Tema 3.

$$\frac{\mathbb{Z}\times\mathbb{Z}}{1\mathbb{Z}\times 2\mathbb{Z}} \cong \mathbb{Z}_1 \times \mathbb{Z}_2$$

$(0, \; 1)$

$(1+2i)(1-2i)$

Congruencia

Def.: es una relación de equivalencia ($\equiv$) compatible con la estructura de anillo:

Subconjunto de $A \times A$ tal que la relación cumple:
- Reflexiva
- Transitiva
- Simétrica

Propiedades $\forall x, y, z, t \in A$ (Anillo)

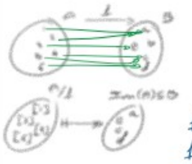
(Compatible con...)

* Suma $\left.\begin{matrix} x \equiv y \\ z \equiv t \end{matrix}\right\} x + z \equiv y + t$

* Producto $\left.\begin{matrix} x \equiv y \\ z \equiv t \end{matrix}\right\} xz \equiv yt$

* Opuestos $x \equiv y \Rightarrow -x \equiv -y$

Viene del producto: $\left.\begin{matrix} -1 \equiv -1 \\ x \equiv y \end{matrix}\right\} -x \equiv -y$



$f_*: A \twoheadrightarrow \mathrm{Im}(f)$ sobreyectiva

$f_*: A/_{\equiv} \boxed{\mapsto\!\twoheadrightarrow} \mathrm{Im}(f)$ $\boxed{\cong}$ Biyectiva = isomorfismo

$B \supseteq \mathrm{Im}(f)$

Estructura de anillo al conjunto de clases de equivalencia ($\boxed{A/_{\equiv}}$)

Siempre significa conjunto de las clases

No es igual que ($\backslash$)

Proyección canónica $\boxed{pr}: A \twoheadrightarrow A/_{\equiv}$ = morfismo de anillos

$$\left.\begin{array}{l} \bullet\ \underset{[a]}{\bar{a}} + \underset{[b]}{\bar{b}} := \underset{[a+b]}{\overline{a+b}} \\ \bullet\ \bar{a} \cdot \bar{b} := \overline{a \cdot b} \\ \bullet\ -\bar{a} := \overline{-a} \end{array}\right\} \forall \bar{a}, \bar{b} \in A/_{\equiv}$$

Núcleo de una congruencia: ($\mathrm{Ker}(\equiv)$)

$$\mathrm{Ker}(\equiv) := \{a \in A \,;\, a \equiv 0\}$$

Propiedades:

- $0 \in \mathrm{Ker}(\equiv)$
- Suma: $a, b \in \mathrm{Ker}(\equiv) \Longrightarrow a + b \in \mathrm{Ker}(\equiv)$
- Opuestos $a \in \mathrm{Ker}(\equiv) \Longrightarrow -a \in \mathrm{Ker}(\equiv)$
- Múltiplos $a \in \mathrm{Ker}(\equiv), \forall x \in A \Longrightarrow ax \in \mathrm{Ker}(\equiv)$

Ideales (I)

Def. Ideal de un anillo A es $\boxed{I \subseteq A}$ tal que:

cumple las propiedades del $\mathrm{Ker}(\equiv)$

De la propiedad de suma y múltiplos deducimos que es cerrado para comb. lineales.

$$\forall a, b \in I, \forall x, y \in A \Rightarrow \underbrace{xa}_{\in I} + \underbrace{yb}_{\in I} \in I$$

*) Todo núcleo de una congruencia es un ideal

*) Todo ideal de un anillo determina una congruencia

Proposición Si $\underbrace{I}_{\text{ideal}} \subseteq \underbrace{A}_{\text{anillo}}$, entonces $(\underbrace{a \equiv_I b}_{\text{congruencia}} \Longleftrightarrow a - b \in I) \Longrightarrow \mathrm{Ker}(\equiv_I) = I$

Demostración Primero debemos demostrar que es compatible con la estructura de anillo.

•) Producto $\left.\begin{matrix} a \equiv b \Longleftrightarrow (a-b) \in I \Longrightarrow (a-b)c \in I \\ c \equiv d \Longleftrightarrow (c-d) \in I \Longrightarrow (c-d)b \in I \end{matrix}\right\} \xRightarrow{\text{Sumando}} ac - \cancel{bc} + \cancel{bc} - db \in I \Longrightarrow ac - db \Longrightarrow \boxed{ac \equiv db}$

•) Suma $\left.\begin{matrix} a \equiv b \Longleftrightarrow (a-b) \in I \\ c \equiv d \Longleftrightarrow (c-d) \in I \end{matrix}\right\} \xRightarrow{\text{Sumando}} a - b + c - d \in I \Longleftrightarrow (a+c) - (b+d) \in I \Longleftrightarrow \boxed{a + c \equiv b + d}$

