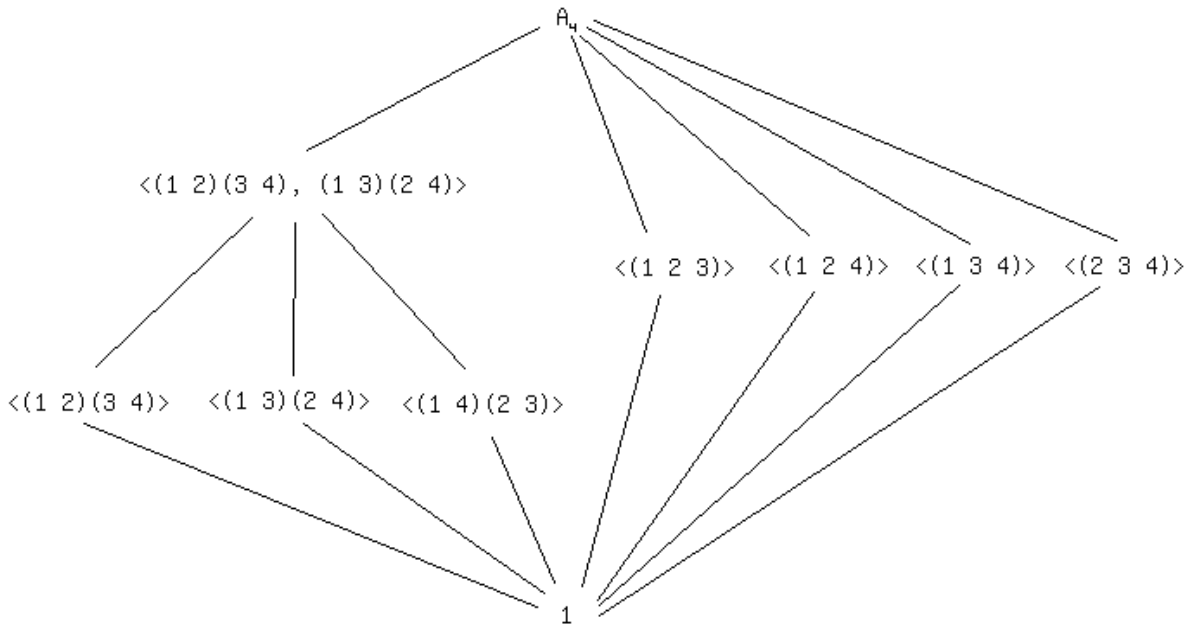
Estructuras Algebraicas

Miguel González
mgonzalez.contacto@gmail.com
miguelgg.com

Enero de 2020



Revisado en 2022
Apuntes de la asignatura impartida por Orlando Villamayor
en la Universidad Autónoma de Madrid en Enero de 2020.

Acerca de este documento

Estos apuntes son una versión revisada de los de la asignatura Estructuras Algebraicas del grado en matemáticas, tomados en Enero de 2020 por Miguel González. La asignatura fue impartida por Orlando Villamayor. A los apuntes originales se les ha añadido esta página, una imagen de portada, y breves párrafos explicativos en las zonas menos completas. Asimismo se han revisado las erratas y completado los contenidos faltantes.

Este documento es:

- Una recopilación ordenada y directa de las definiciones y resultados más importantes del tema en cuestión, al nivel de los estudios de grado.
- Una colección de demostraciones completas de dichos resultados (salvo en los casos más básicos).
- Una *guía* para revisar de manera rápida las ideas que se han adquirido previamente, o para consultar enunciados puntuales que puedan no haberse comprendido en su totalidad.

Este documento NO es:

- Un libro de texto de la asignatura.
- Una colección de ejercicios para practicar los conceptos adquiridos.
- Un listado de ejemplos para ilustrar las ideas tratadas. A pesar de ello, en ocasiones se incluyen ejemplos puntuales que puedan ser de especial interés o curiosidad, pero se intentan reducir al mínimo en virtud del primer punto de la lista anterior.

Sobre Estructuras Algebraicas

En esta asignatura se presentan y estudian dos de las principales estructuras algebraicas: los grupos y los anillos. Estas son la base de multitud de otras áreas de las matemáticas como la teoría algebraica de números, la geometría algebraica, la teoría de Galois o la teoría de representaciones.

Requisitos previos

1. Familiaridad con la notación matemática básica.
2. Aunque no son necesarios, puede ser de ayuda disponder de conocimientos de álgebra lineal.

Índice

1. Grupos

El concepto de *grupo* representa un conjunto que dispone de una operación con ciertas propiedades naturales. Una de las motivaciones para este tipo de objetos es representar las simetrías de otros objetos, que pueden *componerse* entre sí para dar lugar a nuevas simetrías.

Definición 1. Sea G no vacío. Una **operación binaria** en G es una asignación $f : G \times G \to G$.

Normalmente, en adelante, se usará la notación multiplicativa para expresar el resultado de aplicar una operación binaria: $f(g_1, g_2) \equiv g_1 g_2$.

Definición 2. El par $(G, *)$ de un conjunto y una operación en dicho conjunto es un **grupo** si se verifica:

1. $\forall g_1, g_2, g_3 \in G$, se tiene $(g_1 g_2)g_3 = g_1(g_2 g_3)$.
2. $\exists e \in G$ tal que $\forall g \in G$ se tiene $ge = eg = g$.
3. $\forall g \in G\ \exists g^{-1} \in G$ tal que $gg^{-1} = g^{-1}g = e$.

Gracias a la asociatividad, está justificado el uso de la notación con exponentes: $f(g, g) = g^2$, $f(g, f(g, g)) = g^3$, $f(g^{-1}, g^{-1}) = g^{-2}$, $g^a g^b = g^{a+b}$, etcétera. Asimismo, se convendrá la notación $g^0 = e$ para cualquier $g \in G$.

