11-29-1993

Rings.

Definition. A **ring** is a set R equipped with two binary operations, $+$ ("addition") and $\cdot$ ("multiplication"). The operations satisfy the following axioms:

1. R is an abelian group under $+$. The identity element is denoted 0.
2. For all $a, b, c \in R$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$.
3. For all $a, b, c \in R$,
$$a \cdot (b + c) = a \cdot b + a \cdot c \text{ and } (a + b) \cdot c = a \cdot c + b \cdot c.$$

   Some rings satisfy a fourth axiom:

4. There is a multiplicative identity element $1 \in R$, and $1 \neq 0$.

   A ring satisfying property 4 is called a **ring with** 1, or a **ring with unity**.

Remarks. I'll often suppress the multiplication symbol and simply write "ab" for "$a \cdot b$". In this case, a^2 denotes $a \cdot a$, and so on.

However, note that negative powers of elements are not always defined.

Note also that that multiplication need not be commutative. If $ab = ba$ for all $a, b \in R$, R is a **commutative ring**. □

Examples.

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are commutative rings with unity under the usual operations. □

2. Consider the set
$$\mathbb{H} = \{w + xi + yj + zk \mid w, x, y, z \in \mathbb{R}\}.$$

Here i, j, and k correspond to the symbols in the quaternion group $Q = \{\pm 1, \pm i, \pm j, \pm k\}$. Indeed, **H** is referred to as the **ring of quaternions**. Multiply elements using the multiplication table for Q. For example,
$$(3i - 2k) \cdot (3 + 2j) = 15i.$$

$\mathbb{H}$ is a noncommutative ring, since (e.g.) $ij = k$ but $ji = -k$. □

3. The set of even integers $2\mathbb{Z}$ with the usual operations is a ring without 1. □

4. $GL(2, \mathbb{R})$ is the set of 2×2 invertible matrices with real entries. The operations are the usual matrix addition and multiplication. $GL(2, \mathbb{R})$ is a noncommutative ring. □

5. $C[0, 1]$ is the set of continuous functions $f : [0, 1] \to \mathbb{R}$. Operations are pointwise addition and multiplication:
$$(f + g)(x) = f(x) + g(x) \text{ and } (fg)(x) = f(x)g(x).$$

$C[0, 1]$ is a commutative ring. The constant functions 0 and 1 are the additive and multiplicative identities, respectively. □

6. Let R be a commutative ring. $R[x]$ denotes the **ring of polynomials** in one variable with coefficients in R. Add and multiply polynomials as usual.

The formal, precise way to define $R[x]$ is to define it to be the collection of finite ordered n-tuples
$$\{(r_0, r_1, \ldots, r_n) \mid n \geq 0, r_i \in R\}.$$

(That is, a polynomial is the "vector" of its coefficients.) Now you can define addition and multiplication by writing down some ugly, unenlightening formulas. The point of this pedantry is that there is no flim-flam going on in talking about "formal sums in powers of x" — the usual way you think of polynomials.

Note that polynomials are not *functions* in this context. For example, let $R = \mathbb{Z}_2$ and look at $f(x) = x^2 + x$. This is *not* zero *as a polynomial*, even though $f(0) = 0$ and $f(1) = 1$; i.e., even though *it vanishes on every element of the ring.* $\square$

Definition. Let R be a ring. A **zero divisor** is a nonzero element $a \in R$ such that $ab = 0$ for some nonzero $b \in R$.

A commutative ring with unity having no zero divisors is an **integral domain** (or a **domain** for short).

Examples.

1. $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are integral domains. $\square$

2. $\mathbb{Z}_4$ is not an integral domain, since $2 \cdot 2 = 0$. In fact, $\mathbb{Z}_n$ is an integral domain if and only if n is prime. $\square$

3. $C[0, 1]$ is not an integral domain. For example, let

$$f(x) = \begin{cases} 0 & \text{if } 0 \le x \le \dfrac{1}{2} \\ x - \dfrac{1}{2} & \text{if } \dfrac{1}{2} < x \le 1 \end{cases}$$

$$g(x) = \begin{cases} \dfrac{1}{2} - x & \text{if } 0 \le x \le \dfrac{1}{2} \\ 0 & \text{if } \dfrac{1}{2} < x \le 1 \end{cases}$$

Then $f, g \ne 0$, but $fg = 0$. $\square$

Stupid ring tricks. Most elementary algebraic operations work the way you'd expect. Here are some easy ones. Let R be a ring.

