I: GRUPOS

Definición: Dada una operación $*: G \times G \to G$, diremos que

$$(G,*) \text{ grupo} \iff \begin{cases} Ax1.- * \text{ es asociativa} \\ Ax2.- \exists\, e \in G \text{ neutro} : a*e = e*a = a \ \forall a \in G \\ Ax3.- \forall a \in G \ \exists\, a^{-1} \in G : a*a^{-1} = a^{-1}*a = e \end{cases}$$

Diremos que el grupo es **abeliano** o conmutativo si $*$ es conmutativa

Definición: Un subconjunto $H \subseteq (G,*)$ es **subgrupo**, $H \leq G$, si $(H, *|_{H\times H})$ es grupo, ie,

$$(H,*) \leq G \iff \begin{cases} 1)\ a*b \in H \\ 2)\ e \in H \\ 3)\ \exists\, a^{-1} \in H \ \forall a \in H \end{cases} \iff a*b^{-1} \in H \ \ \forall a,b \in H.$$

* Dado $H \leq G$, llamamos **subgrupo conjugado de H por a** a $aHa^{-1} = \{ aha^{-1} : h \in H \}$, que es un subgrupo (Prop).

* Dado G grupo, cada elemento $g \in G$ genera un subgrupo $\langle g \rangle = \operatorname{Im} f_g$

$$\langle g \rangle = \{ ng = g^{+n} + \dots + g : n \in \mathbb{Z} \} \quad \text{NOT. ADITIVA}$$

$$\langle g \rangle = \{ g^n = g^{\cdot n} \cdots g : n \in \mathbb{Z} \} \quad \text{NOT. MULTIPLICATIVA}$$

* Las permutaciones σ de n ptos en un plano que conservan distancias forman un subgrupo de S_n, $G S_n$ = **grupo de simetría**.

Proposición:

a) $H_i \leq G \ \forall i \Rightarrow \bigcap_i H_i \leq G$

b) $H_1 \cup H_2 \leq G \iff H_1 \subseteq H_2$ ó $H_1 \supseteq H_2$

c) $H_1 + H_2 = \{ h_1 + h_2 : h_1 \in H_1,\ h_2 \in H_2 \} \leq G$ si $H_1, H_2 \leq G$.

Definición: Dado $X \subseteq G$, diremos que el subgrupo generado por X es $\bigcap_{H_i \leq G : X \subseteq H_i} H_i$

Teorema: Todos los subgrupos de $(\mathbb{Z}, +)$ son de la forma $n\mathbb{Z}$ para algún $n \in \mathbb{N}$.

Definición: Diremos que a es múltiplo de b $\Leftrightarrow$ b es divisor de a $\Leftrightarrow \exists k \in \mathbb{Z} : a = kb$, ie, $a\mathbb{Z} \subseteq b\mathbb{Z}$. Además, diremos que un $p > 1$ es primo si sus únicos divisores son 1 y p.

Definición: Dados $a, b \in \mathbb{Z}$.

$d = mcm(a,b) \Leftrightarrow \begin{cases} 1) d \text{ es un múltiplo común} \\ 2) \text{divide a cualquier otro múltiplo común (ie, es el menor de ellos)} \end{cases}$

$d = mcd(a,b) \Leftrightarrow \begin{cases} 1) d \text{ es un divisor común} \\ 2) d \text{ es un múltiplo de cualquier otro divisor común (ie, el mayor de todos)} \end{cases}$

Proposición: $m = mcm(a,b) \Leftrightarrow m\mathbb{Z} = a\mathbb{Z} \cap b\mathbb{Z}$

Prop: $d = mcd(a,b) \Leftrightarrow d\mathbb{Z} = a\mathbb{Z} + b\mathbb{Z}$

$\forall a, b \in \mathbb{Z}$.

Corolario (Identidad de Bézout): $d = mcd(a,b) \Rightarrow \exists \alpha, \beta \in \mathbb{Z} : d = \alpha a + \beta b$

Corolario: a, b primos entre sí $\Leftrightarrow \exists \alpha, \beta \in \mathbb{Z} : 1 = \alpha a + \beta b$

Corolario: $\left.\begin{array}{l} n \text{ divide a } a \cdot b \\ n \text{ primo con } a \ (\text{ó } b) \end{array}\right\} \Rightarrow n \text{ divide a } b \ (\text{ó } a)$.

Lema (Euclides): p divide a $u = a_1 \cdots a_r \Rightarrow p$ divide a a_i para algún $i \in \{1, \dots, r\}$.

Teorema (Fundamental de la Aritmética): Todo número natural > 1 es producto de números primos. Esta descomposición es única salvo orden.

Corolario: Hay infinitos números primos.

$\star$ $a \cdot b = mcm(a,b) \cdot mcd(a,b)$.

ALGORITMO DE EUCLIDES: Si $a = bc + r$, entonces $\mathrm{mcd}(a,b) = \mathrm{mcd}(b,r)$

ECUACIONES DIOFÁNTICAS: Dado $ax + by = c$, tiene solución $\Leftrightarrow$ d divide a c.

Si $d = \mathrm{mcd}(a,b)$ entonces las soluciones enteras del sistema son $\begin{cases} x = x_0 \pm \frac{b}{d} n \\ y = y_0 \mp \frac{a}{d} n \end{cases}$, $n \in \mathbb{Z}$ donde (x_0, y_0) es una solución particular de la ecuación.

$x_0 = \frac{c}{d}\alpha$, $y_0 = \frac{c}{d}\beta$; α, β coef. Id. Bezout.

Definición: Diremos que una aplicación $f: (G, \cdot) \to (G', \cdot)$ es un morfismo de grupos si:

$f(a \cdot b) = f(a) \cdot f(b)$. Diremos que f es un isomorfismo si $\exists f^{-1}: G' \to G$:

$f^{-1} \circ f = f \circ f^{-1} = Id$.

Proposición (Propiedades): Sea $f: G \to G'$ morfismo de grupos y $g: G' \to G''$ morfismo de grupos.

a) $f(1_G) = 1_{G'}$

b) $f(a^{-1}) = f(a)^{-1}$

c) $g \circ f: G \to G''$ es un morfismo de grupos.

Definición: $f: G \to G'$ morfismo de grupos.

