Ring theory review

Mendel Keller

November 6, 2017

1 Defining things

A ring A is a set, equipped with two operations, $+, *$ (these take a pair of elements in A to a third element of A), and two special elements, which we denote $0, 1$ satisfying the following properties. For any $a, b, c \in A$:

1. $a + b = b + a$
2. $a + b + c = (a + b) + c = a + (b + c)$
3. $a + 0 = 0 + a = a$
4. $\forall a \in A \exists (-a) \in A : a + (-a) = 0$ (read "for all a in A there exists an element $(-a)$ in A such that...")
5. $a * b = b * a$ (not in general true, but we will only consider these rings, called commutative rings)
6. $a * (b * c) = (a * b) * c = a * b * c$
7. $a * 1 = 1 * a = a$
8. $a * (b + c) = a * b + a * c$

I will from here on sometimes omit the $*$ and write $a * b$ as ab, as this is more natural. I only used it in the above to be clear about how things are being defined.

You'll notice in the above that the axioms could be paired off in the following way: $1 - 4$ tell us how $+$ works, while $5 - 7$ tell us how $*$ works, and 8 tells us how these two relate to each other. Notice that the difference between $+$ and $*$ is that for $+$ we can always find an element to get us to 0, but for $*$ we don't always have an element to get us to 1. This kind of element is called an *inverse* and $0, 1$ are called *identities.*

2 Some examples and properties

A few examples of rings are $\mathbb{Z} = \{\ldots - 2, -1, 0, 1, 2 \ldots\}$ the set of integers, $\mathbb{Q}$ the set of fractions, $\mathbb{R}$ the set of real numbers (where we include things like π,$\sqrt{2}$ and $\sqrt[5]{7}$), and $\mathbb{C}$ the set of complex numbers. In all of these, 0 and 1 have their usual meaning, as do $+$ and $*$ as addition and multiplication, which explains our choice of notation.

Now, we said our ring has the two elements 0 and 1, but we didn't say whether they are the same or different. I.e. one can wonder, what if $0 = 1$? Before we address this, we first prove a fact about 0, one that may well seem unsurprising.

Theorem 1. *For any $a \in A$, we have $a * 0 = 0$.*

Proof. We have that $0 = 0 + 0$ (axiom 3) so that $a * 0 = a(0 + 0) = a * 0 + a * 0$ (axiom 8) but for $a * 0$ we have an element $-(a * 0)$ so that we get $0 = a * 0 - (a * 0) = a * 0 + (a * 0 - (a * 0)) = a * 0 + 0 = a * 0$. ■

Now say that $1 = 0$, then by axiom 7 any element a is equal to $a * 1$ but if $1 = 0$ then this equals $a * 0 = 0$ so that not only is 1 equal to 0 *everything* is equal to 0. This ring where everything is equal to 0 is called the zero ring. A bunch of statements about rings won't apply to the zero ring, and we will generally not be concerned with it.

3 Ideals

An ideal I of a ring A is a subset of A, satisfying the following conditions:

1. $a, b \in I \Rightarrow a + b \in I$
2. $r \in A, a \in I \Rightarrow ar \in I$

Or, in English, adding elements of an ideal stays in the ideal, and multiplying by any ring element stays in the ideal. Ideals are one of the central objects of study in algebra, and are used throughout (algebraic) number theory and algebraic geometry.

4 Examples of ideals

In any ring, we are naturally given two ideals, which we label (0) and (1). The ideal (0) consists of just the element 0. It is easy to see that this is an ideal, since $0 + 0 = 0$ and $a * 0 = 0$ for every a. The other ideal, (1), is just equal to the whole ring A, which is an ideal since addition and multiplication always give you another ring element.

Let's now consider ideals in the above mentioned example rings. In the ring $\mathbb{Z}$, the set of all even integers forms an ideal, since adding two of these remains even, and multiplying by any integer also remains even ($2m + 2n = 2(m+n)$ and $(2m)n = 2(mn)$ so that these are also even). In fact, we can do this in general for any element of $\mathbb{Z}$, and all multiples of that element I.e. all multiples of 3 or 4 etc. We denote all multiples of 3 by (3), and similarly for any $n \in \mathbb{Z}$ we write (n). As above, we get for any n that $na + nb = n(a + b)$ and $(na)b = n(ab)$ so that addition in the ideal and multiplication by ring elements stays in the ideal. This explains our choice of denoting the ideal $(1) = A$, since every element $a \in A$ is a multiple of 1, namely 1 times itself, $1a = a$.

However, when we consider ideals in $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$, we find that if an ideal I has an element a that isn't 0, then there's another element b in the ring such that $ab = 1$ for example in $\mathbb{Q}$ or $\mathbb{R}$ we can take $b = \frac{1}{a}$. But then we can get any other c in the ring, by multiplying $a(bc) = (ab)c = 1 * c = c$ so that everything is in I. We have just seen that these rings have only the two ideals that every ring has, and no more, and that this is somehow related to being able to multiply two elements and get to 1, this brings us to our next topic, fields.

5 Fields

A field is a ring where we have inverses for multiplication, but this is only possible for nonzero elements, so this is how we define a field, as a ring where every nonzero element has an inverse. We write a multiplicative inverse of a as a^{-1}. As noted above, $\mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are fields. An equivalent characterization is that a field is a ring with only two ideals, we will now prove this equivalence.

Theorem 2. *For any ring A: every nonzero element has a multiplicative inverse $\Leftrightarrow$ A has only two ideals.*

Proof. Say that every nonzero element has an inverse, and that $I \neq (0)$ is an ideal of A. Let $x \neq 0$ be an element of I, then for any $y \in A$ we have that $x^{-1}y \in A$ and so $x(x^{-1}y) = (xx^{-1})y = 1 * y = y$ so that $y \in I$ for every $y \in A$ and so $I = (1)$. Therefore, either $I = (0)$ or $I = (1)$.

Now say that A has only two ideals. Take any element x of A, we have an ideal generated by x, which we write (x), consisting of all multiples of x i.e. $(x) = \{ax : a \in A\}$. This is an ideal since $ax + bx = (a+b)x$ and $a(bx) = (ab)x$. Now take $x \neq 0$ since $x \in (x)$ and $x \notin (0)$ we have $(x) \neq (0)$ so that $(x) = (1)$. This tells us that for some $a \in A$ we have that $ax = 1$, and so every nonzero $x \in A$ is invertible, and A is a field. ■