En $\mathbb{Z}$, dado un primo p, el cociente $\mathbb{Z}/p\mathbb{Z}$ es un campo. Por lo tanto $p\mathbb{Z}$ es un ideal maximo para cada primo p. Por otro lado, como $\mathbb{Z}$ es un dominio entero que no es campo, entonces 0 es primo pero no maximo.

Morfismos de anillos

Def: Sean R y T dos anillos. Una función $f: R \to T$ es un morfismo de anillos si cumple que:

·) $f(a+b) = f(a) + f(b) \quad \forall a, b \in R$

·) $f(ab) = f(a)f(b) \quad \forall a, b \in R$

·) $f(1_R) = 1_T$

Ejemplos: Las inclusiones $\mathbb{Z} \hookrightarrow \mathbb{Q} \hookrightarrow \mathbb{R} \hookrightarrow \mathbb{C}$, $K \hookrightarrow K[x]$

Las proyecciones canonicas: Dado un ideal I de un anillo R tenemos el morfismo $\pi: R \to R/I$ dado por $\pi(a) = a + I$.

Dado cualquier anillo R existe un único morfismo de anillos $\eta: \mathbb{Z} \to R$ definido como:

$$\eta: \mathbb{Z} \longrightarrow R$$

$$n>0 \quad \underbrace{1+\cdots+1}_{n \text{ veces}} = n \longmapsto \underbrace{1+\cdots+1}_{n \text{ veces}}$$

$$1 \longmapsto 1_R$$

$$\underbrace{(-1)+\cdots+(-1)}_{n \text{ veces}} = -n \longmapsto \underbrace{(-1)+\cdots+(-1)}_{n \text{ veces}}$$

Def: Sea $f: R \to T$ un morfismo de anillos. El nucleo de f es el conjunto

$$\operatorname{Ker} f = \{a \in R \mid f(a) = 0\}$$

- El núcleo de cualquier morfismo es un ideal.
- $I \subseteq R$ es un ideal si y solo si I es el nucleo de un morfismo de anillos

1.- Sea $r \in R$ y $x \in \operatorname{Ker} f$. Entonces $f(x)=0$.

$$f(rx)=f(r)f(x)=f(r)0=0$$

Por lo tanto $rx \in \operatorname{Ker} f$.

2.- $\Rightarrow)$ Sea I un ideal de R. Entonces $I = \operatorname{Ker} \pi$ donde $\pi: R \twoheadrightarrow R/I$ es la proyeccion canonica.

$\Leftarrow)$ ✓

Prop. Sea $f: R \to T$ un morfismo de anillos. Entonces, f es inyectiva si y solo si $\operatorname{Ker} f = \{0\}$.

Cor. Sea K un campo y $f: K \longrightarrow R$ un morfismo de anillos. Entonces f es inyectiva.

Dem:

Sea K un campo y $f: K \to R$ un morfismo de anillos. Tenemos que $\underline{\operatorname{Ker} f}$ es un ideal de K. Como K es campo, $\operatorname{Ker} f = 0$ ó $\operatorname{Ker} f = K$ pero $f(1) = 1 \neq 0$

Por lo tanto $\operatorname{Ker} f = 0$ ie, f es iny.

Prop. Sea $f: R \to T$ un morfismo de anillos. Si P es un ideal primo de T, entonces $f^{-1}(P) = \{a \in R \mid f(a) \in P\}$ es un ideal primo de R.

Dem:

Sabemos que la imagen inversa de un ideal es un ideal.

Sea $f: R \to T$ un morf. de anillos y P un ideal primo de T. Sean $a, b \in R$ tal que $ab \in f^{-1}(P)$. Ent $f(ab) \in P$ i.e., $f(a)f(b) \in P$. Como P es primo $f(a) \in P$ ó $f(b) \in P$ i.e., $a \in f^{-1}(P)$ ó $b \in f^{-1}(P)$

Cor. Sea $f: R \to D$ un morfismo de anillos con D un dominio entero. Entonces $\operatorname{Ker} f$ es un ideal primo de R.

K campo $\exists!\, \eta: \mathbb{Z} \longrightarrow K$ ent $\operatorname{Ker}\eta = p\mathbb{Z}$ con p primo ó $\operatorname{Ker}\eta = 0$

Sea $f: R \to T$ morfismo de anillos, la imagen de f, $\operatorname{Im} f = \{ f(a) \mid a \in R \}$ es un subanillo de T.

