff equational axiomatization of a quasigroup also uses four axioms, to wit, $x + (x -_\ell y) = y$ and $x -_\ell (x + y) = y$ alongside $(y -_r x) + x = y$ and $(y + x) -_r x = y$.

Unfortunately, we actually need to test all four of these, since our commutativity proof actually used both sides of cancellativity.

Happily however, we actually do end up needing either the former of each pair or the latter - proof left as an exercise to the reader - but both cancellativities are actually necessary as we showed at the very beginning of the musing.

Now we have a neat, satisfactory, and independent axiomatization of rings:

- $x + (x -_\ell y) = y$
- $(y -_r x) + x = y$
- $x + (y + z) = (x + y) + z$
- $x * (y * z) = (x * y) * z$
- $x * 1 = x$
- $1 * x = x$
- $(x + y)z = xz + yz$
- $z(x + y) = zx + zy$.

But what if we add commutativity of addition back in - does anything else then become redundant? Well, our explorations above actually already showed that no such redundancies arise, but there is actually a question they leave unanswered.

That is, what if we remove either quasigroup property or additive associativity, but add back in commutativity as well as an explicit additive identity? Clearly, at least one quasigroup property is necessary, as a rig (or semiring) is precisely the structure you get by removing that imposition, and clearly a commutative one-sided quasigroup is a two-sided quasigroup, but there is one implication that remains unclear:

- Is every commutative loop with a monoid distributing over it a group?

And, no, it isn't. Equip the group of order five with a zero element, take this as multiplication, and then behold this addition:

$$\begin{array}{cccccc} 0 & 1 & 2 & 3 & 4 & 5 \\ 1 & 0 & 3 & 4 & 5 & 2 \\ 2 & 3 & 0 & 5 & 1 & 4 \\ 3 & 4 & 5 & 0 & 2 & 1 \\ 4 & 5 & 1 & 2 & 0 & 3 \\ 5 & 2 & 4 & 1 & 3 & 0 \end{array}$$