

UNIVERSIDAD DEL VALLE DE
GUATEMALA

MM2034 - 2 SEMESTRE - 2022

LICENCIATURA EN MATEMÁTICA APLICADA

Álgebra Moderna 2

Catedrático: Ricardo Barrientos

Estudiante: Rudik Roberto Rompich Cotzojay

Carné: 19857

Correo: rom19857@uvg.edu.gt

24 de noviembre de 2022

Índice

1 Teoría de Anillos	1
2 Teoría de campos	38
2.1 Elementos de la teoría de Galois	66
2.1.1 Solubilidad por radicales	72

1. Teoría de Anillos

Clase: 05/07/2022

Definición 1. Un conjunto no vacío R es un **anillo** si en R están definidas dos operaciones binarias denotadas por $+$ y \cdot , tales que si $r_1, r_2, r_3 \in R$:

1. $r_1 + r_2 \in R$.
2. $(r_1 + r_2) + r_3 = r_1 + (r_2 + r_3)$
3. $\exists 0 \in R \ni 0 + r = r + 0 = r, \forall r \in R$
4. Si $r \in R \implies \exists -r \in R \ni r + (-r) = (-r) + r = 0$
5. $r_1 + r_2 = r_2 + r_1$
6. $r_1 \cdot r_2 \in R$
7. $r_1 \cdot (r_2 \cdot r_3) = (r_1 \cdot r_2) \cdot r_3$
8. $r_1(r_2 + r_3) = r_1r_2 + r_1r_3$ (*distributividad izquierda*) y $(r_1 + r_2)r_3 = r_1r_2 + r_1r_3$ (*distributividad derecha*)

NOTA. $(R, +, \cdot)$

Definición 2. Si $(R, +, \cdot)$ es un anillo en el que existe $1 \in R$ tal que $1 \cdot r = r \cdot 1 = r, \forall r \in R$, entonces R es un anillo con elemento neutro multiplicativo. Suele llamarse **anillo con unidad** en la literatura.

Definición 3. Si $(R, +, \cdot)$ es un anillo en el que si $r_1, r_2 \in R$ (arbitrario) entonces $r_1 \cdot r_2 = r_2 \cdot r_1$, entonces R es un anillo comunitativo.

Definición 4. Si $(R, +, \cdot)$ es un anillo tal que $(R - \{0\}, \cdot)$ es un grupo abeliano, entonces $(R, +, \cdot)$ es un campo.

Construcción de los números racionales.

Ejemplo 1. 1. $(\mathbb{Z}, +, \cdot)$ es un anillo comunitativo con elemento neutro multiplicativo.

2. $(2\mathbb{Z}, +, \cdot)$ es un anillo conmutativo, pero no tiene un elemento neutro multiplicativo.

3. $(\mathbb{Q}, +, \cdot)$ es un campo (*¡ejercicio!*). (Campo finito más pequeño)

4. $(\mathbb{Z}_7, +, \cdot)$ es un campo.

5. $(\mathbb{Z}_6, +, \cdot)$ es un anillo conmutativo con neutro multiplicativo.

6. $(\mathbb{Q}_{2 \times 2}, +, \cdot)$ es un anillo no conmutativo con neutro multiplicativo.

$$\left(\mathbb{Q}_{2 \times 2} = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a, b, c, d \in \mathbb{Q} \right\} \right)$$

7. $(\mathbb{C}, +, \cdot, \mathbb{R})$ es campo.

8. Cuaterniones reales de Hamilton. Sea $Q = \{\alpha_0 + \alpha_1i + \alpha_2j + \alpha_3k : \alpha_1, \alpha_2, \alpha_3, \alpha_4 \in \mathbb{R}\}$ con las operaciones y reglas siguientes:

a) $i^2 = j^2 = k^2 = -1; ij = -ji = k; jk = -kj; ki = -ik = j$. Nótese que $(\{1, -1, i, j, k, -i, -j, -k\}, \cdot)$ es un grupo no abeliano de orden 8.

b) $(\alpha_0 + \alpha_1i + \alpha_2j + \alpha_3k) + (\beta_0 + \beta_1i + \beta_2j + \beta_3k) = (\alpha_0 + \beta_0) + (\alpha_1 + \beta_1)i + (\alpha_2 + \beta_2)j + (\alpha_3 + \beta_3)k$

c) $\alpha_0 + \alpha_1i + \alpha_2j + \alpha_3k = \beta_0 + \beta_1i + \beta_2j + \beta_3k$, si y solo si $\alpha_0 = \beta_0, \alpha_1 = \beta_1, \alpha_2 = \beta_2$ y $\alpha_3 = \beta_3$.

d) $(\alpha_0 + \alpha_1i + \alpha_2j + \alpha_3k)(\beta_0 + \beta_1i + \beta_2j + \beta_3k) = \alpha_0\beta_0 + \alpha_0\beta_1i + \alpha_0\beta_2j + \alpha_0\beta_3k + \alpha_1\beta_0i - \alpha_1\beta_1 + \alpha_1\beta_2ij + \cdots = (\alpha_0\beta_0 + \alpha_1\beta_1 - \alpha_2\beta_2 - \alpha_3\beta_3) + (\alpha_0\beta_1 + \alpha_1\beta_0 + \alpha_2\beta_3 - \alpha_3\beta_2)i + (\alpha_0\beta_2 - \alpha_1\beta_3 + \alpha_2\beta_0 + \alpha_3\beta_1)j + (\alpha_0\beta_3 + \alpha_1\beta_2 - \alpha_2\beta_1 + \alpha_3\beta_0)k$

$\implies (Q, +, \cdot)$ es un anillo no conmutativo con $0 = 0 + 0i + 0j + 0k$ como elemento neutro aditivo, $1 = 1 + 0i + 0j + 0k$ como elemento neutro multiplicativo y para $\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \in Q - \{0\} \implies \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2 \neq 0$ y $(\alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k)^{-1} = \frac{\alpha_0}{\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2} - \frac{\alpha_1}{\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2} i - \frac{\alpha_2}{\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2} j - \frac{\alpha_3}{\alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2} k \in Q$ (**Ejercicio!**)

Los anillos no conmutativos, con neutro multiplicativo e inversos multiplicativos (de elementos no nulos), como los cuaterniones de Hamilton se llaman Anillos de División o Semicampos.

NOTA. Por simplicidad y cuando el contexto lo permita un anillo $(R, +, \cdot)$ se abreviará R .

Definición 5. Si R es un anillo, $r \in R - \{0\}$ es un Divisor de Cero si existe $a \in R - \{0\}$ o $b \in R - \{0\}$ tales que $r \cdot a = 0$ o $b \cdot r = 0$.

Definición 6. Si R es un anillo conmutativo que no tiene divisores de cero es un **dominio entero**.

Ejemplo 2. El anillo de los $(\mathbb{Z}, +, \cdot)$ es un dominio entero.

Clase: 12/07/2022

Lema 1 (3.1). Si R es un anillo, entonces para $r_1, r_2 \in R$.

$$1. r_1 \cdot 0 = 0 \cdot r_1 = 0$$

$$2. r_1 \cdot (-r_2) = (-r_1) \cdot (r_2) = -(r_1 \cdot r_2)$$

$$3. (-r_1) \cdot (-r_2) = r_1 r_2 \text{ Si además } R \text{ tiene neutro multiplicativo } 1, \text{ entonces:}$$

$$4. (-1) \cdot r_1 = r_1$$

$$5. (-1)(-1) = 1$$

Demostración. 1. Usando la ley distributiva derecha, $r_1 \cdot 0 = r_1 \cdot (0 + 0) = r_1 \cdot 0 + r_1 \cdot 0 \implies$ Por la ley de cancelación en $(R, +)$, $r_1 \cdot 0 = 0$. Ahora usando la ley de distributividad izquierda tenemos $0 \cdot r_1 = (0 + 0) \cdot r_1 = 0 \cdot r_1 + 0 \cdot r_1$, y de nuevo, por la ley de cancelación en el grupo $(R, +)$, $0 \cdot r_1 = 0$.

2. $r_1 \cdot r_2 + r_1 \cdot (-r_2) = r_1 \cdot (r_2 - r_2) = r_1 \cdot 0 = 0 \implies$ por el (2) del lema 2.1, unicidad de los inversos en los grupos, $r_1 \cdot (-r_2) = -r_1 \cdot r_2$. Un argumento similar verifica que $(-r_1) \cdot r_2 = -(r_1 \cdot r_2)$
3. $(-r_1) \cdot (-r_2) = -(r_1 \cdot (-r_2)) = -(-(r_1 \cdot r_2)) = r_1 \cdot r_2$
4. Si $\exists 1 \in R$, neutro multiplicativo $\implies r_1 + (-1) \cdot r_1 = (1)r_1 + (-1)r_1 = (1-1)r_1 = 0 \cdot r_1 = 0 \implies$ Lema 2.1, unicidad de inverso $(-1)r_1 = -r_1$.
5. Caso especial de (iv), haciendo $r_1 = -1 \implies (-1)(-1) = -(-1) = 1$.

■

NOTA (El principio de las casillas). *Para $n, m \in \mathbb{Z}^+, n > m$, si n objetos se distribuyen en m casillas, entonces alguna casilla recibe 2 o más objetos. De manera equivalente, si n objetos se distribuyen en n casillas, de forma que ninguna casilla recibe más de un objeto, entonces todas las casillas reciben exactamente un objeto.*

Lema 2 (3.2). *Un dominio entero finito es un campo.*

Demostración. Sea D un dominio entero finito y $D = \{x_1, \dots, x_n\}, n \in \mathbb{Z}^+$. Debemos encontrar: neutro multiplicativo e inversos multiplicativos. Sea $a \in D - \{0\}$ y considérese ax_a, \dots, ax_n . Si $ax_i = ax_j$ con $i \neq j \implies 0 = ax_i - ax_j = a(x_i - x_j) \implies$ Como $a \neq 0$ y D es un dominio entero, y por lo tanto, carece de divisores de 0. $\implies x_i = x_j$ con $i \neq j (\rightarrow \leftarrow) \implies ax_1, \dots, ax_n$ son todos distintos y para el principio de las casillas $D = \{ax_a, \dots, ax_n\} \implies$ Como $a \in D \implies \exists i, 1 \leq i \leq n \ni a = ax_{i_0} = x_{i_0}a$. Si $d \in D \implies \exists i_d, 1 \leq i_d \leq n \ni d = ax_{i_d} \implies dx_{i_d} = (ax_{i_d})x_{i_d} = (x_{i_d}a)x_{i_d} = x_{i_d}(ax_{i_d}) = x_{i_d}a = ax_{i_d} = d \implies x_{i_d} = 1$ es neutro multiplicativo de D . Pero $1 \in D \implies \exists i_1, 1 \leq i_1 \leq n \ni 1 = ax_{i_1} = x_{i_1}a$. Entonces $x_{i_1} = 1$ es inverso multiplicativo de a . ■

Corolario 2.1. *Si p es un número primo, entonces $(\mathbb{Z}_p, +, \cdot)$ es un campo.*

Demostración. Se sabe que $(\mathbb{Z}_n, +, \cdot)$ es un anillo conmutativo $\forall n \in \mathbb{Z}^+$. Si p es un número primo y $\bar{a}, \bar{b} \in \mathbb{Z}_p \ni \bar{a}\bar{b} = \bar{0} \implies ab \equiv 0 \pmod{p} \implies p|ab \implies p|a$ o $p|b \implies a \equiv 0 \pmod{p}$ o $b \equiv 0 \pmod{p} \implies \bar{a} = \bar{0}$ o $\bar{b} = \bar{0} \implies \mathbb{Z}_p$ carece de divisores de 0 $\implies \mathbb{Z}_p$ es un dominio entero \implies por el lema 3.2, \mathbb{Z}_p es un campo. ■

Definición 7. Si $(R, +, \cdot)$ y (R', \oplus, \odot) son anillos y $\phi : R \rightarrow R'$ es una función, entonces ϕ es un homomorfismo.

$$1. \phi(r_1 + r_2) = \phi(r_1) \oplus \phi(r_2)$$

$$2. \phi(r_1 \cdot r_2) = \phi(r_1) \odot \phi(r_2)$$

Lema 3 (3.3). Si R y R' son anillos y $\phi : R \rightarrow R'$ es un homomorfismo entonces:

$$1. \phi(0) = 0'$$

$$2. \phi(-r) = -\phi(r), \forall r \in R.$$

Demostración. Se deduce directamente del hecho que $(R, +)$ y $(R', +)$ son grupos y del lema 2.14. ■

Ejemplo 3. Si $\phi : \mathbb{Z}_6 \rightarrow \mathbb{Z}_6 \ni \phi(\bar{a}) = \bar{0} \implies \phi(\bar{a}_1 + \bar{a}_2) = \bar{0} = \bar{0} + \bar{0} = \phi(\bar{a}_1) + \phi(\bar{a}_2)$ y $\phi(\bar{a}_1 \bar{a}_2) = \phi(\bar{a}_1)\phi(\bar{a}_2)$

que la imagen homomórfica de un neutro multiplicativo no necesariamente es neutro multiplicativo.

Proposición 1. Si R es un anillo con elemento neutro multiplicativo 1, R' un dominio entero y $\phi : R \rightarrow R'$ es un homomorfismo tal que $k_\phi \neq R$, entonces $\phi(1)$ es neutro multiplicativo de R' .

Demostración. Tarea. ■

Proposición 2. Si R es un anillo con elemento neutro 1, R' es un anillo y $\phi : R \rightarrow R'$ es un homomorfismo sobrejetivo, entonces $\phi(1)$ es neutro multiplicativo de R'

Demostración. Tarea. ■

Definición 8. Si R y R' son anillos y $\phi : R \rightarrow R'$ es un homomorfismo, entonces el kernel de ϕ es $k_\phi : \{r \in R : \phi(r) = 0\}$

Lema 4 (3.4). Si R y R' son anillos y $\phi : R \rightarrow R'$ es un homomorfismo, entonces:

1. $(K_\theta, +)$ es un subgrupo de $(R, +)$
2. Si $k \in K_\theta$ y $r \in R \implies kr, rk \in K_\theta$, es decir el núcleo de θ atrapa productos.

Demostración. 1. Lema 2.15

2. Si $k \in K_\theta$ y $r \in R \implies \theta(kr) = \theta(k)\theta(r) = 0' \cdot \theta(r) = 0' = \theta(r) \cdot 0' = \theta(r)\theta(k) = \theta(rk) \implies kr, rk \in K_\theta$

■

Ejemplo 4. 1. Si R es un anillo y $\phi : R \rightarrow R \ni \phi(r) = r \implies \phi$ es el homomorfismo identidad.

2. Si $\mathbb{Z}(\sqrt{2}) = \{m + n\sqrt{2} : m, n \in \mathbb{Z}\} \implies (\mathbb{Z}(\sqrt{2}), +, \cdot)$ con $+$ y \cdot la suma y producto usuales de números reales, es un anillo (ejercicio!). Si $\phi : \mathbb{Z}(\sqrt{2}) \rightarrow \mathbb{Z}(\sqrt{2}) \ni \phi(m + n\sqrt{2}) = m + n\sqrt{2}$. Si $m_1 + n_1\sqrt{2}, m_2 + n_2\sqrt{2} \in \mathbb{Z}(\sqrt{2}) \implies \phi((m_1 + n_1\sqrt{2}) + (m_2 + n_2\sqrt{2})) = \dots = \phi(m_1 + n_1\sqrt{2})\phi(m_2 + n_2\sqrt{2}) \implies \phi$ es homomorfismo y $K_\theta = \{m + n\sqrt{2} : \phi(m + n\sqrt{2}) = m - n\sqrt{2} = 0 = 0 - 0\sqrt{2}\} = \{0\} \implies \phi$ es un homomorfismo inyectivo.

3. Si $\theta : \mathbb{Z} \rightarrow \mathbb{Z}_n \ni \phi(a) = \bar{a}$. Sean $a, b \in \mathbb{Z} \implies \exists q_1, q_2 \in \mathbb{Z}, a = nq_1 + \bar{a}$ y $b = nq_2 + \bar{b}$ con $0 \leq \bar{a} < n$ y $0 \leq \bar{b} < n$. Además, $\exists q_3 \in \mathbb{Z} \ni a + b = q_3 + n + a + b$, con $a \leq \overline{a+b} < n$ y $\exists q_4 \in \mathbb{Z} \ni ab = q_4n + \overline{ab}$ con $0 \leq \overline{ab} < n$. Ahora bien, nótese lo siguiente: $(nq_1 + nq_2) + \bar{a} + \bar{b} = (nq_1 + \bar{a}) + (nq_2 + \bar{b}) = a + b = q_3n + qb$. Eso quiere decir: $\overline{a+b} - (\bar{a} + \bar{b}) = nq_3 - (nq_1 + nq_2) = n(q_3 - q_1 - q_2) \implies n|\overline{a+b} - (\bar{a} + \bar{b}) \implies \overline{a+b} = \bar{a} + \bar{b} \text{ mód } n$. Además, $(n^2q_1q_2 + nq_1\bar{b} + nq_2\bar{a}) + \bar{ab} = \dots$. Por lo tanto, ϕ es homomorfismo, y $K_\phi = n\mathbb{Z}$.

Clase: 14/07/2022

Ejemplo 5. Sea $\mathcal{C}([0, 1]) = \{f : [0, 1] \rightarrow \mathbb{R} \mid f \text{ es continua}\} \implies (\mathcal{C}([0, 1]), +, \cdot)$, con $+$ y \cdot la suma y producto usuales de funciones de variable real y valores reales, es un anillo (¡ejercicio!). Sea además, $\phi : (\mathcal{C}([0, 1]), +, \cdot) \rightarrow (\mathbb{R}, +, \cdot) \ni \phi(f) = f(1/2) \implies \phi \text{ si } f_1, f_2 \in \mathcal{C}([0, 1]) \implies \phi(f_1 + f_2) = (f_1 + f_2)(1/2) = f_1(1/2) + f_2(1/2) = \phi(f_1) + \phi(f_2) \text{ y } \phi(f_1 \cdot f_2) = (f_1 \cdot f_2)(1/2) = f_1(1/2)f_2(1/2) = \phi(f_1)\phi(f_2) \implies \phi \text{ es un homomorfismo. Si } \alpha \in \mathbb{R} \implies \text{sea } f : [0, 1] \rightarrow \mathbb{R} \ni f(x) = \alpha \implies f \in \mathcal{C}([0, 1]) \ni f(1/2) = \alpha \implies \phi(f) = \alpha \implies \phi \text{ es sobreyectivo. Además } k_\phi = \{f \in \mathcal{C}([0, 1]) \ni f(1/2) = 0\}.$

NOTA. Obsérvese que estos cinco ejemplos, aunque ilustrativos, consideran únicamente anillos conmutativos.

Definición 9. Si R y R' son anillos, un homomorfismo $\phi : R \rightarrow R'$ biyectiva es un isomorfismo

Lema 5 (3.5). Un homomorfismo sobreyectivo de anillos es un isomorfismo, si y solo si, su núcleo es trivial.

Demostración. Se deduce directamente del lema 2.16. ■

Definición 10. Si R es un anillo, un subconjunto no vacío U de R es un **ideal** o **ideal bilateral** si:

1. $(U, +)$ es un subgrupo de $(R, +)$.
2. Para todos $u \in U$ y $r \in R$, $ur, ru \in U$ (i.e. U **atrapa** o **absorbe** productos.)

Lema 6 (3.6). Si R es un anillo y U es un ideal de R , entonces R/U es un anillo y es una imagen homomórfica de R .

Tenemos:

$$R/U = \{u + r : r \in R\},$$

donde $\dot{z}u + r$?:

1. $(U, +)$ es un subgrupo normal de $(R, +)$.

Demostración. $(U, +)$ es subgrupo normal de $(R, +) \implies$ por el teorema 2C, $(R/U, +)$ es grupo, donde $(u + r_1) + (u + r_2) = u + (r_1 + r_2)$. Defínase ahora $\cdot: R/U \rightarrow R/U \ni (u + r_1, u + r_2) = (u + r_1)(u + r_2) = u + r_1r_2$. Sean $r_1, r_2, r_3, r_4 \in R \ni u + r_1 = u + r_3$ y $u + r_2 = u + r_4 \implies r_1 \equiv r_3 \pmod{U}$ y $r_2 \equiv r_4 \pmod{U} \implies r_1 - r_3 \in U$ y $r_2 - r_4 \in U \implies$ dado que U atrapa productos, $r_1r_2 - r_3r_2 = (r_1 - r_3) \cdot r_2 \in U$ y además $r_3r_2 - r_3r_4 = r_3(r_2 - r_4) \in U \implies r_1r_2 - r_3r_4 = r_1r_2 + 0 - r_3r_4 = r_1r_2 + (-r_3r_2 + r_3r_2) - r_3r_4 = (r_1r_2 - r_3r_2) + (r_3r_2 - r_3r_4) \in U \implies r_1r_2 \equiv r_3r_4 \pmod{U} \implies U + r_1r_2 = U + r_3r_4 \implies (U + r_1)(U + r_2) = U + r_1r_2 = U + r_3r_4 = (U + r_3)(U + r_4) \implies$ el producto de clases laterales en R/U es una función bien definida, y con lo cual, la cerradura está bien asegurada. Si $U + r_1, U + r_2, U + r_3 \in R/U \implies (U + r_1) + (U + r_2)(U + r_3) = (U + r_1r_2)(U + r_3) = U + (r_1r_2)r_3 = U + r_1(r_2r_3) = (U + r_1)(U + r_2r_3) = (U + r_1)((U + r_2)(U + r_3)) \implies$. Además, $((U + r_1) + (U + r_2))(u + r_3) = (U + (r_1 + r_2))(U + r_3) = U + (r_1 + r_2)r_3 = U + (r_1r_3 + r_2r_3) = (U + r_1r_3)(U + r_2r_3) = (U + r_1)(U + r_3) + (U + r_2)(U + r_3)$ y $(U + r_1)((U + r_2) + (U + r_3)) = (U + r_1)(U + (r_2 + r_3)) = U + r_1(r_2 + r_3) = U + (r_1r_2 + r_1r_3) = (U + r_1r_2) + (U + r_1r_3) = (U + r_1)(U + r_2) + (U + r_1)(U + r_3) \implies$ se cumplen las distributividades izquierda y derecha $\implies (R/U, +, \cdot)$ es un anillo. Considérese $\sigma: (R, +) \rightarrow (R/U, +) \ni \sigma(r) = u + r$ canónico, el cual se sabe que es sobreyectivo, con lo cual $(R/U, +)$ es una imagen homomórfica de $(R, +)$. Pero $\sigma(r_1r_2) = U + r_1r_2 = (U + r_1)(U + r_2) = \sigma(r_1)\sigma(r_2) \implies \sigma: (R, +, \cdot) \rightarrow (R/U, +, \cdot)$ es un homomorfismo sobreyectivo y $(R/U, +, \cdot)$ es una imagen homomórfica de $(R, +, \cdot)$. ■

Definición 11. Si R es un anillo y U es un ideal de R , entonces R/U es el **anillo cociente** de R sobre U .

Teorema 7 (3A (primer teorema de isomorfismos)). Si R y R' son anillos y $\phi: R \rightarrow R'$ es un homomorfismo sobreyectivo, entonces $R' \approx R/K_\phi$. Además, existe una correspondencia biyectiva entre el conjunto de ideales de R' y el conjunto de ideales de R que contienen a K_ϕ . Esta correspondencia biyectiva, puede obtenerse asociando a cada ideal U' de R' el ideal de R , $\phi^{-1}(U')$, con lo cual $R/\phi^{-1}(U) \approx R/U'$.

Demostración. Se deduce directamente del lema 2.17 y los teoremas 2D y 2B. ■

Lema 8 (3.7). Si R es un anillo conmutativo con elemento neutro multiplicativo cuyos únicos ideales son (0) y R , entonces R es un campo.

Demostración. Sea $a \in R - \{0\}$ y considérese $R_a = \{ra : r \in R\}$. Nótese que si $r_1a, r_2a \in Ra \implies r_1a - r_2a = (r_1 - r_2)a \in Ra$ ya que $r_1 - r_2 \in R \implies$ por el corolario al lema 2.3, $(Ra, +)$ es un sugrupo de $(R, +)$. Sea $x \in R, ra \in Ra \implies (ra)x = x(ra) = (xr)a \in Ra$ ya que $xr \in R \implies Ra$ atrapa productos en $R \implies Ra$ es un ideal de $R \implies Ra = (0)$ o $Ra = R$. Pero como $1 \in R$ y $a \neq 0 \implies a = 1 - a \in Ra \implies Ra \neq (0) \implies Ra = R$. Pero además, como ■

Definición 12 (Ideal maximal). Si R es un anillo, y M es un ideal de R , $M \neq R$, entonces M es un **ideal maximal** de R , siempre que si U es un ideal de R tal que $M \subseteq U \subseteq R$, entonces $M = U$ o $U = R$.

Clase: 19/07/2022

Ejemplo 6. Sea U un ideal de $(\mathbb{Z}, +, \cdot)$. Como $(U, +)$ es un subgrupo de $(\mathbb{Z}, +)$. \implies siendo $(\mathbb{Z}, +)$ cíclico e infinito, si $U \neq (0) \implies (U, +)$ es también cíclico e infinito $\implies \exists n_0 \in \mathbb{Z} \ni U = (n_0) = n_0\mathbb{Z}$. Efectivamente, $U = (n_0)$ es un ideal de \mathbb{Z} , ya que si $m \in \mathbb{Z}$ y $u \in U \implies \exists x \in \mathbb{Z} \ni u = xn_0 \implies mu = m(xn_0) = (mx)n_0 \in U$, ya que $mx \in \mathbb{Z}$, y efectivamente, U atrapa productos en \mathbb{Z} . ¿Para qué valores de n_0 , U es un ideal maximal de \mathbb{Z} ? Sea p un número primo y U un ideal de $\mathbb{Z} \ni (p) \subseteq U \subseteq \mathbb{Z}$. Ahora bien, $\exists u_0 \in \mathbb{Z} \ni U = (u_0) = u_0\mathbb{Z} \implies (p) \subseteq (u_0) \subseteq \mathbb{Z}$.

Recordatorio.

$$(p) = p\mathbb{Z} = \{px : x \in \mathbb{Z}\}$$

Nótese que $p = p \cdot 1 \in p\mathbb{Z} = (p) \subseteq (u_0) = u_0\mathbb{Z} \implies u_0|p$.

Generados tamaños.

$$\underbrace{(a)}_{\text{pequeo}} \subseteq \underbrace{(b)}_{\text{grande}} \implies \underbrace{b}_{\text{pequeo}} \mid \underbrace{a}_{\text{grande}}$$

Como p es un número primo, $u_0 = 1$ o $u_0 = p \implies (u_0) = (1) = \mathbb{Z}$ o $(u_0) = (p) \implies (p)$ es un ideal maximal de \mathbb{Z} . Sea M un ideal maximal de $\mathbb{Z} \implies \exists m \in \mathbb{Z} \ni M = (m_0) = m_0\mathbb{Z}$.

y además si U es un ideal de $\mathbb{Z} \ni M \subseteq U \subseteq \mathbb{Z} \implies \exists u_0 \in \mathbb{Z} \ni U = (u_0) \implies (m_0) \subseteq (u_0) \subseteq (1) \implies (m_0) = (u_0)$ o $(u_0) = (1) \implies (m_0) \subseteq (u_0)$ y $(u_0) \subseteq (m_0)$ y $(1) \subseteq (u_0)$ y $(u_0) \subseteq (1) \implies m_0|u_0$ y $u_0|m_0$.

\implies si $a|m_0 \implies (m_0) \subseteq (a) \subseteq \mathbb{Z} \implies$ siendo (m_0) un ideal de $\mathbb{Z} \implies (m_0) = (a)$ o $(a) = \mathbb{Z} \implies a \in (a) \subseteq (m_0)$ o $a = 1 \implies m_0|a$ o $a = 1 \implies m_0 = a$ o $1 = a \implies m_0$ es primo. En el anillo $(\mathbb{Z}, +, \cdot)$, (m) es un ideal maximal de \mathbb{Z} , si y solo si, m es primo.