$\ker f = \{ a \in G : f(a) = 1_{G'} \} \subseteq G$

$\mathrm{Im}\, f = \{ f(a) : a \in G \} \subseteq G'$

Proposición: a) f inyectivo $\Leftrightarrow \ker f = 1_G$

b) f isomorfismo $\Leftrightarrow f$ biyectivo

Proposición: Sea G grupo, $f: G \to G'$ morfismo de grupos, $H \leq G$, $H' \leq G'$

a) $f(H) = \{ f(h) \text{ para algún } h \in H \} \leq G$

b) $f^{-1}(H') = \{ a \in G : f(a) \in H' \} \leq G$

En particular, $f(G) = \mathrm{Im}\, f \leq G'$, y $f^{-1}(1_{G'}) = \ker f \leq G$

Definición: Dado $(G,\cdot)$ grupo y $H \leq G$ define una relación de equivalencia

$$\boxed{a \equiv b \iff a^{-1}\cdot b \in H}$$

* Es fácil comprobar que $[1] = H$ y $[a] = a\cdot H$

El conjunto cociente de G por la rel. de eq. inducida por H se denota

$$G/H = \{[a] = a\cdot H : a \in G\}$$

Definición: Llamamos **orden** de un grupo G a $\text{card}(G) = \#G = |G|$, y **índice** de un subgrupo H de G a $|G/H|$.

Teorema (de Lagrange): $|G/H| = \dfrac{|G|}{|H|}$ si G es finito.

Definición: Dado $H \leq G$, diremos que H es un **subgrupo normal** si $\forall a \in G$ se tiene el subgrupo conjugado de H por a $aHa^{-1} \subseteq H$.

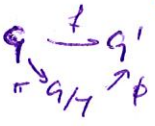
Proposición: Dado un morfismo f, $\ker f$ es siempre un subgrupo normal.

Teorema: Si H es un subgrupo normal, $\exists$ estructura de grupo para G/H : $\pi : G \to G/H$ es un morf. de grupos. Además, $H = \ker \pi$.

* G conmutativo $\Rightarrow$ $H \leq G$ conmutativo y G/H conmutativo.

* **Teorema (Propiedad Universal del grupo Cociente)**: Sea $H \trianglelefteq G$ grupo, $\pi : G \to G/H$ proy. can. y $f : G \to G'$ morf.

$H \subseteq \ker f \iff \exists$ morf de grupos $\phi : G/H \to G'$: $f = \phi \circ \pi$



* **Teorema (Isomorfismo)**: Dado $f : G \to G'$ morf de grupos, la aplicación

$$\phi : G/\ker f \xrightarrow{\cong} \text{Im } f$$
$$[a] \longmapsto \phi([a]) := f(a)$$

es un **isomorfismo de grupos**.

Teorema (Chino de los restos): Dados $m, n \in \mathbb{Z}$ primos entre sí

$\mathbb{Z}/mn\mathbb{Z} \simeq \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$ por el isom. $\phi: \mathbb{Z}/mn\mathbb{Z} \longrightarrow \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$

$[a]_{mn} \longmapsto ([a]_m, [a]_n)$.

EC. DIOFÁNTICAS: Por el Th, $\begin{cases} x \equiv b \ (\mathrm{mód}\ n) \\ x \equiv c \ (\mathrm{mód}\ m) \end{cases}$ sist. tiene sol.

* Sea $(G, \cdot)$ grupo. Cada $g \in G$ define un morfismo de grupos $f_g: (\mathbb{Z}, +) \longrightarrow (G, \cdot)$
donde $\mathrm{Im} f_g = \langle g \rangle$ $\quad n \longmapsto f_g(n) := g^n$

Definición: Llamamos **orden** de un elem $g \in G$ al orden de $\langle g \rangle$.

Propos.: Sea $g \in G$ grupo

* ord g infinito: $g^n = g^m \iff n = m$ $\quad (g^n = 1 \iff n = 0)$
* ord g finito (d): $g^n = g^m \iff n \equiv m \ (\mathrm{mód}\ d)$ $\quad (g^n = 1 \iff n \in d\mathbb{Z})$

Corolario: El orden de un el. g es el primer natural no nulo d: $g^d = 1$. Si $\nexists \Rightarrow \mathrm{ord} = \infty$.

Corolario: Si $\mathrm{ord}(G) = n$, $g^n = 1 \ \forall g \in G$.

Definición: Diremos que un grupo G es **cíclico** si $\exists g \in G : \langle g \rangle = G$ (si está generado por alguno de los elems), en cuyo caso diremos que g es un **generador** de G.

Teorema (Clasificación de grupos cíclicos): Sea G grupo cíclico. $(G = \langle g \rangle)$.

* G infinito: $\mathbb{Z} \simeq G$, $\quad m \longmapsto g^m$
* G finito: $\mathbb{Z}/n\mathbb{Z} \simeq G$, $\quad [m] \longmapsto g^m$
$(\mathrm{ord}(G) = n)$

* $\mathrm{ord}(G) = n$, G cíclico $\iff \exists g \in G : \mathrm{ord}(g) = n$.

* S_n = grupo simétrico de orden n = {permutaciones de n elementos}.

Definición: Diremos que $\sigma \in S_n$ es un **ciclo de longitud d** (orden) si $\sigma = (a_1, \dots, a_d)$ con a_i distintos. Llamaremos **transposiciones** a los ciclos de longitud 2. Diremos que dos ciclos son disjuntos si no tienen elementos en común.

Lema: La composición de ciclos disjuntos es conmutativa.

Teorema: Toda permutación $\sigma \in S_n$ se descompone en producto de ciclos disjuntos, y esta descomposición es única salvo orden de los factores. (Sin Dem).

Corolario: Todo ciclo de longitud d es producto de $d-1$ transposiciones.

Definición: Dada $\sigma = \alpha_1 \dots \alpha_r$, con α_i = ciclo de longitud d_i, $d_1 \geq \dots \geq d_r$, llamaremos **forma de la permutación** a $d_1, \dots, d_r$.

Proposición: La forma de $\sigma = d_1, \dots, d_r$. $\quad \text{ord}(\sigma) = \text{mcm}(d_1, \dots, d_r)$.

Definición: Diremos que $x, y \in G$ son **conjugados** si: $\exists\, a \in G$: $y = axa^{-1}$. Dos elementos conjugados tienen las mismas propiedades ya que $\tau_a : G \to G$, $g \mapsto aga^{-1}$ es un automorfismo.

Definición: Sea el siguiente polinomio con coeficientes enteros,

$$\Delta(x_1, \dots, x_n) = \prod_{i<j} (x_j - x_i)$$

Llamaremos signo de la permutación σ, $\text{sgn}(\sigma) = \pm 1$, a $\Delta(x_{\sigma(1)}, \dots, x_{\sigma(n)}) = \text{sgn}(\sigma) \cdot \Delta(x_1, \dots, x_n)$.

