Álgebra

Juan Dodyk

Índice

Categorías 1
Grupos 2
Grupos finitos 4
Condiciones de cadena 6
Anillos 8
Polinomios 10
Módulos I 12
Módulos II 16
Extensiones de cuerpos 19
Geometría algebraica 22

Categorías Una *categoría* (localmente chica) $\mathcal{C}$ consta de una clase de *objetos* $\operatorname{Obj}\mathcal{C}$ (notada $\mathcal{C}$; si es un conjunto la categoría se dice *chica*) y, para cada par de objetos X e Y, un conjunto de *flechas* o *morfismos* $\operatorname{Hom}_{\mathcal{C}}(X,Y)$ (notada $\mathcal{C}(X,Y)$), de manera que *i.* los conjuntos de flechas son disjuntos de manera que a cada flecha f le corresponde un *dominio* $\operatorname{dom} f = X$ y *codominio* $\operatorname{cod} f = Y$ con $f \in \mathcal{C}(X,Y)$, *ii.* para tres objetos X, Y, Z hay una función $\mathcal{C}(X,Y) \times \mathcal{C}(Y,Z) \to \mathcal{C}(X,Z)$ que se nota $(f,g) \mapsto f \circ g$, *iii.* $(f \circ g) \circ h = f \circ (g \circ h)$ si f, g, h son morfismos y la operación tiene sentido, y *iv.* para todo objeto X hay un morfismo $1_X \in \mathcal{C}(X,X)$ tal que $f \circ 1_X = f$ y $1_X \circ f = f$ para toda f cuando la operación tiene sentido. Notamos $f : X \to Y$ o $X \xrightarrow{f} Y$ en lugar de $f \in \mathcal{C}(X,Y)$. Definimos la *categoría opuesta* $\mathcal{C}^{\mathrm{op}}$ de $\mathcal{C}$ de manera que $\operatorname{Obj}\mathcal{C}^{\mathrm{op}} = \operatorname{Obj}\mathcal{C}$ y $\mathcal{C}^{\mathrm{op}}(X,Y) = \mathcal{C}(Y,X)$. Una categoría se dice *discreta* si sus únicos morfismos son los 1_X, $X \in \mathcal{C}$; la categoría vacía se llama 0; la categoría discreta de un objeto se llama 1; la de dos, 2; los conjuntos forman la categoría Set; dadas categorías $\mathcal{C}, \mathcal{D}$ se define $\mathcal{C} \times \mathcal{D}$ por $\operatorname{Obj}(\mathcal{C} \times \mathcal{D}) = \operatorname{Obj}\mathcal{C} \times \operatorname{Obj}\mathcal{D}$ y $\mathcal{C} \times \mathcal{D}(A \times B, A' \times B') = \mathcal{C}(A,A') \times \mathcal{D}(B,B')$. Si $fg_1 = fg_2$ implica $g_1 = g_2$ para todos g_1, g_2 entonces f se dice *monic*; si $g_1 f = g_2 f$ implica $g_1 = g_2$ entonces f se dice *epic*; si $gf = 1$ entonces f se llama *sección* de g y g una *retracción* de f; si hay g con $gf = fg = 1$ entonces f se dice *isomorfismo* y si $f : X \to Y$ ponemos $X \cong Y$; si $f \in \mathcal{C}(X,X)$ se dice que es un *endomorfismo* y se nota $\operatorname{End}_{\mathcal{C}}(X) = \mathcal{C}(X,X)$; si $f \in \operatorname{End}_{\mathcal{C}}(X)$ es isomorfismo se dice *automorfismo* y se nota $f \in \operatorname{Aut}_{\mathcal{C}}(X)$.

Funtores. Un *funtor* (covariante) $F : \mathcal{C} \to \mathcal{D}$ es una asignación $F : \operatorname{Obj}\mathcal{C} \to \operatorname{Obj}\mathcal{D}$ y $F : \mathcal{C}(X,Y) \to \mathcal{D}(FX,FY)$ tal que $F(1_X) = 1_{FX}$ y $F(fg) = F(f)F(g)$; un *funtor contravariante* es un funtor de $\mathcal{C}$ a $\mathcal{D}^{\mathrm{op}}$; toda categoría $\mathcal{C}$ tiene un funtor identidad $1_{\mathcal{C}}$; un funtor es *fiel* (resp. *full*) si $F : \mathcal{C}(X,Y) \to \mathcal{D}(FX,FY)$ es inyectivo (resp. suryectivo). Si $F, G : \mathcal{C} \to \mathcal{D}$, una *transformación natural* $\eta : F \to G$ es una función $\eta : \mathcal{C}(A,B) \to \mathcal{D}(FA,GB)$ tal que $\eta(f) = \eta(1_B)F(f) = G(f)\eta(1_A)$; se escribe $\eta_A = \eta(1_A)$ y si $f \in \mathcal{C}(A,B)$ entonces el diagrama

$$\begin{tikzcd} \mathcal{F}A \arrow[r, "\eta_A"] \arrow[d, "\mathcal{F}(f)"'] & \mathcal{G}A \arrow[d, "\mathcal{G}(f)"] \\ \mathcal{F}B \arrow[r, "\eta_B"] & \mathcal{G}B \end{tikzcd}$$

conmuta. Dadas $\mathcal{C}$ y $\mathcal{D}$ armamos la categoría $[\mathcal{C},\mathcal{D}]$ o $\mathcal{D}^{\mathcal{C}}$ cuyos objetos son funtores $\mathcal{C}\to\mathcal{D}$ y cuyos morfismos son transformaciones naturales; $\eta: F\cong G$ sii todo η_A es un isomorfismo. Decimos que dos categorías $\mathcal{C},\mathcal{D}$ son *equivalentes*, $\mathcal{C}\simeq\mathcal{D}$, si hay funtores F,G e isomorfismos naturales $\eta: 1_{\mathcal{C}}\to G\circ F$ y $\epsilon: F\circ G\to 1_{\mathcal{D}}$; un funtor $F:\mathcal{C}\to\mathcal{D}$ es equivalencia sii es fiel, full y esencialmente suryectivo (para todo $B\in\mathcal{D}$ hay $A\in\mathcal{C}$ con $FA\cong B$).

Representables. Dado $A\in\mathcal{C}$ tenemos los funtores $H_A=\mathcal{C}(-,A):\mathcal{C}^{\text{op}}\to\text{Set}$ y $H^A=\mathcal{C}(A,-):\mathcal{C}\to\text{Set}$. En general tenemos funtores $H_\bullet:\mathcal{C}\to[\mathcal{C}^{\text{op}},\text{Set}]$ y $H^\bullet:\mathcal{C}^{\text{op}}\to[\mathcal{C},\text{Set}]$. Vale $A\cong A'$ sii $H_A\cong H_{A'}$ sii $H^A\cong H^{A'}$. Tenemos el funtor $\text{Hom}_{\mathcal{C}}:\mathcal{C}^{\text{op}}\times\mathcal{C}\to\text{Set}$ dado por $\text{Hom}_{\mathcal{C}}(f\times g)=g\circ -\circ f$. Lema de Yoneda: $[\mathcal{C}^{\text{op}},\text{Set}](H_A,X)\cong X(A)$ es un isomorfismo de funtores $\mathcal{C}^{\text{op}}\times[\mathcal{C}^{\text{op}},\text{Set}]\to\text{Set}$ (con $(A,X)\in\mathcal{C}^{\text{op}}\times[\mathcal{C}^{\text{op}},\text{Set}]$); en particular un morfismo $\alpha: H_A\to X$ está determinado por $\alpha_A(1_A)$, ya que $\alpha_B(f)=X(f)(\alpha_A(1_A))$; el funtor $H_\bullet:\mathcal{C}\to[\mathcal{C}^{\text{op}},\text{Set}]$ es full y fiel. Una *representación* de $X\in[\mathcal{C}^{\text{op}},\text{Set}]$ es un par (A,α) con $A\in\mathcal{C}$ y $\alpha: H_A\cong X$; están en correspondencia con pares (A,u), $u\in X(A)$ tales que para cada $B\in\mathcal{A}$ y $x\in X(B)$ hay un único $f:B\to A$ con $X(f)(u)=x$.

Adjunciones. Sean $\mathcal{C}\underset{G}{\overset{F}{\rightleftarrows}}\mathcal{D}$ funtores; decimos que son *adjuntos*, $F\dashv G$, si hay iso $\alpha_{A,B}:\mathcal{D}(F(A),B)\cong\mathcal{C}(A,G(B))$ de $[\mathcal{C}^{\text{op}}\times\mathcal{D},\text{Set}]$; en ese caso decimos que F es adjunta a izquierda de G y G es adjunta a derecha de F; notamos $\overline{q}=\alpha_{A,B}(q):A\to GB$ (con $q:FA\to B$) y $\overline{p}=\alpha^{-1}_{A,B}(p):FA\to B$ (con $p:A\to GB$) y $\overline{\overline{q}}=q$. Ejemplo en Set: $(-\times Y)\dashv(-)^Y$. Dada $\alpha:F\dashv G$ tenemos morfismos $\eta:1_{\mathcal{C}}\to G\circ F$ y $\epsilon:F\circ G\to 1_{\mathcal{D}}$, llamados la *unidad* y *counidad* de la adjunción, dados por $\eta_A=\overline{1_{FA}}$ y $\epsilon_B=\overline{1_{GB}}$; vale $\epsilon F\circ F\eta=1_F$ y $G\epsilon\circ\eta G=1_G$. Hay una correspondencia biunívoca entre adjunciones $\alpha:F\dashv G$ y pares (η,ϵ) tales que $\epsilon F\circ F\eta=1_F$ y $G\epsilon\circ\eta G=1_G$. Dados funtores $P:\mathcal{A}\to\mathcal{C}$, $Q:\mathcal{B}\to\mathcal{C}$ se define la *categoría coma* $(P\Rightarrow Q)$ con objetos (A,B,h), $A\in\mathcal{A}$, $B\in\mathcal{B}$, $h:P(A)\to Q(B)$ y morfismos $(f,g):(A,B,h)\to(A',B',h')$ con $f:A\to A'$, $g:B\to B'$ tales que $Q(g)h=h'P(f)$. Hay una correspondencia biunívoca entre adjunciones $\alpha:F\dashv G$ y morfismos $\eta:1_{\mathcal{C}}\to G\circ F$ tales que, para todo $A\in\mathcal{A}$, $\eta:A\to GFA$ es inicial en $(A\Rightarrow G)$ (con $A:1\to\mathcal{C}$, $A(\bullet)=A$). Sea $G:\mathcal{D}\to\mathcal{C}$ un funtor; G tiene una adjunta a izquierda sii, para cada $A\in\mathcal{C}$, $(A\Rightarrow G)$ tiene un objeto inicial.

Límites. Si $\mathcal{I}$ es una categoría chica y $D:\mathcal{I}\to\mathcal{C}$ un funtor, un *cono* en D es un objeto $A\in\mathcal{C}$ con flechas $(A\xrightarrow{q_i}D_i)_{i\in\mathcal{I}}$ tales que, si $i\xrightarrow{u}j$ en $\mathcal{I}$, $Du\circ q_i=q_j$; un *límite* en D es un cono $(L\xrightarrow{p_i}D_i)_{i\in\mathcal{I}}$ tal que para todo cono $(A\xrightarrow{q_i}D_i)_{i\in\mathcal{I}}$ hay un único $q:A\to L$ tal que $p_i\circ q=q_i$ para todo $i\in\mathcal{I}$; se nota $\varprojlim_{\mathcal{I}} D$; si existe es único salvo isomorfismo. Si $\mathcal{I}$ es vacía un límite es el objeto *final*. Si $\mathcal{I}$ es discreta un límite es el *producto* $\prod_{i\in\mathcal{I}}D_i$. Si $\mathcal{I}$ es $\bullet\rightrightarrows\bullet$ un límite es el *ecualizador* para $X\underset{g}{\overset{f}{\rightrightarrows}}Y$. Si $\mathcal{I}$ es $\begin{array}{ccc} & & \bullet \\ & & \downarrow \\ \bullet & \to & \bullet\end{array}$ un límite es un *pull-back*. Set tiene todos los límites. Si $\mathcal{C}$ tiene productos y ecualizadores tiene todos los límites; si tiene final y pull-backs tiene todos los límites finitos. Si $\mathcal{I}$ es chica, definimos el *funtor diagonal* $\Delta:\mathcal{C}\to[\mathcal{I},\mathcal{C}]$ por $\Delta A(f)=1_A$; dado $D:\mathcal{I}\to\mathcal{C}$, un límite es una representación del funtor $[\mathcal{I},\mathcal{C}](\Delta -,D):\mathcal{C}^{\text{op}}\to\text{Set}$. Si $\mathcal{C}$ tiene todos los límites desde $\mathcal{I}$ entonces $\varprojlim_{\mathcal{I}}:[\mathcal{I},\mathcal{C}]\to\mathcal{C}$ es un funtor adjunto a derecha al diagonal: $[\mathcal{I},\mathcal{C}](\Delta A,D)\cong\mathcal{C}(A,\varprojlim_{\mathcal{I}}D)$.

Grupos Un *semigrupo* consta de un conjunto S y una operación $\cdot:S^2\to S$ tal que $(a\cdot b)\cdot c=a\cdot(b\cdot c)$; forman una categoría con los morfismos $\text{Hom}(M,M')$ que son las funciones $f:M\to M'$ tales que $f(ab)=f(a)f(b)$. Un *monoide* M es un semigrupo con un *elemento neutro* $e\in S$ tal que $a\cdot e=e\cdot a$; todo semigrupo se puede meter en un monoide agregando un elemento que hace de neutro; definimos el *monoide libre* sobre un conjunto X como el conjunto de secuencias finitas sobre X con la operación concatenación. Un elemento $a\in M$ se dice *inversible* si hay $a^{-1}\in M$ con $aa^{-1}=a^{-1}a=e$. Un *grupo* es un monoide G en el que todo elemento es inversible; por ejemplo el grupo 0 con un solo elemento. Un grupo se dice *abeliano* si es conmutativo; si G y G' son abelianos le podemos dar estructura de grupo abeliano también a $\text{Hom}(G,G')$ con la suma $(f+g)(x) = f(x)+g(x)$. Si M es un monoide, el conjunto $\mathcal{U}(M)$ de elementos inversibles de M tiene estructura de grupo, el *grupo de unidades* de M. Si $\mathcal{C}$ es una categoría y X es un objeto, $\mathrm{Aut}(X)$ tiene estructura de grupo, el *grupo de automorfismos* de X. En particular, en la categoría de conjuntos, llamamos S_X a $\mathrm{Aut}\, X$, el *grupo simétrico* de X, que consta de todas las biyecciones de X en X.

Subgrupos. Un *subgrupo* H de G es un subconjunto tal que $(H, \cdot|_{H^2})$ es un grupo; se nota $H \leq G$. Si $H \leq G$ definimos la relación $\sim\, \in G^2$ dada por $a \sim b$ sii $ab^{-1} \in H$; las clases de equivalencia son Hg para algún $g \in G$ y se llaman *coclases*; se ve que hay biyecciones entre todo par y, luego, si $(G : H)$, el *índice* de H, es el cardinal de las clases se tiene $|G| = (G : H)|H|$. Si $a \sim b$ implica $ca \sim cb$ o sea que $gHg^{-1} = H$ entonces las clases tienen una estructura de grupo dada por la operación $[x][y] = [xy]$; en ese caso se dice que H es *normal* en G, lo cual se nota $H \lhd G$, y el grupo de las clases se llama *grupo cociente* G/H. Si $f \in \mathrm{Hom}(G, G')$ se tiene $\mathrm{Im}\, f \leq G'$ y *núcleo* $\ker f = \{g \in G \mid f(g) = e\} \lhd G$; f es *epimorfismo* sii $\mathrm{Im}\, f = G'$ y *monomorfismo* sii $\ker f = 0$; isomorfismo sii es mono y epi. Tenemos el morfismo *proyección* $p_H : G \to G/H$ dado por $p_H(x) = [x]$ con núcleo H. El cociente queda determinado por la siguiente propiedad universal: si $f \in \mathrm{Hom}(G, G')$ con $H \lhd G$ y $H \leq \ker f$ entonces existe un único morfismo $\hat{f} \in \mathrm{Hom}(G/H, G')$ tal que $\hat{f} \circ p_H = f$. Tenemos que $\mathrm{Hom}(G, G')$ es la unión disjunta de los conjuntos $\{f \in \mathrm{Hom}(G, G') \mid \ker f = H\}$, donde H recorre los subgrupos normales de G. A su vez $f \mapsto \hat{f}$ es una biyección de $\{f \in \mathrm{Hom}(G, G') \mid \ker f = H\}$ a los monomorfismos de $\mathrm{Hom}(G/H, G')$ con inversa $\hat{f} \mapsto \hat{f} \circ p_H$.

Morfismos canónicos. *i.* Si $f \in \mathrm{Hom}(G, G')$ entonces $G/\ker f \cong \mathrm{Im}\, f$ dado por $\hat{f}$. *ii.* Si $K, H \lhd G$ con $K \lhd H$ entonces $\frac{G/K}{H/K} \cong G/H$ dado por $\hat{f}$ donde $f : xK \mapsto xH$. *iii.* Si $H, K \leq G$ con $k \in K \Rightarrow kHk^{-1} = H$ entonces $HK \leq G$, $H \lhd HK$ y $K/(H \cap K) \cong HK/H$ dado por $\hat{f}$ donde $f : k \mapsto kH$. *iv.* La proyección p_H de $H \lhd G$ manda subgrupos $H \lhd S \leq G$ en subgrupos $p_H(S) \leq G/H$ con $S/H \cong p_H(S)$ y p_H^{-1} es su inversa: dado $L \leq G/H$ lo manda a $H \lhd p_H^{-1}(L) \leq G$ con $p_H^{-1}(L)/H \cong L$; mantiene inclusiones e inclusiones normales. Lema de Zassenhaus: si $u \lhd U$, $v \lhd V$ son subgrupos de G entonces

$$u(U \cap v) \lhd u(U \cap V), \quad (u \cap V)v \lhd (U \cap V)v \quad \text{y} \quad \frac{u(U \cap V)}{u(U \cap v)} \cong \frac{(U \cap V)v}{(u \cap V)v}.$$

Viene de aplicar $H/(H \cap N) \cong HN/N$ a $H = U \cap V$, $N = u(U \cap v)$ y luego a $H = U \cap V$, $N = (V \cap u)v$.

Productos. Sean $H, K \leq G$. Si $HK = G$, $H \cap K = 0$ y $H, K \lhd G$ decimos que G es *producto directo interno* de H y K. Se ve que es equivalente a que $G = HK$ con factorización única $hk, h \in H, k \in K$ y $hk = kh$ para $h \in H, k \in K$. Definimos el *producto directo externo* de grupos H y K como el grupo $H \times K$ con operación $(h, k)(h', k') = (hh', kk')$. Se ve que $H, K \leq G$ están en producto directo interno si y sólo si $f : H \times K \to HK$ dado por $(h, k) \mapsto hk$ es isomorfismo. Si $H, K \leq G$ con $H \lhd G$, $HK = G$ y $H \cap K = 0$ decimos que G es *producto semidirecto interno* de H y K; se nota $G = H \rtimes K$. Si H y K son grupos y $\phi \in \mathrm{Hom}(K, \mathrm{Aut}\, H)$ definimos el *producto semidirecto externo* $H \times_\phi K$ como el conjunto $H \times K$ con la operación $(h, k)(h', k') = (h\phi(k)(h'), kk')$. Se tiene que si $G = H \rtimes K$ entonces $G \cong H \times_\phi K$ con $\phi : k \mapsto (h \mapsto khk^{-1})$, y $H \times_\phi K = (H \times 0) \rtimes (0 \times K)$; además $0 \times K \lhd H \times_\phi K$ si y sólo si ϕ es trivial.

Subgrupos generados, derivados y característicos. Si $S \subset G$ definimos el *subgrupo generado* por S como el conjunto de las palabras finitas $a_1 \ldots a_n$, donde $a_i \in S \cup S^{-1}$; lo notamos $\langle S \rangle$; es $\bigcap_{S \subset T \leq G} T$. Si $x, y \in G$ definimos el *conmutador* $[x, y] = xyx^{-1}y^{-1}$; si $H, K \leq G$ definimos $[H, K]$ como el subgrupo generado por $\{[h, k] \mid h \in H, k \in K\}$ y el *subgrupo derivado* $G' = [G, G]$; se tiene que $H \lhd G$ sii $[H, G] \leq H$. Se tiene que si $H \lhd G$ entonces G/H es abeliano si y sólo si $[G, G] \leq H$. Entonces un morfismo $G \xrightarrow{f} H$ con H abeliano se factoriza como $G \xrightarrow{p} G/G' \xrightarrow{\hat{f}} H$. Un subgrupo $H \leq G$ se dice *característico* si todo automorfismo lo fija, es decir, si $\sigma \in \operatorname{Aut}(G)$ implica $\sigma(H) = H$; se nota $H \operatorname{car} G$. Si $H \operatorname{car} G$ entonces $H \lhd G$ porque las conjugaciones son automorfismos. Si $H \operatorname{car} K$ y $K \operatorname{car} G$ entonces $H \operatorname{car} G$, porque $\sigma \in \operatorname{Aut}(G)$ implica $\sigma|_K \in \operatorname{Aut}(K)$ así que $\sigma|_K(H) = H$ y $\sigma(H) = H$. Si $H \operatorname{car} K$ y $K \lhd G$ entonces $H \lhd G$, por el mismo argumento donde σ es cada conjugación. Veamos que $G' \operatorname{car} G$: $\sigma([x, y]) = [\sigma(x), \sigma(y)] \in G'$.

