Álgebra II Práctica (clase 20)

Iván Sadofschi Costa

Universidad de Buenos Aires

03 de Julio de 2020

Ideales primos en un DIP

Definición

Sea R un anillo conmutativo. Un ideal $I \lhd R$ se dice primo *si R/I es íntegro. Equivalentemente, I es primo si vale que $ab \in I \Rightarrow (a \in I \text{ o } b \in I)$. Un elemento $p \in R$ se dice* primo *si (p) es un ideal primo. Equivalentemente, p es primo si $p \mid ab \Rightarrow (p \mid a \text{ o } p \mid b)$.*

Ideales primos en un DIP

Definición

Sea R un anillo conmutativo. Un ideal $I \triangleleft R$ se dice primo *si R/I es íntegro. Equivalentemente, I es primo si vale que $ab \in I \Rightarrow (a \in I \text{ o } b \in I)$. Un elemento $p \in R$ se dice* primo *si (p) es un ideal primo. Equivalentemente, p es primo si $p \mid ab \Rightarrow (p \mid a \text{ o } p \mid b)$.*

Ojo, con esta definición si R es un dominio íntegro entonces 0 y 1 son primos.

Ideales primos en un DIP

Definición

Sea R un anillo conmutativo. Un ideal $I \triangleleft R$ se dice primo si R/I es íntegro. Equivalentemente, I es primo si vale que $ab \in I \Rightarrow (a \in I \text{ o } b \in I)$. Un elemento $p \in R$ se dice primo si (p) es un ideal primo. Equivalentemente, p es primo si $p \mid ab \Rightarrow (p \mid a \text{ o } p \mid b)$.

Ojo, con esta definición si R es un dominio íntegro entonces 0 y 1 son primos.

Proposición

Sean R un dominio íntegro y $p \in R$ primo. Entonces p es irreducible.

Ideales primos en un DIP

Definición

Sea R un anillo conmutativo. Un ideal $I \triangleleft R$ se dice primo *si R/I es íntegro. Equivalentemente, I es primo si vale que $ab \in I \Rightarrow (a \in I \text{ o } b \in I)$.*
Un elemento $p \in R$ se dice primo *si (p) es un ideal primo.*
Equivalentemente, p es primo si $p \mid ab \Rightarrow (p \mid a \text{ o } p \mid b)$.

Ojo, con esta definición si R es un dominio íntegro entonces 0 y 1 son primos.

Proposición

Sean R un dominio íntegro y $p \in R$ primo. Entonces p es irreducible.

En un DIP primo es lo mismo que irreducible.

Ideales primos en un DIP (cont)

Proposición

Sean R un DIP. y $P \lhd R$ primo. Entonces P es maximal.

Ideales primos en un DIP (cont)

Proposición

Sean R un DIP. y $P \lhd R$ primo. Entonces P es maximal.

Demostración.

Sea p tal que $P = (p)$. Supongamos que $P \subsetneq M \subsetneq R$ es un ideal maximal para llegar a un absurdo. Tomemos m tal que $M = (m)$. Como $p \in M$ existe x tal que $p = mx$. Ahora usamos que p es irreducible (por ser primo). Como m genera un ideal maximal m no es una unidad. Pero entonces m es asociado a p y luego $(m) = (p)$ contradicción. $\square$

Enteros de Gauss

Vamos a ver que si A es DFU entonces $A[x]$ es DFU. Notar que no vale lo mismo si reemplazamos DFU por DIP, $\mathbb{Z}[x]$ no es DIP.

Enteros de Gauss

Vamos a ver que si A es DFU entonces $A[x]$ es DFU. Notar que no vale lo mismo si reemplazamos DFU por DIP, $\mathbb{Z}[x]$ no es DIP.

El anillo $\mathbb{Z}[i] = \{a + bi \ : \ a, b \in \mathbb{Z}\} \subset \mathbb{C}$ se llama el anillo de enteros de Gauss.

Enteros de Gauss

Vamos a ver que si A es DFU entonces $A[x]$ es DFU. Notar que no vale lo mismo si reemplazamos DFU por DIP, $\mathbb{Z}[x]$ no es DIP.

El anillo $\mathbb{Z}[i] = \{a + bi \ : \ a, b \in \mathbb{Z}\} \subset \mathbb{C}$ se llama el anillo de enteros de Gauss.