Proposición: El signo del producto de permutaciones es el producto de los signos. El signo de una transposición es -1, y el de un ciclo de longitud d es $(-1)^{d-1}$, y por tanto el signo de una permutación de forma $d_1, \dots, d_r$ es $(-1)^{d_1 + \dots + d_r - r}$.

Definición: Llamamos **subgrupo alternado** a $A_n = \{\sigma \in S_n : \text{sgn}(\sigma) = 1\}$.

II : ANILLOS

ANILLOS

Definición: Sea A un conjunto dotado de dos o.b.i. $+$ y $\cdot$.

$$(A,+,\cdot) \text{ anillo} \iff \begin{cases} 1) & (A,+) \text{ grp abeliano} \\ 2) & \cdot \text{ asociativa} \\ 3) & \cdot \text{ distributiva resp. } + \end{cases}$$

Diremos que A es un **anillo con unidad** si $1 \in A$, y que es un **anillo conmutativo** si $\cdot$ es conmutativo.

Definiciones:

* Diremos que $a \in A$ es **invertible** si $\exists\, b \in A : ab = 1$. Denotaremos como $A^* = \{\text{invertibles de } A\}$
* Diremos que $a \in A$ es un **divisor de cero** si $\exists\, 0 \neq b \in A : ab = 0$
* Diremos que un anillo $A \neq 0$ es **íntegro** o que es un **dominio** si no tiene divisores de cero $\neq 0$.
* Diremos que un anillo $K \neq 0$ es un **cuerpo** si $K^* = K \setminus \{0\}$; ie,

$$(K,+,\cdot) \text{ cuerpo} \iff \begin{cases} 1) & (K,+) \text{ grp abeliano} \\ 2) & (K^*,\cdot) \text{ grp abeliano} \\ 3) & \cdot \text{ distr. resp. } + \end{cases}$$

* Diremos que un elemento $a \in A$ es **propio** si no es ni nulo ni invertible, ie

$$\{\text{propios}\} = A \setminus \{0, \text{invertibles}\}$$

* Diremos que un elto $a \in A$ es **irreducible** si no se puede descomponer como producto de dos propios (ie, si en toda descomposición hay invertibles).

Definición: Diremos que un subconjunto $B \subseteq A$ es un **subanillo** si $(B, +|_{B\times B}, \cdot|_{B\times B})$ es un anillo, i.e.,

$$(B,+,\cdot) \text{ subanillo} \iff \begin{cases} 1)\ a-b \in B \\ 2)\ a\cdot b \in B \end{cases} \quad \forall\, a,b \in B$$

Definiciones:

* $\mathcal{H}[x] = \left\{ p(x) = \sum_{i=0}^{n} a_i x^i : a_i \in \mathcal{H} \right\} \equiv$ anillo de polinomios con coef. en $\mathcal{H}/\mathbb{Q}/\mathbb{R}/\mathbb{C}$

* $\mathcal{H}[\alpha] = \left\{ z \in \mathbb{C} : z = \sum_{i=0}^{n} a_i \alpha^i : a_i \in \mathcal{H} \right\} \equiv$ menor subanillo que contiene a $\mathcal{H}$ y a α

* $B[\alpha_1,\dots,\alpha_n] = \left\{ a \in A : a = \sum_{i_1,\dots,i_n} b_{i_1,\dots,i_n} \alpha_1^{i_1} \cdots \alpha_n^{i_n} : b_{i_1,\dots,i_n} \in B \right\} \equiv$ subanillo de A **generado** por $B \subseteq A$ y $\alpha_1,\dots,\alpha_n \in A$.

(subanillo $\subseteq A$)

* Todos los cuerpos son anillos íntegros.
* La intersección de subanillos es un subanillo.

* $\mathcal{H}[i] = \mathcal{H} + i\mathcal{H} = \{ a+bi : a,b \in \mathcal{H} \} \equiv$ **enteros de Gauss**

Definición: Sea $\mathcal{J} \subseteq A$. Diremos que $\mathcal{J}$ es un **ideal** si es un subanillo y si el producto por el de A cae en $\mathcal{J}$.

$$(\mathcal{J},+,\cdot) \text{ ideal} \iff \begin{cases} 1)\ a-b \in \mathcal{J} & \forall\, a,b \in \mathcal{J} \\ 2)\ a\cdot c \in \mathcal{J} & \forall\, a \in \mathcal{J},\ c \in A \end{cases}$$

Definiciones: Sea A anillo

* Diremos que un ideal $\mathcal{M} \subsetneq A$ es **maximal** si el único ideal que lo contiene es A.
* Diremos que un ideal $\mathcal{P} \subsetneq A$ es **primo** si $ab \in \mathcal{P} \Rightarrow a \in \mathcal{P}$ ó $b \in \mathcal{P}$.
  ($\equiv$ Lema de Euclides)
* Diremos que dados dos ideales, $\mathcal{J}$ **divide a** $\mathcal{b}$ si $\mathcal{b} \subseteq \mathcal{J}$.

* Llamemos mcm de a y b a $a \cap b$, y mcd de a y b a $a + b$

* $a + b = \{a + b : a \in a, b \in b\}$ = menor ideal que contiene a a y b.

* Denotemos a $\operatorname{Spec} A = \{$ ideales primos de $A\}$; y a $\operatorname{Spec}_{max} = \{$ ideales maximales de $A\}$

* La intersección, suma y producto de ideales es un ideal.

* $bA = (b) = \{ba : a \in A\}$ = ideal generado por b, es el más pq. que b contiene

* Los ideales en $\mathbb{Z}$ son de la forma $n\mathbb{Z}$, y a que tienen que ser subgrupos.

* Dado $\alpha \in \mathbb{C}$, $I = \{p(x) \in \mathbb{Q}[x] : p(\alpha) = 0\}$ es un ideal

* $a \in A^* \iff aA = A$

* $K \neq 0$ cuerpo $\iff$ los únicos ideales que tiene son 0 y K

* $p\mathbb{Z}$ ideal primo $\iff$ primo

Definición: Sean A, B anillos. Diremos que una aplicación $f: A \to B$ es un morfismo de anillos si:

1) $f(a +_A b) = f(a) +_B f(b)$
2) $f(a \cdot_A b) = f(a) \cdot_B f(b)$
3) $f(1_A) = 1_B$

Diremos que f es un isomorfismo de anillos si $\exists\, g: B \to A : (f \circ g) = (g \circ f) = Id$. Además $g = f^{-1}$.