Acciones. Si X es un conjunto, una acción de G en X es un morfismo $\phi \in \operatorname{Hom}(G, S_X)$; $\phi(g)(x)$ se nota $g \cdot x$ o gx. Se ve que $\phi \in \operatorname{Hom}(G, S_X)$ si y sólo si ϕ es una función $G \to (X \to X)$, $(gg')x = g(g'x)$ y $ex = x$. Podemos definir la relación $\sim \in X^2$ dada por $x \sim y$ si y sólo si hay $g \in G$ con $y = gx$; la clase de x se llama *órbita* de x y se denota $\mathcal{O}_x$. Definimos el *estabilizador* de x como el subgrupo $\mathcal{E}_x = \{g \in G \mid gx = x\}$ y tenemos $|\mathcal{O}_x| = (G : \mathcal{E}_x)$ con la biyección $gx \mapsto \mathcal{E}_x g^{-1}$. Si $\chi : G \to \mathbb{N}_0$, el *carácter* de X, está dado por $\chi(g) = |\{x \in X \mid gx = x\}|$ entonces un double counting da $\frac{1}{|G|}\sum_{g \in G} \chi(g) = |X/{\sim}|$. Definimos el *conjunto de invariantes* de la acción como ${}^G X = \{x \in X \mid \mathcal{E}_x = G\}$ y tenemos que X está partido en órbitas disjuntas $X = {}^G X \cup \bigcup_{i \in I} \mathcal{O}_{x_i}$ así que $|X| = |{}^G X| + \sum_{i \in I}(G : \mathcal{E}_{x_i})$, la *ecuación de clases*. Cuando hablamos de la acción de *conjugación* de G en sí mismo dada por $g \cdot h = ghg^{-1}$ llamamos *centralizadores* a los estabilizadores y los notamos $\mathcal{Z}_g$; llamamos *centro* del grupo al conjunto de invariantes y lo notamos $\mathcal{Z}(G)$. Con la acción de conjugación de G en sus subgrupos llamamos *normalizadores* a los estabilizadores y notamos $N_G(H)$; los invariantes son los normales.

Grupos libres y presentaciones. Si X es un conjunto y G es un grupo que lo contiene entonces es un *grupo libre* G con base X sii para todo grupo G' y toda función $f : X \to G'$ hay un único morfismo $\hat{f} : G \to G'$ tal que $\hat{f}|_X = f$. Notar que si existe es único salvo isomorfismo. Lo construimos: sea X^{-1} un duplicado disjunto de X con una biyección ${}^{-1} : X \to X^{-1}$; tomamos el monoide libre M sobre $X \cup X^{-1}$; definimos la relación de equivalencia $\sim \in M^2$ con $a \sim b$ sii metiendo elementos de $\{xx^{-1} \mid x \in X\}$ entre las letras de a y de b obtenemos palabras iguales; el grupo libre con base X es $F(X) = M/{\sim}$ con inverso $[x_1 \dots x_n] \mapsto [x_n^{-1} \dots x_1^{-1}]$. Una *presentación* de un grupo es un par $\langle X \mid \mathcal{R}\rangle$ donde X es un conjunto y $\mathcal{R} \subset F(X)$, que representa el grupo $F(X)/\bigcap_{\mathcal{R} \subset H \lhd G} H$; notar que todo grupo tiene una presentación: $\langle G \mid \ker \hat{\mathrm{id}}\rangle$. Si $G = \langle S \rangle$, $P = \langle X \mid \mathcal{R}\rangle$ y $f : S \to X$ es una biyección, tomamos $\hat{f} : F(X) \to G$; si $\hat{f}(s) = 1$ para $s \in \mathcal{R}$ (o sea los elementos de S cumplen las relaciones $\mathcal{R}$) entonces $\mathcal{R} \subset \ker \hat{f}$, $\bigcap_{\mathcal{R} \subset H \lhd F(X)} H \leq \ker \hat{f}$ y tenemos un epimorfismo $g : P \to G$ con $g \circ p_P = \hat{f}$; por lo tanto para probar que $G \cong P$ basta ver que $|P| \leqq |G|$. Con esto es obvio que $\langle x \mid \varnothing\rangle \cong \mathbb{Z}$ y $\langle x \mid x^n\rangle \cong \mathbb{Z}/n\mathbb{Z}$. Construimos el *grupo dihedral* $D_n = \langle a, b \mid a^n, b^2, baba\rangle$; se ve que todo elemento de D_n es $a^r b^s$ con $0 \leqq r < n, 0 \leqq s < 2$, luego $|D_n| \leqq 2n$; por otro lado se ve que poniendo $a = (1, 0), b = (0, 1)$ en $\mathbb{Z}_n \times_f \mathbb{Z}_2$ con $f(s)(t) = (-1)^s t$ tenemos un epimorfismo $\mathbb{Z}_n \times_f \mathbb{Z}_2 \to D_n$ así que $D_n \cong \mathbb{Z}_n \times_f \mathbb{Z}_2$. Construimos el *grupo de los cuaterniones* $\mathcal{H} = \langle a, b \mid a^4, a^2b^2, bab^{-1}a\rangle$; de nuevo se ve que todo elemento es $a^r b^s$ con $0 \leqq r < 4, 0 \leqq s < 2$ y $|\mathcal{H}| \leqq 8$; ahora armamos un grupo H sobre $\{\pm 1, \pm i, \pm j, \pm k\}$ dado por $i^2 = j^2 = k^2 = -1$, $ij = k, jk = i, ki = j$, $ji = -k, kj = -i, ik = -j$ y $i = a, j = b$ cumplen las relaciones, así que tenemos un epimorfismo $H \to \mathcal{H}$ y $|\mathcal{H}| = 8$.

Grupos finitos Si $x \in G$ definimos el *orden* de x como $|x| = |\langle x \rangle|$. Tenemos $x^k = e$ sii $|x| \mid k$. Si G es finito vale $|x| \mid |G|$. Si $f \in \operatorname{Hom}(G, G')$ entonces $|f(x)| \mid |x|$. Un grupo G de dice *cíclico* si es $\langle x \rangle$, en cuyo caso $|G| = |x|$. Si $|\langle x \rangle| = n$, $\langle x \rangle \cong \mathbb{Z}/n\mathbb{Z}$; si $|\langle x \rangle| = \infty$ entonces $\langle x \rangle \cong \mathbb{Z}$; llamamos $\mathbb{Z}_n$ a $\mathbb{Z}/n\mathbb{Z}$. Los subgrupos de $\mathbb{Z}$ son $m\mathbb{Z}$ con cociente $\mathbb{Z}_m$ y los de $\mathbb{Z}_n$ son $\langle [r] \rangle$, donde $r \mid n$, que es $r\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_{\frac{n}{r}}$, con cociente $\frac{\mathbb{Z}/n\mathbb{Z}}{r\mathbb{Z}/n\mathbb{Z}} \cong \mathbb{Z}_r$. Claramente $\operatorname{Hom}(\mathbb{Z}, \mathbb{Z}) \cong \mathbb{Z}$, $\operatorname{Hom}(\mathbb{Z}_n, \mathbb{Z}) \cong 0$ y $\operatorname{Hom}(\mathbb{Z}, \mathbb{Z}_n) \cong \mathbb{Z}_n$. Además $\operatorname{Hom}(\mathbb{Z}_n, \mathbb{Z}_m) \cong \mathbb{Z}_{(n,m)}$. $\operatorname{Aut} \mathbb{Z} \cong \mathbb{Z}_2$ y $\operatorname{Aut} \mathbb{Z}_n \cong \mathbb{Z}_n^*$, el grupo de unidades del monoide $\mathbb{Z}_n$ con la multiplicación, con el isomorfismo $f \mapsto f([1])$; en particular $|\operatorname{Aut} \mathbb{Z}_n| = \varphi(n)$.

Exponente. Un grupo es de *torsión* si todo elemento tiene orden finito. El *exponente* de un grupo de torsión es el máximo orden de un elemento. Si G es abeliano con exponente finito r veamos que si $x \in G$ entonces $|x| \mid r$. Sea y de orden r; el elemento $yx^{|x|/(r,|x|)}$ tiene orden $\operatorname{mcm}\{r, |x|\} \leqq r$ así que $|x| \mid r$. Sea k un cuerpo, k^* el grupo de unidades de la multiplicación y $G \leq k^*$ finito; si r es el exponente tenemos todo $x \in G$ es raíz de $X^r - 1$, así que $|G| \leqq r$, pero $r \mid |G|$ así que $r = |G|$ y G es cíclico. En particular $\mathbb{Z}_p^* \cong \mathbb{Z}_{p-1}$ y $\operatorname{Hom}(\mathbb{Z}_n, \operatorname{Aut}\mathbb{Z}_p) \cong \mathbb{Z}_{(m,p-1)}$.

Acción en las coclases. Si $H \leq G$ sea $\Omega = \{Hg \mid g \in G\}$ y sea $f \in \operatorname{Hom}(G, S_\Omega)$ dada por $f(x)(Ha) = Hax^{-1}$. Sea $K = \ker f$. Tenemos $K \lhd G$, $K \leq H$ y $(G : K) = |G/K| = |\operatorname{Im} f| \mid (G : H)!$. Si p es el menor primo que divide a $|G|$ y $H \leq G$ con $(G : H) = p$ entonces por lo anterior hay $K \lhd G$ con $|K| \mid |H|$ pero $|G|/|K| \mid p!$ así que $|K| = |H|$ y $K = H$, así que $H \lhd G$. Si $|G| = mp$ con $m \leqq p$ y $H \leq G$ con $|H| = p$ entonces de nuevo hay $K \lhd G$ con $K \leq H$ pero $|G|/|K| \mid m!$; si $K = 0$ resulta que $pm \mid m!$ y $p \mid (m-1)! \mid (p-1)!$, absurdo; luego $K = H$ y resulta que $H \lhd G$.

Teorema de Cauchy. Si $p \mid n = |G|$ con p primo entonces G tiene un elemento de orden p. Sea $X = \{x \in G^p \mid \prod_{i=1}^p x_i = e\}$ y sea C el grupo generado por la permutación $\sigma : i \mapsto r_p(i+1)$, actuando sobre X de la manera obvia. Las órbitas pueden tener orden uno ó p. La ecuación de clases da $p \mid n^{p-1} = |X| = |^C X| + pk$, así que $p \mid |^C X|$ y, como $|^C X| \geqq 1$, resulta que hay $g \in G$ no neutro con $g^p = e$.

Descomposición primaria. Un grupo G se dice p-grupo si todo elemento tiene orden potencia de p, con p primo. El teorema de Cauchy da que un grupo finito es p-grupo sii el orden es potencia de un primo. En el caso abeliano hacemos que $G(p)$ sea el conjunto de los elementos con orden potencia de p de G y es un subgrupo, el p-primario. Si $|G| = n = p_1^{e_1} \dots p_r^{e_r}$ entonces $(np_1^{-e_1}, \dots, np_r^{-e_r}) = 1$ y $a_1 np_1^{-e_1} + \cdots + a_r np_r^{-1} = 1$ así que G es la suma de $G(p)$ para $p \mid n$; por cardinalidad se ve que tiene que ser una suma directa (producto en versión abeliana): $G = \bigoplus_{p \mid |G|} G(p)$.

Grupos de orden pq, con p, q primos, $p > q$. Si $|G| = pq$, por Cauchy hay x, y con $|x| = p$, $|y| = q$; $\langle x \rangle \cap \langle y \rangle = 0$; $G = \langle x \rangle \langle y \rangle$ (por cardinalidad); $\langle x \rangle \lhd G$ (porque $(G : \langle x \rangle) = q$ es el menor primo que divide a $|G|$); luego $G = \langle x \rangle \rtimes \langle y \rangle$. Luego hay $\psi \in \operatorname{Hom}(\langle y \rangle, \operatorname{Aut}\langle x \rangle)$ con $G \cong \langle x \rangle \times_\psi \langle y \rangle$, así que hay $\phi \in \operatorname{Hom}(\mathbb{Z}_q, \operatorname{Aut}\mathbb{Z}_p)$ con $G \cong \mathbb{Z}_p \times_\phi \mathbb{Z}_q$, pero $\operatorname{Hom}(\mathbb{Z}_q, \operatorname{Aut}\mathbb{Z}_p) \cong \mathbb{Z}_{(q,p-1)}$, así que si $q \nmid p-1$ es trivial y $G \cong \mathbb{Z}_p \times \mathbb{Z}_q$. Si $\phi_1, \phi_2 \in \operatorname{Hom}(\mathbb{Z}_q, \operatorname{Aut}\mathbb{Z}_p)$ no son triviales, son inyectivos (viendo el núcleo). Ahora $|\operatorname{Im}\phi_1| = |\operatorname{Im}\phi_2|$, pero $\operatorname{Im}\phi_1, \operatorname{Im}\phi_2 \leq \operatorname{Aut}\mathbb{Z}_p \cong \mathbb{Z}_{p-1}$, pero un grupo cíclico tiene un subgrupo de cada cardinal así que $\operatorname{Im}\phi_1 = \operatorname{Im}\phi_2$ y por tanto hay $f \in \operatorname{Aut}\mathbb{Z}_q$ tal que $\phi_1 = \phi_2 f$ dada por $f = \phi_2^{-1}\phi_1$. Entonces $\mathbb{Z}_p \times_{\phi_1} \mathbb{Z}_q \cong \mathbb{Z}_p \times_{\phi_2} \mathbb{Z}_q$ con isomorfismo $(a, b) \mapsto (a, f(b))$. Luego todo grupo de orden pq con $p > q$ es isomorfo a $\mathbb{Z}_p \times \mathbb{Z}_q$ o, cuando $q \mid p-1$, a $\mathbb{Z}_p \times_\phi \mathbb{Z}_q$, donde $\phi \in \operatorname{Hom}(\mathbb{Z}_q, \operatorname{Aut}\mathbb{Z}_p)$ no trivial, según sea abeliano o no.

Teorema de Sylow. Si $|G| = p^r t$ con p primo y $p \nmid t$ entonces G tiene un subgrupo de orden p^r; estos subgrupos se llaman p-Sylow. Escribimos la ecuación de clases $|G| = |\mathcal{Z}(G)| + \sum \frac{|G|}{|\mathcal{Z}_{x_i}|}$; si $p \nmid |\mathcal{Z}(G)|$ hay $x_i \in G$ con $p \nmid \frac{|G|}{|\mathcal{Z}_{x_i}|}$, $p^r \mid |\mathcal{Z}_{x_i}|$ y usamos inducción sobre $\mathcal{Z}_{x_i}$; si no, tomamos el p-Sylow $H = \mathcal{Z}(G)(p)$ de $\mathcal{Z}(G)$, un p-Sylow L de G/H (por inducción) y hay $H \leq S \leq G$ con $L \cong S/H$, que es p-Sylow de G. Los p-Sylows son conjugados entre sí, y si H es un p-subgrupo está contenido en $1+pt$ p-Sylows; si hay n_p Sylows y P es uno, $p \mid n_p - 1$, $n_p = (G : N_G(P)) \mid \frac{|G|}{p^r}$, y $n_p = 1$ sii $P \lhd G$ sii $P \operatorname{car} G$. Dado H p-subgrupo lo hacemos actuar por conjugación en el conjunto X de los conjugados de P; la ecuación de clases da $p \mid |X| - |^H X|$. Vemos que $^H X = \{P' \in X \mid H \leq P'\}$: si $H \leq N_G(P)$, $\frac{|HP|}{|H|} = \frac{|P|}{|H \cap P|}$, HP es un p-subgrupo, $HP = P$ y $H \leq P$. Pongo $H = P$ y obtengo $p \mid |X| - 1$; luego $p \mid |\{P' \in X \mid H \leq P'\}| - 1$ y poniendo $H = Q$, otro p-Sylow, obtengo que todos son conjugados, por lo que $|X| = n_p$ y $p \mid n_p - 1$.

Argumento de Frattini. Si $H \lhd G$ y P es p-Sylow de H entonces $G = N_G(P)H$: si $g \in G$, $gHg^{-1} = H$, $gPg^{-1} \leq H$ y $gPg^{-1} = hPh^{-1}$ con $h \in H$, porque gPg^{-1} es p-Sylow de H y los p-Sylow son conjugados; entonces $h^{-1}g \in N_G(P)$, $g \in N_G(P)H$ y $G = N_G(P)H$. Si P es Sylow entonces $N_G(N_G(P)) = N_G(P)$, porque $gN_G(P)g^{-1} \leq N_G(P)$ implica $gPg^{-1} \leq N_G(P)$ (porque

$P \triangleleft N_G(P)$ implica que es el único Sylow en $N_G(P)$) que implica $gPg^{-1} = P$ y $g \in N_G(P)$. En general, si $N_G(P) \leq M \leq G$ para un p-Sylow P de G entonces $M = N_G(M)$, porque de $M \triangleleft N_G(M)$ sale $N_G(M) = N_{N_G(M)}(P)M \leq N_G(P)M \leq M$ y $N_G(M) = M$.

Simplicidad de A_n. Toda permutación se puede escribir como producto de ciclos disjuntos de manera única salvo el orden en el que se toma el producto. Dos permutaciones son conjugadas sii son del mismo tipo, es decir, sii una se descompone en ciclos como $\sigma_1 \dots \sigma_k$ y la otra como $\tau_1 \dots \tau_k$ con $|\sigma_i| = |\tau_i|$. Las trasposiciones generan; si $\sigma \in S_n$ es $\tau_1 \dots \tau_k$ con τ_i traspociones entonces $(-1)^k = \operatorname{sig} \sigma$ no depende de la escritura; entonces $\operatorname{sig} \in \operatorname{Hom}(S_n, G_2)$. Definimos el *grupo alternante* A_n como el núcleo de sig; se ve que está generado por los 3-ciclos. Un grupo se dice *simple* si no tiene subgrupos normales propios. A_5 es simple: si $0 \neq H \triangleleft A_5$ no es propio no tiene 3-ciclos; si contiene $\sigma = (1\ 2)(3\ 4)$, contiene $(\tau\sigma\tau^{-1})\sigma^{-1} = (3\ 5\ 4)$, absurdo, donde $\tau = (1\ 2)(3\ 5)$; si contiene $\sigma = (1\ 2\ 3\ 4\ 5)$, contiene $\tau\sigma\tau^{-1}\sigma^{-1} = (1\ 3\ 4)$, absurdo, donde $\tau = (1\ 3\ 2)$. A_6 es simple: seguimos con la misma idea; si H contiene $\sigma = (1\ 2)(3\ 4\ 5\ 6)$ entonces $\sigma^2 = (3\ 5)(4\ 6)$ que vimos que no; si H contiene $\sigma = (1\ 2\ 3)(4\ 5\ 6)$ entonces contiene $\sigma\tau\sigma^{-1}\tau^{-1} = (1\ 5\ 3\ 2\ 4)$ que vimos que no. A_n es simple para $n \geqq 6$: sea $1 \neq \sigma \in H$; sean i, j con $\sigma(i) = j \neq i$; sea τ un 3-ciclo que fija i pero mueve j; entonces $\sigma\tau(i) = \sigma(i) = j$ y $\tau\sigma(i) = \tau(j) \neq j$; entonces $\tau\sigma\tau^{-1}\sigma^{-1} \neq 1$; $\sigma\tau^{-1}\sigma^{-1}$ es del mismo tipo que τ^{-1} así que es 3-ciclo; luego $\tau\sigma\tau^{-1}\sigma^{-1}$ como mucho mueve seis elementos y luego ya vimos que no está en H, absurdo. El único subgrupo normal de S_n, $n \geqq 5$, es pues A_n.

A_5 es el único grupo simple de orden 60. Sea G otro; sea $H \lneqq G$ con $(G : H) = n$; hacemos actuar G en las coclases y obtenemos $K \triangleleft G$, $K \leq H$ y un monomorfismo $G/K \hookrightarrow S_n$; luego, como $|S_4| < 60$ y $K = 0$ por ser G simple, $n \geqq 5$; entonces si $(G : H) = 5$, $G \hookrightarrow S_5$, $\frac{|G|}{|A_5 \cap G|} = \frac{|A_5 G|}{|A_5|} \mid \frac{|S_5|}{|A_5|} = 2$ y de $A_5 \cap G \triangleleft G$ sale que $A_5 = G$; de $n_3 \geqq 5$ (porque $(G : N_G(H)) = n_3$ si H es 3-Sylow), $n_3 \mid 20$ y $3 \mid n_3 - 1$ sale $n_3 = 10$; de $n_5 \geqq 5$, $n_5 \mid 12$ y $5 \mid n_5 - 1$ sale $n_5 = 6$; de $n_2 \geqq 5$, $n_2 \mid 15$ sale n_2 es 5 ó 15; si es 5 estamos así que supongamos que es 15; si A, B son 2-Sylows, $A \cap B \triangleleft A, B$, $A, B \leq N_G(A \cap B)$, $4 \mid |N_G(A \cap B)|$, $5 \leqq (G : N_G(A \cap B)) \mid 15$ o $A \cap B = 0$; si $(G : N_G(A \cap B)) = 5$ estamos; si no es 15, $|N_G(A \cap B)| = 4$ y $A = B$ o $A \cap B = 0$; entonces los 15 2-Sylow son disjuntos; los 3 y 5-Sylows también son disjuntos entre sí porque 3 y 5 son primos; entonces $60 = |G| \geqq 1 + 2 \cdot 10 + 4 \cdot 6 + 3 \cdot 15 = 90$, absurdo.