Sea $N\colon \mathbb{Z}[i] \to \mathbb{N}_0$ dada por $N(a + bi) = a^2 + b^2$ (obs: alternativamente podemos definir $N(z) = z\overline{z}$).

Enteros de Gauss

Vamos a ver que si A es DFU entonces $A[x]$ es DFU. Notar que no vale lo mismo si reemplazamos DFU por DIP, $\mathbb{Z}[x]$ no es DIP.

El anillo $\mathbb{Z}[i] = \{a + bi \ : \ a, b \in \mathbb{Z}\} \subset \mathbb{C}$ se llama el anillo de enteros de Gauss.

Sea $N\colon \mathbb{Z}[i] \to \mathbb{N}_0$ dada por $N(a + bi) = a^2 + b^2$ (obs: alternativamente podemos definir $N(z) = z\overline{z}$).

Ejercicio

$\mathbb{Z}[i]$ es un dominio euclídeo con esta norma, o sea que si $a, b \in \mathbb{Z}[i]$ y $b \neq 0$ existen $q, r \in \mathbb{Z}[i]$ tales que
(i) $a = bq + r$ y
(ii) $r = 0$ o $N(r) < N(b)$.

Enteros de Gauss

Vamos a ver que si A es DFU entonces $A[x]$ es DFU. Notar que no vale lo mismo si reemplazamos DFU por DIP, $\mathbb{Z}[x]$ no es DIP.

El anillo $\mathbb{Z}[i] = \{a + bi \ : \ a, b \in \mathbb{Z}\} \subset \mathbb{C}$ se llama el anillo de enteros de Gauss.

Sea $N \colon \mathbb{Z}[i] \to \mathbb{N}_0$ dada por $N(a + bi) = a^2 + b^2$ (obs: alternativamente podemos definir $N(z) = z\overline{z}$).

Ejercicio

$\mathbb{Z}[i]$ es un dominio euclídeo con esta norma, o sea que si $a, b \in \mathbb{Z}[i]$ y $b \neq 0$ existen $q, r \in \mathbb{Z}[i]$ tales que
(i) $a = bq + r$ y
(ii) $r = 0$ o $N(r) < N(b)$.

Pista: Considerar $x = \frac{a}{b}$ y tomar q entero de Gauss “lo más cerca posible” de x.

Enteros de Gauss (cont.)

Se sigue que es un dominio de ideales principales y por lo tanto un DFU.

Se sigue que es un dominio de ideales principales y por lo tanto un DFU.

Lema

Las unidades de $\mathbb{Z}[i]$ *son* $1, -1, i, -i$.

Enteros de Gauss (cont.)

Se sigue que es un dominio de ideales principales y por lo tanto un DFU.

Lema

Las unidades de $\mathbb{Z}[i]$ *son* $1, -1, i, -i$.

Demostración.

Como la norma es multiplicativa ($N(ab) = N(a)N(b)$) las unidades deben tener norma 1. $\square$

Enteros de Gauss (cont.)

Se sigue que es un dominio de ideales principales y por lo tanto un DFU.

Lema

Las unidades de $\mathbb{Z}[i]$ son $1, -1, i, -i$.

Demostración.

Como la norma es multiplicativa ($N(ab) = N(a)N(b)$) las unidades deben tener norma 1. $\square$

Proposición

Si $a + bi \in \mathbb{Z}[i]$ es tal que $N(a + bi) \in \mathbb{Z}$ es primo, entonces $a + bi \in \mathbb{Z}[i]$ es primo.

Enteros de Gauss (cont.)

Se sigue que es un dominio de ideales principales y por lo tanto un DFU.

Lema

Las unidades de $\mathbb{Z}[i]$ *son* $1, -1, i, -i$.

Demostración.

Como la norma es multiplicativa ($N(ab) = N(a)N(b)$) las unidades deben tener norma 1. $\square$

Proposición

Si $a + bi \in \mathbb{Z}[i]$ *es tal que* $N(a + bi) \in \mathbb{Z}$ *es primo, entonces* $a + bi \in \mathbb{Z}[i]$ *es primo.*

Demostración.

Si $(a + bi) = (c + di)(e + fi)$ entonces $N(a + bi) = N(c + di)N(e + fi)$ y luego $N(c + di) = 1$ o $N(e + fi) = 1$. $\square$

Los primos en $\mathbb{Z}[i]$

Claramente $1 + i$ es primo.