* Si $f: A \to B$, $a \in A$, $b \in B$, definimos $a \cdot b := f(a) \cdot b$

* $z \in \mathbb{C} \xrightarrow{\tau} \bar{z} \in \mathbb{C}$ es un mor. de anillos.

* $p(x) \in \mathbb{Z}[x] \longrightarrow p(\alpha) \in \mathbb{C}$ es un mor de anillos.

Proposición: Sea $f: A \to B$ un mor. de anillos

1) $b \subseteq B$ ideal $\Rightarrow f^{-1}(b) \subseteq A$ ideal. ($\forall p$ $\ker f = f^{-1}(0)$ es un ideal)
2) $a \subset A$ ideal, f epi $\Rightarrow f(a) \subseteq B$ ideal

Corolario: Sea K cuerpo y B anillo. Todo mor. de anillos $f: K \to B$ es inyectivo.

POLINOMIOS

* $A[x] = \{ p(x) = \sum_i a_i x^i : a_i \in A \}$ ≡ anillo de polinomios con coef. en A (coef. / indet.)

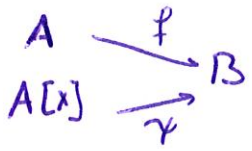
* Sea $0 \neq p(x) = \sum_{i=0}^{d} a_i x^i \in A[x]$. $gr(p(x)) := $ el único n^o nat d : $a_d \neq 0$ y $a_{d+1} = a_{d+2} = \dots = 0$

Proposición: A íntegro $\Rightarrow A[x]$ íntegro, y $gr(p(x) \cdot q(x)) = gr(p(x)) + gr(q(x))$.

Proposición: A íntegro $\Rightarrow A^* = A[x]^*$

Teorema: Sea $f : A \to B$ mor anillos. Para cada $b \in B$ $\exists!$ mor de anillos

$\psi : A[x] \to B$: $\psi(x) = b$ y $\psi_{|A} = f$



Denotaremos $\psi(p(x)) = p(b)$.

* $A[x_1, \dots, x_n] = (A[x_1, \dots, x_{n-1}])[x_n] = \{ p(x_1, \dots, x_n) = \sum_{i_1, \dots, i_n} a_{i_1 \dots i_n} x_1^{i_1} \cdots x_n^{i_n} \}$

≡ anillo de polinomios en n indeterminados con coef. en A.

* Dado $p(x_1, \dots, x_n) \neq 0$, se define $gr(p(x_1, \dots, x_n)) = \max \{ i_1 + \dots + i_n : a_{i_1, \dots, i_n} \neq 0 \}$.

Teorema (Prop. Univ. del Anillo de Pol): Sea $f : A \to B$ mor anillos. Para cada $b_1, \dots, b_n \in B$. $\exists!$ mor de anillos $\psi : A[x_1, \dots, x_n] \to B$: $\psi(x_i) = b_i$ y $\psi_{|A} = f$. Además $\psi(p(x_1, \dots, x_n)) = p(b_1, \dots, b_n)$. SIN DEM

Corolario: A íntegro $\Rightarrow A[x_1, \dots, x_n]$ íntegro y $A[x_1, \dots, x_n]^* = A^*$

ANILLO COCIENTE

* Si $\mathfrak{a}$ es unidad de A, $(\mathfrak{a},+)$ es subgrupo, así que se define rel. de eq.

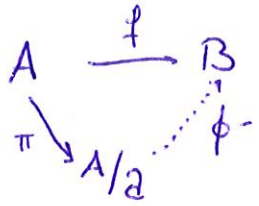
$$a \equiv b \iff b - a \in \mathfrak{a}$$

y $A/\mathfrak{a} = \{\bar{a} = a + \mathfrak{a} \equiv$ clase de restos (mód $\mathfrak{a}$) : $a \in A\} \equiv$ conjunto cociente

Teorema (Estructura de Anillo en el Cociente): Sea $\mathfrak{a}$ ideal de un anillo A. $\exists$ estructura de anillo en $A/\mathfrak{a}$: $\pi : A \longrightarrow A/\mathfrak{a}$ es un morfismo de anillos. Además, $\ker \pi = \mathfrak{a}$.

Teorema: (Prop. Univ. del Anillo Cociente): Sea $\mathfrak{a}$ ideal de un anillo A y $f : A \to B$ un morfismo de anillos y $\pi : A \longrightarrow A/\mathfrak{a}$ la proy. canónica.

$$\mathfrak{a} \subseteq \ker f \iff \exists\, \phi : A/\mathfrak{a} \longrightarrow B : f = \phi \circ \pi$$



Teorema (de (sonofi-): Sea $f : A \to B$ morfismo de anillos.

$$\boxed{A/\ker f \simeq \operatorname{Im} f}$$

$$[a] \longleftrightarrow f(a)$$

Teorema (Chino de los Restos): Sean $\mathfrak{a}, \mathfrak{b}$ ideales de A. Si $A = \mathfrak{a} + \mathfrak{b}$,

$$A/\mathfrak{a}\cap\mathfrak{b} \simeq A/\mathfrak{a} \times A/\mathfrak{b}$$

$$[a]_{\mathfrak{a}\mathfrak{b}} \longleftrightarrow ([a]_{\mathfrak{a}}, [a]_{\mathfrak{b}})$$

Teorema: Sea $\mathfrak{a}$ un ideal de A.

a) $\mathfrak{a}$ ideal primo $\iff$ $A/\mathfrak{a}$ íntegro

b) $\mathfrak{a}$ ideal maximal $\iff$ $A/\mathfrak{a}$ cuerpo

Corolario: $\operatorname{Spec}_{max} A \subseteq \operatorname{Spec} A$

Corolario: Sean $a_1, \dots, a_n \in K$ fijos y sea $\mathfrak{m} := \{p(x) \in K[x_1, \dots, x_n] : p(a_1, \dots, a_n) = 0\}$

a) $K[x_1, \dots, x_n]/\mathfrak{m} \simeq K$

b) $\mathfrak{m}$ es maximal

c) $\mathfrak{m} = (x_1 - a_1, \dots, x_n - a_n)$

Proposición: $[m]$ invertible en $\mathbb{Z}/n\mathbb{Z} \iff m$ primo con n.

