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
- $na = \underbrace{a + ... + a}_{\text{n veces}}$
- $a^n = \underbrace{a \cdot ... \cdot a}_{\text{n veces}}$

Definición 1.2: Cuerpo

Un anillo $(R,+,-)$ es un **cuerpo** si $(R^* = R\backslash\{0\},\cdot)$ 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 $\bar{2} \cdot \bar{3} = 0$.

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

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

Proposición 1.2

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

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 pertecientes 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 continene 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) $\implies I = K$.
$\impliedby$) 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, $1 = \underbrace{2p(x)}_{\text{coef. par}} + \underbrace{q(x)\cancel{x}}_{\cancel{grado \geq 1}}$.

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 $deg(px) = n$ 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 $r(x)$:

  - $r(x) = 0 \implies p(x) \mid q(x)$ ✓
  - $r(x) \neq 0$, $\underbrace{s(x)}_{\in I} = \underbrace{q(x)\underbrace{p(x)}_{\in I}}_{\in I} + r(x) \overset{Prop.1}{\implies} r(x) \in I$. 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 conciente

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: $a - a = 0 \in I$ ✓

ii) Simétrica: $a = b \implies a - b \in I \implies (a-b)\cdot -1 \in I \implies (b-a) \in I \implies b = a$ ✓

iii) Transitiva: $a = b$ y $b = c \implies a-b \in I$ y $b-c \in I \overset{\text{Prop. 1}}{\implies} a-b+b-c = a-b \in I \implies a = c$ ✓

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.

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

<u>Observación:</u>

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

<u>Ejemplos:</u>

1) ${}^{\mathbb{Z}}\!/\!_{n\mathbb{Z}} = \mathbb{Z}_n$

2) ${}^{R}\!/\!_{R} = \{0\}$

3) ${}^{R}\!/\!_{\{0\}} = R$

4) $S = {}^{\mathbb{R}[x]}\!/\!_{\langle x^2+1\rangle}$: ¿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 $p(x) \in \mathbb{R}[x]$, ¿$\overline{p(x)}$? $p(x) = q(x)(x^2+1) + r(x)$ 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:

i) $f(r + r') = f(r) + f(r'),\ \forall r, r' \in R$

ii) $f(r \cdot r') = f(r) \cdot f(r'),\ \forall r, r' \in R$

iii) (Homomorfismo de anillos unitarios) $f(1_R) = 1_T$

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

<u>Ejemplos:</u>

1) Con este ejemplo vamos a comprobar cuántos homomorfismos existen de $\mathbb{Z}$ en $\mathbb{Z}$. Si utilizamos las propiedades vistas anteirormente, tenemos que $1 \longrightarrow 1 \overset{\text{Prop. 1}}{\implies} n = \underbrace{1 + \cdots + 1}_{\text{n veces}} \longrightarrow f(n) = \underbrace{f(1) + \cdots f(1)}_{\text{n veces}} \implies f = Id$

2) Sea R un anillo cualquiera:

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

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 anillos 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) $Ker\ f = f^{-1}(\{0\})$ es un ideal en R.
5) f es inyectivo $\iff Ker\ f = \{0\}$.

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:
   i) $\underbrace{t_1 - t_2}_{\in f^{-1}(J)} = f(s_1) - f(s_2) = f(s_1 - s_2) \in f^{-1}(J) \implies s_1 - s_2 \in J$
   ii) $\forall t \in T,\ t_1 \cdot t \in f^{-1}(J) \implies \exists r \in R$ tal que $f(r) = t_1 \cdot t = f(s_1) - t \implies t = f(\underbrace{r - s_1}_{r'}) \implies$
   $t_1 \cdot t = f(s_1 \cdot s') \in f(J) \implies s_1 \cdot s' \in J$
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:
   i) $t_1 - t_2 = f(s_1) - f(s_2) = f(\underbrace{s_1 - s_2}_{\in I}) \in f(I)$

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

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

   i) $f(s_1 - s_2) = f(s_1) - f(s_2) = 0 \implies s_1 - s_2 \in Ker\ f$
   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.