Los primos en $\mathbb{Z}[i]$

Claramente $1 + i$ es primo. Pero 2 no es primo: $2 = (1 + i)(1 - i)$.

Los primos en $\mathbb{Z}[i]$

Claramente $1+i$ es primo. Pero 2 no es primo: $2=(1+i)(1-i)$.

Proposición

Sea $p \in \mathbb{N}$ primo. Son equivalentes:
(i) p se reduce en $\mathbb{Z}[i]$.
(ii) Existen $a, b \in \mathbb{Z}$ tales que $p=a^2+b^2$.
(iii) Existe x tal que $x^2 \equiv -1 \pmod{p}$.

Los primos en $\mathbb{Z}[i]$

Claramente $1+i$ es primo. Pero 2 no es primo: $2=(1+i)(1-i)$.

Proposición

Sea $p \in \mathbb{N}$ primo. Son equivalentes:
(i) p se reduce en $\mathbb{Z}[i]$.
(ii) Existen $a, b \in \mathbb{Z}$ tales que $p=a^2+b^2$.
(iii) Existe x tal que $x^2 \equiv -1 \pmod{p}$.

Demostración.

(i)$\Rightarrow$ (ii). Sea $p=(a+bi)(c+di)$ fact. no triv. Entonces $p^2=(a^2+b^2)(c^2+d^2)$. Luego $p=(a^2+b^2)=c^2+d^2$.

$\square$

Los primos en $\mathbb{Z}[i]$

Claramente $1+i$ es primo. Pero 2 no es primo: $2=(1+i)(1-i)$.

Proposición

Sea $p \in \mathbb{N}$ primo. Son equivalentes:
(i) p se reduce en $\mathbb{Z}[i]$.
(ii) Existen $a, b \in \mathbb{Z}$ tales que $p=a^2+b^2$.
(iii) Existe x tal que $x^2 \equiv -1 \pmod{p}$.

Demostración.

(i)$\Rightarrow$ (ii). Sea $p=(a+bi)(c+di)$ fact. no triv. Entonces $p^2=(a^2+b^2)(c^2+d^2)$. Luego $p=(a^2+b^2)=c^2+d^2$.
(ii)$\Rightarrow$ (iii). Si $p=a^2+b^2$, tenemos $a^2+b^2 \equiv 0 \pmod{p} \Rightarrow a^2 \equiv -b^2 \pmod{p}$ luego $(a/b)^2 \equiv -1 \pmod{p}$ (acá b^{-1} es el inverso de b módulo p).

$\square$

Los primos en $\mathbb{Z}[i]$

Claramente $1+i$ es primo. Pero 2 no es primo: $2=(1+i)(1-i)$.

Proposición

Sea $p \in \mathbb{N}$ primo. Son equivalentes:
(i) p se reduce en $\mathbb{Z}[i]$.
(ii) Existen $a, b \in \mathbb{Z}$ tales que $p=a^2+b^2$.
(iii) Existe x tal que $x^2 \equiv -1 \pmod{p}$.

Demostración.

(i)$\Rightarrow$ (ii). Sea $p=(a+bi)(c+di)$ fact. no triv. Entonces $p^2=(a^2+b^2)(c^2+d^2)$. Luego $p=(a^2+b^2)=c^2+d^2$.
(ii)$\Rightarrow$ (iii). Si $p=a^2+b^2$, tenemos $a^2+b^2 \equiv 0 \pmod{p} \Rightarrow a^2 \equiv -b^2 \pmod{p}$ luego $(a/b)^2 \equiv -1 \pmod{p}$ (acá b^{-1} es el inverso de b módulo p).
(iii)$\Rightarrow$ (i). Sea x tal que $x^2 \equiv -1 \pmod{p}$. Entonces $p \mid x^2+1=(x+i)(x-i)$. Luego como $p \nmid x+i$ y $p \nmid x-i$ tenemos que p no es primo en $\mathbb{Z}[i]$. Luego no es irreducible (estamos en un DIP!). $\square$

Los primos en $\mathbb{Z}[i]$

Sea p impar. Notemos que existe $x \in \mathbb{Z}_p$ tal que $x^2 \equiv -1 \pmod{p}$ si y solamente si hay un elemento de orden 4 en $\mathbb{Z}_p^*$.