Prop. Dado $f: R \to T$ un morfismo de anillos

$$R/_{\operatorname{Ker} f} \cong \operatorname{Im} f.$$

$$a + \operatorname{Ker} f \mapsto f(a).$$

Teorema de la correspondencia:

Sea I un ideal de R y consideremos

$\pi : R \twoheadrightarrow R/I$. Entonces hay una biyeccion

$$\{J \text{ ideal de } R \text{ y } I \subseteq J\} \longleftrightarrow \{\text{ideales de } R/I\}$$

$$J \longmapsto \pi(J) = \{a+I \mid a \in J\}$$

$$\pi^{-1}(L) \longleftarrow\!\shortmid \quad L$$

Como esto es una biyeccion, $L = \{a+I \mid a \in \pi^{-1}(L)\}$

Entonces a un ideal de R/I se le suele denotar J/I donde J es un ideal de R que contiene a I.

Prop. Sean I y J ideales de R con $\underline{I \subseteq J}$.

Entonces:

$$\frac{R/I}{J/I} \cong R/J$$

$$(a+I) + J/I \overset{\cong}{\longmapsto} a+J$$

$R/I \xrightarrow{g} R/J$

$r+I \mapsto r+J$

$\operatorname{Ker} g = J/I$

g es sobre

por lo tanto

$$\frac{R/I}{J/I} \cong R/J.$$

Anillos Euclidianos

Def: Un dominio entero A se llama anillo euclidiano, si existe una función $N: A\setminus\{0\} \longrightarrow \mathbb{N}\cup\{0\}$, llamada grado o norma, tal que

(i) Para cualesquiera $a,b \in A\setminus\{0\}$, $N(a) \leq N(ab)$.

(ii) (Algoritmo de la división) Dados $a,b \in A$ con $b \neq 0$, existen $q,r \in A$ tales que: $a = bq + r$ con $r = 0$ ó $N(r) < N(b)$.

Ejemplos: Los ejemplos canónicos de anillos euclidianos son $\mathbb{Z}$ y $K[x]$.

Para $\mathbb{Z}$ tenemos la norma $N: \mathbb{Z}\setminus\{0\} \longrightarrow \mathbb{N}\cup\{0\}$, $N(x) = |x|$ (valor absoluto)

Veamos un ejemplo menos trivial. Consideremos el anillo $\mathbb{Z}[i]$ y la función $N: \mathbb{Z}[i]\setminus\{0\} \longrightarrow \mathbb{N}\setminus\{0\}$ dada como $N(a+b) = a^2+b^2$. Entonces $\mathbb{Z}[i]$ es euclidiano.

Como estamos usando la norma compleja, sabemos que $N(uv)=N(u)N(v)$ con $N(u)$ y $N(v)$ no negativos. Por lo tanto:

(i) Para $u,v\in\mathbb{Z}[i]\setminus\{0\}$, $N(u)\leq N(uv)$.

(ii) Algoritmo la división. Tomamos $u=a+bi$ y $v=c+di$ con $v\neq 0$ en $\mathbb{Z}[i]$.

Como complejos podemos hacer la división $\frac{u}{v}$, es decir,

$$\frac{u}{v}=\frac{u\bar{v}}{v\bar{v}}=\frac{(a+bi)(c-di)}{c^2+d^2}=\underbrace{\frac{(ac+bd)}{c^2+d^2}}_{s}+\underbrace{\frac{(bc-ad)}{c^2+d^2}}_{t}i$$

$$s+ti$$

Para $\frac{u}{v}=s+ti$ con $s,t\in\mathbb{Q}$ escojemos enteros $m,n\in\mathbb{Z}$ tales que $|s-m|\leq 1/2$ y $|t-n|\leq 1/2$. Se sigue que

$$\left|\frac{u}{v}-(m+ni)\right|=\left|(s+ti)-(m+ni)\right|=\left|(s-m)+(t-n)i\right|$$

$$=\left((s-m)^2+(t-n)^2\right)^{1/2}\leq\left(\frac{1}{4}+\frac{1}{4}\right)^{1/2}=\frac{1}{\sqrt{2}}$$

Pongamos $q = m + ni$ y así $r = u - vq \in \mathbb{Z}[i]$ y

$$|r| = |u - vq| = \left|v\left(\frac{u}{v} - q\right)\right| = |v|\left|\frac{u}{v} - (m+ni)\right| \leq |v| \frac{1}{\sqrt{2}}$$

Así

$$N(r) = |r|^2 \leq \frac{|v|^2}{\sqrt{2}^2} = \frac{N(v)}{2} < N(v)$$