Algebra Abstracta: Tarea #4

Jonathan Andrés Niño Cortés

23 de febrero de 2015

Sección 8.2 5. Sea R el anillo de enteros cuadráticos $\mathbb{Z}[\sqrt{-5}]$. Defina los ideales $I_2 = (2, 1+\sqrt{-5}), I_3 = (3, 2+\sqrt{-5})$, e $I_3' = (3, 2-\sqrt{-5})$.

(a) Pruebe que I_2, I_3 e I_3', son ideales no principales en R.

Demostración. Vamos a seguir la misma estrategia propuesta en el libro. Tomamos la norma $N(a+b\sqrt{-5}) = a^2 + 5b^2$.

- I_2: Supongamos por contradicción que I_2 es principal. Entonces existiria $a, b \in \mathbb{Z}$ tales que $I_2 = (a + b\sqrt{-5})$. Pero además existirian $\alpha, \beta \in \mathbb{R}$ tales que $2 = \alpha(a+b\sqrt{-5})$ y $1+\sqrt{-5} = \beta(a+b\sqrt{-5})$. Sacando normas en la primera ecuación obtenemos $4 = N(\alpha)N(a+b\sqrt{-5})$. Entonces $N(a+b\sqrt{-5})$ puede ser 1, 2, 4. Si fuera 4, los únicos elementos de norma 4 son ± 2 y no dividen a $1+\sqrt{-5}$ porque no divide a sus coeficientes enteros. No puede ser 2 porque no hay ningun elemento de norma 2. Y si fuera 1 entonces $a + b\sqrt{-5} = \pm 1$ sería todo R. Esto implicaria que existen γ y δ tales que $1 = 2\gamma + (1+\sqrt{-5})\delta$. Multiplicando a ambos lados por $(1-\sqrt{-5})$ obtenemos que $1+\sqrt{-5} = 2(1-\sqrt{-5})\gamma + 6\delta$, es decir que $1+\sqrt{-5}$ es divisible por 2. Claramente una contradicción.
- I_3. Sean $a, b\alpha, \beta, \gamma$ y δ análogos al caso anterior.
  Entonces tenemos que $9 = N(\alpha)N(a+b\sqrt{-1})$. Si $N(a+b\sqrt{-1}) = 9$ entonces $N(\alpha) = 1$ lo que implica que $\alpha = \pm 1$ y por lo tanto $a+b\sqrt{-1} = \pm 3$. Sin embargo, este no puede ser el caso porque $2+\sqrt{-5}$ no es divisible por 3. $N(a+b\sqrt{-5}$ no puede ser 3 porque ningun elemento en el anillo tiene norma 3. Por ultimo si $N(a+b\sqrt{-5} = 1$ entonces $a + b\sqrt{-5} = \pm 1$. Entonces, de nuevo tenemos que $1 = 3\gamma + (2+\sqrt{-5})\delta$, multiplicando por $2-\sqrt{-5}$ tendriamos que $2-\sqrt{-5} = 3(2-\sqrt{-5})\gamma + 9\delta$ y concluiriamos que $2-\sqrt{-5}$ sería divisible por 3 lo cual es falso.
- I_3': Similar al caso anterior.
  $9 = N(\alpha)N(a+b\sqrt{-1})$. Si $N(a+b\sqrt{-1}) = 9$ entonces $N(\alpha) = 1$ lo que implica que $\alpha = \pm 1$ y por lo tanto $a+b\sqrt{-1} = \pm 3$. Sin embargo, este no puede ser el caso porque $2-\sqrt{-5}$ no es divisible por 3. $N(a+b\sqrt{-5}$ no puede ser 3 porque

ningun elemento en el anillo tiene norma 3. Por ultimo si $N(a+b\sqrt{-5}=1$ entonces $a+b\sqrt{-5}=\pm 1$. Entonces, de nuevo tenemos que $1=3\gamma+(2-\sqrt{-5})\delta$, multiplicando por $2+\sqrt{-5}$ tendriamos que $2+\sqrt{-5}=3(2+\sqrt{-5})\gamma+9\delta$ y concluiriamos que $2+\sqrt{-5}$ sería divisible por 3 lo cual es falso.