Los primos en $\mathbb{Z}[i]$

Sea p impar. Notemos que existe $x \in \mathbb{Z}_p$ tal que $x^2 \equiv -1 \pmod{p}$ si y solamente si hay un elemento de orden 4 en $\mathbb{Z}_p^*$. Como $\mathbb{Z}_p^* \simeq \mathbb{Z}_{p-1}$, tenemos que p impar se factoriza en $\mathbb{Z}[i]$ sii $p \equiv 1 \pmod{4}$.

Los primos en $\mathbb{Z}[i]$

Sea p impar. Notemos que existe $x \in \mathbb{Z}_p$ tal que $x^2 \equiv -1 \pmod{p}$ si y solamente si hay un elemento de orden 4 en $\mathbb{Z}_p^*$. Como $\mathbb{Z}_p^* \simeq \mathbb{Z}_{p-1}$, tenemos que p impar se factoriza en $\mathbb{Z}[i]$ sii $p \equiv 1 \pmod{4}$.

Proposición

Un primo $4k+1$ en $\mathbb{Z}$ se factoriza en $\mathbb{Z}[i]$ como producto de dos primos no asociados.

Los primos en $\mathbb{Z}[i]$

Sea p impar. Notemos que existe $x \in \mathbb{Z}_p$ tal que $x^2 \equiv -1 \pmod{p}$ si y solamente si hay un elemento de orden 4 en $\mathbb{Z}_p^*$. Como $\mathbb{Z}_p^* \simeq \mathbb{Z}_{p-1}$, tenemos que p impar se factoriza en $\mathbb{Z}[i]$ sii $p \equiv 1 \pmod{4}$.

Proposición

Un primo $4k+1$ en $\mathbb{Z}$ se factoriza en $\mathbb{Z}[i]$ como producto de dos primos no asociados.

Vimos que el primo 2 se factoriza como producto de dos primos asociados: $2 = (1+i)(1-i)$.

Los primos en $\mathbb{Z}[i]$

Sea p impar. Notemos que existe $x \in \mathbb{Z}_p$ tal que $x^2 \equiv -1 \pmod{p}$ si y solamente si hay un elemento de orden 4 en $\mathbb{Z}_p^*$. Como $\mathbb{Z}_p^* \simeq \mathbb{Z}_{p-1}$, tenemos que p impar se factoriza en $\mathbb{Z}[i]$ sii $p \equiv 1 \pmod{4}$.

Proposición

Un primo $4k+1$ en $\mathbb{Z}$ se factoriza en $\mathbb{Z}[i]$ como producto de dos primos no asociados.

Vimos que el primo 2 se factoriza como producto de dos primos asociados: $2 = (1+i)(1-i)$.

Proposición

Los primos de $\mathbb{Z}[i]$ son:
(i) $\pm p$, $\pm ip$ con $p \in \mathbb{N}$ primo congruente a 3 módulo 4.
(ii) Los $z \in \mathbb{Z}[i]$ tales que $N(z)$ es primo en $\mathbb{Z}$.

Los primos en $\mathbb{Z}[i]$

Sea p impar. Notemos que existe $x \in \mathbb{Z}_p$ tal que $x^2 \equiv -1 \pmod{p}$ si y solamente si hay un elemento de orden 4 en $\mathbb{Z}_p^*$. Como $\mathbb{Z}_p^* \simeq \mathbb{Z}_{p-1}$, tenemos que p impar se factoriza en $\mathbb{Z}[i]$ sii $p \equiv 1 \pmod{4}$.

Proposición

Un primo $4k+1$ en $\mathbb{Z}$ se factoriza en $\mathbb{Z}[i]$ como producto de dos primos no asociados.

Vimos que el primo 2 se factoriza como producto de dos primos asociados: $2 = (1+i)(1-i)$.

Proposición

Los primos de $\mathbb{Z}[i]$ son:
(i) $\pm p$, $\pm ip$ con $p \in \mathbb{N}$ primo congruente a 3 módulo 4.
(ii) Los $z \in \mathbb{Z}[i]$ tales que $N(z)$ es primo en $\mathbb{Z}$.

Demostración.

Estos primos son los primos de $\mathbb{Z}[i]$ que dividen a los primos de $\mathbb{Z}$. Como $p \cdot \overline{p} = N(p)$ y $\mathbb{Z}[i]$ es DFU, todo primo divide a un primo de $\mathbb{Z}$. $\square$