STANDARD DEFINITIONS CONCERNING RINGS

KEITH CONRAD

Some abstract algebra books do not insist rings have a multiplicative identity, leading to the result that $2\mathbf{Z}$ is considered a subring of $\mathbf{Z}$. This is really, really bad. We will set out the correct definitions of subring, ring homomorphism, and ideal, and then come back to the issue of "rings without a multiplicative identity".

Definition 1. A *ring* is a set R equipped with two operations $+$ and $\times$ such that R is an abelian group under addition (identity denoted 0 and the inverse of a denoted as $-a$), while multiplication is associative with an identity element 1. Finally, multiplication distributes over addition: $x(y+z) = xy + xz$ and $(x+y)z = xz + yz$ for all x, y, and z in R.

Basically, R is a commutative group under addition, a "group without inverses" under multiplication, and multiplication distributes over addition. Examples of rings are $\mathbf{Z}$, $\mathbf{Q}$, and $\mathrm{M}_2(\mathbf{R})$, but *not* $2\mathbf{Z}$ since $2\mathbf{Z}$ does not have a multiplicative identity.

Definition 2. A *subring* of a ring R is a subset $R' \subset R$ which is a ring under the same $+$ and $\times$ as R and shares the same multiplicative identity.

Example 3. The ring $\mathbf{Z}$ is a subring of $\mathbf{Q}$. The ring $\mathbf{Z}/(m)$ for $m > 0$ has no subrings other than itself, since 1 additively generates all of $\mathbf{Z}/(m)$, so a subring contains 1 and then contains everything. The same argument (using $m = 0$) shows $\mathbf{Z}$ contains no subrings other than itself.

It might seem odd to insist in the definition of a subring that the subring has the same multiplicative identity as the original ring. Doesn't that follow from the rest of the definition? After all, a subgroup of a group is defined to be a subset which is a group for the same operation; its identity element can be proved to be the identity for the original group (and inverses for the subgroup are therefore the same as for the original group). But the proof of that uses cancellation in the group law, and in a ring we might not have cancellation for multiplication. This is all made clearer by seeing an actual example.

Example 4. In $\mathbf{Z}/(6)$, the subset $\{0, 3\}$ is closed under addition and multiplication since $3^2 = 9 = 3$. So $\{0, 3\}$ is a "subset with ring structure" having multiplicative identity 3. That is not the multiplicative identity for $\mathbf{Z}/(6)$, so we do not consider $\{0, 3\}$ to be a subring of $\mathbf{Z}/(6)$.

Remark 5. If the ring R has cancellation for multiplication (that is, $xz = yz \Rightarrow x = y$ when $z \neq 0$) then a "subset of R with ring structure" has to have the same multiplicative identity as the original ring (and thus is a subring) because if x is the multiplicative identity in a "subset with ring structure" then the equation $x^2 = x$ is satisfied, which is the same as $x \cdot x = x \cdot 1$, forcing $x = 1$ if $x \neq 0$. Thus for rings with cancellation the constraint of having the same multiplicative identity is automatic from the other properties of a subring.

Theorem 6. *If R' is a subring of R then the inclusion mapping $R' \hookrightarrow R$ is a ring homomorphism.*

Proof. Easily the inclusion map sends sums to sums and products to products. The multiplicative identity goes to the multiplicative identity because R' has the same multiplicative identity as R! □

You might be thinking: what is the big fuss about subrings having the same identity for multiplication? There are reasons for wanting this which have to do with invertible elements. An element $x \in R$ is called a *unit* if it has a 2-sided inverse: $xy = yx = 1$ for some $y \in R$. The set of all units forms a group, denoted $R^\times$. For example, $\mathbf{R}^\times = \mathbf{R} - \{0\}$, $\mathbf{Z}^\times = \{\pm 1\}$, and $\mathrm{M}_n(\mathbf{R})^\times = \mathrm{GL}_n(\mathbf{R}) = \{A \in \mathrm{M}_n(\mathbf{R}) : \det A \neq 0\}$.

