La característica de un dominio con 1

Facultad de Ciencias UNAM

Introducción

Supongamos que R es un dominio con unidad y considera la siguiente sucesión de elementos

$$1_R, \quad \underbrace{1_R + 1_R}_{2\cdot 1_R}, \quad \underbrace{1_R + 1_R + 1_R}_{3\cdot 1_R}, \quad \ldots$$

Si $R = \mathbb{Z}$, entonces todos los elementos de esta sucesión son distintos. Pero si $R = \mathbb{Z}_p$ (con $p \in \mathbb{Z}$ primo), entonces $p \cdot 1_R = 0_R$.

De hecho, en general, los siguientes casos son excluyentes y exhaustivos:

1. todos los $k \cdot 1_R$ son distintos.
2. existe $n \in \mathbb{Z}_{\geq 1}$ tal que $n \cdot 1_R = 0_R$.

Para ver esto, basta probar que

$$\text{existe } n \in \mathbb{Z}_{\geq 1} \text{ tal que } n \cdot 1_R = 0_R \iff \text{no todos los } k \cdot 1_R \text{ son distintos}$$

$\Longrightarrow$) Supongamos que existe $n \in \mathbb{Z}_{\geq 1}$ tal que $n \cdot 1_R = 0_R$. Entonces, $(mn) \cdot 1_R = 0$ para toda $m \in \mathbb{Z}$ y en particular, no todos los $k \cdot 1_R$ son distintos.

$\Longleftarrow$) Supongamos que no todos los $k \cdot 1_R$ son distintos. Entonces existen $a, b \in \mathbb{Z}_{\geq 1}$ distintos tales que $a \cdot 1_R = b \cdot 1_R$. Sin perdida de generalidad, supongamos que $a < b$. Entonces la igualdad $a \cdot 1_R = b \cdot 1_R$ implica que $(b - a) \cdot 1_R = 0_R$. En particular, existe $n = b - a \in \mathbb{Z}_{\geq 1}$ tal que $n \cdot 1_R = 0_R$. Esto nos lleva a hacer la siguiente definición.

La característica de un dominio con unidad

Definición

Supongamos que R es un dominio con unidad.

- Si existe $n \in \mathbb{Z}_{\geq 1}$ tal que $n \cdot 1_R = 0_R$, definimos $\mathrm{ch}(R)$ como el entero positivo p mas chico que satisface $p \cdot 1_R = 0$.
- Si todos los $n \cdot 1_R$ son distintos, definimos $\mathrm{ch}(R) = 0$.

El entero $\mathrm{ch}(R)$ es llamado **la característica de** R.

Observación

Usando lo obtenido en la introducción también podemos escribir

$$\operatorname{ch}(R) = \begin{cases} \text{mín}\{n \in \mathbb{Z}_{\geq 1} \mid n \cdot 1_R = 0\} & \text{si } \{n \in \mathbb{Z}_{\geq 1} \mid n \cdot 1_R = 0\} \neq \varnothing \\ 0 & \text{si } \{n \in \mathbb{Z}_{\geq 1} \mid n \cdot 1_R = 0\} = \varnothing \end{cases}$$

y

- $\operatorname{ch}(\mathbb{Z}) = \operatorname{ch}(\mathbb{Q}) = \operatorname{ch}(\mathbb{R}) = \operatorname{ch}(\mathbb{C}) = 0.$
- Si $p \in \mathbb{Z}$ es primo, entonces $\operatorname{ch}(\mathbb{Z}_p) = p.$

La característica es 0 o un numero primo

Proposición 1

Supongamos que R es un dominio con unidad. Si $\mathrm{ch}(R) \neq 0$, entonces $\mathrm{ch}(R)$ es primo.

