Previously.

- Rings
- Commutative Rings
- Fields
- Subrings
- Ring Isomorphisms

This Section.

- Domains
- Integral Domains
- Fields

Recall. We call $a \in R$ a `zero-divisor` if $a \neq 0_R$ and there is some $b \neq 0_R$ in R with $ab = 0_R$.

Example: In $\mathbb{Z}_6$, 2 is a zero divisor. (Verify this!)

Definition. A ring $R \neq \{0\}$ is called a `domain` if $ab = 0$ implies that either $a = 0$ or $b = 0$.

Exercise 1. Which of the following are domains?

(a) $\mathbb{Z}_6$

(b) $\mathbb{Z}_5$

(c) $\mathbb{Q}$

(d) $M_2(\mathbb{R})$

Definition. A commutative domain is called an `integral domain`.

Example. The following are all integral domains.

(a) $\mathbb{Z}$

(b) $\mathbb{Z}[\sqrt{2}]$

(c) $\mathbb{Z}[i]$

(d) Rings of polynomials whose coefficients come from an integral domain, such as $\mathbb{Z}[x]$

Theorem. If $u \in R$ is a unit then u is not a zero divisor.

Exercise 2. Use the last theorem to show that $\mathbb{Z}_p$ is an integral domain if p is prime.

Exercise 3. Some rings that are *not* integral domains. Why are they not?

(a) $M_2(\mathbb{R})$

(b) $\mathbb{Z}_m$ where m is a composite number

(c) $\mathbb{Z} \times \mathbb{Z}$

Theorem 3.2.1. The following are equivalent for a ring R.

1. If $ab = 0$ in R, then $a = 0$ or $b = 0$.
2. If $ab = ac$ in R and $a \neq 0$, then $b = c$.
3. If $ba = ca$ in R and $a \neq 0$, then $b = c$.

Note. Note that what this is say is that we can only cancel in multiplication if there are no zero divisors. In which case, we can always cancel whether or not a^{-1} exists!!!

Recall. A field is a commutative ring such that every non-zero element is a unit.

Note. From the last Theorem, every field is a division ring.

Exercise 4. Claim: $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ is a field
Given $r = a + b\sqrt{2} \in \mathbb{Q}(\sqrt{2})$ with $r \neq 0$, what is r^{-1}?
That is, write $r^{-1} = c + d\sqrt{2}$ where c, d are rational numbers in terms of a and b.

Definition. We say $z \in \mathbb{C}$ is algebraic over $\mathbb{Q}$ if there is some polynomial $p \in \mathbb{Q}[x]$ such that $p(z) = 0$.

Definition. The number field generated by z is the field $\mathbb{Q}(z)$, which is the set of complex numbers of the form $a_0 + a_1z + a_2z^2 + \cdots + a_kz^k$ where $k \in \mathbb{N}$ and $a_0, a_1, \ldots, a_k \in \mathbb{Q}$.

Exercise 5. Why is $\mathbb{Z}[i]$ not a field? (It is an integral domain though!)

Exercise 6. Show $\mathbb{Z}_3(i) = \{a + bi \;:\; a, b \in \mathbb{Z}_3, i^2 = -1\}$ is a field.

Theorem 3.2.2. The characteristic of any domain is either zero or a prime.

Question 7. Verify $\text{char}(\mathbb{Z}_n) = n$. How does this theorem imply $\mathbb{Z}_n$ is a domain if and only if n is prime.

Theorem 3.2.3. Every finite integral domain is a field.

Question 8. How does this theorem imply $\mathbb{Z}_p$ if a field for p prime?

Wedderburn's Theorem. Every finite division ring is a field.

Note. A division ring is a ring in which every nonzero element has an inverse. (i.e., every $r \neq 0 \in R$ is a unit). But division rings are called fields if they are commutative.

Question 9. Can you think of a non-commutative division ring?