   $\impliedby$) 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:

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

<u>Observación:</u> 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 $f : K \longrightarrow T$, entonces f es necesariamente inyectivo.

<u>Demostración:</u> Como $Ker\ f$ es un ideal en K y este es un cuerpo, entonces por la proposición 1.6 $Ker\ f$ 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.

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

Teorema 1.1: 1$^{\text{er}}$ Teorema de isomorfía

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

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

$$\begin{tikzcd}
R \arrow[r, "f"] \arrow[d] & T \\
R/_{Ker\ f} \arrow[ur, "\bar{f}"'] &
\end{tikzcd}$$

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

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

1.6 Característica de un anillo

Sea R un anillo cualquiera y f un homomorfismo de $\mathbb{Z}$ en R, entonces se tiene que $Ker\ f \in \mathbb{Z}$ es un ideal pero, ¿cómo son los ideales de $\mathbb{Z}$?

a) $Ker\ f = \{0\} \implies \mathbb{Z} \hookrightarrow R$, es decir, $\mathbb{Z}$ es un subanillo de R.

b) $ker\ f = \langle n \rangle,\ n \neq 0$

Utilizando el primer teorema de isomorfía podemos ver que $\mathbb{Z}/_{n\mathbb{Z}} \hookrightarrow R$, por lo que podemos pensar que $\mathbb{Z}_n$ es un subanillo de R. Con esto llegamos a la siguiente definición:

Definición 1.17: Característica de un anillo

Sea R un anillo y f un homomorfismo de anillos de $\mathbb{Z}$ en R, entonces definimos la **característica de un anillo** como:

$$char(R) = \begin{cases} 0 \text{ si } Ker\ f = 0 \\ n \text{ si } ker\ f = \langle n \rangle \end{cases}$$

Otro modo de definir $char(R)$, es decir que es el orden de 1_R como elemento de $(R, +)$. Si el orden de 1_R no es finito, entonces decimos que $char(R) = 0$.

Notación: Cuando decimos por ejemplo que $\mathbb{Z} \subset R$ o alguno de sus conjuntos cocientes en realidad hacemos una abuso de lenguaje y a lo que nos referimos es a que existe un anillo S tal que $\mathbb{Z} \simeq S \subset R$.

Observación: Volviendo al ejemplo del homomorfismo de Frobenius, se tiene que si $char(R) = p$, entonces la función $\begin{array}{c} R \xrightarrow{F} R \\ a \longrightarrow a^p \end{array}$ es un homomorfismo de anillos.

Ejemplos:

1) $char(\mathbb{Z}) = 0$
2) $char(\mathbb{Q}) = 0$ (inyectivo)
3) $char(\mathbb{R}) = char(\mathbb{C}) = 0$
4) $char(\mathbb{Z}_n) = n \begin{pmatrix} \mathbb{Z} \longrightarrow \mathbb{Z}_n = \mathbb{Z}/_{n\mathbb{Z}} \\ 1 \longrightarrow \bar{1} \end{pmatrix}$
5) $char(R) = char(R[x]) \quad \begin{pmatrix} \mathbb{Z} \longrightarrow R \hookrightarrow R[x] \\ 1 \longrightarrow 1_R \longrightarrow 1_R \end{pmatrix}$
6) Sea $R = \mathbb{Z} \times \mathbb{Z}_5$ con las operaciones coordenada a coordenada, $char(R) = 0 \quad \begin{pmatrix} \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}_5 \\ 1 \longrightarrow \ (1, \bar{1}) \end{pmatrix}$

Proposición 1.9: Característica de un dominio de integridad

Sea R un dominio de integridad, entonces la característica de R será 0 o prima.

Demostración: Por el primer teorema de isomorfía, tenemos que:

$$\begin{tikzcd} \mathbb{Z} \arrow[r, "f"] \arrow[d] & R \\ \mathbb{Z}/_{Ker\ f} \arrow[ur, "\bar{f}"'] & \end{tikzcd}$$

Entonces, $\mathbb{Z}/_{Ker\ f} = \mathbb{Z}/_{n\mathbb{Z}} \subset R$ y como $\bar{f}$ es inyectiva y R un DI, $\mathbb{Z}_n$ tiene que ser también un DI, por lo que n solo podrá ser primo o 0.