Condiciones de cadena Una *cadena normal* de subgrupos es una cadena $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n$; los cocientes G_i/G_{i+1} se llaman *factores*; si los factores abelianos la secuencia se dice *abeliana*; si son cíclicos se dice *cíclica*; son simples y la sucesión llega a 1 se dice *serie de composición*; una cadena se dice que es un *refinamiento* de sus subsecuencias. Dos cadenas normales de G que terminan en el grupo trivial tienen refinamientos equivalentes, es decir, con el mismo conjunto de factores salvo isomorfismo: (Schreier) si $G = G_1 \triangleright G_2 \cdots \triangleright G_r = 1$ y $G = H_1 \triangleright H_2 \triangleright \cdots \triangleright H_s = 1$ son las dos secuencias entonces ponemos $G_{ij} = G_{i+1}(H_j \cap G_i)$ y tenemos un refinamiento de la primera; $H_{ji} = H_{j+1}(G_i \cap H_j)$ y tenemos un refinamiento de la segunda; por el lema de Zassenhaus tenemos $G_{ij}/G_{i,j+1} \cong H_{ji}/H_{j,i+1}$ y los refinamientos son equivalentes. Todo grupo finito tiene una serie de composición: sea G un contraejemplo mínimo; si es simple $G \triangleright 1$ es serie de composición; si no, hay $H \triangleleft G$ propio; lo tomamos maximal; entonces G/H es simple y pegamos G a una serie de composición de H. El teorema de Jordan-Hölder dice que si un grupo tiene una serie de composición entonces el conjunto de factores no depende de la serie elegida. Por lo anterior basta ver que al refinar se mantienen los factores, pero esto es obvio porque G/H es simple sii $H \triangleleft G$ es maximal.

Grupos solubles. Un grupo G se dice *soluble* si tiene una cadena abeliana que llega a 1. Si G es finito entonces toda cadena abeliana se puede refinar a una serie de composición, es decir, a una cadena cíclica con factores de orden primo. Si $H \triangleleft G$ entonces G es soluble sii H y G/H son: si G es, $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_n = 1$; tomando $H_i = G_i \cap H$ obtenemos que H es soluble; tomando $H_i = G_i H/H$ obtenemos que G/H es soluble; si $G/H = K_0 \triangleright K_1 \triangleright \cdots \triangleright K_n = 1$, tomando

$H_i = p_H^{-1}(K_i)$ obtenemos una cadena de G que termina en H, y la podemos pegar con la de H; $H \times K$ es soluble sii H y K son. La *serie derivada* de G es la sucesión $G^{(0)} \geq G^{(1)} \geq \cdots$, donde $G^{(0)} = G$ y $G^{(i+1)} = (G^{(i)})'$. Como $G' \operatorname{car} G$ tenemos que $G^{(i)} \operatorname{car} G$ y es una cadena normal. Si G es soluble, sea $G = G_0 \rhd G_1 \rhd \cdots \rhd G_n = 1$ abeliana; se ve por inducción que $G^{(i)} \leq G_i$; el caso base es trivial; como G_i/G_{i+1} es abeliano, $G_{i+1} \geq G_i' \geq (G^{(i)})' = G^{(i+1)}$; concluímos que la serie derivada termina en 1. Recíprocamente si la serie derivada termina en el 1 es una sucesión abeliana así que un grupo es soluble sii $G^{(n)} = 1$ para algún n. Si G es soluble y N es un subgrupo normal minimal entonces N es un p-grupo abeliano: tenemos $N' \operatorname{car} N$ y $N' \lhd G$; como N es soluble, $N' \neq N$, $N' = 1$ y N es abeliano; si $P \neq 1$ es p-Sylow de N se ve que $P \operatorname{car} N$ así que $P \lhd G$ y tiene que ser $P = N$.

Teorema de P. Hall. Si G es soluble de orden mn con $(m,n) = 1$ entonces G contiene un subgrupo de orden m, todos los de orden m son conjugados y todo subgrupo de orden $k \mid m$ está contenido en un subgrupo de orden m. *Caso 1.* Hay $H \lhd G$ propio con $n \nmid |H|$. $|H| = m_1 n_1, m_1 \mid m, n_1 \mid n$, G/H es soluble, tiene por inducción un subgrupo A/H de orden m/m_1; A tiene orden $mn_1 < mn$; A tiene un subgrupo de orden m. Si B, C son subgrupos de orden m, se ve que $|HB| = |HC| = mn_1$, $HB/H, HC/C \leq G/H$ de orden m/m_1, son conjugados por inducción, $\overline{x}(HB/H)\overline{x}^{-1} = HC/H$ con $\overline{x} \in G/H$, $xBx^{-1}, C \leq HC$ de orden m así que por inducción son conjugados y listo. Si $K \geq G$, $|K| = k \mid m$, $|HK/H| \mid m/m_1$, por inducción hay $HK/H \leq A/H \leq G/H$ con $|A/H| = m/m_1$, $K \leq A$ con $|A| = mn_1 < mn$ así que por inducción $K \leq H \leq A \leq G$ con $|H| = m$. *Caso 2.* Si $H \lhd G$ propio entonces $n \mid |H|$. Tomamos H normal minimal, por el lema es p-grupo abeliano, de $n \mid p^r$ y $(m,n) = 1$ sale $n = p^r$, y es el único normal minimal así que está contenido en todo normal. Sea K/H normal minimal de G/H; entonces $H \lhd K \lhd G$, K/H es q-grupo, $|K| = p^r q^s$ y $K = HS$, donde S es q-Sylow; tenemos $\mathcal{Z}(K) \operatorname{car} K$ y $\mathcal{Z}(K) \lhd G$, luego $H \leq \mathcal{Z}(K)$ en cuyo caso $S \lhd K$, luego $S \operatorname{car} K$ por Sylow, $S \lhd G$, $H \leq S$ y absurdo o $\mathcal{Z}(K) = 1$; usamos el seguiente lema: si $K = HS$, $H \lhd K$ abeliano, $H \cap S = 1$ y $\mathcal{Z}(K) = 1$ entonces $N_K(S) = S$; entonces $|H| = (K : S) = (K : N_K(S)) = (G : N_G(S))$ porque los conjugados de S en G son los conjugados de S en K porque K es normal; entonces $|N_K(S)| = m$, como queremos. Ahora supongamos que $B \leq G$ de orden m; por órdenes $G = BK$ y $|B \cap K| = q^s$; por Sylow $B \cap K$ y S son conjugados en K; $B \cap K \lhd B$, $B \leq N_G(B \cap K)$; como normalizadores de conjugados con conjugados, $N_G(B \cap K)$ y $N_G(S)$ son conjugados pero $|N_K(S)| = m$, luego B y $N_G(S)$ son conjugados. Sea $D \leq G$, $|D| = k \mid m$; $D \cap H = 1$, $|DH| = kp^r$, $N_G(S)(DH) \geq N_G(S)H = G$ y $|N_G(S) \cap DH| = k$; sea $D^* = N_G(S) \cap DH$; $D = gD^*g^{-1}$ por lo anterior en DH; luego $D = gD^*g^{-1} \leq gN_G(S)g^{-1}$, como queremos.

Grupos nilpotentes I. Una *cadena central ascendente* es una sucesión creciente de subgrupos normales $(N_i)_{i \geqq 0}$ tales que $N_0 = 1$ y $N_{i+1}/N_i \leq \mathcal{Z}(G/N_i)$; un grupo se dice *nilpotente* si tiene una cadena central ascendente que llega a G. Definimos la *cadena central superior* de G así: $Z_0 = 1$, $Z_{i+1}/Z_i = \mathcal{Z}(G/Z_i)$, es decir, $Z_{i+1} = p_{Z_i}^{-1}(\mathcal{Z}(G/Z_i)) = \{g \in G \mid [g, G] \subset Z_i\}$. Se ve que si $H \operatorname{car} G$ y $\sigma \in \operatorname{Aut}(G)$ entonces hay $\hat{\sigma} \in \operatorname{Aut}(G/H)$ tal que $\hat{\sigma} \circ p_H = p_H \circ \sigma$. Veamos por inducción que $Z_i \operatorname{car} G$; el caso base es obvio; sea $\sigma \in \operatorname{Aut}(G)$, $\hat{\sigma} \in \operatorname{Aut}(G/Z_i)$ tal que $\hat{\sigma} \circ p_{Z_i} = p_{Z_i} \circ \sigma$, hay que ver que $x \in Z_{i+1}$ entonces $\sigma(x) \in Z_{i+1}$, esto es, $[\sigma(x), G] \leq Z_i$, o sea $1 = p_{Z_i}[\sigma(x), G]$; ahora $p_{Z_i}[\sigma(x), G] = p_{Z_i}\sigma[x, G] = \hat{\sigma} p_{Z_i}[x, G] = 1$. Vemos que un grupo es nilpotente sii su cadena central superior llega a G: si (N_i) llega y es central se prueba que $Z_i \leq N_i$ así que la superior también. Definimos la *cadena central inferior* de G así: $G_0 = G$, $G^{i+1} = [G^i, G]$. De nuevo $G^{i+1} \operatorname{car} G^i$ así que es normal. Veamos que hay $n \in \mathbb{N}$ tal que $Z_n = G$ sii $G^n = 1$ y en ese caso $G^i \leq Z_{n-i}$. Supongamos que $Z_n = G$ y probemos que $G^i \leq Z_{n-i}$; $i = 0$ es trivial; si $G^i \leq Z_{n-i}$ entonces $G^{i+1} = [G^i, G] \leq [Z_{n-i}, G] \leq Z_{n-i-1}$. Supongamos que $G^n = 1$ y probemos que $G^{n-i} \leq Z_i$; $i = 0$ es trivial; si $[G^{n-i-1}, G] = G^{n-i} \leq Z_i$ entonces dado $g \in G^{n-i-1}$ tenemos $[g, G] \subset Z_i$ así que $g \in Z_{i+1}$. Definimos el *índice de nilpotencia* de G como el menor $n \in \mathbb{N}$ tal que $Z_n(G) = G$ ó $G^n = 1$.

Grupos nilpotentes II. Nilpotente implica soluble porque se ve que $G^{(i)} \leq G^i$. Si G es nilpotente de índice n entonces todo subgrupo $H \leq G$ es nilpotente de índice a lo sumo n y si $H \triangleleft G$ entonces G/H también; lo primero porque $H^i \leq G^i$, por inducción; lo segundo porque $(G/H)^i \leq p_H(G^i)$, por inducción. Se ve que producto de nilpotentes da nilpotente. Si $G/\mathcal{Z}(G)$ es nilpotente entonces G es nilpotente: se ve por inducción que $Z_{i+1}(G)/\mathcal{Z}(G) = Z_i(G/\mathcal{Z}(G))$ así que $Z_n(G/\mathcal{Z}(G)) = G/\mathcal{Z}(G)$ implica $Z_{n+1}(G) = G$. Si G es nilpotente y $1 \neq H \triangleleft G$ entonces $H \cap \mathcal{Z}(G) \neq 1$: sea m mínimo tal que $H \cap Z_m \neq 1$; $[H \cap Z_m, G] \leq [H, G] \cap [Z_m, G] \leq H \cap Z_{m-1} = 1$ así que $1 \neq H \cap Z_m \leq H \cap \mathcal{Z}(G)$. Si $H \lneqq G$ entonces $H \lneqq N_G(H)$; en particular todo subgrupo maximal es normal: sea m el mínimo tal que $G^m \leq H$; ahora $[G^{m-1}, H] \leq [G^{m-1}, G] = G^m \leq H$ entonces G^{m-1} normaliza H y $H \lneqq G^{m-1} \leq N_G(H)$. Todo p-grupo es nilpotente: vemos por inducción que $G/\mathcal{Z}(G)$ es nilpotente usando que $\mathcal{Z}(G) \neq 1$, que sale de ver la ecuación de clases con la acción conjugación. Un grupo finito es nilpotente sii es isomorfo al producto de sus subgrupos de Sylow: si P es Sylow, $N_G(N_G(P)) = N_G(P)$, luego $N_G(P) = G$, $P \triangleleft G$ y sale. De acá sale que nilpotente es equivalente a que todo subgrupo maximal sea normal: si P es Sylow no normal, $N_G(P) \lneqq G$ y hay $N_G(P) \leq M \leq G$ con M maximal; luego $M \triangleleft G$ en contradicción con el argumento de Frattini que dice que $N_G(M) = M$. Vemos que todo p-grupo P tiene subgrupos de todos los órdenes divisores de $|P|$ por inducción, separando el caso abeliano, aplicando la hipótesis inductiva sobre $P/\langle x \rangle$, x de orden p por Cauchy y luego usando $p_{\langle x \rangle}^{-1}$, y el caso no abeliano, aplicando la hipótesis sobre $P/\mathcal{Z}$, porque $\mathcal{Z} \neq 1$ y luego usando $p_{\mathcal{Z}}^{-1}$; entonces si G es nilpotente finito tiene subgrupos de todos los órdenes divisores de $|G|$.

Anillos Un *semianillo* es una terna $(A, +, \cdot)$ donde $(A, +)$ es un monoide conmutativo, $(A, \cdot)$ es un semigrupo, $a(b + c) = ab + ac$ y $(a + b)c = ac + bc$; un *anillo* es un semianillo con $(A, +)$ grupo; se dice *con unidad* si $(A, \cdot)$ es monoide; *conmutativo* si $(A, \cdot)$ es conmutativo; *de división* si tiene unidad y el *grupo de unidades* notado $\mathcal{U}(A)$ o $A^\times$ es $A \setminus 0$; un *dominio* es un anillo conmutativo con unidad; se dice *dominio íntegro* si $ab = 0$ implica $a = 0$ ó $b = 0$; un *cuerpo* es un anillo de división conmutativo; cuerpo implica dominio íntegro. Un morfismo de anillos es una función $f : A \to A'$ que es morfismo con respecto a las dos operaciones. Un morfismo es *monomorfismo* o *inmersión* si es inyectivo, *epimorfismo* si es epimorfismo; es isomorfismo sii es mono y epi. El producto (categórico) de $\{A_i\}_{i \in I}$ es $\prod_{i \in I} A_i$ con la suma y el producto coordenada a coordenada. Dado A anillo tomamos el grupo $A \oplus \mathbb{Z}$ y le damos multiplicación $(a, m)(b, n) = (ab + na + mb, mn)$; tiene unidad $(0, 1)$ y $a \mapsto (a, 0)$ es una inmersión; por lo tanto todo anillo se puede meter en un anillo con unidad. Un *subanillo* es un subconjunto no vacío tal que las operaciones restringidas forman un anillo. El *núcleo* de un morfismo f se define como el núcleo para la suma y se nota $\ker f$. Un *ideal* de A es un subanillo I tal que $r \in A, a \in I$ implica $ra, ar \in I$; todo núcleo es ideal; recíprocamente si I es ideal, el grupo cociente A/I tiene estructura de anillo con $(a + I)(b + I) = ab + I$, se llama *anillo cociente* y la proyección canónica es un epimorfismo $p_I : A \to A/I$ con $\ker p_I = I$. Cumple la propiedad universal: si $f : A \to B$ es morfismo y $I \subset \ker f$ es ideal entonces hay $\hat{f} : A/I \to B$ tal que $f = \hat{f} \circ p_I$. Los morfismos canónicos en grupos funcionan: $(B + I)/I \cong B/(B \cap I)$ si B es subanillo y I es ideal; si $I \subset J$ son ideales entonces $(A/I)/(J/I) = R/J$; si I es ideal hay una correspondencia entre subanillos de A que contienen I y subanillos de I que preserva inclusiones y B subanillo de A que contiene I es ideal de A sii B/I es ideal de A/I. Definimos la *característica* de un anillo $\operatorname{car} A$ como el menor $n \in \mathbb{N}$ tal que $na = 0$ para $a \in A$ (o sea $n1 = 0$) si existe y cero si no; si no hay divisores de cero entonces n es primo porque $pq1 = (p1)(q1)$; si además es finito resulta de división.

Ideales. Si X es un subconjunto de A definimos el *ideal generado* (X) como la interseccion de todos los ideales I que contienen X; se ve que (X) es el conjunto de todas las sumas finitas $a_1x_1b_1 + \cdots + a_nx_nb_n$ donde $a_i, b_i \in A$ y $x_i \in X$; un ideal se dice *principal* si está generado por un solo elemento; un *dominio de ideales principales* (DIP) es un dominio íntegro en el que todos los ideales son principales. Dados ideales I, J definimos la suma $I + J = \{a + b \mid a \in I, b \in J\}$ y el producto IJ como el generado por $\{ab \mid a \in I, b \in J\}$; tenemos $IJ \subset I \cap J$. Un ideal I es *maximal* si es maximal con respecto a la inclusión y $I \neq A$; Zorn da que si A es unitario entonces existe un ideal maximal; si A es un domnio, I es maximal sii A/I es un cuerpo; un ideal $P \neq A$ es *primo* sii $ab \in P$ implica $a \in P$ ó $b \in P$; P es primo sii A/P es dominio íntegro; en particular los ideales maximales son primos. Si $a, b \in A$ decimos que $a \mid b$ sii hay $c \in A$ con $ac = b$, o sea $(a) \supset (b)$; decimos que a y b son *asociados* si $(a) = (b)$; si A es dominio íntegro esto es equivalente a que haya una unidad c con $a = bc$. Un elemento $a \in A$ se dice *irreducible* sii $a = bc$ implica que b ó c es una unidad o sea sii (a) es maximal entre los ideales principales; $a \in A$ se dice *primo* sii $a \mid bc$ implica $a \mid b$ ó $a \mid c$, es decir, sii (a) es primo; en particular todo primo es irreducible y en un DIP se cumple la recíproca. Teorema chino del resto: sean $I_1, \ldots, I_n$ ideales de A tales que $I_i + I_j = A$ si $i \neq j$; entonces $f : A \to \prod_{i=1}^n A/I_i$ dado por $f(a)_i = p_{I_i}(a)$ es epimorfismo así que $A/\bigcap_{i=1}^n I_i \cong \prod_{i=1}^n A/I_i$. En efecto, dado i, sean $a_j^i \in I_i, b_j^i \in I_j$ con $a_j^i + b_j^i = 1$ para $j \neq i$; $\prod_{i \neq j}(a_j^i + b_j^i) = 1$ da $a_i + b_i = 1$ con $a_i \in I_i$, $b_i = \prod_{i \neq j} b_j^i \in \bigcap_{i \neq j} I_j$; entonces si $(p_{I_i}(x_i)) \in \prod_{i=1}^n A/I_i$, $f(\sum_{i=1}^n b_i x_i) = (p_{I_i}(x_i))$ y f es epi.

Factorización. Un anillo se dice *noetheriano* si toda cadena ascendente de ideales $I_1 \subset I_2 \subset \cdots$ se estaciona, es decir, hay $n \in \mathbb{N}$ con $I_m = I_n$ si $m \geqq n$; es equivalente a que todo ideal sea finitamente generado. Un dominio se dice *de factorización* sii todo elemento se escribe como producto de irreducibles; claramente noetheriano implica de factorización. Un dominio se dice *de factorización única* (DFU) si todo elemento se escribe como producto de irreducibles de forma única salvo orden y asociación. Si un dominio íntegro es de factorización entonces es DFU sii todo irreducible es primo; si todo irreducible es primo y tenemos dos factorizaciones distintas, cancelamos los asociados, tomamos un irreducible, como es primo divide alguno de los de la otra factorización y resultan asociados, absurdo; el recíproco es obvio. En particular todo DIP es DFU. Una *norma de Dedekind-Hasse* es una función $N : A \to \mathbb{N}_0$ tal que $N(a) = 0$ sii $a = 0$ y, dados $a, b \in A$ no nulos $a \mid b$ o hay $c \in (a, b)$ con $0 < N(c) < N(a)$; si A tiene una norma de Dedekind-Hasse entonces es DIP: si $I \neq 0$ es un ideal, sea $a \in I$ no nulo con $N(a)$ mínimo; si $b \in I$ entonces $a \mid b$ o hay $c \in (a, b) \subset I$ con $0 < N(c) < N(a)$, absurdo; entonces $I = (a)$. Recíprocamente, si A es DIP, es DFU y podemos construir una norma de Dedekind-Hasse así: $N(0) = 0$, $N(a) = 1$ si a es unidad, $N(a) = 2^n$ si $a = p_1 \ldots p_n$ con p_i irreducibles. Una *norma euclídea* es una función $N : A \to \mathbb{N}_0$ tal que $N(a) = 0$ sii $a = 0$ y tal que si $a, b \in A$ no nulos hay $q, r \in A$ con $a = qb + r$ con $N(r) < N(b)$; un *dominio euclídeo* es un dominio que tiene una norma euclídea; como toda norma euclídea es de Dedekind-Hasse, todo dominio euclídeo es DIP. Sea $\tilde{R} = R^\times \cup \{0\}$; $u \in R \setminus \tilde{R}$ se dice *divisor universal de lado* si para todo $x \in R$ hay $z \in \tilde{R}$ con $u \mid x - z$; si R es dominio euclídeo vemos que $u \in R \setminus \tilde{R}$ de norma mínima cumple; esto sirve para demostrar que un dominio no es euclídeo.