Ejemplo 7. Sea $M = \{f \in \mathcal{C}([0, 1]) : f(1/2) = 0\}$ un ideal de $(\mathcal{C}[0, 1], +, \cdot)$. Sea U un ideal de $\mathcal{C}([0, 1]) \ni M \subset U \implies \exists g \in U - M \implies g : [0, 1] \rightarrow \mathbb{R}$, continua y $g(1/2) \neq 0$. Sea $h : [0, 1] \rightarrow \mathbb{R} \ni h(x) = g(x) - g(1/2) \implies h(1/2) = 0$ y $h(x)$ es continua en $[0, 1] \implies h \in M \subseteq U \implies h \in U \implies g - h \in U$, pero $(g - h)(x) = g(x) - h(x) = g(x) - g(x) + g(1/2) = g(1/2) \neq 0$ y $g(1/2) \in U \implies 1/g(1/2) \in \mathcal{C}([0, 1])$ y como U es ideal, atrapa productos. $\implies 1 = g(\frac{1}{2}) \cdot \frac{1}{g(\frac{1}{2})} \in U \implies$ si $f(x) \in \mathcal{C}([0, 1])$, como U atrapa productos $f(x) = f(x) \cdot 1 \in U \implies \mathcal{C}([0, 1]) \subseteq U \subseteq \mathcal{C}([0, 1]) \implies U = \mathcal{C}([0, 1]) \implies M$ es un ideal maximal de $\mathcal{C}([0, 1])$. Ahora bien, si $\gamma \in [0, 1]$, sea $M_\gamma = \{f \in \mathcal{C}([0, 1]) \ni f(\gamma) = 0\}$. \implies usando el mismo argumento se demuestra que M_γ es un ideal maximal de $\mathcal{C}([0, 1])$. Además, si M es un ideal maximal del anillo de $\mathcal{C}([0, 1]) \implies \exists \gamma \in [0, 1] \ni M = M_\gamma$. Entonces, existe una biyección entre los elementos de $[0, 1]$ y los ideales maximales del anillo $\mathcal{C}([0, 1], +, \cdot)$.

Teorema 9 (3B). Si R es un anillo conmutativo con elemento neutro multiplicativo y M es un ideal de R , entonces M es un ideal maximal de R , si y solo si, R/M es un campo.

Demostración. Sea

- [\Rightarrow] Se sabe que $(R/M, +, \cdot)$ es un anillo comutativo. Considérese el homomorfismo canónico $\sigma : R \rightarrow R/M \ni \sigma(r) = M + r$ y $K_\sigma = M \Rightarrow$ por el teorema 3A, existe una correspondencia biyectiva entre los ideales de R/M y los ideales de R que contienen a $K_\sigma = M \Rightarrow$ Como M es ideal maximal, los únicos ideales de R que contienen a M son R y $M \Rightarrow$ los únicos ideales de R/M son (M) y R/M . Además, como R tiene elemento neutro multiplicativo 1, $M + 1$ es el elemento neutro multiplicativo de R/M , entonces por el lema 3.7, R/M es campo.
- [\Leftarrow] Si $(R/M, +, \cdot)$ es un campo $\Rightarrow (M)$ y R/M son los únicos ideales de $R/M \Rightarrow$ aplicando de nuevo el teorema 3A al homomorfismo canónico, por la correspondencia biyectiva, los únicos ideales de R que contienen a M son R y $M \Rightarrow M$ es un ideal maximal de R .

■

Clase: 21/07/2022

Definición 13. Si R y R' son anillos y $\phi : R \rightarrow R'$ es un homomorfismo inyectivo, entonces se dice que ϕ **sumerge** a R en R' , o que ϕ es una **inmersión** de R en R' o que con la acción de ϕ , R puede sumergirse en R' . Si R puede sumergirse en R' , entonces R' es un **Sobre Anillo** o una **Extensión** de R .

Teorema 10 (3C). Todo dominio entero puede sumergirse en un campo.

Demostración. Sea D un dominio entero y defínase en $D \times D - \{0\}$ la relación binaria $\sim \exists$ si $a, m \in D$ y $b, n \in D - \{0\} \Rightarrow (a, b) \sim (m, n)$ si y solo si, $an = mb$. Nótese que:

- $ab = ba \Rightarrow (a, b) \sim (a, b), \forall (a, b) \in D \times D - \{0\} \Rightarrow \sim$ es reflexiva.
- Si $(a, b) \sim (m, n) \Rightarrow an = mb \Rightarrow mb = na \Rightarrow (m, n) \sim (a, b) \Rightarrow \sim$ es simétrica.

- Si $(a_1, b_1) \sim (a_2, b_2)$ y $(a_2, b_2) \sim (a_3, b_3) \implies a_1b_2 = b_1a_2$ y $a_2b_3 = b_2a_3 \implies a_1b_2b_3 = b_1a_2b_3$ y $a_2b_3b_1 = b_2a_3b_1 \implies a_1b_3b_2 = a_2b_1b_3 = a_3b_1b_2 = (a_1b_3 - a_3b_1)b_2 \implies$ como $b_2 \neq 0$ y D carece de divisores de cero $\implies a_1b_3 - a_3b_1 = 0 \implies a_1b_3 = b_1a_3 \implies (a_1, b_1) \sim (a_3, b_3) \implies \sim$ es transitiva. $\implies \sim$ es una relación de equivalencia, y para $(a, b) \in D \times D - \{0\}$, sea $[(a, b)]$ la clase de equivalencia de (a, b) respecto a \sim , es decir $[(a, b)] \in D \times D - \{0\} / \sim$.

Sea $+: D \times D - \{0\} / \sim \times D \times D - \{0\} / \sim \rightarrow D \times D - \{0\} / \sim$

$$+([(a, b)], [(m, n)]) = [(a, b)] + [(m, n)] = [(an + bm, bn)]$$

Si $a_1, a_2, m_1, m_2 \in D, b_1, b_2, n_1, n_2 \in D - \{0\} \ni [(a_1, b_1)] = [(a_1, b_1)]$ y $[(m_1, n_1)] = [(m_2, n_2)] \implies (a_1, b_1) \sim (a_2, b_2)$ y $(m_1, n_1) \sim (m_2, n_2) \implies a_1b_2 = b_1a_2$ y $m_1n_2 = n_1m_2$. Entonces $[(a_1, b_1)] + [(m_1, n_1)] = [(a_1n_1 + b_1m_1, b_1n_2)] \implies a_1b_2n_1n_2 = b_1a_2n_1n_2$ y $m_1n_2b_1b_2 = n_1m_2b_1b_2 \implies a_1n_1b_2n_2 = b_1n_1a_2n_2$ y $b_1m_1b_2n_2 = b_1n_1b_2m_2 \implies a_1n_1b_2n_2 + b_1m_1b_2n_2 = b_1n_1a_2n_2 + b_1n_1b_2m_2 \implies (a_1n_1 + b_1m_1)(b_2n_2) = (b_1n_1)(a_2n_2 + b_2m_2) \implies (a_1n_1 + b_1m_1, b_1n_1) \sim (a_2n_2 + b_2m_2, b_2n_2) \implies [(a_1n_1 + b_1m_1b_1n_1)] = [(a_2 \dots)] \implies [(a_1, b_1)] + [(m_1, n_1)] = [(a_1n_1 + b_1m_1, b_1n_1)] = [(a_2m_2 + b_2m_2, b_2n_2)] = [(a_2, b_2)] + [(m_2, n_2)] \implies$ las imágenes de $+$ son invariantes a cambios en los representantes de las clases de equivalencia. $\implies +$ es una función bien definida. $\implies (D \times D - \{0\} / \sim, +)$ es cerrada.

Si $[(a, b)], [(m, n)] \in D \times D - \{0\} / \sim \implies [(a, b)] + [(m, n)] = [(an + bm, bn)] = [(mb + na, nb)] = [(m, n)] + [(a, b)] \implies (D \times D - \{0\} / \sim, +)$ es conmutativa.

Si $[(a, b)], [(c, d)], [(e, f)] \in D \times D - \{0\} / \sim \implies ([(a, b)] + [(c, d)]) + [(e, f)] = [(ad + bc, bd)] + [(e, f)] = [(ad + bc)f + (bd)e, (bd)f] = [(adf + bcf + bde, bdf)] = [(adf + bcf + bde, bdf)] = [a(df) + b(cf + de), b(df)] = [(a, b)] + [(cf + de, df)] = [(a, b)] + ([c, d] + [(d, f)]) \implies (D \times D - \{0\} / \sim, +)$ es asociativo.

Si $b \in D - \{0\}$, entonces $[(0, b)] \in D \times D - \{0\}/ \sim$ y si $[(c, d)] \in D \times D - \{0\}/ \sim \Rightarrow [(0, b)] + [(c, d)] = [(0 + bc, bd)] = [(bc, bd)]$. Peor $(bc)d = (bd)c \Rightarrow [(bc, db)] = [(c, a)] \Rightarrow [(0, b)] + [(c, d)] = [(bc, bd)] = [(c, d)]$, $\forall [(c, d)] \in D \times D - \{0\}/ \sim \Rightarrow [(0, b)]$ es neutro de $(D \times D - \{0\}/ \sim, +)$.

Si $[(a, b)] \in D \times D - \{0\}/ \sim \Rightarrow a \in D$ y $b \in D - \{0\} \Rightarrow -a \in D \Rightarrow [(-a, b)] \in D \times D - \{0\}/ \sim \ni [(a, b)] + [(-a, b)] = [(ab + b(-a), bb)] = [(ab - ab, bb)] = [(0, bb)] = [(0, b)] \Rightarrow [(-a, b)] = -[(a, b)] \Rightarrow$ todo elemento de $D \times D - \{0\}/ \sim$ tiene inverso aditivo. $\Rightarrow (D \times D - \{0\}/ \sim, +)$ es grupo abeliano.

Sea ahora $\because D \times D - \{0\}/ \sim \times D \times D - \{0\}/ \sim \rightarrow D \times D - \{0\}/ \sim \ni \cdot([(a, b)], [(m, n)]) = [(a, b)] \cdot [(m, n)] = [(am, bn)]$. Sea $a_1, a_2, m_1, m_2 \in D, b_1, b_2, n_1, n_2 \in D - \{0\} \ni [(a_1, b_1)] = [(a_2, b_2)]$ y $[(m_1, n_1)] = [(m_2, n_2)] \Rightarrow a_1 b_2 = b_1 a_2$ y $m_1 n_2 = n_1 m_2 \Rightarrow (a_1 b_2)(m_1 n_2) = (b_1 a_2)(n_1 m_2) \Rightarrow (a_1 m_1)(b_2 n_2) = (b_1 n_1)(a_2 m_2) \Rightarrow [(a_1 m_1, b_1 n_1)] = [(a_2 m_2, b_2 n_2)]$. Entonces, $[(a_1, b_1)][(m_1, n_1)] = [(a_1 m_1, b_1 n_1)] = [(a_2 m_2, b_2 n_2)] = [(a_2, b_2)][(m_2, n_2)] \Rightarrow$ las imágenes de \cdot son invariantes a cambios en los representantes de las clases de equivalencia $\Rightarrow \cdot$ es una función bien definida $\Rightarrow (D \times D - \{0\}/ \sim - \{(0, b)\}, \cdot)$

$(D \times D - \{0\}/ \sim - \{(0, b)\}, \cdot)$ es conmutativo.

Si $[(a, b)], [(c, d)], [(e, f)] \in D \times D - \{0\}/ \sim \Rightarrow ([(a, b)] \cdot [(c, d)]) \cdot ([(e, f)]) = [(ac, bd)][(e, f)] = [(ac)e, (bd)f] = [a(ce), b(df)] = [(a, b)] \cdot [(ce, df)] = [(a, b)] \cdot ([(c, d)] \cdot [(e, f)]) \Rightarrow (D \times D - \{0\}/ \sim - \{(0, b)\}, \cdot)$ es asociativo.

Si $b \in D - \{0\} \Rightarrow [(b, b)] \in D \times D - \{0\}/ \sim$ y si $[(c, d)] \in D \times D - \{0\}/ \sim \Rightarrow [(b, b)] \cdot [(c, d)] = [(bc, bd)] = [(c, d)] \Rightarrow [(b, b)]$ es neutro multiplicativo de $(D \times D - \{0\}/ \sim - \{(0, b)\}, \cdot)$

Si $a, b \in D - \{0\} \Rightarrow [(a, b)] \in D \times D - \{0\}/ \sim - \{(0, b)\} \Rightarrow [(b, a)] \in D \times D - \{0\}/ \sim - \{(0, b)\} \ni [(a, b)] \cdot [(b, a)] = [(ab, ba)] = [(ab, ab)]$, el neutro multiplicativo de $(D \times D - \{0\}/ \sim - \{(0, b)\})$ $\Rightarrow [(b, a)] = [(a, b)]^{-1} \Rightarrow$ todo elemento de $(D \times D - \{0\}/ \sim - \{(0, b)\}, \cdot)$ tiene inverso. $\Rightarrow (D \times D - \{0\}/ \sim - \{(0, b)\}, \cdot)$ es un grupo abeliano.

Si $[(a, b)], [(c, d)], [(e, f)] \in D \times D - \{0\}/\sim$ \Rightarrow $([(a, b)] + [(c, d)]) \cdot [(e, f)] = [(ade + cbe, bdf)] = [((ade + cbe)f, (b + f)f)] = [(ae)(df) + (bf)(ce), (bf)(df)] = [(ae, bf)] + [(ce, df)]$ \Rightarrow Se cumplen las leyes distributivas en $(D \times D - \{0\}/\sim, +, \cdot)$ se cumplen las leyes distributivas.

$\Rightarrow (D \times D - \{0\}/\sim, +, \cdot)$ es un campo.

Si $b \in D - \{0\}$, sea $\phi : D \rightarrow D \times D - \{0\}/\sim \rightarrow \phi(d) = [(db, b)]$. Si $d_1, d_2 \in D$ \Rightarrow $\phi(d_1 + d_2) = [((d_1 + d_2)b, b)] = [((d_1 + d_2)bb, bb)] = [((d_1b + d_2b, bb))] = [(d_1b, b)] + [(d_2b, b)] = \phi(d_1) + \phi(d_2)$. Además, $\phi(d_1d_2) = [((d_1d_2)b, b)] = [((d_1d_2)bb, bb)] = [((d_1b(d_2b)), bb)] = [(d_1b, b)][(d_2b, b)] = \phi(d_1)\phi(d_2)$ $\Rightarrow \phi$ es homomorfismo.

Si $d \in K_\phi$ $\Rightarrow \phi(d) = [(db, b)] = [(0, b)] \Rightarrow (db, b) \sim (0, b) \Rightarrow (db)b = 0 \cdot b = 0 \Rightarrow d(bb) = 0$. Como $b \neq 0 \Rightarrow$ y como D no tiene divisores de 0, entonces $bb \neq 0 \Rightarrow$ de nuevo, como D no tiene divisores de cero, $d = 0 \Rightarrow K_\phi = (0) \Rightarrow \phi$ es inyectivo. $\Rightarrow \phi$ es una inmersión. $\Rightarrow D$ está sumergido en el campo $D \times D - \{0\}/\sim$. ■

Definición 14. Si D es un dominio entero, el campo construido en la prueba del teorema 3C se llama **Campo de Cocientes** de D .

Ejemplo 8. $(\mathbb{Z}, +, \cdot)$ es un dominio entero y $(\mathbb{Q}, +, \cdot)$ es un campo de cocientes.

Clase: 26/07/2022

Definición 15. Un dominio entero R es un **Anillo Euclídeo** si existe una función $d : R - \{0\} \rightarrow \mathbb{Z}^+ \cup \{0\}$, llamada d -valor tal que si $a, b \in R - \{0\}$, entonces:

1. $d(a) \leq d(ab)$.
2. $\exists q, r \in R \ni a = bq + r$, donde $r = 0$ o $d(r) < d(b)$.

Ejemplo 9. $(\mathbb{Z}, +, \cdot)$ con $d(n) = |n|$, el valor absoluto de $n \in \mathbb{Z}$, es un anillo euclídeo.

Teorema 11 (3D). Si R es un anillo euclídeo y U es un ideal de R , entonces existe: $a_0 \in R$ tal que $U = \{a_0r : r \in R\} = (a_0)$.

Demostración. Si $U = \{0\} \Rightarrow$ sea $a_0 = 0 \Rightarrow U = \{0\} = \{0 \cdot r : r \in R\} = (0)$.

Si $U \neq \{0\} \implies \exists a \in U \ni a \neq 0$. Sea $a_0 \in U - \{0\} \ni d(a_0)$ es mínimo. Siendo R anillo euclídeo existen $q, r \in R \ni u = aq + r$, con $r = 0$ o $d(r) < d(a_0)$. Si $r = 0 \implies u = aq \in (a)$. Pero $a \in U$ y U atrapa productos $\implies aq \in U \implies r = u - aq \in U$. Si $r \neq 0 \implies r \in U$ y $d(r) < d(a_0)$ no es mínimo en U ($\rightarrow \leftarrow$). $\implies U \subseteq (a) \subseteq U \implies U = (a)$. ■

Corolario 11.1. *Todo anillo euclídeo tiene elemento neutro multiplicativo.*

Demostración. Si R es un anillo euclídeo $\implies R$ es ideal de $R \implies$ por el teorema 3D $\exists a_0 \in R \ni R = (a_0)$, ya que $R \neq (0) \implies r \in R \implies \exists x_1 \in R \ni r = a_0 x_1$. En particular, $a_0 \in R \implies \exists x_0 \in R \ni a_0 = a_0 x_0 \implies rx_0 = (x_r a_0)x_0 = x_r(a_0 x_0) = x_r a_0 = a_0 x_r = r \implies x_0$ es neutro multiplicativo de R . ■

Definición 16. *Un dominio entero R con elemento neutro multiplicativo es un Anillo de Ideales Principales si para todo ideal A de R existe $a_0 \in R$ tal que $A = (a) = \{ar : r \in R\}$*

Corolario 11.2. *Todo anillo euclídeo es un anillo de ideales principales.*

Definición 17. *Si R es un anillo conmutativo, $r_1, r_2 \in R, r_1 \neq 0$, entonces r_1 divide a r_2 si existe $r_3 \in R$ tal que: $r_2 = r_1 r_3$, denotado por $r_1 | r_2$.*

Proposición 3. *Si R es un anillo conmutativo y $r_1, r_2, r_3 \in R - \{0\}$, entonces:*

1. *Si $r_1 | r_2$ y $r_2 | r_3 \implies r_1 | r_3$*
2. *Si $r_1 | r_2$ y $r_1 | r_3 \implies r_1 | (r_2 \pm r_3)$*
3. *Si $r_1 | r_2 \implies r_1 | r_2 r_3$*

Demostración. Tenemos:

1. Si $r_1 | r_2$ y $r_2 | r_3 \implies \exists x_1, x_2 \in R \ni r_2 x_1 r_1$ y $r_3 = x_2 r_2 \implies r_3 = x_2(x_1 r_1) = (x_2 x_1) r_1 \implies r_1 | r_3$.
2. $r_1 | r_2$ y $r_1 | r_3 \implies \exists x_1, x_2 \in R \ni r_2 = x_1 r_1$ y $r_2 \pm r_3 = (x_1 r_1) \pm (x_2 r_1) = (x_1 \pm x_2) r_1 \implies r_1 | (r_2 \pm r_3)$

3. Si $r_1|r_2 \implies \exists x \in R \ni r_2 = xr_1 \implies r_2r_3 = r_3r_2 = r_3(xr_3) = (r_3xr_1), x_3 \in R \implies r_1|r_2r_3.$

■

Clase: 28/07/2022

Definición 18. Si R es un anillo conmutativo y $r_1, r_2 \in R$, entonces $d \in R$ es **Máximo Común Divisor** de r_1 y r_2 si:

1. $d|r_1$ y $d|r_2$ (d es divisor común de r_1 y r_2)
2. Si $c|r_1$ y $c|r_2 \implies c|d$

Lema 12 (3.8). Si R es un anillo euclídeo y $r_1, r_2 \in R$, entonces un máximo común divisor $d \in R$ de r_1 y r_2 . Además, existen $\alpha, \beta \in R$ tales que:

$$d = \alpha r_1 + \beta r_2$$

Demostración. Sea $A = \{\delta r_1 + \gamma r_2 : \delta, \gamma \in R\}$. Sean $\delta_1, \delta_2, \alpha_1, \alpha_2 \in R \ni \delta_1 r_1 + \gamma_1 r_2, \delta_2 r_1 + \gamma_2 r_2 \in A$ y $(\delta_1 r_1 + \gamma_1 r_2) - (\delta_2 r_1 + \gamma_2 r_2) = (\delta_1 \delta_2)r_1 + (\gamma_1 - \gamma_2)r_2 \in A$, ya que $\delta_1 - \delta_2, \gamma_1 - \gamma_2 \in R \implies$ por el corolario al lema 2.3 ($A, +$) es un subgrupo de $(R, +)$. Además, si $\delta, \gamma, r \in R \implies \gamma r_1 + \gamma r_2 \in A$ y $(\delta r_1 + \delta r_2)r = (\delta r_1)r + (\delta r_2)r = (\delta r)r_1 + (\delta r)r_2 \in A$, ya que δr y $\gamma r \in R \implies A$ atrapa productos en $R \implies A$ es un ideal de R . Siendo R un anillo euclídeo, por el teorema 3D, R es un anillo de ideales principales $\implies \exists a \in R \ni A = (a) \implies a|\delta r_1 + \gamma r_2, \forall \delta, \gamma \in R$. Además, por el corolario al teorema 3D, $\exists 1 \in R \ni 1$ es neutro multiplicativo de R . Entonces, en particular cuando $\delta = 1$ y $\gamma = 0 \implies a|1 \cdot r_1 + 0 \cdot r_2 = r_1$ y cuando $\delta = 0$ y $\gamma = 1 \implies a|0 \cdot r_1 + 1 \cdot r_2 = r_2 \implies a$ es divisor común de r_1 y r_2 . En particular, $a = a \cdot 1 \in A \implies \exists \delta_a, \gamma_a \in R \ni a = \delta_a r_1 + \gamma_a r_2$. Si $c \in R \ni c|r_1$ y $c|r_2 \implies c|\gamma_a r_1$ y $c|\delta_a r_2 \implies c|\gamma_a r_1 + \gamma_a r_2 = a \implies a = \delta_a r_1 + \gamma_a r_2$ es máximo común divisor de r_1 y r_2 .

■

Definición 19. Sea R un anillo con elemento neutro multiplicativo 1, entonces $a \in R$ es una **Unidad** de R si existe $b \in R$ tal que $ab = 1$.

Lema 13 (3.9). *Si R es un dominio entero con elemento neutro multiplicativo 1 y $r_1, r_2 \in R - \{0\}$ tales que $r_1|r_2$ y $r_2|r_1$, entonces existe $u \in R$, unidad de R , tal que $r_1 = ur_2$.*

Demostración. Si $r_1|r_2 \implies \exists x_1 \in R \ni r_2 = x_1r_1$ y por otro lado $r_2|r_1 \implies \exists x_2 \ni r_1 = x_2r_2 \implies r_1 = x_2(x_1r_1) = (x_2x_1)r_1 \implies 0 = r_1 - (x_2x_1)r_1 = 1 \cdot r_1 - (x_2x_1)r_1 = (1 - x_1x_2) \cdot r_1 \implies$ siendo R un dominio entero, y por ello carece de divisores de 0, y además $r_1 \neq 0 \implies 0 = 1 - x_1x_2 \implies x_1x_2 = 1 \implies x_1, x_2$ son unidades de R . ■

Definición 20. *Si R es un anillo comutativo con elemento neutro multiplicativo, $r_1, r_2 \in R$ y $u \in R$ es unidad de R tales que $r_1 = ur_2$, entonces r_1 y r_2 son elementos **asociados**.*

Proposición 4. *En un anillo comutativo con elemento neutro multiplicativo la relación ser asociado es de equivalencia.*

Demostración. Sea R un anillo comutativo con neutro multiplicativo 1. Entonces,

1. Si $r \in R \implies r = 1 \cdot r$, y como $1 \cdot 1 = 1$, i.e. es unidad de R , entonces r es asociado de r , $\forall r \in R$
 2. Si r_1 es asociado a $r_2 \implies \exists u \in R$, unidad de $R \ni r_1 = ur_2 \implies u^{-1} \in R$ y también es unidad de $R \implies r_2 = u^{-1}r_1 \implies r_2$ es asociado a r_1 .
 3. Si r_1 es asociado de r_2 y r_2 es asociado a $r_3 \implies \exists u_1, u_2 \in R$, unidades de $R \ni r_1 = u_1r_2$ y $r_2 = u_2r_3 \implies r_1 = u_1(u_2r_3) = (u_1u_2)r_3$. Pero $u_2^{-1}u_1^{-1} \in R \ni \cdots u_1u_2$ es unidad de $R \implies r_1$ es asociado a r_3 .
-

Proposición 5. *Si R es un anillo comutativo con el neutro multiplicativo 1, $r_1, r_2 \in R$ y $d_1, d_2 \in R$ son máximos comunes divisores de r_1 y r_2 entonces d_1 y d_2 son asociados.*

Demostración. Si d_1 es máximo común divisor de r_1 y $r_2 \implies d_1|r_1$ y $d_1|r_2$, pero como d_2 es máximo común divisor de r_1 y $r_2 \implies d_1|d_2$. Un argumento simétrico verifica que $d_1|d_2 \implies$ por el lema 2.9, $\exists u \in R$, unidad de $R \ni d_1 = ud_2 \implies d_1$ y d_2 son asociados. ■

Definición 21. Si R es un anillo conmutativo con elemento neutro multiplicativo, r_1 y $r_2 \in R$, entonces el **Máximo Común Divisor** de r_1 y r_2 , denotado por (r_1, r_2) es la clase de equivalencia a la asociación de cualesquiera máximo común divisor de r_1 y r_2 .

Clase: 02/08/2022

Lema 14 (3.10). Si R es un anillo euclídeo $r_1, r_2 \in R - \{0\}$ y r_2 no es una unidad de R , entonces $d(r_1) < d(r_1r_2)$.

Demostración. Considérese $(r_1) = \{r_1 \cdot r : r \in R\}$, un ideal de R . Por la condición (i) de la definición de anillo euclídeo, $d(r_1) \leq d(r_1r_2)$. Nótese que $r_1r_2 \in (r_1)$ y si se supone $d(r_1) = d(r_1r_2) \implies$ por el argumento usado por la prueba del teorema 3D, el d -valor de r_1 es mínimo en $(r_1) \implies d(r_1r_2)$ también es mínimo en $(r_1) \implies$ todo elemento de (r_1) es múltiplo de $r_1r_2 \implies (r_1) \subseteq (r_1r_2) \implies r_1r_2|r_1 \implies \exists x \in R \ni r_1 = (r_1r_2)x = r_1(r_2x) \implies 0 = r_1 - r_2(r_2x) = r_1 \cdot 1 - r_1(r_2x) = r_1(1 - r_2x) \implies$ como $r_1 \neq 0$ y R es dominio entero y por lo tanto carece de divisores de 0.

$$0 = 1 - r_2x \implies 1 = r_2x \implies$$

r_2 es unidad ($\rightarrow \leftarrow$). $\implies d(r_1) < d(r_1r_2)$ ■

Definición 22. Si R es un anillo euclídeo, $\pi \in R$ es un **Elemento Primo** de R , si π no es una unidad de R y si $\pi = r_1r_2$, entonces r_1 ó r_2 es una unidad de R .

Proposición 6. Si R es un anillo euclídeo y $r \in R - \{0\}$, entonces r es una unidad de R , si y solo si, $d(r) = d(1)$.

Demostración. Tenemos

- (\Rightarrow) Si r es unidad de $R \Rightarrow \exists u \in R \ni ru = 1 \Rightarrow$ por (1) de la definición de anillo euclídeo, $d(r) \leq d(ru) = d(1) \leq d(1r) = d(r) \Rightarrow d(r) = d(1)$
- (\Leftarrow) Si $d(r) = d(1) \Rightarrow \exists q_1\sigma \in R \ni 1 = q\sigma$ con $\sigma = 0$ o $d(\sigma) < d(r) = d(1)$. Si $\sigma \neq 0 \Rightarrow d(\sigma) < d(1) = d(1 \cdot \sigma) = d(\sigma) (\rightarrow \Leftarrow) \Rightarrow 1 = qr \Rightarrow r$ es una unidad de R .

■

Lema 15 (3.11 - Existencia de las factorizaciones primas). *Si R es un anillo euclídeo y $r \in R - \{0\}$, entonces r puede factorizarse como el producto de un número finito de elementos primos de R .*

Demostración. Procediendo por inducción sobre $d(r)$:

- Si $d(r) = d(1) \Rightarrow r$ es una unidad de $R \Rightarrow$ es el producto de 0 elementos primos de R , y el lema es válido.
- Supóngase el lema válido para todo $x \in R - \{0\} \ni d(x) < d(r)$
- Si r es un elemento primo de $R \Rightarrow r$ se factoriza como el producto de 1 elemento primo de R . Supóngase que r no es una unidad de R y que existen $a, b \in R - \{0\}$ ninguno unidad de R tales que $r = ab \Rightarrow$ por (i) de la definición de anillo euclídeo, $d(a) \leq d(ab) = d(r) \Rightarrow$ por la hipótesis inductiva $\exists m \in \mathbb{Z}^+, \pi_1, \dots, \pi_m \ni a = \prod_{i=1}^m \pi_i$. Además, también por el lema 3.10, $d(b) < d(ba) = d(ab) = d(r) \Rightarrow$ por la hipótesis inductiva $\exists n \in \mathbb{Z}^+, \pi'_1, \dots, \pi'_n \ni b = \prod_{j=1}^n \pi'_j \Rightarrow r = ab = (\prod_{i=1}^m \pi_i) \left(\prod_{j=1}^n \pi'_j \right)$

■

Definición 23. *Si R es un anillo euclídeo y $r_1, r_2 \in R - \{0\}$, entonces r_1 y r_2 son **Primos Relativos** si (r_1, r_2) es una unidad de R .*

NOTA. Se sabe que el (r_1, r_2) es la clase de equivalencia respecto a la asociación de algún máximo común divisor de r_1 y r_2 . También se sabe que todo unidad es asociado a 1, es decir, sin perdida de generalidad se puede afirmar que en un anillo euclídeo r_1 y r_2 son primos relativos $\iff (r_1, r_2) = 1$

Lema 16 (3.12). Si R es un anillo euclídeo, $r_1, r_2, r_3 \in R - \{0\}$ tales que $r_1|r_2r_3$ y $(r_1, r_2) = 1$ entonces $r_1|r_2$.