Además, si $1 = \alpha m + \beta n$, $\underline{[m]^{-1} = [\alpha]}$

Corolario: $(\mathbb{Z}/n\mathbb{Z}, +, \cdot)$ cuerpo $\iff n$ primo

POLINOMIOS CON COEF. EN K

Teorema (de División de Polinomios): Sean $p(x) = a_n x^n + \dots + a_0$, $q(x) = b_d x^d + \dots + b_0 \in A[x]$, con $a_n \in A^*$. Existen polinomios $c(x), r(x) \in A[x]$: $q(x) = p(x) \cdot c(x) + r(x)$, con $\operatorname{gr}(r(x)) < \operatorname{gr}(p(x))$ ó $r(x) = 0$. $\overline{\text{Ojo: } q(x) - \frac{b_d}{a_n} x^{d-n} \cdot p(x)}$

Definición: Se dice que un polinomio $p(x) \in K[x]$ es irreducible si no existen polinomios $g(x), r(x) \in K[x]$, con $1 \le \operatorname{gr}(g(x)), \operatorname{gr}(r(x)) < \operatorname{gr}(p(x))$ tal que $p(x) = g(x) \cdot r(x)$. Es decir, si en toda factorización $p(x) = g(x) \cdot r(x)$ $g(x)$ ó $r(x)$ son ctes (con $\operatorname{gr} = 0$).

Definición: Diremos que $a \in k$ es una raíz de $p(x) \in k[x]$ si: $p(a) = 0$.

Teorema: Si un polinomio $p(x) = c_n x^n + \dots + c_0$, $c_n \neq 0$, $c_i \in \mathbb{Z}$, tiene la raíz $\frac{a}{b} \in \mathbb{Q}$, irreducible ($a, b$ primos) $\Rightarrow$ b divide a c_n y a divide a c_0.

* Este Th permite hallar todas las raíces en $\mathbb{Q}$ de un pol con coef en $\mathbb{Q}$. Las posibles raíces racionales son $\frac{\{\text{divisores de } c_0\}}{\{\text{divisores de } c_n\}}$.

Teorema: $p(x) \in k[x]$, $gr(p(x)) = 1 \Rightarrow p(x)$ irreducible en $k[x]$ y $\exists$ raíz.

Teorema (Regla de Ruffini): Sea $p(x) \in A[x]$, $a \in A$, A anillo. El resto de la división de $p(x)$ por $(x-c) \Rightarrow p(c)$. Por tanto, a raíz de $p(x) \iff p(x) = (x-c)\,g(x)$.

Corolario I: $p(x) \in k[x]$ irreducible, $gr(p(x)) > 1 \Rightarrow \nexists$ raíces $\in k$

Corolario II: $p(x) \in k[x]$, $gr(p(x)) = 2$ ó 3, $p(x)$ irreducible en $k[x] \iff \nexists$ raíces $\in k$

Corolario III: $p(x) \in k[x]$, $a_1, \dots, a_n \in k$ raíces $\Rightarrow (x-a_1) \cdot \dots \cdot (x-a_n)$ divide a $p(x)$

Corolario IV: El número de raíces de un polinomio $0 \neq p(x) \in k[x]$ no supera su grado

Teorema (de D'Alembert ó Fundamental del Álgebra): Todo polinomio no nulo en $\mathbb{C}[x]$ tiene alguna raíz compleja.

Corolario: en $\mathbb{C}[x]$, irreducible $\iff$ gr 1

Corolario: en $\mathbb{R}[x]$ irreducible $\iff$ $\begin{cases} \text{gr } 1 \\ \text{ó} \\ \text{gr } 2 \text{ sin raíces en } \mathbb{R} \end{cases}$

Lema: $p\mathbb{Z}[x]$ es un ideal primo.

Lema (Gauss): $cte \neq p(x) \in \mathbb{Z}[x]$ irreducible $\Rightarrow$ $p(x)$ irreducible en $\mathbb{Q}[x]$.

Criterio de Reducción: Sea $q(x) = a_n x^n + \dots + a_0 \in \mathbb{Z}[x]$, y sea p primo : $c_n \notin p\mathbb{Z}$.

Si los coef. de $q(x)$ no tienen factores primos comunes, y la reducción $\bar{q}(x) = \bar{a}_n x^n + \dots + \bar{a}_0 \in \mathbb{F}_p[x]$ es irreducible en $\mathbb{F}_p[x] \Rightarrow q(x)$ irreducible en $\mathbb{Z}[x]$ y $\mathbb{Q}[x]$.

Criterio de Einstein: Dado $q(x) = c_n x^n + \dots + c_0 \in \mathbb{Z}[x]$, si $\exists$ p primo tal que

1) $c_0, \dots, c_n$ no tienen factores irreducibles comunes en $\mathbb{Z}$
2) p divide a $c_0, \dots, c_{n-1}$
3) p^2 no divide a c_0

$\Rightarrow$ $q(x)$ irreducible en $\mathbb{Z}[x]$ y $\mathbb{Q}[x]$.

Criterio de Nietsnesie: Dado $q(x) = c_n x^n + \dots + c_0 \in \mathbb{Z}[x]$, si $\exists$ p primo tal que

1) $c_0, \dots, c_n$ no tienen factores primos comunes.
2) p divide a $c_1, \dots, c_n$
3) p^2 no divide a c_n

$\Rightarrow$ $q(x)$ irreducible en $\mathbb{Z}[x]$.

Corolario: $x^{p-1} + \dots + x + 1$ es irreducible en $\mathbb{Z}[x]$ y $\mathbb{Q}[x]$.

Congruencia de Euler: $((\mathbb{Z}/n\mathbb{Z})^*, \cdot)$ grupo cultivo, ϕ de n, si

a y n primos entre sí, $\Rightarrow a^{\phi(n)} \equiv 1 \mod(n)$

Prop. indicador Euler:

1) $\phi(p^r) = (p-1)\,p^{r-1}$, p primo

2) $\phi(n \cdot m) = \phi(n) \cdot \phi(m)$, n, m primos entre sí.

Congruencia de Fermat: $a \in \mathbb{Z}$, $a \notin p\mathbb{Z} \Rightarrow a^{p-1} \equiv 1 \mod(p)$.

Corolario: $a^p \equiv a \mod(p)$. $\forall a \in \mathbb{Z}$, p primo.

DIP

Definición: Se dice que un ideal I es principal si está generado por algún elemento, es decir, si $I = (a)$. Se dice que un anillo íntegro A es un dominio de ideales principales si todo ideal es principal.