Theorem 7. *If R is a ring and R' is a subring then $R'^\times$ is a subgroup of $R^\times$.*

Proof. Let 1 be the multiplicative identity in R, so it is also the multiplicative identity in R'. Since R' has the same multiplicative identity as R, if $x \in R'^\times$ then $xy = yx = 1$ for some $y \in R'$, so $x \in R^\times$ and the inverse of x in R' is also its inverse in R. We have shown $R'^\times$ is a subset of $R^\times$. Since the group law (multiplication) and inversion in R' are the same as in R, $R'^\times$ is a subgroup of $R^\times$. □

Example 8. We return to the nonexample of $\{0, 3\}$ in $\mathbf{Z}/(6)$. As a "subset with ring structure," $\{0, 3\}$ has multiplicative identity element 3, which is not a unit in $\mathbf{Z}/(6)$. So the one unit in the "ring that's not a subring" $\{0, 3\}$ is not a unit in $\mathbf{Z}/(6)$.

It would be terrible for the units in a subring not to be units in the larger ring, and insisting that subrings have the same multiplicative identity as the whole ring means this weirdness will not happen: units of a subring are units of the larger ring.

Definition 9. If R and S are rings, a *ring homomorphism* $f\colon R \to S$ is a function that preserves addition, multiplication, and the multiplicative identity: $f(x + y) = f(x) + f(y)$ and $f(xy) = f(x)f(y)$ for all x and y in R, and $f(1) = 1$.

Again we see an awkward, but necessary, axiom about the multiplicative identity. The definition does not include the analogous additive condition $f(0) = 0$ since that is automatic because f is an additive group homomorphism and group homomorphisms always preserve the identities (and inverses). But under multiplication a ring is not a group, and sometimes weird things can happen as in the next example (which builds on the previous one).

Example 10. Let $f\colon \mathbf{Z}/(6) \to \mathbf{Z}/(6)$ by $f(x) = 3x$. Since $3^2 = 3$ in $\mathbf{Z}/(6)$, we have $f(x) + f(y) = 3x + 3y = 3(x + y) = f(x + y)$ and also (the key point) $f(x)f(y) = 3x \cdot 3y = 3^2xy = 3xy = f(xy)$. Thus f is additive and multiplicative, but $f(1) \neq 1$ so f is *not* a ring homomorphism. In fact, the *only* ring homomorphism $\mathbf{Z}/(6) \to \mathbf{Z}/(6)$ is the identity function: once 1 goes to 1 everything else is fixed too by additivity.

Here is a result involving units which would not be true if a ring homomorphism did not preserve the multiplicative identities.

Theorem 11. *Let $f\colon R \to S$ be a ring homomorphism. Then $f(R^\times) \subset S^\times$ and the function $f\colon R^\times \to S^\times$ is a group homomorphism.*

Proof. If $xy = yx = 1$ in R then applying f gives us $f(x)f(y) = f(y)f(x) = f(1) = 1$, so f sends units in R to units in S. Since f is multiplicative, it is a group homomorphism from $R^\times$ to $S^\times$. □

When $R \subset S$, this theorem recovers Theorem 7 since the inclusion mapping $R \to S$ is a ring homomorphism.

In group theory, the kernel and image of a group homomorphism are subgroups. For a ring homomorphism $f\colon R \to S$, we have the kernel $\ker f = \{x \in R : f(x) = 0\}$ and image $f(R)$. Are these subrings (of R and S respectively)?

Theorem 12. *Let $f\colon R \to S$ be a ring homomorphism. Then the image is a subring of S, but the kernel is not a subring of R unless S is the zero ring.*

Proof. From the definition of a ring homomorphism, the sum and product of f-values are f-values. The image also contains 1 since $f(1) = 1$. So the image of f is a subring of S.