Demostración. Por el lema 3.8, $\exists \lambda, \mu \in R \ni 1 = (r_1, r_2) = \lambda r_1 + \mu r_2 \implies r_3 = r_1\lambda r_1 + r_3\mu r_2 = r_1(r_3\lambda) + r_2(r_3\mu)$. Pero $r_1|r_2r_3 \implies \exists x \in R \ni r_2r_3 = r_1x \implies r_3 = r_1(r_3\lambda) + (r_2r_3)\mu = r_1(r_3\lambda) + (r_1x)\mu = r_1(r_3\lambda) + r_1(x\mu) = r_1(r_3\lambda + x\mu) \implies r_1|r_3$. ■

Proposición 7. Si R es un anillo euclídeo, π es un elemento primo de R y $r \in R - \{0\}$, entonces $\pi|r$ o $(\pi, r) = 1$.

Demostración. Tenemos $(\pi, r)|\pi \implies (\pi, r) = \pi$ o $(\pi, 1) = 1$ (o cualquiera de esta unidad) \implies si $\pi = (\pi, r)|r$ o $(\pi, r) = 1$. ■

Lema 17 (3.13). Si R es un anillo euclídeo, π es un elemento primo de R . $r_1, r_2 \in R - \{0\} \ni \pi|r_1r_2$, entonces

Demostración. Si $\pi \nmid r_1 \implies (\pi, r_1) = 1 \implies$ por el lema 3.12, $\pi|r_2$. Un argumento simétrico, asegura $\pi \nmid r_2 \implies \pi|r_1$ ■

Corolario 17.1. Si R es un anillo euclídeo, π es un elemento primo de R y $r_1, \dots, r_n \in R - \{0\}$ y $\pi|\prod_{i=1}^n \pi_i$ entonces existe i , $1 \leq i \leq n \ni \pi|r_i$.

Demostración. Por inducción matemática y el lema 3.13. ■

Clase: 04/08/2022

Teorema 18 (3E (unicidad de la factorización)). *Si R es un anillo euclídeano y $r \in R - \{0\}$ que no es una unidad de R y existen $m, n \in \mathbb{Z}^+, \pi_1, \dots, \pi_m, \pi'_1, \dots, \pi'_n$ elementos primos de R tales que*

$$r = \prod_{i=1}^m \pi_i = \prod_{j=1}^n \pi'_j,$$

entonces $m = n$ y cada π_i es asociado de algún π'_j , para $1 \leq i, j \leq m$ y recíprocamente cada π'_k es asociado de algún π_k , $1 \leq k, l \leq m$.

Demostración. Sea

$$\pi_1 \left(\prod_{i=2}^m \pi_i \right) = \prod_{i=1}^m \pi_i = \prod_{j=1}^n \pi'_j$$

$$\pi_1 \mid \prod_{j=1}^n \pi'_j$$

\implies por el lema 3.13, $\exists j, 1 \leq j \leq n \ni \pi_i \mid \pi'_j$. Pero, como π_1 y π'_j son elementos primos de $R \implies \exists u_1$, unidad de $R \ni \pi'_j = u_1 \pi_1$. ■

Corolario 18.1. *Todo elemento de un anillo euclídeano tiene una única factorización prima, salvo asociación.*

NOTA (Anillo euclídeano). Tenemos:

1. Dominio entero
 - a) Campo de cocientes
 - b) Anillo conmutativo
 - c) \nexists divisores de cero
2. d -valor
3. Algoritmo de la división
4. Neutro multiplicativo
5. Anillo de ideales principales
6. Máximo común divisor único, excepto asociación
7. Lema de Bezzout
8. U es unidad y $r \in R \implies d(r) = d(ur)$
9. Propiedades aritméticas de la divisibilidad.
10. Es unidad $\iff d(u) = d(1)$
11. r_1 y r_2 asociados $\iff d(r_1) = d(r_2)$.

Lema 19 (3.14). Si R es un anillo euclídeo y $r_0 \in R$, entonces (r_0) es un elemento primo de R .

Clase: 09/08/2022

Definición 24. El conjunto $\mathbb{Z}(i) = \{a + bi : a, b \in \mathbb{Z}, i = \sqrt{-1}\}$ es el conjunto de los **Enteros Gaussianos**.

Proposición 8. Sea $(\mathbb{Z}(i), +, \cdot)$, donde $+, \cdot$ son las operaciones usuales de números complejos es un dominio entero.

Teorema 20 (3F). Sea $(\mathbb{Z}(i), +, \cdot)$ es un anillo euclídeo.

Demostración. Considérese la función

$$d : \mathbb{Z} - \{0\} \rightarrow \mathbb{Z}^+ \cup \{0\} \ni d = (a + bi) = a^2 + b^2$$

De esta definición, $d(a+bi) \in \mathbb{Z}^+ \cup \{0\}$, $\forall a+bi \in \mathbb{Z}(i) - \{0\}$. Además, si $a_1+b_1i, a_2+b_2i \in \mathbb{Z}(i) - \{0\} \implies d((a_1+b_1i)(a_2+b_2i)) = d((a_1a_2 - b_1b_2) + (b_1a_2 + a_1b_2)i) = (a_1a_2 - b_1b_2)^2 + (b_1a_2 + a_1b_2)^2 = \dots = a_1^2(a_2^2 + b_2^2) + b_1^2(a_2^2 + b_2^2) = (a_1^2 + b_1^2)(a_2^2 + b_2^2) = d(a_1 + b_1i)d(a_2 + b_2i)$. Ahora bien, si $0 = d(a+bi) = a^2 + b^2 \implies a = b = 0 \implies d(a+bi) > 0, \forall a+bi \in \mathbb{Z}(i) - \{0\} \implies d(a+bi) \geq 1, \forall a+bi \in \mathbb{Z}(i) - \{0\} \implies d(a_1 + b_1i)d(a_2 + b_2i) = (a_1^2 + b_1^2)(a_2^2 + b_2^2) \geq a_1^2 + b_1^2 = d(a_1 + b_1i) \implies d$ es un d -valor para $\mathbb{Z}(i)$.

Considérese el caso especial $n \in \mathbb{Z}$ y $a+bi \in \mathbb{Z}(i) \implies$ por el algoritmo de la división en \mathbb{Z} , $\exists q_1, q_2, r_1, r_2 \in \mathbb{Z} \ni a = q_1n + r_1$ y $b = q_2n + r_2$, con $0 \leq r_2 < n$ y $0 \leq r_2 < n$. Si $0 \leq r_1 < n/2$ y $0 \leq r_2 < n/2$, sean $\delta_1 = q_1, \delta_2 = q_2, \sigma_1 = r_1$ y $\sigma_2 = r_2$. Si $n/2 < r_1 < n \implies -n/2 > -r_1 > -n \implies n/2 \geq n - r_1 > 0 > -n/2 \implies |n - r_1| < n/2 \implies$ sean $\delta_1 = q_1 + 1$ y $\delta_1 = r_1 - n \implies a = 1_1n + r_1 = q_1n + n - n + r_1 = (q_1 + 1)n + (r_1 - n) = \delta_1n + \sigma_1$, con $|\sigma_1| < n/2$. De igual forma, si $n/2 < r_2 < n$, sean $\delta_2 = q_2 + 1$ y $\delta_2 = r_2 - n \implies b = q_2n + r_2 = q_2n + n - n + r_2 = (q_2 + 1)n + (r_2 - n) = \delta_2n + \sigma_2$, $|\sigma_2| < n/2$. Entonces, $a+bi = (\delta_1n\sigma_1) + (\delta_2n + \sigma_2)i = \delta_1n + \sigma_1 + \delta_2ni + \sigma_2i = (\delta_1 + \delta_2i)n + (\sigma_1 + \sigma_2i)$, con $d(\sigma_1 + \sigma_2i) = \sigma_1^2 + \sigma_2^2 < n^2/4 + n^2/4 = n^2/2 < n^2 = d(n + 0i) = d(n)$, con $\sigma_1 + \sigma_2i, \sigma_1 + \sigma_2i \in \mathbb{Z}(i)$

Sean ahora $a_1 + b_1i, a_2 + b_2i \in \mathbb{Z}(i)$ y $a_2 + b_2i \neq 0 \implies (a_2 + b_2i)\overline{(a_2 + b_2i)} = (a_2 + b_2i)(a_2 - b_2i) = a^2 + b_2^2 \in \mathbb{Z}^+$. Además, $(a_1 + b_1i)\overline{(a_2 + b_2i)} = (a_1 + b_1i)(a_2 - b_2i) \in \mathbb{Z}(i) \implies$ aplíquese el caso especial a $(a_2 + b_2i)\overline{(a_2 + b_2i)} \in \mathbb{Z}^+$ y $(a_1 + b_1i)\overline{(a_2 + b_2i)} \in \mathbb{Z}(i) \implies \exists \delta_1, \delta_2, \sigma_1, \sigma_2 \in \mathbb{Z} \ni (a_1 + b_1i)\overline{(a_2 + b_2i)} = (\delta_1 + \delta_2i) \left[(a_2 + b_2i)\overline{(a_2 + b_2i)} \right] + (\sigma_1 + \sigma_2i) \ni d(a_2 + b_2i)d(\overline{(a_2 + b_2i)}) = d((a_2 + b_2i)\overline{(a_2 + b_2i)}) > d(\sigma_1 + \sigma_2i) = d((a_1 + b_1i)\overline{(a_2 + b_2i)} - (\sigma_1 + \sigma_2i) \left[(a_2 + b_2i)\overline{(a_2 + b_2i)} \right]) = d \left(\left[(a_1 + b_1i) - (\sigma_1 + \sigma_2i)(a_2 + b_2i)\overline{(a_2 + b_2i)} \right] \right) = d((a_1 + b_1i) - (\delta_1 + \delta_2i)(a_2 + b_2i))d(\overline{(a_2 + b_2i)}) \implies d(a_2 + b_2i) >$

$d((a_1 + b_1 i) - (\delta_1 + \delta_2 i)(a_2 + b_2 i))$. Sea $R_1 + R_2 i \in \mathbb{Z}(i)$ $\exists R_1 + R_2 i = (a_1 + b_1 i)(\delta_1 + \delta_2 i)(a_2 + b_2 i)$. Es conclusión, $\delta_1 + \delta_2 i, R_1 + R_2 i \in \mathbb{Z}(i)$ $\exists a_1 + b_1 i = (\delta_1 + \delta_2)(a_2 + b_2 i) + (R_1 + R_2 i)$, con $R_1 + R_2 = 0$ o $d(R_1 + R_2 i) < d(a_2 + b_2 i)$. ■

Clase: 11/08/2022

Teorema 21 (Wilson).

Lema 22 (3.15). *Sea p un número primo y supóngase que para $c \in \mathbb{Z}$, $(c, p) = 1$ existen $x, y \in \mathbb{Z}$, tales que: $cp = x^2 + y^2$, entonces existen $a, b \in \mathbb{Z}$ tales que $p = a^2 + b^2$.*

Demostración. Nótese que $(\mathbb{Z}, +, \cdot)$ es un subanillo de $(\mathbb{Z}(i), +, \cdot)$ y p es un elemento primo de $(\mathbb{Z}, +, \cdot)$. Supóngase que p es elemento primo de $(\mathbb{Z}(i), +, \cdot)$, pero por hipótesis, $cp = x^2 + y^2 = (x + yi)(x - yi) \implies$ por el lema 3.13, $p|x + yi$ o $p|x - yi \implies p|x + yi \implies \exists u + iv \in \mathbb{Z}(i) \ni x + iy = p(u + iv) = pu + i(pv) \implies x = pu, y = pv \implies x - iy = pu - i(pv) = p(u - iv) \implies p|x - yi \implies p^2|(x + iy)(x - iy) = cp \implies p|c \implies 1 = (p, c) > p(\rightarrow \leftarrow) \implies p$ no es elemento primo de $\mathbb{Z}(i) \implies a + bi, \alpha + \beta i \in \mathbb{Z}(i)$, ninguno de los dos unidades de $\mathbb{Z}(i) \ni p = (a + bi)(\alpha + \beta i) \implies d(a + bi) = a^2 + b^2 \neq 1$ y $d(\alpha - \beta i) = \alpha^2 + \beta^2 \neq 1$. Pero $p = (a + bi)(\alpha + \beta i) = (a\alpha b\beta) + (a\beta + b\alpha)i \implies a\beta + b\alpha = 0 \implies p = (a\alpha - b\beta) - 0 = (a\alpha - b\beta) - (a\beta + b\alpha)i = a\alpha - a\beta i - b\beta - b\alpha i = a(\alpha - \beta i) - bi(\alpha - \beta i) = (a - bi)(\alpha - \beta i)$. Entonces $p^2 = pp = (a + bi)(\alpha + \beta i)(a - bi)(\alpha - \beta i) = (a^2 + b^2)(\alpha^2 + \beta^2) \implies a^2 + b^2 | p^2$ y como $\alpha^2 + \beta^2 > 1$ y $a^2 + b^2 < p^2 \implies a^2 + b^2 = 1$ o $a^2 + b^2 = p \implies p = a^2 + b^2$. ■

Lema 23 (3.16). *Si p es un número primo de la forma $4n + 1$, entonces la congruencia $x^2 \equiv -1 \pmod{p}$ tiene solución.*

Demostración. Sea $x = \binom{p-1}{2}! \implies$ como p es de la forma $4n + 1 \implies x = \binom{p-1}{4}$ tiene un número par de factores $\implies x = \prod_{i=1}^{p-1/2} i = \prod_{i=1}^{p-1/2} -i$. Ahora bien, $p - k \equiv -k \pmod{p} \implies x^2 = x \cdot x = \left(\prod_{i=1}^{p-1/2} i \right) \left(\prod_{i=1}^{p-1/2} -i \right) = \left(\prod_{i=1}^{(p-1)/2} i \right) \left(\prod_{i=1}^{(p-1)/2} p - i \right) = \left(\prod_{i=1}^{(p-1)/2} i \right) \left(\prod_{i=\frac{p-1}{2}+1}^{p-1} i \right) = \prod_{i=1}^{p-1} i = (p-1) \equiv -1 \pmod{p}$. ■

Teorema 24 (3.6 - Fermat). *Si p es un número primo de la forma $4n + 1$, entonces existen $a, b \in \mathbb{Z}$ tales que $p = a^2 + b^2$.*

Demostración. Por el lema 3.15, $\exists x \in \mathbb{Z} \ni x^2 \equiv -1 \pmod{p}$ y elíjase $x \ni 0 \leq x \leq p - 1$. Si $x < p/2 \implies (p - x)^2 = p^2 - 2px + x^2 \equiv -1 \pmod{p}$ y $|p - x| = |p - x| = |x - p| < p/2$. De cualquier forma, siempre es posible elegir X de manera que $|x| \leq p/2$ y $p|x^2 + 1| \implies \exists c \in \mathbb{Z} \ni pc = x^2 + 1 \leq p^2/4 + 1 < p^2 \implies p \nmid c \implies (p, c) = 1 \implies$ por el lema 3.15 $\exists a, b \in \mathbb{Z} \ni p = a^2 + b^2$. ■

Definición 25. *Si F es un campo, el conjunto de polinomios en la variable x con coeficientes en F o sobre F es $F[x] = \{\sum_{i=0}^n a_i x^i : a_i \in F \wedge n \in \mathbb{Z}^+ \cup \{0\}\}$.*

Clase: 16/08/2022

Definición 26. *Si F es un campo,*

$$p(x) = \sum_{i=0}^m a_i x^i, \quad q(x) = \sum_{j=0}^n b_j x^j \in F[x],$$

entonces:

1. $p(x) = q(x)$, si y solo si, $m = n$ y $a_i = b_i, 1 \leq i \leq m$.
2. $p(x) + q(x) = \sum_{k=0}^{\max\{m,n\}} (a_k + b_k)x^k, a_k = 0$ para $k > m$ y $b_k = 0$ para $k > n$
3. $p(x)q(x) = \sum_{k=0}^{m+n} \left(\sum_{l=0}^k a_l b_{k-l} \right) x^k, a_l = 0$ para $l > m$ y $b_{k-l} = 0$ para $k - l > n$.

Proposición 9. *Si F es un campo, entonces $(F[x], +, \cdot)$ es un anillo conmutativo con elemento neutro multiplicativo.*

Definición 27. *Si F es un campo y $f(x) = \sum_{i=0}^n a_i x^i \in F[x], a_n \neq 0$, entonces el **grado** de $f(x)$ es $gr(f) = n$. No está definido el grado del polinomio cero y si $gr(f) = 0$, entonces $f(x)$ se dice constante.*

Lema 25 (3.17). *Si F es un campo y $f(x), g(x) \in F[X] - \{0\}$, entonces $gr(fg) = gr(f) + gr(g)$.*

Demostración. Se deduce directamente de la definición de producto en $F[x]$. ■

Corolario 25.1. Si F es un campo y $f(x), g(x) \in F[x] - \{0\}$, entonces $\text{gr}(f) \leq \text{gr}(fg)$

Demostración. Sea $0 \leq \text{gr}(g) \implies \text{gr}(f) = \text{gr}(f) + 0 \leq \text{gr}(f) + \text{gr}(g) = \text{gr}(fg)$. ■

Corolario 25.2. Si F es un campo, entonces $(F[x], +, \cdot)$ es un dominio entero.

Definición 28. Si F es un campo, entonces el campo de cocientes del dominio entero $(F[X], +, \cdot)$ es $(F(x), +, \cdot)$, el campo de las funciones racionales en x sobre F .

Proposición 10. Si F es un campo, entonces la función $\text{gr} : F[X] - \{0\} \rightarrow \mathbb{Z}^+ \cup \{0\}$ cumple:

1. $\text{gr}(f) \in \mathbb{Z}^+ \cup \{0\}, \forall f \in F[X] - \{0\}$

2. $\text{gr}(f) \leq \text{gr}(f, g), \forall f, g \in F[X] - \{0\}$

Lema 26 (3.18 - Algoritmo de la división). Si F sea un campo, $f(x), g(x) \in F[X]$ y $g(x) \neq 0$, entonces existen $q(r), r(x) \in F[X]$ tales que $f(x) = q(x)g(x) + r(x)$, con $r(x) < 0$ o $\text{gr}(r) < \text{gr}(g)$.

Demostración. Si $\text{gr}(f) < \text{gr}(g) \implies q(x) = 0$ y $r(x) = f(x)$ ■

Teorema 27 (3H). Si F es un campo, entonces $(F[X], +, \cdot)$ es un anillo euclideo.

Demostración. Se deduce directamente de las definiciones y propiedades de $F[X]$ y gr y del lema 3.18. ■

Lema 28 (3.19). Si F es un campo, entonces $(F[x], +, \cdot)$ es un anillo de ideales principales.

Demostración. Se deduce directamente de los teoremas 3D y 3H. ■

Lema 29 (3.20). *Si F es un campo, entonces $f(x), g(x) \in F[X] - \{0\}$ siempre tiene un máximo común divisor $d(x) \in F[x]$ y es tal que existen $\lambda(x), \delta(x) \in F[x]$ tales que $d(x) = \lambda(x)f(x) + \delta(x)g(x)$.*

Demostración. Se deduce directamente del teorema 3H y el lema 3.8 ■

Definición 29. *Si F es un campo, $p(x) \in F[X]$ es irreducible sobre F si $p(x) = g(x)h(x)$, con $g(x)h(x) \in F[X] - \{0\}$, entonces $\text{gr}(g) = 0$ o $\text{gr}(h) = 0$*

Ejemplo 10. $x^2 + 1$ es irreducible sobre \mathbb{Q} pero no es irreducible sobre \mathbb{C} .

Lema 30 (3.21). *Si F es un campo, entonces todo polinomio en $F[X]$ puede factorizarse de manera única, salvo asociación, como producto de un número finito de polinomios de $F[X]$ irreducibles sobre F .*

Demostración. Se deduce directamente de los teoremas 3E y 3H. ■

Lema 31 (3.22). *Si F es un campo, el ideal generado por el polinomio $p(x)$ de $F[X]$ es un ideal maximal del anillo de polinomios si y solo si, $p(x) \in F[x]$ es irreducible sobre F .*

Demostración. Se deduce de los lemas 3.14, 3.21 y teorema 3H. ■

Clase: 18/08/2022

$$(x^2 - 2)(x^2 + 1)$$

$$(x^3 - 2) = \{f(x)(x^3 - 2) : f(x) \in \mathbb{Q}[x]\}$$

Ejemplo 11. $x^2 - 2 \in \mathbb{Q}[x]$, irreducible sobre $\mathbb{Q} \implies$ por el lema 3.22 ($x^3 - 2$) es un ideal maximal de $\mathbb{Q}[x] \implies$ por el teorema 3B, $\mathbb{Q}[x]/(x^3 - 1)$. Se verificará detalladamente este hecho, nótese que $\mathbb{Q}[x]/(x^3 - 2) = \{f(x) + [x^3 - 2] : f(x) \in \mathbb{Q}[x]\}$. Por el algoritmo de la división en $\mathbb{Q}[x]$, $\exists q(x), r(x) \in \mathbb{Q}[x] \ni f(x) = q(x)(x^2 - 2) + r(x)$, con $r(x) = 0$ o $gr(r) < gr(x^3 - 2) = 3 \implies \exists a_0, a_1, a_2 \in \mathbb{Q} \ni r(x) = a_0 + a_1x + a_2x^2 \implies f(x) + [x^3 - 2] = (q(x)(x - 2) + r(x)) + [x^3 - 2] = q(x)(x^3 - 2) + [x^3 - 2] + r(x) + [x^3 - 2] = (x^3 - 2) + r(x) + [x^3 - 2] = r(x) + [x^3 - 2] = (a_0 + a_1x + a_2x^2) + (x^3 - 2) = [a_0 + [x^3 - 2]] + [a_1x + [x^3 - 2]] + [a_2x^2 + [x^3 - 2]] = a_0[x + [x^3 - 2]]^0 + a_1[x + [x^3 - 2]]^1 + a_2[x + [x^3 - 2]]^2$

$$q(x)(x^3 - 2) + [x^3 - 2] = 0 + [x^3 - 2] = [x^3 - 2]$$

Sea $\alpha = x + [x^3 - 2] \in \mathbb{Q}[x]/(x^3 - 2)$, con lo cual $f(x) + [x^3 - 2] = a_0 + a_1\alpha + a_2\alpha^2$

$$\langle\{1, \alpha^1, \alpha^2\}\rangle_{\mathbb{Q}}$$

$\implies \langle\{1, \alpha^1, \alpha^2\}\rangle_{\mathbb{Q}} = \mathbb{Q}[x]/(x^3 - 2)$. Por otro lado, nótese que $\alpha^3 - 2 \approx [x + (x^3 - 2)]^3 - [2 + (x^3 - 2)] = [x^3 + (x^3 - 2)] - [2 + (x^3 - 2)] = (x^3 - 2) + [x^3 - 2] = 0 + [x^3 - 2] = [x^3 - 2] \approx 0 \implies \alpha$ es una raíz de $x^3 - 2 \implies \alpha \in \mathbb{Q}[x]/(x^3 - 2) - \mathbb{Q}$ (Nótese que si $a \in \mathbb{Q} \implies a \approx a + (x^3 - 2) \in \mathbb{Q}[x]/(x^3 - 2)$, con lo cual, $\mathbb{Q} \subseteq \mathbb{Q}[x]/(x^3 - 2)$) contiene una raíz de $x^2 - 2$. Si $\exists a_0, a_1, a_2 \in \mathbb{Q}$ no todos cero $\exists a_0 + a_1\alpha + a_2\alpha^2 = 0 \implies -a_0 - a_2\alpha^2 = a_1\alpha \in \mathbb{Q}(\rightarrow\leftarrow) \implies \{1, \alpha, \alpha^2\}$ es linealmente independiente sobre $\mathbb{Q} \implies \{1, \alpha, \alpha^2\}$ es una base para el espacio vectorial $(\mathbb{Q}[X]/(x^3 - 2), +, \cdot, \mathbb{Q}) \implies \dim(\mathbb{Q}[x]/(x^3 - 2), +, \cdot, \mathbb{Q}) = 3 = gr(x^3 - 2)$. Por otro lado, si $a_0, a_1, a_2, b_0, b_1, b_2 \in \mathbb{Q} \ni a_0 + a_1\alpha + a_2\alpha^2 = f(x) + (x^3 - 2) = a_0(x + (x^3 - 2)) + a_1(x + (x^3 - 2)) + a_2(x + (x^3 - 2))^2 = f(x) + (x^2 - 2) = b_0(x^0 + (x^3 - 2)) + b_1(x + (x^3 - 2)) + b_2(x^2 + (x^2 - 2)) \implies (a_0 - b_0)(x^0 + (x^3 - 2)) + (a_1 - b_1)(x + (x^2 - 2)) + (a_2 - b_2)(x^2 + (x^3 - 2)) = (a_0 - b_0) + (a_1 - b_1)x + (a_2 - b_2)x^2 + [x^2 - 2] = [x^3 - 2] = 0 + [x^2 - 2] \implies (a_0 - b_0) + (a_1 - b_1)x + (a_2 - b_2)x^2 \equiv 0 \pmod{(x^2 - 2)} \implies x^3 - 2|(a_0 - b_0) + (a_1 - b_1)x + (a_2 - b_2)x^2 \implies a_0 - b_0 = a_1 - b_1 = a_2 - b_2 = 0 \implies a_0 = b_0, a_1 = b_1$ y $a_2 = b_2 \implies$ todo elemento $f(x) + (x^3 - 2)$ de $\mathbb{Q}[x]/(x^3 - 2)$ de $\mathbb{Q}[x]/(x^3 - 2)$ tiene representación única como polinomio cuadrático en α sobre \mathbb{Q} . Sea $a_0 + a_1\alpha + a_2\alpha^2 \in \mathbb{Q}[x]/(x^2 - 2) - \{(x^3 - 2)\} \implies a_0, a_1$ y a_2 no son todos

cero. El lema 3.22 asegura que $\mathbb{Q}[x]/(x^3 - 2)$ es un campo $\implies \exists b_0, b_1, b_2 \in \mathbb{Q} \ni 1 = (a_0 + a_1\alpha + a_2\alpha^2)(b_0 + b_1\alpha + b_2\alpha^2) = a_0b_0 + a_0b_1\alpha + a_0b_2\alpha^2 + a_1b_0\alpha + a_1b_1\alpha^2 + a_1b_2\alpha^3 + a_2b_0\alpha^2 + a_2b_1\alpha^3 + a_2b_2\alpha^4 = a_0b_0 + a_0b_1\alpha + a_0b_2\alpha^2 + a_1b_0\alpha + a_1b_1\alpha^2 + 2a_1b_2 + a_2b_0\alpha^2 + 2a_2b_1 + 2a_2b_2\alpha = (a_0b_0 + 2a_1 + b_2 + 2a_2b_1) + (a_0b_1 + a_1b_0 + 2a_2b_2) + (a_0b_2 + a_1b_1 + a_2b_0)\alpha^2 \implies$ resolviendo el sistema de ecuaciones... por medio de la regla de Cramer, encontramos que el determinante es $a_0^3 + 2a_1^3 + 4a_2^3 - 6a_0a_1a_2 \neq 0$. Nótese que $a_0 = p_0/q_0, a_1 = p_1/q_1, a_2 = p_2/q_2 \in \mathbb{Q} \ni \dots$

Clase: 23/08/2022

Definición 30. $f(x) = \sum_{i=0}^n a_i x^i \in \mathbb{Z}[x]$ es primitivo si $(a_0, \dots, a_n) = 1$

Lema 32 (3.23). Si $f(x), g(x) \in \mathbb{Z}[x]$ son primitivos, entonces $f(x)g(x)$ es primitivo.

