

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 $\exists x, y : nx + my = 1$ (Bezout's identity)

$$\begin{array}{l|l} a^n = b^n & a^m = b^m \\ a^n - b^n = 0 & a^m - b^m = 0 \end{array}$$

$$\begin{aligned} a^n - b^n &= a^m - b^m \\ a^n - a^m &= b^n - b^m \end{aligned}$$

Si $n < m$:

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

$$a^{m-n} \cancel{-1} = b^{m-n} \cancel{-1}$$

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

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

$\exists x, y$

$$\begin{aligned} a^{nx - nx - my + ny} &= b^{nx - nx - my + ny} \\ (a^{-nx - my}) a^{nx + ny} &= (b^{-nx - my}) b^{nx + ny} \end{aligned}$$

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

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

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

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

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

$$\overset{1}{\cancel{a^{ny}}} \overset{1}{\cancel{a^{ny}}} = a b^{-1} \overset{1}{\cancel{b^{ny}}} \overset{1}{\cancel{b^{ny}}}$$

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

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

$$b = a \quad \square$$

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 $\langle a \rangle = J$ o $J = A$.

Assume por Absurdo entonces que a es
reducible luego:

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

Caso 1) $\langle a \rangle = \langle C_1 \rangle$, $a = C_1 \cdot \dots \cdot C_n$
donde cada C_i es un factor irreducible.

$$\{ax : x \in A\} = \{C_1 x : x \in A\}$$

$$\{C_1 \cdot \dots \cdot C_n x : x \in A\} = \{C_1 x : x \in A\}$$

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 $C_1 \cdot \dots \cdot C_n$ y C_1 son asociados
(\Rightarrow) ($=$)

Caso 2) $\langle C_1 \rangle = A$, $\langle a \rangle \subseteq \langle C_1 \rangle \subseteq A$
 $a = C_1 \cdot \dots \cdot C_n$
Cada C_i es irreducible.

$$A = \langle C_1 \rangle = \{C_1 x : x \in A\}$$

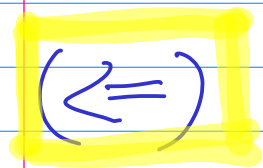
$$\langle a \rangle = \{ax : x \in A\} = \{C_1 \cdot \dots \cdot C_n x : x \in A\}$$

Porque $A = \langle C_1 \rangle = \{C_1^2 \cdot C_2 \cdot \dots \cdot C_n x : x \in A\}$

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

Así a es asociado de $c_1 a$, más claramente $c_1 \dots c_n$ es asociado de $c_1^2 \cdot c_2 \dots c_n$. ($\Rightarrow \Leftarrow$)

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



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

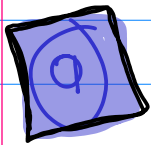
$$\langle a \rangle \subseteq \langle b \rangle \subseteq A.$$



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: $p = \pi \bar{\pi}$;
[Sugerencia: $\pi \mid p \implies \bar{\pi} \mid p$.]
- 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.]

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 $p \equiv 1 \pmod{4}$.



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 gaussianos enteros, cuyas normas sean menores que π)

Suponga 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 \leadsto debe tener parte imaginaria luego

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

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 $a \mid (a^2 + b^2)$

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 $a \mid b^2$, $am = b^2$ retornando (2):

$$\begin{aligned} p &= \frac{a^2c}{a} + \frac{b^2c}{a} = \frac{c(a^2 + b^2)}{a} \\ &= \frac{c \cdot a(a + m)}{a} \\ &= c(a + m) \end{aligned}$$

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

② Considere $c = \pm 1$

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

$$\begin{aligned} p &= \frac{a^2c}{a} + \frac{b^2c}{a} = \frac{c(a^2 + b^2)}{a} = \cancel{aK(a^2 + b^2)} \\ p &= K(a^2 + b^2) = Kq, \quad q = (a^2 + b^2) \end{aligned}$$

$b^2 = am$
 $\Rightarrow a = b = m$
 ej: $4 \cdot 4 = 0 \cdot 2$

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

Por (2) decimos que

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

En particular $\pi \bar{\pi} = p$.

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

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

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

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

(2.1) Note que por $p < \infty$ $p = \pm 2 + 0i$
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

No se
cómo seguir
¿?

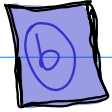
norma menor a ρ .

luego

$$\rho = \pi \bar{\pi}$$

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

$$= a^2 + b^2$$



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

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

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

$$k = c_1 \cdots c_n$$

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

[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 geoméricamente, encuentre $m, n \in \mathbb{Z}$ tales que $|(u + iv) - (m + in)| \leq 1/\sqrt{2}$.]