

Teoría de Galois

Carlos Gómez-Lobo

1 Anillos

A continuación vamos a repasar algunos conceptos sobre anillos y especialmente anillos de polinomios, empezando por la definición de anillo.

Definición 1.1: Anillo

Un **anillo** es un conjunto no vacío dotado de dos operaciones, que denotaremos como suma $(+)$ y multiplicación (\cdot) y que cumplen las siguientes propiedades:

- $(R, +)$: grupo abeliano
- (R, \cdot) : operación binaria interna y cumple la propiedad asociativa

Si además (R, \cdot) tiene identidad, es decir, existe un elemento $e \in R$ tal que $e \cdot r = r \cdot e = r \ \forall r \in R$, diremos que R es un anillo con unidad y si además es abeliano, entonces será un anillo conmutativo.

A nosotros en esta asignatura nos interesarán especialmente estos últimos y nos referiremos a estos simplemente como anillos sin especificar que son conmutativos y sin unidad.

Ejemplos: $\mathbb{Z}, \mathbb{Z}_n, \mathbb{R}, \mathbb{C}, \mathbb{Q}, M_n(\mathbb{R})$ (no conmutativo), etc.

Notación:

- 0 para el elemento neutro de la suma
- $-a$ para el elemento inverso aditivo (opuesto).
- 1 para el elemento neutro de la multiplicación
- a^{-1} para el inverso multiplicativo, si existe
- $na = \underbrace{a + \dots + a}_{n \text{ veces}}$
- $a^n = \underbrace{a \cdot \dots \cdot a}_{n \text{ veces}}$

Definición 1.2: Cuerpo

Un anillo $(R, +, -)$ es un **cuerpo** si $(R^* = R \setminus \{0\}, \cdot)$ es un grupo abeliano.

Ejemplos: $\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Z}_p$ p primo, etc.

Notación: $\mathbb{Z}_n \begin{cases} \text{grupo aditivo} \rightarrow \mathbb{C}_n \\ \text{anillo} \rightarrow \mathbb{Z}_n \\ \text{cuerpo} \rightarrow \mathbb{F}_n (\text{n primo}) \end{cases}$

Definición 1.3: Divisor de cero

Sea R un anillo. Diremos que un elemento $a \in R$, $a \neq 0$ es un **divisor de cero** si $\exists b \in R$, $b \neq 0$ tal que $a \cdot b = 0$.

Ejemplo: En \mathbb{Z}_6 : $\bar{2}, \bar{3} \neq \bar{0}$ y $\bar{2} \cdot \bar{3} = \bar{0}$.

Definición 1.4: Dominio de integridad

Sea R un anillo, si R no tiene divisores de cero, entonces se dice que es un **dominio de integridad**.

Ejemplos: $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{F}_p$

Definición 1.5: "Divide a"

Diremos que a **divide a** b en R si $\exists c \in R$ tal que $b = a \cdot c$ y escribiremos $a|b$.

1.1 Subanillos

Definición 1.6: Subanillo

Diremos que $S \subset R$ es un **subanillo** si $(S, +, \cdot)$ es un anillo.

Observación: $S \subset R$ es un subanillo s y solo si:

- 1) $S \neq \emptyset$
- 2) $\forall a, b \in S, a + b \in S$
- 3) $\forall a, b \in S, a \cdot b \in S$
- 4) $1 \in S$

Ejemplo: $\mathbb{Z} \subset \mathbb{Q} \subset \mathbb{R} \subset \mathbb{C}$

Definición 1.7: Menor subanillo que contiene a un elemento

Dado un anillo R y un elemento a , podemos definir el **menor subanillo que contiene a R y al elemento a** como $R[a] = \left\{ \sum r_i \cdot a^k, \forall r \in R; i, k \in \mathbb{N} \right\}$

Ejemplo: $\mathbb{Z}[i] = \{a + bi, a, b \in \mathbb{Z}\} \subset \mathbb{C}$. Otra forma de ver este anillo es como la intersección de todos los subanillos de \mathbb{C} que contienen a \mathbb{Z} y a i .

Observación: De la misma forma podemos definir el menor cuerpo que contiene a un elemento y que denotamos como $R(a)$.