Demostración. Si $f(x) = \sum_{i=0}^n a_i x^i$ y $g(x) = \sum_{j=0}^m b_j x^j$, supóngase que el máximo común divisor de los coeficientes de $f(x)g(x)$ es mayor que 1. $\implies \exists p$, número primo \ni divisor al máximo común divisor de los coeficientes $f(x)g(x)$. Como $f(x)$ es primitivo, $p \nmid (a_0, \dots, a_m) \implies$ sea i^* el índice más pequeño tal que $p \nmid a_{i^*}$. De igual manera, sea j^* el índice más pequeño tal que $p \nmid b_j$. Entonces, el coeficiente de $x^{i^*+j^*}$ en $f(x)g(x)$ es

$$C_{i^*+j^*} = \sum_{k=0}^{i^*+j^*} a_k b_{i^*+j^*-k} = a_{i^*} + b_{j^*} + \sum_{k=0}^{i^*-1} a_k b_{i^*+j^*-k} + \sum_{k=i^*+1}^{i^*+j^*} a_k b_{i^*+j^*-k}.$$

Por la elección de i^* y j^* , $p \mid a_i$ para $0 \leq i < i^*$ y $p \mid b_j$ para $0 \leq j < j^* \implies p \mid a_k b_{i^*+j^*-k}$ para $0 \leq k \leq i^* - 1$ y $p \mid a_k b_{i^*+j^*-k}$ para $i^* + 1 \leq k \leq i^* + j^* \implies p \mid \sum_{k=0}^{i^*-1} a_k b_{i^*+j^*-k}$ y $p \mid \sum_{k=i^*+1}^{i^*+j^*} a_k b_{i^*+j^*-k}$ y por hipótesis, $p \mid c_{i^*+j^*} \implies p \mid (c_{i^*+j^*} - \sum_{k=0}^{i^*-1} a_k b_{i^*+j^*-k} - \sum_{k=i^*+1}^{i^*+j^*} a_k b_{i^*+j^*-k}) = a_{i^*} b_{j^*} \implies p \mid a_{i^*} \text{ o } p \mid b_{j^*} (\rightarrow \leftarrow) \implies f(x)g(x) \text{ es primitivo.}$ ■

Definición 31. El contenido de $f(x) = \sum_{i=0}^n a_i x^i \in \mathbb{Z}[x]$ es (a_0, \dots, a_n) . Notación, $C(f)$.

Proposición 11. Si $f(x) \in \mathbb{Z}[x]$, entonces existe $p(x) \in \mathbb{Z}[x]$, primitivo, tal que $f(x) = C(f)p(x)$.

Teorema 33 (3I - Lema de Gauss). Si $p(x) \in \mathbb{Z}[x]$ es primitivo y puede factorizarse como el producto de dos polinomios con coeficientes racionales, entonces puede factorizarse como el producto de dos polinomios con coeficientes enteros.

Demostración. Si $u(x) = \sum_{i=0}^m \frac{\alpha_i}{\beta_i} x^i, v(x) = \sum_{j=0}^n \frac{\delta_j}{\gamma_j} x_j \in \mathbb{Q}[x]$. Es decir, $\alpha_i, \delta_i \in \mathbb{Z}$ y $\beta_i, \gamma_j \in \mathbb{Z} - \{0\} \exists$

$$\begin{aligned} p(x) &= u(x)v(x) \\ &= \left(\sum_{i=0}^m \frac{\alpha_i}{\beta_i} x^i \right) \left(\sum_{j=0}^n \frac{\delta_j}{\gamma_j} x_j \right) \\ &= \frac{1}{(\prod_{i=0}^m \beta_i) (\prod_{j=0}^n \gamma_j)} \left(\sum_{i=0}^m \alpha_i \left(\prod_{l+i} \beta_l \right) x^i \right) \left(\sum_{j=0}^n \delta_j \left(\prod_{r+j} \gamma_r \right) x^j \right) \end{aligned}$$

Sea $\sigma(x) = \sum_{i=0}^m \alpha_i (\prod_{l+i} \beta_l) x^i, \nu(x) = \sum_{j=0}^n \delta_j (\prod_{r+j} \gamma_r) x^j \in \mathbb{Z}[x] \implies p(x) = 1 / \left((\prod_{i=0}^m \beta_i) (\prod_{j=0}^n \gamma_j) \right) \sigma(x)\nu(x) = \frac{a}{b} q_1(x)q_2(x)$, donde $a = C(\delta)c(\nu) \in \mathbb{Z}, b = (\prod_{i=0}^m p_i) (\prod_{j=0}^n \gamma_j) \in \mathbb{Z} - \{0\}$, sea $q_1(x), q_2(x) \in \mathbb{Z}[x]$ primitivos y $\sigma(x) = C(\sigma)q_1(x)$ y $\nu(x) = C(\nu)q_2(x) \implies$ por el lema 3.23 $q_1(x)q_2(x)$ es primitivo y $bp(x) = aq_1(x)q_2(x)$. Como $p(x)$ es primitivo, el contenido de $bp(x)$ es b y como $q_1(x)q_2(x)$ primitivo. \implies el contenido de $aq_1(x)q_2(x)$ es $a \implies$ como los contenidos de polinomios es iguales de ser iguales, $a = b \neq 0 \implies a/b = 1 \implies p(x) = q_1(x)q_2(x)$.

■

Definición 32. Si $f(x) = \sum_{i=0}^n a_i x^i \in \mathbb{Z}[x]$ y $a_n = 1$, entonces $f(x)$ se dice **Entero Mónico**.

Proposición 12. Todo polinomio mónico de $\mathbb{Z}[x]$ es primitivo.

Corolario 33.1. Si un polinomio mónico de $\mathbb{Z}[x]$ se factoriza como el polinomio en $\mathbb{Q}[x]$, entonces se factoriza como el producto de los polinomios enteros mónicos.

Demostración. Se deduce del lema de Gauss (3I) y la propiedad anterior. ■

Teorema 34 (3J - Criterio de Eisenstein). Si $f(x) = \sum_{i=0}^n a_i x^i \in \mathbb{Z}[x]$ y p es un número primo que $p \nmid a_n$, $p|(a_0, \dots, a_{n-1})$ y $p^2 \nmid a_0$, entonces $f(x)$ es irreducible en $\mathbb{Q}[x]$.

Demostración. Sea $p(x) \in \mathbb{Z}[x]$, primitivo $\exists f(x) = C(f)p(x)$, y nótese que $f(x)$ es irreducible sobre $\mathbb{Q} \iff p(x)$ es irreducible sobre \mathbb{Q} . Además, la hipótesis se cumplen, ya que $(C(f), p) = 1$. Sea $p(x) = \sum_{i=0}^n \alpha_i x^i$, con $p \nmid |\alpha_n, p|(a_0, \dots, a_{n-1})$ y $p^2 \nmid \alpha_0$. Supóngase que $p(x)$ no es irreducible sobre $\mathbb{Q} \implies u(x), v(x) \in \mathbb{Q}[x], gr(u) > 0$ y $gr(v) > 0 \exists p(x) = u(x)v(x) \implies$ por el teorema de Gauss (3I) $\exists r(x) = \sum_{j=0}^{m_1} \beta_j x^j, s(x) = \sum_{k=0}^{m_2} \delta_k x^k \in \mathbb{Z}[x], m_1 = gr(r) > 0$ y $m_2 = gr(s) > 0 \exists \sum_{i=0}^n a_i x^i = p(x) = r(x)s(x) = \sum_{i=0}^{m_1+m_2+m} \left(\sum_{t=0}^i \beta_t \delta_{i-t} \right) x^i$. Entonces, $p|\alpha_0 = \beta_0 \delta_0 \implies p|\beta_0$ o $p|\delta_0$. Pero, $p^2 \nmid \alpha_0 = \beta_0 \delta_0 \implies p|\beta_0$ o $p|\delta_0$. Si $p|(\beta_0, \dots, \beta_{m_1}) \implies p|\beta_{m_1}| \beta_{m_1} \delta_{m_2} = \alpha_{m_1+m_2} = \alpha_n (\rightarrow \leftarrow) \implies$ Sea j^* el primer subíndice tal que $\exists p \nmid \beta_{j^*} \implies$ si $0 \leq j \leq j^* - 1 \implies p|\beta_j$. Pero, $\alpha_{j^*} = \sum_{t=0}^{j^*} \beta_t \delta_{j^*-t}$, entonces $p|\alpha_{j^*}, p|\beta_t| \beta_t | \beta_t \delta_{j^*-t}$ para $0 \leq t \leq j^* - 1 \implies p|\sum_{t=0}^{j^*-1} \beta_t \delta_{j^*-t} \implies p|(\alpha_{j^*} - \sum_{t=0}^{j^*} \beta_t \delta_{j^*-t}) = \beta_{j^*} \delta_0 \implies p|\beta_{j^*}$ o $p|\delta_0 \implies p|\delta_0 \implies p \nmid \beta_0$. Entonces $p(x)$ es irreducible sobre \mathbb{Q} . ■

Clase: 25/08/2022

Proposición 13. Si R es un anillo conmutativo con elemento neutro multiplicativo, entonces $R[x]$ es un anillo conmutativo con elemento neutro multiplicativo.

Demostración. ejercicio. ■

Definición 33. Si R es un anillo conmutativo con elemento neutro multiplicativo, entonces $R[x_1, \dots, x_n]$ se define: $R_1 = R[x]; R_2 = R_1[x_2] = (R[x_1])[x_2] = R[x_1, x_2]; R_3 = R_2[x_3] = ((R[x_1])[x_2])[x_3] = R[x_1, x_2, x_3]; \dots; R_n = R_{n-1}[x_n] = R[x_1, \dots, x_n]$, el anillo de polinomios en las variables x_1, \dots, x_n con coeficientes en R .

Proposición 14. Si R es un anillo conmutativo con elemento neutro multiplicativo, entonces los elementos de $R[x_1, \dots, x_n]$ son de la forma $\sum a_i, \dots, i_n \prod_{j=1}^n x_j^{i_j}$, con $a_i, \dots, i_n \in R$, y la suma de estos polinomios definidos por las operaciones entre coeficientes, y el producto de estos polinomios usando la ley distributiva y las reglas de exponentes $\left(\prod_{j=1}^n x_j^{i_j}\right) \left(\prod_{j=1}^n x_j^{k_j}\right) = \prod_{j=1}^n x_j^{i_j+k_j}$

Lema 35. Si R es un dominio entero, entonces $R[x]$ es un dominio entero.

Demostración. Nótese que en la demostración del lema 3.17 y sus corolarios no se usó la existencia de inversos multiplicativos en el campo F , por lo que esos argumentos son válidos para el dominio entero R . ■

Corolario 35.1. Si R es un dominio entero, entonces $R[x_1, \dots, x_n]$ es un dominio entero.

Demostración. Se deduce del lema 3.24 y la definición de $R[x_1, \dots, x_n]$ ■

NOTA. Si R es dominio entero $\implies R[x_1, \dots, x_n]$ es dominio entero. $\implies R(x_1, \dots, x_n)$ es el campo de las funciones racionales en las variables x_1, \dots, x_n con coeficientes en R . Si F es un campo, en particular es un dominio entero y $F(x_1, \dots, x_n)$ es el campo de las funciones racionales en las variables x_1, \dots, x_n con coeficientes en F , el cual juega un papel importante en Geometría Algebraica y la teoría de Galois.

Ejemplo 12. El teorema 3D dice que si F es un campo, entonces $F[x]$ es un anillo de ideales principales (de hecho, 3F a continuación asegura que $F[x]$ son anillos euclidianos). Ahora, si F es un campo, ¿ $F[x_1, \dots, x_n]$ es también un anillo de ideales principales? Considérese el anillo $\mathbb{Q}[x, y]$, los polinomios $x, y \in \mathbb{Q}[x, y]$ y el conjunto $(x, y) = \{\alpha(x, y)x + \beta(x, y)y : \alpha(x, y), \beta(x, y) \in \mathbb{Q}[x, y]\} \subseteq \mathbb{Q}[x, y]$. Sean $\alpha_1(x, y) + \beta_1(x, y)y, \alpha_2(x, y)x + \beta_2(x, y)y \in (x, y) \implies \alpha_1(x, y)x + \beta_1(x, y)y - (\alpha_2(x, y)x + \beta_2(x, y)y) = (\alpha_1(x, y) - \alpha_2(x, y))x + (\beta_1(x, y) - \beta_2(x, y))y \in (x, y)$, ya que $\alpha_1(x, y) - \alpha_2(x, y), \beta_1(x, y) - \beta_2(x, y) \in \mathbb{Q}[x, y] \implies$ por el corolario al lema 2.3, $((x, y), +)$ es un subgrupo $(\mathbb{Q}[x, y], +)$. Sea ahora $f(x, y) \in \mathbb{Q}[x, y]$ y $\alpha(x, y)x + \beta(x, y)y \in (x, y) \implies f(x, y)(\alpha(x, y) + \beta(x, y)y) = (f(x, y)\alpha(x, y))x + (f(x, y)\beta(x, y))y \in (x, y)$, ya que $f(x, y)\alpha(x, y), f(x, y)\beta(x, y) \in \mathbb{Q} \implies (x, y)$ es un ideal de $\mathbb{Q}[x, y]$.

Supóngase que existe $d(x, y) \in \mathbb{Q}[x, y]$ s.t. $(x, y) = (d(x, y))$. Nótese que si $\alpha(x, y) = 1$ y $\beta(x, y) = 0 \implies x = 1 \cdot x + 0 \cdot y = \alpha(x, y)x + \beta(x, y)y \in (x, y) \implies d(x, y)|x$. Además, si $\alpha(x, y) = 0$ y $\beta(x, y) = 1 \implies y = 0 \cdot x + 1 \cdot y = \alpha(x, y)x + \beta(x, y)y \in (x, y) \implies d(x, y)|y$. Por otro lado, si $\exists g(x, y), h(x, y) \in \mathbb{Q}$ s.t. $x = g(x, y)h(x, y) \implies g(x, y)$ o $h(x, y)$ es constante $\implies x$ es irreducible en $\mathbb{Q}[x, y]$ sobre \mathbb{Q} . Con igual argumento, se sabe que y es irreducible en $\mathbb{Q}[x, y]$ sobre $\mathbb{Q} \implies x, y$ son primos relativos en $\mathbb{Q}[x, y]$ sobre $\mathbb{Q} \implies$ su máximo común divisor es 1. Ahora bien, se demostró que $d(x, y)$ es divisor común de $x, y \implies d(x, y)|1 \implies d(x, y)$ es una unidad $\implies (d(x, y)) = \mathbb{Q}[x, y] \implies 1 \in \mathbb{Q}[x, y] = (x, y) \implies \exists \alpha(x, y), \beta(x, y) \in \mathbb{Q}[x, y] \ni 1 = 0 \cdot x + 0 \cdot y + 1 = \alpha(x, y)x + \beta(x, y)y + 0 \implies 1 = 0(\rightarrow\leftarrow)$ el ideal (x, y) no tiene generador en $\mathbb{Q}[x, y] \implies [x, y]$ no es un anillo de ideales maximales $\implies \mathbb{Q}[x, y]$ no es un anillo euclídeo. Con este ejemplo se puede asegurar que si F es campo, $F[x_1]$ es un anillo euclídeo. pero en general $F[x_1, \dots, x_n], n > 1$ no es un anillo euclídeo.

Por otro lado, el teorema 3E, dice que si F es un campo, entonces $F[x]$ tiene factorización prima única (de hecho, el teorema 3F asegura que $F[x]$ es anillo euclídeo)

Si R es un dominio entero con factorización prima única, ¿ $R[x]$ es también dominio entero con factorización prima única? En caso afirmativo, ¿ $R[x_1, \dots, x_n]$ es también un dominio entero con factorización prima única?

Definición 34. Un dominio entero con elemento neutro multiplicativo es un dominio de factorización única si:

1. Todo elemento de $R - \{0\}$ es una unidad o puede factorizarse como el producto de un número finito de elementos irreducibles (primos) de R .
2. La factorización de (i) es única salvo el orden de los factores y asociación.

Clase: 30/08/2022

Ejemplo 13. El teorema 3.E muestra que todo anillo euclídeo es un dominio de factorización única.

Lema 36 (3.25). Si R es un dominio de factorización única, $r_1, r_2 \in R$ entonces r_1 y r_2 tienen un único (salvo asociación) máximo común divisor $(r_1, r_2) \in R$. Además, si r_1 y r_2 son primos relativos $r_1|r_2r_3$, entonces $r_1|r_3$.

Demostración. Si r_1 o r_2 son unidades, entonces $(r_1, r_2) = 1$ (salvo asociación). Si r_1 y r_2 no son unidades de $R \implies \exists p_1, \dots, p_m, q_1, \dots, q_j \in R$, elementos primos de R , $m, n \in \mathbb{Z}^+$ $\exists r_1 = \prod_{i=1}^m p_i^{\alpha_i}$ y $r_2 = \prod_{j=1}^n q_j^{\beta_j}$, $\alpha_i, \beta_j \in \mathbb{Z}^+$ las factorizaciones primas únicas de r_1 y r_2 en R . Sea $S = \{p_1, \dots, p_m\} \cap \{q_1, \dots, q_n\}$. Si $S = \emptyset \implies (r_1, r_2) = 1$. Si $S = \{s_1, \dots, s_k\} \implies \prod_{l=1}^k s_l^{\delta_l}$, donde $s_l = p_{i_l} = q_{j_l}$ y $\delta_l = \min\{\alpha_{i_l}, \beta_{j_l}\} \implies \prod_{l=1}^k s_l^{\delta_l}|r_1$ y $\prod_{l=1}^k s_l^{\delta_l}|r_2$. Sea $d \in R \ni d|r_1$ y $d|r_2 \implies$ sea $d = \prod_{h=1}^t a_h^{\gamma_h}$, la factorización prima de d en R . Es decir, a_n son elementos primos de R y $\gamma_n \in \mathbb{Z}^+$. Pero $a_h^k|\prod_{h=1}^t a_h^{\gamma_h} = d|r_1 = \prod_{i=1}^m p_i^{\alpha_i} \implies \exists \sigma \in R \ni a_h \sigma = \prod_{i=1}^m p_i^{\alpha_i}$. Sea $\alpha = \prod_{g=1}^r \pi_g^{\nu_g} \implies a_n \prod_{g=1}^r \pi_g^{\nu_g} = \prod_{i=1}^m p_i^{\alpha_i} \implies$ por la unicidad de las factorizaciones primas en R , debe existir $i_n, 1 \leq i - h \leq m \ni a_h = p_{i_n}$. De igual forma $a_n|\prod_{h=1}^t a_h^{\gamma_h} = d|r_2 = \prod_{j=1}^n q_j^{\beta_j} \implies \exists j_n, 1 \leq j_n \leq n \ni a_h = q_{j_n} \implies a_h \in S \implies d|\prod_{g=1}^r s_l^{\delta_l} \implies (r_1, r_2) = \prod_{l=1}^k s_l^{s_l}$, el cual es único en R porque se construyó a partir de la factorización única de r_1 y r_2 . Ahora, si r_1 y r_2 son primos relativos $\implies (r_1, r_2) = 1$. Además, si $r_3 = \prod_{z=1}^{\phi} c_z^{\psi_z}$, la factorización prima única de r_3 en $R \implies \prod_{i=1}^m p_i^{\alpha_i}|\left(\prod_{j=1}^n q_j^{\beta_j}\right)\left(\prod_{z=1}^{\phi} c_z^{\psi_z}\right) \implies$ por la unicidad de las factorizaciones primas en R , cada p_i debe coincidir con algún elemento primo de R en la lista $q_1, \dots, q_n, c_1, \dots, c_{\phi}$. Pero como $(r_1, r_2) = 1 \implies \{p_i\} \cap \{q_1, \dots, q_n\} = \emptyset \implies p_i \in \{c_1, \dots, c_{\phi}\} \implies r_1 = \prod_{i=1}^m p_i^{\alpha_i}|\prod_{z=1}^{\phi} c_z^{\psi_z} = r_3$. ■

Corolario 36.1. Si R es un dominio de factorización única $p, r_1, r_2 \in R$, p elemento primo de R y $p|r_1r_2$, entonces $p|r_1$ o $p|r_2$.

Demostración. Si $p|r_1$ y $p|r_2$, el corolario es válido. Si $p \not|r_1 \implies (p, r_1) = 1 \implies$ por el lema 3.25, $p|r_2$. El caso restante es simétrico. ■

Lema 37 (3.26). Si R es un dominio de factorización única, entonces el producto de dos polinomios primativos en $R[x]$ es también primitivo en $R[x]$.

Demostración. Por la unicidad de la factorización prima en R , la existencia y unicidad de los máximos comunes divisores en R , garantizado por el lema 3.25 y por la propiedad de divisibilidad demostrada también el lema 3.25, los argumentos del lema 3.23, válido para $\mathbb{Z}[x]$, son también válidos para $R[x]$. ■

Corolario 37.1. Si R es un dominio de factorización única y $f(x), g(x) \in R[x]$, entonces $c(fg) = c(f)c(g)$, salvo asociación.

Demostración. Sea $f(x) = c(f)f_1(x)$ y $g(x) = c(g)g_1(x)$, con $f_1(x), g_1(x)$ primos en $R[x] \implies f(x)g(x) = (c(f))f_1(x)(c(g)g_1(x)) = (c(f)c(g))f_1(x)g_1(x) \implies$ por el teorema 2.26 $f_1(x)g_1(x)$ es primo en $R[x] \implies c(f)c(g)$ es el contenido de $(c(f)c(g))f_1(x)g_1(x) = f(x)g(x) \implies c(f)c(g) = c(fg)$. ■

Corolario 37.2. Si R es dominio de factorización única $f_1(x), \dots, f_n(x) \in R[x]$, entonces $c(f_1, \dots, f_n) = \prod_{i=1}^n c(f_i)$, excepto asociación.

Lema 38 (3.27). Si R es un dominio de factorización única, $f(x) \in R[x]$ es primo y F es el campo de cocientes de R . Entonces, $f(x)$ es irreducible en $R[x]$ si y solo si, $f(x)$ es irreducible en $F[x]$.

Demostración. Tenemos

- (\implies) si $f(x)$ es irreducible sobre R , pero $\exists g(x), h(x) \in F[x] \ni gr(g) > 0$ y $gr(h) > 0 \ni f(x) = g(x)h(x) \implies \exists a, b \in R - \{0\}, g_1(x), h_1(x) \in R[x] \ni g(x) = \frac{1}{a}g_1(x)$ y $h(x) = \frac{1}{b}h_1(x) \implies abf(x) = g_1(x)h_1(x)$. Además, $\exists g_2(x), h_2(x) \in R[x]$, primos $\ni g_1(x) = c(g_1)g_2(x)$ y $h_1(x) = c(h_1)h_2(x) \implies abf(x) = c(g_1)c(h_1)g_2(x)h_2(x)$ por el lema 3.26, $g_2(x)$ es primo y $c(g_1)c(h_1)$ es el contenido de $c(g_1)c(g_2)g_2(x)h_2(x) = abf(x)$ y $f(x)$ es primo en $R[x]$, ab es el contenido de $abf(x) \implies c(g_1)c(g_2) = ab \implies f(x) = g_2(x)h_2(x)$. Pero $gr(g_2) = gr(g) > 0$ y $gr(h_2) = gr(h_1) = gr(h) > 0 \implies f(x)$ no es irreducible. ($\rightarrow \leftarrow$) $f(x)$ es irreducible sobre F .

- (\Leftarrow) Si $f(x)$ es irreducible sobre F , pero existen $g(x), h(x) \in R[x] \ni gr(g) > 0, gr(h) > 0$ y $f(x) = g(x)h(x)$, como $R \subseteq F \implies R[x] \subseteq F[x] \implies g(x), h(x) \in F[x]$, $f(x)$ no es irreducible ($\rightarrow \Leftarrow$) $f(x)$ es irreducible sobre R .

■

Clase: 01/09/2022

Lema 39 (3.28). *Si R es un dominio es un dominio de factorización única y $p(x) \in R[x]$ es primitivo, entonces $p(x)$ puede factorizarse de manera única como producto de polinomios irreducibles en $R[x]$.*

Demostración. Sea F el campo de cocientes de $R \implies R \subseteq F \implies R[x] \subseteq F[x] \implies p(x) \in F[x] \implies$ por el lema 3.21, $\exists p_1(x), \dots, p_n(x) \in F[x]$, irreducibles sobre F , $n \in \mathbb{Z}^+$, únicos salvo asociación $\exists p(x) = \prod_{i=1}^n p_i(x)$.

$p_i(x) \in F[x]$, $p_i(x)$ es irreducible sobre F .

$$p_i(x) = \sum_{j=0}^m \frac{a_j}{b_j} x^j, \quad a_j, b_j \in R, b_j \neq 0$$

Además,

$$\begin{aligned} p_i(x) &= \sum_{j=0}^m \frac{a_j}{b_j} x^j \\ &= 1 \cdot \sum_{j=0}^m \frac{a_j}{b_j} x^j \\ &= \frac{\prod_{i=0}^m b_j}{\prod_{j=0}^m b_j} \sum_{j=0}^m \frac{a_j}{b_j} x^j \\ &= \frac{1}{\prod_{j=0}^m b_j} a_j \left(\prod_{k \neq j} b_k \right) x^j \end{aligned}$$

Por el lema 3.25 $\exists q_i(x) \in R[x]$ primitivo sobre R , irreducible sobre F tal que:

$$p_i(x) = \frac{\left(a_0(\prod_{j \neq 0} b_j), \dots, a_m(\prod_{j \neq m} b_j) \right)}{\prod_{j=0}^m b_j} q_i(x)$$

Entonces para cada $p_i(x)$, $\exists f_i(x) \in R[x]$ y $b \in R - \{0\} \ni p_i(x) = \frac{1}{b}f_i(x)$ y $f_i(x)$ es irreducible sobre F . Además, para cada $f_i(x)$, $\exists q_i(x) \in R[x]$, primitivo en $R[x]$, irreducible sobre $F \ni p_i(x) = \frac{c(f_i)}{b_i}q_i(x) \implies$ por el lema 3.27, $q_i(x)$ es irreducible sobre R . Pero $p(x) = \prod_{i=1}^n p_i(x) = \prod_{i=1}^n \frac{c(f_i)}{b_i}q_i(x) = \left(\prod_{i=1}^n \frac{c(f_i)}{b_i}\right)(\prod_{i=1}^n q_i(x))$. Ahora bien, por el lema 3.23, $\prod_{i=1}^n q_i(x)$ es primitivo en $R[x] \implies$ el contenido de $\left(\prod_{i=1}^n \frac{c(f_i)}{b_i}\right)(\prod_{i=1}^n q_i(x))$ es $\prod_{i=1}^n \frac{c(f_i)}{b_i}$ y también debe ser igual al contenido de $p(x)$, que por ser primitivo $1 = c(p) = \prod_{i=1}^n \frac{c(f_i)}{b_i} \implies p(x) = \prod_{i=1}^n q_i(x)$. La unicidad, salvo asociación, de los $q_i(x)$, se deriva de la unicidad de los $p_i(x)$. ■

Teorema 40 (3K). *Si R es un dominio de factorización única, entonces $R[x]$ es un dominio de factorización única.*

Demostración. Por el lema 3.24, $R[x]$ es un dominio entero, y como R tiene elemento neutro multiplicativo, este lo es también de $R[x]$. Sea $f(x) \in R[x] - \{0\} \implies \exists f_1(x) \in R[x] - \{0\}$, primitivo sobre $R \ni f(x) = c(f)f_1(x) \implies$ por el teorema 3.28 $\exists p_1(x), \dots, p_n(x) \in R[x], n \in \mathbb{Z}^+$, todos irreducibles sobre R , únicos salvo asociación $\ni f_i(x) = \prod_{i=1}^n p_i(x) \implies f(x) = c(f)f_1(x) = c(f)\prod_{i=1}^n p_i(x)$. Si $\exists q_1(x), \dots, q_m(x) \in R[x] \ni c(f) = \prod_{i=1}^m q_i(x) \implies 0 = gr(c(f)) = \sum_{i=1}^m \underbrace{gr(q_i)}_{\text{lema 2.17}} \implies gr(q_i) = 0 \implies q_i(x)$ son polinomios constantes \implies la única factorización de $c(f)$ como elemento de $R[x]$ es la misma factorización que tiene como elemento de R , la cual también es única $\implies R[x]$ es un dominio de factorización única. ■

Corolario 40.1. *Si R es un dominio de factorización única, entonces $R[x_1, \dots, x_n]$ es también un dominio de factorización única.*

Demostración. Aplicación sucesiva del teorema 3k en la definición de $R[x_1, \dots, x_n]$. ■

Corolario 40.2. *Si F es un campo, entonces $F[x_1, \dots, x_n]$ es un dominio de factorización única.*

Demostración. F es un dominio de factorización única. ■

2. Teoría de campos

Definición 35. Si F es un campo, un campo K es una extensión de F si $F \subseteq K$, es decir, si F es un subcampo de K .

Definición 36. Si F es un campo y K es una extensión de F , entonces el grado de K sobre F es la dimensión de K como espacio vectorial sobre F .

$[K : F]$, el grado de K sobre F . Si $[K : F] \in \mathbb{Z}^+$, entonces K se dice que una extensión finita de F .

Teorema 41 (5A). Si L es una extensión finita del campo K y K es una extensión finita del campo F , entonces L es una extensión finita de F , $[L : F] = [L : K][K : F]$

Demostración. Sea $\{l_1, \dots, l_{[L:K]}\}$ una base de L sobre K y $\{k_1, \dots, k_{[K:F]}\}$ una base de K sobre F . Sea ahora $l \in L \implies \exists \alpha_1, \dots, \alpha_{[L:K]} \in K \ni l = \sum_{i=1}^{[L:K]} \alpha_i l_i$, pero para cada $i \exists \beta_1, \dots, \beta_{[L_k]} \in F \ni \alpha_i = \sum_{j=1}^{[L:K]} \beta_j k_j \implies l = \sum_{i=1}^{[L:K]} \sum_{j=1}^{[L:K]} \beta_j \alpha_i k_j$. ■

Clase: 06/09/2022

Corolario 41.1. Si F es un campo, L es una extensión finita de F y K es un subcampo de L tal que $F \subseteq K$, entonces $[K : F][L : F]$.