Localización. R va a ser conmutativo. Sea $\varnothing \neq S \subset R$ un subconjunto *multiplicativo*, es decir, tal que $a, b \in S \Rightarrow ab \in S$. Sea $\sim$ una relación en $R \times S$ dada por $(r, s) \sim (r', s')$ sii hay $s_1 \in S$ con $s_1 r s' = s_1 r' s$; es de equivalencia; llamamos $S^{-1}R$ al conjunto de las clases, notadas r/s; es un dominio con operaciones $r/s + r'/s' = (rs' + r's)/(ss')$ y $(a/s)(a'/s') = (aa')/(ss')$ llamado *anillo de cocientes* de R en S; si R es íntegro y $0 \notin S$ entonces $S^{-1}R$ es íntegro; si $S = R \setminus 0$, $S^{-1}R$ es un cuerpo, el *cuerpo de cocientes* de R. El morfismo $\phi_S : R \to S^{-1}R$ dado por $r \mapsto rs/s$ para algún $s \in S$ manda unidades a unidades; si no hay divisores de cero en S entonces ϕ_S es un monomorfismo; en particular, todo dominio íntegro se puede meter en su cuerpo de cocientes. El par $(S^{-1}R, \phi_S)$ cumple la propiedad universal: si T es un dominio y $f : R \to T$ es un morfismo tal que $f(S) \subset T^\times$ entonces se puede factorizar en $R \xrightarrow{\phi_S} S^{-1}R \xrightarrow{\hat{f}} T$. Ahora R tiene unidad. Si I es un ideal definimos la *extensión* en $S^{-1}R$ como $S^{-1}I = \{a/s \mid a \in I, s \in S\}$; es un ideal y $S^{-1}I = S^{-1}R$ sii $S \cap I \neq \varnothing$. Si J es un ideal de $S^{-1}R$ definimos la *contracción* de J en R como $\phi_S^{-1}(J)$; es un ideal y $I \subset \phi_S^{-1}(S^{-1}I)$;

$I = \phi_S^{-1}(J) \Rightarrow S^{-1}I = J$; si P es primo y $S \cap P = \varnothing$ entonces $S^{-1}P$ es primo y $\phi_S^{-1}(S^{-1}P) = P$; la transformación $P \mapsto S^{-1}P$ es una biyección entre los $P \in \operatorname{Spec} R$ disjuntos de S y $\operatorname{Spec} S^{-1}R$, donde $\operatorname{Spec} R$, el *espectro* de R, es el conjunto de ideales primos. Si $P \in \operatorname{Spec} R$ entonces $S = R \setminus P$ es multiplicativo y $S^{-1}R$ se llama *localización* de R en P y se nota R_P; si I es ideal, $S^{-1}I$ se nota I_P. Hay una biyección entre los ideales primos de R contenidos en P y los ideales primos de R_P dada por $I \mapsto I_P$; el ideal P_P es el único ideal maximal en R_P. Un *anillo local* es un dominio con un único ideal maximal; las localizaciones son pues anillos locales; un dominio D es local sii $D \setminus D^\times$ es ideal. Si I es ideal entonces $\theta : S^{-1}R \to p_I(S)^{-1}(R/I)$ dada por $r/s \mapsto p_I(r)/p_I(s)$ es un epimorfismo con núcleo $S^{-1}I$; luego $S^{-1}R/S^{-1}I \cong p_I(S)^{-1}(R/I)$. Un *anillo de valuación discreta* (AVD) es un DIP local; si (t) es el ideal maximal todo $x \neq 0$ se escribe como ut^n con $u \in R^\times$ y n no depende de t; una *valuación discreta* sobre un cuerpo K es una función $\phi : K \to \mathbb{Z} \cup \{\infty\}$ tal que $\phi(0) = \infty$, $\phi(ab) = \phi(a) + \phi(b)$, $\phi(a+b) \geqq \text{mín}\{\phi(a), \phi(b)\}$; el anillo $\{x \in K \mid \phi(x) \geqq 0\}$ es un DVR; recíprocamente un DVR R induce una vd sobre su cuerpo de cocientes por $\phi(ut^n) = n$ $(u \in R^\times)$.

Radicales. Sea A un dominio. Si I es ideal definimos su *radical* como $\sqrt{I} = \{a \in A \mid \exists n \in \mathbb{N}(a^n \in I)\}$; es un ideal; un ideal I se dice *radical* si $\sqrt{I} = I$; los ideales primos son radicales; $\sqrt{0}$ se llama *nilradical* de A y se nota $\operatorname{nil} A$; sus elementos se llaman *nilpotentes*. Tenemos $\sqrt{I}/I = \operatorname{nil}(A/I)$ y $\sqrt{I} = p_I^{-1}(\operatorname{nil}(A/I))$. Tenemos $\sqrt{I} = \bigcap_{I \subset P \in \operatorname{Spec} A} P$: una inclusión es obvia; sea $a \notin \sqrt{I}$; sea $S = \{a^n \mid n \in \mathbb{N}\}$, cerrado multiplicativamente; sea J un ideal maximal de $S^{-1}R$ que contiene a $S^{-1}I$; es primo, luego hay $P \in \operatorname{Spec} R$ con $P \cap S = \varnothing$ y $J = S^{-1}P$; ahora $I \subset \phi_S^{-1}(S^{-1}I) \subset \phi_S^{-1}(S^{-1}P) = P$; entonces $a \notin P$ con $I \subset P \in \operatorname{Spec} A$, $a \notin \bigcap_{I \subset P \in \operatorname{Spec} A} P$ y tenemos la otra inclusión. En particular $\operatorname{nil} A = \bigcap_{P \in \operatorname{Spec} A} P$. Definimos el *radical de Jacobson* de A como $J(A)$, la intersección de todos los ideales maximales de A. Es el conjunto de los $x \in A$ tales que para cada $y \in A$, $1 - xy \in A^\times$; si x cumple y $\mathfrak{m}$ es maximal, $A/\mathfrak{m}$ es cuerpo; si $x \notin \mathfrak{m}$, hay $y \in A$ con $1 - xy \in \mathfrak{m}$, luego $1 - xy \notin A^\times$, absurdo; si x no cumple, hay $y \in A$ con $1 - xy \notin A^\times$; luego $(1 - xy) \neq A$, luego $x \notin (1 - xy)$; entonces el lema de Zorn da un maximal I con $x \notin I$ pero $1 - xy \in I$; si no fuera maximal en A, habría J con $I \subsetneqq J \subsetneqq A$; $I \subset J$ da $1 - xy \in J$; $J \neq A$ da $x \notin J$; absurdo.

Polinomios Si A es unitario y G es un monoide, definimos el *anillo de monoide* $A[G]$ como las funciones $\alpha : G \to A$ con $\alpha(x) = 0$ para todo x salvo una cantidad finita con la suma punto a punto y el producto $(\alpha\beta)(z) = \sum_{xy=z} \alpha(x)\beta(y)$; identificamos x con $\alpha(z) = \{\begin{smallmatrix} 1 \text{ si } z = x \\ 0 \text{ si no} \end{smallmatrix}$ y $\alpha = \sum_x a_x x$, $\alpha + \beta = \sum_x (a_x + b_x)x$, $\alpha\beta = \sum_{x,y} a_x b_y xy$; tenemos inmersiones $G \hookrightarrow A[G]$ y $A \hookrightarrow A[G]$. Si S es un conjunto definimos el *anillo de polinomios* sobre S como $A[S] = A[\mathbb{N}^{(S)}]$. De la propiedad universal: si A, B son dominios y G un monoide, todos morfismos $G \overset{\text{ev}}{\to} (B, \cdot)$ y $A \overset{\varphi}{\to} B$ se factorizan como $G \hookrightarrow A[G] \overset{\hat\varphi}{\to} B$ y $A \hookrightarrow A[G] \overset{\hat\varphi}{\to} B$ con $\hat\varphi$ único, llamamos a $\hat\varphi$ una *evaluación* de $A[G]$; en el caso de polinomios requiere una función $S \overset{\text{ev}}{\to} B$. Todo polinomio se puede escribir como una suma de *monomios* $a \prod_{\text{finito}} x_i^{r_i}$ donde $S = \{x_i \mid i \in I\}$; los a se llaman *coeficientes*; el *grado* del monomio es $\sum_{i \in I} r_i$ y el grado del polinomio es el máximo de la suma de los grados de sus monomios y se nota $\deg p$; un polinomio se dice *homogéneo* si los grados de sus monomios son todos iguales. Si A es unitario definimos el *anillo de series formales* de A como el conjunto $A^\mathbb{N}$ con la suma punto a punto y el producto $(a_n)(b_n) = (c_n)$ con $c_n = \sum_{i+j=n} a_i b_j$. Tenemos que $a \in A[[x]]^\times$ sii $a_0 \in A^\times$; una implicación es obvia; para la otra, encontrar b con $ab = ba = 1$ es resolver las ecuaciones. Si k es un cuerpo, las no unidades de $k[[x]]$ serían (x); entonces $k[[x]]$ es un anillo local.

División de polinomios. Si A es unitario, $f, g \in A[x]$ son no nulos y el coeficiente principal de g es una unidad entonces hay únicos polinomos $q, r \in A[x]$ con $f = qg + r$ y $\deg r < \deg g$; la existencia sale por inducción en $\deg f$ ya que podemos arrancarle el término principal hasta que $\deg f < \deg g$ y es el resto; unicidad es fácil. Con esto tenemos que $k[x]$ es un dominio euclídeo si k es un cuerpo. Además $A[x]$ es DIP sii A es cuerpo: si es DIP, sea $(b) = (a, x)$ con $a \in A$; de $b \mid x$ sigue que b es unidad y $(a, x) = A[x]$; luego $(a) = A$ y a es unidad. Lema de Gauss: si A es un DFU y $f \in A[x]$ definimos $C(f)$ como el divisior común minimal de sus coeficientes; tenemos $C(fg) = C(f)C(g)$: suponemos wlog que $C(f) = C(g) = 1$, sea p un primo que divide a $C(fg)$; hay s, t con $p \mid f_i, g_j$ para $i < s, j < t$ pero $p \nmid f_s, g_t$; $p \mid f_0 g_{s+t} + \dots + f_{s-1}g_{t+1} + f_s g_t + f_{s+1}g_{t-1} + \dots + f_{s+t}g_0$; luego $p \mid f_s g_t$, absurdo. Entonces f es irreducible en $A[x]$ sii es irreducible en $F[x]$, donde F es el cuerpo de cocientes de A: si $f = gh$, $g, h \in F[x]$, entonces $af = g_1 h_1$, $a \in A$, $g_1, h_1 \in A[x]$; si $C(f) \neq 1$ está; si no, $a = C(g_1)C(h_1)$, $g_1 = C(g_1)g_2$, $h_1 = C(h_1)h_2$ y $f = g_2 h_2$. Resulta que $A[x]$ es DFU sii A es. Criterio de Eisenstein: si P es un ideal primo, $a \in A[x]$ de grado n, $a_n \notin P$, $a_{n-1}, \dots, a_0 \in P$ pero $a_0 \notin P^2$ entonces a es irreducible.

Raíces. Decimos que $s \in A^S$ es *raíz* de $f \in A[S]$ sii la evaluación de f en s es cero; llamamos $Z(f)$ al conjunto de raíces. En $A[x]$, c es raíz sii $x - c \mid f$; si A es íntegro entonces $f \neq 0$ tiene a lo sumo $\deg f$ raíces; iterando obtenemos que si $n \in \mathbb{N}$ y $\{A_x\}_{x \in n} \subset 2^A$ con $|A_x| > \deg_x f$, donde $\deg_x$ es el máximo exponente de x, entonces hay $s \in \prod_{x \in n} A_x$ que no es raíz; también (Schwartz-Zippel) que tiene a lo sumo $|A|^{n-1} \deg p$ raíces: sea q con $p = q x_0^{\deg_0 p} + r$ y $\deg_0 r < \deg_0 p$ entonces q tiene al menos $|A|^{n-1}(1 - \frac{\deg p - \deg_0 p}{|A|})$ no raíces y, para cada una, hay al menos $|A|(1 - \frac{\deg_0 p}{|A|})$ no raíces de p; luego hay al menos $|A|^n (1 - \frac{\deg p - \deg_0 p}{|A|})(1 - \frac{\deg_0 p}{|A|}) \geqq |A|^n - |A|^{n-1} \deg f$ no raíces. Si A es DFU, F es su cuerpo de cocientes, c/d es raíz de $a \in A[x]$ con $\operatorname{mcd}\{c, d\} = 1$ entonces $c \mid a_0$ y $d \mid a_n$. Si A es íntegro, $f = (x - c)^m g$ y c no es raíz de g, decimos que c es raíz de f con *multiplicidad* m. Definimos el *polinomio derivado* y c tiene multiplicidad mayor a uno como raíz de f sii $f(c) = f'(c) = 0$ y si $(f, f') = 1$ en un cuerpo entonces f no tiene raíces múltiples. Si $A \subset B$ son cuerpos, $f, g \in A[x]$, f irreducible, $f(c) = g(c) = 0$ para $c \in B$ entonces $f \mid g$, porque $r = (f, g)$ implica $r \mid f$, $r = 1$ y $af + bg = 1$, que evaluando en c da $0 = 1$, o $r = f$ y $f \mid g$. Probamos usando raíces que $\mathbb{Z}_p^\times \cong \mathbb{Z}_{p-1}$; el teorema chino del resto da $\mathbb{Z}_n^\times \cong \mathbb{Z}_{p_1^{\alpha_1}}^\times \times \dots \times \mathbb{Z}_{p_r^{\alpha_r}}^\times$ donde $n = p_1^{\alpha_1} \dots p_r^{\alpha_r}$; la proyección $\mathbb{Z}_{p^n}^\times \to \mathbb{Z}_p^\times$ tiene núcleo el p-primario; vemos que $1 + p$ tiene orden p^{n-1} para p impar así que $\mathbb{Z}_{p^\alpha}^\times$ es cíclico; si $n \geqq 3$, $\langle 2^{n-1} + 1 \rangle$ y $\langle 2^{n-1} - 1 \rangle$ son dos subgrupos de orden 2 de $\mathbb{Z}_{2^n}$; luego no es cíclico, pero 5 es de orden 2^{n-2}; queda que $\mathbb{Z}_{2^n}^\times \cong \mathbb{Z}_{2^{n-2}} \times \mathbb{Z}_2$.

Polinomios simétricos. S_n actúa sobre $R[x_1, \dots, x_n]$ por $\sigma f = f(x_{\sigma(1)}, \dots, x_{\sigma(n)})$; un polinomio f es *simétrico* si $\sigma f = f$ si $\sigma \in S_n$. Los polinomios simétricos elementales son $s_k = \sum_{i_1 < \dots < i_k} x_{i_1} \dots x_{i_k}$ para $k = 1, \dots, n$; tenemos $(X - x_1) \dots (X - x_n) = \sum_{k=0}^n (-1)^k s_k X^{n-k}$. El conjunto de pol simétricos es $R[s_1, \dots, s_n]$ (por inducción en n y $\deg f$: $f(x_1, \dots, x_{n-1}, 0) = p(s_1|_{x_n=0}, \dots, s_{n-1}|_{x_n=0})$ por inducción, luego $f_1 = f(x_1, \dots, x_n) - p(s_1, \dots, s_{n-1})$ es simétrico y $f_1(x_1, \dots, x_{n-1}, 0) = 0$, luego $x_n | f_1$ y $s_n | f_1$ por ser simétrico, luego $f = p(s_1, \dots, s_{n-1}) + s_n f_2$ con $\deg f_2 < \deg f$). Fórmula de Newton: si $p_k = \sum_{i=1}^n x_i^k$, $n s_n = \sum_{k=1}^n (-1)^{k+1} s_{n-k} p_n$ (de $f(X) = \prod_{i=1}^n (X - x_i) = \sum_{k=0}^n (-1)^k s_k X^{n-k}$ obtenemos $0 = \sum_{i=1}^n f(x_i) = \sum_{k=0}^n (-1)^k s_k p_{n-k}$).

Resultante. Si $f = \sum_{k=0}^n a_k X^k$, $g = \sum_{k=0}^m b_k X^k$, defino su resultante $\operatorname{Res}(f, g)$ como

$$\begin{vmatrix}
a_n & a_{n-1} & \cdots & a_0 & & & & \\
 & a_n & a_{n-1} & \cdots & a_0 & & & \\
 & & \ddots & & & \ddots & & \\
 & & & a_n & a_{n-1} & \cdots & a_0 & \\
b_m & b_{m-1} & \cdots & b_0 & & & & \\
 & b_m & b_{m-1} & \cdots & b_0 & & & \\
 & & \ddots & & & \ddots & & \\
 & & & b_m & b_{m-1} & \cdots & b_0 &
\end{vmatrix}$$

Si $C_1, \dots, C_{n+m}$ son las columnas, tenemos $C = (X^{m-1}f, X^{m-2}f, \dots, f, X^{n-1}g, \dots, g)$ cumple $C = X^{n+m-1}C_1 + \dots + 1 \cdot C_{n+m}$, por lo que $\det(C_1, \dots, C_{n+m-1}, C) = \det(C_1, \dots, C_{n+m}) =$

$\mathrm{Res}(f,g)$, pero se ve que el primer término es $\phi f+\psi g$. Entonces si $f(\alpha)=g(\alpha)=0$, $\mathrm{Res}(f,g)=0$. Si $f=a\prod_{k=1}^n(X-t_k)$ y $g=b\prod_{k=1}^m(X-u_k)$, $R=\mathrm{Res}(f,g)$ es un polinomio en $\mathbb{Z}[a,b,t,u]$; si $t_i=u_j$, $R=0$, por lo que $t_i-u_j\mid R$, luego $S=a^mb^n\prod_{i,j}(t_i-u_j)\mid R$, y $S=a^m\prod_{i=1}^n g(t_i)=(-1)^{nm}b^n\prod_{i=1}^n f(u_i)$; S y R son homogéneos de grado $n+m$ en $\mathbb{Z}[a_i,b_j]$, y el coef de $a_n^mb_0^n$ en ambos es 1, luego son iguales. En particular si f es mónico $\mathrm{Res}(f,f')=(-1)^{n(n-1)/2}\prod_{i<j}(t_i-t_j)=(-1)^{n(n-1)/2}D(f)$, con $D(f)$ el *discriminante* de f.

Base de Hilbert. Si R es Noetheriano entonces $R[X]$ también. Sea I un ideal no fg; sea $p_1\in I$ de grado mínimo, y elegidos $p_1,\dots,p_i$, sea p_{i+1} en $I\smallsetminus(p_1,\dots,p_i)$ de grado mínimo; sean a_i y d_i el coef principal y el grado de p_i y $J=(a_i)_{i\in I}$ el ideal en R; como R es noetheriano $J=(a_1,\dots,a_n)$; entonces $a_{n+1}=r_1a_1+\dots+r_na_n$ y $p_{n+1}=a_{n+1}X^{d_{n+1}}+h=\sum_{i=1}^n r_iX^{d_{n+1}-d_i}p_i+g$ (porque $d_1\leqq d_2\leqq\cdots$), con $\deg h,\deg g<\deg p_{n+1}$, y $g\in I\smallsetminus(p_1,\dots,p_n)$ contradice que $\deg p_{n+1}$ es mínimo. Sale que $R[X_1,\dots,X_n]$ es noetheriano.

Bases de Gröbner. Sea k cuerpo, $R=k[x_1,\dots,x_n]$; ordenamos los monomios por orden lexicográfico; llamamos $\ell(f)$ al mayor monomio, $\delta(f)$ a $\ell(f)$ mónico; si I es ideal, $\ell(I)=(\ell(a))_{a\in I}$; $\{g_i\}_{i=1}^n$ se dice una *base de Gröbner* de I sii $I=(g_i)_{i=1}^n$ y $\ell(I)=(\ell(g_i))_{i=1}^n$. Algoritmo de división: dados $f,\{g_i\}_{i=1}^n$, hay $\{q_i\}_{i=1}^n$ y r con $f=\sum_{i=1}^n q_ig_i+r$, $\ell(q_ig_i),\ell(r)\leqq\ell(f)$ y ningún monomio de r es múltiplo de un $\ell(g_i)$ (vamos tomando f y restando qg_i si $\ell(g_i)\mid\ell(f)$ o $\ell(f)$ y sumándolo a r); si $\{g_i\}_{i=1}^n$ es base de Gröbner de I esto da $f=f_I+r$ con $f_I\in I$, ningún monomio de r divisible por un $\ell(g_i)$, f_I, r únicos; en particular $r=0$ sii $f\in I$. Algoritmo de Buchberger: si $f_1,f_2\in R$, definimos $S(f_1,f_2)=\frac{M}{\ell(f_1)}f_1+\frac{M}{\ell(f_2)}f_2$, donde M es $\mathrm{mcm}(\delta(f_1),\delta(f_2))$; dado $I=(g_i)_{i=1}^n$, si $S(g_i,g_j)$ tienen resto 0 en la división por $\{g_i\}_{i=1}^n$, es una base de Gröbner; si no, lo agregamos y probamos de nuevo (supongamos que el resto de $S(g_i,g_j)$ es 0 y que $f\in I$ y veamos que $\ell(f)$ es divisible por un $\ell(g_i)$; tomo $f=\sum_{i=1}^n h_ig_i$ con h_i monomios y $m=\max\delta(h_ig_i)$ mínimo; si $\delta(f)<m$, $f=\sum_{\delta(h_ig_i)=m}h_ig_i+\sum_{\delta(h_ig_i)<m}h_ig_i$, $\delta(\sum_{\delta(h_ig_i)=m}h_ig_i)<m$; si $c_1f_1',\dots,c_rf_r'$ son esos h_ig_i, con $c_i\in k$, f_i' mónicos, tenemos $\sum_i c_if_i'=c_1(f_1'-f_2')+(c_1+c_2)(f_2'-f_3')+\dots+(c_1+\dots+c_r)f_r'$, pero este último término es el único con $\delta=m$, luego es 0, y $\sum_{\delta(h_ig_i)=m}h_ig_i=\sum_i a_iS(h_ig_i,h_{i+1}g_{i+1})$ con $a_i\in k$; ahora $S(h_ig_i,h_{i+1}g_{i+1})=p_iS(g_i,g_{i+1})$ con p_i monomio, $S(g_i,g_{i+1})$ es $\sum q_jg_j$ por hipótesis con $\delta(q_jg_j)<\delta(S(g_i,g_{i+1}))$, luego $\sum_{\delta(h_ig_i)=m}h_ig_i$ es suma de $a_ip_iq_jg_j$ con $\delta(a_ip_iq_jg_j)<m$, luego m no es mínimo, absurdo, y resulta $\delta(f)=m$; entonces $\ell(f)$ es divisible por un $\ell(g_i)$, listo). Decimos que $\{g_i\}_{i=1}^n$ es una base *reducida* si los g_i son mónicos y el resto de dividir g_i por $\{g_j\}_{j\neq i}$ es g_i; es única (primero vemos que los $\ell(g_i)$ son todos distintos y están determinados). Eliminación: si $G=\{g_i\}_{i=1}^m$ es base de Gröbner del ideal I entonces $G\cap k[x_i,\dots,x_n]$ es base de Gröbner del ideal $I\cap k[x_i,\dots,x_n]$. Si I,J son ideales, $tI+(1-t)J$ es ideal de $k[t,x_1,\dots,x_n]$ y $I\cap J=(tI+(1-t)J)\cap k[x_1,\dots,x_n]$.

