§1 11-04

Definition 1.1. An element $a \in \mathbb{R}$ is a zero-divisor if $\exists b \neq 0$ such that $ab = 0$ or $ba = 0$. You can get more specific and declare a left zero-divisor or a right zero-divisor.

Definition 1.2. $u \in \mathbb{R}$ is a unit if u has a multiplicative inverse.

Lemma 1.3

Let R be a ring with unity. The set $U(R) = \mathbb{R}^*$ of units of R forms a group using multiplication.

Note 1.4. Some people assume that when you say a ring, it means a ring with unity.

Recall 1.5. $\mathbb{Z}[x]$ is a ring of polynomials. Variable is x with coefficients in $\mathbb{Z}$.

Lemma 1.6

$\mathbb{Z}[x]$ is an integral domain. Because it is commutative, includes the identity element, and when $ab = 0$, either $a = 0$ or $b = 0$.

Lemma 1.7

$\mathbb{Z}_p[x]$ is integral domain when p is prime.

Example 1.8

$$\mathbb{Z}_6[x] = \{2x^5 + 3x^4 + 5x^3 + 1x^2 + 0x^1 + 4x^0, \cdots\}$$
$$(2x+2)(3x+3) = 0$$

So $\mathbb{Z}_6[x]$ is not an integral domain. In general, $\mathbb{Z}_n[x]$ is not an integral domain when n is composite.

Definition 1.9. $M_{n\times n}(\mathbb{R})$ is the set of $n \times n$ matrices with real coefficients. Addition and multiplication of matrices as defined in linear algebra.

$$1 = I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

Note that this ring is not an integral domain because it contains zero divisors.

$$\underbrace{\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}\begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}}_{\text{Zero divisors}} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$

Note 1.10. $U(M_{n\times n}(\mathbb{R})) = \mathrm{GL}_n(\mathbb{R})$

Note 1.11. $M_{n\times n}(\mathbb{Z}_m)$ has m^{n^2} elements and works very nicely when n is prime.

Example 1.12

$$M_{2\times 2}(\mathbb{Z}_2) =$$
$$\{\begin{pmatrix}1&1\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\1&1\end{pmatrix}, \begin{pmatrix}1&0\\1&0\end{pmatrix}, \begin{pmatrix}1&1\\0&0\end{pmatrix}, \begin{pmatrix}1&0\\1&1\end{pmatrix}, \begin{pmatrix}0&1\\1&0\end{pmatrix}, \begin{pmatrix}1&0\\0&0\end{pmatrix}, \begin{pmatrix}0&0\\0&1\end{pmatrix},$$
$$\begin{pmatrix}0&0\\0&0\end{pmatrix}, \begin{pmatrix}1&0\\0&1\end{pmatrix}, \begin{pmatrix}0&0\\1&1\end{pmatrix}, \begin{pmatrix}0&1\\0&1\end{pmatrix}, \begin{pmatrix}1&1\\1&0\end{pmatrix}, \begin{pmatrix}0&1\\1&1\end{pmatrix}, \begin{pmatrix}0&1\\0&0\end{pmatrix}, \begin{pmatrix}0&0\\1&0\end{pmatrix}\}$$
$$\text{Example of multiplication:} \quad \begin{pmatrix}1&1\\0&1\end{pmatrix}\begin{pmatrix}1&0\\1&0\end{pmatrix} = \begin{pmatrix}0&0\\1&0\end{pmatrix}$$

Note 1.13. Each element is its own additive inverse.

$$(M_{2\times 2}(\mathbb{Z}_2), +) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$$

Definition 1.14. The "real-quaternions" $\mathbb{R}Q$ forms a division ring that isn't a field (because it isn't commutative).

$$\mathbb{R}Q = \{a_1 + bi + cj + dk : a, b, c, d \in \mathbb{R}\}$$

Addition and multiplication works like in $\mathbb{C}$. Let scalars commute with i, j, k.

$$\begin{aligned} i^2 = j^2 = k^2 &= -1 \\ ij = k \quad ji &= -k \\ jk = i \quad kj &= -i \\ ki = j \quad ik &= -j \end{aligned}$$

There is crazy algebra to show that:

$$(a + bi + cj + dk)(a - bi - cj - dk) = a^2 + b^2 + c^2 + d^2$$

Hence when $a^2 + b^2 + c^2 + d^2 \neq 0$, we get the following:

$$(a + bi + cj + dk)^{-1} = \frac{a - bi - cj - dk}{a^2 + b^2 + c^2 + d^2}$$

Proposition 1.15 (16.8)
Let R be a ring and let $a, b \in R$.

1. $a0 = 0 = 0a$
2. $a(-b) = (-a)(b) = -(ab)$
3. $(-a)(-b) = ab$

Proof.

1. $a0 = a(0+0) = a0 + a0 \Rightarrow 0 = a0$
   $0a = (0+0)a = 0a + 0a \Rightarrow 0 = 0a$
2. $0 = a0 = a(b + -b) = ab + a(-b)$ so $-(ab)$ is the additive inverse of $a(-b)$ i.e. $-(ab) = a(-b)$.
   Similarly, $(-a)(b) = -(ab)$ because $0 = 0b = (a + -a)b = ab + (-a)b \Rightarrow -(ab) = (-a)(b)$
3. $(-a)(-b) = -(-(a)b) = -(-(ab))$. But $-(-ab) = ab$ because inverse of inverse is itself. Note, use notation $a - b = a + -b$.

$\square$