□

(b) Pruebe que el producto de dos ideales no principales puede ser principal mostrando que I_2^2 es el ideal principal generado por 2, i.e., $I_2^2=(2)$.

Demostración. Probemos por doble contenencia.

Tome un elemento en $x\in I_2^2$. Por definición,

$$\begin{aligned}
x &= \sum_{i=0}^{n}(2\alpha_i+\beta_i(1+\sqrt{-5}))(2\delta_i+\gamma_i(1+\sqrt{-5})).\\
x &= \sum_{i=0}^{n}(4\alpha_i\delta_i+2\delta_i\beta_i(1+\sqrt{-5})+2\alpha\gamma_i(1+\sqrt{-5})+\beta_i\gamma(1+\sqrt{-5})^2).\\
x &= \sum_{i=0}^{n}(4\alpha_i\delta_i+2\delta_i\beta_i(1+\sqrt{-5})+2\alpha\gamma_i(1+\sqrt{-5})+\beta_i\gamma(-4+2\sqrt{-5})).\\
x &= 2\sum_{i=0}^{n}(2\alpha_i\delta_i+\delta_i\beta_i(1+\sqrt{-5})+\alpha\gamma_i(1+\sqrt{-5})+\beta_i\gamma(-2+\sqrt{-5})).
\end{aligned}$$

Por lo tanto vemos que x es divisible por 2. Luego $x\in(2)$ y $I_2^2\in(2)$.

Para la contenencia contraria nótese que $(1+\sqrt{-5})(2-(1+\sqrt{(-5)}))=2+2\sqrt{-5}+4-2\sqrt{-5}-2*2=6-2*2=2$. Luego $2\in I_2^2$ y por lo tanto $(2)\subseteq I_2^2$. □

(c) Pruebe similarmente que $I_2I_3=(1-\sqrt{-5})$ y que $I_2I_3'=(1+\sqrt{-5})$ son principales. Concluya que el ideal principal (6) es el producto de 4 ideales. $(6)=I_2^2I_3I_3'$.

Demostración. I_2I_3 : Tome $x\in I_2I_3$. Luego

$$\begin{aligned}
x &= \sum_{i=0}^{n}(2\alpha_i+\beta_i(1+\sqrt{-5}))(3\delta_i+\gamma_i(2+\sqrt{-5})).\\
x &= \sum_{i=0}^{n}(6\alpha_i\delta_i+3\delta_i\beta_i(1+\sqrt{-5})+2\alpha\gamma_i(2+\sqrt{-5})+\beta_i\gamma(1+\sqrt{-5})(2+\sqrt{-5})).\\
x &= \sum_{i=0}^{n}(6\alpha_i\delta_i+\delta_i\beta_i(3+3\sqrt{-5})+\alpha\gamma_i(4+2\sqrt{-5})+\beta_i\gamma(-3+3\sqrt{-5})).
\end{aligned}$$

Ahora obsérvese que $6, 3+3\sqrt{-5}, 4+2\sqrt{-5}, -3+3\sqrt{-5}$ son todos divisibles por $1-\sqrt{-5}$.

$$\begin{aligned} 6 &= (1+\sqrt{-5})(1-\sqrt{-5}) \\ 3+3\sqrt{-5} &= (-2+\sqrt{-5})(1-\sqrt{-5}) \\ 4+2\sqrt{-5} &= (-1+\sqrt{-5})(1-\sqrt{-5}) \\ -3+3\sqrt{-5} &= -3(1-\sqrt{-5}) \end{aligned}$$

Por lo tanto, concluimos que $x \in (1-\sqrt{-5})$. Es decir, $I_2 I_3 \subseteq (1-\sqrt{5})$.

Para la conversa nótese que $1-\sqrt{5} = -3-3\sqrt{-5}+4+2\sqrt{-5} = (1+\sqrt{-5})(-3)+2(2+\sqrt{-5})$. Por lo tanto, $1-\sqrt{5} \in (I_2 I_3)$. Luego $(1-\sqrt{5}) \subseteq I_2 I_3$.

