Integral Domains "nicer rings"

Definition: If $R$ is a commutative ring, we say $a \neq 0$ in $R$ is a zero-divisor iff $ab = 0$ for some $b \neq 0$ in $R$.

Example $\mathbb{Z}_6$:

- 2 and 3 are zero divisors since $2 \cdot 3 \equiv 0 \pmod{6}$.

Definition: A commutative ring with unity 1.

$\mathbb{Z}$ is an integral domain iff $\mathbb{Z}$ has no zero divisors.

I'm thinking: Zero divisors are "bad". $\mathbb{Z}$ is "good" if it has none.

Example:

1. $\mathbb{Z}$ is an integral domain.
2. $\mathbb{Z}_6$ is not an integral domain since $2 \cdot 3 \equiv 0 \pmod{6}$.
3. $\mathbb{Z}_5$ is an integral domain.

$a \cdot b \equiv 0 \pmod{5} \iff 5 | a \cdot b \Rightarrow 5 | a \text{ or } 5 | b$ by Euclid's Lemma, (Gallian p. 7).

Fact: If $R$ = integral domain, then if $a \neq 0$ in $R$, $a$, $b$, $c \in R$ and $ab = ac$ then $b = c$.

That is, cancellation is legal (even though $a^{-1}$ may not be in $R$).
Proof
\[ ab = ac \implies ab - ac = 0 \]
\[ \implies a(b - c) = 0 \]
\[ \implies b - c = 0 \quad \text{as } a \neq 0 \implies R \text{ has no zero divisors.} \]

Defn. Field = \{\text{commutative ring } F \text{ with unity } 1 \}
\text{such that } \forall a, b \in F, \quad a \cdot b = 0 \implies a = 0 \text{ or } b = 0.

That is, \( \forall x \in F, \ x \neq 0, \implies x^{-1} \in F. \)

Examples
1. \( \mathbb{Z} \) = ring of integers is not a field as \( \mathbb{Z} \) has \( \mathbb{Z}^{-1} \neq \{ \pm 1 \} \).
2. \( \mathbb{Z}_5 \) is a field
   \[ 1^{-1} \equiv 1 \pmod{5} \quad 3^{-1} \equiv 2 \pmod{5} \]
   \[ 2^{-1} \equiv 3 \pmod{5} \quad 4^{-1} \equiv 4 \equiv -1 \pmod{5} \]
   \text{More generally } \mathbb{Z}_p \text{ is a field } \iff p \text{ is prime.}
3. \( \mathbb{Q} \) = rational \# s = \{ \frac{n}{m} | n, m \in \mathbb{Z}, m \neq 0 \}
   \text{is a field.}
4. \( \mathbb{R}, \mathbb{C} \) also are fields.

Thm.
1. A field is an integral domain.
2. Any finite integral domain (e.g., \( \mathbb{Z}_p \), \( p \) = prime) is a field.
Proof

1. For $a, b \in F$ with $a \neq 0$ and $ab = 0$
   \[
   \Rightarrow b = a^{-1}(ab) = a^{-1} \cdot 0 = 0
   \]
   \[
   \Rightarrow b = 0
   \]
   So $F$ has no $0$-divisors and is an integral domain.

2. $D$ is a finite integral domain. Let $a \neq 0, a \in D$.
   We must show there exists $a_i \in D, i \in \mathbb{N}$
   \[
   S = \{a, a^2, a^3, \ldots \} \subset D. \quad D \text{ finite } \Rightarrow S \text{ finite}
   \]
   \[
   \Rightarrow a_i = a_j \quad \text{for some } i \geq j
   \]
   \[
   \Rightarrow a^{i-j}(a^j) = 1 \cdot a^j
   \]
   \[
   \Rightarrow a^{i-j} = 1 \quad \text{by cancellation (see p. 7)}
   \]
   \[
   \Rightarrow a \cdot \left(\frac{a^j}{a^{i-j}}\right) = 1
   \]
   \[
   \Rightarrow \frac{a^i}{a^j} = a^{-1}
   \]
   So $\mathbb{Z}_p, p = \text{prime}$ is a field. In many ways you can view it as a finite analogue of the real line. But it is a finite circle, really.

Note: If $n \neq \text{prime}$

\[
\Rightarrow \mathbb{Z}_n \text{ is not an integral domain and thus not a field as}
\]

\[
\begin{align*}
& a \equiv 0 \pmod{n}, \quad a \cdot b \equiv 0 \pmod{n} \\
& b \equiv 0 \pmod{n}
\end{align*}
\]
Are there other finite fields?

Yes! You can imitate the construction that gives the complex numbers \( \mathbb{C} \).

Example: Field with 9 elements

\[ F_9 = \mathbb{Z}_3[i] = \{ a + bi \mid a, b \in \mathbb{Z}_3 \} \]

Here \( i^2 = -1 \). \( |F_9| = 9 \) (as there are 3 choices of \( a + b \))

add a multiply as in \( \mathbb{C} \) but mod 3

See Gallian, p. 251.

Why is it a field?