- Se deducen directamente
  - Id Bézout: $\exists \alpha, \beta$: $d = \mathrm{mcd}(a,b) = \alpha a + \beta b$
  - Corolario: a, b primos entre sí, $\exists \alpha, \beta \in A$: $1 = \alpha a + \beta b$.

Lema: Si n divide a ab, y es primo con b $\Rightarrow$ n divide a a.

Lema (Euclides): Sea p un elemento no nulo de un DIP A. Son equivalentes:

1) p irreducible en A
2) (p) ideal maximal
3) (p) ideal primo

Proposición: En un DIP, todo cadena de ideales estabiliza.

Teorema: Todo elemento propio de un DIP descompone de forma única salvo orden y factores invertibles en producto de factores irreducibles: $a = p_1 \cdot \ldots \cdot p_n$, $n \geq 1$.

Definición: Dado $p(x) \in K[X]$, y $\alpha \in K$ es una raíz de $p(x)$, llamamos multiplicidad de la raíz α al mayor m tal que $(x-\alpha)^m$ divide a $p(x)$.

* Si $p(x) = c_0 x^n + \ldots + c_{n-1} x + c_n$ tiene todas sus raíces $\alpha_1, \ldots, \alpha_n \in K$, por Ruffini se tiene $c_0 x^n + \ldots + c_{n-1} x + c_n = c_0 (x-\alpha_1) \cdot \ldots \cdot (x-\alpha_n)$ e igualando coeficientes se obtiene:

$$\boxed{(-1)^r \frac{c_r}{c_0} = \sum_{i_1 < \ldots < i_r} \alpha_{i_1} \cdot \ldots \cdot \alpha_{i_r}} \qquad 1 \leq r \leq n.$$

III : MÓDULOS

Definición: Sea A un anillo conmutativo con unidad y sea M un conjunto dotado de una ley $M \times M \xrightarrow{+} M$ y una acción $A \times M \to M$.

$$(M, +, \cdot) \text{ } A\text{-módulo} \iff \begin{cases} 1) & (M,+) \text{ grupo Abeliano} \\ 2) & a\cdot(m+n) = am + an \\ 3) & (a+b)m = am + bm \\ 4) & (ab)m = a(bm) \\ 5) & 1 \cdot m = m \end{cases} \quad \begin{array}{l} \forall a, b \in A \\ m, n \in M. \end{array}$$

Definiciones:

* Una aplicación $f: M \to N$ es un **morfismo de A-módulos** si

$$f(m+m') = f(m) + f(m')$$
$$f(am) = a f(m)$$

diremos que es **isomorfismo** de A-módulos si es biyectiva ($\exists f^{-1}$ isom. de A-mód.)

* Diremos que $N \subset M$ es un **submódulo** si $an \in N \quad \forall a \in A, n \in N$.

* $\ker f$, $\operatorname{Im} f$ son submódulos (de M y N, resp). La intersección y suma de submódulos es un submódulo.

* K-módulos $\equiv$ K-espacio vectorial

* $\mathbb{Z}$-módulos $\equiv$ subgrupos

* E k-ev, $T \in \mathrm{End}(E)$, llevamos E_T al $k[x]$-módulo que induce $p(x)\cdot e = p(T)(e)$.

* $Am_1 + \dots + Am_n = \langle m_1, \dots, m_n \rangle = \{a_1 m_1 + \dots + a_n m_n : a_i \in A\} \equiv$ submódulo generado por $m_1, \dots, m_n$

* $\partial M = \{a_1 m_1 + \dots + a_n m_n : a_i \in \partial\}$ (∂ ideal).

* Producto directo $\equiv \prod_{i\in I} M_i = M_1 \times M_2 \times \dots$ ($M_i = M\ \forall i$) $= M^I$

* Suma directa $\equiv \bigoplus_{i\in I} M_i = \{(m_i)_{i\in I} : \text{todas las coords nulas salvo finitas}\} = M^{(I)}$

* $\bigoplus_{i\in I} M_i = \prod_{i\in I} M_i$ si $\#I < +\infty$. Todos son módulos con $a\cdot(m_i)_{i\in I} := (am_i)_{i\in I}$.

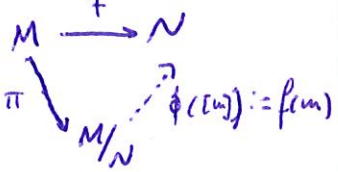
* Si $N_1, \dots, N_r$ son submódulos, dicen que N es suma directa si: $N_1 \oplus \dots + N_r \simeq N_1 + \dots + N_r$.

MÓDULO COCIENTE

Con M $g.a.$, se induce una rel. de eq. $m \equiv m' \ (\mathrm{mód}\ N) \Leftrightarrow m - m' \in N$, y la operación $a\cdot[m] = [am]$ define en M/N una estructura de A-módulo.

Teorema (Prop. Univ. del Módulo Cociente): N subm. de M A-módulo, $\pi : M \to M/N$, $f : M \to M'$ mf. de A-mód.

$$N \subseteq \ker f \iff \exists!\ \text{mf. de } A\text{-módulos } \phi : M/N \to M' : f = \phi \circ \pi.$$



Teorema (de Isomorfía):

$$\boxed{\begin{array}{c} M/\ker\varphi \simeq \mathrm{Im} f \\ [m] \longleftrightarrow f(m) \end{array}}$$

Corolario: M_1, M_2 módulos, N_1, N_2 submódulos respectivos, entonces

$$\frac{M_1 \oplus M_2}{N_1 \oplus N_2} \simeq M_1/N_1 \oplus M_2/N_2$$

Teorema: $\pi: M \to M/N$, $P \subset M/N$ (submód.) $\Rightarrow \pi^{-1}(P)$ es un submódulo de M que contiene a N. En particular,

$$\{\text{submódulos de } M/N\} = \{\text{subm. de } M : N \subset \text{subm.}\}$$

$$\bar{P} \longmapsto \pi^{-1}(\bar{P})$$

$$\pi(P) \longleftarrow P$$

Ejercicio: $P \subseteq \pi^{-1}(\pi(P)) = P + \ker \pi = P$ (pues $N \subseteq P$)

Corolario: $I \subset A$ ideal, $\pi: A \to A/I$.

$$\{\text{ideales de } A/I\} = \{\text{ideales de } A : I \subset \text{ideal}\}$$

Además, si $\bar{J} \subset A/I$ es el ideal correspondiente a $I \subset J \subset A$, $A/J \simeq \frac{A/I}{\bar{J}}$

Teorema: Todo anillo no nulo tiene algún ideal maximal.