Demostración. Del álgebra lineal, si $F \subseteq K \subseteq L \implies [L : K] \leq [L : F] \in \mathbb{Z}^+ \implies [L : K] \in \mathbb{Z}^+$. Además, $(K, +, \cdot, F)$ es subespacio de $(L, +, \cdot, F) \implies [K : F] \leq [L : F] \in \mathbb{Z}^+ \implies [K : F] \in \mathbb{Z}^+$ por el teorema, 5.A. $[L : K][K : F] = [L : F] \implies [K : F][L : F]$. ■

Corolario 41.2. Si F es un campo, L es una extensión finita de F y $[L : F]$ es un número primo, entonces no existe K extensión de F tal que $F \subset K \subseteq L$; es decir L es la extensión propia de F más pequeña (en el orden parcial de la contención).

Definición 37. Sea F un campo, K una extensión de F , entonces $a \in K$ es algebraico sobre F si existen $n \in \mathbb{Z}^+, \alpha_0, \dots, \alpha_n \in F$, no 0, tales que $\sum_{i=0}^n \alpha_i a^i = 0$.

$a \in K$ es algebraico sobre $F \iff \exists f(x) \in F[x] \ni f(a) = 0$. En donde,

$$f(x) = \sum_{i=0}^n \alpha_i x^i \in F[x], \quad \alpha_0, \dots, \alpha_n \in F$$

Definición 38. Si F es un campo y K es una extensión de F , $f(x) = \sum_{i=0}^n \alpha_i x^i \in F[x]$ y $a \in K$, entonces $f(a) = \sum_{i=0}^n \alpha_i a^i \in K$ es el valor de $f(x)$ en a . Si $f(a) = 0$, entonces se dice que a satisface a $f(x)$ o que a es una raíz de $f(x)$.

Proposición 15. Si F es un campo y K es una extensión de F , entonces $a \in K$ es algebraico sobre F , si existe $f(x) \in F[x] \ni f(a) = 0$.

Proposición 16. Si F es un campo, K es una extensión de F , $a \in K$ y $\mathbb{M} = \{L : L \text{ es una extensión de } F \text{ y } a \in L\}$, entonces:

1. $\mathbb{M} \neq \emptyset$

2. $\bigcap \mathbb{M} \in \mathbb{M}$

Demostración. Tenemos

1. $k \in \mathbb{M} \implies \mathbb{M} \neq \emptyset$

2. $F \subseteq \bigcap \mathbb{M}, a \in \bigcap \mathbb{M}$ y la intersección de campo es campo.

■

NOTA. Notación. Si F es un campo, k es una extensión de F y $a \in K$ entonces $F(a) = \bigcap \{L : L \text{ es una extensión de } F \ni a \in L\}$. La propiedad asegura que $F(a) \neq \emptyset$ y $F(a)$ es la extensión más pequeña de F que contiene a a como uno de sus elementos. En particular, $F \subseteq F(a) \subseteq K$.

Definición 39. Si F es un campo, K es una extensión de F y $a \in K$, entonces $F(a)$ se le llama subcampo de K obtenido por la adjunción de a .

Proposición 17. Si F es un campo, K es una extensión de F y $a \in K$, entonces

$$F(a) = \left\{ \frac{f(a)}{g(a)} \mid f(x), g(x) \in F[x], g(a) \neq 0 \right\}$$

Demostración. Tenemos:

- (\subseteq) Nótese que $\left\{ \frac{f(a)}{g(a)} \mid f(x), g(x) \in F[x], g(a) \neq 0 \right\}$ es una copia isomórfica del campo de las funciones racionales en x sobre F , $F(x) = \left\{ \frac{f(x)}{g(x)} \mid f(x), g(x) \in F[x], g(x) \neq 0 \right\}$. Nótese que si $\alpha \in F \implies$ sean $f(x) = \alpha$ y $g(x) = 1 \in F[x] \implies f(a) = \alpha$ y $g(a) = 1 \implies \alpha = \frac{\alpha}{1} = \frac{f(a)}{g(a)} \in \left\{ \frac{f(a)}{g(a)} \mid f(x), g(x) \in F[x] \text{ y } g(a) \neq 0 \right\} \implies F \subseteq \left\{ \frac{f(a)}{g(a)} \mid f(x), g(x) \in F[x], g(a) \neq 0 \right\}$. Sean $f(x) = x, g(x) = 1 \in F[x] \implies a = \frac{a}{1} = \frac{f(a)}{g(a)} \in \left\{ \frac{f(a)}{g(a)} : f(x), g(x) \in F[x] \text{ y } g(a) \neq 0 \right\}$ es un campo que contiene a F y a a . $\implies F(a) \subseteq \left\{ \frac{f(a)}{g(a)} \mid f(x), g(x) \in F[x], g(a) \neq 0 \right\}$.
- (\supseteq) Sea $\frac{p(a)}{q(a)} \in \left\{ \frac{f(a)}{g(a)} : f(x), g(x) \in F[x] \text{ y } g(a) \neq 0 \right\} \implies \exists m, n \in \mathbb{Z}^+, \alpha_0, \dots, \beta_0, \dots, \beta_n \in F \ni p(x) = \sum_{i=0}^m \alpha_i x^i, q(x) = \sum_{j=0}^n \beta_j x^j, q(a) = \sum_{j=0}^n \beta_j a^j \neq 0$. Ahora bien, $a \in F(a) \implies a^x \in F(a), \forall x \in \mathbb{Z}$. Además, $F \subseteq F(a) \implies \delta \in F(a), \forall \delta \in F \implies \alpha_i a^i, \beta_j a^j \in F(a) \implies f(a) = \sum_{i=0}^m \alpha_i a^i, q(a) = \sum_{j=0}^n \beta_j a^j \in F(a)$ y como $q(a) \neq 0 \implies f(a), \frac{1}{q(a)} \in F(a) \implies \frac{f(a)}{q(a)} \in F(a) \implies \left\{ \frac{f(a)}{g(a)} \mid f(x), g(x) \in F[x], g(a) \neq 0 \right\} \subseteq F(a)$

■

Clase: 08/09/2022

Teorema 42 (5B). Si F es un campo, K es una extensión de F y $a \in K$, entonces es algebraico sobre F si y solo si, $F(a)$ es una extensión finita de F .

Demostración. Tenemos:

- (\implies) Supóngase que a es algebraico sobre $F \implies$ el conjunto de polinomios en $F[x]$ satisfecho por a no es vacío \implies sea $p(x) \in F[x]$, de grado mínimo tal que $p(a) = 0$. Si existen $f(x), g(x) \in F[x] - \{0\}$ tales que $p(x) = f(x)g(x) \implies 0 = p(a) = f(a)g(a)$. Pero $f(a) \in K$, que por ser campo carece de divisores de cero, $f(a) = 0$ o $g(a) = 0$, $gr(f) \geq gr(p)$ o $gr(g) \geq gr(p)$. Pero por otro lado, $p(x) = f(x)g(x) \implies gr(f) \leq gr(p)$ o $gr(g) \leq gr(p) \implies gr(f) = 0$ o $gr(g) = 0 \implies f(x)$ o $g(x)$ es constante en $F[x] \implies p(x)$ es irreducible sobre F . Por el lema 3.22 $[p(x)]$ es un ideal máxima de $F[x] \implies$ por el teorema 3.B, el cociente $F[x]/[p(x)]$ es campo. Sea $f(x) + [p(x)] \in F[x]/[p(x)]$, y por el algoritmo de la división en $F[x]$ (lema 3.17) $\exists q(x), r(x) \in F[x] \ni r(x) = 0$ o $gr(r) < gr(p) \implies \exists \alpha_0, \dots, \alpha_{gr(p)-1} \in F \ni r(x) = \sum_{i=0}^{gr(p)-1} \alpha_i x^i$, tales que $f(x) + [p(x)] = (p(x)q(x) + r(x)) + [p(x)] = [p(x)q(x) + [p(x)]] + [r(x) + [p(x)]] = [p(x)] + [r(x) + [p(x)]] = r(x) + [p(x)] = \sum_{i=0}^{gr(p)-1} a_i x^i + [p(x)] =$

$$p(x)q(x) - 0 = p(x)q(x) \in [p(x)] \implies p(x)q(x) \in [p(x)] \implies p(x)q(x) \equiv 0 \pmod{[p(x)]} \implies p(x)q(x) + [p(x)] = [p(x)]$$

$$= \sum_{i=0}^{gr(p)-1} [\alpha_i x^i + [p(x)]] = \sum_{i=0}^{gr(p)-1} [\alpha_i + [p(x)]] [x^i + [p(x)]] = \sum_{i=0}^{gr(p)-1} [\alpha_i + [p(x)]] [x + [p(x)]]^i.$$

El intento fallido. Sea $\psi : F[x]/[p(x)] \rightarrow F(a) \ni \psi(f(x) + [p(x)]) = f(a)$. Si $f(x) + [p(x)], g(x) + [p(x)] \in F[x]/[p(x)] \ni f(x) + [p(x)] = g(x) + [p(x)] \implies f(x) \equiv g(x) \pmod{[p(x)}} \implies f(x) - g(x) \in [p(x)] \implies \exists q(x) \in F[x] \ni p(x)q(x) = f(x) - g(x) \implies f(x) = g(x) + p(x)q(x) \implies f(a) = \psi[f(x) + [p(x)]] = \psi[(g(x) + p(x) + q(x)) + [p(x)]] = g(a) + p(a)q(a) = g(a) + 0q(a) = q(a) = \psi(g(x) + [p(x)]) \implies \psi$ es una función bien definida.

Además, $\psi[f(x) + [p(x)]] + [g(x) + [p(x)]] = \psi[(f(x) + g(x)) + [p(x)]] = f(a) + g(a) = \psi[f(x) + [p(x)]] + \psi[g(x) + [p(x)]]$ y $\psi[f(x) + [p(x)]] [g(x) + [p(x)]] = \psi[f(x)g(x) + [p(x)]] = f(a)g(a) = \psi[f(x) + [p(x)]] \psi[g(x) + [p(x)]] \implies \psi$ es un homomorfismo.

Sea $\psi : F[x] \rightarrow \psi(F[x])$ es homomorfismo sobrejetivo \implies por el primer teorema de isomorfismos (3A), $F[x]/K_\psi \approx \psi(F[x])$. Ahora bien, $p(x) \in K_\psi \implies (p(x)) \subseteq K_\psi \implies [p(x)] \subseteq K_\psi \subseteq F[x]$, pero siendo $[p(x)]$ un ideal maximal de $F[x]$ y claramente $K_\psi \neq F[x] \implies K_\psi = [p(x)] \implies F[x]/[p(x)] \approx \psi(F[x]) \implies \psi(F[x])$ es un campo $\implies F(a)$ es una extensión de $\psi(F[x])$. Explicitando el isomorfismo de la relación $F[x]/[p(x)] \approx \psi(F[x])$, como $\phi : F[x]/[p(x)] \rightarrow \psi(F[x]) \ni \phi[f(x) + [p(x)]] = \psi[f(x)] = f(a)$, isomorfismo. Entonces, nótese que $\phi(\alpha_i + [p(x)]) = \alpha, \forall \alpha \in F \implies F \subseteq \psi(F[x])$. Además, $\phi(x + [p(x)]) = a \implies a + \psi(F[x]) \implies \psi(F[x])$ es una extensión de F y $a \in \psi(F[x]) \implies F(a) \subseteq \psi(F[x])$. Por lo tanto, $F(a) = \psi(F[x]) \approx F[x]/[p(x)]$. Pero se había demostrado que $f(x) + [p(x)] = \sum_{i=0}^{gr(p)-1} (\alpha_i + [p(x)])(x + [p(x)])^i$, pero $\alpha_i + [p(x)] \approx \alpha_i$ y $x + [p(x)] \approx a \implies f(x) + [p(x)] = \sum_{i=0}^{gr(p)-1} [\alpha_i + [p(x)]] [x + [p(x)]]^i \approx \sum_{i=0}^{gr(p)-1} \alpha_i a^i$ con $\alpha_0, \dots, \alpha_{gr(p)-1} \in F \implies F(a) \approx F[x]/[p(a)] = \langle \{1, \dots, a^{gr(p)-1}\} \rangle_F$. Pero además, si $\beta_0, \dots, \beta_{gr(p)-1} \in F \ni \sum_{i=0}^{gr(p)-1} \beta_i a^i = 0 \implies h(x) = \sum_{i=0}^{gr(p)-1} \beta_i x^i \in F[x]$, de grado a lo más $gr(p) = 1$ y satisfecho por $a \implies h(x) = 0 \implies \beta_0 = \dots = \beta_{gr(p)-1} = 0 \implies \{1, \dots, a^{gr(p)-1}\}$ es l.i en $F(a)$ sobre $F \implies [F(a) : F] = gr(p) \in \mathbb{Z}^+$

- (\implies) Versión 2. Sea $a \in K$ algebraico sobre $F \implies \exists p(x) \in F[x]$, de grado mínimo $\ni p(a) = 0$. Además, supóngase sin pérdida de generalidad que $p(x)$ es mónico. Si $p(x) = \sum_{i=0}^n \alpha_i x^i$ y $q(x) = \sum_{i=0}^n \beta_i x^i, \alpha_n = \beta_n = 1, p(a) = q(a) = 0$ y n es mínimo en $F[x] \implies 0 = \sum_{i=0}^n \alpha_i a^i = \sum_{i=0}^n \beta_i a^i \implies 0 = \sum_{i=0}^n (\alpha_i - \beta_i) a^i = (a^n - a^n) + \sum_{i=0}^{n-1} (\alpha_i - \beta_i) a^i = \sum_{i=0}^{n-1} (\alpha_i - \beta_i) a^i$. Si existe $0 \leq i^* \leq n-1 \ni \alpha_i - \beta_i \neq 0 \implies \sum_{i=0}^{i^*} (\alpha_i - \beta_i) x^i \in F[x]$, satisfecho por a y de grado menor a n ($\rightarrow \leftarrow$) $\implies p(x)$ es único en $F[x]$. Si $p(x) = \sum_{i=0}^{gr(p)} \alpha_i x^i, \alpha_{gr(p)} = 1 \implies 0 = p(a) = \sum_{i=0}^{gr(p)} \alpha_i a^i = a^{gr(p)} +$

$$\sum_{i=0}^{gr(p)-1} \alpha_i a^i \implies a^{gr(p)} = \sum_{i=0}^{gr(p)-1} (-\alpha_i) a^i \implies$$

$$\begin{aligned} a^{gr(p)+1} &= \sum_{i=0}^{gr(p)-1} (-\alpha_i) a^{i+1} \\ &= -\alpha_{gr(p)-1} a^{gr(p)} + \sum_{i=0}^{gr(p)-2} (-\alpha_i) a^{i+1} \\ &= -\alpha_{gr(p)-1} \left(\sum_{i=0}^{gr(p)-1} (-\alpha_i) a^i \right) + \sum_{i=0}^{gr(p)-2} (-\alpha_i) a^{i+1} \\ &= -\alpha_{gr(p)-1} \left(-\alpha_0 + \sum_{i=1}^{gr(p)-1} (-\alpha_i) a^i \right) + \sum_{i=0}^{gr(p)-2} (-\alpha_i) a^{i+1} \\ &= \alpha_{gr(p)-1} \alpha_0 + \sum_{i=1}^{gr(p)-1} \alpha_{gr(p)-1} \alpha_i a^i + \sum_{i=1}^{gr(p)-1} (-\alpha_{i-1}) a^i \\ &= \alpha_{gr(p)-1} \alpha_0 + \sum_{i=1}^{gr(p)-1} (\alpha_{gr(p)-1} \alpha_i - \alpha_{i-1}) a^i \end{aligned}$$

$\implies a^{gr(p)+1}$ es combinación lineal de $\{1, \dots, a^{gr(p)-1}\}$. Un proceso inductivo muestra que si $k \in \mathbb{Z}^+$, $a^{gr(p)+k}$ es combinación lineal de $\{1, \dots, a^{gr(p)-1}\}$. Nótese que $\langle \{1, \dots, a^{gr(p)-1}\} \rangle_F \implies \{a^n : n \in \mathbb{Z}^+\} \subseteq \langle \{1, \dots, a^{gr(p)-1}\} \rangle_F$ es cerrado bajo la suma y el producto en $F(a)$ y por las propiedades de este conjunto, se puede demostrar, $(\langle \{1, \dots, a^{gr(p)-1}\}, +, \dots \rangle)$ es un anillo conmutativo con neutro multiplicativo. Además, si $\alpha \cdot 1 \in \langle \{1, \dots, a^{gr(p)-1}\} \rangle_F \implies F \subseteq \langle \{1, \dots, a^{gr(p)-1}\} \rangle_F$ y claramente $a \in \{1, \dots, a^{gr(p)-1}\} \subseteq \langle \{1, \dots, a^{gr(p)-1}\} \rangle_F$. Sean $\sum_{i=0}^{gr(p)-1} \delta_i a^i \in \langle \{1, \dots, a^{gr(p)+1}\} \rangle_{F-\{0\}}$ y $q(x) = \sum_{i=0}^{gr(p)-1} \delta_i x^i \in F[x] \implies$ como $gr(q) < gr(p) \implies p(x) /| q(x)$. Usando el mismo argumento empleado en la versión de la prueba, se puede demostrar que $p(x)$ es irreducible sobre $F \implies q(x) /| p(x) \implies (p(x), q(x)) = 1 \implies$ por el lema 3.20, $f(x), g(x) \in F[x] \ni 1 = f(x)p(x) + g(x)q(x)$. Pero, $1 = f(a)p(a) + g(a)q(a) = f(a) \cdot 0 + g(a)q(a) = g(a)q(a)$. Si $g(x) = \sum_{j=0}^m \gamma_j x^j \in F[x] \implies g(a) = \sum_{j=0}^m \gamma_j a^j \in \langle \{1, \dots, a^{gr(p)-1}\} \rangle_F \implies 1 = g(a) \sum_{i=0}^{gr(p)-1} \delta_i a^i \implies g(a) = \left(\sum_{i=0}^{gr(p)-1} \delta_i a^i \right)^{-1} \implies \langle \{1, \dots, a^{gr(p)-1}\} \rangle_F$ es campo $\implies \langle \{1, \dots, a^{gr(p)-1}\} \rangle_F$ es una extensión de F que contiene a a $\implies F(a) \subseteq \langle \{1, \dots, a^{gr(p)-1}\} \rangle_F \implies \langle \{1, \dots, a^{gr(p)-1}\} \rangle_F = F(a)$. Si

$\gamma_0, \dots, \gamma_{gr(p)-1} \in F \ni \sum_{i=0}^{gr(p)-1} \gamma_i a^i = 0 \implies$ sea $h(x) = \sum_{i=0}^{gr(p)-1} \gamma_i x^i \in F[x] \ni h(a) = 0$ y $gr(h) \leq gr(p) - 1 \leq gr(p) \implies$ como el $gr(p)$ es el mínimo de los polinomios en $F[x]$ satisfechos por $a \implies h(x) = 0 \implies \gamma_0 = \dots = \gamma_{gr(p)-1} = 0 \implies \{1, \dots, a^{gr(p)-1}\}$ es linealmente independiente en $F(a)$ sobre $F \implies \{1, \dots, a^{gr(p)-1}\}$ es una base pero $F(a)$ sobre $F \implies [F(a) : F] = gr(p) \in \mathbb{Z}^+$.

- (\Leftarrow) Si $[F(a) : F] \in \mathbb{Z}^+ \implies \{1, \dots, a^{[F(a):F]}\}$ por tener $[F(a) : F] + 1$ elementos, es linealmente dependiente en $F(a)$ sobre $F \implies \exists \alpha_0, \dots, \alpha_{[F(a):F]} \in F$, no todos cero $\ni \sum_{i=0}^{[F(a):F]} \alpha_i a^i = 0 \implies$ sea $f(x) = \sum_{i=0}^{[F(a):F]} \alpha_i x^i \in F[x] - \{0\} \ni f(a) = 0 \implies a$ es algebraico sobre F . ■

Clase: 22/09/2022

Definición 40. Si F es un campo y K es una extensión de F , entonces $a \in K$ es **algebraico grado n sobre F** si existe un polinomio no nulo en $F[x]$ de grado $n \in \mathbb{Z}^+$ satisfecho por a , y no existe ningún polinomio en $F[x]$ satisfecho por a de grado menor a n .

Teorema 43 (5C). Si F es un campo, K es una extensión de F y $a \in K$ es algebraico de grado n sobre F , entonces $[F(a) : F] = n$.

Demostración. Úsese la prueba del teorema 5B. ■

Teorema 44 (5D). Si F es un campo, K es una extensión de F y $a, b \in K$ son algebraicos sobre F , entonces $a \pm b, ab$ son algebraicos sobre F . Además, si $b \neq 0$, entonces ab^{-1} es algebraico sobre F . Es decir, el conjunto de elementos de K algebraicos sobre F son un campo.

Demostración. Supóngase que a es algebraico de grado $m \in \mathbb{Z}^+$ sobre F y que b es algebraico de grado $n \in \mathbb{Z}^+$ sobre F . \Rightarrow por el teorema 5.C. $[F(a) : F] = m$. Por otro lado, $F \subseteq F(a) \Rightarrow F \subseteq F(b) \subseteq F(a)(b) \Rightarrow b \in F(a)(b)$ es algebraico de grado a lo más n sobre $F \Rightarrow b \in F(a)(b)$ es algebraico de grado a lo más n sobre $F(a) \Rightarrow$ por teorema 5C $[F(a)(b) : F(a)] \leq n \Rightarrow$ Por teorema 5A, $[F(a)(b) : F(a)][F(a) : F] \leq nm \in \mathbb{Z}^+ \Rightarrow F(a)(b)$ es una extensión finita de F . Ahora bien, $a, b \in F(a)(b) \Rightarrow a \pm b, ab \in F(a)(b)$ y cuando $b \neq 0, ab^{-1} \in F(a)(b) \Rightarrow$ por el teorema 3B, $a \pm b, ab$ son algebraicos sobre F y cuando $b \neq 0, ab^{-1}$ es algebraico sobre F . ■

Corolario 44.1. Si F es un campo, K es una extensión de F , $a \in K$ es algebraico de grado $m \in \mathbb{Z}^+$ sobre F y $b \in K$ es algebraico de grado $n \in \mathbb{Z}^+$ sobre F , entonces $a \pm b, ab$ y cuando $b \neq 0, ab^{-1}$ son algebraicos sobre F de grado a lo más mn .

Demostración. Se deduce directamente de la prueba del teorema 5D. ■

NOTA. Si F es un campo, K es una extensión de F y $a, b \in K$, entonces $F(a, b) = F(a)(b)$ y $F(b, a) = F(b)(a)$.

Proposición 18. Si F es un campo, K es una extensión de F y $a, b \in K$, entonces $F(a, b) = F(b, a)$.

Demostración. Sea $a \in F(a) \Rightarrow a \in F(a)(b)$. Además, $b \in F(a)(b)$ y $F \subseteq F(a) \subseteq F(a)(b) \Rightarrow F(b) \subseteq F(a)(b) \Rightarrow F(b)(a) \subseteq F(a)(b)$. La contención del otro lado es simétrica. ■

NOTA. Si F es un campo, K es una extensión de F y $\alpha_1, \dots, \alpha_n \in K \Rightarrow F(\alpha_1, \dots, \alpha_n)$ es la extensión más pequeña de F que contiene a $\alpha_1, \dots, \alpha_n$.

Definición 41. Si F es un campo, una extensión K de F es algebraica si todos los elementos de K son algebraicos sobre F .

Teorema 45 (5E). Si F es un campo, L es una extensión algebraica de K y K es una extensión algebraica de F , entonces L es extensión algebraica de F .

Demostración. Sea $l \in L \implies \exists k_1, \dots, k_m \in K \ni \sum_{i=0}^m k_i l^i = 0$. Pero k_1 es algebraico sobre $F \implies$ por el teorema 5BC, $[F(k_1) : F] \in \mathbb{Z}^+$. Ahora bien, k_2 es algebraico sobre $F \implies k_2$ es algebraico sobre $F(k_1)$.

⋮

Me cansé xd

■

Definición 42. $a \in \mathbb{C}$ es un número algebraico si es algebraico sobre \mathbb{Q} .

Definición 43. Un número complejo que no es algebraico es trascendente.

Ejemplo 14. e es trascendente

Clase: 27/09/2022

Lema 46 (5.1 (Teorema del residuo)). Si F es un campo, K es una extensión de F , $p(x) \in F[x]$, entonces para todo $k \in K$, existe $q(x) \in K[x]$ tal que $gr(q) = gr(p) - 1$ y $p(x) = (x - k)q(x) + p(k)$

Demostración. Sea $F \subseteq K \implies F[x] \subseteq K[x] \implies p(x) \in K[x]$. Por el lema 3.18 (algoritmo de la división) aplicado a $p(x)$ y $x - k$ en $K[x]$, se tiene que existen $q(x), r(x) \in K[x] \ni p(x) = (x - k)q(x) + r(x)$, donde $r(x) = 0$ o $gr(r) < gr(x - k) = 1$. Pero $p(k) = (k - k)q(k) + r(k) = 0 \cdot q(k) + r(k) = r(k) \in K \implies p(x) = (x - k)q(x) + p(k)$, con $gr(q) = gr((x - k)q(x)) = gr(x - k) + gr(q) = 1 + gr(q) \implies gr(q) = qr(p) - 1$. ■

Corolario 46.1. Si F es un campo, K es una extensión de F , $p(x) \in F[x]$ y $a \in K$ es una raíz de $p(x)$, entonces $(x - a)|p(x)$.

Definición 44. Si F es un campo y K es una extensión de F y $p(x) \in F[x]$, entonces $a \in K$ es una raíz de $p(x)$ de multiplicidad $m \in \mathbb{Z}^+$, cuando $(x - a)^m | p(x)$ y $(x - a)^{m+1} \nmid p(x)$

Lema 47. Un polinomio de grado $n \in \mathbb{Z}^+$ sobre un campo F tiene a lo más n raíces en cualquier extensión de F , contando m raíces en el caso de las raíces de multiplicidad m .

Teorema 48 (5G). Si F es un campo, $p(x) \in F[x]$, $\text{gr}(p) \geq 1$, irreducible sobre F , entonces existe E , extensión de F tal que $[E : F] = \text{gr}(p)$ y E contiene por lo menos una raíz de $p(x)$.

Demostración. Por el lema 3.22, $((p(x)))$ es un ideal maximal de F en $F[x] \implies$ por el teorema 3B, $F[x]/((p))$ es un campo. Si $f(x) + [p(x)] \in F[x]/(p(x))$ con $f(x) \in F[x]$, aplicando el algoritmo de la división en $F[x]$ (lema 3.17), a $f(x)$ y $p(x)$, $\exists q(x), r(x) \in F[x], r(x) = 0$ o $r(x) = \sum_{i=0}^{\text{gr}(p)-1} \alpha_i x^i$, i.e. $\text{gr}(r) < \text{gr}(p) \implies f(x) + [p(x)] = (q(x)p(x) + r(x)) + [p(x)] = [q(x)p(x) + [p(x)]] + [r(x) + [p(x)]] = [0 + [p(x)]] + [r(x) + [p(x)]] = [p(x)] + [r(x) + [p(x)]] = r(x) + [p(x)] = \sum_{i=0}^{\text{gr}(p)-1} \alpha_i x^i + [p(x)] = \sum_{i=0}^{\text{gr}(p)-1} (\alpha_i + [p(x)]) = \sum_{i=0}^{\text{gr}(p)-1} \alpha_i (x^i + [p(x)]) = \sum_{i=0}^{\text{gr}(p)-1} \alpha_i (x + (p(x)))^i \implies F[x]/(p(x)) = \langle \{1, \dots, (x + [p(x)])^{\text{gr}(p)-1}\} \rangle_F$. Sea $\phi : F[x] \rightarrow F[x]/(p(x))$. Si $\beta_0, \dots, \beta_{\text{gr}(p)-1} \in F \ni ((p(x))) = \sum_{i=0}^{\text{gr}(p)-1} \beta_i (x + [p(x)])^i = \left(\sum_{i=0}^{\text{gr}(p)-1} \beta_i x^i\right) + [p(x)]$. Sea $g(x) = \sum_{i=0}^{\text{gr}(p)-1} \beta_i x^i \in F[x] \implies [p(x)] = g(x) + [p(x)] \implies g(x) \in [p(x)] \implies p(x)|g(x) \implies \text{gr}(p) - 1 \geq \text{gr}(q) \geq \text{gr}(p) \implies p(x) = 0 \implies \beta_0 = \dots = \beta_{\text{gr}(p)-1} \implies \{1, \dots, (x + [p(x)])^{\text{gr}(p)-1}\}$ es linealmente independiente en $F[x]/(p(x))$ sobre $F \implies \{1, \dots, (x + [p(x)])^{\text{gr}(p)-1}\}$ es una base de $F[x]/(p(x))$ sobre F . Nótese que además, $p(x + [p(x)]) = p(x) + [p(x)] = 0 + [p(x)] = [p(x)] \implies x + [p(x)] \in F[x]/(p(x))$ es una raíz de $p(x)$. Si $\phi : F \rightarrow F[x]/(p(x)) \ni \phi(\alpha) = \alpha + [p(x)]$ y nótese que $\phi(\alpha_1 + \alpha_2) = (\alpha_1 + \alpha_2) + [p(x)] = (\alpha + [p(x)]) + (\alpha_2 + [p(x)]) = \phi(\alpha_1) + \phi(\alpha_2)$ y $\phi(\alpha_1 \alpha_2) = \alpha_1 \alpha_2 + [p(x)] = (\alpha_1 + [p(x)]) (\alpha_2 + [p(x)]) = \phi(\alpha_1) \phi(\alpha_2) \implies \phi$ es un homomorfismo. Sea $\alpha \in K_\phi \implies \phi(\alpha) = \alpha + [p(x)] = [p(x)] \implies \alpha \in [p(x)] \implies p(x)|\alpha \implies \alpha = 0 \implies K_\phi = (0) \implies \phi$ es inyectivo F está inmerso en $F[x]/(p(x)) \implies$ salvo isomorfismo, $F \subseteq F[x]/(p(x))$ y $F[x]/(p(x))$ es la extensión de F requerida. Si $E = F[x]/(p(x)) \implies [E : F] = \text{gr}(p)$ y E contiene una raíz de $p(x)$. ■

Corolario 48.1. Si F es un campo, $f(x) \in F[x]$, entonces existe una extensión E de F , finita, tal que contiene por lo menos una raíz de $f(x)$ y $[E : F] \leq \text{gr}(f)$.