Módulos I Si R es un anillo, un *R-módulo a izquierda* o un R-mód es un grupo abeliano ${}_RM$ con una operación $R\times M\to M$ notada rm para $r\in R,m\in M$ tal que $(r+s)m=rm+sm$, $(rs)m=r(sm)$, $r(m+n)=rm+rn$ y si R tiene 1, $1m=m$; análogamente se definen módulos a derecha o mód-R M_R; un R-módulo es lo mismo que una *representación*, esto es, un morfismo de anillos $R\to\mathrm{End}(M)$, donde M es un grupo abeliano. Si R,S son anillos, un *R-S-bimódulo* es un grupo abeliano ${}_RM_S$ que es un R-mód y un mód-S tal que $(rm)s=r(ms)$ para $r\in R,m\in M,s\in S$. Si R es conmutativo con unidad, una *R-álgebra* es un R-módulo A con estructura de anillo con unidad tal que $(rm)n=r(mn)$ y $m(rn)=r(mn)$ para $r\in R$; equivalentemente es un anillo con unidad y un morfismo $f:R\to A$ tal que $\mathrm{Im}\,f$ está en el centro de A. Si M y N son R-módulos, un *morfismo de R-módulos* es un morfismo de grupos f tal que $f(rx)=rf(x)$ para $r\in R$; el conjunto se nota $\mathrm{Hom}_R(N,M)$ y es un grupo abeliano; si R es conmutativo es un R-módulo y $\mathrm{Hom}_R(M,M)=\mathrm{End}_R(M)$ una R-álgebra. Un *morfismo de R-álgebras* A y B es un morfismo de anillos f tal que $f(ra)=rf(a)$ para $r\in R$.

Submódulos. Un *submódulo* de M es un subgrupo N tal que $rn\in N$ si $r\in R,n\in N$. Los

$\mathbb{Z}$ módulos son los grupos abelianos; los submódulos son los subgrupos. Si k es un cuerpo, los $k[x]$-módulos están en biyección con los endomorfismos f de k-módulos; los $k[x]$-submódulos son k-submódulos W con $f(W) \subset W$. Si N es submódulo de M se le puede dar estructura de R-módulo al cociente de grupos abelianos M/N y funcionan los morfismos canónicos. Si I es ideal se define $IM = \{\sum_{\text{finita}} a_i m_i \mid a_i \in I, m_i \in M\}$ y es submódulo; M/IM es un R/I-mód naturalmente. Un elemento $m \in M$ se dice de *torsión* si $rm = 0$ para algún $r \in R$ no nulo; forman M_{tor}; un módulo M se dice de *torsión* si $M_{\text{tor}} = M$; se define el *anulador* del submódulo N como $\operatorname{ann}(N) = \{r \in R \mid \forall n \in N(rn = 0)\}$ y el anulador del ideal I como $\operatorname{ann}(I) = \{m \in M \mid \forall a \in I(am = 0)\}$. Teorema chino del resto: si $I_1, \ldots, I_n$ son ideales con $I_j + I_j = R$ para $i \neq j$ entonces $M/(\bigcap_{i=1}^n I_i)M \cong \prod_{i=1}^n M/I_iM$. Si $\{N_i\}_{i\in I}$ es una familia de submódulos definimos la suma como $\sum_{i\in I} N_i = \{\sum_{\text{finito}} x_i \mid x_i \in N_i\}$; si $X \subset M$ definimos el R-submódulo generado por X como $\langle X\rangle = \bigcap_{X\subset N \text{ submódulo}} N = \sum_{x\in X} Rx$. Un submódulo es *cíclico* si está generado por un elemento sii es isomorfo a R/I; *finitamente generado* si está generado por finitos sii es isomorfo a un cociente de R^n. Definimos el *producto* de módulos $\prod_{i\in I} M_i$ y la *suma directa* módulos $\bigoplus_{i\in I} M_i$ como el submódulo del producto cuyas secuencias tienen finitos elementos no nulos. Si $\{N_i\}_{i\in I}$ es una familia de submódulos de M, decimos que la suma $\sum_{i\in I} N_i$ es directa si es $f : \sum_{i\in I} N_i \to \bigoplus_{i\in I} N_i$ dado por $f(\sum_{i\in I} x_i) = \sum_{i\in I} x_i$ es isomorfismo sii $N_i \cap \sum_{j\in I\setminus\{i\}} N_j = 0$ para todo $i \in I$ sii todo $x \in \sum_{i\in I} N_i$ se escribe de manera única como $\sum_{i\in I} x_i$ con $x_i \in N_i$; se nota $\bigoplus_{i\in I} N_i$. Si R es DIP y P es el conjunto de primos y M es de torsión entonces $M = \bigoplus_{p\in P} \bigcup_{r\in\mathbb{N}} \operatorname{ann}(p^r)$; si es finitamente generado, $\operatorname{ann}(M) = (\prod_{i=1}^r p_i^{\alpha_i})$ y $M = \bigoplus_{i=1}^r \operatorname{ann}(p_i^{\alpha_i})$.

Módulos libres. Un R-módulo se dice *libre* en $X \subset F$ sii permite escritura única como $\sum_{x\in X} a_x x$ sii es isomorfo $\bigoplus_{x\in X} R$ también notado $R^{\oplus X}$ y $R^{(X)}$ sii cumple la propiedad universal: si M es un R-módulo y $f : X \to M$ entonces se extiende de manera única a un morfismo $\hat{f} : F \to M$. Ejemplo: $\mathbb{Z}^{\mathbb{N}}$ no es libre: si tiene una base es no numerable; $\mathbb{Z}^{\oplus\mathbb{N}}$ como submódulo es numerable; luego está contenido en un submódulo generado por numerables elementos de la base; luego podemos definir $f : \mathbb{Z}^{\mathbb{N}} \to \mathbb{Z}$ no nulo que se anule en $\mathbb{Z}^{\oplus\mathbb{N}}$; ahora si $a \in \mathbb{Z}^{\mathbb{N}}$ definimos b, c con $b_i 2^i + c_i 3^i = a_i$ y tenemos $f(a) = f(b_i 2^i) + f(c_i 3^i)$; ahora $f(b_i 2^i) = f(b_1 2, \ldots, b_r 2^r, 0, \ldots) + 2^{r+1} f(b'_r) = 2^{r+1} f(b'_r)$; luego $2^r \mid f(b_i 2^i)$ para todo $r > 0$ y $f(b_i 2^i) = 0$; similarmente $f(c_i 3^i) = 0$, $f(a) = 0$ y $f = 0$, contradicción. Ejemplo de módulo libre sin rango único: sea $R = \operatorname{End}_{\mathbb{Z}}(\mathbb{Z}^{\mathbb{N}})$, $\phi_1, \phi_2 \in R$ dados por $\phi_1(a_1, a_2, a_3, \ldots) = (a_1, a_3, a_5, \ldots)$ y $\phi_2(a_1, a_2, a_3, \ldots) = (a_2, a_4, a_6, \ldots)$ y $\psi_1, \psi_2 \in R$ dados por $\psi_1(a_1, a_2, a_3, \ldots) = (a_1, 0, a_2, 0, \ldots)$ y $\psi_2(a_1, a_2, a_3, \ldots) = (0, a_1, 0, a_2, \ldots)$; se tiene $\phi_i\psi_i = 1$, $\phi_1\psi_2 = \phi_2\psi_1 = 0$, $\psi_1\phi_1 + \psi_2\phi_2 = 1$; luego $\{\phi_1, \phi_2\}$ es base de R como R-mód; luego $R \cong R^2$ y, en general, $R \cong R^n$ para $n \in \mathbb{N}$. Todo módulo sobre un anillo de división es libre: usar que si B es independiente y $x \notin \langle B\rangle$ entonces $B \cup \{x\}$ es independiente y buen orden. Si F es un cuerpo entonces $F^{(X)} \cong F^{(Y)}$ sii $|X| = |Y|$: expresamos los de la base más chica en la base más grande; en el caso finito es resolver un sistema de ecuaciones; en el infinito por cardinalidad alguno de la base grande no lo estamos usando, así que lo podemos sacar. Si R es dominio sea I un ideal maximal; $R^{(X)} \cong R^{(Y)}$ implica $R^{(X)}/IR^{(X)} \cong R^{(Y)}/IR^{(Y)}$; ahora $R^{(X)}/IR^{(X)} \cong (R/IR)^{(X)}$, $(R/IR)^{(X)} \cong (R/IR)^{(Y)}$ y, como R/I es un cuerpo, $|X| = |Y|$; luego podemos definir el cardinal de una base de un módulo libre; lo llamamos su *dimensión* o *rango*.

Matrices I. Llamamos *matrices* a los elementos de $R^{m\times n}$ con R dominio. Si $A \in R^{n\times m}, B \in R^{m\times r}$ definimos $A \cdot B \in R^{n\times r}$ de manera que $(A \cdot B)_{ij} = \sum_{k=1}^m A_{ik} B_{kj}$; es lineal en A y en B y es asociativa. Hay un isomorfismo $R^{m\times n} \cong \operatorname{Hom}_R(R^n, R^m)$ dado por $A \mapsto (v \mapsto Av)$; la multiplicación de matrices es la composición de sus morfismos asociados. Definimos $I_n \in R^{n\times n}$ tal que $(I_n)_{ij} = \delta_{ij} = [i = j]$ y vemos que $AI_n = A$ si $A \in R^{m\times n}$ y $I_n A = A$ si $A \in R^{n\times m}$. Llamamos $M_n(R)$ a $R^{n\times n}$; es una R-álgebra; definimos el *grupo lineal general* de orden n sobre R notado $GL_n(R)$ como $M_n(R)^\times$. Una función n-lineal alternada es una función $M : (R^n)^n \to R$ lineal en cada coordenada tal que $M(u) = 0$ si $u_i = u_{i+1}$ para algún i. Si $i \neq j$, $M(u) = 0$ si $u_i =$

u_j y $M(\ldots,v_i,\ldots,v_j,\ldots) = -M(\ldots,v_j,\ldots,v_i,\ldots)$; si $\sigma \in S_n$ entonces $M(v_{\sigma(1)},\ldots,v_{\sigma(n)}) = (-1)^{\operatorname{sig}\sigma} M(v_1,\ldots,v_n)$ y si $\sigma : [n] \to [n]$ no es biyectiva $M(v_{\sigma(1)},\ldots,v_{\sigma(n)}) = 0$; sigue que si $v'_i = a_{i1}v_1 + \cdots + a_{in}v_n$ entonces $M(v'_1,\ldots,v'_n) = \sum_{\sigma\in S_n}(-1)^{\operatorname{sig}\sigma} a_{1\sigma(1)}\ldots a_{n\sigma(n)} M(v_1,\ldots,v_n)$. Un *determinante* es una función D n-lineal alternada con $\det I_n = 1$; notamos $|A|$ o $\det A$. Lo anterior da $M(A) = D(A)M(I_n)$, $D(AB) = D(A)D(B)$ y que D es única. Construimos los determinantes inductivamente: para $n = 1$, $D(a_{11}) = a_{11}D(1) = a_{11}$. Para n, si lo definimos para $n-1$, hacemos corresponder a a_{ij} el cofactor C_{ij} cono el determinante de la matriz sin la fila i y la columna j multiplicado por $(-1)^{i+j}$ y ponemos $D(A) = a_{i1}C_{i1} + \cdots + a_{in}C_{in}$. Veamos que cumple las reglas: la linealidad es obvia; si dos columnas A_k y A_{k+1} son iguales, los cofactores de las columnas que no son k o $k+1$ se anulan y $a_{ik}C_{ik} = -a_{i(k+1)}C_{i(k+1)}$; la tercera regla es obvia. Notar que podríamos haber hecho todo por columnas sin cambiar el resultado. Si $A \in R^{n\times n}$ sea $\operatorname{adj} A \in R^{n\times n}$ dada por $(\operatorname{adj} A)_{ij} = C_{ji}$; la llamamos *adjunta* de A. Tenemos $\operatorname{adj}(A)A = A\operatorname{adj}(A) = |A|I_n$, por la fórmula de la construcción, ya que $a_{i1}C_{j1}+\cdots+a_{in}C_{jn} = |A|$ si $i = j$ y es igual al determinante de A con dos filas iguales, o sea cero, si $i \neq j$. Se sigue que $A \in GL_n(k)$ sii $|A| \in R^\times$; la otra implicación porque $1 = |AA^{-1}| = |A||A^{-1}|$. Si $A \in R^{n\times n}$ y $B \in R^{m\times m}$ tenemos que $\left|\begin{smallmatrix} A & C \\ 0 & B\end{smallmatrix}\right|$ es n-lineal alternada en A así que es $|A|\left|\begin{smallmatrix} I_n & C \\ 0 & B\end{smallmatrix}\right| = |A||B|$. Si $a_1,\ldots,a_n \in R$ y $A_{ij} = a_i^{j-1}$ entonces $|A| = \prod_{i>j}(a_i - a_j)$; sale sustrayendo la $k-1$-ésima fila multiplicada por x_1 a la k-ésima para $k = n, n-1,\ldots,2$; factorizando cada columna por $x_i - x_1$ queda el paso inductivo. Si $p = x^n + a_{n-1}x^{n-1} + \cdots + a_1x + a_0$ entonces $|xI - \mathcal{A}(p)| = p$, donde

$$\mathcal{A}(p) = \begin{pmatrix} 0 & & & & -a_0 \\ 1 & 0 & & & -a_1 \\ & 1 & \ddots & & \vdots \\ & & \ddots & 0 & -a_{n-2} \\ & & & 1 & -a_{n-1} \end{pmatrix}$$

es la matriz *acompañante* de p.

Módulos finitamente generados (f.g.). Si R es conmutativo y M está generado por $\{x_1,\ldots,x_n\}$, $I \subset R$ es ideal, $\phi \in \operatorname{End}_R(M)$ con $\phi(M) \subset IM$ entonces ϕ es raíz del polinomio $|A - xI_n| = x^n + a_{n-1}x^{n-1} + \cdots + a_0$, donde A es la matriz de ϕ sobre $\{x_1,\ldots,x_n\}$ y $a_i \in I$: $A \in I^{n\times n}$; la matriz de endomorfismos $A - \phi I_n$ anula al vector $(x_1,\ldots,x_n)$ y está en el subanillo $\{\sum_{\text{finita}} a_i\phi^i \mid a_i \in R\}$ de $\operatorname{End}_R(M)$ que es conmutativo; luego podemos multiplicar por la adjunta y obtenemos $|A - \phi I_n|x_i = 0$; luego $|A - \phi I_n| = 0$, como queríamos. Con $I = R$ obtenemos Cayley-Hamilton; si pedimos $IM = M$ y ponemos $\phi = 1$ obtenemos que $x = 1 + a_{n-1} + \cdots + a_0$ es el morfismo cero con $a_i \in I$; luego $x - 1 \in I$ y $xM = 0$. Obtenemos el lema de Nakayama: si M es f.g. y I es un ideal contenido en el radical de Jacobson, $IM = M \Rightarrow M = 0$, porque $xM = 0$ con $x - 1 \in J(R)$ así que $x \in R^\times$ y $M = x^{-1}xM = 0$; si $I \subset J(R)$, $N \subset M$ entonces $M = IM + N \Rightarrow M = N$, por $I(M/N) = (IM + N)/N$ y Nakayama; si R es local, $\mathfrak{m} = J(R)$ es maximal, $M/\mathfrak{m}M$ es un $A/\mathfrak{m}$-e.v.; las imágenes de $x_i \in M$ forman una base de $M/\mathfrak{m}M$ sii x_i es un sistema de generadores minimal: si $N = \langle x_i\rangle$, $N + \mathfrak{m}M = M$ y $N = M$. Si $\phi \in \operatorname{End}_R(M)$ es epi, es iso: M es un $R[x]$-mód por ϕ; $IM = M$ con $I = \langle x\rangle$; luego hay $p \in R[x]$ con $pM = 0$ y $p = qx + 1$; luego $p(\phi) = 0$, $-q(\phi)\phi = 1$ y ϕ es mono. Si $R \subset S$ son anillos conmutativos decimos que $u \in S$ es *integral* sobre R si hay $f \in R[X]$ mónico con $f(u) = 0$; forman un anillo (si $u, v \in S$ son integrales, $R[u, v]$ es un R-mod fg, luego si $w \in R[u, v]$, por Cayley-Hamilton sobre $\phi(x) = wx$ tenemos w integral sobre R).

Matrices II. Permutación, multiplicación por unidades y suma de múltiplos de filas y columnas se logra multiplicando a izquierda y derecha, respectivamente, por matrices inversibles. Resulta como consecuencia que los ideales de $M_n(R)$ son $M_n(I)$ con I ideal de R. Si R es DIP y $A \in R^{n\times m}$ la podemos llevar a la forma PSQ, donde $P, Q \in M_n(R)^\times$, $S_{ij} = 0$ si $i \neq j$, $a_i = S_{ii}$ y $a_1 \mid a_2 \mid \cdots \mid a_n$, su *forma normal de Smith.* (Itero sobre $i = 1,\ldots,\min\{n, m\}$. En el paso i logro que $A_{i'j} = A_{ji'} = 0$ para $i' \leqq i$, $j \neq i'$. Hay un método para poner $A_{ii} \leftarrow \operatorname{mcd}\{A_{ji} \mid j \in [n]\}$ y $A_{ji} \leftarrow 0$ para $j \neq i$, y un método para poner $A_{ii} \leftarrow \operatorname{mcd}\{A_{ij} \mid j \in [m]\}$ y $A_{ij} \leftarrow 0$ para $j \neq i$. El primero: tomo cada $j > i$; sean $a = A_{ii}, b = A_{ji}, d = (a, b), d = ax + by, x' = \frac{b}{d}, y' = -\frac{a}{d}$;

cambiamos las filas A_i y A_j por $xA_i + yA_j$ y $x'A_i + y'A_j$; eso es multiplicar a izquierda por una matriz inversible como acá: $\begin{pmatrix} x & y \\ x' & y' \end{pmatrix}\begin{pmatrix} a & * \\ b & * \end{pmatrix} = \begin{pmatrix} d & * \\ 0 & * \end{pmatrix}$; queda $A_{ii} = d$ y $A_{ji} = 0$. Para las columnas se hace algo similar. Alternando los métodos tenemos que los ideales (A_{ii}) forman una cadena ascendente; cuando se estaciona tenemos que A_{ii} divide a todos los de su fila y columna; entonces los podemos reducir a cero *a todos* sumando múltiplos de la fila/columna i. Al final la matriz queda diagonal. Ponemos el mcd de todo en A_{11} siguiendo pasos como el siguiente: $\begin{pmatrix} a & \\ & b \end{pmatrix} \to \begin{pmatrix} a & \\ b & b \end{pmatrix} \to \begin{pmatrix} d & dr \\ & ds \end{pmatrix} \to \begin{pmatrix} d & \\ & ds \end{pmatrix}$; ahora ponemos el mcd del resto en A_{22}, etc y queda.) Los i-menores de una matriz son las submatrices en $R^{i\times i}$ que vienen de quitar filas y columnas; los determinantes de los i-menores de PA y AQ son combinacion lineal de los det. de los de A (las filas de PA son combinación lineal de las filas de A, luego el det del r-menor de filas $\{i_1, \ldots, i_r\}$ y columnas $\{j_1, \ldots, j_r\}$ es $D(P_{i_1 1}A_{1,\{j_1,\ldots,j_r\}} + \cdots + P_{i_1 n}A_{n,\{j_1,\ldots,j_r\}}, \ldots)$, que por multilinealidad alternada se expresa como combinación lineal de $D(A_{k_1,\{j_1,\ldots,j_r\}}, \ldots, A_{k_r,\{j_1,\ldots,j_r\}})$, que son det de r-menores de A), luego sus mcds son divisibles por los mcds de los de A; en $A = PSQ$ obtenemos que los mcds de los det. de los i-menores de A, llamados Δ_i, y los de S coinciden salvo asociación; los segundos son $a_1 \ldots a_i$; luego a_i y Δ_i/Δ_{i-1} son asociados, por lo que la S de la forma normal de Smith es única salvo asociación; los a_i se llaman *factores invariantes* de A.