Ejemplo: $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2}, a, b \in \mathbb{Q}\}$, $\mathbb{Q}(\sqrt{2}) = \left\{ \underbrace{\frac{a + b\sqrt{2}}{c + d\sqrt{2}}}_{\neq 0}, a, b, c, d \in \mathbb{Q} \right\}$, $\mathbb{Q} \subset \mathbb{Q}[\sqrt{2}] \subset \mathbb{Q}(\sqrt{2}) \subset \mathbb{R}$

1.2 Anillos de polinomios

Definición 1.8: Anillo de polinomios

Sea R un anillo, llamaremos a $R[x]$ al **anillo de polinomios con coeficientes en R** y que será de la forma $R[x] = \left\{ \sum_{k=0}^n r_k x^k, \forall r \in R \right\}$.

Ejemplos: $\mathbb{C}[x], \mathbb{R}[x], \mathbb{Q}[x], \mathbb{Z}[x]$, etc.

Definición 1.9: Coeficiente director

El **coeficiente director** de un polinomio es el coeficiente distinto de 0 que multiplica a la x de mayor grado.

Notación: Grado de $p(x) := \deg(p(x))$

Proposición 1.1

El grado del producto de dos polinomios puede tener distintos valores en función de si el anillo sobre el que se construye es o no un DI:

$$\deg(p(x) \cdot q(x)) = \begin{cases} \deg(p(x)) + \deg(q(x)) & \text{si } R \text{ es dominio de integridad} \\ \leq \deg(p(x)) + \deg(q(x)) & \text{si no lo es} \end{cases}$$

Demostración: Obvio.

Ejemplo: $\mathbb{Z}_4, \begin{matrix} p(x) = 2x + 1 \\ q(x) = 2x \end{matrix} \left\} \deg(p(x) \cdot q(x)) = 1 < 2 \right.$

Proposición 1.2

Sea R un cuerpo, entonces R es siempre dominio de integridad y para cualesquiera polinomios de $R[x]$ se cumple que $\deg(p(x)) + \deg(q(x)) = \deg(p(x) \cdot q(x))$.

Demostración: Para demostrar que un cuerpo siempre es un DI vamos a ver por reducción al absurdo que todo elemento de un anillo que tenga inverso multiplicativo no es divisor de cero.

Suponemos que $r \neq 0 \in R$ es divisor de cero, es decir, $\exists r^{-1}$ tal que $r' \neq 0, r \cdot r' = 0$. Ahora suponemos además que r es invertible, es decir, $\exists r^{-1}$ tal que $r \cdot r^{-1} = 1$. Entonces $r \cdot r^{-1} = 1 \implies (r' \cdot r) \cdot r^{-1} = b \implies 0 = b$. Contradicción.

De la misma forma se puede ver que una unidad no puede ser un divisor de cero y como en un cuerpo todos sus elementos son unidades, no hay ningún divisor de cero y por tanto es un dominio de integridad. Por esto y por la proposición 1.1, queda demostrado.

Proposición 1.3

Sea K un cuerpo, entonces el anillo de polinomios asociado a K , $K[x]$ **no** es un cuerpo y sus únicos elementos invertibles son los pertenecientes al cuerpo K no nulos.

Demostración: Sea $p(x) \in K[x]$, $p(x) \neq 0$ invertible en $K[x]$. Entonces $p(x) \cdot p^{-1}(x) = 1$, $\deg(1) = 0$ y como por la proposición 1.1, $\deg(p(x) \cdot p^{-1}(x)) \leq \deg(p(x)) + \deg(p^{-1}(x))$, se tiene que $\deg(p(x)) = \deg(p^{-1}(x)) = 0$, por lo que los únicos elementos invertibles en $K[x]$ son los de grado 0, que son los no nulos que pertenecen a K . Entonces, puesto que no todos los elementos de $K[x]$ son invertibles, $K[x]$ no es un cuerpo.

Observación: El menor cuerpo que contiene a x y a los elementos de K es $K(x) = \left\{ \frac{p(x)}{q(x)} : p(x), q(x) \in K[x], q(x) \neq 0 \right\}$, teniendo en cuenta que $\frac{p(x)}{q(x)} = \frac{p'(x)}{q'(x)} \iff p(x)q'(x) = p'(x)q(x)$.

Definición 1.10: Polinomio mónico

Un **polinomio mónico** es aquel cuyo coeficiente director es 1.