•) Opuesto por el producto deducimos que $\left.\begin{matrix} -1 \equiv -1 \\ a \equiv b \end{matrix}\right\} \Longrightarrow -1 \cdot a \equiv -1 \cdot b \Longrightarrow \boxed{-a \equiv -b}$

Ahora calculamos el núcleo:

$$\mathrm{Ker}(\equiv_I) = \{a \in A;\ a \equiv_I 0\} = \{a \in A;\ a - 0 \in I = a \in I\} = I$$

Dada una congruencia $\equiv$ en A, $\equiv_{\mathrm{Ker}(\equiv)} = \equiv$

$$\Downarrow$$

Dar una congruencia en $A \Longleftrightarrow$ Dar un ideal

$I \subseteq A \Longleftrightarrow \underbrace{a \equiv_I b}$ $a, b \in A \Longleftrightarrow$ "a es congruente con b modulo I" ($a \equiv b \bmod I$)

Todas las congruencias serán de esta forma

$A/_{\equiv_I} \Longleftrightarrow A/_I = \{$clases de equiv. modulo $I\}$ Usar esta

$A/_I$: $\bar{a} = \{x \in A;\ x \equiv_I a\} = \{x \in A;\ x - a \in I\} = a + I$

$\bar{a} \quad = \quad a + I$

$A/I : \bar{a} = \{x \in A;\ x \equiv_I a\} = \{x \in A;\ x - a \in I\} = a + I$

$\bar{a} = \underbrace{a + I}_{= \{a+y\ ;\ \forall y \in I\}}$

Propiedades de A/I

- $(a+I) + (b+I) := (a+b) + I$
  $\bar{a} + \bar{b} := \overline{a+b}$
- $(a+I) \cdot (b+I) := (a \cdot b) + I$
  $\bar{a} \cdot \bar{b} := \overline{ab}$
- $-(a+I) := (-a) + I$
  $-\bar{a} := \overline{-a}$

$pr : A \twoheadrightarrow A/I \quad a \in A \ pr(a) = a + I \in A/I$

Todo anillo tendrá al menos 2 ideales (Impropios)

- $\underbrace{0}_{\text{Ideal cero}} = \{0\} \leq A$ $\quad$ - $\underbrace{A}_{\text{Ideal total}} \leq A$

Si A es un anillo y $a \in A \Longrightarrow \exists I \leq A \ I = \underbrace{aA}_{\text{Múltiplos de } a}$

- Ideal cero = múltiplos de 0 $\quad 0 = 0A$
- Ideal total = múltiplos de 1 $\quad A = 1A$

$I \leq A$ será principal si $\exists a \in A$ tq $I = aA$

En $\mathbb{Z}$ todo ideal es principal

Demostración: $\underbrace{I}_{\text{Ideal no trivial } (I=1A)} \leq A \Longrightarrow I^+ = \{a \in I\ ;\ 0 < a\} \subseteq \mathbb{N}$

si $a \in I \Longrightarrow -1 \cdot a \in I = -a \in I$

Como $I^+ \neq \emptyset$, $a = \min(I^+)$. Ya que $a \in I^+ \subseteq I \Rightarrow \boxed{aA \subseteq I}$*

Tomemos $b \in I \Longrightarrow$ ya que $\underset{(a>0)}{a \neq 0}$ $\quad \frac{b}{a} \Rightarrow \exists q, r$ tq $b = aq + r$
$0 \leq r < |a| = a$ $\qquad$ * $\underline{I = aA}$

$r = 0$ ya que si $r \neq 0 \Longrightarrow \overset{\in I}{r} = \overset{\in I}{b} - \overset{\in I}{aq}$ y $r < a$ lo cual contradice $a = \min(I^+)$

Por lo que, con $r = 0 \Longrightarrow b = \overbrace{aq}^{\text{Múltiplo de } A} \in aA \Longrightarrow \boxed{I \subseteq aA}$*

Primer teorema de Isomorfía

$f : A \longrightarrow B \Longrightarrow \operatorname{Ker} f = \{a \in A; f(a) = 0\}$

$(0 \in \operatorname{Ker} f)$ y $\operatorname{Ker} f = I \leq A$

Para $\underbrace{\equiv}_{\text{una congruencia}}$ en A : $\operatorname{Ker}(\equiv) = \operatorname{Ker}(pr)$

$pr : A \twoheadrightarrow A/\equiv$

- Prop. Universal de la proyección canónica

$I \leq A \quad \underbrace{\bar{f}}_{\text{Morfismo/aplicación}} A/I \longrightarrow B \Longrightarrow \bar{f}(a+I) := f(a) \ \forall a \in A \Longleftrightarrow f(y) = 0 \ \forall y \in I$

