1.4 Lecture 4: Integral Domains and Zero-Divisors

We saw in Theorem 2 that whenever an element of a ring is multiplied by zero, the result is zero. When working in the set of real numbers we often use the converse of this - a product ab can be zero in $\mathbb{R}$ only if at least one of a and b is equal to zero.
Question: When/how do we use this?

Question: Is it true in every ring that the product of two elements can be zero only if at least one of the elements is zero? To think about this question, look at some examples.

Example 6. *1. In* $M_2(\mathbb{Q})$

$$\begin{pmatrix} 1 & -1 \\ -2 & 2 \end{pmatrix}\begin{pmatrix} 1 & 1 \\ 1 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

So the product of two non-zero matrices in $M_2(\mathbb{Q})$ *can be the zero matrix.*

2. *In* $\mathbb{Z}/6\mathbb{Z}$, $\bar{2} \times \bar{3} = \bar{0}$

These examples show that the answer to the question is no in general. This basically means that it does not follow from the ring axioms that the product of a pair of non-zero elements can't be zero. However, we can study the class of rings in which this property holds.

Definition 7. *Let* R *be a ring with zero element* 0_R. *An element* a *of* R *is called a* (left) zero-divisor *in* R *if* $a \neq 0_R$ *and there exists an element* $b \neq 0_R$ *of* R *for which* $ab = 0_R$. *(In this situation,* b *is a right zero-divisor).*

Note: If R is commutative then $ab = ba$ and we just talk about zero-divisors (not left and right zero-divisors).

Definition 8. *A commutative ring that contains no zero-divisors is called an* integral domain *(or just a domain).*

In an integral domain, the product of two elements can be zero only if one of the elements is zero.

EXAMPLES

1. $\mathbb{Z}$ is an integral domain. Somehow it is the "primary" example - the integers gives us the term "integral domain". The adjective "integral" in this context refers to "integer" (nothing to do with integrals in calculus).

2. Every *field* is an integral domain. To see this, let F be a field and suppose that a, b are elements of F for which $ab = 0_F$. Assume $a \neq 0$. Then a has a multiplicative inverse in F and

$$\begin{aligned} ab &= 0_F \\ \Longrightarrow a^{-1}(ab) &= a^{-1}0_F \\ \Longrightarrow (a^{-1}a)b &= 0_F \text{ by Theorem 2} \\ \Longrightarrow 1_F b &= 0_F \\ \Longrightarrow b &= 0_F. \end{aligned}$$

   Remark: It follows from the above argument that no element of any ring can be both a unit and a zero-divisor.

3. An example of a commutative ring that is not an integral domain is $\mathbb{Z}/6\mathbb{Z}$.

Questions to think about:

1. For which natural numbers n is $\mathbb{Z}/n\mathbb{Z}$ a field?
2. For which natural numbers n is $\mathbb{Z}/n\mathbb{Z}$ an integral domain?
3. For a natural number n, which elements of $\mathbb{Z}/n\mathbb{Z}$ are units?
4. Is it true for every natural number n that every non-zero element of $\mathbb{Z}/n\mathbb{Z}$ is either a unit or a zero-divisor? Can we prove this?

Problem Prove that every *finite* integral domain is a field.

Cancellation in integral domains: We can think of integral domains as those commutative rings in which we can *cancel* a non-zero factor that appears on both sides of an equation. For example suppose we want to solve the equation $3x = 6$ for x. If we are working in the integers (or rational or real numbers) we would immediately cancel the 3 on both sides and conclude that $x = 2$ is the only solution. Here we are (implicitly or even maybe even subconsciously) using the fact that 3 is not a zero-divisor in $\mathbb{Z}$. The details of the argument are

$$3x = 6 \Longrightarrow 3x - 6 = 0 \Longrightarrow 3(x - 2) = 0.$$

Now we have the product of two elements equal to zero in an integral domain. This means that at least one of them is zero. We know that the first factor (3) is not zero. So it must be that the other factor $x - 2$ is zero, so $x = 2$ is the only solution.

We can't apply this logic in a ring where 3 is a zero divisor. For example in $\mathbb{Z}/12\mathbb{Z}$, $3 \times 4 = 0$ and $x = 2,\ x = 6,\ x = 10$ are all solutions to the equation $3x = 6$.

In general, if we know that $ab = ac$ in an integral domain and we know that $a \neq 0$, we can write $a(b-c) = 0$ and conclude that $b-c = 0$ and $b = c$. So we can cancel the a from the equation $ab = ac$.