Corolario: Todo ideal $\neq A$ está contenido en algún ideal maximal de A.

Corolario: $a \in A^* \iff a \notin$ algún ideal maximal

MÓDULOS LIBRES

Definición: Cada familia $\{m_1, \dots, m_n\}$ define un morfismo $\phi: A^n \to M$, $(a_1, \dots, a_n) \mapsto a_1 m_1 + \dots + a_n m_n$.

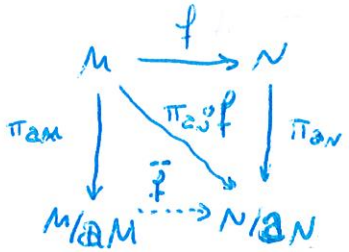
Diremos que $\{m_i\}$ forma un *sistema de generadores* de M cuando $M = \langle m_1, \dots, m_n \rangle$, i.e., cuando ϕ sea epiyectivo; y diremos que son *A-L.I.* cuando ϕ sea inyectivo; y diremos que son *base* cuando ϕ sea isomorfismo.

Definición: M se dice de **tipo finito** si admite algún sistema finito de generadores. En particular, diremos que un A-módulo de tipo finito L es **libre** si admite base (ie, si $L \simeq A^n$ para algún $n \in \mathbb{N}$). Llamaremos **rango de L** al número de elementos de la base.

* $f: M \to M'$, M, M' fin.gen; f epi $\Rightarrow$ manda generadores a generadores.

Proposición: Todas las bases de un A-módulo libre tienen el mismo número de elementos.

Para poder probar esto, hay que considerar que dado $\mathfrak{a} \subset A$, en $M/\mathfrak{a}M$ hay una estructura natural de $A/\mathfrak{a}$-módulo, con la operación $[a] \cdot [m] := [a \cdot m]$. Si $f: M \to N$ es un A-mód, $f(\mathfrak{a}M) \subseteq \mathfrak{a}N$, hay $\mathfrak{a}M \subseteq \ker(\pi_{\mathfrak{a}N} \circ f)$, hay podemos aplicar la PUMC.



$\exists\, \bar{f}: M/\mathfrak{a}M \to N/\mathfrak{a}N$, $[m] \mapsto [f(m)]$

Y si f epi $\Rightarrow$ $\bar{f}$ epi.

Definición: Diremos que una sucesión $\cdots \to M_{i-1} \xrightarrow{f_i} M_i \xrightarrow{f_{i+1}} M_{i+1} \to$ es **exacta** en el término M_i cuando $\operatorname{Im} f_i = \ker f_{i+1}$. Se dice que una suc. es exacta cuando lo es $\forall i$. Se dice que es exact. corta cuando empieza y termina en 0.

Teorema: $0 \to M' \xrightarrow{i} M \xrightarrow{p} L \to 0$ es exacta, L libre $\Rightarrow \exists\, s: L \to M$: $ps = \mathrm{Id}_L$. Además, $M \simeq M' \oplus L$.

epi: $m - sp(m)$

* Dado $f: M \to N$, llamaremos $\operatorname{Coker} f = N/\operatorname{Im} f$. Así,

f epi $\Leftrightarrow \operatorname{Im} f = N \Leftrightarrow \operatorname{Coker} f = 0$
f inj $\Leftrightarrow \ker f = 0$
$\Rightarrow f$ isom. $\Leftrightarrow \ker f = 0 = \operatorname{Coker} f$.

TEOREMAS DE DESCOMPOSICIÓN

Ahora A = D.I.P.

Proposición: Todo submódulo de un módulo libre de rango finito r es también libre de rango $\leq r$.

Corolario: Todo submódulo de un A-módulo finito generado es también finito generado.

Definición: Se dice que $m \in M$ es de **torsión** si $\exists\, a \in A \setminus \{0\} : am = 0$. (ie, $\ker(A \xrightarrow{a\cdot m} M) \neq 0$)

$T(M) = \{$ elems de torsión de $M \}$, que es un submódulo.

Se dice que M es de torsión si $T(M) = M$; y que carece de torsión si $T(M) = 0$.

En general, $T(A \oplus B) = T(A) \oplus T(B)$.

Lema: M finito generado, $T(M) = 0 \Rightarrow M$ libre.

Teorema (Primer Teorema de Descomposición): Todo A-módulo finito generado descompone de forma única salvo isomorfismos en suma directa de un A-módulo libre y de un A-módulo de torsión:

$$M \simeq (A \oplus \overset{r)}{\cdots} \oplus A) \oplus T(M)$$

y se dice que r es el **rango** de M.

Definición: Llamaremos **ideal anulador** de un elemento $m \in M$ a

$$\mathrm{Ann}\langle m \rangle = \{a \in A : am = 0\} = \ker(A \xrightarrow{\cdot m} M)$$

y llamaremos **ideal anulador** de un A-módulo M a

$$\mathrm{Ann}\, M = I = \{a \in A : aM = 0\} = \bigcap_{m \in M} \mathrm{Ann}\langle m \rangle \overset{A \text{ DIP}}{=} (\alpha)$$

α anulador de M.

* $\mathrm{Ann}(A/bA) = bA$.

* $\mathrm{Ann}(A \oplus B \oplus C) = \mathrm{Ann}(A) \oplus \mathrm{Ann}(B) \oplus \mathrm{Ann}(C)$. En general

* $N, P \subseteq M$, $N+P = M$, $N \cap P = 0 \Rightarrow \underline{N \oplus P \simeq M}$.

Lema: Si p, q primos entre sí, y $\ker a^k := \{m \in M : a^k m = 0\}$,

$$\ker pq = \ker p \oplus \ker q.$$

Teorema (Segundo Teorema de Descomposición): Sean $p_1^{n_1} \cdots p_s^{n_s}$ la descomposición en factores irreducibles del anulador de un A-módulo M. M descompone de modo único en suma directa de submódulos M_i anulados por $p_i^{n_i}$:

$$M = \ker p_1^{n_1} \oplus \cdots \oplus \ker p_s^{n_s}$$

Lema: Todo elemento del anillo $B = A/p^n A$, con p irreducible, es de la forma $b = u[p]^r$, donde u es invertible y $1 \le r \le n$. Además, $B/bB \simeq A/p^n A$.