1.3 Ideales en un anillo

Definición 1.11: Ideal

Sea R un anillo. Un **ideal** en R es un subconjunto no vacío $I \subset R$ tal que:

- i) $(I, +)$ es un subgrupo de R .
- ii) $\forall r \in R, \forall a \in I, r \cdot a \in I$ (Propiedad de absorción).

Proposición 1.4: Criterio para ideales

Para que un subanillo $I \subset R$, $I \neq \emptyset$ sea un ideal tiene que cumplir que:

- i) $\forall a, b \in I, a - b \in I$ ($a + b \in I$).
- ii) $\forall r \in R, \forall a \in I, r \cdot a \in I$.

Ejemplos:

1) R anillo cualquiera

- i) R es un ideal (el ideal trivial).
- ii) $\{0\}$ siempre es un ideal.

Si $I \subset R$ es un ideal e $I \neq R$, diremos que I es un **ideal propio**.

2) En \mathbb{Z} todos los anillos de la forma $I = \{2n : n \in \mathbb{Z}\}$ son ideales.

3) $\mathbb{Q}[x]$, $I = \{p(x) : p(r_0) = 0, r_0 \in \mathbb{Q}\}$

Comprobación: Sean $p(x), q(x), t(x) \in \mathbb{Q}[x]$ tal que $p(r_0) = q(r_0) = 0$, $t(x)$ cualquiera, entonces:

- i) $s(r_0) = p(r_0) - q(r_0) = 0 \implies s(x) \in I$.
 ii) $z(r_0) = p(r_0) \cdot t(r_0) = 0 \implies z(x) \in I$.
 4)

Proposición 1.5

Todos los ideales de \mathbb{Z} son de la forma $\{kn : n \in \mathbb{Z}\}$.

Demostración: Sale del algoritmo de la división.

Observación: Sea R un anillo y sean $I, J \subset R$ ideales, entonces:

- i) En general, $I \cup J$ **no** es un ideal.
 ii) $I \cap J$ es un ideal

Proposición 1.6

Sea K un anillo, entonces K es un cuerpo si y solo si contiene dos ideales: $\{0\}$ y K .

Demostración:

\implies) Sea $I \in K$, $I \neq \{0\}$ un ideal y $r \in I$, $r \neq 0$ uno de sus elementos. Por ser K un cuerpo $\exists r^{-1}$ tal que $r \cdot r^{-1} = 1 \in I$ (Propiedad de absorción) $\implies I = K$.

\Leftarrow) Sea K un anillo y $r \in K$, $r \neq 0$. Vamos a ver que r tiene un inverso.

Definimos $I := \{rs : s \in K\}$ que es un ideal. Puesto que $I \neq \{0\}$ y solo hay dos ideales, $I = K \implies 1 \in K \implies \exists s \in K$ tal que $s \cdot r = 1 \implies s = r^{-1}$.

Definición 1.12: Ideal generado

Sea R un anillo y $\{r_i\}$ una familia de elementos de R . Diremos que el **ideal generado** por $\{r_i\}_{i \in I}$ es el ideal más pequeño que contiene a $\{r_i\}_{i \in I}$ y lo denotamos por $\langle r_i \rangle_{i \in I} = \left\{ \sum s_j r_i : s_j \in R \right\}$.

Ejemplo: En $\mathbb{Z}[x]$ el ideal generado por $\langle 2, x \rangle = \{2q(x) + xp(x) : q(x), p(x) \in \mathbb{Z}\}$

Definición 1.13: Ideal principal

Sea R un anillo, diremos que $I \subset R$ es un **ideal principal** si $\exists a \in R$ tal que $I = \langle a \rangle$.

Ejemplo:

- 1) En \mathbb{Z} todos los ideales son principales.
 2) $\langle 2, x \rangle \subset \mathbb{Z}[x]$ no es principal.

Comprobación: Suponemos que $\exists g(x) \in \mathbb{Z}[x]$ tal que $\langle 2, x \rangle = \langle g(x) \rangle$, entonces $\exists q(x)$ tal que $g(x) \cdot q(x) = 2 \implies \deg(g(x)) = 0 \implies g(x) = k \in \mathbb{Z} \implies k = \pm 1, \pm 2$

Supongamos que $k = \pm 1$. Entonces $\langle g(x) \rangle = \langle \pm 1 \rangle = \langle 2, x \rangle = \mathbb{Z}[x]$. Sin embargo, $1 =$

$\underbrace{2p(x)}_{\text{coef. par}} + \underbrace{q(x)x^0}_{\text{grado} \geq 1}$. Contradicción.

