

Special Rings

Definition: An integral domain is a commutative ring with unity that has no zero divisors.

Integral domains can have either finite order or infinite order. Z_7 is an integral domain of finite order but Z_6 is not. The reals are an integral domain of infinite order, but the 2×2 matrices are not an integral domain because they have zero divisors and also they are not commutative.

Definition: A division ring is a ring with unity in which every non-zero element is a unit.

Definition: A field is a commutative ring with unity in which every non-zero element is a unit.

Clearly every field is also a division ring but not every division ring is a field. The key is commutativity. If a division ring is not commutative it can not be a field. Since multiplication is well defined, closed and associative in any ring, the definitions of both fields and division rings guarantee that with respect to multiplication both of these rings form groups. Therefore both division rings and fields form groups with respect to both of their binary operations.

Theorem: If R is either a field or a division ring then R has no zero divisors.

Proof: Suppose not. Suppose x is a zero divisor and $x \in R$. By definition $x \neq 0$. Therefore, since R is a field or a division ring, x^{-1} exists. Further, there must exist $y \neq 0$ such that $x \cdot y = 0$ or $y \cdot x = 0$. Without loss of generality, let's suppose $x \cdot y = 0$.

$$\begin{aligned} \therefore x^{-1}(x \cdot y) &= x^{-1} \cdot 0 \\ \Rightarrow (x^{-1} \cdot x)y &= 0 \\ \Rightarrow 1 \cdot y &= 0 \\ \Rightarrow y &= 0 \\ \longrightarrow &\longleftarrow \end{aligned}$$

If $y \cdot x = 0$, the sequence of steps is similar.

QED

Theorem: Let R be a ring with unity. No non-trivial ideal of R can contain 1.

Proof: Suppose I is an ideal of R and $1 \in I$. Let x be any element of R . Since I is an ideal, $x \cdot 1 \in I$. $\therefore x \in I$. Since x was any element of R , $I = R$.

QED

Theorem: Division rings and fields have no non-trivial ideals.

Proof: Let R be either a division ring or a field. Let I be an ideal of R . If $I = \{0\}$, we are done. If $I \neq \{0\}$, there must be an element $x \in R$ such that $x \neq 0$ and $x \in I$. Since x must be a unit, x^{-1} exists. Since I is an ideal, $x^{-1} \cdot x \in I$. $\therefore 1 \in I$. By our previous theorem, I must be trivial. $\therefore I = R$.

QED

There are a couple of ways to view the last result. Fields and division rings don't have the interesting substructure possibilities that exist in other rings. Another consideration is the fact that there exist no non-trivial ring homomorphic images of fields and division rings.

Theorem: A finite integral domain is always a field.

Proof: Let R be a finite integral domain. Let $R = \{0, 1, a_1, a_2, a_3, \dots, a_n\}$ where each element is distinct. We must prove that every non-zero element of R is a unit. Clearly 1 is a unit whose multiplicative inverse is itself. Let a_i be an arbitrary non-zero, non-unity element of R . Construct the set:

$$\begin{aligned} A &= \{0 \cdot a_i, 1 \cdot a_i, a_1 \cdot a_i, a_2 \cdot a_i, a_3 \cdot a_i, \dots, a_n \cdot a_i\} \\ &= \{0, a_i, a_1 \cdot a_i, a_2 \cdot a_i, a_3 \cdot a_i, \dots, a_n \cdot a_i\} \end{aligned}$$

Since R is an integral domain and $a_i \neq 0$, the only time 0 appears in A is as the first named element. Could $a_k \cdot a_i = a_i$ for some k where $1 \leq k \leq n$?

$$\begin{aligned} \text{If } a_k a_i &= a_i \text{ then} \\ a_k \cdot a_i &= 1 \cdot a_i \\ \Rightarrow a_k &= 1 \end{aligned}$$

But each element in the original list for R is distinct. $\therefore a_k \neq 1$ for $1 \leq k \leq n$. $\therefore a_i$ only appears as the second named element in A . Could $a_j \cdot a_i = a_s \cdot a_i$ where $s \neq j$?

$$\begin{aligned} \text{Suppose } a_j a_i &= a_s a_i \\ \Rightarrow a_j &= a_s \end{aligned}$$

However, each element in the original list for R is distinct. Therefore $a_j \neq a_s$ if $s \neq j$. Therefore $a_j \cdot a_i \neq a_s \cdot a_i$ whenever $s \neq j$. \therefore Every element in A is distinct. $\therefore A = R$. Hence each element of R appears only once in A . $\therefore a_i \cdot a_t = 1$ for some a_t . Since R is commutative $a_t \cdot a_i$ must also be 1. $\therefore a_i$ is a unit. Since a_i was arbitrary, R is a field.