Corolario 1.2: Característica de un cuerpo

Sea K un cuerpo , entonces su característica será 0 o prima.

Demostración: Resultado directo pues todo cuerpo es un DI.

Proposición 1.10

Sea R un anillo , $I \subset R$ un ideal y π una función de la forma:

$$\begin{aligned} R &\xrightarrow{\pi} R/_{I} \\ a &\longrightarrow \bar{a}\ mod(I) \end{aligned}$$

Entonces π es un homomorfismo de grupos y se tiene que:

1. Si π es sobreyectivo y $J \subset R$ un ideal, entonces $\pi(J) \subset R/_{I}$ es un ideal.
2. Si $a \in R$ entonces $\pi(a) = \pi(a + I)$.
3. Si $J \subset R$ es un ideal, entonces $\pi(J) = \pi(J + I)$, siendo $J + I$ el ideal más pequeño que contiene a J y a I.
4. Sea $L \subset R/_{I}$ un ideal, entonces $\pi^{-1}(L)$ es un ideal en R y además $I \subset \pi^{-1}(L)$.
5. Sean $J_1,\ J_2 \subset R$ ideales tal que $I \subset J_1 \subsetneq J_2$ entonces $\pi(J_1) \subsetneq \pi(J_2)$.

Demostración: Vamos a demostrar el punto 5. Está claro que $\pi(J_1) \subset \pi(J_2)$ pero, ¿cómo sabemos que son distintos? Lo comprobamos por redicción al absurdo. Para ello supondremos que $\pi(J_1) = \pi(J_2)$, por lo que $\exists a \in J_2 \setminus J_1,\ b \in J_1$ tal que $\pi(a) = \pi(b)$. Enotnces $\underbrace{a}_{\in J_2\setminus J_1} = \underbrace{\underbrace{b}_{\in J_1} + \underbrace{r}_{\in I\subset J_1}}_{\in J_1}$. Contradicción.

Teorema 1.2: Correspondencia biyectiva

Sean R un anillo , $I \in R$ un ideal y π un homomorfismo de R en $R/_{I}$, entonces se tiene que existe una **correspondencia biyectiva** entre los ideales de R que contienen a I y los ideales de $R/_{I}$.

Demostración: Se deja como ejercicio para el lector.

Ejemplos:

1) Sea $\pi : \mathbb{Z} \longrightarrow \mathbb{Z}/_{6\mathbb{Z}}$. Vamos a estudiar los ideales que contienen a $\langle 6\rangle$:

$$\langle 6\rangle \subset \left\{\begin{array}{c} \langle 6\rangle \\ \langle 2\rangle \\ \langle 3\rangle \\ \mathbb{Z} \end{array}\right. \longleftrightarrow \begin{array}{l} \langle\bar{6}\rangle = \{\bar{0}\} \\ \langle\bar{2}\rangle = \{\bar{2},\ \bar{4},\ \bar{6}\} \\ \langle\bar{3}\rangle = \{\bar{0},\ \bar{3}\} \\ \langle\bar{1}\rangle = \mathbb{Z}_6 \end{array}$$

2) Sea $\pi : \mathbb{Q}[x] \longrightarrow \mathbb{Q}[x]/_{\langle x^2-1\rangle}$. Repetimos:

$$\langle x^2-1\rangle \subset \left\{\begin{array}{c} \langle x^2-1\rangle \\ \langle x-1\rangle \\ \langle x+1\rangle \\ \langle 1\rangle \end{array}\right. \longleftrightarrow \begin{array}{l} \langle\overline{x^2-1}\rangle = \{\bar{0}\} \\ \langle\overline{x-1}\rangle \\ \langle\overline{x+1}\rangle \\ \langle\bar{1}\rangle \end{array}$$

En este caso es muy práctico porque es muy sencillo saber cuántos y qué anillos pertenecen a $\mathbb{Q}[x]$ y contienen a $\langle x^2-1\rangle$.