Ahora si suponemos que $k = \pm 2 \implies \langle g(x) \rangle = \langle \pm 2 \rangle = \langle 2, x \rangle =$ polinomios con coeficientes pares, pero $x \notin \langle \pm 2 \rangle$. Contradicción.

Definición 1.14: Dominio de ideales principales (DIP)

Sea R un anillo, si todos los ideales contenidos en R con principales se dice que es un **dominio de ideales principales**.

Proposición 1.7

Sea K un cuerpo entonces $K[x]$ es un dominio de ideales principales.

Demostración: Sea $I \subset K[x]$ un ideal.

- Si $I = \{0\}$ ✓
- Suponemos que $I \neq \{0\} \implies \exists p(x) \in I, p(x) \neq 0$ y podemos definir $\Lambda = \{\deg(p(x)) : p(x) \in I\} \neq \emptyset, \Lambda \subset \mathbb{N}$. Por la propiedad de buen orden de \mathbb{N} podemos afirmar que Λ tiene un elemento mínimo n , por lo que $\exists p(x) \in I$ tal que $\deg(p(x)) = n$ y además $\langle p(x) \rangle \subseteq I$. Ahora vamos a demostrar por el algoritmo de la división de polinomios que $\langle p(x) \rangle = I$.

Sea $s(x) \in I \implies s(x) = q(x)p(x) + r(x)$ y hay dos posibilidades para $r(x)$:

- $r(x) = 0 \implies p(x) \mid q(x)$ ✓
- $r(x) \neq 0, \underbrace{s(x)}_{\in I} = q(x) \underbrace{p(x)}_{\in I} + \underbrace{r(x)}_{\in I} \xrightarrow{\text{Prop. 1}} r(x) \in I$. Contradicción porque $\deg(r(x)) < \deg(p(x))$
que es el grado mínimo en I .

Ejemplo: Usando un argumento similar con el algoritmo de la división en \mathbb{Z} se puede probar que este es un DIP.

Observación: El generador de un ideal $I \subset K[x]$ no tiene por qué ser único: si $I = \langle p(x) \rangle$ y $a \in K$, entonces $I = \langle ap(x) \rangle$. Para describir estos anillos de forma canónica utilizaremos como generador un polinomio mónico.

1.4 Anillos cociente

Definición 1.15: Anillo cociente

Sea $I \subset R$ un ideal en R , podemos definir como en los grupos al conjunto R/I como el **anillo cociente** según la relación de equivalencia $a = b \iff a - b \in I$.

Ahora vamos a comprobar algunas cosas sobre la definición anterior:

1. La relación de equivalencia usada es realmente una relación de equivalencia estudiando sus tres propiedades:

- i) Reflexiva: $a - a = 0 \in I \checkmark$
 ii) Simétrica: $a = b \implies a - b \in I \implies (a - b) \cdot -1 \in I \implies (b - a) \in I \implies b = a \checkmark$
 iii) Transitiva: $a = b$ y $b = c \implies a - b \in I$ y $b - c \in I \xrightarrow{\text{Prop. 1}} a - b + b - c = a - c \in I \implies a = c \checkmark$
2. El conjunto cociente resultado tiene estructura de anillo. Para ello solo es necesario comprobar que el producto está bien definido, es decir, de dos elementos no depende del representante escogido.

$$\text{Sean } \bar{a} = \{a + I\}, \bar{b} = \{b + I\}, \text{ entonces } (a + I)(b + I) = ab + \overbrace{aI + bI}^{\in I} + I = ab + I \implies \bar{a}\bar{b} = \overline{ab} \checkmark$$

Observación:

- Si el anillo R es conmutativo y con unidad, entonces R/I también lo es y su unidad es $\bar{1}$.
- $\forall a \in I, \bar{a} = 0$.