$I_2 I_3'$: Muy similar a la anterior.

Tome $x \in I_2 I_3'$. Luego

$$\begin{aligned} x &= \sum_{i=0}^{n} (2\alpha_i + \beta_i(1+\sqrt{-5}))(3\delta_i + \gamma_i(2-\sqrt{-5})). \\ x &= \sum_{i=0}^{n} (6\alpha_i\delta_i + 3\delta_i\beta_i(1+\sqrt{-5}) + 2\alpha\gamma_i(2-\sqrt{-5}) + \beta_i\gamma(1+\sqrt{-5})(2-\sqrt{-5})). \\ x &= \sum_{i=0}^{n} (6\alpha_i\delta_i + \delta_i\beta_i(3+3\sqrt{-5}) + \alpha\gamma_i(4-2\sqrt{-5}) + \beta_i\gamma(7-\sqrt{-5})). \end{aligned}$$

Ahora obsérvese que $6, 3+3\sqrt{-5}, 4-2\sqrt{-5}, 7+\sqrt{-5}$ son todos divisibles por $1+\sqrt{-5}$.

$$\begin{aligned} 6 &= (1-\sqrt{-5})(1+\sqrt{-5}) \\ 3+3\sqrt{-5} &= 3(1+\sqrt{-5}) \\ 4-2\sqrt{-5} &= (-1-\sqrt{-5})(1+\sqrt{-5}) \\ 7+\sqrt{-5} &= (2-\sqrt{-5})(1+\sqrt{-5}) \end{aligned}$$

Por lo tanto, concluimos que $x \in (1+\sqrt{-5})$. Es decir, $I_2 I_3' \subseteq (1+\sqrt{5})$.

Para la conversa nótese que $1+\sqrt{5} = 7+\sqrt{-5}-6 = (1+\sqrt{-5})(2-\sqrt{-5})+2*3$. Por lo tanto, $1+\sqrt{5} \in (I_2 I_3')$. Luego $(1+\sqrt{5}) \subseteq I_2 I_3'$.

Concluimos que $I_2^2 I_3 I_3' = I_2 I_3 I_2 I_3' = (1-\sqrt{5})(1+\sqrt{5}) = (6)$. Esto ultimo es igual a (6) por un lema demostrado en una tarea anterior.

□

Sección 8.2 6. Sea R un dominio integral y suponga que cualquier primo ideal en R es principal. Este ejercicio prueba que cualquier ideal de R es principal, i.e., es un D.I.P.

(a) Asuma que el conjunto de ideales de R que no son principales es no vacío y pruebe que el conjunto tiene un elemento máximal bajo la inclusión (que, por hipótesis no es primo)[Use el Lema de Zorn].

Demostración. Sea P dicho conjunto. Para usar el lema de Zorn debemos asumir que P no es vacío y probar que cualquier cadena de ideales en P esta acotada por encima por algún ideal también en P. Sea T una cadena, es decir, una colección de subconjuntos linealmente ordenados por contenencia. Entonces el ideal $I = \bigcup_{J \in T} J$ es una cota superior de T contenida en P.

Para probar que es un ideal tomese cualesquiera dos elementos $a, b \in I$. Entonces existen ideales $A, B \in T$ tales que $a \in A$ y $b \in B$ pero además como T esta linealmente ordenado, o $A \subseteq B$ o $B \subseteq A$. En el primer caso, entonces $a \in B$, por lo que $a - b$ y $ra \in B \subseteq J$ para cualquier $r \in R$. En el segundo caso entonces $b \in A$ y por lo tanto $a - b$ y $rb \in A \subseteq J$ lo que muestra que I es un ideal.

Lo segundo es que $I \in P$. Supongase por contradicción que es principal y sea α tal que $I = (\alpha)$. Tenemos que $\alpha \in I$, por lo que existe algún $J \in T$ tal que $\alpha \in J$. Pero esto significa que $(\alpha) \subseteq J$. Pero además se cumple que $J \subseteq I$, luego $J = I = (\alpha)$ y J sería un ideal principal. Contradicción.

