Integral Domains

As we saw in the example of the ring $\mathbb{Z}_6$, in some rings it's possible to have two non-zero elements a, b such that $ab = 0$. In $\mathbb{Z}_6$, $(2)(3) = 0$. In elementary algebra you learn to solve quadratic equations by factoring.

Ex. Solve $x^2 - 3x + 2 = 0$ where $x \in \mathbb{R}$.

$$x^2 - 3x + 2 = (x - 2)(x - 1) = 0$$

We conclude that either $x - 2 = 0$ or $x - 1 = 0$ and the solutions are $x = 2, 1$.

But this relies on the idea that if $ab = 0$ then $a = 0$ or $b = 0$ (or both). This is true for a field like $\mathbb{R}$ or $\mathbb{C}$, but for a general ring $ab = 0$ does not imply $a = 0$ or $b = 0$. Thus in a general ring we may get more that 2 solutions to a quadratic equation.

Ex. Solve $x^2 - 3x + 2 = 0$ where $x \in \mathbb{Z}_6$.

We start by factoring:

$$x^2 - 3x + 2 = (x - 2)(x - 1) = 0.$$

Notice that in $\mathbb{Z}_6$ there are several pairs of non-zero factors whose product is 0.

$$(2)(3) = (3)(2) = (3)(4) = (4)(3) = 0.$$

So, for example if $x - 2 = 2$ and $x - 1 = 3$ (both must happen) has a solution in $\mathbb{Z}_6$ (which it does, $x = 4$) then 4 is a solution to the quadratic equation in $\mathbb{Z}_6$.

Notice $4^2 - 3(4) + 2 = 16 - 12 + 2 = 6 = 0\ (mod\ 6)$.

So in this case, since the factors are $x - 2$ and $x - 1$, the pair of factors whose product is 0 must differ by 1. The other pair that works in $\mathbb{Z}_6$ is $x - 2 = 3$ and $x - 1 = 4$, i.e. $x = 5$.

Since $(x - 2)(x - 1) = 0$ also has $x = 2, x = 1$ as solutions we have the full set of solutions in $\mathbb{Z}_6$ is $x = 1, 2, 4, 5$.

Def. If a and b are non-zero elements of a ring R such that $ab = 0$, then a and b are called **zero divisors**.

Theorem: In the ring $\mathbb{Z}_n$, the zero divisors are those non-zero elements that are not relatively prime to n.

Corollary: If p is a prime number, then $\mathbb{Z}_p$ has no zero divisors.

Theorem: The cancellation laws (e.g. if $ba = ca$ then $b = c$) hold in a ring R if, and only if, R has no zero divisors.

Thus, in a ring R with no zero divisors the linear equation:

$$ax = b, \text{ with } a \neq 0,$$

can have **at most one solution**. Since if $ax_1 = b$ and $ax_2 = b$ then, $ax_1 = ax_2$ and $x_1 = x_2$ by our last theorem. Notice that $\mathbb{Z}$ is a ring with no zero divisors but $2x = 3$ does not have a solution.

If R has unity $1 \neq 0$ and a is a unit in R (i.e. a^{-1} exists in R) then the solution to $ax = b$ is $x = a^{-1}b$.

If R is a field then $a^{-1}b = ba^{-1}$ and this is what we call $\frac{b}{a}$ (if R is not commutative then $\frac{b}{a}$ is ambiguous since $a^{-1}b \neq ba^{-1}$, and the notation shouldn't be used).

Def. An **integral domain** D is a commutative ring with unity $1 \neq 0$ containing no zero divisors.

Thus, if the coefficients of a polynomial are from an integral domain (like $\mathbb{Z}$), and one can factor the polynomial into linear factors, then one can try to find solutions by setting each linear factor equal to zero and solving. However, there is no guarantee there will be a solution in the integral domain (e.g. $2x = 3$, where the integral domain is $\mathbb{Z}$).

Ex. $\mathbb{Z}$ and $\mathbb{Z}_p$, for any prime number p are integral domains. $\mathbb{Z}_n$, where n is not prime is not an integral domain. If R and S are two non-zero rings (integral domain or not) then $R \times S$ is not an integral domain because:

$$(r, 0) \cdot (0, s) = (0, 0), \text{ for any } r \in R \text{ and } s \in S.$$

Ex. Show $M_2(\mathbb{Z}), M_2(\mathbb{C}), M_2(\mathbb{R}), M_2(\mathbb{Q})$ and $M_2(\mathbb{Z}_n)$ are not integral domains even though $\mathbb{Z}$, $\mathbb{C}$, $\mathbb{R}$, $\mathbb{Q}$, and $\mathbb{Z}_p$, p a prime number, are integral domains.

Notice: $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$ in $M_2(\mathbb{Z}), M_2(\mathbb{C}), M_2(\mathbb{R}), M_2(\mathbb{Q}), M_2(\mathbb{Z}_n)$.

In addition, the multiplication in these rings of matrices in not commutative.

Thus, none of those rings is an integral domain.

Theorem: Every field F is an integral domain.