Módulos fg sobre DIPs. Si M es libre con base $\{x_1, \ldots, x_n\}$ y N es submódulo entonces N es libre de rango a lo sumo n: por inducción asumimos que $N_r = N \cap \langle x_1, \ldots, x_r\rangle$ es libre de dimensión a lo sumo r; ahora los $a \in R$ tales que hay $x \in N_{r+1}$ con $\pi_{r+1}(x) = a$ forman un ideal (a_{r+1}); si $a_{r+1} = 0$, $N_{r+1} = N_r$; si no, sea $w \in N_{r+1}$ con $\pi_{r+1}(w) = a_{r+1}$; se ve que $N_{r+1} = N_r \oplus \langle w\rangle$ y listo. Ahora sea $y_1, \ldots, y_m$ una base de N; hay una matriz A con $(y_1, \ldots, y_m) = A(x_1, \ldots, x_n)$; ponemos $A = PSQ$, su forma normal de Smith, y tenemos $P^{-1}(y_1, \ldots, y_m) = SQ(x_1, \ldots, x_n)$; $Q(x_1, \ldots, x_n)$ es una base $v_1, \ldots, v_n$ de M y $P^{-1}(y_1, \ldots, y_m)$ una base $a_1v_1, \ldots, a_mv_m$ de N con $a_1 \mid \cdots \mid a_m$. Ahora sea M un módulo f.g. de rango n; hay un epimorfismo $\phi : L \to M$ con L libre; lo anterior sobre $\ker\phi$ da que es $\bigoplus_{i=1}^n \langle a_ie_i\rangle$ con $L = \bigoplus_{i=1}^n \langle e_i\rangle$ y $a_1 \mid \cdots \mid a_n$ así que $M \cong L/\ker\phi = \bigoplus_{i=1}^n R/(a_i)$. Notar que $M_{\text{tor}} \cong \bigoplus_{i=1}^s R/(a_i)$ y $M \cong M_{\text{tor}} \oplus R^r$, donde r, s son los números de elementos nulos y no nulos en $a_1, \ldots, a_n$; los no nulos se llaman *factores invariantes* de M. Si factorizamos en primos, $a_i = p_1^{\alpha_{i1}} \ldots p_r^{\alpha_{it}}$ y $M \cong \bigoplus_{i=1}^s \bigoplus_{j=1}^t R/(p_j^{\alpha_{ij}})$ y los $p_j^{\alpha_{ij}}$ se llaman *divisores elementales*. Veamos que los factores invariantes y los divisores elementales están determinados salvo asociación: si $\phi : M \to N$ es iso, $\phi(M_{\text{tor}}) = N_{\text{tor}}$, $M/M_{\text{tor}} \cong N/N_{\text{tor}}$, $R^{r_1} \cong R^{r_2}$ y $r_1 = r_2$; sea p primo; tomamos los submódulos p-primarios, el isomorfismo los preserva, luego son isomorfos y son $\operatorname{ann}(p^k)$; vemos que comparten factores elementales por inducción en k; si los de M son $\underbrace{p, \ldots, p}_{m \text{ veces}}, p^{\alpha_1}, \ldots, p^{\alpha_s}$ y los de N son $\underbrace{p, \ldots, p}_{n \text{ veces}}, p^{\beta_1}, \ldots, p^{\beta_r}$, los de pM son $p^{\alpha_1-1}, \ldots, p^{\alpha_s-1}$ y los de pN son $p^{\beta_1-1}, \ldots, p^{\beta_r-1}$; luego $s = r$ y $\alpha_i = \beta_i$ por inducción; ahora $M/pM \cong (R/(p))^{m+s}$, $N/pN \cong (R/(p))^{n+r}$ y $m = n$, así que los divisores elementales coinciden; los factores elementales se arman a partir de sus divisores elementales, así que también coinciden. Obtenemos que si G es un grupo abeliano finitamente generado entonces es $\mathbb{Z}^r \oplus \mathbb{Z}_{a_1} \oplus \cdots \oplus \mathbb{Z}_{a_n}$ con $a_1 \mid \cdots \mid a_n$ y los $r, a_1, \ldots, a_n$ están determinados.

Endomorfismos en un k-mod de dimensión finita. Sea $f \in \operatorname{End}_k(V)$, V un k-mod con $\dim V = n$, k cuerpo. V es un $k[x]$-mód de torsión con la acción que viene de extender $a \cdot v = av$ para $a \in k$ y $x \cdot v = f(v)$; sea (u_i) una base de V como k-mod y sea $\phi : k[x]^n \to V$ dado por $e_i \mapsto u_i$; es suryectivo; sea $A = (a_{ij})$ la matriz de f en (u_i); $(f_i = xe_i - \sum_{j=1}^n a_{ij}e_j) = (xI - A)(e_i)$ es base de $\ker\phi$; ponemos $xI - A$ en su forma normal de Smith PSQ, $d_1 \mid \cdots \mid d_n$ son sus factores invariantes, luego $(g_i) = Q(e_i)$ es base de $k[x]^n$ con (d_ig_i) es base de $\ker\phi$; entonces $V = \langle\phi(g_1)\rangle \oplus \cdots \oplus \langle\phi(g_n)\rangle$ como $k[x]$-mód; entonces $\{z_1, fz_1, \ldots, f^{\deg d_1 - 1}z_1, \ldots, z_n, fz_n, \ldots, f^{\deg d_n - 1}z_n\}$ es una base de V como k-e.v., la matriz de f en esa base es $\mathcal{A}(d_1)\oplus\cdots\oplus\mathcal{A}(d_n)$, la *forma normal racional* de f. Notar que $|xI-A| = d_1\dots d_n$; cuando se factoriza linealmente, los divisores elementales de $xI-A$ son $(x-\lambda_i)^{e_i}$, entonces $V=\bigoplus_{i=1}^m\langle z_i\rangle$ con $(x-\lambda_i)^{e_i}z_i=0$ en $k[x]$ así que en k tenemos que $\bigcup_{i=1}^m\{z_i,\dots,(f-\lambda_i)^{e_i-1}z_i\}$ es base y la matriz de f en esa base es $\bigoplus_{i=1}^m\mathcal{J}(\lambda_i,e_i)$ donde $\mathcal{J}(\lambda,r)$ es

$$\begin{pmatrix}\lambda & & & \\ 1 & \ddots & & \\ & \ddots & \lambda & \\ & & 1 & \lambda\end{pmatrix}$$

en $k^{r\times r}$, lo que se conoce como *forma de Jordan* de A. Dos matrices A,B se dicen *semejantes* si hay C inversible con $A=CBC^{-1}$; lo que hicimos muestra que A y B son semejantes sii $xI-A$ y $xI-B$ tienen la misma forma normal de Smith sii A,B tienen la misma forma racional canónica.

Módulos II Si $f\in\operatorname{Hom}_R(M,N)$, definimos el *núcleo* $\ker f=f^{-1}(0)$, la *imagen* $\operatorname{im} f=f(M)$ y el *conúcleo* $\operatorname{coker} f=N/\operatorname{im} f$. Decimos que f es *monomorfismo* si f es inyectiva sii $\ker f=0$ sii para todo R-mód T y morfismos $g,h:T\to M$ se tiene $f\circ g=f\circ h\Rightarrow g=h$ y además sii $f\circ g=0\Rightarrow g=0$. Decimos que f es *epimorfismo* si f es sobreyectiva sii $\operatorname{coker} f=0$ sii $g\circ f=h\circ f\Rightarrow g=h$ y además sii $g\circ f=0\Rightarrow g=0$. Decimos que f es *sección* si existe g con $g\circ f=id$; *retracción* si existe g con $f\circ g=id$. Una sucesión (M_n,f_n) de R-módulos y morfismos $f_n:M_n\to M_{n+1}$ se dice *exacta* en el lugar n si $\operatorname{im} f_n=\ker f_{n+1}$; se dice exacta si es exacta en todo lugar. En el diagrama donde las filas son exactas

$$\begin{tikzcd} 0 \arrow[r] & A \arrow[r, "f"] \arrow[d, "\alpha"] & B \arrow[r, "g"] \arrow[d, "\beta"] & C \arrow[r] \arrow[d, "\gamma"] & 0 \\ 0 \arrow[r] & A' \arrow[r, "f'"] & B' \arrow[r, "g'"] & C' \arrow[r] & 0 \end{tikzcd}$$

si hay α y β que lo hacen conmutar existe un único γ que lo completa; en ese caso si α y γ son mono (epi, iso) entonces β también. En el diagrama

$$\begin{tikzcd} A_1 \arrow[r] \arrow[d, "\alpha_1"] & A_2 \arrow[r] \arrow[d, "\alpha_2"] & A_3 \arrow[r] \arrow[d, "\alpha_3"] & A_4 \arrow[r] \arrow[d, "\alpha_4"] & A_5 \arrow[d, "\alpha_5"] \\ B_1 \arrow[r] & B_2 \arrow[r] & B_3 \arrow[r] & B_4 \arrow[r] & B_5 \end{tikzcd}$$

si α_2,α_4 son mono y α_1 es epi entonces α_3 es mono; si α_2,α_4 son epi y α_5 es mono entonces α_3 es epi; si $\alpha_1,\alpha_2,\alpha_4,\alpha_5$ son iso, α_3 también. Una *sucesión exacta corta* es $0\to M\xrightarrow{f}N\xrightarrow{g}T\to 0$; son equivalentes que f sea una sección, g una retracción y que $N\cong M\oplus T$: si $h\circ f=\mathrm{id}$, $n\mapsto(h(n),g(n))$ es una biyección. En ese caso decimos que la sucesión se parte, se escinde o es split. Si $M,M',P\in A$-mód y $f\in\operatorname{Hom}_A(M,M')$ definimos $f_*^P: h\mapsto f\circ h$ y $0\to M'\xrightarrow{f}M\xrightarrow{g}M''$ es exacta sii $0\to\operatorname{Hom}_A(N,M')\xrightarrow{f_*^N}\operatorname{Hom}_A(N,M)\xrightarrow{g_*^N}\operatorname{Hom}_A(N,M'')$ es exacta para todo $N\in A$-mód; esto dice que $N\mapsto\operatorname{Hom}_A(N,-)$ es un funtor exacto a izquierda; similarmente $N\mapsto\operatorname{Hom}_A(-,N)$ es exacto a derecha: $M'\xrightarrow{f}M\xrightarrow{g}M''\to 0$ es exacta sii $0\to\operatorname{Hom}_A(M'',N)\xrightarrow{g_N^*}\operatorname{Hom}_A(M,N)\xrightarrow{f_N^*}\operatorname{Hom}_A(M',N)$ es para todo N. $0\to M'\xrightarrow{f}M\xrightarrow{g}M''\to 0$ es split sii $0\to\operatorname{Hom}_A(N,M')\xrightarrow{f_*^N}\operatorname{Hom}_A(N,M)\xrightarrow{g_*^N}\operatorname{Hom}_A(N,M'')\to 0$ es exacta para todo $N\in A$-mód: tomamos $N=M''$ y usamos la suryectividad de $g_*^{M''}$ para encontrar $\mu\in\operatorname{Hom}(M'',M)$ con $g\circ\mu=1_{M''}$.

Módulos proyectivos. Un R-mód P es *proyectivo* sii $\operatorname{Hom}_R(P,-)$ es exacto sii para $M,N\in R$-mód con $M\xrightarrow{\phi}N\to 0$ exacta y $f\in\operatorname{Hom}(P,N)$ hay $F\in\operatorname{Hom}(P,M)$ tal que

$$\begin{tikzcd} & P \arrow[dl, "F"'] \arrow[d, "f"] & \\ M \arrow[r, "\phi"] & N \arrow[r] & 0 \end{tikzcd}$$

conmuta sii toda sucesión exacta $0 \to L \to M \to P \to 0$ es split sii P es un sumando directo de un R-mód libre: las dos primeras vimos que son equivalentes; dada la segunda, de $M \xrightarrow{\phi} P \to 0$ factorizamos $P \xrightarrow{id} P = P \xrightarrow{\mu} M \xrightarrow{\phi} P$ y ϕ es retracción; P es L/M con L libre, así que partimos $0 \to M \to L \to P \to 0$; si $P \oplus M = L$, $M, N \in R$-mód con $M \xrightarrow{\phi} N \to 0$ exacta y $f \in \mathrm{Hom}(P, N)$, tomamos $F' : L \to M$ con $L \xrightarrow{\pi} P \xrightarrow{f} N = L \xrightarrow{F'} M \xrightarrow{\phi} N$ y ponemos $F = F' \circ \iota$, con $P \xrightarrow{\iota} L$ la inclusión. Si $(M_i)_{i \in I}$ son A-mód entonces $\bigoplus_{i \in I} M_i$ es proyectivo sii M_i es para todo i; si $\prod_{i \in I} M_i$ es entonces M_i son.

Módulos inyectivos. Un R-mód Q es *inyectivo* sii $\mathrm{Hom}_R(-, Q)$ es exacto sii para $L, M \in R$-mód con $0 \to L \xrightarrow{\psi} M$ exacta y $f \in \mathrm{Hom}(L, Q)$ hay $F \in \mathrm{Hom}(M, Q)$ tal que

$$\begin{tikzcd} 0 \arrow[r] & L \arrow[r, "\psi"] \arrow[d, "f"'] & M \arrow[dl, "F"] \\ & Q & \end{tikzcd}$$

conmuta sii toda sucesión exacta $0 \to Q \to M \to N \to 0$ se parte: partir $0 \to Q \to M \to N \to 0$ se hace buscando la sección; sea Q' inyectivo con $\iota : Q \hookrightarrow Q'$; entonces $Q' = Q \oplus K$; si $0 \to A \xrightarrow{\psi} B$ exacta y $f \in \mathrm{Hom}(L, Q)$, levantamos $\iota \circ f$ a $F' : B \to Q'$ y $F = \pi \circ F' : B \to Q$ levanta. Criterio de Baer: Q es inyectivo sii para todo ideal izquierdo I de R todo $g : I \to Q$ se extiende a $G : R \to Q$: sean L, M con $0 \to L \to M$ exacta y $f \in \mathrm{Hom}(L, Q)$; ordenamos las extensiones (F', L') con $F' : L' \to Q$, $L \leq L \leq M$ por inclusión y aplicamos el lema de Zorn, que da $F : M' \to Q$ maximal; sea $m \in M \setminus M'$, $I = \{r \in R \mid rm \in M'\}$ (ideal izquierdo), $g(x) = F(xm)$ en $I \to Q$, G la extensión a $R \to Q$; $F' : M' + \langle m \rangle \to Q$ con $F'(m' + rm) = F(m') + F(r)$ extiende a F, absurdo. Si R es DIP, Q es inyectivo sii $rQ = Q$ para todo $r \in R$ no nulo; en ese caso se dice que Q es *de división*. Si M es un $\mathbb{Z}$-mód es $\mathbb{Z}^{(I)}/K \subset \mathbb{Q}^{(I)}/K$, luego es submódulo de un $\mathbb{Z}$-mód inyectivo; en general si M es un R-mód donde R es un anillo con 1, $M \hookrightarrow D$ con D un $\mathbb{Z}$-mód inyectivo, $M \cong \mathrm{Hom}_R(R, M) \subset \mathrm{Hom}_{\mathbb{Z}}(R, M) \subset \mathrm{Hom}_{\mathbb{Z}}(R, D)$; ahora $I = \mathrm{Hom}_{\mathbb{Z}}(R, D)$ es inyectivo: para levantar $f : A \to I$ a $F : B \to I$ ponemos $f' : A \to D$ con $f'(a) = f(a)(1)$, levantamos a $F' : B \to D$ y ponemos $F(a)(r) = F'(ra)$; entonces M es submódulo de un inyectivo.

Producto tensorial. Si M_R y ${}_RN$ son módulos, defino el *producto tensorial* $M \otimes_R N$ como el grupo abeliano libre $\mathbb{Z}^{(M \times N)}$ cocientado por las relaciones $(m + m', n) - (m, n) - (m', n)$, $(m, n+n') - (m, n) - (m, n')$ y $(mr, n) - (m, rn)$; llamo $m \otimes n$ a la proyección $p(m, n)$ y generan. Si G es un grupo abeliano, un morfismo $M \otimes_R N \xrightarrow{\bar{f}} G$ viene dado por una función R-balanceada $f : M \times N \to G$ viz que cumple $f(m+m', n) = f(m, n) + f(m', n)$, $f(m, n+n') = f(m, n) + f(m, n')$, $f(m, n) = f(m, rn)$ por $\bar{f} = f \circ p$. Se ve que si M es S-mod, $M \otimes_R N$ es con $s(m \otimes n) = (sm) \otimes n$. Vale $R \otimes_R M \cong M$, $R/I \otimes_R N \cong N/IN$, $\mathbb{Z}_n \otimes_{\mathbb{Z}} \mathbb{Z}_m \cong \mathbb{Z}_{(n,m)}$, $(\bigoplus_{i \in I} M_i) \otimes_R N \cong \bigoplus_{i \in I} (M_i \otimes_R N)$, si ${}_AX_B, {}_BY_C, {}_AZ_C$ entonces ${}_A \mathrm{Hom}_C(X \otimes_B Y, Z) \cong {}_A \mathrm{Hom}_B(X, \mathrm{Hom}_C(Y, Z))$ y $\mathrm{Hom}_A(X \otimes_B Y, Z)_C \cong \mathrm{Hom}_B(Y, \mathrm{Hom}_A(X, Z))_C$, isomorfismos naturales de funtores. Se ve que dados ${}_AX_B, {}_AY_B$ tales que para todo A-mod Z hay un isomorfismo natural $\mathrm{Hom}_A(X, Z)_B \cong \mathrm{Hom}_A(Y, Z)_B$ entonces $X \cong Y$; con eso se ve que $(M \otimes_B N) \otimes_C P \cong M \otimes_B (N \otimes_C P)$. Tenemos que $M \otimes_R -$ es un funtor que manda $N \xrightarrow{f} N'$ a $M \otimes_R N \xrightarrow{f'} M \otimes_R N$ dado por $f'(m \otimes n) = m \otimes f(n)$; es exacto a derecha usando que $\mathrm{Hom}(-, P)$ es exacto a derecha, $\mathrm{Hom}(M, -)$ exacto a izquierda y $\mathrm{Hom}(M, \mathrm{Hom}(-, P)) \cong \mathrm{Hom}(M \otimes -, P)$ isomorfismo natural. Un módulo P se dice *plano* si $M \otimes_R -$ es exacta; proyectivo implica plano (se ve para libre $R^{(I)} = P \oplus L$ y luego P). Si R es conmutativo, S multiplicativamente cerrado y M un R-mod definimos $S^{-1}M$ como $S^{-1}R \otimes_R M$ con $M \xrightarrow{\iota_S} S^{-1}M$ por $m \mapsto \frac{s}{s} \otimes m$; cumple la propiedad universal si N es un R-mod tal que $n \mapsto sn$ es automorfismo para cada $s \in S$ entonces todo $M \xrightarrow{f} N$ es $M \xrightarrow{\iota_S} S^{-1}M \xrightarrow{\bar{f}} N$; $S^{-1}M$ es plano; $\mathbb{Q}$ no es $\mathbb{Z}$-proyectivo.

Módulos noetherianos y artinianos. Un R-mod M es *noetheriano* sii todo submódulo es f.g. sii toda cadena ascendente de submódulos se estaciona. Un R-mod M es *finitamente cogenerado* si para todos submódulos $\{N_i\}_{i\in I}$ vale que si $\bigcap_{i\in I} N_i = 0$ entonces hay $J \subset I$ finito con $\bigcap_{i\in J} N_i = 0$. M es *artiniano* sii todo cociente es finitamente cogenerado sii toda cadena descendente de submódulos se estaciona. Si $0 \to N \to M \to N' \to 0$ es exacta, M es noetheriano/artiniano sii N y N' son. Un mod M es *hopfiano* si todo morfismo suryectivo $M \xrightarrow{f} M$ es inyectivo; *cohopfiano* si todo inyectivo $M \xrightarrow{f} M$ es suryectivo; noetheriano implica hopfiano (si f no es inyectivo $\ker f^n \subsetneqq \ker f^{n+1}$ por inducción: $\ker f^{n+1} = f^{-1}(\ker f^n) \subsetneqq f^{-1}(\ker f^{n+1}) = \ker f^{n+2}$) y artiniano implica cohopfiano (si f no es suryectivo, $\operatorname{im} f^n \supsetneqq \operatorname{im} f^{n+1}$).