QED

Z_5 is an example of a finite integral domain. As a result of the theorem above, Z_5 is a field. In fact, if p is any prime number then Z_p can have no zero divisors because all non-zero integers smaller than p are relatively prime to p . Therefore, Z_p has to be a field for every prime p .

Let's take a moment away from the development of this material to consider once again our three definitions of special rings. As yet, we have no examples of a division ring that is not also a field. We need a ring with non-commutative multiplication that has the property that every non-zero element is a unit. The Quaternions will be our example. Since

$$(0 + 1i + 0j + 0k) \cdot (0 + 0i + 1j + 0k) = i \cdot j = k \text{ and since}$$

$$(0 + 0i + 1j + 0k) \cdot (0 + 1i + 0j + 0k) = j \cdot i = -k, \text{ quaternion multiplication is not}$$

commutative. Is every non-zero quaternion a unit? Suppose $a + bi + cj + dk$ is a quaternion where a, b, c and d can not all equal 0. We can deduce that $a^2 + b^2 + c^2 + d^2 \neq 0$. Let

$S = a^2 + b^2 + c^2 + d^2$. Let's construct the quaternion $\frac{a}{S} - \frac{b}{S}i - \frac{c}{S}j - \frac{d}{S}k$. Consider

$$(a + bi + cj + dk) \cdot \left(\frac{a}{S} - \frac{b}{S}i - \frac{c}{S}j - \frac{d}{S}k\right) = \left(\frac{a^2}{S} + \frac{b^2}{S} + \frac{c^2}{S} + \frac{d^2}{S}\right) +$$

$$\left(-\frac{ab}{S} + \frac{ab}{S} - \frac{cd}{S} + \frac{cd}{S}\right)i + \left(-\frac{ac}{S} + \frac{bd}{S} + \frac{ac}{S} - \frac{bd}{S}\right)j + \left(-\frac{ad}{S} - \frac{bc}{S} + \frac{bc}{S} + \frac{ad}{S}\right)k = 1 + 0i + 0j + 0k$$

which is the unity of the ring. It is easy to prove that $\left(\frac{a}{S} - \frac{b}{S}i - \frac{c}{S}j - \frac{d}{S}k\right)(a + bi + cj + dk)$ produces the same result. Therefore, every non-zero quaternion is a unit.

We now offer a partial converse to a previous theorem. Recall that a field has no non-trivial ideals.

Theorem: If R is a commutative ring with unity that has no non-trivial ideals then R is a field.

Proof: Let a be any non-zero element of R . Let $A = \{ra | r \in R\}$.

Let's show that A is an ideal.

Additive Closure

$$r_1a + r_2a = (r_1 + r_2)a \in A$$

Additive Inverse Closure

$$-ra = (-r)a \in A$$

Multiplicative Absorption

$$r_2 \cdot (r_1a) = (r_2r_1)a \in A$$

Since A is an ideal, $A = \{0\}$ or $A = R$. Since $a \in A$, $A \neq \{0\}$. $\therefore A = R$.

Since R possesses unity, $1 \in A$. $\therefore \exists$ an element $s \in R \ni sa = 1$.

By commutivity, $as = 1$ also. $\therefore a$ is a unit.

Since a was arbitrary, all non-zero elements of R are units. $\therefore R$ is a field.

QED

Definition: Let R be a ring. Let k be a positive integer and $r \in R$. The symbol kr is defined to be the sum $r + r + \dots + r$ with k addends.

Definition: Let R be a ring. The characteristic of R is the least positive integer k such that $kr = 0$ for all r in R . If such an integer does not exist, we say that the characteristic of R is 0.