Demostración. Si F contiene a todas las raíces de $f(x)$, entonces $E = F$ y $[E : F] = [F : F] \leq gr(f)$. Si $p(x)$ es un factor de $f(x)$, irreducible sobre F , entonces por el teorema 5.G existe E , extensión de F , tal que contiene una raíz de $p(x)$ y por lo tanto, también de $f(x)$ y $[E : F] = gr(p) \leq gr(f)$. ■

Definición 45. Si F es un campo y $f(x) \in F[x]$, E es un campo de descomposición de $f(x)$ sobre F , si E es una extensión finita de F en la que $f(x)$ puede factorizarse como producto de polinomios lineales sobre E , y esta factorización no es posible sobre ningún subcampo propio de E .

Es decir, E es un campo de descomposición de $f(x)$ sobre F , si E es una extensión finita de F que contiene a todas las raíces de $f(x)$ y $[E : F]$ es mínimo.

Ejemplo 15. Tenemos

$$x^3 - 2 \in \mathbb{Q}(\sqrt[3]{2})[x]$$

en donde:

$$x^3 - 2 = (x - \sqrt[3]{2})(x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2)$$

en donde $a_2x^2 + a_1x + a_0$ es irreducible sobre $\mathbb{Q}(\sqrt[3]{2})$, por el teorema 5.B.C.G
 $\implies \exists E$ extensión de $\mathbb{Q}(\sqrt[3]{2}) \ni \alpha_1 = x + (x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2) \in \mathbb{Q}[x]/(x^2 + \sqrt[3]{2}x + (\sqrt[3]{2})^2) \sim \mathbb{Q}(\sqrt[3]{2})(\alpha_1)$. Tenemos:

$$[\mathbb{Q}(\sqrt[3]{2})(\sqrt[3]{2}w) : \mathbb{Q}(\sqrt[3]{2})] = 2$$

$$[\mathbb{Q}(\sqrt[3]{2}, \sqrt[3]{2}w) : \mathbb{Q}] =$$

Teorema 49 (5H-Existencia de los campos de descomposición). Si F es un campo, $f(x) \in F[x]$ y $gr(f) \geq 1$, entonces existe una extensión de F , de grado a lo más $gr(f)!$ tal que contiene a las $gr(f)$ raíces de $f(x)$.

Demostración. Procediendo por inducción sobre $gr(f)$:

1. Si $gr(f) = 1 \implies f(x) = a_1x + a_0$, con $a_1, a_0 \in F, a_1 \neq 0 \implies -a_0/a_1 \in F$ es raíz de $f(x) \implies F$ es la extensión requerida de F , con $[F : F] = 1$.
 2. Supóngase el teorema válido para todos los polinomios en $F[x]$ de grado menor a $gr(f)$.
 3. Por el corolario al teorema 5G, existe E_0 extensión de F , $[E_0 : F] \leq gr(f)$ y $\exists \alpha \in E_0 \ni f(\alpha) = 0 \implies$ por el teorema del residuo (lema 3.1) y su corolario, $\exists q(x) \in E_0[x] \ni (x - \alpha)q(x) = f(x) \implies gr(f) = gr(x - \alpha) + gr(q) = 1 + gr(q) > gr(q) \implies$ por la hipótesis inductiva, $\exists E$, extensión de E_0 , $[E : E_0] \leq gr(q)!$ y todas las raíces de $q(x)$ están contenidas en E . Ahora bien, $\alpha \in E_0 \subseteq E \implies \alpha \in E \implies E$ contiene a todas las raíces de $f(x)$. Además, por el teorema 3A, $[E : F] = [E : E_0][E_0 : F] \leq ((gr(f) - 1)!)gr(f)!$
-

NOTA. Si F es un campo y $f(x) \in F[x]$, el teorema 5H garantiza la existencia de E , extensión de F , que contiene a todas las raíces de $f(x)$ y $[E : F] \leq gr(f)!$ $\implies \{E : [E : F] \in \mathbb{Z}^+ \text{ y todas las raíces de } f(x) \text{ están contenidas en } E\} \neq \emptyset \implies$ existe un elemento de este conjunto $\exists [E : F]$ es mínimo, y en ese caso, un campo de descomposición de $f(x)$ sobre F .

NOTA. Se verá más adelante que existen campos F y polinomios $f(x) \in F[x]$, cuyos campos de descomposición E sobre F alcanzan la cota superior $[E : F] = gr(f)!$. Por ejemplo, $x^3 - 2 \in \mathbb{Q}[x]$, se demostrará que si E es el campo de descomposición de $x^3 - 2$ sobre \mathbb{Q} entonces $[E : \mathbb{Q}] = 6 = 3! = gr(x^3 - 2)!$

NOTA. Si F es un campo, $f(x) \in F[x]$ y E_1, E_2 son campos de descomposición de $f(x)$ sobre F . ¿Existe alguna relación entre E_1 y E_2 ?

Clase: 24/11/2022

Lema 50 (5.3). Si F y F' son campos, $\tau : F \rightarrow F'$ es un isomorfismo, entonces $\tau^* : F[x] \rightarrow F'[t] \ni f(x) = \sum_{i=0}^n \alpha_i x^i \in F[x] \rightarrow \tau^*(f(x)) = \tau * (\sum_{i=0}^n \alpha_i x^i) = \sum_{i=0}^n \tau(\alpha_i)t^i = \sum_{i=0}^n \alpha'_i t^i$.

Demostración. Si $f(x) = \sum_{i=0}^m \alpha_i x^i, g(x) = \sum_{j=0}^n \beta_j x^j \in F[x] \implies$

$$\begin{aligned}
\tau^*(f(x) + g(x)) &= \tau^*\left(\sum_{i=0}^m \alpha_i x^i + \sum_{j=0}^n \beta_j x^j\right) \\
&= \tau^*\left(\sum_{k=0}^{\max(m,n)} (\alpha_k + \beta_k) x^k\right) \\
&= \sum_{k=0}^{\max(m,n)} \tau(\alpha_k + \beta_k) t^k \\
&= \sum_{k=0}^{\max(m,n)} (\tau(\alpha_k) + \tau(\beta_k)) t^k \\
&= \sum_{k=0}^{\max(m,n)} (\alpha'_k + \beta'_k) t^k = \sum_{i=0}^m \alpha'_i t^i + \sum_{j=0}^n \beta'_j t^j \\
&= \sum_{i=0}^m \tau(\alpha_i) t^i + \sum_{j=0}^n \tau(\beta_j) t^j \\
&= \tau^*\left(\sum_{i=0}^m \alpha_i x^i\right) + \tau^*\left(\sum_{j=0}^n \beta_j x^j\right) = \tau^*(f(x)) + \tau^*(g(x))
\end{aligned}$$

Además,

$$\begin{aligned}
\tau^*(f(x)g(x)) &= \tau^*\left(\left(\sum_{i=0}^m \alpha_i x^i\right) \left(\sum_{j=0}^n \beta_j x^j\right)\right) \\
&= \tau^*\left(\sum_{k=0}^{m+n} \left(\sum_{l=0}^k \alpha_l \beta_{k-l}\right) x^k\right) \\
&= \sum_{k=0}^{m+n} \tau\left(\sum_{l=0}^k \alpha_l \beta_{k-l}\right) t^k \\
&= \sum_{k=0}^{m+n} \left(\sum_{l=0}^k \tau(\alpha_l) \beta_{k-l}\right) t^k \\
&= \sum_{k=0}^{m+n} \left(\sum_{l=0}^k \tau(\alpha_l) \tau(\beta_{k-l})\right) t^k \\
&= \dots \\
&= \tau^*\left(\sum_{i=0}^m \alpha_i x^i\right) \tau^*\left(\sum_{j=0}^n \beta_j x^j\right)
\end{aligned}$$

Entonces τ^* es homomorfismo.

Si $f(x) \in K_{\tau^*} \implies 0 = \tau^*(f(x)) = \tau^*(\sum_{i=0}^m \alpha_i x^i) = \sum_{i=0}^m \tau(\alpha_i)t^i \implies 0 = \tau(\alpha_0) = \dots = \tau(\alpha_m) \implies$ como τ es isomorfismo, $0 = \alpha_0 = \dots = \alpha_m \implies f(x) = 0 \implies K_{\tau^*} = 0 \implies$ por lema 3.5 , τ^* es inyectivo.

Si $f(t) \in F'[t] \implies \exists \alpha'_0, \dots, \alpha'_m \in F' \ni f(t) = \sum_{i=0}^m \alpha'_i t^i \implies$ por la sobre-
yectividad de τ , $\exists \alpha_0, \dots, \alpha_m \in F \ni \tau(\alpha_0) = \alpha'_0, \dots, \tau(\alpha_m) = \alpha'_m \implies f(x) = \sum_{i=0}^m \alpha_i x^i \in F[x] \ni \tau^*(f(x)) = \tau^*(\sum_{i=0}^m \alpha_i x^i) = \sum_{i=0}^m \tau(\alpha'_i)t^i = \sum_{i=0}^m \alpha'_i t^i = f(t) \implies \tau^*$ es sobreyectivo. $\implies \tau^*$ es isomorfismo. ■

NOTA. En los teoremas 5BCG se recurrió al cociente $F[x]/(p(x))$ para obtener una extensión finita de F que contenga una raíz de $p(x)$. Por esta razón se estudiará la relación entre los cocientes entre el anillo $F[x]/(f(x))$ y $F'[t]/(f(t))$ cuando $F[x] \sum F'[t]$

Lema 51 (5.4). Si F y F' son campos, τ y τ^* definidos como en el lema 5.3, entonces $\tau^{**} : F[x]/(f(x)) \rightarrow F'[t]/(f'(t))$, isomorfismo, tal que $\tau^{**}(\alpha) = \tau(\alpha) = \alpha'$, $\forall \alpha \in F$.

Demostración. Considérese la identificación isomorfica $\alpha \approx \alpha + [f(x)]$, $\forall \alpha \in F$ y con ello $F \subseteq F[x]/((f(x)))$. De manera similar, $\alpha' \approx \alpha' + [f'(t)]$, $\forall \alpha' \in F' \implies F' \subseteq F'[t]/(f'(t))$. Sea $\tau^{**} : F[x]/(f(x)) \rightarrow F'[t]/(f'(t)) \ni \tau^{**}(g(x) + [f(x)]) = \tau^{**}(g(x)) + [f'(t)] = g'(t) + [f'(t)]$ y nótense que si $\alpha \in F \implies \tau^{**}(\alpha) = \tau^{**}(\alpha + [f(x)]) = \tau'(\alpha) + [f'(t)] = \tau(\alpha) + [f'(t)] = \alpha' + [f'(t)] \approx \alpha'$.

Demostrar que está bien definido, si $g_1(x), g_2(x) \in F[x] \ni g_1(x) + [f(x)] = g_2(x) + [f(x)] = g_1(x) \equiv g_2(x) \text{ mód } (f(x)) \implies g_1(x) - g_2(x) \in (f(x)) \implies f(x)|g_1(x) - g_2(x) \implies \exists q(x) \in F[x] \ni f(x)q(x) = g_1(x) - g_2(x) \implies f'(t)q'(t) = \tau^*(f(x))\tau^*(q(x)) = \tau^*(f(x)q(x)) = \tau^*(g_1(x) - g_2(x)) = \tau^*(g_1(x)) - \tau^*(g_2(x)) = g'_1(t) - g'_2(t) \implies f'(t)|g'_1(t) - g'_2(t) \implies g'_1(t) - g'_2(t) \in (f'(t)) \implies g'_1(t) \equiv g'_2(t) \text{ mód } (f'(t)) \implies \tau^*(g(t) + [f(x)]) = \tau^*(g_1(x)) + (f'(t)) = g'_1(t) + [f'(t)] = g'_2(t) + [f'(t)] = \tau^*(g_2(x)) + (f'(t)) = \tau^{**}(g_2(x) + f(x)) \implies \tau^{**}$ es una función bien definida.

Homomorfismo. Si $g_1(x), g_2(x) \in F[x]$ \implies
 $\tau^{**}((g_1(x) + [f(x)]) + (g_2(x) + [f(x)])) = \tau^{**}((g_1(x) + g_2(x)) + [f(x)]) =$
 $\tau^*(g_1(x) + g_2(x)) + [f'(t)] = \tau^*(g_1(x)) + \tau^*(g_2(x)) + [f'(t)] = (g'_1(t) + g'_2(t)) + [f'(t)] =$
 $g'(t) + [f'(t)] + g'_2(t) + [f'(t)] = \tau^*(g_1(x)) + [f'(t)] + \tau^*(g_2(x) + [f'(t)]) = \tau^{**}(g_1(x) +$
 $[f(x)]) + \tau^{**}(g_2(x) + [f(x)]). Además, \tau^{**}((g_1(x) + [f(x)])(g_2(x) + [f(x)])) =$
 $\tau^{**}(g_1(x)g_2(x) + [f(x)]) = \tau^*(g_1(x)g_2(x)) + [f'(t)] = \tau^*(g_1(x))\tau^*(g_2(x)) + [f'(t)] =$
 $\dots = \tau^{**}(g_1(x) + [f(x)])\tau^{**}(g_2(x) + [f(x)]) \implies \tau^{**}$ es homomorfismo.

Sea $f(x) + [f(x)] \in K_{\tau^{**}} \implies (f'(t)) = \tau^{**}(g(x) + [f(x)]) = \tau^*(g(x)) + [f'(t)] =$
 $g'(t) + [f'(t)] \implies g'(t) \in (f'(t)) \implies f'(t)|g'(t) \implies \exists q'(t) \in F'[t] \ni$
 $f'(t)q'(t) = g'(t)$. Por la sobreyectividad de τ^* , $\exists q(x) \in F[x] \ni \tau^*(q(x)) =$
 $q'(t) \implies f(x)q(x) = (\tau^*)^{-1}(f'(t))(\tau^*)^{-1}(q'(t)) = (\tau^*)^{-1}(f'(t)q'(t)) =$
 $(\tau^*)^{-1}(g'(t)) = g(x) \implies f(x)|g(x) \implies g(x) \in (f(x)) \implies g(x) + [f(x)] =$
 $[f(x)] \implies K_{\tau^{**}} = (f(x)) \implies$ por el lema 3.5, τ^{**} es inyectivo.

Si $g'(t) + (f'(t)) \in F'[t]/(f'(t)) \implies g'(t) \in F'[t]$ y por la sobreyectividad
de $\tau^* \ni g(x) \in F[x] \ni \tau^*(g(x)) = g'(t) \implies g(x) + [f(x)] \in F[x]/(f(x)) \ni$
 $\tau^{**}(g(x) + [f(x)]) = \tau^*(g(x)) + (f'(t)) = g'(t) + [f'(t)] \implies \tau^{**}$ es sobreyectivo.
 $\implies \tau^{**}$ es isomorfismo. ■

Lema 5.4 es un lema de presentación más avanzada de teoría de anillos.

Clase: 25/11/2022

Teorema 52 (5I). Si F y F' son campos, $\tau : F \rightarrow F'$ es un isomorfismo,
 $p(x) \in F[x]$ es irreducible sobre F y v es una raíz de $p(x)$, entonces existe
 $\sigma : F(v) \rightarrow F'(w)$, isomorfismo, donde w es una raíz de $p'(t) = \tau^*(p(x))$, y este
isomorfismo σ puede elegirse tal que:

1. $\sigma(v) = w$
2. $\sigma(\alpha) = \tau(\alpha) = \alpha'$, $\forall \alpha \in F$. Es decir, σ deja fijos (salvo el isomorfismo) a
los elementos de F

Demostración. Considere $M = \{f(x) \in F[x] : f(v) = 0\}$. Si $f_1(x), f_2(x) \in M \implies f_1(v) - f_2(v) = 0 - 0 = 0 \implies f_1(x) - f_2(x) \in M \implies$ por el corolario al lema 2.3 ($M, +$) es subgrupo de $(F[x], +)$. Si $g(x) \in F[x]$ y $f(x) \in M \implies g(v)f(v) = g(v) = 0 = 0 \implies g(x)f(x) \in M \implies M$ es un ideal de $F[x]$. Además, $p(v) = 0 \implies p(x) \in M \implies (p(x)) \subseteq M$. Como existen polinomios en $F[x]$, no satisfechos por $v \implies M \subset F[x]$, no satisfechos por $v \implies M \subset F[x]$. Pero, siendo $p(x)$ irreducible sobre F , por el lema 3.22, $(p(x))$ es un ideal maximal en $F[x] \implies M = (p(x))$. Considerese el homomorfismo $\psi : F[x] \rightarrow F[v] \ni \psi(f(x)) = f(v)$ empleando los argumentos de la prueba de los teoremas 5.B.C.G, ψ es un homomorfismo $\exists K_\psi = M = (p(x))$ y existe $\psi^* F[x]/(p(x)) \rightarrow F(v) \ni \psi^*(f(x) + [p(x)]) = f(v)$, isomorfismo.

$$F[x]/(p(x)) \approx F(v)$$

$F[x] \xrightarrow{\psi} \Psi(F[x]) \subseteq F(v)$

$\phi \downarrow \quad \delta \nearrow$

$F[x]/(p(x))$

1er teorema de isomorfismos
δ es surtivo

S.B. $\left\{ \begin{array}{l} F[x]/(p(x)) \subseteq F(v) \\ \text{Si } d \in F \Rightarrow d \approx dt \text{ en } (p(x)) \in F[x]/(p(x)) \Rightarrow F \subseteq F[x]/(p(x)) \quad \left| \quad F(v) \subseteq F[x]/(p(x)) \right. \\ v \approx x + (p(x)) \in F[x]/(p(x)) \Rightarrow v \in F[x]/(p(x)) \end{array} \right. \quad \text{Teorema 3.B: } F[x]/(p(x)) \text{ es campo}$

Como $p(x)$ es irreducible en $F[x]$ y por el lema 5.3 $\tau^* : F[x] \rightarrow F'[t]$ es un isomorfismo entonces $\tau^*(p(x)) = p'(t)$ es irreducible en $F'[t]$. Entonces replicando los argumentos ya usados, existe $\theta^* : F'[t]/(p'(t)) \rightarrow F(w) \ni \theta^*(f'(t) + [p'(t)]) = f'(w)$, isomorfismo. Además, por el lema 5.4, $\tau^{**} : F[x]/(p(x)) \rightarrow F'[t]/(p'(t)) \ni \tau^{**}(f(x) + [p(x)]) = f'(t) + (p'(t))$ es un isomorfismo de campos $\exists \alpha \in F \implies$

$\tau^{**}(\alpha) \approx \tau^{**}(\alpha + (p(x))) = \tau(\alpha) + (p'(t)) = \alpha' + (p'(t)) \approx \alpha'$ y $\tau^{**}(x + (p(x))) = \tau^*(x) + (p'(t)) = t + (p'(t))$. Considérese el siguiente diagrama:

$$\begin{array}{ccc}
 F[x] / (p(x)) & \xrightarrow{\tau^{**}} & F[t] / (p'(t)) \\
 \downarrow \psi^* & & \downarrow \theta^* \\
 F(v) & \dashrightarrow & F'(w)
 \end{array}$$

■

Si $F = F'$ (automorfismo), y donde $\sigma : F(v) \rightarrow F(w)$ y más precisamente $\sigma|_F = I_F$

y la función $\sigma = (\psi^*)^{-1}\tau^{**}\theta^* : F(v) \rightarrow F'(w)$, un isomorfismo, por ser la composición de isomorfismos. Nótese que $\sigma(v) = (\psi^*)^{-1}\tau^{**}\theta^{**}(v) = \theta^{**}(\tau^{**}(\psi^{*-1}(v))) =_{5B} \theta^{**}(\theta^{**}(x + (p(x)))) = \theta^{**}(t + (p'(t))) = w$ y si $\alpha \in F \implies \sigma(\alpha) = \psi^{*-1}\tau^{**}\theta^{**}(\alpha) = \theta^{**}(\theta^{**}(\psi^{*-1}(\alpha))) = \theta^{**}(\tau^{**}(\alpha + p(w))) = \theta^{**}(\tau^*(\alpha) + (p'(t))) =_{5,3} \theta^{**}(\tau(\alpha) + p'(t)) = \theta^{**}(\alpha' + (p'(t))) = \alpha'$.

Corolario 52.1. Si F es un campo, $p(x) \in F[x]$ es irreducible sobre F y a, b son raíces de $p(x)$ entonces existe $\sigma : F(a) \rightarrow F(b)$, isomorfismo, tal que $\sigma(a) = b$ y $\sigma(\alpha) = \alpha$, $\forall \alpha \in F$.

Demostración. Aplíquese el teorema 5I al caso especial $F = F'$ y $\tau = I_F$. ■

Clase: 13/11/2022

Teorema 53 (5J- Unicidad de los campos de descomposición). *Si F y F' son campos, τ, τ^* y τ^{**} definidos como en los lemas 5.3 y 5.4 $f(x) \in F[x]$, $f'(t) = \tau^*(f(x)) \in F'[t]$, E es un campo de descomposición de $f(x)$ sobre F y E' es un campo de descomposición de $f'(t)$ sobre F' , entonces existe $\phi : E \rightarrow E'$, isomorfismo tal que $\phi(\alpha) = \tau(\alpha) = \alpha', \forall \alpha \in F$*

Demostración. Procediendo sobre $[E : F]$:

1. $[E : F] = 1 \implies E$ es un espacio vectorial de dimensión 1 sobre $F \implies \exists \{a\} \subseteq E \ni \{a\}$ es base de E sobre $F \implies$ como $E \neq \{0\}, a \neq 0$ y además como $E = \langle \{a\} \rangle_F$ y $1 \in E \implies \exists \alpha \in F - \{0\} \ni 1 = \alpha a \implies a = \alpha^{-1} \cdot 1 = \alpha^{-1} \in F \implies F = \langle \{a\} \rangle_F = E \implies F = E$ es campo de descomposición de $f(x)$ sobre F . Sea $\phi = \tau \implies E = F \approx F'$. Por el lema 5.3, por lo que τ^* es un isomorfismo $\implies f(x)$ y $f'(t)$ tienen las mismas raíces, salvo $\tau^* \implies F'$ contiene a todas las raíces de $f'(t) \implies E' \subseteq F'$. Pero E' es extensión de $F' \implies E' = F'$. Sea $\phi = \tau$, el isomorfismo requerido y $E \approx E'$.
2. Supóngase el teorema válido para todos los polinomios $g(x) \in F_0[x]$ con campo de descomposición E_0 sobre F_0 tales que $[E_0 : F_0] < [E : F]$, si E'_0 es el campo de descomposición de $g'(t) = \tau^*(g(x))$, entonces $E_0 \approx E'_0$ y $[E_0 : F'_0] = [E'_0 : F'_0]$.
3. Si $[E : F] > 1 \implies$ existen raíces de $f(x)$ que no pertenecen a $F \implies \exists p(x) \in F[x]$ irreducible sobre $F \ni p(x) | f(x)$ y $1 < gr(p) \leq gr(f) \implies$ por el lema 5.3, τ^* es isomorfismo $p'(t) = \tau^*(p(x))$ es un factor irreducible de $f'(t)$ y $1 < gr(p') = gr(p) \leq gr(f) = gr(f')$. Sea $v \in E$ una raíz de $p(x) \implies$ por el teorema 5.C, $[F(v) : F] = gr(p)$. Sea $w \in E'$ una raíz de $p'(t) \implies$ por el teorema 5.I, $\exists \sigma : F(v) \rightarrow F'(w)$ isomorfismo y es tal que $\sigma(v) = w$ y $\sigma(\alpha) = \tau(\alpha) = \alpha'$. Por el teorema 5.A, $[E : F] = [E : F(v)][F(v) : F]$ y como $[F(v) : F] = gr(p) > 1 \implies [E : F(v)] = [E : F]/[F(v) : F] < [E : F]$. Considérese ahora a $f(x) \in F(v)[x]$. Si E no es campo de descomposición de $f(x)$ sobre $F(v) \implies$ por el teorema 5.H $\exists E_1$ campo de descomposición de $f(x)$ sobre $F(v) \implies [E : F(v)] > [E_1 : F(v)] \implies$ por el teorema 5.A, $[E : F] = [E : F(v)] > [E_1 : F(v)][F(v) : F] = [E_1 : F] \implies E$

no es campo de descomposición de $f(x)$ sobre $F(\rightarrow\leftarrow) \implies E$ es campo de descomposición de $f(x)$ sobre $F(v)$. Replicando este argumento, E' es campo de descomposición de $f'(t)$ sobre $F'(w)$. Aplicando la hipótesis inductiva a $f(x) \in F(v)[x]$, E es campo de descomposición de $f(x)$ sobre $F(v)$ y $[E : F(v)] < [E : F]$, entonces existe $\phi : E \rightarrow E'$, isomorfismo $\exists \phi(\alpha) = \tau(\alpha) = \alpha', \forall \alpha \in F$.

■

NOTA. En particular, si $F = F'$ y $\tau = I_F$, $f(x) \in F[x]$ y E_1, E_2 son campos de descomposición de $f(x)$ sobre F , el teorema 5J asegura la existencia de $\phi : E_1 \rightarrow E_2$, isomorfismo $\exists \phi|_F = I_F$

Clase: 18/11/2022

Ejemplo 16. 1. Si F es un campo, sea $p(x) = x^2 + \alpha x + \beta \in F[x]$. Sean K una extensión de F y $a_1 \in K \ni p(a_1) = 0 \implies a_2 = -\alpha - a_1 \in K$ es también raíz de $p(x)$. En efecto,

$$\begin{aligned} p(a_2) &= a_2^2 + \alpha a_2 + \beta \\ &= (-\alpha - a_1)^2 + \alpha(-\alpha - a_1) + \beta \\ &= \alpha^2 + 2\alpha a_1 + a_1^2 - \alpha^2 - \alpha a_1 + \beta \\ &= a_1^2 - \alpha a_1 + \beta = 0 \end{aligned}$$

Entonces K contiene el campo de descomposición de $p(x)$. Si $a_2 = a \implies p(x) = (x - a_1)(x - a_2) = (x - a_1)^2 = x^2 - 2a_1 x + a_1^2 \in F[x] \implies -2a_1 \in F \implies F$ es el campo de descomposición de $p(x)$. Nótese que estos hechos confirman el teorema 5H.