Proof: Let $a, b \in F$ and suppose $a \neq 0$. Then if $ab = 0$, $a^{-1} = \frac{1}{a}$ (since every non-zero element of a field is a unit, and all fields are commutative) and:

$0 = \frac{1}{a}(ab) = \left(\frac{1}{a} \cdot a\right) b = 1 \cdot b = b$. Thus if $ab = 0$, $a \neq 0$ then b must equal 0 so there is no zero divisor in F.

Theorem: Every finite integral domain is a field (note: we have already seen that $\mathbb{Z}_p, p$ prime, is an integral domain).

Proof: Let $D = \{0,1, x_1, \dots, x_n\}$ be a finite integral domain.

Given any $x \in D,\ x \neq 0$ we must show there is, $y \in D$, with $xy = 1$.

By the cancellation law $x1, xx_1, \dots, xx_n$ must be distinct since if $xx_j = xx_k$ then $x_j = x_k$.

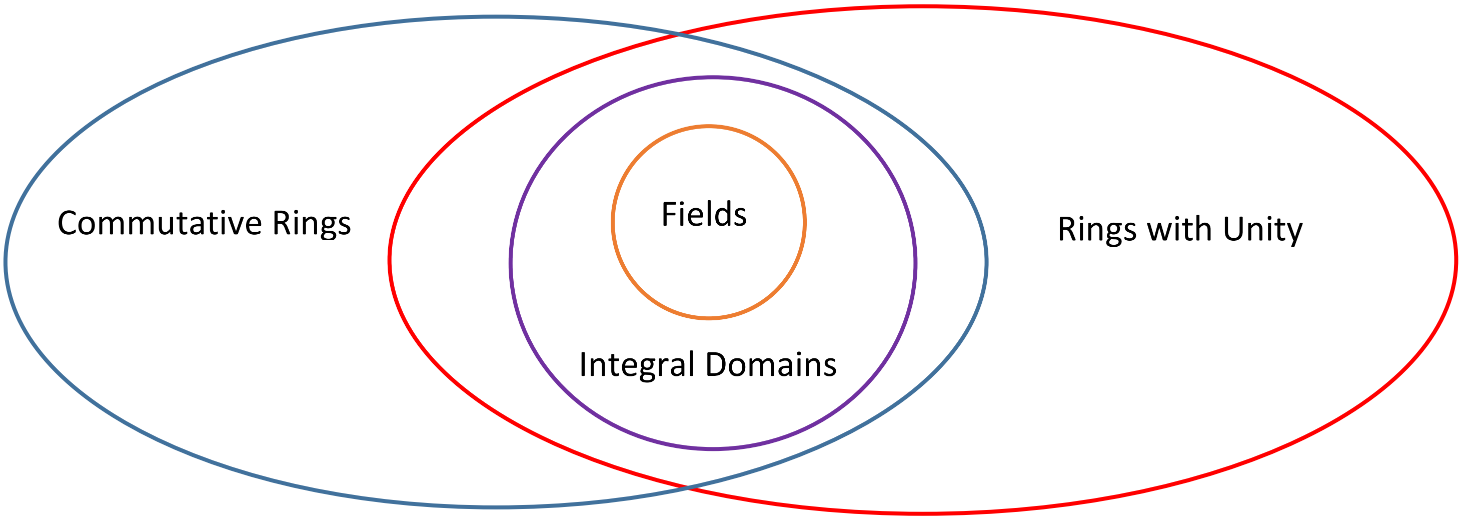
Hence $xx_m = 1$ for some $1 \leq m \leq n$ or $x1 = 1$.

In either case, there is a $y \in D$, with $xy = 1$.

Thus all non-zero elements of D are units and D is a field.

Corollary: If p is prime, $\mathbb{Z}_p$ is a field.

Diagram of Rings



Ex. Solve $5x = 3$ in $\mathbb{Z}_7$ and $\mathbb{Z}_{19}$.

$\mathbb{Z}_7$ and $\mathbb{Z}_{19}$ are both fields because 7 and 19 are prime. If we can find the multiplicative inverse of 5 in each field we can multiply both sides of the equation to solve it.

We want to know, for what $a \in \mathbb{Z}_7$ is $5a = 1$? That is, $5a = 1\ (mod\ 7)$.

So we want to solve $5a = 7b + 1$ for some integers a and b.

So when is $7b+1$ a multiple of 5?

Here we just have to search.

$b=2$ gives $7(2)+1=15$. When $a=3,\ 5(3)=15\ (mod\ 7)=1$.

Thus 3 is the multiplicative inverse of 5 and

$$5x=3$$

$$3(5x)=3(3)$$

$x=2$ in $\mathbb{Z}_7$. (notice that $5(2)=3\ (mod\ 7)$)

In $\mathbb{Z}_{19}$ we want to know for what $a\in\mathbb{Z}_{19}$ is $5a=1$?

That is $5a=1\ (mod\ 19)$.

So $5a=19b+1$ for some integers a and b.

So when is $19b+1$ a multiple of 5?

Again we just have to search.

$b=1$ works because $19(1)+1=20$ and $a=4$ i.e. $5(4)=20$.

So 4 is the multiplicative inverse of 5 in $\mathbb{Z}_{19}$.

$$5x=3$$

$$4(5x)=4(3)$$

$x=12$ in $\mathbb{Z}_{19}$ (notice that $5(12)=3\ (mod\ 19)$).