Taller Preparcial #2

Estudiante: David Alsina **Nota:** 5.0?

1. [1 pt] Sea D un dominio de integridad y sean $a, b \in D$. Asuma que $a^n = b^n$ y $a^m = b^m$ para dos enteros positivos n y m primos entre sí. Demuestre que $a = b$.

Como D es un dominio de integridad sabemos que es conmutativo con identidad y sin divisores de cero.

tenemos $a^n = b^n$ y $a^m = b^m$, para dos enteros positivos primos entre sí.

- $\gcd(m, n) = 1$, m no es multiplo de n y viceversa
- Si n y m son primos entre sí entonces $\exists\, x, y : nx + my = 1$ (Bezóuts identity)

(Note que Bezóuts implica o que x es negativo o y es negativo, luego para evitar exponentes negativos diremos lo siguiente.

Como D es PID por teorema se sabe que se puede crear un homomorfismo de D en su campo de fracciones, donde si tenemos elementos a una potencia negativa. (esto lo usaremos más adelante).

$$a^n = b^n \qquad \Big| \qquad a^m = b^m$$
$$a^n - b^n = 0 \qquad \Big| \qquad a^m - b^m = 0$$

$$a^n - b^n = a^m - b^m$$
$$a^n - a^m = b^n - b^m$$

Si $n < m$:

$$\varphi(a^n - a^m) = \varphi(b^n - b^m)$$
$$\varphi(a^n) - \varphi(a^m) = \varphi(b^n) - \varphi(b^m)$$
$$\varphi\left(\prod^n a\right) - \varphi\left(\prod^m a\right) = \varphi\left(\prod^n b\right) - \varphi\left(\prod^m b\right)$$
$$\varphi(a)^n - \varphi(a)^m = \varphi(b)^n - \varphi(b)^m$$
$$\varphi(a)^n\left(1 - \varphi(a)^{m-n}\right) = \varphi(b)^n\left(1 - \varphi(b)^{m-n}\right)$$
$$\cancel{\varphi(a^n)}\left(1 - \varphi(a)^{m-n}\right) = \cancel{\varphi(b^n)}\left(1 - \varphi(b)^{m-n}\right)$$
$$\left(\cancel{1} - \varphi(a)^{m-n}\right) = \left(\cancel{1} - \varphi(b)^{m-n}\right)$$
$$\cancel{-}\varphi(a)^{m-n} = \cancel{-}\varphi(b)^{m-n}, \quad \exists x, y \text{ de bezóut}$$
$$(\varphi(a)^{m-n})^{x-y} = (\varphi(b)^{m-n})^{x-y}$$
$$\varphi(a)^{mx - nx - my + ny} = \varphi(b)^{mx - nx - my + ny}$$
$$\left(\varphi(a)^{nx+my}\right)^{-1} \varphi(a)^{mx} \varphi(a)^{ny} = \left(\varphi(b)^{nx+my}\right)^{-1} \varphi(b)^{mx} \varphi(b)^{ny}$$
$$\varphi(a)^{-1} \cancel{\varphi(a)^{mx}} \cancel{\varphi(a)^{ny}} = \varphi(b)^{-1} \cancel{\varphi(b)^{mx}} \cancel{\varphi(b)^{ny}}$$
$$\varphi(a)^{-1} = \varphi(b)^{-1}$$
$$\varphi(a) = \varphi(b)$$
$$\varphi(a) - \varphi(b) = 0 = \varphi(0)$$
$$\varphi(a-b) = \varphi(0) \Rightarrow a - b = 0$$
$$a = b \quad \blacksquare$$

2. [1 pt] Sea A un PID y sea $a \in A$ con $a \neq 0$. Demuestre que $\langle a \rangle$ es un ideal maximal de A si y solo si a es irreducible.

Dado A PID digamos $\langle c \rangle$ genera A y además A es un dominio de Integridad. En el cual cualquier ideal es principal.

$(\Rightarrow)$ Suponga que $\langle a \rangle$ es un maximal de A. luego si J es un ideal t.q. $\langle a \rangle \subseteq J \subseteq A$ tenemos que $\langle a \rangle = J$ ó $J = A$.