2. $x^3 - 2 \in \mathbb{Q}[x]$. Se sabe que si $w = -1/2 - \sqrt{3}/2i \implies$ las raíces de $x^3 - 2$ son $\sqrt[3]{2}, \sqrt[3]{2}w, \sqrt[3]{2}w^2 \in \mathbb{C} - \mathbb{Q} \implies x^3 - 2$ es irreducible sobre $\mathbb{Q} \implies$ por el teorema 5C, $[\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = 3$. Si E es el campo de descomposición de $x^3 - 2$ sobre $\mathbb{Q} \implies$ por el teorema 5H, $6 = 3! = \text{gr}(x^3 - 2) \geq [E : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt[3]{2})][\mathbb{Q}(\sqrt[3]{2}) : \mathbb{Q}] = [E : \mathbb{Q}(\sqrt[3]{2})] \cdot 3 \implies [E : \mathbb{Q}(\sqrt[3]{2})] \leq 6/3 = 2 \implies [E : \mathbb{Q}(\sqrt[3]{2})] = 1$ o $[E : \mathbb{Q}(\sqrt[3]{2})] = 2$. Ahora bien, $\mathbb{Q}(\sqrt[3]{2}) = \langle \{1, \sqrt[3]{2}, (\sqrt[3]{2})^2\} \rangle_{\mathbb{Q}} \implies \sqrt[3]{2} \notin \mathbb{Q}(\sqrt[3]{2}) \implies E \neq \mathbb{Q}(\sqrt[3]{2}) \implies [E : \mathbb{Q}(\sqrt[3]{2})] \neq 1 \implies [E : \mathbb{Q}(\sqrt[3]{2})] = 2 \implies [E : \mathbb{Q}] = 6$. Nótese que, en este ejemplo, se alcanza de cota superior del teorema 5H. Además $\mathbb{Q}(\sqrt[3]{2}) \subseteq E$ y $\sqrt[3]{2}, \sqrt[3]{2}w, \sqrt[3]{2}w^2 \in E$.

$$\begin{aligned}\sqrt[3]{2} &= 1 \cdot \sqrt[3]{2} \\ -\frac{\sqrt[3]{2}}{2} + \frac{\sqrt[3]{2}\sqrt{3}}{2}i &= -\frac{1}{2}(\sqrt[3]{2}) + \frac{1}{2}(\sqrt[3]{2}\sqrt{3}i) \\ -\frac{3\sqrt[3]{2}}{2} - \frac{\sqrt[3]{2}\sqrt{3}}{2}i &= -\frac{1}{2}(\sqrt[3]{2}) - \frac{1}{2}(\sqrt[3]{2}\sqrt{3}i)\end{aligned}$$

$$\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2, \sqrt{3}i, \sqrt[3]{2}\sqrt{3}i, (\sqrt[3]{2})^2, (\sqrt[3]{2})^2\sqrt{3}i\}$$

Además, nótese que:

$$\begin{aligned}\sqrt[3]{2} &= 0 \cdot 1 + 1(\sqrt[3]{2}) + 0 \cdot (\sqrt[3]{2})^2 + 0 \cdot (\sqrt{3}i) + 0 \cdot (\sqrt{3}i\sqrt[3]{2}) + 0 \cdot (\sqrt{3}i(\sqrt[3]{2})^2) \\ \sqrt[3]{2}w &= -\frac{1}{2} + \frac{\sqrt[3]{2}\sqrt{3}}{2}i = -\frac{1}{2}(1) + 0(\sqrt[3]{2}) + 0(\sqrt[3]{2})^2 + 0(\sqrt[3]{2})^2 + 0(\sqrt{3}i) + \\ &\quad + \frac{1}{2}(\sqrt{3}i\sqrt[3]{2}) + 0((\sqrt[3]{2})^2\sqrt{3}i) \\ \sqrt[3]{2}w^2 &= -\frac{1}{2} - \frac{\sqrt[3]{2}\sqrt{3}}{2}i = -\frac{1}{2}(1) + 0(\sqrt[3]{2}) + 0(\sqrt[3]{2})^2 + 0(\sqrt{3}i) - \frac{1}{2}(\sqrt[3]{2}\sqrt{3}i) + \\ &\quad + 0((\sqrt[3]{2})^2\sqrt{3}i)\end{aligned}$$

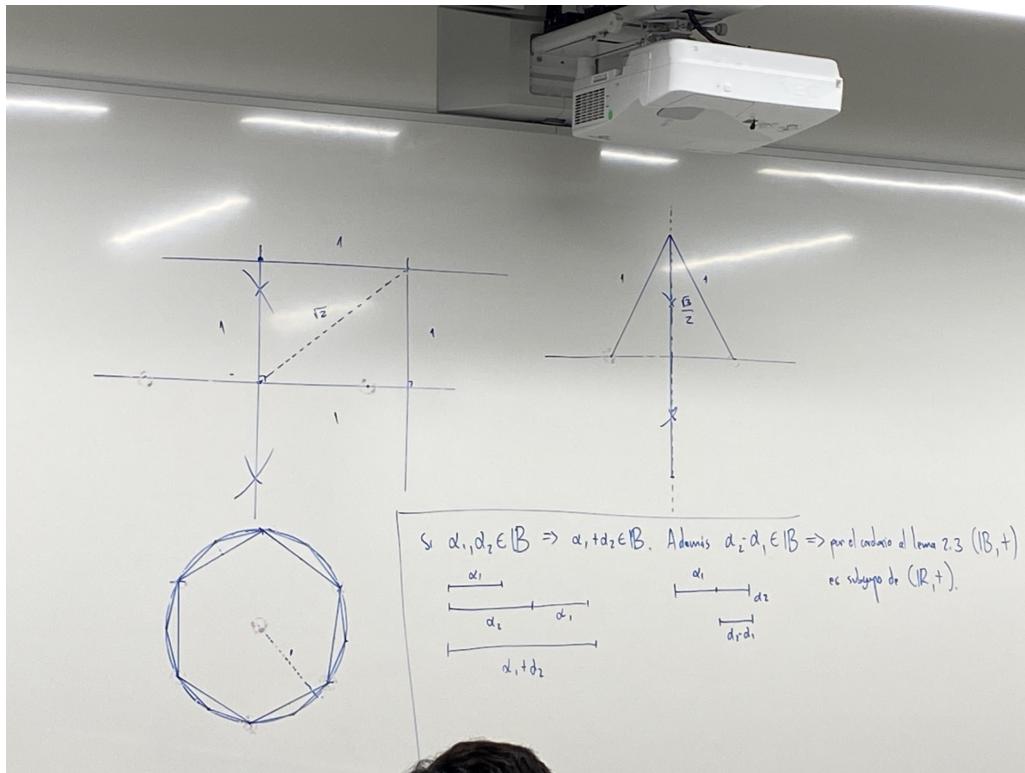
Además, $\{1, \sqrt[3]{2}, (\sqrt[3]{2})^2, \sqrt{3}i, \sqrt[3]{2}\sqrt{3}i, (\sqrt[3]{2})^2, (\sqrt[3]{2})^2\sqrt{3}i\}$ es ligeramente independiente sobre $\mathbb{Q} \implies \mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i) = \langle \{1, \sqrt[3]{2}, (\sqrt[3]{2})^2, \sqrt{3}i, \sqrt[3]{2}\sqrt{3}i, (\sqrt[3]{2})^2, (\sqrt[3]{2})^2\sqrt{3}i\} \rangle_{\mathbb{Q}}$ \implies por el teorema 5J, $\mathbb{Q}(\sqrt[3]{2}, \sqrt{3}i)$ es el campo de descomposición de $x^3 - 2$ sobre \mathbb{Q} , salvo isomorfismo.

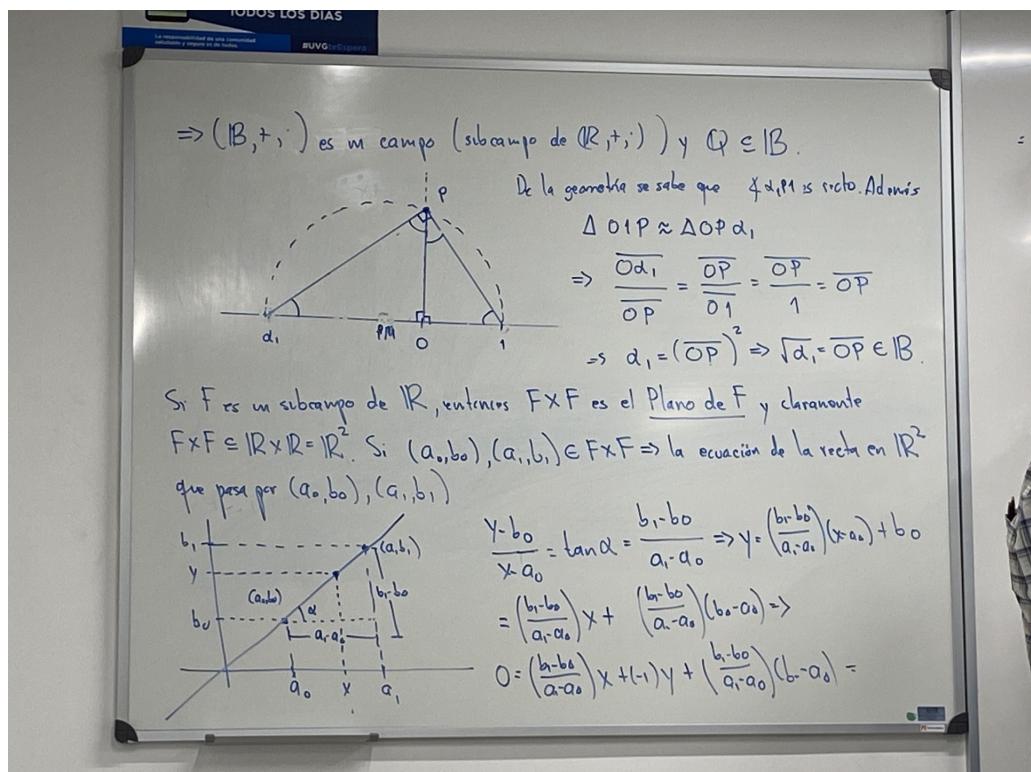
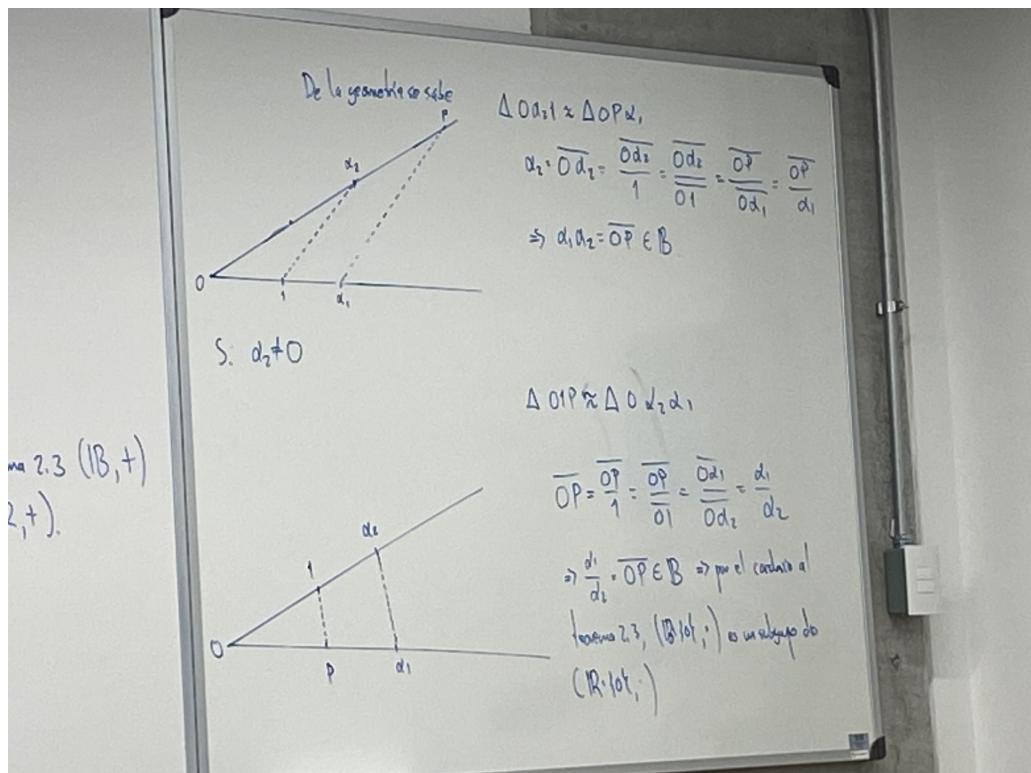
3. Sea $f(x) = x^4 + x^2 + 1 \in \mathbb{Q}[x]$. Si $a \in \mathbb{Q} \implies a^2 \geq 0$ y $a^4 \geq 0 \implies a^4 + a^2 \geq 0 \implies a^4 + a^2 + 1 > 0 \implies f(x)$ es irreducible sobre \mathbb{Q} . Si E es el campo de descomposición de $f(x)$ sobre $\mathbb{Q} \implies$ por el teorema 3H, $[E : \mathbb{Q}] \leq 4! = 24$. Tenemos $x^4 + x^2 + 1 \in \mathbb{Q}[x] \implies x^4 + x^2 + 1 = x^4 + 2x^2 + 1 - x^2 = (x^2 + 1)^2 - x^2 = (x^2 + x + 1)(x^2 - x + 1) \implies$ las raíces de $x^4 + x^2 + 1$ son $\pm\frac{1}{2} \pm \frac{\sqrt{3}}{2}i$. Si $w = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$, entonces $\mathbb{Q}(w)$ es el campo de descomposición de $x^4 + x^2 + 1$ sobre \mathbb{Q} y $[\mathbb{Q}(w) : \mathbb{Q}] = 2$. Nótese que $\mathbb{Q}(\sqrt{3}i)$ también es campo de descomposición de $x^4 + x^2 + 1$ sobre \mathbb{Q} , y por el teorema 5J, $\mathbb{Q}(w) \approx \mathbb{Q}(\sqrt{3}i)$

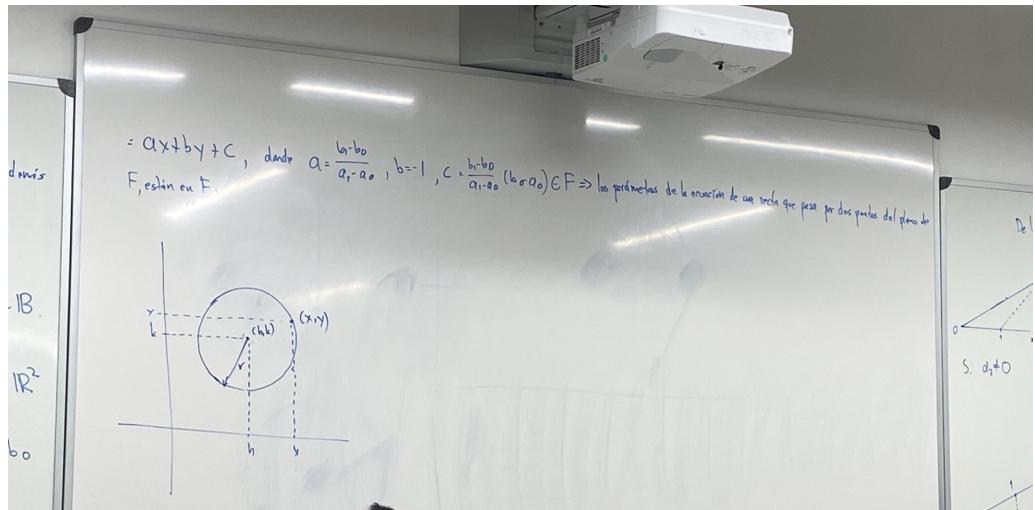
4. Un número $\alpha \in \mathbb{R}$ es constructible si dado un segmento rectilíneo de longitud unitaria, es posible únicamente empleando la regla y el compás, construir un segmento rectilíneo de longitud α .

Sea $\mathbb{B} = \{\alpha \in \mathbb{R} \text{ es constructible}\}$. Claramente $\mathbb{Z} \subseteq \mathbb{B}$.

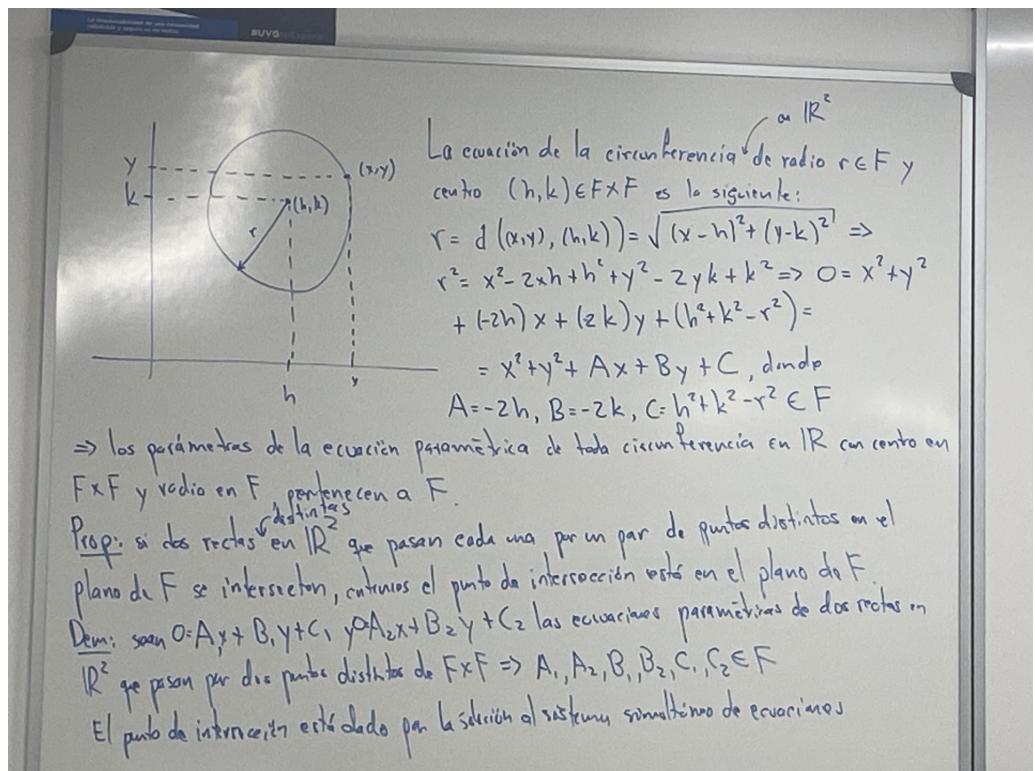
Clase: 25/11/2022

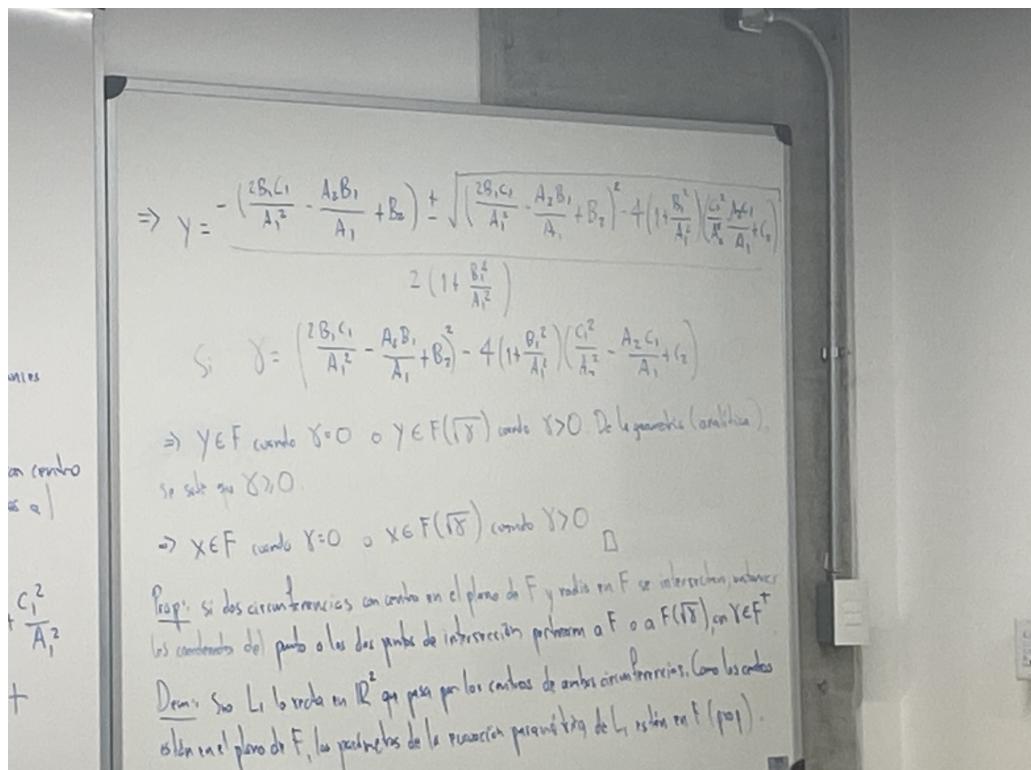
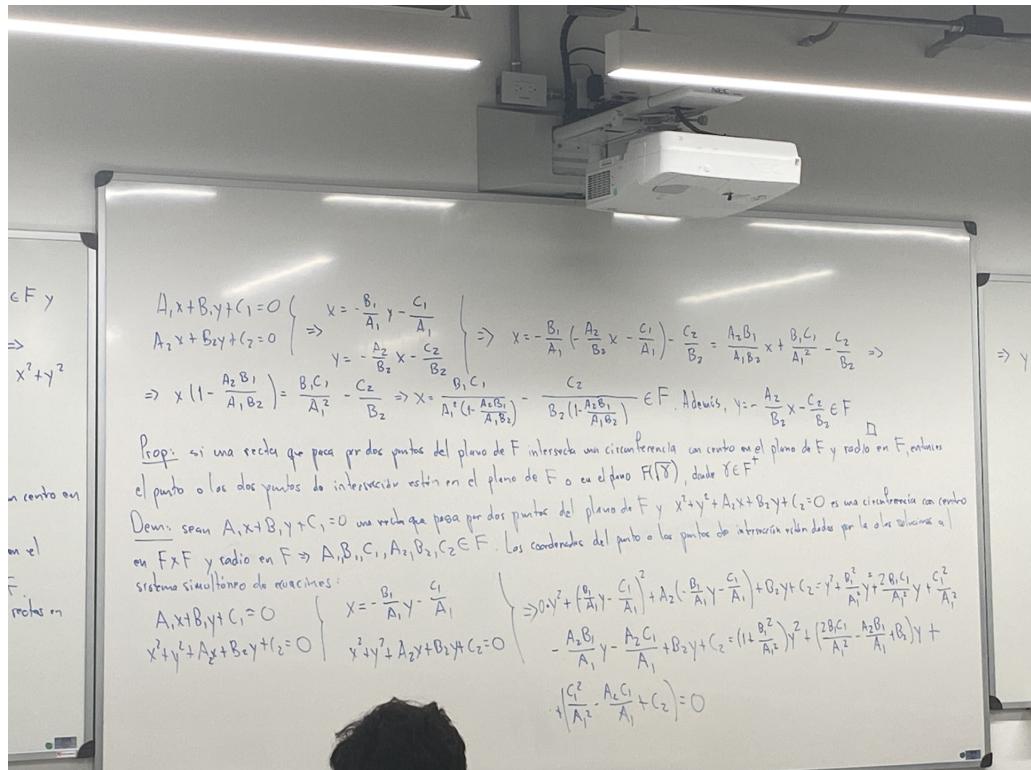


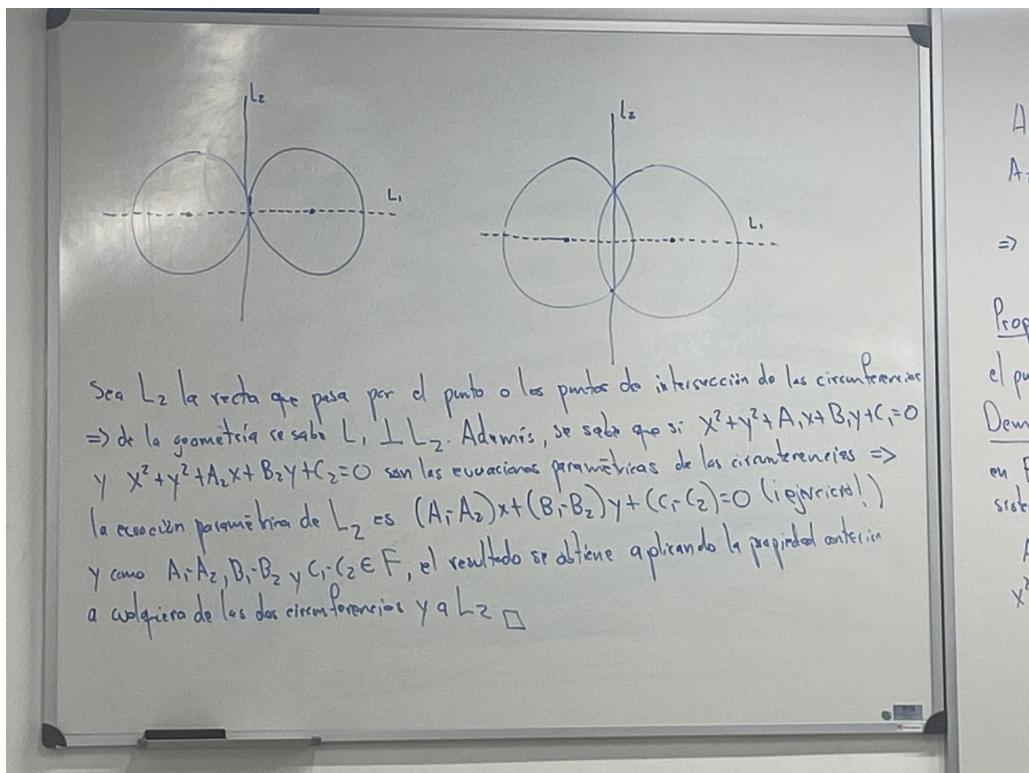




Clase: 29/11/2022







Clase: 15/11/2022

Teorema 54. Si $\alpha \in \mathbb{B}$ es constructible, si y solo si, existen $\lambda, \dots, \lambda_n \in \mathbb{R}^+$, tales que

1. $\lambda_i^2 \in \mathbb{Q}$
2. $\lambda_i^2 \in \mathbb{Q}(\lambda_1, \dots, \lambda_{i-1})$ y $\alpha \in \mathbb{Q}(\lambda_1, \dots, \lambda_n)$

Demostración. ■

Corolario 54.1. Sea $\alpha \in \mathbb{R}$ es constructible si y solo si α pertenece a una extensión de \mathbb{Q} de grado potencia de 2 sobre \mathbb{Q} .

Corolario 54.2. Si $\alpha \in \mathbb{R}$ satisface un polinomio irreducible en $\mathbb{Q}[x]$ de grado K y K no es un polinomio de 2, entonces α no es constructible.

Ejemplo 17. Múltiples aplicaciones.

Teorema 55 (De la raíz racional). Si $f(x) = \sum_{i=0}^n a_i x^i \in \mathbb{X}[x]$, $a_n, a_0 \in \mathbb{Z} - \{0\}$. Sea $p/q \in \mathbb{Q} \ni f(p/q) = 0$ y $(p, q) = 1$, entonces $p|a_0$ y $q|a_n$.

Demostración.

■

Definición 46. Si F es un campo,

$$f(x) = \sum_{i=0}^n a_i x^i \in F[x],$$

entonces la derivada de $f(x)$ es

$$f'(x) = \sum_{i=1}^n i a_i x^{i-1} \in F[x]$$

Definición 47. Un dominio entero D es de característica 0 si la relación $ma = 0, a \in D - \{0\}, m \in \mathbb{Z}$, es válido solo si $m = 0$

Definición 48. Un dominio entero D es de característica finita, si existe $m \in \mathbb{Z}^+$ tal que $ma = 0$ para todo $a \in D$. Si D es de característica finita, entonces la característica de D es el entero positivo más pequeño p tal que $pa = 0$, para todo $a \in D$.

Proposición 19. Si D es un dominio entero de característica finita, entonces su característica es un número primo.

Ejemplo 18. Múltiples ejemplos.

Lema 56 (5.5). Si F es un campo, $f(x), g(x) \in F[x]$ y $\alpha \in F$, entonces:

1. $(f(x) + g(x))' = f'(x) + g'(x)$
2. $(\alpha f(x))' = \alpha f'(x)$
3. $(f(x)g(x))' = f'(x)g(x) + f(x)g'(x)$

Lema 57 (5.5). Si F es un campo, K es una extensión de F y $f(x), g(x) \in F[x]$ tiene un factor común trivial (i.e de grado positivo) en $K[x]$, entonces tienen un factor común no trivial en $F[x]$.

Lema 58 (5.6). Si F es un campo, entonces $f(x) \in F[X]$ tiene una raíz múltiple, si y solo si, $f(x)$ y $f'(x)$ tienen un factor común no trivial.

Corolario 58.1. Si F es un campo, y $f(x) \in F[x]$ es irreducible sobre F , entonces

1. Si la característica de F es 0, entonces $f(x)$ no tiene raíces comunes.
2. Si la característica de F es $p \neq 0$, entonces $f(x)$ tiene una raíz múltiple si y solo si, $\exists g(x) \in F[x] \ni f(x) = g(x^p)$

Corolario 58.2. Si F es un campo de característica de $p \neq 0$ entonces el polinomio $x^{p^n} - x \in F[x], n \in \mathbb{Z}^+$ no tiene raíces múltiples

Definición 49. Si F es un campo, entonces una extensión K de F es simple si existe $\alpha \in K$ tal que

Definición 50. Si F es un campo y K es una extensión de F , $a \in K$ separable sobre F si satisface un polinomio en $F[x]$

Definición 51. Si F es un campo, entonces una extensión K de F simple si existe $\alpha \in K$ tal que $K = F(\alpha)$

Definición 52. Si F es un campo, y K es una extensión de F , $\alpha \in K$ es separable sobre F si satisface un polinomio en $F[x]$ sin raíces múltiples. K es separable sobre F si todos los elementos K son separables sobre F . Un campo es perfecto, si todas sus extensiones finitas son separables.

