Section IV.19. Integral Domains

Note. In classical algebra, we solve polynomial equations by: setting equal to 0, factoring, and setting factors equal to 0. For example, $x^2 - 5x + 6 = 0$ factors as $(x-3)(x-2) = 0$ which implies that $x = 2$ and $x = 3$ are (real) solutions. However, there are more solutions in different settings. Example 19.1 shows that in $\mathbb{Z}_{12}$ the solutions are 2, 3, 6, and 11. Notice that when $x = 6$ we have $(x - 3)(x - 2) = (3)(4) = 12 \equiv 0 \pmod{12}$. This example illustrates the unfamiliar result that the product of two "numbers" (elements of a group) can be "zero" (the additive identity) without one of the numbers being zero. This leads us to consider the following.

Definition 19.2. If a and b are two nonzero elements of a ring R such that $ab = 0$ then a and b are *divisors of* 0.

Example. In $\mathbb{Z}_{12}$, the divisors of 0 are 2, 3, 4, 6, 8, 9, and 10.

Theorem 19.3. In the ring $\mathbb{Z}_n$, the divisors of 0 are precisely the nonzero elements that are not relatively prime to n.

Corollary 19.4. If p is a prime, then $\mathbb{Z}_p$ has no divisors of 0.

Theorem 19.5. The left cancellation law states that "$ab = ac$ with $a \neq 0$ implies $b = c$." The right cancellation law states that "$ba = ca$ with $a \neq 0$ implies $b = c$." The cancellation laws hold in a ring R if and only if R has no divisors of 0.

Note. If we are in a ring with no divisors of 0, then we can **SOLVE THE ALGEBRAIC EQUATION** (finally!!!) $ax = b$ were $a \neq 0$ in at most one way. If R has unity $1 \neq 0$ and a is a unit, then the solution is $x = a^{-1}b$.

Definition 19.6. An *integral domain* D is a commutative ring with unity $1 \neq 0$ and containing no divisors of 0.

Note 19.A. An integral domain has almost all of the classical algebraic structure we could wish for. Notice that in an integral domain it may not be the case that nonzero elements are units (i.e., have multiplicative inverses). Notice the difference between an integral domain and a division ring:

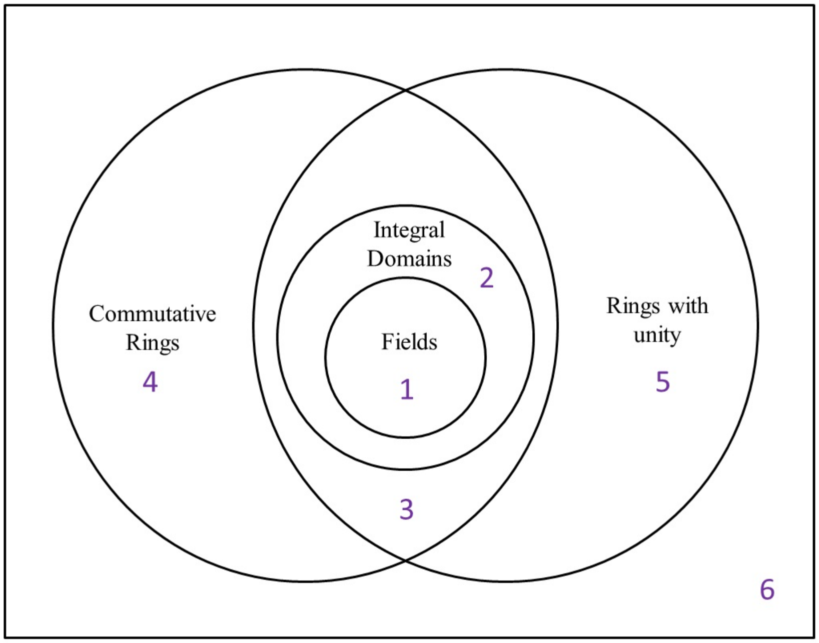
Integral Domain	Division Ring
Ring with unity $1 \neq 0$	Ring with unity $1 \neq 0$
Commutative	Maybe not commutative
Some nonzero elements may not be units	All nonzero elements are units (so no zero divisors)

We defined a field as a commutative division ring. We could just as well have defined a field as an integral domain in which every nonzero element is a unit.

Example 19.7. $\mathbb{Z}$ is an integral domain (but not a division ring). $\mathbb{Z}_p$ where p is prime is an integral domain, a division ring, and a field.

Theorem 19.9. Every field F is an integral domain.

Note. Fraleigh's Figure 19.10 is a Venn diagram of the algebraic structures we have encountered:



Theorem 19.11. Every finite integral domain is a field.

Note. We have claimed that $\mathbb{Z}_p$ for p prime is a field, but we have not yet proved this.

Corollary 19.12. If p is prime, then $\mathbb{Z}_p$ is a field.

Definition 19.13. If for a ring R there is $n \in \mathbb{N}$ such that $n \cdot a = 0$ for all $a \in R$ (remember that "$n \cdot a$" represents repeated addition), then the least such natural number is the *characteristic* of the ring R. If no such n exists, then ring R is of *characteristic* 0.

Example 19.14. The ring $\mathbb{Z}_n$ has characteristic n. Rings $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ have characteristic 0.

Note. The following result streamlines the process of determining the characteristic of a ring by showing that we can restrict our attention to the multiplicative identity 1.

Theorem 19.15. Let R be a ring with unity. If $n \cdot 1 \neq 0$ for all $n \in \mathbb{N}$, then R has characteristic 0. If $n \cdot 1 = 0$ for some $n \in \mathbb{N}$, then the smallest such natural number n is the characteristic of R.

Exercise 19.10. Find the characteristic of ring $\mathbb{Z}_6 \times \mathbb{Z}_{15}$.

Solution. Unity is $(1, 1)$ and the smallest $n \in \mathbb{N}$ for which $n \cdot (1, 1) = (0, 0)$ is $n = \text{lcm}(6, 15) = 30$. □

Revised: 7/14/2023