Theorem: If R is a ring with unity and if k is the least positive integer such that $k \cdot 1 = 0$ then the characteristic of R is k .

Proof: Let $r \in R$.

$$\begin{aligned}
 k \cdot r &= \underbrace{r + r + \dots + r}_{k \text{ addends}} \\
 &= \underbrace{(r \cdot 1 + r \cdot 1 + \dots + r \cdot 1)}_{k \text{ addends}} \\
 &= r \cdot \underbrace{(1 + 1 + \dots + 1)}_{k \text{ addends}} \\
 &= r \cdot 0 = 0 \\
 \therefore k \cdot r &= 0 \text{ for all } r.
 \end{aligned}$$

QED

Theorem: The characteristic of any integral domain is either 0 or a prime number.

Proof: Suppose not. Suppose R is an integral domain whose characteristic is k which is not a prime number. There exist positive integers s and t such that $1 < s < k$ and $1 < t < k$ and $k = s \cdot t$.

$$\begin{aligned}
 &\underbrace{(1 + 1 + \dots + 1)}_{s \text{ addends}} \cdot \underbrace{(1 + 1 + \dots + 1)}_{t \text{ addends}} \\
 &= (st)1 = k \cdot 1 = 0 \\
 \therefore (s \cdot 1)(t \cdot 1) &= 0
 \end{aligned}$$

Since R is an integral domain, either $s \cdot 1 = 0$ or $t \cdot 1 = 0$. This is a contradiction of the previous theorem since we know that k is the characteristic of R .

Why are the special rings so important? Let's get some insight. Later in the text we will study polynomials. However, we can informally introduce an example now to illustrate concepts from the current chapter. Suppose you are told to solve the second degree equation $x^2 + 2x = 0$. If x has to be a real number, we know that there are at most two solutions (including multiple roots). If x can be a complex number (considering the reals as a subset of the complex numbers), we know there are exactly two solutions (including multiple roots). It is alien to us for this equation to have more than two solutions. Let's solve:

$$\begin{aligned}
 x^2 + 2 &= 0 \\
 x \cdot (x + 2) &= 0 \\
 \text{Either } x = 0 &\quad \text{or} \quad x + 2 = 0 \\
 \text{Either } x = 0 &\quad \text{or} \quad x = -2
 \end{aligned}$$

The step to focus on is the transition from $x \cdot (x + 2) = 0$ to $x = 0$ or $x + 2 = 0$. The key to this step is the fact that both the reals and complex numbers constitute integral domains.

Z_8 is not an integral domain. Let's solve $x^2 + 2x = 0$ over Z_8 . $2x$ means $x + x$ as discussed in this chapter. x^2 means $x \cdot x$.

If $x = 2$, $x^2 + 2x = 4 + 4 = 0$. $\therefore x = 2$ is a solution.

If $x = 4$, $x^2 + 2x = 0 + 0 = 0$. $\therefore x = 4$ is a solution.

If $x = 6$, $x^2 + 2x = 4 + 4 = 0$. $\therefore x = 6$ is a solution.

There are three solutions! How did this happen? $x^2 + 2x$ still equals $x(x + 2)$. However $x \cdot (x + 2) = 0$ does not guarantee that either $x = 0$ or $x + 2 = 0$. Obviously, solving polynomials in a well behaved ring like the reals is much simpler than in an ill behaved ring like Z_8 .

1. Prove that the set of all matrices of the form $\begin{pmatrix} x & 0 \\ 0 & x \end{pmatrix}$ form a field. [You can use the fact that the set of all 2×2 matrices forms a ring].
2. Give an example of a field that has two non-zero elements x and y such that $x^2 + y^2 = 0$.
3. Suppose R is an integral domain. Suppose a and b are elements of R such that $a^5 = b^5$ and $a^3 = b^3$. Prove $a = b$.
4. Find an example of an integral domain R and distinct positive integers n and m such that for a and b in R :
 - a) $a^n = b^n$
 - b) $a^m = b^m$
 - c) $a \neq b$
5. Give an example of a commutative ring without zero divisors that is not an integral domain.
6. Find all solutions of $x^3 - 2x^2 - 3x = 0$ in Z_{12} .