$\bar{f} \Longleftrightarrow \underset{\forall a,b \in A}{a \equiv_I b} \Rightarrow f(a) = f(b)$

$a \equiv_I b \Longleftrightarrow a - b \in I \Longrightarrow f(a-b) = 0 \Longrightarrow f(a) = f(b)$

$\forall y \in I \ \ f(y) = 0 \qquad \bar{f}(0) = y$

Propiedad: $I \leq A \quad \bar{f} : A/I \longrightarrow B \Leftrightarrow f : A \longrightarrow B$ tq $f^*(I) = 0$

$$\begin{tikzcd} I \arrow[r, hook, "i"] \arrow[dr] & A \arrow[r, two heads, "pr"] \arrow[d, "\forall f"] & A/I \arrow[dl, dashed, "\exists! \bar{f}"] \\ & B & \end{tikzcd}$$

$f(y) = 0$
$\forall y \in I$

$\bar{f}(a+I) = \bar{f}(\bar{a}) = f(a)$

Demostración: Dado $f : A \longrightarrow B \Longrightarrow \bar{f} : A/I \longrightarrow B$ lo definimos como $\bar{f}(\overbrace{a+I}^{\bar{a}}) := f(a) \ \forall a \in A \Longleftrightarrow f(y) = 0 \ \forall y \in I$

$\forall a, b \in A \Rightarrow a \equiv_I b \Longrightarrow f(a) = f(b)$

$a \equiv_I b \Longleftrightarrow \underbrace{a-b}_{= y} \in I \Rightarrow f(a-b) = 0 \Rightarrow f(a) - f(b) = 0$
$f(a) = f(b)$

$\forall y \in I \ f(y) = 0 \Longrightarrow \underline{\bar{f}(I) = 0}$

$\bar{f} \Longrightarrow f$ $\quad \to f(y) = 0 \ \Downarrow \ \to f(a) = f(b) \Rightarrow a \equiv_I b$ $\Big]$ f tiene que cumplir que...

Sigue estudiando rey ♡

- Primer teorema de la Isomorfía

$f : A \longrightarrow B \quad \exists$ un isomorfismo ($\cong$) de anillos $\ b : A/\operatorname{Ker}_f \longrightarrow \operatorname{Im}(f)$

$$\begin{tikzcd} A \arrow[r, two heads, "pr"', "\text{sobreyectiva}"] \arrow[d, "f", "\text{nada}"'] & A/\operatorname{Ker} f \arrow[d, "b \cong"', "\text{Biyectiva}"] \\ B & \operatorname{Im}(f) \arrow[l, hook', "\text{Inyectiva}"', "\text{(inclusión)}"] \end{tikzcd}$$

Demostración

b lo definimos como $\ b : A/\operatorname{Ker}_f \longrightarrow \operatorname{Im}(f)$
$b(a + \operatorname{Ker} f) = f(a) \ \forall a \in A$

b es biyectiva ya que $\forall \bar{x} \in A/\operatorname{Ker} f \ \exists! f(x)$ tq $b(\bar{x}) = f(x)$

Ejemplo: $n \geq 2 \quad \underbrace{R}_{\text{morfismo de anillos}} : \mathbb{Z} \longrightarrow \mathbb{Z}_n$ $\ \to$ resto de dividir $\frac{a}{n}$
$\forall a \in \mathbb{Z} \longmapsto r$

La definimos como sobreyectiva ya que $\mathbb{Z}_n = \{x \in \mathbb{Z}\ ; 0 \leq x < n\}$

y $\forall a \in \mathbb{Z}$ tq $a < n \quad \underline{R(a) = a}$

Claramente, $R(a) = 0$ cuando $a \in n\mathbb{Z} \Longrightarrow \operatorname{Ker} R = n\mathbb{Z}$

El Primer Teorema de Isomorfía nos asegura que:

$b : \mathbb{Z}/n\mathbb{Z} \xrightarrow{\cong} \mathbb{Z}_n ; \ a + n\mathbb{Z} \longmapsto R(a)$

Hola guapito ♡ estudia muxooo

muac
muac

Operaciones con ideales

A : anillo $\qquad I, J \leq A$

- $I \cap J$ = ideal
- $I \cup J \neq$ no es ideal (por lo general)
- $I + J = \{a+b;\ a \in I\ b \in J\}$ = ideal El menor ideal que contiene a I y J
- $IJ = \left\{ \sum_{i=1}^{n} a_i b_i\ ;\ a_i \in I,\ b_i \in J \right\}$ = ideal $\subseteq (I \cap J)$

Si los ideales son principales $\left.\begin{array}{l} I = aA \\ J = bA \end{array}\right\} IJ = aAbA = (ab)A$