Asuma por Absurdo entonces que a es reducible luego:

Como $\langle a \rangle$ es maximal hay 2 casos:

Caso 1) $\langle a \rangle = \langle c_1 \rangle$, $a = c_1 \cdot \ldots \cdot c_n$ donde cada c_i es un factor irreducible.

$$\{ax : x \in A\} = \{c_1 x : x \in A\}$$

$$\{c_1 \cdot \ldots \cdot c_n x : x \in A\} = \{c_1 x : x \in A\}$$

Como A es PID el hecho de que $\langle a \rangle = \langle c_1 \rangle$ implica que a y c_1 son asociados

más claramente $c_1 \cdot \ldots \cdot c_n$ y c_1 son asociados

$(\Rightarrow)(\Leftarrow)$

Caso 2)

$\langle c_1 \rangle = A$, $\langle a \rangle \subseteq \langle c_1 \rangle \subseteq A$

$a = c_1 \cdot \ldots \cdot c_n$

Cada c_i es irreducible.

$$A = \langle c_1 \rangle = \{ c_1 x : x \in A \}$$

$$\langle a \rangle = \{ ax : x \in A \} = \{ c_1 \cdot \ldots \cdot c_n x : x \in A \}$$

Porque $A = \langle c_1 \rangle$ $= \{ c_1^2 \cdot c_2 \cdot \ldots \cdot c_n x : x \in A \}$

lo anterior nos dice $\langle a \rangle = \langle c_1 a \rangle$

Así a es asociado de $c_1 a$, más claramente $c_1 \cdot \ldots \cdot c_n$ es asociado de $c_1^2 \cdot c_2 \cdot \ldots \cdot c_n$. ($\Longrightarrow$ $\Longleftarrow$)

Contradicción que surge en ambos casos por asumir que a es reducible, luego a debe ser irreducible.

$(\Longleftarrow)$ Sea a irreducible, recordemos que $a \in A$, A es PID.

escoja un $\langle b \rangle$ tal que

$$\langle a \rangle \subseteq \langle b \rangle \subset A.$$

entonces $a = bx$, para algún $x \in A$.
debido a que a es irreducible entonces hay 2 casos:

① b es unidad, luego $\langle b \rangle = A$.

② x es unidad, $a = bx$
$ax^{-1} = bxx^{-1}$
$ax^{-1} = b$

Como x^{-1} también es unidad surge que
$\langle a \rangle = \langle b \rangle$.

esto corresponde entonces a que $\langle a \rangle$ sea maximal.

3. [2 pts]

a) Sea p un número entero primo. Demuestre que o p sigue siendo primo en $\mathbb{Z}[i]$ o p es el producto de dos primos en los enteros de Gauss conjugados: $p = \pi\overline{\pi}$;
[*Sugerencia:* $\pi \mid p \implies \overline{\pi} \mid p$.]

b) Sea π un primo en los enteros de Gauss. Luego o $\pi\overline{\pi}$ es un primo en $\mathbb{Z}$ o es el cuadrado de un primo en $\mathbb{Z}$.
[*Sugerencia: una factorización en primos en* $\mathbb{Z}$ *es todavía una factorización en* $\mathbb{Z}[i]$*, no necesariamente en irreducibles.*]

Observación: este ejercicio implica que los primos en $\mathbb{Z}[i]$ *son los primos* $p \in \mathbb{Z}$ *que no se pueden escribir como suma de cuadrados o los elementos de la forma* $a + bi$ *tales que* $a^2 + b^2$ *sea un primo en* $\mathbb{Z}$*. Un teorema de teoría de los números dice que* $p \in \mathbb{Z}$ *es una suma de cuadrados si y solo si* $p = 2$ *o* $p \equiv 1 \pmod 4$.

a) Sea p un número entero primo

① Sea π un entero de gauss primo
(π, su norma es mayor que 1 y no puede descomponerse en un producto de dos gausianos enteros, cuyas normas sean menores que π)

Suponga que $\pi \mid p \therefore \exists \pi_* $ t.q. $p = \pi\pi_*$

$$p = (a+bi)(c-di)$$
$$= ac - adi + bci + bd$$
$$= (ac+bd) + i(bc-ad)$$

Como p es entero no debe tener parte imaginaria luego

$$ad = bc \Rightarrow d = \frac{bc}{a} \quad (1)$$

Así:

$$p = ac + bd$$
$$p = ac + \frac{b^2c}{a}$$
$$p = \frac{a^2c}{a} + \frac{b^2c}{a} = \frac{c(a^2+b^2)}{a} \quad (2)$$

Como p debe ser entero no puede ser de una forma racional como tenemos, lo que nos lleva a 2 casos:

② $a \mid c$, $c = ak$, $k \in \mathbb{Z}^+$.

$$p = \frac{a^2c}{a} + \frac{b^2c}{a} = \frac{c(a^2+b^2)}{a} = \frac{\cancel{a}k(a^2+b^2)}{\cancel{a}}$$
$$p = k(a^2+b^2) = kq, \; q = (a^2+b^2)$$

para no llegar a un absurdo $p = kq$ debe tener como unidad a uno de sus factores, vea note que debe ser k, luego $c = a$.