Demostración. Procedamos por contradicción, es decir, supongamos que $\mathrm{ch}(R) \neq 0$ y que $\mathrm{ch}(R)$ no es un numero primo. Por definición, existen $a, b \in \mathbb{Z}_{\geq 2}$ tales que $\mathrm{ch}(R) = ab$ (y en particular, $a < \mathrm{ch}(R)$ y $b < \mathrm{ch}(R)$). Pero entonces,

$$0 = \mathrm{ch}(R) \cdot 1_R = (ab) \cdot 1_R = (a \cdot 1_R)(b \cdot 1_R)$$

y como R es un dominio con unidad, entonces $a \cdot 1_R = 0$ o $b \cdot 1_R$. En cualquier caso, las desigualdades $a < \mathrm{ch}(R)$ y $b < \mathrm{ch}(R)$ contradicen la definición de $\mathrm{ch}(R)$. $\square$

$\mathrm{ch}(R) \cdot a = 0$ para toda $a \in R$

Proposición 2

Supongamos que R es un dominio con unidad. Si $a \in R$, entonces $\mathrm{ch}(R) \cdot a = 0$.

Demostración. Si $a \in R$, entonces

$$\mathrm{ch}(R) \cdot a = \underbrace{a + \cdots + a}_{\mathrm{ch}(R)\text{-veces}} = (\underbrace{1_R + \cdots + 1_R}_{\mathrm{ch}(R)\text{-veces}})a = (\mathrm{ch}(R) \cdot 1_R)a = 0a = 0.$$

$\square$

$\mathrm{ch}(R) = \mathrm{ch}(S)$ si R es subanillo de S y $1_R \in S$

Proposición 3

Supongamos que R, S son dominios con unidad. Si R es subanillo de S y $1_R \in S$, entonces $\mathrm{ch}(R) = \mathrm{ch}(S)$.

Demostración. Como R es subanillo de S, entonces $0_R = 0_S$ y como $1_R \in S$, entonces $1_S = 1_R$. Usando esto, obtenemos

$$\{n \in \mathbb{Z}_{\geq 1} \mid n \cdot 1_R = 0_R\} = \{n \in \mathbb{Z}_{\geq 1} \mid n \cdot 1_S = 0_S\}$$

De donde,

$$\mathrm{ch}(R) = \text{mín}\{n \in \mathbb{Z}_{\geq 1} \mid n \cdot 1_R = 0_R\} = \text{mín}\{n \in \mathbb{Z}_{\geq 1} \mid n \cdot 1_S = 0_S\} = \mathrm{ch}(S).$$

$\square$

En particular,

- $\mathrm{ch}(R[x]) = \mathrm{ch}(R)$ para todo dominio con unidad R.
- $\mathrm{ch}(F) = \mathrm{ch}(E)$ si E es campo y F es subcampo de E.

El subanillo $\{n \cdot 1_R \mid n \in \mathbb{Z}\}$

Proposición 4

Supongamos que R es un dominio con unidad. Entonces $\{n \cdot 1_R \mid n \in \mathbb{Z}\}$ es un subanillo de R tal que

$$\{n \cdot 1_R \mid n \in \mathbb{Z}\} \cong \begin{cases} \mathbb{Z} & \text{si } \operatorname{ch}(R) = 0 \\ \mathbb{Z}_p & \text{si } \operatorname{ch}(R) = p \text{ con } p \text{ primo} \end{cases} \tag{1}$$

Demostración. Es fácil verificar que $\{n \cdot 1_R \mid n \in \mathbb{Z}\}$ es un subanillo. Para ver (1), considera

$$\begin{aligned} \varphi : \mathbb{Z} &\to R \\ n &\mapsto n \cdot 1_R \end{aligned}$$

donde $0 \cdot 1_R := 0_R$. Es fácil verificar que φ es un homomorfismo de anillos.

Caso 1. $\mathrm{ch}(R) = 0$.
Por definición, esto significa que todos los $n \cdot 1_R$ son distintos y por lo tanto, φ es inyectiva. Finalmente, como $\operatorname{im} \varphi = \{n \cdot 1_R \mid n \in \mathbb{Z}\}$, la inyectividad de φ implica que $\mathbb{Z} \cong \{n \cdot 1_R \mid n \in \mathbb{Z}\}$.