Por ultimo I es una cota superior por para todo J esta contenido en la unión de todos los $J \in T$, es decir, I. Entonces por el Lema de Zorn, P tiene al menos un elemento máximal. □

(b) Sea I un ideal que es máximal con respecto a ser no principal, y sea $a, b \in R$ con $ab \in I$ pero $a \notin I$ y $b \notin I$. Sea $I_a = (I, a)$ el ideal generado por I y a, sea $I_b = (I, b)$ el ideal generado por I y b, y defina $J = \{r \in R | rI_a \subseteq I\}$. Pruebe que $I_a = (\alpha)$ y $J = (\beta)$ son ideales principales en R con $I \subsetneq I_b \subseteq J$ y que $I_a J = (\alpha\beta) \subseteq I$.

Demostración. Por nuestras suposiciones I_α es un ideal que contiene propiamente a I pues el generado por I y un elemento que no esta en I pero como I es máximal concluimos que I_α debe ser principal. I_β también es principal por la misma razón.

Para demostrar que J es un ideal tomemos $c, d \in J$, y tomemos $x \in (d-c)I_a$. Entonces $x = (d-c)e$ con $e \in I_a$. Pero $x = ce - de$ y vemos que ce y $de \in I$. Por lo tanto, como I es cerrado bajo resta $x = cd - bd \in I$. Por lo tanto J también es cerrado bajo resta. Por una demostración similar podemos mostrar que $rj \in J$ con $r \in R$ y $j \in J$. Luego J es un ideal. Además tenemos que $I \subseteq J$, pues si tomamos $i \in I$ entonces $iI_j \subseteq I$ es trivial porque I es un ideal. Pero la contenencia es estricta pues $b \in J$ y $b \notin I$ por nuestra suposición. En efecto tomemos bI_a, y tomemos cualquier elemento $x \in bI_a$. Entonces $x = b(i + ra)$, con $i \in I$, y $r \in R$. Esto también muestra que $I_b \in J$. Por

lo tanto, $x = ib + rab$ pertenece a I porque i y ab estan en I. Luego J también es un ideal principal porque si no lo fuera contradeciría la maximalidad de I.

Por ultimo, probemos que $(\alpha\beta) \subseteq I$. En efecto, $\beta \in J$ luego tenemos que $\beta I_a \subseteq I$ y $\alpha \in I_a$ por lo que $\beta\alpha \in I$. □

(c) Si $x \in I$ muestre que $x = s\alpha$ para algún $s \in J$. Deduzca que $I = I_a J$ es principal, una contradicción, y concluya que R es un D.I.P.

Demostración. Sabemos que $I \subseteq I_a$, por lo tanto $x = s\alpha$ para algún $s \in R$. Pero además, si tomamos sI_a tenemos que $sI_a \subseteq I$. Para probar esto tome $y \in sI_a$, es decir que $y = sr\alpha$ para algún $r \in R$. Luego $y = s\alpha r = xr$ y claramente $xr \in I$. Esto demuestra que $s \in J$. Con esto concluimos que $x \in I_a J$ por lo que $I \subseteq I_a J$. Esto y lo demostrado en el punto anterior implican que $I = I_a J$ pero vimos que $I_a J = (\alpha\beta)$, es decir que I es un ideal principal por lo que llegamos a una contradicción pues I era máximal de los ideales no principales. Nuestra suposición inicial fue que el conjunto de ideales no principales era no vacío, por lo tanto concluimos que este conjunto es vacío, es decir que R es un D.I.P. □

Sección 8.2 8. Pruebe que si R es un Dominio de ideales principales y que D es un subconjunto multiplicativo cerrrado de R, entonces $D^{-1}R$ es también un P.I.D.

Demostración. Sea I un ideal de $D^{-1}R$. Tenemos que en $D^{-1}R$ hay contenida una copia isomorfa de R, sea R' dicha copia. Entonces tomemos la intersección $I \cap R'$. En primer lugar, $I \cap R'$ nunca es vacío porque para cualquier $d^{-1}i \in I$, con $d \in D$ e $i \in R'$ tenemos que $dd^{-1}i = i \in I$.