Por (2) decimos que

$$p = \frac{\cancel{a}(a^2+b^2)}{\cancel{a}\; 1} = a^2+b^2$$
$$= (a+bi)(a-bi)$$
$$= \pi\,\overline{\pi}$$

en particular $\pi = \overline{\pi}$.

Así llegamos a que p primo es $p = \pi\overline{\pi}$.

luego si $\pi \mid p \Rightarrow p = \pi\,\overline{\pi}$, note que el caso contrario es directo, si $p = \pi\overline{\pi}$ entonces $\pi \mid p$. ergo $\pi \mid p \Leftrightarrow \pi\overline{\pi} = p$

en particular decimos que dado p primo lo podemos escribir como producto de complejos en particular $p = \pi\overline{\pi}$.

2 Sea p primo podemos escribirlo en $\mathbb{Z}[i]$ como $p = p + 0i$.

2.1 note que por poco $p = \pm 2 + 0i$ y $\|p\| > 1$ en este caso, entonces $|p|$ siempre será mayor a 1.

2.2 Por absurdo suponga que $p + 0i$ se puede descomponer en producto de 2 complejos de norma menor a p.

luego $p = \pi\,\overline{\pi}$
$$= (a+bi)(c+di)$$
$$= ac + adi + bci - bd$$

$= (ac - bd) + i\underbrace{\cancel{(ad + bc)}}_{0}$

$\Rightarrow ad = bc$, $a = \frac{bc}{d}$, luego:

$$p = \frac{bc^2}{d} - \frac{bd^2}{d} = \frac{b(c^2 - d^2)}{d}$$
$$= \frac{b(c+d)(c-d)}{d}$$

entonces hay que $d \mid b$ ó $d \mid (c+d)$ ó $d \mid (c-d)$
en cualquier caso se tendrá que p es el producto de enteros.

- Si $d \mid b \Rightarrow p = k(c+d)(c-d)$ $(\Rightarrow\Leftarrow)$
- si $d \mid (c+d) \Rightarrow p = bm(c-d)$ $(\Rightarrow\Leftarrow)$
- si $d \mid (c-d)$ análogo. $(\Rightarrow\Leftarrow)$

luego p debe ser primo en $\mathbb{Z}[i]$.

b

b) Sea π un primo en los enteros de Gauss. Luego o $\pi\overline{\pi}$ es un primo en $\mathbb{Z}$ o es el cuadrado de un primo en $\mathbb{Z}$.
[*Sugerencia: una factorización en primos en* $\mathbb{Z}$ *es todavía una factorización en* $\mathbb{Z}[i]$, *no necesariamente en irreducibles.*]

4. [1 pt] Demuestre que los enteros de Gauss son un dominio euclídeo con función euclidea: $d(x+iy) = x^2 + y^2$.

[Sugerencia: si $z_1, z_2 \in \mathbb{Z}[i]$, con $z_2 \neq 0$, se puede escribir $z_1/z_2 = u + iv \in \mathbb{C}$, con u, v racionales. Razonando geometricamente, encuentre $m, n \in \mathbb{Z}$ tales que $|(u+iv) - (m+in)| \leq 1/\sqrt{2}$.]

observe nuestra función d es la norma al cuadrado entonces para decir que los enteros de gauss son dominio euclideo hay que probar 2 cosas sobre nuestra función d.

① $d(ab) \geq d(a)$ para $a, b \neq 0$ y $a, b \in \mathbb{Z}[i]$

$a = k + mi$, $b = l + ni$, $k, m, n, l \in \mathbb{Z}$

$$ab = (kl - mn) + i(ml + kn)$$

$$\Rightarrow d(ab) = (kl - mn)^2 + (ml + kn)^2$$

$$= (kl)^2 - \cancel{2klmn} + (mn)^2 + (ml)^2 + \cancel{2klmn} + (kn)^2$$

$$= (kl)^2 + (mn)^2 + (ml)^2 + (kn)^2$$

$$= k^2(l^2 + n^2) + m^2(l^2 + n^2)$$

$$= (l^2 + n^2)(k^2 + m^2)$$

$$= d(a) \cdot d(b)$$, note que como $b \neq 0$ $d(b) \geq 1$

$$\Rightarrow d(ab) = d(a) \cdot d(b) \geq d(a)$$

② Sean $a, b \in \mathbb{Z}[i]$, $b \neq 0$ queremos decir que $\exists\, q, r \in R$ con $a = bq + r$ y hay 2 casos: $r = 0$ ó $d(r) < d(b)$

