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 comutativo 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)

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

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

Si $n < m$:

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

$\exists x, y$

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

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

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

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

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

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

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

$1 \qquad 1$

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

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

$$b = a \quad \blacksquare$$

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:

Caso 1) a es cero o es una unidad.
(Busco llegar a un absurdo en cada caso)

- si a no es cero por hipótesis
- Si a es una unidad,

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

¿Que procede aquí?

Caso 2) a, se puede factorizar a irreducibles.
(esto porque todo PID es UFD).
$a = c_1 \cdots c_n$, donde c_i es irreducible.

luego $\langle a \rangle = aR = \{ax : x \in A\}$

$$= \{c_1 \cdots c_n x : x \in A\}$$

Como A es PID todo sub Anillo es principal entonces considere $\langle c_1 \rangle$.

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

Note que $\langle a \rangle \subseteq \langle c_1 \rangle \subseteq A$
considere entonces $X_{min} = \min\{x : x \in A\}$

$$c_1 X_{min} < c_1 \cdots c_n X_{min}$$

luego $c_1 x_{min} \in \langle c_1 \rangle$, $c_1 x_{min} \notin \langle a \rangle$
entonces $\langle a \rangle \neq \langle c_1 \rangle$ $\langle c_1 \cdots c_n \rangle$ $(\Rightarrow)\langle=)$.

luego a debe ser irreducible

$(\Leftarrow)$ Sea A un PID y $a \in A$, $a \neq 0$, a irreducible (Queremos decir que $\langle a \rangle$ es maximal).

Dado que A es PID todos sus subanillos son principales así:

$\langle a \rangle$ también es un subanillo

$$\langle a \rangle = \{ax : x \in A\}$$

Suponga entonces otro anillo $\langle b \rangle$, $b \in A$ $b \neq 0$, $b \neq 1$.

Caso A)

- $a \nmid b$, como $a \nmid b$ y a es irreducible también tenemos que $b \nmid a$.

Caso B)

- $a \mid b$ entonces $b = aq$, $q \in A$.

$$\langle b \rangle = \langle aq \rangle = \{aqx : x \in A\}$$

$\langle a \rangle = \{ ax : x \in A \}$

$(\subseteq)$: $\langle a \rangle \subseteq \langle b \rangle$

Sea $a_i \in \langle a \rangle$ este es de la forma $a x_i$, $x_i \in A$. Sea $b_i \in \langle b \rangle$
b_i es de la forma $a q x_j$, $x_j \in A$.

¿Como sigo? =C

$(\supseteq)$: $\langle b \rangle \subseteq \langle a \rangle$

$\forall b_i \in \langle b \rangle \ \exists \ a_i \in \langle a \rangle$ t.q.

$$b_i = a_i \,, \ a_i = a x_i \,, \ x_i \in A.$$
$$b = a x_i \,, \ x_i = q x_j \,, \ x_j \in A.$$
$$b = a q x_j \,.$$

luego $\langle a \rangle \subseteq \langle b \rangle$

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* $p \equiv 1$ (mód 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)

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

$$\begin{aligned} p &= (a+bi)(c-di) \\ &= ac - adi + bci + bd \\ &= (ac+bd) + i(bc-ad) \end{aligned}$$

Como p es entero no debe tener parte imaginaria luego

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

Así:

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

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

① $$a \mid (a^2+b^2)$$

$bb = am \Rightarrow a = b$ 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 $a \mid b^2$, $b^2 = am$

$b \cdot b = am$, luego forzosamente $b = a$ ó $b = m$

en cualquier caso concluimos que $a = b$

si $a = b$, por (1) tenemos que

$$d = c$$

entonces:

$$(a + ai)(d - di)$$

$$ad \cancel{- adi + adi} + ad$$

$$p = 2ad$$

Contradicción que surge de asumir $a \mid (a^2+b^2)$ luego $a \nmid (a^2+b^2)$.

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, veq note que debe ser k, luego $c = a$.

Por (2) decimos que

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

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

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

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

en particular decimos que dado p primo G 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.

¿No sé cómo seguir (:) ?

Luego $p = \pi\bar{\pi}$

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

$= a^2+b^2$

b

b) Sea π un primo en los enteros de Gauss. Luego o $\pi\bar{\pi}$ 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.*]

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

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

$k = c_1 \cdots c_n$