Elementos primos, irreducibles, y asociados

Facultad de Ciencias UNAM

Introducción

En esta sección continuamos generalizando conceptos de divisibilidad en $\mathbb{Z}$. A diferencia de la sección anterior, los conceptos que generalizaremos aquí (por ejemplo, el concepto de numero primo) requieren de la existencia de una unidad y por lo tanto, en esta sección trabajamos en anillos conmutativos con unidad.

Recordemos que decimos que $p \in \mathbb{Z}_{\geq 0}$ es un numero primo si $\forall k \in \mathbb{Z}_{\geq 0} \left(k|p \implies k \in \{1, p\}\right)$. En palabras, los únicos divisores positivos de p son 1 y p.

Es natural intentar usar esta definición para generalizar el concepto de numero primo. Por ejemplo, podríamos decir que $p \in R$ es primo si

$$\forall k \in R \left(k|p \implies k \in \{\pm 1, \pm p\}\right)$$

Esta condición generaliza el concepto de numero primo, pero es demasiado restrictiva. Por ejemplo, si R tuviera un elemento invertible $u \neq \pm 1$, entonces con esta definición, todo elemento $p \notin \{\pm 1, \pm u\}$ no seria primo porque u divide a p: $u\left(u^{-1}p\right) = p$.

Podríamos seguir intentando y usar la siguiente condición.

$$\forall k \in R \left(k|p \implies k \in \{\pm u, \pm pu\} \text{ para alguna } u \in R \text{ invertible} \right).$$

Es fácil verificar que esto es equivalente a que

$$\forall a, b \in R \, (p = ab \implies a \text{ es invertible o } b \text{ es invertible}).$$

Obviamente esta seria una definición perfectamente valida (como cualquier otra) pero la vamos a reservar para otro concepto.

Al final del dia, ocuparemos la siguiente equivalencia:

$$p \in \mathbb{Z}_{\geq 0} \text{ es primo} \iff \forall a, b \in \mathbb{Z}_{\geq 0} \left(p|ab \implies p|a \text{ o } p|b \right).$$

El punto de todo este confuso debraye fue simplemente explicar porque no ocupamos la definición usual de numero primo para generalizar el concepto de numero primo.

Elementos primos

Definición

Supongamos que R es un anillo conmutativo con 1. Decimos que $p \in R$ es **primo** si p no es invertible y

$$\forall a, b \in R \left(p|ab \implies p|a \text{ o } p|b \right).$$

p es un elemento primo $\iff$ (p) es un ideal primo

Proposición 1

Supongamos que R es un anillo conmutativo con 1. Si $p \in R$, entonces

$$p \text{ es un elemento primo de } R \iff (p) \text{ es un ideal primo de } R.$$

Demostración. Usando que para cualesquiera dos elementos $x, y \in R$ tenemos que $x|y \iff y \in (x)$, obtenemos que

$$\begin{aligned}
p \text{ es un elemento primo de } R &\iff p \text{ no es invertible y} \\
&\qquad \forall a, b \in R \left(p|ab \implies p|a \text{ o } p|b\right) \\
&\iff (p) \text{ es un ideal propio y} \\
&\qquad \forall a, b \in R \left(ab \in (p) \implies a \in (p) \text{ o } b \in (p)\right) \\
&\iff (p) \text{ es un ideal primo de } R.
\end{aligned}$$

□

Elementos irreducibles y asociados

Definición

Supongamos que R es un anillo conmutativo con 1.

- Decimos que $r \in R$ es **irreducible** si $r \neq 0$, r no es invertible, y

  $$\forall a, b \in R \, (r = ab \implies a \text{ es invertible o } b \text{ es invertible}) \, .$$

  Naturalmente, también decimos que $r \in R$ es **reducible** si no es irreducible.
- Decimos que $a, b \in R$ son **asociados** si existe $u \in R$ invertible tal que $a = ub$.

Comentario

De la misma manera que el concepto de divisibilidad depende del anillo en donde estemos considerando a los elementos, todos los conceptos anteriores también dependen del anillo R.

Por ejemplo, seria mas preciso decir que $r \in R$ es irreducible en R si $r \neq 0$, r no es invertible en R y

$$\forall a, b \in R \, (r = ab \implies a \text{ es invertible en } R \text{ o } b \text{ es invertible en } R) \, .$$

Sin embargo, en este momento siempre lidiamos con un solo anillo R y por lo tanto no hace falta tener mucho cuidado. Pero de cualquier manera es muy importante tener esto en mente. De hecho, en el futuro estudiaremos la irreducibilidad de polinomios y veremos que aquí es muy importante tener este cuidado.

Invertible $\implies$ irreducible

Proposición 2

Supongamos que R es un anillo conmutativo con 1. Si $r \in R$ es invertible, entonces $r \in R$ es irreducible.

Demostración. Supongamos que $r \in R$ es invertible y que $r = ab$ para algunos $a, b \in R$. Como r es invertible, entonces r^{-1} existe y por lo tanto, la igualdad $r = ab$ implica que

$$1 = r^{-1}r = r^{-1}ab = \left(r^{-1}a\right) b$$

En particular, b es invertible y $b^{-1} = r^{-1}a$. Por lo tanto, r es irreducible. $\square$

Obviamente a también es invertible y $a^{-1} = r^{-1}b$.

En un dominio entero, primo $\implies$ irreducible

Proposición 3

Supongamos que R es un dominio entero con 1 y $p \in R$. Entonces

1. p primo $\implies p$ irreducible.
2. p primo $\not\Longleftarrow p$ irreducible.

Demostración.