digamos $\frac{a}{b} = \frac{k+mi}{l+ni} \cdot \frac{(l-ni)}{(l-ni)} = \frac{kl - kni + mli + mn}{l^2+n^2}$

$$= \frac{(kl+mn) + i(ml - kn)}{l^2+n^2}$$

$$= \frac{kl+mn}{l^2+n^2} + i\,\frac{ml-kn}{l^2+n^2}$$

Aquí tendremos que usar la Sugerencia:

- encuentre $m, n \in \mathbb{Z}$ tales que

$$|(u+iv) - (m+in)| < \frac{1}{\sqrt{2}}, \quad \frac{z_1}{z_2} = u+iv,\ u,v \in \mathbb{Q}$$

$$\sqrt{d((u+iv)-(m+in))} < \frac{1}{\sqrt{2}}$$

$$d((u+iv)-(m+in)) < \frac{1}{2}$$

Note que $\frac{kl+mn}{l^2+n^2}$ es racional y $\frac{ml-kn}{l^2+n^2}$ también (obviando su parte compleja).

luego u es parecido a $\frac{kl+mn}{l^2+n^2}$,

también vi es parecido a $\frac{ml-kn}{l^2+n^2}i$.

el ejercicio consiste en encontrar un entero "m" para $\frac{kl+mn}{l^2+n^2}$ (parecido a u) y otro entero "n" para $\frac{ml-kn}{l^2+n^2}$ (parecido a v), respectivamente estos enteros serán: q_1 y q_2.

función techo

función piso

$$\left\lfloor \frac{kl+mn}{l^2+n^2} \right\rfloor \leq \frac{kl+mn}{l^2+n^2} \leq \left\lceil \frac{kl+mn}{l^2+n^2} \right\rceil$$

luego $q_1 = \left\lfloor \frac{kl+mn}{l^2+n^2} \right\rfloor$ ó $q_1 = \left\lceil \frac{kl+mn}{l^2+n^2} \right\rceil$

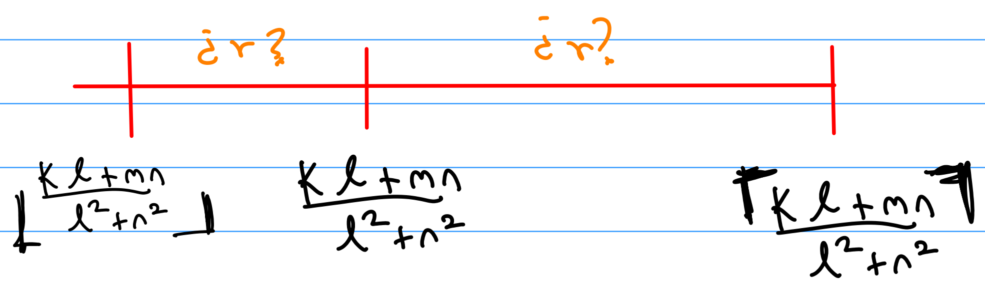
Análogamente $q_2 = \left\lfloor \frac{ml-kn}{l^2+n^2} \right\rfloor$ ó $q_2 = \left\lceil \frac{ml-kn}{l^2+n^2} \right\rceil$

entonces hemos encontrado q_1 y q_2

$$re(a) = q_1 b + r_1$$
$$Im(a) = q_2 b + r_2$$

Como vemos

Nos falta hablar sobre r_1, r_2 ya que bq_1, $b_2 q_2$ produce un número un poco más grande o más pequeño que $re(a)$, $Im(a)$ respectivamente.



Para caracterizar r_1 y r_2 tenga en cuenta el hecho de que:

$$\left\lceil \frac{kl+mn}{l^2+n^2} \right\rceil - \left\lfloor \frac{kl+mn}{l^2+n^2} \right\rfloor = 1$$

luego análogamente r_1, r_2 van a ser a lo sumo $\frac{1}{2}$.

todo junto es:

$$a = (q_1+q_2)b + r_1 + r_2 i$$

luego

$$d(r_1+r_2 i) = \left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2$$
$$= \frac{1}{2}$$

Vea que $d(b)$ es claramente más grande que $\frac{1}{2}$.

Por otra parte el caso $r=0$ es solo otro caso particular de lo construido anteriormente.