1.7 Ideales primos y maximales

Definición 1.18: Ideal primo

Sea R un anillo e $I \in R$ un ideal , se dice que I es un **ideal primo** si:

i) $I \subsetneq R$.

ii) Si $\forall a, b \in R,\ a \cdot b \in I \implies a \in I$ ó $b \in I$.

Ejemplos:

1) En $\mathbb{Z}$, $\langle 6 \rangle$ no es primo ya que $2 \cdot 3 \in \langle 6 \rangle$ pero $2, 3 \notin \langle 6 \rangle$, mientras que $\langle 3 \rangle$ sí lo es.

2) En $\mathbb{Z}_6$, $\langle 0 \rangle$ no es primo porque $\bar{2} \cdot \bar{3} = \bar{0},\ \bar{2}, \bar{3} \notin \{\bar{0}\}$.

Proposición 1.11

Un anillo R es un dominio de integridad si y solo si $\{0\}$ es primo.

Demostración: Obv.

Proposición 1.12

Sea R un anillo e $I \subset R$ un ideal , I es primo si y solo si ${R}/{I}$ es un dominio de integridad.

Demostración: Sale directa de traducir la condición de un ideal primo al cociente ${R}/{I}$:

$$\begin{array}{rcl} a \cdot b \in I & \iff & a \in I \text{ ó } b \in I \\ \bar{a} \cdot \bar{b} = \bar{0} & \iff & \bar{a} = 0 \text{ ó } \bar{b} = 0 \end{array}$$

Definición 1.19: Ideal maximal

Sea R un anillo e $I \subset R$ un ideal, diremos que I es un **ideal maximal** si:

i) $I \subsetneq R$

ii) Si existe un ideal $J \subset R$ tal que $I \subset J$ entonces o bien $I = J$ o $J = R$.

Ejemplos:

1) En $\mathbb{Z}$ los ideales maximales son los generados por números primos.

2) En $\mathbb{Z}_6$, $\langle \bar{2} \rangle$ y $\bar{3}$ son maximales

Observación: Como la correspondencia biyectiva respeta los contenidos de los ideales también se extiende a los ideales maximales.

Proposición 1.13

Sea R un anillo e $I \subsetneq R$ un ideal , entonces I es maximal si y solo si ${R}/{I}$ es un cuerpo .

Demostración:
$\Longrightarrow$) Si I es maximal, por la correspondencia biyectiva, ${}^{R}\!/\!_{I}$ solo tiene dos ideales, $\{0\}$ y ${}^{R}\!/\!_{I}$, por lo que es un cuerpo.
$\Longleftarrow$) Si ${}^{R}\!/\!_{I}$ es un cuerpo entonces solo tiene dos ideales, $\{0\}$ y ${}^{R}\!/\!_{I}$, y por la correspondencia biyectiva I solo está contenido en I y en R, por lo que I es maximal.

Corolario 1.3

Todo ideal maximal es también primo.

Demostración: Sea R un anillo e $I \subset R$ un ideal, I maximal $\overset{1.13}{\Longrightarrow}$ ${}^{R}\!/\!_{I}$ es cuerpo $\overset{1.2}{\Longrightarrow}$ ${}^{R}\!/\!_{I}$ es DI $\overset{1.11}{\Longrightarrow}$ I es prmio.

Observación: El recíproco no es cierto en general.

1.8 Ideales primos y maximales en $K[x]$

Proposición 1.14

Sean $I, J \in K[x]$ dos ideales tal que $I = \langle p(x) \rangle$ y $J = \langle q(x) \rangle$ entonces $I \subset J \iff q(x) \mid p(x)$.

Demostración: Se deja como ejercicio.

Definición 1.20: Elemento irreducible

En un anillo R se dice que un elemento a es **irreducible** si para $a = b \cdot c,\ b, c \in R$, se tiene que b ó c son unidades.

Ejemplo: En $\mathbb{Z}$ los elementos irreducibles son los primos.

