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 múltiplo de n y viceversa
- Si n y m son primos entre sí entonces $\exists\, x, y : nx + my = 1$ (Bezóuts identity)

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

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

Si $n < m$:

$$\cancel{a^n}(a^{m-n} - 1) = \cancel{b^n}(b^{m-n} - 1)$$
$$a^{m-n} \cancel{-1} = b^{m-n} \cancel{-1}$$
$$a^{m-n} = b^{m-n}$$
$$(a^{m-n})^{x-y} = (b^{m-n})^{x-y}$$

$\exists\, x, y$

$$a^{mx - nx - my + ny} = b^{mx - nx - my + ny}$$
$$(a^{-nx - my})\, a^{mx + ny} = (b^{-nx - my})\, b^{mx + ny}$$

$$(a^{-nx-my})\, a^{mx+ny} = (b^{-nx-my})\, b^{mx+ny}$$

$$(a^{nx+my})^{-1}\, a^{mx+ny} = (b^{nx+my})^{-1}\, b^{mx+ny}$$

$$(a^{1})^{-1}\, a^{mx+ny} = (b^{1})^{-1}\, b^{mx+ny}$$

$$a^{-1}\, a^{mx+ny} = b^{-1}\, b^{mx+ny}$$

$$a^{mx}\, a^{ny} = a\, b^{-1}\, b^{my}\, b^{ny}$$

$$\frac{a^{my}\, a^{ny}}{b^{my}\, b^{ny}} = a\, b^{-1}$$

1 1

$$1 = a b^{-1}$$

$$b = a(b^{-1} b)$$

$$b = a \quad \blacksquare$$

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 $c_n a$, 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.

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

luego podemos crear un subanillo de A $\langle a \rangle$ y por qué no otro $\langle b \rangle$ con el requisito $\langle a \rangle \subseteq \langle b \rangle$, naturalmente

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

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 $\pi \mid p \therefore \exists\, \pi_* \text{ t.q. } p = \pi\pi_*$

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

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:

① $a \mid (a^2 + b^2)$

$bb = an \not\Rightarrow a = b$ ó $b = m$

ej: $4 \cdot 4 = 8 \cdot 2$

Suponga que $a \mid (a^2+b^2)$, $aK = (a^2 + b^2)$

$$k = \frac{a^2}{a} + \frac{b^2}{a}$$

$$K = a + \frac{b^2}{a}$$

Pero k es entero por lo que es necesario $a \mid b^2$, $am = b^2$ retomando (2):

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

$$= \frac{c\, a(a+m)}{a}$$

$$= c\,(a+m)$$

para que p siga siendo primo o c es ± 1 o $(a+m)$ es ± 1.

ⓐ Considere $c = \pm 1$

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

$$p = \frac{a^2c}{a} + \frac{b^2c}{a} = \frac{c(a^2+b^2)}{a} = \frac{\cancel{a}K(a^2+b^2)}{\cancel{a}}$$

$$p = K(a^2+b^2) = Kq, \quad q = (a^2+b^2)$$

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 $\pi_y = \overline{\pi}$.

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

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

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 $p = \pi\overline{\pi}$

$= (a+bi)(a-bi)$

$= a^2+b^2$

No sé como seguir ¿(:)?

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.*]

$\pi = a + bi$, $\|\pi\| > 1$

$\pi\overline{\pi} = a^2 + b^2$

$k = c_1 \cdots c_n$

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* $|(u+iv) - (m+in)| \leq 1/\sqrt{2}$.]