15. Basic Properties of Rings

We first prove some standard results about rings.

Lemma 15.1. *Let R be a ring and let a and b be elements of R.*
Then

(1) $a0 = 0a = 0$.
(2) $a(-b) = (-a)b = -(ab)$.

Proof. Let $x = a0$. We have

$$\begin{aligned} x &= a0 \\ &= a(0+0) \\ &= a0 + a0 \\ &= x + x. \end{aligned}$$

Adding $-x$ to both sides, we get $x = 0$, which is (1).

Let $y = a(-b)$. We want to show that y is the additive inverse of ab, that is we want to show that $y + ab = 0$. We have

$$\begin{aligned} y + ab &= a(-b) + ab \\ &= a(-b + b) \\ &= a0 \\ &= 0, \end{aligned}$$

by (1). Hence (2). □

Lemma 15.2. *Let R be a set that satisfies all the axioms of a ring, except possibly $a + b = b + a$.*
Then R is a ring.

Proof. It suffices to prove that addition is commutative. We compute $(a + b)(1 + 1)$, in two different ways. Distributing on the right,

$$\begin{aligned} (a+b)(1+1) &= (a+b)1 + (a+b)1 \\ &= a + b + a + b \\ &= a + (b + a) + b. \end{aligned}$$

On the other hand, distributing this product on the left we get

$$\begin{aligned} (a+b)(1+1) &= a(1+1) + b(1+1) \\ &= a + a + b + b. \end{aligned}$$

Thus

$$a + (b + a) + a = (a + b)(1 + 1) = a + a + b + b.$$

Cancelling an a on the left and a b on the right, we get

$$b + a = a + b,$$

which is what we want. $\square$

Note the following identity.

Lemma 15.3. *Let R be a ring and let a and b be any two elements of R.*

Then

$$(a + b)^2 = a^2 + ab + ba + b^2.$$

Proof. Easy application of the distributive laws. $\square$

Definition 15.4. *Let R be a ring. We say that R is* **commutative** *if multiplication is commutative, that is*

$$a \cdot b = b \cdot a.$$

Note that most of the rings introduced in the the first section are not commutative. Nevertheless it turns out that there are many interesting commutative rings. Compare this with the study of groups, when abelian groups are not considered very interesting.

Definition-Lemma 15.5. *Let R be a ring. We say that R is* **boolean** *if for every $a \in R$, $a^2 = a$.*

Every boolean ring is commutative.

Proof. We compute $(a + b)^2$.

$$\begin{aligned} a + b &= (a + b)^2 \\ &= a^2 + ba + ab + b^2 \\ &= a + ba + ab + b. \end{aligned}$$

Cancelling we get $ab = -ba$. If we take $b = 1$, then $a = -a$, so that $-(ba) = (-b)a = ba$. Thus $ab = ba$. $\square$

Definition 15.6. *Let R be a ring. We say that R is a* **division ring** *if $R - \{0\}$ is a group under multiplication. If in addition R is commutative, we say that R is a* **field**.

Note that a ring is a division ring iff every non-zero element has a multiplicative inverse. Similarly for commutative rings and fields.

Example 15.7. *The following tower of subsets*

$$\mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$$

is in fact a tower of subfields. Note that $\mathbb{Z}$ is not a field however, as 2 does not have a multiplicative inverse. Further the subring of $\mathbb{Q}$ given *by those rational numbers with odd denominator is not a field either. Again 2 does not have a multiplicative inverse.*

Lemma 15.8. *The quaternions are a division ring.*

Proof. It suffices to prove that every non-zero number has a multiplicative inverse.

Let $q = a + bi + cj + dk$ be a quaternion. Let

$$\bar{q} = a - bi - cj - dk,$$

the conjugate of q. Note that

$$q\bar{q} = a^2 + b^2 + c^2 + d^2.$$

As a, b, c and d are real numbers, this product if non-zero iff q is non-zero. Thus

$$p = \frac{\bar{q}}{a^2 + b^2 + c^2 + d^2},$$

is the multiplicative inverse of q. □

Here is an obvious necessary condition for division rings:

Definition-Lemma 15.9. *Let R be a ring. We say that $a \in R$, $a \neq 0$, is a* **zero-divisor** *if there is an element $b \in R$, $b \neq 0$, such that, either,*

$$ab = 0 \qquad \text{or} \qquad ba = 0.$$

If a has a multiplicative inverse in R then a is not a zero divisor.

Proof. Suppose that $ba = 0$ and that c is the multiplicative inverse of a. We compute bac, in two different ways.

$$\begin{aligned} bac &= (ba)c \\ &= 0c \\ &= 0. \end{aligned}$$

On the other hand

$$\begin{aligned} bac &= b(ac) \\ &= b1 \\ &= b. \end{aligned}$$

Thus $b = bac = 0$. Thus a is not a zero divisor. □

Definition-Lemma 15.10. *Let R be a ring. We say that R is a* **domain** *if R has no zero-divisors. If in addition R is commutative, then we say that R is an* **integral domain***.*

Every division ring is a domain.

Unfortunately the converse is not true.

Example 15.11. *$\mathbb{Z}$ is an integral domain but not a field.*

In fact any subring of a division ring is clearly a domain. Many of the examples of rings that we have given are in fact not domains.

Example 15.12. *Let X be a set with more than one element and let R be any ring. Then the set of functions from X to R is not a domain. Indeed pick any partition of X into two parts, X_1 and X_2 (that is suppose that X_1 and X_2 are disjoint, both non-empty and that their union is the whole of X). Define $f\colon X \longrightarrow R$, by*

$$f(x) = \begin{cases} 0 & x \in X_1 \\ 1 & x \in X_2, \end{cases}$$

and $g\colon X \longrightarrow R$, by

$$g(x) = \begin{cases} 1 & x \in X_1 \\ 0 & x \in X_2. \end{cases}$$

Then $fg = 0$, but neither f not g is zero. Thus f is a zero-divisor.

Now let R be any ring, and suppose that $n > 1$. I claim that $M_n(R)$ is not a domain. We will do this in the case $n = 2$. The general is not much harder, just more involved notationally. Set

$$A = B = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}.$$

Then it is easy to see that

$$AB = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

Note that the definition of an integral domain involves a double negative. In other words, R is an integral domain iff whenever

$$ab = 0,$$

where a and b are elements of R, then either $a = 0$ or $b = 0$.

18.703 Modern Algebra
Spring 2013