Ejemplos:

- $\mathbb{Z}/n\mathbb{Z} = \mathbb{Z}_n$
- $R/R = \{0\}$
- $R/\{0\} = R$
- $S = \mathbb{R}[x]/\langle x^2 + 1 \rangle$: ¿Qué pinta tiene? En primer lugar, vamos a comprobar que todo elemento de S es equivalente a un elemento de la forma $ax + b$, $a, b \in \mathbb{R}$. Sea $p(x) \in \mathbb{R}[x]$, ¿ $\overline{p(x)}$? $\overline{p(x)} = q(x)(x^2 + 1) + r(x)$ donde $r(x) = 0$ ó $\deg(r(x)) \leq 1 \implies p(x) - r(x) \in \langle x^2 + 1 \rangle \implies \overline{p(x)} = \overline{r(x)}$.

1.5 Homomorfismos de anillos

Definición 1.16: Homomorfismo de anillos

Sean R y T anillos. Un **homomorfismo de anillos** $f : R \longrightarrow T$ es una función que verifica las siguientes propiedades:

- $f(r + r') = f(r) + f(r'), \forall r, r' \in R$
- $f(r \cdot r') = f(r) \cdot f(r'), \forall r, r' \in R$
- (Homomorfismo de anillos unitarios) $f(1_R) = 1_T$

Observación: Nosotros siempre utilizaremos homomorfismos de anillos unitarios y nos referiremos a ellos simplemente como homomorfismos.

Ejemplos:

- Con este ejemplo vamos a comprobar cuántos homomorfismos existen de \mathbb{Z} en \mathbb{Z} . Si utilizamos las propiedades vistas anteriormente, tenemos que $1 \longrightarrow 1 \xrightarrow{\text{Prop. 1}} n = \underbrace{1 + \dots + 1}_{n \text{ veces}} \longrightarrow f(n) = \underbrace{f(1) + \dots + f(1)}_{n \text{ veces}} \implies f = Id$
- Sea R un anillo cualquiera:

$$\begin{aligned} f : \mathbb{Z} &\longrightarrow R \\ 1 &\longrightarrow 1_R \\ n &\longrightarrow f(n) = \underbrace{1_R + \dots + 1_R}_{n \text{ veces}} \end{aligned}$$

Un caso especial de este tipo es cuando $p \in \mathbb{Z}$ es un primo y $f(p) = 0_R$, entonces la función:

$$\begin{aligned}\bar{f} : R &\longrightarrow R \\ a &\longrightarrow a^p\end{aligned}$$

Es un homomorfismo de anillos llamado el "homomorfismo de Frobenius" y cumple que en R , $(a + b)^p = a^p + b^p$.

3) En este comprobaremos si existe algún homomorfismo de $\mathbb{Z}[i]$ en $\mathbb{Z}[\sqrt{2}]$:

$$\begin{aligned}f : \mathbb{Z}[i] &\longrightarrow \mathbb{Z}[\sqrt{2}] \\ 1 &\longrightarrow 1 \\ n \in \mathbb{Z} &\longrightarrow n \in \mathbb{Z}\end{aligned}$$

La función f mandará al elemento i a un elemento de $\mathbb{Z}[\sqrt{2}]$ de la forma $a + b\sqrt{2}$, sin embargo:

$$f(i^2) = \begin{cases} f(i)^2 = (a + b\sqrt{2})^2 \geq 0 \\ f(-1) = -1 \end{cases} \implies \text{Contradicción}$$

4) Sea $\mathbb{Z}[x]$ el anillo de polinomios con coeficientes enteros y T un anillo cualquiera:

$$\begin{aligned}f : \mathbb{Z}[x] &\longrightarrow T \\ x &\longrightarrow t \in T \\ p(x) &\longrightarrow p(t)\end{aligned}$$

Proposición 1.8: Propiedades de los homomorfismos de anillos

Sea $f : R \longrightarrow T$ un homomorfismo de anillos:

- 1) Si $S \in R$ es un subanillo, entonces $f(S) \in T$ es un subanillo
- 2) Si $J \in T$ es un ideal, entonces $f^{-1}(J)$ es un ideal de R .
- 3) Si f es sobreyectivo e $I \in R$ un ideal, entonces $f(I)$ es un ideal en T .
- 4) $\text{Ker } f = f^{-1}(\{0\})$ es un ideal en R .
- 5) f es inyectivo $\iff \text{Ker } f = \{0\}$.