Teorema (Tercer Teorema de Descomposición): Sea $p \in A$ un elemento irreducible. Si un A-módulo finito-generado está anulado por alguna potencia de p, $\exists$ sucesión decreciente $n_1 \ge \cdots \ge n_s$ tal que

$$M \simeq \left(A/p^{n_1}A\right) \oplus \cdots \oplus \left(A/p^{n_s}A\right)$$

*

* Aplicando los 3 Th. de Descomposición (aplicar el 2º a la parte de torsión del 1º; y el 3º a cada uno de los sumandos del 2º), Vemos que

$$M \simeq \left(A \oplus \overset{r)}{\cdots} \oplus A\right) \oplus \left(\bigoplus_{i,j} A/p_i^{n_{ij}} A\right)$$

Definición: Llamamos rango del cálculo A-módulo finitamente generado a r y a cada $p_i^{n_{ij}}$ divisores elementales.

Teorema (de Clasificación de A-módulos (1ª versión)):

Dos módulos son isomorfos $\iff$ tienen el mismo rango y los mismos factores invariantes.

Teorema (Factores Invariantes): Dado M A-módulo finitamente generado, $\exists$ sucesión creciente de ideales

$\phi_1 A \subseteq \phi_2 A \subseteq \cdots \subseteq \phi_m A$ tal que

$$M \simeq A/\phi_1 A \oplus \cdots \oplus A/\phi_m A$$

Definición: Llamamos factores invariantes de M a los dados $\phi_1, \ldots, \phi_m$. Nota que ϕ_1 es el anulador del módulo.

CLASIFICACIÓN DE GRUPOS ABELIANOS

Corolario: Todo grupo abeliano descompone de modo único salvo orden, en suma directa de:

* Grupos cíclicos infinitos y grupos cíclicos de órdenes de potencias de primo, si G finitamente generado
* " " " " " " " " " si G finito

Corolario (Recíproco de Lagrange): Si $d \in \mathbb{N}$ divide al orden de un grupo abeliano finito $\Longrightarrow \exists$ algún subgrupo de G de orden d.

Corolario: G g.a. finito-generado.

G finito $\Longleftrightarrow$ rg $G = 0$ $\Longleftrightarrow$ $\phi_1 \neq 0$ (el ordenado)

y además, $|G| = \phi_1 \cdots \phi_m$

Corolario: Sea G g.a. finito generado

G cíclico $\Longleftrightarrow$ G sólo tiene un único factor invariante.

CÁLCULO DE FACTORES INVARIANTES

* El 3$^{\text{er}}$ Th asegura que dado un A-módulo finito generado, hay dos módulos libres tal que

$$L_n \longrightarrow L_m \longrightarrow M \longrightarrow 0$$

es una presentación ($\equiv$ suc. exacta) de M. Al ser exacta, se dice que $\text{Coker } f = L_m / \text{Im } f \simeq M$. Manipulando la matriz de f con transformaciones elementales, podemos hacerla diagonal, y se puede probar que los coef. de su diagonal son los factores invariantes de $\text{Coker } f \simeq M$.

* Sistema de ec. diofánticas: $AX = Y$, $A \xrightarrow{\text{trasf. elem.}} \bar{A}$ diagonal, para $\bar{A} = C^{-1}AB$ $\Rightarrow$ $AX = Y \Leftrightarrow \bar{A}\bar{X} = \bar{Y}$. Resolvemos este sistema (diagonal)

(C: cambios por filas; B: cambios por columnas)

y ahora $\boxed{X = B\bar{X}}$.

La matriz B se calcula poniendo una identidad al lado de A al hacer las trasf. elem. para llevar la cuenta de los cambios por columnas.

* Compatibilidad de un sistema (con parámetros): no hace falta llevar la matriz de la B, sólo hay que decir cuándo uno de los elementos de la diagonal por hacer cero es igual a los parámetros. Hecho, y decir que "el sistema es compatible precisamente cuando ___ sea múltiplo de ___".

* Clasificar un grupo abeliano G def por unas ecuaciones: Se define un morfismo de módulos de $\mathbb{Z}^{\text{nº de ecua.}} \xrightarrow{f} \mathbb{Z}^{\text{nº de generadores de } G}$, donde $f \equiv A$ = matriz con los coef. de cada ec. por columnas. El 3er Th Desc. dice que se puede construir una suc. exacta que vaya de $\mathbb{Z}^{\text{nº de gen.}} \longrightarrow G$, y por tanto, $G \simeq \operatorname{Coker} f = \mathbb{Z}^{\text{nº gen}} / \operatorname{Im} f$.
Se puede demostrar que los elementos de la matriz reducida de f son los factores invariantes de $\operatorname{Coker} f$, y por tanto de G, y queda definido.

* Clasificar un submódulo de $\mathbb{Z}^n/M$ generado por unos elementos: Se define un morf. de módulos $\mathbb{Z}^{\text{nº de generadores}} \xrightarrow{f} \mathbb{Z}^n$, donde $\operatorname{Im} f = M$. Se reduce la matriz de f, y los vectores columna son la base de M. $\mathbb{Z}^3/M = \mathbb{Z}^3/\operatorname{Im} f = \operatorname{Coker} f$, que queda def por los factores invariantes.

$$G \simeq \underbrace{\mathbb{Z}}_{\text{parte libre}} \oplus \underbrace{\mathbb{Z}/a\mathbb{Z} \oplus \mathbb{Z}/s\mathbb{Z} \oplus}_{\text{parte de torsión}}$$

* G finito si no tiene parte libre (si ϕ's $\neq 0$); infinito si algún $\phi = 0$.
* G cíclico si $G \simeq \mathbb{Z}$ ó $G \simeq \mathbb{Z}/n\mathbb{Z}$; no cíclico si no. (cíclico es sólo 1 fact. inv.)
* G libre si sólo tiene parte libre.
* $\operatorname{Ann}(G) = \phi_1$
* $T(G)$ = parte de torsión

Torsion :

* G grp fnto $\Rightarrow$ G torsion
* $T(M \oplus N) = T(M) \oplus T(N)$
* L libre $\Rightarrow$ L sans de torsion (M fnto gener, $T(M) = 0 \iff M$ libre)

Annul :

* $\mathrm{Ann}(L) = 0$ (L libre)
* $\mathrm{Ann}(M) \neq 0 \Rightarrow M$ de torsion
* $\mathrm{Ann}(M) \neq 0$ $\Leftarrow$ fint. gen, de torsion
* $\mathrm{Ann}(A/\mathfrak{a}) = \mathfrak{a}$
* $\mathrm{Ann}(M \oplus M' \oplus M'') = \bigcap \mathrm{Ann}\, M_i$