# Class 19

April 5, 2024

## Characteristic

Let $R$ be a ring. The characteristic of $R$, $\text{Char}(R)$ is the least positive integer such that $n * x = 0$ for all $x \in R$. (Here, we mean $n * x$ to be repeated addition of $x$, **not** multiplication in $R$ using the multiplication operation in $R$). If no such $n$ exists, we say the $\text{Char}(R) = 0$.

### Ex 1

Consider $R_1 = \mathbb{Q}$. $\text{Char}(R_1) = 0$ as $n * 1 \neq 0$ for any positive $n$.

### Ex 2

$R_2 = \mathbb{Z}_5$. $\text{Char}(R_2) = 5$. To show this, let's take the repeated sum of each element mod 5.

$$0 + 0 + 0 + 0 + 0 =_5 0$$

$$1 + 1 + 1 + 1 + 1 =_5 0$$

$$2 + 2 + 2 + 2 + 2 =_5 0$$

$$3 + 3 + 3 + 3 + 3 =_5 0$$

$$4 + 4 + 4 + 4 + 4 =_5 0$$

To show there cannot be a smaller positive $n$, add 1 to itself mod 5. If you add less than 5 of them, you will not get 0 mod 5. This will motivate our final theorem.

### Thm

Let $R$ be a ring with unity 1. The order of 1 under addition is the same as $\text{Char}(R)$ if the order of 1 is finite. (Recall the order of 1 is the smallest positive integer $n$ such that $n * 1 = 0$). If the order of 1 is infinite, than $\text{Char}(R) = 0$.

### Pf

Let's consider the case where the order of 1 is infinite first. This means there is no positive integer $n$ such that $n * 1 = 0$, thus $\text{Char}(R) = 0$. Now, suppose the order of 1 is finite and equals $n$. That is

$$n * 1 = 1 + 1 + \ldots + 1 = 0$$

Then for any $x \in R$

$$n * x = n * 1x = 1x + 1x + \ldots + 1x$$

$$(1 + 1 + \ldots + 1)\, x = (n * 1)\, x = 0x = 0$$

As the order of 1 is $n$, there cannot exist a smaller positive integer $m$ such that $m * x = 0$ for all $x \in R$, as this is not true for 1.

### Thm

The characteristic of an integral domain is 0 or prime.

### Pf

This is analogous to stating that for any integral domain with a non-zero characteristic $n$, then $n$ must be prime. Suppose $n$ is not prime. That is $\exists s, t$ such that $1 < s, t < n$ such that $n = st$. Then for all $x \in R$,

$$n * x = st * x = 0$$

If we multiply both sides by $x$, and break $n$ into it's factors, we get

$$(s * x)(t * x) = st * x^2 = 0x = 0$$

but since $R$ is an integral domain, this implies $s * x = 0$ or $t * x = 0$, and as $s, t < n$, this means the characteristic is not $n$! Thus to avoid contradiction, $n$ must be prime if $n$ exists.

## Activity

For the three rings below, determine the following:

1. Is $R$ an integral domain?
2. Is $R$ a field?
3. Char $(R)$

**The Rings**

1. $R_1 = \mathbb{C}$, the complex numbers under the usual definition of addition and multiplication
2. $R_2 = \mathbb{Z}[x]$, the set of all polynomials with integer coefficients under the usual definition of multiplication and addition
3. $R_3 = M_2[\mathbb{Z}_2]$, the set of all $2 \times 2$ matrices with elements in $\mathbb{Z}_2$, where element wise addition and multiplication are mod 2. (Basically use elements of $\mathbb{Z}_2$ instead of $\mathbb{R}$ when doing matrix computations)

$R_1$

$\mathbb{C}$ is an integral domain. Consider $a + bi, c + di \in \mathbb{C}$. Suppose the product of these two elements is 0. That is

$$(a + bi)(c + di) = 0 + 0i$$

$$= ac - bd + (bc + ad)i = 0 + 0i$$

$$ac - bd = 0$$

$$bc + ad = 0$$

As we showed in a previous example (The Gaussian integers), this is only possible if $c, d = 0$ or $a, b = 0$, thus $\mathbb{C}$ is an integral domain. $\mathbb{C}$ is a field. Consider $a + bi \neq 0$. We want to show that there are multiplicative inverses for each complex number. Consider

$$\frac{1}{a + bi} = \frac{1}{a + bi} * \frac{a - bi}{a - bi} = \frac{a - bi}{a^2 + b^2} = \frac{a}{a^2 + b^2} + \frac{-b}{a^2 + b^2} i \in \mathbb{C}$$

as $a + bi \neq 0$, thus each nonzero complex number $a + bi$ has a multiplicative inverse, so $\mathbb{C}$ is a field. Char $(\mathbb{C}) = 0$ as

$$n * 1 \neq 0 \; \forall n > 0$$

$R_2$

$R_2$ is an integral domain. Consider the product of two nonzero polynomials $\sum_{i=0}^{n} a_i x^i$, $\sum_{i=0}^{m} b_i x^i$. Then the highest order term of their product will be

$$a_n b_m x^{n+m} \neq 0$$

as $a_n, b_m \neq 0$ in the highest order term, thus their product cannot be 0 (Which would require the coefficient in each term of the product to be zero). $R_2$ is not a field. Consider the polynomial 2. There is not an integer $a$ such that

$$2a = 1$$

thus there cannot be a polynomial with integer coefficients such that $2 \sum_{i=0}^{\infty} a_i x^i = 1$. Char$(R_2) = 0$ as

$$n * 1 \neq 0 \ \forall n > 0$$

$R_3$

$M_2\left[\mathbb{Z}_2\right]$ is not an integral domain. Consider the matrices $\begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$. Then

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

Thus $R_3$ contains zero divisors. As $R_3$ contains zero divisors, it is not an integral domain. $R_3$ is not a field as it is not an integral domain. Char$\left(R_3\right) = 2$ as for any matrix $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in R_3$

$$A + A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+a & b+b \\ c+c & d+d \end{pmatrix}$$

since $\mathbb{Z}_2$ only contains $0, 1$ as elements, we get two cases. Suppose WLOG $a = 0$. Then $a + a = 0 + 0 =_2 0$. If $a = 1$ then $a + a = 1 + 1 =_2 0$, thus for each entry-wise sum of $A + A$, we get an entry of 0, so

$$A + A = \begin{pmatrix} a+a & b+b \\ c+c & d+d \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}$$