\( a + ib \neq 0 \) in \( \mathbb{Z}_3[i] \)

\[ \Rightarrow \frac{1}{a + ib} = \frac{a - ib}{(a + ib)(a - ib)} = \frac{a - ib}{a^2 + b^2} \]

\[ = (a - ib) \cdot \frac{1}{a^2 + b^2} \in \mathbb{Z}_3[i] \]

Here to show \( \frac{1}{a^2 + b^2} \) exists in \( \mathbb{Z}_3 \) we need to show \( 3 \nmid (a^2 + b^2) \). This is true as

say \( a \neq 0 \mod 3 \) and so \( a^2 \equiv 1 \mod 3 \)

while \( b^2 \equiv 0 \) or \( 1 \mod 3 \).

So \( a^2 + b^2 \equiv 1 \) or \( 2 \mod 3 \) not \( 0 \).
A $z \in \mathbb{Z}_3[i]$ has the property $3z = 0$.

Why?

$z = x + iy$, with $x, y \in \mathbb{Z}_3$

$3z = (x + iy) + (x + iy) + (x + iy)$

$= (3x) + i(3y) = 0 + i0 \quad (\text{mod } 3)$.

So we say $\mathbb{Z}_3[i]$ "has characteristic 3".

**Defn.** The characteristic of a ring $R$ is the smallest $n \in \mathbb{Z}^+$ such that

$n \cdot x = x + x + \cdots + x = 0 \quad \forall x \in R.$

If no such $n$ exists, we say $R$ has characteristic 0.

**Lemma.** $R$ is a ring with identity $1$ for multiplication. Then $R = 0$ if $R$ has infinite additive order, characteristic $R = n$.

**Examples.** $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ all have characteristic 0.

For $n \in \mathbb{Z}^+$, $x \in \mathbb{C}$, $n \cdot x = 0 \implies x = 0$

So $nx$ is not 0 for all $x \in \mathbb{C}$ ever.

2. $\mathbb{Z}_p$ has characteristic $p$ as

$p \cdot x = x + \cdots + x = 0 \quad (\text{mod } p)$

**Fact.** The characteristic of an integral domain $R$ is a prime or 0.

**Proof.** If the additive order of 1 is not finite, then char $R = 0$ by the Lemma above.
Suppose additive order of 1 is \( n \). We must show \( n = \text{prime} \). For \( n \) is characteristic of \( R \),

\[
0 = n \cdot 1 = (a \cdot 1)(b \cdot 1) \Rightarrow (a \cdot 1)(b \cdot 1) = 0 \Rightarrow a \cdot 1 = 0 \text{ or } b \cdot 1 = 0 \text{ as } R \text{ is an integral domain.}
\]

But this contradicts minimality of \( n \).

Problems

2. Which of Examples below are Fields?

1. \( \mathbb{Z} \) is not a field as \( \frac{1}{2} \notin \mathbb{Z} \)
2. \( \mathbb{Z}[i] \) is not a field as \( \frac{1}{2} \notin \mathbb{Z}[i] \)
3. \( \mathbb{Z}[x] \) is not a field as \( \frac{1}{x} \notin \mathbb{Z}[x] \)
4. \( \mathbb{Z}[\sqrt{2}] \) is not a field as \( \frac{1}{2} \notin \mathbb{Z}[\sqrt{2}] \)
5. Finally, \( \mathbb{Z}_p \) is a field \( \Leftrightarrow \) \( p = \text{prime} \) by the Corollary to Theorem 13.2 in Gallian, p. 251 (or these notes pp 8-9).

Subfield Test: \( F \) = field, \( K \subseteq F \)

with \( |K| = 2 \). Prove \( K \) is a subfield of \( F \) (meaning it's a field under the operations of \( F \)) if \( \forall a, b \in K \) \( b \neq 0 \), we have \( a - b \) and \( ab^{-1} \in K \).
Here you just need to note that our hypotheses \( \Rightarrow \) by the 1-step subgroup test (Gallian, Thm 3.1, p. 58) that \( K \) is a subgroup of \( F \) under addition and \( K - \{0\} \) is a subgroup of \( F - \{0\} \) under multiplication. The distributive laws are automatic. The unit is in \( K \) as \( a.a^{-1} = 1 \in K \).

\[ (x + y)^p = x^p + y^p \]

By the binomial theorem,

\[ (x + y)^p = \sum_{k=0}^{p} \binom{p}{k} x^k y^{p-k} \]

So we need to show

\[ p \text{ divides } \binom{p}{k} \text{ for } k = 1, 2, \ldots, p-1 \]

\[ \binom{p}{k} = \frac{p(p-1) \cdots (p-k+1)}{k(k-1) \cdots 1} \in \mathbb{Z} \]

If \( 0 < k < p \), \( p \) prime.

Since \( p \) obviously divides the numerator, \( p \) divides \( \binom{p}{k} \), \( k = 1, \ldots, p-1 \).

Thus only the \( k = 0 \) and \( k = p \) terms

\[ x^p + y^p \]

are non-vanishing.

Proof.