Vamos a demostrar que $I = D^{-1}(I \cap R')$. Es claro que $I \subseteq D^{-1}(I \cap R')$, pues cualquier $x \in I$ es igual a $d^{-1}r'$ con $d \in D$ y $r' \in R'$. Para demostrar que $r' \in I$, tomamos $dd^{-1}r' = r' \in I$. Para la conversa tómese cualquier $x \in D^{-1}(I \cap R')$ este es de la forma $x = d^{-1}i$ con $d \in D$ e $i \in I \cap R'$ y claramente x pertenece a I porque $i \in I$ y cualquier producto con un elemento del anillo $d^{-1}i$ está en el ideal.

Ahora queremos ver que $I \cap R'$ es ideal en R'. Tomemos cualquiera dos elementos $a, b \in I \cap R'$. Por un lado, $a - b \in I \cap R'$ porque tanto I como R' son cerrados bajo resta. Por otro lado, si tomamos $r'a$ con $r' \in R'$, vemos que también pertenece a $I \cap R'$ porque tanto el uno como el otro son cerrados para multiplicación de elementos de R'.

Ahora por nuestra suposición R' es un D.I.P. Por lo tanto, existe $\alpha \in R'$ tal que $I \cap R' = (\alpha)$ como ideal de R'. Ahora veamos que $I = (\alpha)$. Por un lado, tenemos que $\alpha \in (I \cap R') \subseteq I$. por lo que $(\alpha) \subseteq I$. Pero además tenemos que $I = D^{-1}(I \cap R')$, es decir que cualquier $i \in I$ es de la forma $d^{-1}r'\alpha$ por lo que $x \in (\alpha)$. Concluimos que $(\alpha) = I$ y como esto fue para cualquier ideal de $D^{-1}R$ concluimos que $D^{-1}R$ es un dominio de ideales principales. Cabe mencionar que si R es un dominio integral entonces $D^{-1}R$ también lo es. Con esto concluimos la demostración. □

Sección 8.3 4. Pruebe que si un entero es la suma de dos cuadrados racionales, entonces esta en la suma de dos cuadrados enteros (por ejemplo, $13 = (1/5)^2 + (18/5)^2 = (2^2 + 3^2)$.

Demostración. Sea n suma del cuadrado de dos racionales. Entonces existen $a, b, d \in \mathbb{Z}$ tales que

$$n = \frac{a^2 + b^2}{d^2}$$

Por lo tanto,

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

Por el teorema fundamental de la aritmética, $nd^2 = 2^k p_1^{\alpha_1} \cdots p_n^{\alpha_n} q_1^{\beta_1} \cdots q_m^{\beta_m}$ donde $p_i \equiv 3 \pmod 4$ y $q_i \equiv 1 \pmod 4$ y $\alpha_1 \cdots \alpha_n \beta_1 \cdots \beta_m \neq 0$. Además por el Corolario 19 de la sección 8.3 tenemos que todo B_i es par.

Además n y d también tienen factorización única en primos. De hecho tenemos que $n = 2^l p_1^{\gamma_1} \cdots p_n^{\gamma_n} q_1^{\delta_1} \cdots q_m^{\delta_m}$ y $d = 2^j p_1^{\epsilon_1} \cdots p_n^{\epsilon_n} q_1^{\omega_1} \cdots q_m^{\omega_m}$ y se debe cumplir que $k = l + 2j$, $\alpha_i = \gamma_i + 2\epsilon_i$ y $\beta_r = \delta_r + 2\omega_r$.

En particular, si reducimos la ultima ecuación módulo 2, obtenemos

$$\beta_r = \delta_r (\text{mod} 2).$$

Entonces como β es par δ también es par. Luego n es igual a una suma de cuadrados en $\mathbb{Z}$.

□

Sección 8.3 7. Sea π un elemento irreducible en $\mathbb{Z}[i]$.