1. If $r \in R$, then $r \cdot 0 = 0 = 0 \cdot r$.

   Note that
   $$r \cdot 0 = r \cdot (0 + 0) = r \cdot 0 + r \cdot 0.$$

   Therefore $0 = r \cdot 0$. $\square$

2. Let $r \in R$, and let $-r$ denote the additive inverse of r. If R is a ring with unity, then $(-1) \cdot r = -r$.

   Compute:
   $$(-1) \cdot r + r = (-1) \cdot r + 1 \cdot r = (-1 + 1) \cdot r = 0 \cdot r = 0.$$

   Therefore, $(-1) \cdot r$ is the additive inverse of r, i.e. $(-1) \cdot r = -r$. $\square$

3. Let $r, s \in R$. Then $(-r) \cdot s = -(rs) = r \cdot (-s)$.

   The proof is similar to the proof of 2. $\square$

Convention. If R is a ring and n is a positive integer, nr is short for $r + r + \cdots r$ (n summands). Likewise, if n is a negative integer, nr is $(-n)r$.

Notice that, for example, $13 \cdot 1 \in \mathbb{Z}_6$ makes sense according to this convention: It is 1 added to itself 13 times. However, you should not write "$13 \in \mathbb{Z}_6$", since 13 is *not* an element of $\mathbb{Z}_6$. $\square$

Lemma. Let R be a commutative ring with 1. R is a domain if and only if for all $r, s, t \in R$, $rs = rt$ and $r \ne 0$ implies $s = t$.

Remark. In other words, you can "cancel" nonzero factors in a domain.

Proof. Suppose R is a domain. Let $r, s, t \in R$, where $r \neq 0$, and suppose $rs = rt$. Then $rs - rt = 0$, so $r(s-t) = 0$. Since $r \neq 0$ and since R has no zero divisors, $s - t = 0$. Therefore, $s = t$.

Conversely, suppose for all $r, s, t \in R$, $rs = rt$ and $r \neq 0$ implies $s = t$. I will show that R has no zero divisors. Suppose $ab = 0$, where $a \neq 0$. Now $ab = 0 = a \cdot 0$, and by cancellation, $b = 0$. This shows that R has no zero divisors, so R is a domain. □

Example. $x^2 + 3x - 4 \in \mathbb{Z}_{12}$ has roots 1, 4, 5, 8 in $\mathbb{Z}_{12}$. Thus, a polynomial of degree n can have more than n roots in a ring. The problem is that $\mathbb{Z}_{12}$ is not a domain: $(x+4)(x-1) = 0$ does not imply one of the factors must be zero. □

Definition. A **division ring** is a ring with 1 in which every nonzero element has a multiplicative inverse. (Thus, the nonzero elements in a division ring form a group under multiplication.) A commutative division ring is a **field**.

Remark. Here is a picture which shows how the various types of rings are related:

$$\begin{array}{ccccc} & & \text{ring} & & \\ & \swarrow & & \searrow & \\ \text{commutative ring} & & & & \\ \downarrow & & & & \text{division ring} \\ \text{domain} & & & & \\ & \searrow & & \swarrow & \\ & & \text{field} & & \end{array}$$

Lemma. Fields are integral domains.

Proof. Let F be a field. I must show that F has no zero divisors. Suppose $ab = 0$ and $a \neq 0$. Then a has an inverse a^{-1}, so $a^{-1}ab = a^{-1} \cdot 0$, or $b = 0$. Therefore, F has no zero divisors, and F is a domain. □

Examples.

1. $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ are fields. $\mathbb{Z}$ is not a field, though it is a domain. □

2. The ring of quaternions

$$\mathbb{H} = \{w + xi + yj + zk \mid w, x, y, z \in \mathbb{R}\}$$

is a division ring, but not a field (it's not commutative). □

3. Consider

$$\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}.$$

Use the operations inherited from the reals. This is clearly a commutative ring. To show that it's a field, suppose $a + b\sqrt{2} \neq 0$. Then

$$a + b\sqrt{2} = \frac{a - b\sqrt{2}}{a^2 - 2b^2}.$$

I must show that $a^2 - 2b^2 \neq 0$.

If $a = 0$ and $b \neq 0$ or if $a \neq 0$ and $b = 0$, then $a^2 - 2b^2 \neq 0$. Since $a + b\sqrt{2} \neq 0$, the only other possibility is $a, b \neq 0$.

Thus, $a^2 = 2b^2$ with $a, b \neq 0$. Clearing denominators if necessary, I may assume that a and b are integers — in fact, positive integers, thanks to the squares. Now 2 divides $2b^2$, so $2 \mid a^2$. This forces $2 \mid a$, so $a = 2c$ for some integer c. Plugging in gives $4c^2 = 2b^2$, or $2c^2 = b^2$.

Repeat the argument: $2 \mid b^2$, so $2 \mid b$, so $b = 2d$. Plugging in gives $2c^2 = 4d^2$, or $c^2 = 2d^2$.

