2 Integral Domains

Let R be a ring and $a, b \in R$. Then $ab = 0$ may not imply $a = 0$ or $b = 0$. For example,

1. In $R = \boldsymbol{Z}_4$, $2 \cdot 2 = 0$.
2. In $M_2(\boldsymbol{R})$,

$$\begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix}, \text{ and } \begin{bmatrix} 1 & 0 \\ 0 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}.$$

   $AB = O$ may not imply $BA = O$.

In this course, we discuss only the case when R is commutative.

Definition 2.1 Zero-Divisor: A *zero-divisor* is a nonzero element a of a commutative ring R such that there is a nonzero element $b \in R$ with $ab = 0$.

Integral Domain: An integral domain is a commutative ring with unity and no zero divisors.

Field: A *field* is a commutative ring with unity in which every nonzero element is a unit.

- For non-commutative rings, right and left zero divisors have to be defined separately and distinguished.
- Let R be an integral domain. If $ab = ac$ with $a \neq 0$, then $b = c$. (Theorem 13.1)

  In particular, if $a \neq 0$, then $a^n \neq 0$ for any positive integer n.
- Every field is an integral domain.
- Let R be an integral domain. If S is a subring of R containing 1, then S is an integral domain. Note that if e is a unity of S, then $ee = e$ implies $e(e-1) = 0$ and $e = 1$ as $e \neq 0$.

Proposition 2.1 (Theorem 13.2) *A finite integral domain is a field.*

Proof. Let R be a finite integral domain and $a \in R \setminus \{0\}$. Since R is finite, there exist positive integers $i < j$ such that $a^i = a^j$. Then $a^i(1 - a^{j-i}) = 0$ and we have $a^{j-i} = 1$. Hence a^{j-i-1} is the multiplicative inverse of a. ∎

Example 2.1 1. $\boldsymbol{Z}$.

2. $\boldsymbol{Z} \oplus \boldsymbol{Z}$ is not an integral domain.
3. $\boldsymbol{Z}_n$ is an integral domain, and hence a field, if and only if n is a prime.

Example 2.2 1. $\boldsymbol{Z}[x]$

2. $R[x]$: polynomial ring over an integral domain. $R[x]$ is an integral domain.

$$\deg(f(x)g(x)) = \deg f(x) + \deg g(x). \quad -\infty + a = -\infty.$$

3. $\boldsymbol{Z}_6[x]$: $(2x+4)(3x+3)=0$.

4. $x^2-4x+3=(x-3)(x-1)=(x-7)(x-9)$ has four roots in $\boldsymbol{Z}_{12}$. $x^2-4x+3=(x-2)^2-1$. So if $y=x-2$, $y^2=1$. Since $y^2=1$ implies $y=1,-1,5,-5$, $x=3,1,7,-3=9$.

Definition 2.2 [Characteristic of a Ring] The *characteristic* of a ring R is the least positive integer n such that $nx=0$ for all $x \in R$. If no such integer exists, we say that R has characteristic 0. The characteristic of R is denoted by $\mathrm{char}R$.

Suppose R is a ring with unity 1. If $n1=0$, then $nx=(n1)x=0$ for any integer $n \in \boldsymbol{Z}$. So if there is no positive integer n such that $n1=0$, then $\mathrm{char}R=0$, otherwise $\mathrm{char}R$ is the additive order of 1.

Proposition 2.2 *The characteristic of an integral domain is* 0 *or prime.*

Proof. We may assume that $m=\mathrm{char}(R)>0$. If $m=m_1m_2$ a composite number with $0<m_1,m_2<m$, $0=m1=(m_1m_2)1=(m_11)(m_21)$. Since R is an integral domain, $m_11=0$ or $m_1=0$, which contradicts the minimality of m. ∎

Example 2.3 Recall that every subring with 1 of an integral domain is an integral domain.

1. $\boldsymbol{Z}[i]$.

2. $\boldsymbol{Z}[\sqrt{2}]=\{a+b\sqrt{2} \mid a,b \in \boldsymbol{Z}\}$.

3. $\boldsymbol{Q}[i]=\{a+bi \mid a,b \in \boldsymbol{Q}\}$ is a field.

4. $\boldsymbol{Q}[\sqrt{2}]=\{a+b\sqrt{2} \mid a,b \in \boldsymbol{Q}\}$ is a field.

Example 2.4 1. $\boldsymbol{Z}_3[i]$: Field with nine elements.

2. $\boldsymbol{Z}_5[i]$: $(1+2i)(1-2i)=5=0$. Hence $\boldsymbol{Z}_5[i]$ is not an integral domain. However, since i is an element such that $i^2=-1$, $i=2,3$. Hence we can also say that $\boldsymbol{Z}_5[i]=\boldsymbol{Z}_5$. See Exercise 24.

3. $\boldsymbol{Z}_n[i]$? Check the definition.[8] Assume that there is a ring R containing $\boldsymbol{Z}_n$ and a such that $a^2=-1$, and set $a=i$. The definition of the textbook seems to be $\boldsymbol{Z}_n[i]=\boldsymbol{Z}_n[x]/\langle x^2+1\rangle$, or $\boldsymbol{Z}_n[i]=\{a+bi \mid a,b \in \boldsymbol{Z}_n\}$ and i is a symbol such that $i^2=-1$.

Further Readings

1. E. Berg, A Family of Fields, Pi Mu Epsilon 9 (1990), 154–155.

2. N. A. Koan, The Characteristic of a Ring, American Mathematical Monthly 70 (1963), 736–738.

3. R. McLean, Groups in Modular Arithmetic, The Mathematical Gazette 62 (1978), 94–104.

[8] $\boldsymbol{Z}[i]=\boldsymbol{Z}[x]/\langle x^2+1\rangle$ with $i=x+\langle x^2+1\rangle$. Since, in general, the number of solutions to $x^2=-1$ is dependent on n, it is safer to restrict the case when n is a prime number.