(a) Para cualquier entero $n \geq 0$, pruebe que $(\pi^{n+1}) = \pi^{n+1}\mathbb{Z}[i]$ es un ideal en $(\pi^n) = \pi^n\mathbb{Z}[i]$ y que la multiplicación por π^n induce un isomorfismo $\mathbb{Z}[i]/(\pi) \cong (\pi^n)/(\pi^{n+1})$ como grupos abelianos aditivos.

Demostración. Primero obsérvese que $\pi^{n+1} \in (\pi^n)$ pues $\pi^{n+1} = \pi\pi^n$ es un múltiplo de π^n por lo que $(\pi^{n+1}) \subseteq (\pi^n)$. Ahora para probar que es un ideal de (π^n), ya tenemos que es un grupo aditivo porque es un ideal. Solo basta demostrar que para cualquier $x \in (\pi^n)$, $y \in (\pi^{n+1})$, $xy \in (\pi^{n+1})$. Y este es el caso porque $xy = r\pi^n r'\pi^{n+1}$ es un múltiplo de π^{n+1}.

Ahora, para demostrar que $\mathbb{Z}[i]/(\pi) \cong (\pi^n)/(\pi^{n+1})$, como grupos abelianos aditivos, primero obsérvese que $\mathbb{Z}[i] \cong (\pi^n)$ y que el isomorfismo es precisamente multiplicación por π^n. Además $(\pi) \cong (\pi^{n+1})$ y el isomorfismo es de nuevo multiplicación por π^n. Podemos tomar el homomorfismo sobreyectivo de $\mathbb{Z}[i]$ a $(\pi^n)/(\pi^{n+1})$, composición de la multiplicación por π^n con la proyección natural de (π^n). El kernel de la proyección es (π^{n+1}) luego el kernel de la proyección son aquellos que son mapeados a (π^{n+1}), es decir, (π). Luego por el primer teorema del isomorfismo de grupos $\mathbb{Z}[i]/(\pi) \cong (\pi^n)/(\pi^{n+1})$.

Por lo tanto, $\mathbb{Z}[i]/(\pi) \cong (\pi^n)/(\pi^{n+1})$ y el isomorfismo es multiplicación por π^n. □

(b) Pruebe que $|\mathbb{Z}[i]/(\pi^n)| = |\mathbb{Z}[i]/(\pi)|^n$.

Demostración. Vamos a demostrarlo por inducción. El caso base cuando $n = 1$ es trivial. Ahora para el paso inductivo suponga que $|\mathbb{Z}[i]/(\pi^n)| = |\mathbb{Z}[i]/(\pi)|^n$ y tomemos $\mathbb{Z}[i]/(\pi^{n+1})$. Por el tercer teorema del isomorfismo de grupos tenemos que $\mathbb{Z}[i]/(\pi^n) \cong (\mathbb{Z}[i]/(\pi^{n+1}))/((\pi^n)/(\pi^{n+1}))$ y por el punto anterior tenemos que

$$\mathbb{Z}[i]/(\pi^n) \cong (\mathbb{Z}[i]/(\pi^{n+1}))/(\mathbb{Z}[i]/(\pi))$$

Finalmente utilizando el teorema de Lagrange concluimos que

$$|\mathbb{Z}[i]/(\pi^n)| = |(\mathbb{Z}[i]/(\pi^{n+1}))|/|(\mathbb{Z}[i]/(\pi))|$$

y utilizando la hipótesis de inducción llegamos al resultado deseado.

$$\begin{aligned} |\mathbb{Z}[i]/(\pi^n)||(\mathbb{Z}[i]/(\pi))| &= |(\mathbb{Z}[i]/(\pi^{n+1}))| \\ |\mathbb{Z}[i]/(\pi)|^n|(\mathbb{Z}[i]/(\pi))| &= |(\mathbb{Z}[i]/(\pi^{n+1}))| \\ |\mathbb{Z}[i]/(\pi)|^{n+1} &= |(\mathbb{Z}[i]/(\pi^{n+1}))| \end{aligned}$$

□

(c) Pruebe para cualquier α diferente de cero en $\mathbb{Z}[i]$ que el anillo conciente $\mathbb{Z}[i]/(\alpha)$ tiene orden igual a $N(\alpha)$.

