Anillos Conmutativos

Def: Un anillo es un conjunto R con dos operaciones binarias $+$ y $\cdot$ tales que

Suma

$(R,+)$ es un grupo abeliano

Neutro: 0

Inverso: $\forall a \in R \ \exists -a \in R$ t.q. $a+(-a)=0$

Multiplicación:

·) Es asociativa

·) Neutro: $1 \neq 0$

·) $ab = ba \quad \forall a,b \in R$

Distributividad: $a(b+c) = ab + ac$.

Ejemplos: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_n$. Si K es un campo tenemos el anillo $K[x]$.

Consideremos $i \in \mathbb{C}$ ie, $i^2 = -1$. Entonces el conjunto $\mathbb{Z}[i] = \{a+bi \,/\, a,b \in \mathbb{Z}\}$ es un anillo

Dados $a+bi$ y $c+di$ en $\mathbb{Z}[i]$, ie, $a,b,c,d \in \mathbb{Z}$. Así:

$(a+bi)+(c+di) = (a+b)+(c+d)i$ con $a+b$ y $c+d$ en $\mathbb{Z}$

$(a+bi)(c+di)=(ac-bd)+(ad+bc)i$ con $(ac-bd)$ y $(ad+bc) \in \mathbb{Z}$

Por lo tanto, con la suma y producto de numeros complejos, $\mathbb{Z}[i]$ es un anillo.

Def: Sea R un anillo e $I \subseteq R$. Decimos que I es un ideal si:

-) $0 \in I$
-) $a, b \in I$, ent $a+b \in I$
-) $\forall r \in R$ $\forall a \in I$ se tiene que $ra \in I$

Ejemplos: 0 y R siempre son ideales. Para cada $n\in\mathbb{Z}$, $n\mathbb{Z}=\{na \mid a\in\mathbb{Z}\}$ es un ideal.

Recordemos que un anillo K es un campo si todo elemento distinto de cero tiene inverso multiplicativo.

Prop. Un anillo R es campo si y solo si sus unicos ideales son 0 y R

Dem:

$\Rightarrow$) Sea $0\neq I$ un ideal. Ent existe $0\neq a\in I$. Por hip a tiene inverso mult a^{-1}. Asi $1=aa^{-1}\in I$. Por lo tanto $\forall r\in R$, $r=r\cdot 1\in R$ $\therefore$ $I=R$.

$\Leftarrow$ 0 y R son los unicos ideales. Sea $a \neq 0$
$Ra = \{ra \mid r \in R\}$ es un ideal. Por hip. $Ra = R$
$\therefore 1 = ra$ p.a. $r \in R$ $\therefore$ $r = a^{-1}$

Def: Sea R un anillo y P un ideal propio de R. Decimos que P es primo si $ab \in P \Rightarrow a \in P$ ó $b \in P$ para cualesquiera $a, b \in R$.

Def: Sea R un anillo y $\mathcal{M}$ un ideal propio de R. Decimos que $\mathcal{M}$ es máximo si siempre que $\mathcal{M} \subsetneq I \subseteq R$ entonces $I = R$.

Prop. 1.- Todo anillo contiene ideales maximos. Hay que usar Lemma de Zorn.
2.- Todo ideal maximo es primo.

Dem:

2: Sea $\mathcal{M}$ un ideal maximo de R y sup que $\underline{ab \in \mathcal{M}}$. Sup que $a \notin \mathcal{M}$ ni $b \notin \mathcal{M}$. Consideramos $\mathcal{M}+Ra=\{m+ra \mid m \in \mathcal{M}\ r \in R\}$. Como $\mathcal{M}$ es maximo $\mathcal{M}+Ra=R$. Ent $1=m+ra$.

Multiplicando por b:

$$b = b(m+ra) = \underline{mb} + \underline{rab} \in \mathcal{M} \ !$$

$\therefore$ $\mathcal{M}$ es primo.

Anillo Cociente

Consideremos R un anillo e I un ideal. El anillo cociente R/I son las clases de equivalencia de la relacion: $a \sim b \Leftrightarrow a-b \in I$.

$R/I = \{a+I \,/\, a \in R\}$ es un anillo con las siguientes operaciones

$(a+I)+(b+I) = (a+b)+I \qquad (a+I)(b+I) = ab+I$.

Def: Un anillo R es un dominio entero si 0 es un ideal primo, es implica $a=0$ ó $b=0$.

Prop: Sea R un anillo y P un ideal propio de R:

1.- P es primo $\Leftrightarrow R/P$ es un dominio entero

2.- P es maximo $\Leftrightarrow R/P$ es campo.

Dem:

1.- $\Rightarrow$ | Sup $(a+P)(b+P) = 0 \in R/P$ $\therefore$ $ab+P = 0+P$ $\therefore$ $ab \in P$. Como

P es primo $a\in P$ ó $b\in P$. Si $a\in P$ ent $\underline{a+P}=0+P$. Si $b\in P$, ent $\underline{b+P}=0+P$.

$\therefore$ R/P es dominio entero.

$\underline{\Leftarrow}|$ Sup. $ab\in P$. Pasando a R/P, $0+P=ab+P$
$=(a+P)(b+P)$. Como R/P es dom. ent.
$a+P=0+P$ ó $b+P=0+P$ ie $a\in P$ ó $b\in P$.

$\underline{2:\ \Rightarrow}|$ Sup. que P es maximo y $0\neq a+P\in R/P$
ie $a\notin P$. Por lo tanto $P+Ra=R$. Tomando
$1=p+ra \Rightarrow 1-ra\in P \therefore 1+P=ra+P$
$=(r+P)(a+P)$.

$\Leftarrow$ Sup R/P es campo. Sea I un ideal t.q.

$\underbrace{P \subsetneq I}$. Sea $\hat{I} = \{\underline{a+P} \mid a \in I\} \subseteq R/P$

Ent $\hat{I}$ es un ideal de R/P y además

$\hat{I} \neq 0$. Por lo tanto $\hat{I} = R/P$. Entonces

$1+P \in \hat{I}$ i.e. $1+P = a+P$ con $a \in I$. Así

$1-a \in P \Rightarrow 1-a = p \Rightarrow 1 = p+a \in I$

$\therefore \underline{I = R}$

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:

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 $\pi(a) = a + I$.