The kernel of f is closed under addition and multiplication, but $f(1) = 1$ and $1 \neq 0$ in S unless S is the zero ring, so except when $S = \{0\}$ the kernel of f is not a subring of R. □

It is this theorem which probably accounts for authors not insisting that rings contain 1. Kernels of ring homomorphisms have all the properties of a subring except they almost never contain the multiplicative identity. So if we want ring theory to mimic group theory by having both kernels and images of ring homomorphisms be subrings, then we should not insist that subrings contain 1 (and thus perhaps not even insist that rings contain 1). Then kernels of ring homomorphisms could be considered subrings. But the progress of ring theory has shown that this is a bad idea. While kernels of group homomorphisms are special kinds of subgroups (normal subgroups), kernels of ring homomorphisms are simply something *other than* subrings. What are they?

The kernel of a ring homomorphism satisfies a stronger multiplicative condition than being closed under multiplication in itself: if $f\colon R \to S$ is a ring homomorphism and $x \in \ker f$, so $f(x) = 0$, then for *any* $y \in R$ we have $f(xy) = f(x)f(y) = 0 \cdot f(y) = 0$ and $f(yx) = f(y)f(x) = f(y) \cdot 0 = 0$, so xy and yx are in the kernel too. The kernel of f is closed under multiplication by *arbitrary* elements of the ring. Contrast this with $\mathbf{Z}$ as a subring of $\mathbf{Q}$: multiplication of an integer by most elements of $\mathbf{Q}$ will not again be an integer.

Definition 13. An *ideal* in a ring R is an additive subgroup $I \subset R$ such that $RI \subset I$ and $IR \subset I$. That is, if $x \in I$ then $Rx \subset I$ and $xR \subset I$: all multiples of x in R lie in I.

Example 14. A basic example of an ideal in any commutative ring R is the multiples of one element: for $a \in R$, $Ra = \{ra : r \in R\}$ is an ideal in R since a sum and difference of two multiples is again a multiple and (most importantly) any multiple of a multiple is again a multiple. These ideals are called *principal ideals*. For instance, the even numbers $2\mathbf{Z}$ are a principal ideal in the ring $\mathbf{Z}$ but they are not a subring of $\mathbf{Z}$.

If R is noncommutative then this attempt to construct an ideal runs into trouble when you switch the side you multiply on. We need to consider not only left multiples of a but also right multiples. We're still not done: this set $RaR = \{ras : r, s \in R\}$ is usually not closed under addition. So we have to take finite sums of these little two-sided products, getting $r_1as_1 + \cdots + r_nas_n$ for $n \geq 1$ and $r_i, s_i \in R$. Now *that* is an ideal. Very tedious! This is why you should not try to learn about ideals first in noncommutative rings. It's too darn complicated. Focus on ideals in the commutative setting until you get used to them.

Example 15. An ideal in a commutative ring which is not of the special form Ra is the polynomials in $\mathbf{Z}[X]$ with even constant term: $I = \{f(X) \in \mathbf{Z}[X] : f(0) \text{ is even}\}$. Examples of elements of I are 2, X, and $X^2 + 3X + 10$. Check I is an ideal in $\mathbf{Z}[X]$ yourself. We will show I is not the multiples of some polynomial by contradiction. Assume $I = \mathbf{Z}[X]f(X)$ for some $f(X)$. Since $2 \in I$, $2 = g(X)f(X)$ for some $g(X)$, so $f(X)$ has to be a constant

polynomial. Write $f(X) = c$. Then $2 = g(X)c$, so $c = \pm 1$ or ± 2. Since c is in the ideal, it must be even, so $c = \pm 2$. Because $X \in I$, $X = h(X)c$ for some $h(X)$, but the left side is a monic polynomial and the right side has even leading coefficient. We have a contradiction.

Example 16. The most important way ideals occur in mathematics is as kernels of ring homomorphisms. Any kernel of a ring homomorphism is an ideal. Using quotient rings (analogous to quotient groups) one can show any ideal in a ring can be viewed as the kernel of a suitable ring homomorphism. This is parallel to the position of normal subgroups in group theory: any kernel of a group homomorphism is a normal subgroup and the quotient group construction shows any normal subgroup is the kernel of some group homomorphism.