Demostración. Si α es una unidad entonces $\mathbb{Z}[i]/(\alpha) = \mathbb{Z}[i]/\mathbb{Z}[i] \cong \{0\}$. Luego $|\mathbb{Z}[i]/(\alpha)| = 1 = N(\alpha)$.

Primero demostremos que esto se cumple para los elementos irreducibles de $\mathbb{Z}[i]$. Los irreducibles de $\mathbb{Z}[i]$ son o bien los p, primos en $\mathbb{Z}$ que son congruentes a 3 módulo 4, o bien los elementos los elementos π tales que $\pi\overline{\pi} = p.$, donde p es congruente a 2 o a 1 módulo 4.

Ambos casos se demuestran en el ejercicio anterior. En el primer caso tenemos que $|\mathbb{Z}/(p)| = p^2 = p\overline{p} = N(p)$. En el segundo caso tenemos que $\mathbb{Z}/(\pi) = p = \pi\overline{\pi} = N(\pi)$.

Ahora consideremos los α igual a una potencia de un irreducible, π^n. Por el punto anterior $|\mathbb{Z}[i](\pi^n)| = |\mathbb{Z}[i](\pi)|^n = N(\pi)^n = N(\pi^n)$ donde la ultima equivalencia es cierta porque la norma es multiplicativa.

Finalmente si tomamos cualquier α que no sea unidad, entonces tiene un descomposición única en irreducibles porque R en un D.F.U. Entonces sea $\alpha = \pi_1^{\alpha_1} \cdots \pi_n^{\alpha_n}$, con π_i irreducible y $\alpha_1 \cdots \alpha_n \neq 0$. Ahora obsérvese que $(\pi_{i_i}^{\alpha})$ y $(\pi_j^{\alpha_j})$ son comáximales para $i \neq j$. En efecto, $(\pi_i^{\alpha_i}, \pi_j^{\alpha_j}) = (d)$ pues estamos en un dominio euclideano y d sería el máximo común divisor de $\pi_{i_i}^{\alpha}$ y $\pi_j^{\alpha_j}$. Pero como son potencias de elementos irreducibles diferente el máximo común divisor sería una unidad. Luego $(\pi_i^{\alpha_i}, \pi_j^{\alpha_j}) = (1) = \mathbb{Z}[i]$. Por lo tanto podemos utilizar el teorema chino del residuo para concluir que $\mathbb{Z}[i]/(\alpha) = \mathbb{Z}[i]/(\pi_1^{\alpha_1}) \times \cdots \times \mathbb{Z}[i]/(\pi_n^{\alpha_n})$. Y entonces $|\mathbb{Z}[i]/(\alpha)| = |\mathbb{Z}[i]/(\pi_1^{\alpha_1})| \cdots |\mathbb{Z}[i]/(\pi_n^{\alpha_n})| = N(\pi_1^{\alpha_1}) \cdots N(\pi_n^{\alpha_n}) = N(\alpha)$.

□

Sección 8.3 11. *Caracterización de P.I.D.s*) Pruebe que R es un D.I.P si y solo si R es un D.F.U que también es un Dominio de Bezout.

Demostración. Una dirección esta dada porque un D.I.P. implica un D.F.U. Para la otra dirección tome un ideal I y tome un elemento $a \in I$ diferente de 0, con un mínimo número de factores irreducibles. Ahora supongase que existe un $b \in I$ tal que $b \notin (a)$. Entonces como estamos en un dominio de Bezout sabemos que existe $d \in R$ tal que $(a, b) = (d)$. En primer lugar obsérvese que $(a, b) \in I$, pues ambos elementos pertenecen a I, por lo tanto $d \in I$. Pero además $d|b$ y $d|a$, (de hecho d es el máximo común divisor de a, b por un punto de la sección anterior), entonces los factores irreducibles de d debe ser un subconjunto de los factores que dividen a a y a b. Pero como b no es un múltiplo de a debe existir algún elemento irreducible π que divide a a pero no divide b. Concluimos que π no es un factor de d, es decir, el número de factores irreducibles de d es menor al número de factores irreducibles de a, una contradicción. □