I can continue this process indefinitely. Notice that $a > c > \ldots$ and $b > d > \ldots$. This yields infinite descending sequences of positive integers, contradicting well-ordering. Therefore, $a^2 - 2b^2 \neq 0$. (This is called an argument by **infinite descent**.)

It follows that every nonzero element of $\mathbb{Q}[\sqrt{2}]$ is invertible, so $\mathbb{Q}[\sqrt{2}]$ is a field. □

Proposition. A finite integral domain is a field.

Proof. Let R be a finite domain. Say

$$R = \{r_1, r_2, \ldots, r_n\}.$$

I must show that nonzero elements are invertible. Let $r \in R$, $r \neq 0$.

Consider the products $rr_1, rr_2, \ldots, rr_n$. If $rr_i = rr_j$, then $r_i = r_j$ by cancellation. Therefore, the rr_i are distinct. Since there are n of them, they must be exactly all the elements of R:

$$R = \{rr_1, rr_2, \ldots, rr_n\}.$$

Then $1 \in R$ equals rr_i for some i, so r is invertible. $\square$

Proposition. $m \in \mathbb{Z}_n$ is a zero divisor if and only if $(m, n) \neq 1$.

Proof. First, I'll show that if $(m, n) = 1$, then m is not a zero divisor. Suppose $(m, n) = 1$, so $am + bn = 1$ for some $a, b \in \mathbb{Z}$. Reducing the equation mod n, $a'm = 1$ for some $a' \in \mathbb{Z}_n$, where $a = a' \bmod n$.

Now suppose $k \in \mathbb{Z}_n$ and $mk = 0$. Then

$$a'm = 1, \quad a'mk = k, \quad 0 = k.$$

Therefore, m is not a zero divisor.

Conversely, suppose that $(m, n) = k > 1$. Say $n = ka$, where $1 < a < n$. In particular, I may regard a as a nonzero element of $\mathbb{Z}_n$.

The order of m in $\mathbb{Z}_n$ is $\dfrac{n}{(m, n)} = \dfrac{n}{k} = a$. Thus, $ma = 0$ in $\mathbb{Z}_n$, and m is a zero divisor. $\square$

Corollary. $\mathbb{Z}_n$ is a field if and only if n is prime.

Proof. If n is composite, I may find a, b such that $1 < a, b < n$ and $ab = n$. Regarding a and b as elements of $\mathbb{Z}_n$, I obtain $ab = 0$ in $\mathbb{Z}_n$. Therefore, $\mathbb{Z}_n$ has zero divisors, and is not a domain. Since fields are domains, $\mathbb{Z}_n$ is not a field.

Suppose n is prime. The nonzero elements $1, \ldots, n-1$ are all relatively prime to n. Hence, they are not zero divisors in $\mathbb{Z}_n$, by the preceding result. Therefore, $\mathbb{Z}_n$ is a domain. Since it's finite, it's a field. $\square$

The fields $\mathbb{Z}_p$ for p prime are examples of fields of **finite characteristic**.

Definition. The **characteristic** of a ring R is the smallest positive integer n such that $n \cdot 1 = 0$. If there is no such integer, the ring has **characteristic** 0. Denote the characteristic of R by $\operatorname{char} R$.

Examples. $\mathbb{Z}$, $\mathbb{R}$, and $\mathbb{C}$ are fields of characteristic 0. If p is prime, $\mathbb{Z}_p$ is a field of characteristic p.

More generally, if F is a field of characteristic $n > 0$, then n is prime. For if n is composite, write $n = rs$, where $1 < r, s < n$. Then

$$(r \cdot 1)(s \cdot 1) = rs \cdot 1 = n \cdot 1 = 0.$$

But $r \cdot 1 \neq 0$ and $s \cdot 1 \neq 0$ since $r, s < n$. Therefore, F has zero divisors, contradicting the fact that fields are domains.

Note, however, that $\mathbb{Z}_p$ for p prime is not the only field of characteristic p. In fact, for each $n > 0$, there is a unique field F of characteristic p such that $|F| = p^n$. $\square$

Lemma. $\operatorname{char} R = n$ if and only if $nr = 0$ for all $r \in R$.

Proof. ($\Rightarrow$) Suppose $\operatorname{char} R = n$. If $r \in R$, then $r \cdot 1 = r$, so $n \cdot (r \cdot 1) = n \cdot r$.

$$n \cdot (r \cdot 1) = \underbrace{r \cdot 1 + \ldots + r \cdot 1}_{n \text{ times}} = r \cdot \underbrace{(1 + \ldots + 1)}_{n \text{ times}} = r \cdot (n \cdot 1) = 0.$$

($\Leftarrow$) $n \cdot r = 0$ for all $r \in R$ implies $n \cdot 1 = 0$. $\square$