Módulos y anillos semisimples. Un R-mod M es *simple* si $M \neq 0$ y sus únicos submódulos son 0 y M; *semisimple* si es suma directa de submod simples, sii todo submódulo es sumando directo (si $M = \bigoplus_{i\in I} M_i$ y N es submod, sea $J \subset I$ maximal con $N \cap \bigoplus_{i\in J} M_i = 0$; si $i \in I$, $M_i \cap (N \oplus \bigoplus_{i\in J} M_i)$ no es 0 porque J es maximal, luego es M_i, M_i está contenido para todo $i \in I$ y $N \oplus \bigoplus_{i\in J} M_i = M$; si todo submod es sumando directo, sea $\bigoplus_{i\in I} M_i$ maximal con M_i simples, $M = \bigoplus_{i\in I} M_i \oplus N$; si $N \neq 0$, $m \in N$ no nulo, $\operatorname{ann}(m) \subset I$ con I ideal izquierdo maximal, luego Rm/Im es simple, $M = Im \oplus L$, $Rm = Rm \cap L \oplus Im$ y $S = Rm \cap L \cong Rm/Im$ es submod simple; $S \cap \bigoplus_{i\in I} M_i = 0$ y $\{M_i\}_{i\in I}$ no es maximal, absurdo). Si N es submod de M semisimple, N y M/N son (si N' es N-submod, $M = N' \oplus L$ y $N = N' \oplus \pi_L(N)$; $M/N \cong N'$ con $M = N \oplus N'$). Un anillo R se dice *semisimple* si es semisimple como R-mod, sii todo R-mod es semisimple sii todo R-mod es proyectivo sii todo R-mod es inyectivo sii todo ideal izquierdo de R es inyectivo (M es cociente de $R^{(M)}$, obviamente semisimple; si $0 \to A \to B \to M \to 0$, B semisimple, la suc se parte y M es proyectivo, etc). R semisimple es noetheriano y artiniano a izquierda (si I ideal izquierdo, $R = I \oplus J$, $I \cong R/J$, generado por $1 + J$, y R es noetheriano; si $I_1 \supsetneqq I_2 \supsetneqq \cdots$, $I_1 = I_2 \oplus J_1$, $I_2 = I_3 \oplus J_2$, etc, y $J_1 \subsetneqq J_1 \oplus J_2 \subsetneqq \cdots$, abs). Si R es de división, $M_n(R)$ es semisimple, suma de los ideales izquierdos que tienen todos ceros salvo en la i-columna; recíprocamente (Wedderburn) si R es semisimple es $\prod_{i=1}^n M_{r_i}(R_i)$ con R_i de división: si $R \cong \bigoplus_{i=1}^n E_i^{r_i}$ con E_i simples, $E_i \not\cong E_j$ si $i \neq j$, $R^{\mathrm{op}} \cong \operatorname{Hom}_R(R,R) \cong \prod_{i=1}^n \operatorname{Hom}_R(E_i^{r_i}, E_i^{r_i}) = \prod_{i=1}^n M_{r_i}(\operatorname{End}(E_i))$, los $\operatorname{End}(E_i)$ son de división, y $R \cong \prod_{i=1}^n M_{r_i}(\operatorname{End}(E_i)^{\mathrm{op}})$. Maschke: si G grupo finito, k cuerpo y $|G| \in k^\times$, $k[G]$ es un anillo semisimple (si S es $k[G]$-submod, $k[G] = S \oplus L$ como k-mod con $\pi_S|_S = \mathrm{id}_S$, defino $\phi : k[G] \to S$ por $\phi(m) = \frac{1}{|G|}\sum_{g\in G} g\pi_S(g^{-1}m)$; vemos $\phi(s) = s$ si $s \in S$ y $\phi(hm) = h\phi(m)$ si $h \in G, m \in k[G]$, luego es morfismo en $k[G]$-mod con $\phi|_S = \mathrm{id}_S$, luego S es sumando directo).

Álgebras tensoriales, simétricas y exteriores. Una R-álgebra A se dice *graduada* si es $\bigoplus_{n=1}^\infty A_n$, con $A_n A_m \subset A_{n+m}$; un *ideal graduado* es un ideal $I = \bigoplus_{n=1}^\infty (I \cap A_n)$; el cociente A/I resulta naturalmente un álgebra graduada. Dado M un R-mód, R dominio íntegro, ponemos $\mathcal{T}_n(M) = M^{\otimes n}$ ($\mathcal{T}_0 = R$, $\mathcal{T}_{n+1} = \mathcal{T}_n \otimes M$) y $\mathcal{T}(M) = \bigoplus_{n=0}^\infty \mathcal{T}_n(M)$ resulta un álgebra graduada, el *álgebra tensorial* de M. Los morfismos $\mathcal{T}_n(M) \to N$ son morfismos n-lineales $M^n \to N$; si M es libre de rango m, $\mathcal{T}_n(M)$ es libre de rango m^n; si A es R-álgebra, $M \to A$ se factoriza de manera única por $M \to \mathcal{T}(M) \to A$. El ideal I de $\mathcal{T}(M)$ generado por los $m \otimes n - n \otimes m$ es graduado; defino $\mathcal{S}(M) = \mathcal{T}(M)/I$, el *álgebra simétrica* de M; los morfismos $\mathcal{S}_n(M) \to N$ son morfismos n-lineales $M^n \xrightarrow{f} N$ con $f(x_{\sigma_1}, \ldots, x_{\sigma_n}) = f(x_1, \ldots, x_n)$ para $\sigma \in S_n$; si M es libre de rango m, $\mathcal{S}_n(M)$ es libre de rango $\binom{n+m-1}{n}$; si A es R-álgebra conmutativa, $M \to A$ se factoriza de manera única por $M \to \mathcal{S}(M) \to A$. El ideal I de $\mathcal{T}(M)$ generado por los $m \otimes m$ es graduado; defino $\mathcal{A}(M) = \mathcal{T}(M)/I$, el *álgebra exterior* de M; los morfismos $\mathcal{A}_n(M) \to N$ son morfismos n-lineales $M^n \xrightarrow{f} N$ con $f(x) = 0$ si $x_i = x_j$, $i \neq j$; si M es libre de rango m, $\mathcal{A}_n(M)$ es libre de rango $\binom{m}{n}$; si A es álgebra con $a^2 = 0$, $M \to A$ se factoriza por $M \to \mathcal{S}(M) \to A$.

Homología. Lema de la serpiente: dado el siguiente diagrama conmutativo con filas exactas en R-mód

$$\begin{array}{ccccccc}
 & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow 0 \\
 & \downarrow{\scriptstyle a} & & \downarrow{\scriptstyle b} & & \downarrow{\scriptstyle c} & \\
0 \longrightarrow & A' & \xrightarrow{f'} & B' & \xrightarrow{g'} & C' &
\end{array}$$

hay una secuencia exacta $\ker a \to \ker b \to \ker c \xrightarrow{\partial} \operatorname{coker} a \to \operatorname{coker} b \to \operatorname{coker} c$. Un *complejo de cadena* $C^\bullet$ es una secuencia de morfismos $\cdots \to C^{n+1} \xrightarrow{d_{n+1}} C^n \xrightarrow{d_n} \cdots \to C^1 \xrightarrow{d_1} C^0 \to 0$ tales que $d_n d_{n+1} = 0$. Un morfismo f de complejos $C^\bullet$ y $D^\bullet$ son morfismos $f_n : C_n \to D_n$ con $d_n f_n = f_{n-1} d_n$. Definimos el funtor *homología* con $H(C^\bullet)$ el complejo con $H_n(C) = \ker d_n / \operatorname{im} d_{n+1}$ y los d_n inducidos, y $H(f) : H(C^\bullet) \to H(D^\bullet)$ inducido. Si $0 \to A^\bullet \to B^\bullet \to C^\bullet \to 0$ es exacta, por el lema de la serpiente induce una secuencia exacta

$$\cdots \to H_n(A) \to H_n(B) \to H_n(C) \xrightarrow{\partial} H_{n-1}(A) \to H_{n-1}(B) \to H_{n-1}(C) \to \cdots \to 0.$$

Extensiones de cuerpos Sea k un cuerpo; si K es otro cuerpo y $k \subset K$ se dice que K es una *extensión* de k y se nota K/k; se define un morfismo de extensiones $K/k \to L/k$ como un morfismo de cuerpos $K \to L$ que fija k; se define el *grado* de K/k como $[K : k]$, la dimensión de K como k-e.v.; si $L/K, K/k$ son extensiones, $[L : k] = [L : K][K : k]$; la extensión se dice *(in)finita* si $[K : k]$ es; si $S \subset K$, $k(S)$ es el subcuerpo minimal de K que contiene a $k \cup S$; $a \in K$ se dice *algebraico* sii $[k(a) : k] < \infty$ sii hay $f \in k[X]$ con $f(a) = 0$, *trascendente* si no; si a es algebraico hay un polinomio $m_{\alpha,K} \in k[x]$ mónico irreducible único de grado mínimo, el *minimal* de a, que tiene a a como raíz; K/k se dice algebraica si todo elemento es algebraico; finita implica algebraica; si L/K y K/k son extensiones algebraicas L/k también es (si $a \in L$, B los coef de $m_{a,K}$, $k(a, B)/k(B)$ finita luego $k(a, B)/k$ finita y a es algebraico); el conjunto $\{a \in K \mid a \text{ es algebraico}\}$ es una extensión de k porque $a + b, ab, a^{-1} \in k(a, b)$ que es finita; si K/k está generada por un elemento a, se dice *simple* y a se dice *elemento primitivo*.

Cuerpo de descomposición y clausura algebraica. Si $f \in k[x]$ es irreducible, $K = k[x]/(f)$ es un cuerpo, extensión de k, y $\alpha = \pi(x)$ es una raíz de f; $\{1, \alpha, \dots, \alpha^{\deg f - 1}\}$ es una base de K así que $[K : k] = \deg f$. Dado un morfismo $\sigma : k \to l$ hay tantas maneras de extenderlo a $\overline{\sigma} : k(\alpha) \to l$ como raíces de $\sigma(m_{\alpha,k})$ en l. Si $\{f_\alpha\}_{\alpha\in\omega} \subset k[x]$, ω ordinal, un *cuerpo de descomposición* de $\{f_\alpha\}$ es una extensión minimal K/k donde los f_α se factorizan linealmente; existe: vamos agregando inductivamente raíces de irreducibles; unicidad salvo isomorfismo: vamos construyendo inductivamente un isomorfismo a medida que se agregan raíces. Decimos que k es *algebraicamente cerrado* si todo polinomio no cte tiene una raíz; una extensión $\overline{k}/k$ se dice *clausura algebraica* si es algebraica y $\overline{k}$ es alg cerrado; $\overline{k}$ es un cdd de $k[x]$: si f irreducible en $\overline{k}[x]$, extendemos a $\overline{k}(\alpha)$, $k(\alpha)/k$ alg y α raíz de pol de $k[x]$, luego $\alpha \in \overline{k}$; entonces existe y es única salvo isomorfismo.

Cuerpos finitos[1]. Si $K/\mathbb{F}_p$ es finita tiene p^n elementos que son las raíces de $x^{p^n} - x$ así que es su cuerpo de desc. y por lo tanto es único salvo isomorfismo; se lo nota $\mathbb{F}_{p^n}$; notar que existe porque el conjunto de raíces de $x^{p^n} - x$ en un cuerpo de descomposición es un cuerpo de p^n elementos; se deduce que $\mathbb{F}_{p^a} \subset \mathbb{F}_{p^b}$ sii $a \mid b$, $\mathbb{F}_{p^a} \cap \mathbb{F}_{p^b} = \mathbb{F}_{p^{(a,b)}}$, $\mathbb{F}_{p^n}\mathbb{F}_{p^m} = \mathbb{F}_{p^{[n,m]}}$ y $\overline{\mathbb{F}_p} = \bigcup_{n\geqq 1} \mathbb{F}_{p^n}$ en el sentido de $\mathbb{F}_{p^n} = \{\alpha \in \overline{\mathbb{F}_p} \mid \alpha^{p^n} = \alpha\}$; se ve que $x^{p^n} - x$ es el producto de los $f \in \mathbb{F}_p[x]$ irr con $\deg f \mid n$; $\operatorname{Aut}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \{\sigma^k \mid 0 \leqq k < n\} \cong \mathbb{Z}_n$, donde $\sigma : x \mapsto x^p$ es el *automorfismo de Frobenius.*

Extensiones separables. Dada K/k algebraica defino el *grado de separabilidad* de K/k como $[K : k]_s = |\operatorname{Hom}(K/k, \overline{k}/k)|$; vale $[K : k]_s \leqq [K : k]$ y $[E : k]_s = [E : K]_s[K : k]_s$. Un elemento

[1] Sea a_n la cantidad de polinomios mónicos de grado n en $\mathbb{Z}_p[x]$ y b_n la cantidad de irreducibles entre ellos; tenemos $a_n = p^n$ y la identidad $\frac{1}{1-pz} = \sum_{n\geqq 0} a_n z^n = \prod_{n\geqq 1}(1 + z^n + z^{2n} + \cdots)^{-b_n} = \prod_{n\geqq 1} \frac{1}{(1-z^n)^{b_n}}$; cambiando $f = g$ por $f'/f = g'/g$ obtenemos $\frac{p}{1-pz} = \sum_{n\geqq 1} \frac{b_n n z^{n-1}}{1-z^n} = \sum_{m\geqq 1} \left(\sum_{n\mid m} b_n n\right) z^{m-1}$ y $p^m = \sum_{n\mid m} b_n n$, de lo que $b_n = \frac{1}{n} \sum_{d\mid n} \mu(\frac{n}{d}) p^d = \frac{p^n}{n} + O(p^{n/2})$.

de $\alpha \in K/k$ se dice *separable* si $m_{\alpha,k}$ no tiene raíces múltiples (en un cdd) sii $\operatorname{mcd}(f, f') = 1$ sii $\operatorname{car} k = 0$ o $\operatorname{car} k = p$, $f = g(X^p)$ sii $[k(\alpha) : k]_s = [k(\alpha) : k]$. Una extensión alg K/k se dice *separable* si todo $\alpha \in K$ es separable sii todos los generadores son; y en el caso finito sii $[K : k]_s = [K : k]$. Defino K_s, la *clausura separable* de K/k, como $\{x \in K \mid x \text{ separable}\}$; K_s/k es extensión y vale $[K_s : k] = [K : k]_s$. Defino el *grado de inseparabilidad* de K/k como $[K : k]_i$ dado por $[K : k] = [K : k]_s[K : k]_i$. Digo que K/k es *puramente inseparable* si los únicos elementos separables son los de k, sii para todo $x \in K$ hay $n \in \mathbb{N}$ con $x^{p^n} \in k$, sii $[K : k]_s = 1$, sii $[K : k]_i = [K : k]$; K/K_s es. Dado $\alpha \in K$, hay g irreducible separable con $m_{\alpha,k} = g(X^{p^n})$ y $k(\alpha)_s = k(\alpha^{p^n})$, $[k(\alpha) : k]_s = \deg g$, $[k(\alpha) : k]_i = p^n$. Digo que k es *perfecto* si toda extension es separable; sii $\operatorname{car} k = 0$ o $\operatorname{car} k = p$ y el Frobenius es epi; en particular cuerpos finitos.

Elemento primitivo. Si K/k es finita y hay finitos intermedios $K/L/k$ o $K = k(\alpha_1, \alpha_2, \ldots, \alpha_n)$ con $\alpha_2, \ldots, \alpha_n$ separables entonces $K = k(\alpha)$: si k es finito es obvio porque todas las extensiones finitas son simples; si k es infinito y hay finitos subcuerpos, hay $c \neq c'$ con $k(\alpha + c\beta) = k(\alpha + c'\beta)$ y $(c - c')\beta \in k(\alpha + c\beta)$, α, β están y $K = k(\alpha + c\beta)$; sean f, g los minimales de α, β y α_i, β_j las raíces; encontramos c tal que $\alpha_i + c\beta_j \neq \alpha + c\beta$ salvo que $i = j = 1$; ponemos $\gamma = \alpha + c\beta$ y $g(X), f(\gamma - cX)$ tienen coef en $k(\gamma)$ y tienen a β como raíz común, pero sólo a β; luego su mcd es $X - \beta$ así que $\beta \in k(\gamma)$ y listo; recíprocamente hay sólo finitas subextensiones de $k(\alpha)/k$ algebraica: si L es, viendo grados se ve que L es el generado por los coef de $m_{\alpha,k(\alpha)/L}$ que como $m_{\alpha,k(\alpha)/L} \mid m_{\alpha,k(\alpha)/k}$ hay finitos. Ej de no simple: en $k(x, y)/k(x^p, y^p)$ con car $k = p$ y k infinito, $k(x + cy)$ tienen grado p así que son todos distintos e infinitos, porque si dos son iguales serían $k(x, y)$ que tiene grado p^2.

Extensiones normales y de Galois. Digo que K/k algebraica es *normal* si para todo $\alpha \in K$, $m_{\alpha,k}$ se factoriza linealmente en K, sii eso pasa para generadores, sii es el cdd de un conjunto $\{f_i\}$ de polinomios de $k[X]$, sii $\operatorname{Hom}(K/k, \overline{k}/k) = \operatorname{Aut}(K/k)$. La *clausura normal* de K/k es una extensión E/K normal minimal: el cdd de los minimales de los generadores; finita si K/k es; única salvo iso. Digo que K/k es *galoisiana* si es normal y separable; si es finita sii $[K : k] = |\operatorname{Aut}(K/k)|$; llamamos $\operatorname{Gal}(K/k) = \operatorname{Aut}(K/k)$ al *grupo de Galois*. (Artin) Si G es un grupo finito de automorfismos de K/k entonces $[K : K^G] \leqq |G|$ (pruebo que si $\alpha \in K$, $\deg m_{\alpha,k} \leqq |G|$ separable: sea $\{\sigma_1, \ldots, \sigma_n\} \in G$ maximal con $\sigma_1\alpha, \ldots, \sigma_n\alpha$ distintos, y $f = \prod_{i=1}^n (X - \sigma_i\alpha)$; vale $f(\alpha) = 0$ y $f \in K^G[X]$, porque si $\tau \in G$, $\tau f = \prod_{i=1}^n (X - \tau\sigma_i\alpha) = f$, porque τ es inyectivo y si $\tau\sigma_i\alpha \notin Z(f)$, agrego $\tau\sigma_i$; sea $\alpha \in K$ con $[K^G(\alpha) : K^G] \leqq |G|$ máximo; si $\beta \in K$, $K^G(\alpha, \beta)$ es separable finita, luego por primitivo $K^G(\alpha, \beta) = K^G(\gamma)$, y por maximalidad de α, $K^G(\gamma) = K^G(\alpha)$, y $K^G(\alpha) = K$). Corolario: si G es un grupo finito de automorfismos de K/k, $G = \operatorname{Aut}(K/K^G)$: $[K : K^G] \leqq |G| \leqq |\operatorname{Aut}(K/K^G)| \leqq [K : K^G]$. Entonces K/k finita es galoisiana sii $k = K^{\operatorname{Aut}(K/k)}$. Si K/k es galoisiana, $\alpha \in K$, los $\sigma\alpha$ para $\sigma \in \operatorname{Gal}(K/k)$ se dicen *conjugados* de α y recorren las raíces de $m_{\alpha,k}$. Si K/k es separable la clausura normal se llama la *clausura de Galois* de K/k. Una extensión K/k se dice *cíclica, abeliana, soluble* si es galoisiana con grupo de Galois cíclico, abeliano, soluble.

Teorema de Galois. Sea K/k una extensión galoisiana finita y sea $G = \operatorname{Gal}(K/k)$; hay una biyección entre las subextensiones $K \supset L \supset k$ y los subgrupos $1 \leq H \leq G$ dada por $L \mapsto \operatorname{Gal}(K/L)$ y $H \mapsto K^H$ tal que: invierte inclusiones: $H_1 \leq H_2$ sii $K^{H_1} \supset K^{H_2}$; dualidad: $K^{H_1}K^{H_2} \leftrightarrow H_1 \cap H_2$ y $K^{H_1} \cap K^{H_2} \leftrightarrow \langle H_1 \cup H_2 \rangle$; los índices son los grados: $(H_1 : H_2) = [K^{H_2} : K^{H_1}]$; $\sigma H \sigma^{-1} \leftrightarrow \sigma M$ o sea $K^{\sigma H \sigma^{-1}} = \sigma(K^H)$ y $\operatorname{Gal}(K/\sigma L) = \sigma \operatorname{Gal}(K/L)\sigma^{-1}$; H es normal en G sii K^H/k es normal (luego Galois), en cuyo caso $\operatorname{Gal}(K^H/k) \cong G/H$. Biyección: $H = \operatorname{Gal}(K/K^H)$ y como K/L es Galois $K^{\operatorname{Gal}(K/L)} = L$. Inclusiones: $H_1 \geq H_2 \Rightarrow K^{H_1} \subset K^{H_2} \Rightarrow \operatorname{Gal}(K/K^{H_1}) \geq \operatorname{Gal}(K/K^{H_2})$ trivialmente; lo último es $H_1 \geq H_2$. Dualidad: $K^{H_1}K^{H_2}$ es el menor que los incluye así que es mayor contenido en H_1, H_2; igual lo otro. Índices: teníamos $[K : K^H] = (\operatorname{Gal}(K/K^H) : 1)$ así que usando $(H_1 : 1) = (H_1 : H_2)(H_2 : 1)$ y $[K : K^{H_1}] = [K : K^{H_2}][K^{H_2} : K^{H_1}]$ sale. Conjugación: $\tau\alpha = \alpha$ sii $(\sigma\tau\sigma^{-1})(\sigma\alpha) = \sigma\alpha$ da $\operatorname{Gal}(K/\sigma L) = \sigma\operatorname{Gal}(K/L)\sigma^{-1}$ y $\sigma\operatorname{Gal}(K/L)\sigma^{-1} \leftrightarrow \sigma L$. Normal: si $H \triangleleft G$ como $\sigma H \sigma^{-1} = H$

tenemos $\sigma(K^H) = K^H$ así que podemos definir un morfismo $\phi : G \to \mathrm{Aut}(K^H/k)$ dado por $\sigma \mapsto \sigma|_{K^H}$; es epi con núcleo H así que $G/H \cong \mathrm{Aut}(K^H/k)$; ahora $(K^H)^{\phi(G)} = k$ así que K^H/k es Galois y $G/H \cong \mathrm{Aut}(K^H/k)$; recíprocamente, si L/k es normal, $\sigma \in G$, $\alpha \in L$, $\sigma\alpha$ es raíz del minimal así que está en L, $\sigma L = L$ y $\sigma H \sigma^{-1} = H$. Si K, L son extensiones de k, K/k Galois, entonces KL/L y $K/K \cap L$ son Galois y $\sigma \mapsto \sigma|_K$ es un isomorfismo $\mathrm{Gal}(KL/L) \cong \mathrm{Gal}(K/K \cap L)$: si K es el cuerpo de desc de $f \in k[x]$, KL es el cpo de desc de f sobre L; corolario: $[KL : k] = \frac{[K:k][L:k]}{[K \cap L:k]}$; si L/k es Galois, KL/k y $K \cap L/k$ son Galois y $\sigma \mapsto (\sigma|_K, \sigma|_L)$ es un iso $\mathrm{Gal}(KL/k) \cong \{(\sigma_1, \sigma_2) \in \mathrm{Gal}(K/k) \times \mathrm{Gal}(L/k) \mid \sigma_1|_{K\cap L} = \sigma_2|_{K \cap L}\}$. Si $H \leq G$ y $L = K^H$ el máximo subgrupo maximal en H es $N = \bigcap_{\sigma \in G} \sigma H \sigma^{-1}$ así que K^N, la composición de los cuerpos σM es la clausura de Galois.