Demostración:

- 1) Por las propiedades de homomorfismos $f(S)$ es un grupo aditivo y el producto es interno y asociativo.
- 2) Teniendo que $\forall s_1, s_2 \in f^{-1}(J)$, $\exists t_1, t_2 \in J$ tal que $s_1 = f^{-1}(t_1)$, $s_2 = f^{-1}(t_2)$, vamos a comprobar que cumple las propiedades de un ideal:

$$\text{i) } \underbrace{t_1 - t_2}_{\in f^{-1}(J)} = f(s_1) - f(s_2) = f(s_1 - s_2) \in f^{-1}(J) \implies s_1 - s_2 \in J$$

$$\text{ii) } \forall t \in T, t_1 \cdot t \in f^{-1}(J) \implies \exists r \in R \text{ tal que } f(r) = t_1 \cdot t = f(s_1) - t \implies t = \underbrace{f(r - s_1)}_{r'} \implies t_1 \cdot t = f(s_1 \cdot s') \in f(J) \implies s_1 \cdot s' \in J$$

- 3) Como f es sobreyectivo, podemos afirmar que $\forall t \in T$, $\exists r \in R$ tal que $f(r) = t$ y teniendo $t_1, t_2 \in f(I)$ tal que $t_1 = f(s_1)$, $t_2 = f(s_2)$, $s_1, s_2 \in I$ entonces:

$$\text{i) } t_1 - t_2 = f(s_1) - f(s_2) = f(\underbrace{s_1 - s_2}_{\in I}) \in f(I)$$

$$\text{ii) } t_1 \cdot t \stackrel{\text{sobre}}{=} f(s_1) \cdot f(s) = f(\underbrace{s_1 \cdot s}_{\in I}) \in f(I)$$

4) Comprobamos una vez más que cumple las propiedades de un ideal teniendo $s_1, s_2 \in \text{Ker } f$:

$$\text{i) } f(s_1 - s_2) = f(s_1) - f(s_2) = 0 \implies s_1 - s_2 \in \text{Ker } f$$

$$\text{ii) } \forall r \in R, f(s_1 \cdot r) = f(s_1) \cdot f(r) = 0 \cdot f(r) = 0 \implies s_1 \cdot r \in I$$

5) Vamos a demostrar ambas implicaciones:

\implies) Es obvio que la antiimagen del 0_T es el 0_S , y por ser inyectiva es el único.

\Leftarrow) Vamos a demostrarlo por reducción al absurdo. Supongamos que f no es inyectiva, es decir, $\exists r_1, r_2 \in R, r_1 \neq r_2$ tal que $f(r_1) = f(r_2) = t, t \in T$, entonces:

$$f(r_1 - r_2) = f(r_1) - f(r_2) = t - t = 0 \implies r_1 - r_2 \in \text{Ker } f \implies r_1 - r_2 = 0 \implies r_1 = r_2 \implies \text{Contradicción}$$

Observación: Si $I \in R$ es un ideal, en general $f(I) \in T$ no es un ideal.

Corolario 1.1

Sea K un cuerpo y $f : K \rightarrow T$, entonces f es necesariamente inyectivo.

Demostración: Como $\text{Ker } f$ es un ideal en K y este es un cuerpo, entonces por la proposición 1.6 $\text{Ker } f$ tiene que ser o bien K , que no puede ser porque 1_K no iría a 1_T , o bien $\{0\}$, por lo que es inyectivo.

Observación: Si $f : R \rightarrow T$ es un homomorfismo de anillos biyectivo, entonces su inverso $f^{-1} : T \rightarrow R$ es un homomorfismo de anillos. Por tanto, todo homomorfismo de anillos biyectivo es un isomorfismo.

Teorema 1.1: 1^{er} Teorema de isomorfía

Sea $f : R \rightarrow T$ es un homomorfismo de anillos, entonces:

- 1) Existe un homomorfismo de anillos \bar{f} de $R/\text{Ker } f$ en T que está bien definido tal que $\forall r \in R, \bar{f}(\bar{r}) := f(r)$.

$$\begin{array}{ccc} R & \xrightarrow{f} & T \\ \downarrow & \nearrow \bar{f} & \\ R/\text{Ker } f & & \end{array}$$

- 2) \bar{f} es inyectivo y por tanto hay un isomorfismo:

$$R/\text{Ker } f \simeq f(R) \in T$$

Definición 1.17: Característica de un anillo

Sea R un anillo cualquiera y f un homomorfismo de \mathbb{Z} en R