1. Supongamos que p es primo. Para ver que es irreducible, sean $a, b \in R$ tales que $p = ab$. Entonces $ab = p \in (p)$ y como p es primo, entonces $a \in (p)$ o $b \in (p)$. Sin perdida de generalidad, supongamos que $a \in (p)$. Entonces existe $r \in R$ tal que $a = pr$. De donde, $p = ab = (pr)b$. Luego, como R es dominio entero, entonces[1] la ecuación anterior implica que $1 = rb$. Es decir, b es invertible. Por lo tanto, p es irreducible.

[1]Recordemos que en un dominio entero podemos cancelar factores no nulos.

2. Veamos que el $3 \in \mathbb{Z}[\sqrt{-5}]$ es un elemento irreducible pero que no es primo. Antes de empezar, denotemos por N a la norma usual en $\mathbb{Z}[\sqrt{-5}]$, es decir, sea N tal que $N(a + b\sqrt{-5}) = a^2 + 5b^2$ para toda $a, b \in \mathbb{Z}$. Ahora si, veamos que $3 \in \mathbb{Z}[\sqrt{-5}]$ es irreducible y no primo.

   Irreducible. Supongamos que $3 = \alpha\beta$ con $\alpha, \beta \in \mathbb{Z}[\sqrt{-5}]$. Como N es multiplicativa, entonces $9 = N(3) = N(\alpha)N(\beta)$. Sin embargo, como $N(x) \in \mathbb{Z}_{\geq 0}$ para toda $x \in \mathbb{Z}[\sqrt{-5}]$, entonces
   Caso 1. $N(\alpha) = 3 = N(\beta)$.
   Lo cual es imposible porque no existen $a, b \in \mathbb{Z}$ tales que $a^2 + 5b^2 = 3$. Por lo tanto, estamos en el siguiente caso.
   Caso 2. $N(\alpha) = 1$ y $N(\beta) = 9$.
   Pero entonces, como la única pareja $a, b \in \mathbb{Z}$ tal que $a^2 + 5b^2 = 1$ es cuando $a = \pm 1$ y $b = 0$, entonces α es invertible[2].

   No primo. $3 | 9 = (2 + \sqrt{-5})(2 - \sqrt{-5})$ pero $3 \nmid (2 + \sqrt{-5})$ y $3 \nmid (2 - \sqrt{-5})$.

$\square$

[2]Debería de ser claro que al considerar el caso 2, ya no hay necesidad de considerar el caso $N(\alpha) = 9$ y $N(\beta) = 1$

En $\mathbb{Z}$, primo $\iff$ irreducible

Definición

Supongamos que $k \in \mathbb{Z}$. Entonces, k es primo si y solo si k es irreducible.

Demostración. Por la proposición anterior, basta probar la implicación "$\Longleftarrow$". Por eso, supongamos que $k \in \mathbb{Z}$ es irreducible y veamos que es primo, usando la otra definición de entero primo: $p \in \mathbb{Z}$ es primo si los únicos divisores de p son $\pm p$ y ± 1. Entonces supongamos que $a \in \mathbb{Z}$ es divisor de k. Es decir, existe $b \in \mathbb{Z}$ tal que $k = ab$. Luego, como k es irreducible, la igualdad anterior implica que k es invertible o b es invertible. Como los únicos elementos invertibles en $\mathbb{Z}$ son ± 1, entonces $a = \pm 1$ o $b = \pm 1$. En cualquier caso, el otro entero es $\pm k$ y por lo tanto acabamos de demostrar que los únicos divisores de un entero irreducible k son precisamente ± 1 y $\pm k$. $\square$

El producto de un irreducible con un invertible es irreducible

Proposición 4

Supongamos que R es un anillo conmutativo y que $u, v \in R$. Si u es invertible y v es irreducible, entonces uv es irreducible.

Demostración. Supongamos que $a, b \in R$ son tales que $uv = ab$. Queremos ver que a es invertible o que b es invertible. Como u es invertible, la igualdad anterior implica que $v = u^{-1}(ab) = (u^{-1}a)b$. Como v es irreducible, la igualdad anterior implica que $u^{-1}a$ es invertible o b es invertible. En caso de que b sea invertible ya acabamos. En caso de que $u^{-1}a$ sea invertible, entonces existe $k \in R$ tal que $u^{-1}ak = 1$. Usando conmutatividad, veamos que $a(u^{-1}k) = 1$ y por lo tanto a es invertible. $\square$

Los isomorfismos preservan a los elementos irreducibles, primos, y asociados

Proposición 5

Supongamos que R, R' son anillos conmutativos con unidad y que $\varphi : R \to R'$ es un isomorfismo de anillos.

1. Si $r \in R$ es irreducible, entonces $\varphi(r)$ es irreducible.
2. Si $p \in R$ es primo, entonces $\varphi(p)$ es primo.
3. Si $a, b \in R$ son asociados, entonces $\varphi(a), \varphi(b)$ son asociados.

Demostración. Veamos el inciso 1. El resto son igual de sencillos y se los dejamos al lector.

A manera de contrapuesta, supongamos que $\varphi(r)$ es reducible. Entonces, existen $x, y \in R'$ no invertibles tales que $\varphi(r) = xy$.

Ahora bien, como φ es isomorfismo, existen $a, b \in R$ tales que $x = \varphi(a)$ y $b = \varphi(b)$. De donde, $\varphi(r) = \varphi(a)\varphi(b)$ y (de nuevo) como φ es isomorfismo, $r = ab$. Para finalizar, notemos que a y b no son invertibles. En efecto, esto es consecuencia inmediata de que

- φ es isomorfismo,
- $\varphi(a) = x$, $\varphi(b) = y$, y
- x y y no son invertibles.

$\square$