Sabemos que en $\mathbb{Z}$ todos los ideales son de la forma $\langle n \rangle$, $n \in \mathbb{Z}$

$$\langle a, b \rangle = \{ r \cdot a + b j \, , \, r, j \in \mathbb{Z} \}$$

ideal de $\mathbb{Z}$.

$\Rightarrow \exists d \in \mathbb{Z} : \quad \langle a, b \rangle = \langle d \rangle$

Prop: Sean $a, b \in \mathbb{Z}$ no ambos 0 sea $d \in \mathbb{Z}$ $\langle d \rangle = \langle a, b \rangle$

Luego:

- $d = ar + bj$ por algún $r, j \in \mathbb{Z}$.
  (↳ Identidad de Bezout)
- d divide a a y b
- Si $e \in \mathbb{Z}$ divide a a y b, luego e divide d.

(d es el máximo divisor común entre a y b.)

Dem:

$d \in \langle d \rangle = \langle a, b \rangle$

$= \{ ar + bj, \; r, j \in \mathbb{Z} \}$

ideal

- $a, b \in \langle a, b \rangle = \langle d \rangle \Rightarrow d \mid a$ y $d \mid b$
- $e \mid a$ y $e \mid b$ luego $e \mid (ar + bj) = d$

Def:

Sea A un anillo. Si $a \in A$ t.q $\exists a^{-1} \in A$. se llama unidad.

↝ unidad es cualquier elemento invertible

- 1_A es unidad
- si $a \in A$ es unidad, también $a^{-1} \in A$ lo es: $a \cdot a^{-1} = 1$, $(a^{-1})^{-1} = a$
- si a, b unidades $(ab)^{-1} = b^{-1} a^{-1}$

Desde Ahora todos los anillos son conmutativos con 1.

Quiero decir que en esta parte del curso los anillos son inútiles :

Sean $a, b \in A$, a y b son asociados si existe $\mu \in A$ unidad t.q. $a = \mu b$

en $\mathbb{Z}$ las unidades son ± 1 y por ende a es asociado $a \pm a$.

Ser asociado es relación de equivalencia.

Dos números asociados son la misma factorización con cambio de signo. Por eso digo que solo nos sirve uno de ellos.

Def Primo:

Sean A un anillo, $a \in A$ y $a \neq 0$ y a no es unidad es irreducible (no lo puedo romper en producto de 2 cosas) si todas veces

$$a = bc$$

b ó c son unidades (± 1).

En $\mathbb{Z}$ esto está diciendo p es irreducible sii los únicos divisores de p son $\pm 1, \pm p$.

Def Primo Un entero p es primo si cuando $p|ab$.

Necesariamente $p|a$ ó $p|b$.

Lema: un entero es primo sii es irreducible.

Dem: Puedo asumir $p > 0$

($\Rightarrow$): Si p fuera reducible existirían a, b:

$$1 < a, b < p \quad \text{con}$$

$$a \mid p \quad \text{y} \quad b \mid p.$$

luego $p \mid p = ab$ pero $p \nmid a$, $p \nmid b$.

($\Leftarrow$): Sea p irreducible y $p \mid ab$

Asumimos $p \nmid a$ y mostramos $p \mid b$.

por hipótesis el $\gcd(p, a) = 1$

por Bézout

$$1 = pr + as, \quad r, s \in \mathbb{Z}$$

equivalentemente

$$b = pbr + abs$$

$$p \mid pbr \quad \text{y} \quad p \mid abs$$

luego $p \mid (pbr + abs) = b$ ■.

Teorema fundamental de la aritmética

Sea $a \in \mathbb{Z}$, $a \neq 0$. Luego

$$a = c p_1 \cdots p_K$$

Con $c = \pm 1$, $p_i \geq 0$ primos, $K \geq 0$.

Además la escritura es única a menos que reordenemos los p_i's.

Dem:

① Existencia:

Podemos asumir $a \geq 1$. Por inducción fuerte sobre a.

Base) $a = 1$

Nada que hacer.

Paso Inductivo) Si a es primo $a = p \cdot 1$.

Si no, existen

$$1 < b, b' < a$$

Con $a = bb'$.

Por hipótesis inductiva b y b' tiene una factorización. Juntándolas - multiplicandolas obtenemos una factorización de a.

Unicidad:

$$a = \pm 1 \cdot p_1 p_2 \cdots p_k = \pm 1\, q_1 q_2 \cdots q_r$$

Siendo $p_i, p_j \geq 0$ el signo es igual

$p_1 \mid p_1 p_2 \cdots p_k$ luego $p_1 \mid q_1 \cdots p_r$

es decir existe $q_j = p_1$. Puedo, al menos reordenar, asumir $q_1 = p_1$ Dividiendo por p_1 obtenemos:

$$p_2 \cdots p_k = q_2 \cdots q_r$$

Repetimos para obtener $k = r$ y $p_i = q_i$. ∎

Ejercicio: en $\mathbb{Z}$ un ideal es primo sii es maximal.