As David Rohrlich has nicely put it, ideals are "contagious for multiplication." That may help you remember their defining property when you're first working with them.

The ring $\mathbf{Z}$ is not an ideal in $\mathbf{Q}$, since rationals times integers are not always integers. More generally, a proper subring of a ring is not an ideal: if $R' \subset R$ are rings and R' is an ideal of R, then since $1 \in R'$ (!) we get for all $x \in R$ that $x = x \cdot 1 \in R'$. Thus $R = R'$. So except for the whole ring, which is both a subring and ideal of itself, subrings and ideals are absolutely separate concepts.

Having tried to explain why rings should contain a multiplicative identity (and what this implies about the correct definitions of subring and ring homomorphism), we should admit that "ring-like" systems without a multiplicative identity do occur in mathematics, especially in analysis.

Example 17. Consider the ring $C_0(\mathbf{R})$ of continuous functions $\mathbf{R} \to \mathbf{R}$ which vanish at $\pm\infty$. Under pointwise addition and multiplication this has the properties of a commutative ring, but it does not have a multiplicative identity since that should be the constant function 1, which does not vanish at $\pm\infty$.

Besides pointwise multiplication of functions, another (more?) important commutative multiplication-like operation in analysis is *convolution* (look up the definition in any analysis book). In many important cases there is no convolution identity, so under addition and convolution one has another example in analysis of a "commutative ring without identity".

On account of these examples, do analysts use the word "ring" without requiring an identity? No, because there already is a perfectly standard term for "rings possibly without identity": they are $\mathbf{Z}$-algebras in the sense of the following definition.

Definition 18. Let R be a commutative ring with identity. An *R-algebra* is an abelian group A which admits an associative multiplication $A \times A \to A$ and a scalar multiplication by R, $R \times A \to A$. Denoting these by $(a, b) \mapsto ab$ and $(r, a) \mapsto ra$, respectively, the conditions are

(1) $a(b + c) = ab + ac$, and $(a + b)c = ac + bc$ for all a, b, and c in A,
(2) $r(a + b) = ra + rb$ for all $r \in R$ and a and b in A,
(3) $r(ab) = (ra)b = a(rb)$ for all $r \in R$ and a and b in A,
(4) $(rs)(a) = r(sa)$ for all r and s in R and a in A,
(5) $1 \cdot a = a$ for all $a \in A$.

If S is a ring containing R as a subring then S is an R-algebra using the multiplication in S to define how R multiplies elements of S. Also $\mathrm{M}_n(\mathbf{R})$ is an $\mathbf{R}$-algebra by the usual scaling of real $n \times n$ matrices by real numbers. The set $C([0, 1])$ of continuous functions $[0, 1] \to \mathbf{R}$ is an $\mathbf{R}$-algebra under pointwise addition and multiplication.

With this terminology, a "ring possibly without identity" is the same thing as a $\mathbf{Z}$-algebra. (Requiring $1 \cdot a = a$ forces a unique meaning on $n \cdot a$ for all $n \in \mathbf{Z}$.) Returning to our example from analysis, the set $C_0(\mathbf{R})$ with pointwise addition and multiplication is not just a $\mathbf{Z}$-algebra but also an $\mathbf{R}$-algebra (which is usually how analysts think about it). In analysis there are other "algebras," such as Banach algebras and C^*-algebras. These are certain kinds of algebras over $\mathbf{R}$ and $\mathbf{C}$ with additional constraints coming from analysis.

Usually one also assumes the multiplication in an R-algebra is associative ($a(bc) = (ab)c$ for all a, b, and c in the algebra), so usually "R-algebra" means "associative R-algebra." There are some important examples of nonassociative algebras. The most basic one is $\mathbf{R}^3$ under addition and the cross product, which is an $\mathbf{R}$-algebra but is not associative. (There is definitely no identity for the cross product!) This is an example of a *Lie algebra*.