Rules for arithmetic

A (commutative) ring (with unit) is a set R such that for each pair of elements a, b in R there are elements $a + b$ (a plus b) and $a \cdot b = ab$ (a times b) satisfying the following 8 rules (axioms for a ring):

(1) There exists an element 0 in R such that if a is in R then $a + 0 = a$ (additive identity).

(2) There exists an element 1 in R such that if a is in R then $a \cdot 1 = a$ (multiplicative identity).

(3) If a, b are in R then $a + b = b + a$ (commutatitivity of addition or the commutative rule for addition).

(4) If a, b are in R then $ab = ba$ (commutatitivity of multiplication commutative rule for multiplication).

(5) If a, b, c are in R then $(a + b) + c = a + (b + c)$ (associatitivity of addition or the associative rule for addition).

(6) If a, b, c are in R then $(ab)c = a(bc)$ (associatitivity of multiplication or the associative rule for multiplication).

(7) If a is in R there is an element b in R such that $a + b = 0$. (Additive inverse or negative of a).

(8) If If a, b, c are in R then $a(b + c) = ab + ac$ (the distributive rule).

Our knowledge of arithmetic yields many examples of rings. For example:

I. The integers, $\mathbb{Z} = \{0, \pm 1, \pm 2, ..., \pm n, ...\}$ with the usual addition and multiplication.

2.The rational numbers $\mathbb{Q}$ consisting of the elements $\frac{a}{b}$ with a an integer and b a non-zero integer.

3. The real numbers, $\mathbb{R}$.

However there are many other examples for which the 8 rules above are true.

Example 1. $R = \{0\}$. That is it only has one element. Rule (1) says that R must have at least one element 0. The addition and multiplication must take values in R so we are forced to have $0 + 0 = 0$ and $00 = 0$.

Exercise. Show with this definition of addition and multiplication $(1)-(8)$ are satisfied (For instance: (5) is satisfied since $0 + (0 + 0) = 0 + 0$ (since $0 + 0 = 0$) and $0 + 0 = 0$ thus $0 + (0 + 0) = 0$ and $(0 + 0) + 0 = 0 + 0 = 0$ so $0 + (0 + 0) = 0 = (0 + 0) + 0$.)

Example 2. $R = \{0, 1\}$ and addition is given as follows:

$$0+0=0, 0+1=1, 1+0=1, 1+1=0.$$

Multiplication is given as follows:

$$0\cdot 0=0, 0\cdot 1=0, 1\cdot 0=0, 1\cdot 1=1.$$

Notice that if the 8 rules are to be satisfied then the first three formulas for addition and the last three for multiplication are forced. We will see below that all are forced.

Exercise. Show that the 8 rules are true for this addition and multiplication.

We will now prove some theorems about rings. In other words we assume the truth of statements (1)-(8) above and use our rules of reasoning to show that other statements are true.

All elements below will be assumed to be in a ring R and $+$ and $\cdot$ will be the operations in the ring.

Theorem 1 *If* $a+0'=a$ *for all* a *in* R *then* $0'=0$.

Proof. Since 0 is in R the hypothesis implies that $0+0'=0$. But $0+0'=0'+0=0'$ by rule (1). Thus $0=0+0'=0'+0=0'$. ■

Discussion. The structure of this theorem is P implies Q which we also write as if P then Q. Here P is the statement: $a+0'=a$ for all a in R and Q is the statement $0'=0$. P is called the hypthesis and Q is called the conclusion. The proof says that the statement that the hypothesis implies the conclusion is true.

Exercise. Prove

If $a1'=a$ for all a in R then $1'=1$.

Theorem 2 *If* $a+b=0$ *and* $a+b'=0$ *then* $b=b'$.

Proof. The hypothesis implies that $a+b'=a+b=0$. Thus using rule (1) we have $(a+b)+b'=b'$. Using the commutative rule (3) we have $(a+b)+b'=(b+a)+b'$. The associative rule (5) implies that $(b+a)+b'=b+(a+b')$. The hypothesis implies that $a+b'=0$ and $b+0=b$. Thus we have the chain of equalities:

$$b' = (a+b)+b' = (b+a)+b' = b+(a+b') = b+0 = b.$$

■

This theorem allows us to use a special notation for the unique element that satisfies $a+b=0$. We denote it by $-a$. We will also write $c-a$ for $c+(-a)$.

Exercise. Use the same argument to prove that if for one a the element b satisfies $a+b=a$ then $b=0$.

This exercise shows that in our example above with exactly two elements $0,1$ as in rules 1 and 2 and $1 \neq 0$ we must have $1+1=0$. To see this suppose that instead we tried to define $1+1=1$ then the exercise implies that $1=0$. But this is false. So if $1+1=1$ and $1\neq 0$ the addition and multiplication as above (with this change) would not define a ring.

The next theorem involves a "trick". We start the argument with a true assertion about elements in a that appears to have nothing to do with the actual result that we are trying to prove.

Theorem 3 *If a is in a then $a\cdot 0 = 0$.*

Proof. Rule (2) says $a = a\cdot 1$. Rule (1) says that $1+0=1$ so $a = a(1+0)$. Rule (8) says that $a(1+0) = a1+a0$. Rule (2) says that $a1 = a$ so we have the conclusion

$$a = a + a0.$$

We add $-a$ to a and get 0 by definition of $-a$. Thus

$$0 = (a+a0)+(-a).$$

We use the commutative rule to get

$$0 = (a+a0)+(-a) = (a0+a)+(-a).$$

The associative rule yields

$$0 = (a+a0)+(-a) = (a0+a)+(-a) = a0+(a+(-a)).$$

Finally the definition of $-a$ implies that $a+(-a)=0$. So we conclude that $0 = a0+0 = a0$ by rule (1). The theorem is proved. ■

Discussion. This theorem implies that if we had a ring R with exactly 2 elements 0 and 1 as in rules 1 and 2 then we must have $00=0$ as in the example above.

Exercise. Prove that if R is a ring and $1=0$ in R then $R=\{0\}$.