Grupo de Galois de un polinomio. Sea $f \in k[x]$ es separable, k_f su cpo de desc, $G_f = \mathrm{Gal}(k_f/k)$, el *grupo de Galois* de f; $f = \prod_{i=1}^n (X - \alpha_i)$ en k_f; los elementos de G_f permutan las raíces y están determinados por esa permutación; G_f se puede ver como el conjunto de las permutaciones σ tales que para todo $P \in k[x_1, \ldots, x_n]$, $P(\alpha_1, \ldots, \alpha_n) = 0 \Rightarrow P(\sigma\alpha_1, \ldots, \sigma\alpha_n) = 0$. El polinomio $X^n - s_1X^{n-1} + s_2X^{n-2} + \cdots + (-1)^n s_n$ sobre $k(s_1, \ldots, s_n)$ (cuerpo de cocientes del anillo de polinomios $k[s_1, \ldots, s_n]$) tiene grupo de Galois S_n: hay un isomorfismo entre el cpo de desc y $k(x_1, \ldots, x_n)$ que manda la raíz α_i a x_i ya que si $p \in k[x_1, \ldots, x_n]$ y $p(\alpha_1, \ldots, \alpha_n) = 0$, multiplicamos por $p(\alpha_{\pi_1}, \ldots, \alpha_{\pi_n})$, obtenemos cero de nuevo pero esta vez el polinomio es sobre s_i y es cero; ahora toda permutación es obviamente automorfismo. Llamamos $D = \prod_{i<j} (\alpha_i - \alpha_j)^2$, con α_i las raíces de $f \in k[x]$, el *discriminante* de f; $\Delta = \sum_{i<j} (\alpha_i - \alpha_j) = \sqrt{D}$ queda fijo por σ sii $\sigma \in A_n$; entonces $G_f \subset A_n$ sii D es cuadrado (asumiendo $D \neq 0$). Teorema fundamental del álgebra: $\mathbb{C}$ es alg cerrado porque si $f \in \mathbb{C}[x]$, $\mathbb{C}_f$ es de Galois, $\mathbb{R}(i, f)$ también; el 2-Sylow de $\mathrm{Gal}(\mathbb{R}(i, f)/\mathbb{R})$ da una subextensión impar que es imposible así que es un 2-grupo, $\mathrm{Gal}(\mathbb{C}_f/\mathbb{C})$ también, luego tiene un subgrupo de índice 2 (por ser p-grupo) pero $\mathbb{C}$ no tiene extensiones cuadráticas. Si p es primo, S_p está generado por $\tau = (1\,2)$ y σ un p-ciclo: una potencia de σ lo escribe como $(1\,2\,\ldots)$ que renombrando es $(1\,2\,3\,\ldots\,p)$; ahora $(i\; i+1) = \sigma^i (1\,2) \sigma^{-i}$ generan. Si $f \in \mathbb{Q}[x]$ irreducible de grado p tiene exactamente dos raíces complejas, $G_f = S_p$: por Cauchy tiene un elemento de orden p que es un p-ciclo; conjugación compleja es una trasposición; juntos generan S_p. El polinomio $(x^2 + m)(x - n_1) \ldots (x - n_{p-2}) - \frac{2}{n}$ es irreducible por 2-Eisenstein si m, n_i son pares y si n es grande tiene dos raíces complejas, así que su Galois es S_p.

Extensiones ciclotómicas. Una *n-raíz primitiva de 1* es un $\zeta_n \in \overline{k}$ de orden n en $\overline{k}^\times$; existe sii $\operatorname{car} k \nmid n$; $k(\zeta_n)$ se llama *extensión ciclotómica*, es el cdd de $X^n - 1$. En $\mathbb{Q}$ defino el *polinomio ciclotómico* $\Phi_n = \prod_{\substack{0 \leqq k < n \\ (n,k)=1}} (X - \zeta_n^k)$, $X^n - 1 = \prod_{d \mid n} \Phi_d$ y $\Phi_n \in \mathbb{Z}[X]$; vale $\Phi_n = m_{\zeta_n, \mathbb{Q}}$, es decir, Φ_n irreducible (si $\Phi_n = fg$, $fg \in \mathbb{Z}[X]$, hay que mostrar que si $f(\zeta) = 0$, $f(\zeta^p) = 0$ para todo primo p con $p \nmid n$; si no $f(X)$ y $g(X^p)$ tienen raíz común y factor común; proyecto a $\mathbb{F}_p$ y $\overline{f}(X)$ y $\overline{g}(X^p) = \overline{g}(X)^p$ tienen factor común, pero $X^n - 1 = \overline{f}(X)\overline{g}(X)$ es separable); entonces $[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \phi(n)$. Si $p \nmid n$, $[\mathbb{F}_{p^r}(\zeta_n) : \mathbb{F}_{p^r}] = m$ el menor tal que $n \mid p^{rm} - 1$.

Independencia de caracteres y base normal. (Dedekind) Si k es un cuerpo, G monoide y $\{\chi_1, \ldots, \chi_m\}$ son morfismos $G \to k^\times$ entonces son li sobre k, es decir, si $\sum_{i=1}^m a_i \chi_i = 0$ con $a_i \in k$ entonces $a_i = 0$: $\sum a_i \chi_i = 0$ implica $\sum a_i \chi_i(g) \chi_i = 0$ y $\sum a_i \chi_j(g) \chi_i = 0$ así que $\sum a_i (\chi_i(g) - \chi_j(g)) \chi_i = 0$, lo que da una combinación con más ceros. Una *base normal* de K/k galoisiana finita es una base $\{\sigma\alpha \mid \sigma \in \mathrm{Gal}(K/k)\}$; siempre existe (sean $\{\sigma_i\} = \mathrm{Gal}(K/k)$; pongo $f(x) = \det(\sigma_i \sigma_j(x))$; sea $\{\alpha_i\}$ base de K/k; $f(\sum_{i=1}^n a_i \alpha_i)$ es un polinomio $g(a_1, \ldots, a_n)$ si $a_i \in k$; ahora como los σ_i son independientes, los $e_i = (\sigma_i(\alpha_1), \ldots, \sigma_i(\alpha_n))$ son indeptes en K^n, y hay $a_1, \ldots, a_n \in K$ con $\sum_{k=1}^n a_k \sigma_i \alpha_k = \begin{cases} 1, \text{ si } i=1 \\ 0, \text{ si no} \end{cases}$, luego $\sum_{k=1}^n a_k \sigma_i \sigma_j \alpha_i = \begin{cases} 1, \text{ si } \sigma_i\sigma_j = \sigma_1 \\ 0, \text{ si no} \end{cases}$; luego $g(a_1, \ldots, a_n) = 1$ y $g \neq 0$; si k es infinito hay $a_1, \ldots, a_n \in k$ con $g(a_1, \ldots, a_n) \neq 0$, y $f(\sum_{i=1}^n a_i \alpha_i) \neq 0$, listo; si k es finito, K/k es cíclica, y $\mathrm{Gal}(K/k)$ está generado por σ; por Dedekind, $1, \sigma, \ldots, \sigma^{n-1}$ son li, luego el minimal de σ es $x^n - 1$ y hay α con $\{\sigma^i \alpha \mid 0 \leqq i < n\}$

li).

Norma y traza. Sea K/k finita. Dado $\alpha \in K$ sea $G = \mathrm{Hom}(K/k, \overline{k}/k)$; defino la *traza* $\mathrm{Tr}_k^K(\alpha) = [K:k]_i \sum_{\sigma\in G} \sigma\alpha$ y la *norma* $N_k^K(\alpha) = (\prod_{\sigma\in G}\sigma\alpha)^{[K:k]_i}$; vale $\mathrm{Tr}_k^K, N_k^K : K \to k$, Tr es k-lineal y $N_k^K : K^\times \to k^\times$ es morfismo. Si $E/K/k$ vale $\mathrm{Tr}_k^E = \mathrm{Tr}_k^K \circ \mathrm{Tr}_K^E$ y $N_k^E = N_k^K \circ N_K^E$. Si $K = k(\alpha)$ y $m_{\alpha,k} = X^n + a_{n-1}X^{n-1} + \cdots + a_0$ entonces $\mathrm{Tr}_k^K(\alpha) = -a_{n-1}$ y $N_k^K(\alpha) = (-1)^n a_0$. Defino $m_\alpha(x) = \alpha x$ endormorfismo k-lineal; vale $\mathrm{Tr}_k^K(\alpha) = \mathrm{Tr}\, m_\alpha$ y $N_k^K(\alpha) = \det m_\alpha$.

Extensiones cíclicas y resolubles. (Hilbert 90) Sea K/k una extensión cíclica, con $G = \langle\sigma\rangle$, $|G| = n$. Si $\beta \in K$ con $N_k^K(\beta) = 1$, hay $\alpha \in K$ con $\beta = \frac{\alpha}{\sigma\alpha}$ (por Dedekind $f = \mathrm{id} + \beta\sigma + \beta\sigma\beta\sigma^2 + \cdots + \beta\sigma\beta\ldots\sigma^{n-1}\beta\sigma^{n-1}$ no es siempre 0, luego $\alpha = f(\theta) \neq 0$ cumple). Si $\beta \in K$ con $\mathrm{Tr}_k^K(\beta) = 0$, hay $\alpha \in K$ con $\beta = \alpha - \sigma\alpha$ (por Dedekind hay θ con $\mathrm{Tr}_k^K(\theta) \neq 0$, luego $\alpha = \frac{1}{\mathrm{Tr}_k^K(\theta)}(\beta\sigma\theta + (\beta+\sigma\beta)\sigma^2\theta + \cdots + (\beta+\sigma\beta+\cdots+\sigma^{n-2}\beta)\sigma^{n-1}\theta)$ cumple). Si $p = \mathrm{car}\, k$, $p \nmid n$ y hay n-raíz primitiva de 1 $\zeta \in k$, hay $\alpha \in K$ con $K = k(\alpha)$ y $\alpha^n \in k$ ($N(\zeta^{-1}) = (\zeta^{-1})^n = 1$, luego hay $\alpha \in K$ con $\sigma\alpha = \zeta\alpha$, $\sigma^i\alpha$ son distintos ($0 \leqq i < n$) luego $[k(\alpha):k] = n$, $K = k(\alpha)$ y $\alpha^n \in k$). (Artin-Schreier) Si $n = \mathrm{car}\, k$, hay $\alpha \in K$ con $K = k(\alpha)$ y $\alpha^p - \alpha \in k$ ($\mathrm{Tr}(-1) = 0$ da $\alpha \in K$ con $\sigma\alpha = \alpha + 1$, luego $\sigma^i\alpha$ son distintos ($0 \leqq i < n$) y $[k(\alpha):k] = p$, $K = k(\alpha)$ y $\alpha^p - \alpha \in k$). Una extensión finita separable K/k se dice *soluble* si su clausura galoisiana F/k tiene $\mathrm{Gal}(F/k)$ soluble; se dice *resoluble (por radicales)* si hay una cadena $k = K_1 \subset K_2 \subset \cdots \subset K_m = K$ con $K_{i+1} = K_i[\alpha]$, con α n-raíz primitiva de 1, $\alpha^n \in K_i$ ($\mathrm{car}\, k \nmid n$) o $\alpha^p - \alpha \in K_i$ ($p = \mathrm{car}\, k$); son equivalentes.

Extensiones abelianas de exponente m. Si K/k abeliana finita con $\sigma \in G \Rightarrow \sigma^m = 1$, y k con una m-raíz primitiva de 1, $G = G_1 \oplus \cdots \oplus G_t$ con $G_i = \langle\sigma_i\rangle$ con $|\sigma_i| = m_i$; llamo $\mathrm{X} = \mathrm{Hom}(G, k^\times)$; definimos $\chi_i \in \mathrm{X}$ por $\chi_i(\sigma_i) = \epsilon_i$ con ϵ_i una m_i-raíz y $\chi_i(\sigma_j) = 1$ si $i \neq j$; esto define un isomorfismo $G \to \mathrm{X}$. Sea $B = K^m \cap k^\times$; $K = k(B^{1/m})$; hay un morfismo $B \to \mathrm{X}$ dado por $b \mapsto (\sigma \mapsto \frac{\alpha}{\sigma\alpha})$ con $\alpha^m = b$; el núcleo es $k^{\times m}$; es suryectiva, porque si $\chi \in \mathrm{X}$, hay $\alpha = \sum_{\sigma\in G}\chi(\sigma)\sigma(\theta) \neq 0$, luego $\chi(\sigma) = \frac{\alpha}{\sigma\alpha}$ y $\alpha^m \in k^{\times m}$. Entonces $G \cong \mathrm{X} \cong B/k^{\times m}$. La función $B \mapsto k(B^{1/m})$ es una biyección entre subgrupos de $k^\times$ que contienen a $k^{\times m}$ con índice finito y extensiones abelianas finitas de k de exponente m (inyectiva: si $k(B_1^{1/m}) = k(B_2^{1/m})$, sea $b \in B_1$; tengo $(B_2\langle b\rangle : B_2) = \frac{(B_2\langle b\rangle : k^{\times m})}{(B_2 : k^{\times m})} = \frac{[k(B_2^{1/m}, b^{1/m}):k]}{[k(B_2^{1/m}):k]} = 1$ y $b \in B_2$).

Bases de trascendencia. Dado K/k, decimos que $S \subset K$ es *algebraicamente independiente* si dado $\sum_{J\subset S \text{ finito}} a_J \prod_{x\in J} x = 0$ con $a_J \in k$ y $a_J = 0$ salvo finitos vale $a_J = 0$ para todo J. Una *base de trascendencia* es un conjunto S alg indep maximal (existen por Zorn); $K/k(S)$ es algebraico. Si S es una base finita, toda base es finita y del mismo cardinal: si $\{x_1, \ldots, x_n\}$ es base y $\{w_1, \ldots, w_m\}$ es parte de otra, W, con $n \leqq m$, tenemos $f(w_1, x_1, \ldots, x_n) = 0$, luego hay un x_1 (renombrando) con $x_1 \in k(w_1, x_2, \ldots, x_n)$; siguendo resulta que K es algebraica sobre $k(w_1, \ldots, w_n)$ por lo que $|W| = |S|$.

Geometría algebraica Sea k un cuerpo. Un *conjunto algebraico* es un conjunto $S = V(I) = \{x \in k^n \mid \forall f \in I. f(x) = 0\}$, donde I es un ideal de $k[x_1, \ldots, x_n]$; intersección arbitraria de algebraicos es algebraico y $V(I) \cup V(J) = V(IJ)$. Defino el ideal $\mathcal{I}(S) = \{f \in k[x_1, \ldots, x_n] \mid \forall x \in S. f(x) = 0\}$. (Zariski) Si K/k es extensión de cuerpos con $K = k[v_1, \ldots, v_n]$ entonces K/k es algebraica (inducción en n; $n = 1$ es obvio; supongamos que $k(v_1)/k$ no es algebraico; $K/k(v_1)$ es alg por inducción, luego hay $a \in k[v_1]$, $a \neq 0$, con av_i integral sobre $k[v_1]$ ($1 \leqq i \leqq n$); sea $c \in k[v_1]$ con $(c, a) = 1$; hay N con $a^N c^{-1}$ integral; luego $a^N c^{-1} \in k[v_1]$, absurdo). (Nullstellensatz débil) Si k es alg cerrado y I es un ideal con $V(I) = \varnothing$ entonces $1 \in I$ (tomamos I maximal; $K = k[x_1, \ldots, x_n]/I$ es un cuerpo; por lo anterior K/k es algebraico, luego $K = k$, $u_i = p_I(x_i) \in k$, $(x_i - u_i) = I$ y $(u_1, \ldots, u_n) \in I$, absurdo). (Nullstellensatz) Si k alg cerrado, $\mathcal{I}(V(I)) = \sqrt{I}$ (sea $I = (f_1, \ldots, f_n)$ y $g \in \mathcal{I}(V(I))$; pongo $J = (f_1, \ldots, f_n, x_{n+1}g - 1)$; $V(J) = \varnothing$, luego $1 = \sum_{i=1}^n a_i(x_1, \ldots, x_{n+1})f_i + b(x_{n+1}g - 1)$; pongo $x_{n+1} = \frac{1}{g}$, multiplico por g^n y obtengo $g^n \in I$, listo). Hay pues una biyección entre ideales radicales de $k[x_1, \ldots, x_n]$ y conjuntos algebraicos que invierte inclusiones; hay también una biyección entre ideales maximales y puntos.

Componentes irreducibles. Un conjunto algebraico $V \subset k^n$ se dice *irreducible* si no hay conj alg V_1, V_2 distintos de V con $V = V_1 \cup V_2$, sii $\mathcal{I}(V)$ es primo (si no es primo, $fg \in I$ pero $f, g \notin I$, luego $V = (V(f) \cap V) \cup (V(g) \cap V)$; si V es reducible, como $V_i \neq V$, hay $f_i \in \mathcal{I}(V_i)$ con $f_i \notin \mathcal{I}(V)$, pero $f_1 f_2 \in \mathcal{I}(V)$). Si V es algebraico se descompone como unión finita de irreducibles $\bigcup_{i=1}^n V_i$ con $V_i \not\subset V_j$ de manera única (el conjunto de los $\mathcal{I}(V)$ donde V no se descompone así tiene un maximal $\mathcal{I}(V)$ porque $k[x_1, \ldots, x_n]$ es noetheriano; luego V no es irreducible, $V = V_1 \cup V_2$, $V_1, V_2 \neq V$, absurdo; si $\bigcup_{i=1}^n V_i = \bigcup_{i=1}^m W_i$, $V_j = \bigcup_{i=1}^m (V_j \cap W_i)$, $V_j \subset W_i$, además $W_i \subset V_k$ y $V_j = W_i$). Si $f = f_1^{r_1} \ldots f_m^{r_m}$ es la descomposición en irreducibles de $f \in k[x_1, \ldots, x_n]$ entonces $V(f) = \bigcup_{i=1}^m V(f_i)$ es la desc en irreducibles y $\mathcal{I}(V(f)) = (f_1 \ldots f_m)$. En k^2 los conjuntos algebraicos irreducibles son $\varnothing$, k^2, puntos y $V(f)$ con $f \in k[x,y]$ irreducible (si $f, g \in \mathcal{I}(V)$ son irreducibles y distintos, en $k(x)[y]$ son irreducibles y coprimos, luego hay $a, b, c \in k[x]$ con $af + bg = c$, luego x puede tomar finitos valores; igualmente y y V es finito, o sea un punto o $\varnothing$; si $\mathcal{I}(V) \neq \varnothing$ hay f irreducible y $\mathcal{I}(V) = (f)$; si $\mathcal{I}(V) = \varnothing$, $V = k^2$).

Variedades afines. Llamamos *variedad afín* a un conjunto algebraico irreducible de k^n. Si, $V \subset k^n, W \subset k^m$ son variedades, un *morfismo* es una función $\phi(t) = (f_1(t), \ldots, f_m(t))$ con $f_i \in k[x_1, \ldots, x_n]$ tal que $\phi(V) \subset W$. El *anillo de coordenadas* de V es $\Gamma(V) = k[x_1, \ldots, x_n]/\mathcal{I}(V)$; hay una biyección entre morfismos $\phi : V \to W$ y morfismos de anillos $\tilde{\phi} : \Gamma(W) \to \Gamma(V)$ dada por $\phi \mapsto \tilde{\phi}(\overline{f}) = \overline{f \circ \phi}$ (dada $\alpha : \Gamma(W) \to \Gamma(V)$ elijo $f_i \in k[x_1, \ldots, x_n]$ con $\alpha(\overline{x_i}) = \overline{f_i}$ y $\phi(t) = (f_i(t_i))$ es morfismo con $\tilde{\phi} = \alpha$). Dada una variedad V y $p \in V$ defino el *anillo local de V en p* como la localización $\mathcal{O}_p(V)$ de $\Gamma(V)$ en el ideal maximal $m_p = \{\overline{f} \mid f(p) = 0\}$; hay una evaluación $\mathrm{ev} : \mathcal{O}_p(V) \to k$ dada por $\mathrm{ev}(\frac{f}{g}) = \frac{f(p)}{g(p)}$; el ideal maximal de $\mathcal{O}_p(V)$ es pues $\mathfrak{m}_p = \ker \mathrm{ev} = (\overline{x_1}, \ldots, \overline{x_n})$; $\mathcal{O}_p(V)$ es noetheriano; $\mathfrak{m}_p$ es principal sii $\mathcal{O}_p(V)$ es DVR. Si I es un ideal de $k[x_1, \ldots, x_n]$, k es alg cerrado, $V(I) = \{p_1, \ldots, p_m\}$ y llamo $\mathcal{O}_{p_i} = \mathcal{O}_{p_i}(k^n)$ entonces $k[x_1, \ldots, x_n]/I \cong \prod_{i=1}^m \mathcal{O}_{p_i}/I\mathcal{O}_{p_i}$ (...).