Proposición 1.15

Sea $K[x]$ el anillo de polinomios generado por el cuerpo K, se tiene que $\forall p(x) \in K[x]$ si $deg(p(x)) = 1$ entonces $p(x)$ es irreducible.

Demostración: Supongamos que $p(x) = s(x) \cdot q(x)$, entonces $deg(s(x)) + deg(q(x)) = 1 \implies q(x)$ ó $p(x)$ debe ser una unidad.

Proposición 1.16

Sea $K[x]$ el anillo de polinomios generado por el cuerpo K, se tiene que $\forall p(x) \in K[x], p(x) \neq 0$ tal que $p(x)$ no es ireducible $\exists q(x), s(x) \in K[x]$ con $deg(q(x)), deg(s(x)) < deg(p(x))$ tal que $p(x) = q(x) \cdot s(x)$.

Demostración: Por reducción al absurdo, suponemos por ejemplo que $deg(q(x)) = deg(p(x))$, entonces $deg(s(x)) = 0 \implies s(x)$ es una unidad $\implies p(x)$ es irreducible. Contradicción.
Ejemplo: En $\mathbb{Z}[x]$ el polinomio $2x + 2$ no es irreducible ya que $2x + 2 = 2 \cdot (x + 1)$ y ni 2 ni $x + 1$ son unidades.

Definición 1.21: Elemento primo

Sea R un anillo , se dice que $a \in R$ es **primo** si cada vez que $a|b \cdot c$ entonces $a|b$ ó $a|c$. Esto es lo mismo que decir que a es **primo** si $\langle a \rangle$ es primo.

Ejemplos:

1) En $\mathbb{Z}$ los elementos primos son, sorpresa, los primos.
2) Consideremos $R = \mathbb{Z}[\sqrt{-3}] \subset \mathbb{C}$ y el elemento $(1+\sqrt{-3})$, vemos que es irreducible y $(1+\sqrt{-3})(1-\sqrt{-3}) = 2 \cdot 2$ pero $(1+\sqrt{-3}) \nmid 2$ por lo que $1+\sqrt{-3}$ *no* es primo.

Proposición 1.17

Todo elemento primo es irreducible.

Demostración: Supongamos que $a \in R$ es primo. Tenemos que $a = b \cdot c$ para algunos $b, c \in R$, en particular, $a|b \cdot c$ y por ser a primo entonces $a|b$ ó $a|c$. Sin perder en generalidad suponemos que $a|b$ y por tanto $\exists k \in R$ tal que $b = a \cdot k$. Si sustituimos en la expresión inicial, obtenemos que $a = a \cdot k \cdot \cdot c$, que por la propiedad cancelativa vemos que $k \cdot c = 1$ lo que implica que c es unidad en R.

Observación: El recíproco en general no es cierto.

Teorema 1.3

Sea $I = \langle p(x) \rangle \subset K[x]$ un ideal , entonces I es maximal si y solo si $p(x)$ es irreducible.

Demostración:
$\Longrightarrow$) Vamos a comprobarlo por reducción al absurdo. Para ello, supongamos que $p(x)$ no es irreducible, es decir, $\exists q(x), s(x)$ tal que $p(x) = q(x) \cdot s(x)$, $deg(q(x), s(x)) > 1$, entonces tendríamos que $I = \langle p(x) \rangle \subsetneq \langle q(x) \rangle \subsetneq K[x]$. Contradicción porque I es un ideal maximal.
$\Longleftarrow$) De nuevo, vamos a probarlo por reducción al absurdo. Empezamos suponiendo que existe un ideal J tal que $I \subsetneq J \subsetneq K[x]$, entonces como $K[x]$ es un dominio de ideales principales, existe un polinomio $q(x)$ tal que $J = \langle q(x) \rangle$ y que cumple que $q(x)|p(x)$, $q(x) \notin K$ porque $I \subsetneq J$. Por tanto tenemos que $\exists s(x) \in K[x]$ tal que $p(x) = q(x) \cdot s(x)$ con $s(x) \notin K$ ya que si no $I = J$, pero si $deg(q(x), s(x)) > 1$ entonces $p(x)$ no es irreducible. Contradicción.