Clase: 15/11/2022

Teorema 59 (5K). Si F es un campo de característica 0 y $a, b \in F$ son algebraicos, entonces existen $c \in F(a, b)$ tal que $F(a, b) = F(c)$

Demostración. Sean $f(x), g(x) \in F[x]$ ambos irreducibles sobre F y $f(a) = g(b) = 0$. Sea k una extensión de F es la que $f(x)$ y $g(x)$ se factorizan como el producto de polinomios lineales en $K[x]$. Por el corolario al lema 5.6, todas las raíces de $f(x)$ y de $g(x)$ son distintos (i.e. no tienen raíces de multiplicidad 2 o mayor). Sean $\{a = a_1, \dots, a_{gr(f)}\} \subseteq K$ las raíces de $f(x)$ y $\{b = b_1, \dots, b_{gr(g)}\} \subseteq K$ las raíces de $g(x)$.

Si $j \neq 1 \implies$ la ecuación $a_i + \lambda b_j = a_1 + \lambda b_1 = a + \lambda b$ tiene una única solución en K , $a_i - a = \lambda(b - b_j) \implies \lambda = \frac{a_i - a}{b - b_j}$. Además, si F es de característica 0 $\implies F$ es infinito $\implies \exists \gamma \in F \ni a_i + \gamma b_j \neq a + \gamma b, \forall i = 1, \dots, gr(f)$ y $j \neq 1$. Sea $c = a + \gamma b$, $c = a + \gamma b \in F(a, b) \implies F(c) \subset F(a, b)$.

Como $g(b) = 0$, b es raíz de $g(x) \in F[x] \implies b$ es raíz de $g(x) \in F(c)[x]$. Además, si $h(x) = f(c - \gamma x) \in F(c)[x]$ y $h(b) = f(c - \gamma b) = f(a) = 0 \implies$ existe una extensión de $F(c)$ sobre la cual $g(x)$ y $h(x)$ tienen a $x - b$ como factor común. Si $j \neq 1 \implies b_j \neq b$ es otra raíz de $g(x) \implies h(b_j) = f(c - \gamma b_j) \neq 0$ ya que $c - \gamma b_j$ no coincide con ninguna raíz de $f(x)$. Además, $(x - b)^2 \nmid g(x) \implies (x - b)^2 \nmid (g(x), h(x)) \implies x - b = (g(x), h(x))$ sobre alguna extensión de $F(c)$. Por lema previo al lema 5.6, $x - b = (g(x), h(x))$ sobre $F(c)$. Entonces, $x - b \in F(c)[x] \implies b \in F(b) \implies a = c - \gamma b \in F(x) \implies F(a, b) \subseteq F(c)$. En resumen, $F(c) = F(a, b)$. ■

Corolario 59.1. *Toda extensión finita de un campo de característica 0 es simple.*

Demostración. Un argumento inductivo (tarea) asegura que si $\alpha_1, \dots, \alpha_n$ son algebraicos sobre F entonces $\exists c \in F(\alpha_1, \dots, \alpha_n) \ni F(c) = F(\alpha_1, \dots, \alpha_n)$ ■

Revisar los problemas, 6,7, 8 de la sección 3.2 asignados en la tarea 12 y resolver los problemas 1,2,3,4,5,14 de la sección 5.5

2.1. Elementos de la teoría de Galois

Teorema 60 (5L). Si K es un campo y $\sigma_1, \dots, \sigma_n$ son automorfismos distintos de K , entonces es imposible encontrar $k_1, \dots, k_n \in K$, no todos cero, tales que la suma $\sum_{i=1}^n k_i \sigma_i(u) = 0$, para todo $u \in K$.

Demostración. Supóngase que existe $\{k_1, \dots, k_n\} \subset K$, por lo menos un $k_i \neq 0$ s.t. $\sum_{i=1}^n k_i \sigma_i(u) = 0, \forall u \in K$. Elijase el subconjunto de elementos no nulos de $\{k_1, \dots, k_n\}$ el subconjunto retiquetado más pequeños de elementos no nulos de $\{k_1, \dots, k_n\} = \sum_{j=1}^m k_j \sigma_j(u) = 0, \forall u \in K$.

$$\text{Si } m = 1 \implies k_1 \sigma_1(u) = 0, \forall u \in K \implies k_1 = 0 (\rightarrow \leftarrow)$$

Si $m > 1$, como $\sigma_1, \dots, \sigma_n$ son distintos, $\exists c \in K$ s.t. $\sigma_1(c) \neq \sigma_m(c)$. Ahora bien, $\sum_{j=1}^m k_j \sigma_j(u) = 0, \forall u \in K \implies 0 \sum_{j=1}^m k_j \sigma_j(cu) = \sum_{j=1}^m k_j \sigma_j(c) \sigma_j(u), \forall u \in K$. Además, $0 = \sigma_1(c) \left(\sum_{j=1}^m k_j \sigma_j(u) \right) = \sum_{j=1}^m k_j \sigma_j(u) = 0 = 0 \cdot 0 = \sum_{j=1}^m k_j - \sum_{j=1}^m k_j \sigma_1(c) \sigma_j(u) = \sum_{j=1}^m k_j (\sigma_1(c) - \sigma_j(c)) \sigma_j(u) = \sum_{j=2}^m k_j (\sigma_1(c) - \sigma_j(c)) \sigma(u)$.

Como $k_j(\sigma_1(c) - \sigma_j(c)) \in K, k_j \neq 0, \sigma_1(c) - \sigma_j(c) \neq 0 \implies k_m(\sigma_1(c) - \sigma_m(c)) \neq 0 \implies \{k_1, \dots, k_m\}$ no es el subconjunto de elementos no nulos de $\{k_1, \dots, k_n\}$ tales que $\sum_{j=1}^m k_j \sigma_j(u) = 0, \forall u \in K$

Definición 53. Si K es un campo y G es un subgrupo de $\mathbb{A}(K)$ (i.e G es un grupo de automorfismos de K), entonces el subcampo de K fijado por G es $\{k \in K : \sigma(k) = k, \forall \sigma \in G\}$.

NOTA. La definición sigue teniendo sentido si, en vez de un subgrupo de $\mathbb{A}(k)$, se considera un subconjunto no vacío de $\mathbb{A}(K)$. El problema 1 de la tarea 24 se verifica que el subcampo fijado de un conjunto de automorfismos y del subgrupo de $\mathbb{A}(k)$ generado por ese subconjunto, en efecto son iguales.

■

Lema 61. Si K es un campo, G es un subgrupo de $\mathbb{A}(K)$, entonces el subcampo de K fijado por G , en efecto es un subcampo de K .

Demostración. Sean k_1, k_2 elementos del subcampo de k fijado por $G \implies \sigma(k_1) = k_1$ y $\sigma(k_2) = k_2, \forall \sigma \in G$.

■

Clase: 17/11/2022

Definición 54. Si F es un campo y K es una extensión de F , entonces el Grupo de Automorfismos de K relativo a F , denotado por $G(K, F)$ es

$$\{\sigma \in \mathbb{A}(K) : \sigma(\alpha) = \alpha, \forall \alpha \in F\}$$

Lema 62 (5.8). Si F es un campo y K es una extensión de F , entonces, $G(K, F)$ es un subgrupo de $\mathbb{A}(K)$

Demostración.

■

Si K es un campo de característica 0 $\implies \mathbb{Q} \subseteq K$. Entonces, el subcampo fijado por cualquier grupo de automorfismos de K , siendo campo, debe contener a \mathbb{Q} . Entonces todo racional queda invariante por cualquier automorfismo de K .

Ejemplo 19. Tenemos los siguientes ejemplos:

1. a

2. b

3. c

Teorema 63 (5M). Si K es una extensión finita del campo F , entonces el $o(G(K, F)) \leq [K : F]$

Demostración.

■

NOTA. Si F es un campo, $\sigma \in S_n$ y $r(x_1, x_2, \dots, x_n) \in F(x_1, \dots, x_n) \implies \sigma$ puede ser extendido sobre $F(x_1, \dots, x_n)$ de la función siguiente

$$r(x_1, \dots, x_n) \in F(x_1, \dots, x_n) \rightarrow_{\sigma} r(x_{\sigma(1)}, \dots, x_{\sigma(n)}) \in F(x_1, x_2, \dots, x_m)$$

Vista así,

$$\sigma \in \mathbb{A}(F(x_1, \dots, x_m))$$

Definición 55. SI F es campo, el campo de las funciones racionales simétricas, denotado por S , es el subcampo de $F(x_1, x_2, \dots, x_n)$ fijado por S_n

Definición 56. Las funciones simétricas elementales de x_1, \dots, x_n son:

1. 1,

$$\sum_{i=1}^n x_i$$

2. 2,

$$\sum_{i < j} x_i x_j$$

3. 3,

$$\sum_{i \leq j \leq k} x_i x_j x_k$$

4. 4,

$$a_n = \prod_{i \leq k}^n x_i$$

Ejemplo 20. Tenemos múltiples ejemplos.

Clase: 22/11/2022

Teorema 64 (5N). Si F es un campo, entonces:

$$1. [F(x_1, \dots, x_n) : S] = n!$$

$$2. G[F(x_1, \dots, x_n), S] = S_n$$

3. Si a_1, \dots, a_n son las funciones simétricas elementos de x_1, \dots, x_n entonces

$$S = F(a_1, \dots, a_n)$$

4. $F(x_1, \dots, x_n)$ es el campo de descomposición de

$$p(t) = \sum_{i=0}^n (-1)^i a_i t^{n-i}$$

$$\text{sobre } F(a_1, \dots, a_n) = S$$

Demostración. Sea

$$[F(x_1, \dots, x_n) : S] \geq o(G(F(x_1, \dots, x_n), S)) \geq o(S_n) = n!$$

Se sabe que $F(x_1, \dots, x_n)$ contiene todas las raíces $p(t) = \sum_{i=0}^n (-1)^i a_i t^{n-i} \in F(a_1, \dots, a_n)[t]$, $a_0 = 1$, ya que $p(t) = \sum_i^n (-1)^i a_i t^{n-1} = \prod_{i=1}^n (t - x_i) \implies F(x_1, \dots, x_n)$ contiene al campo de descomposición sobre $F(a_1, \dots, a_n)$. Pero, por otro lado, $F(x_1, \dots, x_n)$ es la extensión más pequeña de F que contiene a $x_1, \dots, x_n \implies F(x_1, \dots, x_n)$ es el campo de descomposición de $p(t)$ sobre $F(a_1, \dots, a_n) \implies$ por el teorema 5H, siendo $n = gr(p)$, entonces $[F(x_1, \dots, x_n) : F(a_1, \dots, a_n)] \leq n!$ Ahora bien, $F(a_1, \dots, a_n)$ es un subcampo de S . Entonces, por el teorema 5A, $n! \geq [F(x_1, \dots, x_n) : F(a_1, \dots, a_n)] = [F(x_1, \dots, x_n) : S][S : F(a_1, \dots, a_n)] \geq n![S : F(a_1, \dots, a_n)] \implies 1 \geq [S : F(a_1, \dots, a_n)] \implies [S : F(a_1, \dots, a_n)] = 1 \implies S = F(a_1, \dots, a_n)$ (parte (iii)) $\implies n! \geq [F(x_1, \dots, x_n) : F(a_1, \dots, a_n)] = [F(x_1, \dots, x_n) : S] \geq o(G(F(x_1, \dots, x_n), S)) \geq n!$ (parte (i)) y $G(F(x_1, \dots, x_n), S) = S_n$ (parte 2). ■

NOTA. En los comentarios al teorema 5H se mencionó que dado $n \in \mathbb{Z}^+$, es posible construir un campo F y un polinomio sobre F de grado n cuyo campo de descomposición alcanza la cota superior $[E : F] = n!$. El teorema 5N muestra lo aseverado. $S = F(a_1, \dots, a_n)$ es el campo de descomposición de

$$p(t) = \sum_{i=0}^n (-1)^i a_i t^{n-1} \in F(a_1, \dots, a_n)[t]$$

sobre $F(a_1, \dots, a_n)$ y $[F(x_1, \dots, x_n) : F(a_1, \dots, a_n)] = n!$.

Definición 57. Un campo K es una extensión normal de un campo F , si $[K : F] \in \mathbb{Z}^+$ y F es el subcampo de K fijado por $G(K, F)$.

Proposición 20. Un campo K es una extensión normal de un campo F , si y solo si, $k \in K - F$ no queda invariante por ningún elemento de $F(K, F)$.

Ejemplo 21. En los ejemplos anteriores, 1 y 3 muestran extensiones normales, mientras que 2 es una extensión normal.

Sea F un campo, K no es una extensión de F y H es un subgrupo de $G(K, F)$, entonces $K_H = \{k \in K : \sigma(k) = k, \forall \sigma \in H\}$, el subcampo de K fijado por H .

Teorema 65 (5O). Sean F un campo de característica 0, K es una extensión normal de F y H es un subgrupo de $G(K, F)$, entonces:

1. $[K : K_H] = o(H)$

2. $H = G(K, K_H)$

Demostración.

■

Corolario 65.1. Si F es un campo de característica 0, K es una extensión normal de F , entonces $[K : F] = o(G(K, F))$

Demostración. Es el caso especial del teorema 5O, $H = G(K, F)$, con lo cual $K_H = K_{G(K, F)} = F$. ■

Lema 66 (5.9). Si F es un campo, K el campo de descomposición sobre F de $f(x) \in F[x]$ y $p(x) \in F[x]$ es un factor de $f(x)$ irreducible sobre F y $\alpha_1, \dots, \alpha_{gr(p)} \in K$ son las raíces de $p(x)$, entonces para cada α_i existe $\sigma_i \in G(K, F)$ tal que $\sigma_i(\alpha_i) = \alpha_i$.

Demostración. Por el teorema 5I, existe un isomorfismo $i : F(\alpha_i) \rightarrow F(\alpha_i) \ni i(\alpha_i) = \alpha_i$ e I deja fijo a F . Por el argumento usado en la prueba del teorema 5J, si K es el campo de descomposición de $f(x)$ sobre $F \implies K$ es el campo de descomposición de $f(x)$ sobre $F(\alpha_i)$ y sobre $F(\alpha_i) \implies$ por el teorema 5J, existe un isomorfismo $\sigma_i : K \rightarrow K \ni \sigma_i$ deja fijo a F , es decir $\sigma_i \in G(K, F)$ y coincide en i en $F(\alpha_1) \implies F(\alpha_i) = i(\alpha_i) = \alpha_i$. ■

Teorema 67 (5P). Si F es un campo de característica 0, entonces K es una extensión normal de F si y solo si, K es el campo de descomposición de algún polinomio sobre F .

Demostración. Sea

- (\implies) F tiene característica 0 $\implies K$ tiene característica 0 \implies por el corolario al teorema 5K, K es una extensión simple de $F \implies \exists \gamma \in K \ni K = F(\gamma)$. Además, K es una extensión normal de $F \implies [K : F] = [F(\gamma) : F] \in \mathbb{Z}^+$ $\implies a$ es algebraico sobre F de grado $[F(a) : F] =_{cor, 5O} o(G(F(a), F))$. Sea $G(F(a), F) = \{\sigma_1, \dots, \sigma_{[F(a) : F]} : F\}$ y $p(x) = \prod_{i=1}^{[F(a) : F]} (x - \sigma_i(a)) = \sum_{i=0}^{[F(a) : F]} (-1)^i \alpha_i x^{[F(a) : F] - i} \in F(a)[x]$, $\alpha_0 = 1, \alpha_1, \dots, \alpha_{[F(a) : F]}$ las funciones simétricas elementales en $\alpha_1(a) = a_1, \dots, \alpha_{[F(a) : F]}(a)$. Nótese que si $\sigma \in G(F(a), F) \implies \sigma(\alpha_i) = \alpha_i \implies \alpha_i \in F(a)_{G(F(a), F)} = F \implies p(x) \in F[x]$. Ahora bien, $\sigma_i(a) = a_1, \dots, \sigma_{[F(a) : F]}(a) \in F(a)$ contiene al campo de descomposición de $p(x)$ sobre F . Pero siendo a raíz de $p(x)$, $F(a)$ debe a su vez estar contenido en el campo de descomposición de $f(x)$ sobre F . En resumen, $K = F(a)$ es el campo de descomposición de $f(x)$ sobre F .
- (\Leftarrow) Supóngase que existe $f(x) \in F[x] \ni K$ es el campo de descomposición de $f(x)$ sobre F . Procediendo por inducción sobre $[K : F]$
 - $[K : F] = 1 \implies K = F \implies K_{G(k,k)} = K = F \implies K$ es extensión normal de K .
 - Supónganse el teorema válido para todo par de campos F, K_1 extensión de F_1 y $[K_1 : F_1] < [K : F]$

- Si F no es un campo de descomposición de $f(x)$ sobre $F \implies \exists p(x) \in F[x]$, irreducible sobre F , $p(x)|f(x)$, $1 < gr(p)$ y todas las raíces de $p(x)$ y $[F(\alpha_1) : F] = gr(p)$ (teorema 5BC). Por el argumento usado en las demostraciones del teorema 5J, K es el campo de descomposición de $f(x)$ sobre $F(\alpha_1)$. Entonces, por el teorema 5A, $[K : F] = [K : F(\alpha_1)][F(\alpha_1) : F] = [K : F(\alpha_1)]gr(p) > [K : F(\alpha_1)] \implies$ por la hipótesis inductiva, K es una extensión normal de $F(\alpha_1)$. Por definición, $F \subseteq K_{G(K,F)}$. Sea $\theta \in K_{G(K,F)} \implies \theta \in K_{G(K,F(\alpha_1))} \implies$ por la normalidad de K sobre $F(\alpha_1)$, $\theta \in K_{G(K,F(\alpha_1))} = F(\alpha_1) \implies$ por el teorema 5BC, existen $\lambda_0, \dots, \lambda_{gr(p)} \in F$ $\ni \theta = \sum_{j=0}^{gr(p)-1} \lambda_j \alpha_i^j$. Por lema 5.9 $\exists \sigma_i \in G(K, F)$ tal que $\sigma_i \in G(K, F) \ni \sigma_i(\alpha_i) = \alpha_i$ y además que $\theta \in K_{G(K,F)} \implies \sigma_i(\theta) = \theta$ y $\sigma_i(\lambda_j)$ por $j = 0, \dots, gr(p) - 1$ entonces $\theta = \sigma(\theta) = \sigma_i(\theta)$

■

Clase: 24/11/2022

2.1.1. Solubilidad por radicales

NOTA. Si $x^3 + 3x + 4 \in \mathbb{Q}[x]$ usando la fórmula cuadrática de Viete se sabe que sus raíces son:

$$-\frac{3}{2} \pm \frac{1}{2}\sqrt{7}i$$

Entonces, $\mathbb{Q}(\sqrt{7}i)$ es el campo de descomposición de $x^3 + 3x + 4$ sobre \mathbb{Q} . Es decir si $\gamma = -7 \in \mathbb{Q} \implies \mathbb{Q}(w)$, con $w^2 = \gamma$, es campo de descomposición de $x^3 + 3x + 4$. Dado el polinomio cuadrático general $p(x) = x^2 + a_1x + a_2 \in F[x]$, en particular también $x^2 + a_1x + a_2 \in F(a_1, a_2)[x]$, donde $F(a_1, a_2)$ es el campo de todas las funciones racionales en dos variables evaluadas en a_1, a_2 , con coeficientes en F . Entonces, si $w^2 = a^2 - 4a_2 \in F(a_1, a_2) \implies \mathbb{Q}(w)$ contiene a las raíces $x^2 + a_1x + a_2$, y con ella, el campo de descomposición de este polinomio sobre F . De hecho, la fórmula de Vietta expresa las raíces de $x^2 + a_1x + a_2$ en términos de a_1 y a_2 , y raíces cuadradas de funciones racionales en $F(a_1, a_2)$. Para el polinomio cúbico general $p(x) = x^3 + a_1x^2 + a_2x + a_3$, la situación es similar,

las fórmulas de Cardano expresa las raíces $p(x)$ en términos de a_1, a_2 y a_3 y combinaciones cuadradas y cúbicas de funciones racionales en $F(a_1, a_2, a_3)$. Si $p = a_2 - \frac{1}{3}a_1^2, q = \frac{2}{27}a_1^3 - \frac{1}{3}a_1a_2 + a_3$. De esto

$$p = \sqrt{-\frac{1}{2}q + \sqrt{\frac{1}{27}p^3 + \frac{1}{4}q^2}}$$

$$q = \sqrt[3]{-\frac{1}{2}q - \sqrt{\frac{1}{27}p^3 + \frac{1}{4}q^2}}$$

raíces cúbicas a conveniencia, entonces las tres raíces de $p(x)$ son $x_1 = P + Q - \frac{1}{3}a_1$, $x_2 = wP + w^2Q - \frac{1}{3}a_1$ y $x^3 = w^2P + wQ - \frac{1}{3}a_1$, donde w es una raíz cúbica de la unidad y $w \neq 1$. Estas fórmulas ilustran que, extendiendo \mathbb{Q} con la adjunción de cierta raíz cuadrada y luego una raíz cúbica de elementos de $\mathbb{Q}(a_1, a_2, a_3)$ se tiene una extensión finita de \mathbb{Q} que contiene al campo de descomposición de $p(x)$. Se puede demostrar que usando funciones racionales sobre \mathbb{Q} evaluadas en los cuatro coeficientes y raíces cuadradas, el problema de encontrar las cuatro raíces se reduce a buscar las raíces de cierto polinomio cúbico, usando las fórmulas de Cardano, las cuatro raíces se pueden expresar con fórmulas en términos de radicales de funciones racionales sobre \mathbb{Q} evaluadas en los coeficientes (ejercicio). Se demostrará que para polinomios generales de grado 5 o superior no existen fórmulas para las raíces en términos de radicales de funciones racionales sobre \mathbb{Q} evaluadas en los coeficientes.

Definición 58. Si F es un campo y $p(x) \in F[x]$, entonces $p(x)$ es soluble por radicales sobre F si existe una colección finita de campos, $F = F(w_1), \dots, F_k = F_{k-1}(w_k)$, donde $w_1^{r_1} \in F, w_2^{r_2} \in F_1, \dots, w_k^{r_k} \in F_k, r_1, \dots, r_k \in \mathbb{Z}^+$ tales que F_k contiene al campo de descomposición de $p(x)$ sobre F .

Proposición 21. Si F es un campo de característica 0, $p(x) \in F[x]$ es soluble por radicales sobre F , entonces F_k es una extensión normal de F .

Definición 59. Si F es un campo, $p(x) \in \sum_{i=0}^n a_i x^i \in F[x], a_0 = 1$, es el **polinomio general de grado n sobre F**. En particular $p(x) \in F(a_1, \dots, a_k)[x]$. Además, $p(x)$ es soluble por radicales si es soluble por radicales sobre $F(a_1, \dots, a_k)$

NOTA. Esta definición formaliza la idea intuitiva de fórmula para las raíces de $p(x)$ que las expresan en términos de radicales de elementos de $F(a_1, \dots, a_n)$. Se mencionó que estas fórmulas existen para todos los polinomios de grado 1, 2, 3 y 4. Abel demostró no existen para todos los polinomios de grado 4 o superior. Lo que se desea investigar es si para un polinomio $p(x) \in \mathbb{Q}[x]$, $gr(p) \geq 5$ particular es específico, existen fórmulas que expresen n raíces como radicales de funciones racionales de sus coeficientes.

NOTA. Objetivo: usando el grupo de Galois, desarrolear un criterio para determinar cuando un polinomio es soluble por radicales.

Definición 60. Un grupo es soluble si existe una cadena finita de subgrupos

$$G = N_0 \supseteq N_1 \subseteq \cdots \subseteq N_k = (e),$$

es lo que cada N_i es un subgrupo normal de N_{i-1} y N_{i-1}/N es abeliano.

Ejemplo 22. Tenemos:

1. Todo grupo abeliano es soluble sea $N_0 = G$ y $N_1 = (e)$
2. S_3 es soluble; sean $N = \{e, (123), (132, 132)\}$ es un subgrupo normal de S_3 \implies

$$o(S_3/N_1) = \frac{o(S_3)}{o(N_1)} = \frac{6}{3} = 2$$

Entonces, S_3/N_1 es abeliano y sea $N_2 = (e)$ subgrupo normal de N_1 y $N_1/N_2 \approx N_1$ un grupo cíclico y por lo tanto, abeliano.

3. S_4 es soluble.
4. En el teorema 5R se demostrará que S_5 no es soluble.

Definición 61. Dados un grupo G , $g_1, g_2 \in G$, el conmutador de g_1 y g_2 es $g_1^{-1}g_2^{-1}g_1g_2$. El subgrupo conmutador de G es $G' = \langle \{g_1^{-1}g_2^{-1}g_1g_2 : g_1, g_2 \in G\} \rangle$

Proposición 22. Si G es un grupo, entonces G' es un subgrupo normal de G .

Demostración. tarea

Proposición 23. Si G es un grupo, entonces G/G' es abeliano.

Demostración. Si $G'g_1, G'g_2 \in G/G' \implies (G'g_1)(G'g_2) = G'(g_1G')g_2 = G'(G'g_1)g_2 = (G'G')g_1g_2 = G'g_1g_2 = g_1g_2G' = g_1g_2(g_2^{-1}g_1^{-1}g_2g_1G') = g_1(g_2g_2^{-1})g_1^{-1}g_2g_1G' = g_1eg_1^{-1}g_2g_1G' = g_2g_1^{-1}g_2g_1G' = eg_2g_2G' = g_2g_1G' = G'g_2g_1 = (G'g_2)(G'g_1)$ ■

Proposición 24. Si G es grupo, M es subgrupo normal de G tal que G/M es abeliano, entonces $G' \subseteq M$.

Demostración. Si $g_1, g_2 \in G \implies Mg_2g_1 = (Mg_1)(Mg_2) = (Mg_2)(Mg_1) = Mg_2g_1 \implies g_1g_2(g_2g_1)^{-1} \in M \implies g_1g_2g_1^{-1}g_2^{-1} \in M, \forall g_1, g_2 \in G \implies G' \subseteq M$. (Hay que arreglar los inversos de la demostración) ■

Proposición 25. Si G es un grupo, entonces $G'' = (G')'$ es subgrupo normal de G .

Demostración. Tarea. ■

Proposición 26. Si G es un grupo, $G^{(m)} = (G^{(m-1)})^1$ es un subgrupo normal de G y $G^{(m-1)}/G^{(m)}$ es abeliano.

Lema 68 (5.10). G es un grupo soluble, si y solo si, $\exists k \in \mathbb{N} \ni G^{(k)} = (e)$.

Demostración. Sea

- (\implies) Si G es soluble $\implies \exists$ una cadena $G = N_0 \supseteq N_1 \supseteq_1 \dots \supseteq N_k = (e)$, donde N_i es un subgrupo normal de N_{i-1} y N_{i-1}/N_i es abeliano, $\forall i = 0, \dots, k$. Ahora bien, la propiedad, como N_i es subgrupo normal de N_{i-1} y N_{i-1}/N_i es abeliano $\implies N'_{i-1} \subseteq N_i, \forall i = 0, \dots, k$ en particular, $N_1 \supseteq N'_0 = G', N_2 \supseteq N'_1 \subseteq G'', N_3 \supseteq N'_2 \supseteq G''', \dots, N^i \supseteq N'_{i-1} \supseteq G^{(i)}, \dots, (e) = N_k \supseteq N'_{k-1} \supseteq G^{(k)} \implies G^{(k)} = (e)$
- (\Leftarrow) Si $G^{(k)} = (e)$, sean $N_0 = G, N_1 = G', \dots, N_i = G^i, \dots, N_k = G^{(k)} = (e) \implies G = N_0 \subseteq G' \supseteq \dots \supseteq G^{(i)} \supseteq \dots \supseteq G^{(k)} = (e)$, $G^{(i)}$ es un subgrupo normal de $G^{(i-1)}$ y $G^{i-1}/G^{(i)}$ es abeliano $\implies G$ es soluble.

■

Corolario 68.1. Si G es un grupo soluble y \overline{G} es una imagen homomórfica de G , entonces \overline{G} es soluble.

Demostración. Nótese que si $\phi : G \rightarrow \overline{G}$ es un homomorfismo sobreyectivo y $g_1, g_2 \in G \implies \phi(g_1^{-1}g_2^{-1}g_1g_2) = \phi(g_1^{-1})(g_1g_2) = \phi(g_1^{-1})\phi(g_2^{-1})\phi(g_1)\phi(g_2) = \phi(g_1)^{-1}\phi(g_2)^{-1}\phi(g_1)\phi(g_2)$. Es decir, $\phi(G) = \phi(\overline{G}') = \overline{G}' \implies$ por el lema 5.10, $\exists k \in \mathbb{N} \ni G^{(k)} = (e) \implies (\bar{e}) = \phi((e)) = \phi(G^k) = \overline{G}^{(k)} \implies$ por el lema 5.10, \overline{G} es soluble. ■