Caso 2. $\mathrm{ch}(R) = p$ con p primo.
Veamos que $\ker \varphi = \mathrm{ch}(R)\mathbb{Z}$. Para esto, recordamos que en la sección 1.1 demostramos que para todo subanillo S de $\mathbb{Z}$ tenemos

$$S = \text{mín}\left(S \cap \mathbb{Z}_{\geq 1}\right) \mathbb{Z}.$$

Usando (i) esto, (ii) la definición de $\mathrm{ch}(R)$ y (iii) la equivalencia

$$k \in \ker \varphi \iff k \cdot 1_R = 0_R,$$

obtenemos $\ker \varphi = \mathrm{ch}(R)\mathbb{Z} = p\mathbb{Z}$. Finalmente, por el 1er teorema de isomorfismos,

$$\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z} = \mathbb{Z}/\ker \varphi \cong \operatorname{im} \varphi = \{n \cdot 1_R \mid n \in \mathbb{Z}\}$$

$\square$

El subcampo primo de un campo

Definición

Supongamos que F es un campo. El **subcampo primo de** F, denotado F_{pri}, es el subcampo no trivial mas chico de F. Equivalentemente[1], el subcampo primo de F es

$$F_{\text{pri}} := \bigcap \left\{ S \subset F \mid S \text{ es un subcampo no trivial de } F \right\}.$$

[1] El hecho de que el siguiente campo este bien definido es consecuencia de que la intersección arbitraria de subcampos es un subcampo.

Proposición 5

Si F es un campo, entonces

$$F_{\text{pri}} \cong \begin{cases} \mathbb{Q} & \text{si } \mathrm{ch}(F) = 0 \\ \mathbb{Z}_p & \text{si } \mathrm{ch}(F) = p \text{ con } p \text{ primo} \end{cases}$$

Demostración. Antes que nada, notemos que como (i) todo subcampo de F contiene a 1_F y (ii) todo subcampo es un subgrupo aditivo, entonces

$$\{n \cdot 1_F \mid n \in \mathbb{Z}\} \subset F_{\text{pri}}. \tag{2}$$

Caso 1. $\mathrm{ch}(F) = 0$.

Por (2) y la proposición anterior, tenemos que

$$\mathbb{Z} \cong \{n \cdot 1_F \mid n \in \mathbb{Z}\} \subset F_{\text{pri}}.$$

Mas aun, si

$$E := \left\{(n \cdot 1_F)\,(m \cdot 1_F)^{-1} \mid n, m \in \mathbb{Z}\right\}$$

entonces es fácil verificar que E es un subcampo de F_{pri} y que la función

$$\frac{n}{m} \in \mathbb{Q} \mapsto (n \cdot 1_F)\,(m \cdot 1_F)^{-1} \in E$$

es un isomorfismo de campos. En resumen, tenemos $\mathbb{Q} \cong E \subset F_{\text{pri}}$.

Pero como F_{pri} es el subcampo no trivial mas chico de F y E es un subcampo de F, entonces también $F_{\text{pri}} \subset E$ y por lo tanto

$$F_{\text{pri}} = E \cong \mathbb{Q}.$$

Caso 2. $\mathrm{ch}(R) = p$ con p primo.

Por (2) y la proposición anterior, tenemos que

$$\mathbb{Z}_p \cong \left\{ n \cdot 1_F \mid n \in \mathbb{Z} \right\} \subset F_{\mathrm{pri}} \subset E. \tag{3}$$

Ahora bien, como $\mathbb{Z}_p$ es un campo, entonces $\left\{ n \cdot 1_F \mid n \in \mathbb{Z} \right\}$ es un subcampo de F y por lo tanto,

$$F_{\mathrm{pri}} \subset \left\{ n \cdot 1_F \mid n \in \mathbb{Z} \right\}.$$

Juntando esto con (3), obtenemos lo deseado. $\square$

$\mathrm{ch}(R)$ divide a $|R|$ si $|R| < \infty$

Proposición 6

Si R es un dominio finito con 1, entonces $\mathrm{ch}(R)$ divide a $|R|$.

Demostración. Usaremos el siguiente resultado básico de teoría de grupos.

> *Si H es un subgrupo de G, entonces $|H|$ divide a $|G|$.*

Ahora bien, como R es finito, entonces $\mathrm{ch}(R) \neq 0$ (demuéstralo por contrapuesta). Por lo tanto,

$$\left|\{n \cdot 1_R \mid n \in \mathbb{Z}\}\right| = \mathrm{ch}(R),$$

Considerando únicamente la estructura aditiva de R y usando el recordatorio y la igualdad anterior, obtenemos lo deseado. $\square$