Definición 3. $(G, *)$ es un **grupo abeliano** si, además de ser un grupo, verifica que $\forall g, h \in G$, se tiene $gh = hg$.

En adelante, para referirnos de forma genérica a un grupo $(G, *)$, en ocasiones utilizaremos simplemente el símbolo de su conjunto (En este caso, G), aunque el grupo requiere de una operación.

Definición 4. El grupo G es **finito** si $|G| < \infty$. Decimos que tiene **orden** $|G|$.

En este caso, para describirlo basta con dar una tabla que indique a qué elemento se asocia cada par de elementos. Por ejemplo, el grupo $(\frac{\mathbb{Z}}{2\mathbb{Z}}, +)$, con la suma usual, podría definirse:

$+$	0	1
0	0	1
1	1	0

Otros ejemplos de grupos finitos son el multiplicativo de unidades de $\mathbb{Z}_n$, es decir, $(\mathcal{U}(\frac{\mathbb{Z}}{n\mathbb{Z}}), \cdot)$, o el grupo de biyecciones $S_n = \{f : \mathbb{N}_n \to \mathbb{N}_n | f \text{ es biyección}\}$.

Proposición 1. *Si G es un grupo, se tiene la propiedad cancelativa: $\forall g, g_1, g_2$, $g_1 g = g_2 g \implies g_1 = g_2$, así como $gg_1 = gg_2 \implies g_1 = g_2$.*

Demostración. $g_1 g = g_2 g \implies (g_1 g)g^{-1} = (g_2 g)g^{-1} \implies g_1(gg^{-1}) = g_2(gg^{-1}) \implies g_1 e = g_2 e \implies g_1 = g_2$. Análogo por la izquierda. □

Esta propiedad implica, por tanto, que la aplicación $f_g : G \to G$ tal que $f_g(h) = gh$ (o hg) es inyectiva, y, en grupos finitos, biyectiva. En cierta medida es un "desplazamiento" dentro del grupo.

Proposición 2. *El elemento neutro de un grupo es único. Asimismo, cada elemento g tiene un único opuesto.*

Demostración. Si $e, e' \in G$ y ambos verifican la propiedad de elemento neutro, entonces $ee' = e$ por ser e' neutro, pero $ee' = e'$ por serlo e, luego $e = e'$. Dado $g \in G$, si g_1 y g_2 son inversos suyos, entonces está claro que $gg_1 = gg_2$ y cancelando g se tiene el resultado. □

Definición 5. El **producto directo** de $(G, \cdot_1)$ y $(H, \cdot_2)$ es el grupo $(G \times H, \cdot)$ con $(g, h) \cdot (g_2, h_2) = (gg_2, hh_2)$.

Definición 6. Si G es un grupo, diremos que $g \in G$ tiene **orden finito** si $\exists r \in \mathbb{N}$ tal que $g^r = e$.

Con el fin de identificar todos los exponentes que anulan un elemento de orden finito, veamos el siguiente resultado:

Proposición 3. *Sea G un grupo y g un elemento de orden finito. Entonces, $\exists r \in \mathbb{N}$ tal que $g^r = e$, y además $g^N = e \iff r|N$. Este valor se conoce como **orden** del elemento g.*

Demostración. Está claro que $A_g = \{x \in \mathbb{N} : g^x = e\}$ es no vacío por definición, luego podemos tomar $r = \min A_g$. Por construcción, $g^r = e$. Ahora, si $r|N$, entonces $g^N = g^{kr} = e^k = e$. Asimismo, si $g^N = e$, y escribimos $N = rk + t$ con $0 \leq t < r$, veremos que $e = g^N = g^{rk}g^t = g^t$, y como $t < r$ y r es el menor exponente con esa propiedad, no queda otra que $t = 0$ y por tanto $r|N$. □

Obsérvese que, en este caso, el conjunto $\{g, g^2, g^3, \ldots, g^r\}$ no puede tener duplicados. Si los tuviese, digamos $g^i = g^j$ con $1 \leq i < j < r$, entonces $g^{j-i} = e$, lo cual es imposible dado que $j - i < r$.

Proposición 4. *Si el grupo G es finito, entonces $g \in G$ tiene orden finito menor o igual que $|G|$.*

Demostración. Consideremos la secuencia $g, g^2, g^3, g^4, \ldots$. Como G es finito, en algún momento encontraremos $j \in \mathbb{N}$ tal que $g^j = g^i$ para algún $i < j$, y además será $j \leq |G|+1$ al solo haber $|G|$ elementos. En ese caso, $g^{j-i} = e$, y como $j - i \leq |G|$, tiene orden finito como se quería. □

1.1. Subgrupos

Definición 7. Dado un grupo $(G, *)$, se dice que el conjunto $H \subset G$ es un **subgrupo** (denotado $H \leq G$) si verifica:

1. $\forall h_1, h_2 \in H$, $h_1 * h_2 \in H$
2. $e \in H$ (Donde e es el neutro de G)
3. $\forall h \in H$, $h^{-1} \in H$ (Donde h^{-1} es el inverso de h en G)

En ese caso, $* : H \times H \to H$ está bien definida (por 1), y como se hereda la asociativa de G, y por 2 y 3 hay neutro e inversos en H, se tiene que $(H, *)$ es grupo también.

Por ejemplo, si consideramos $GL(2)$ (Grupo multiplicativo de isomorfismos de $\mathbb{R}^2$), y consideramos $O(2)$ como el grupo de aplicaciones ortogonales de $\mathbb{R}^2$, tenemos que $O(2) \subset GL(2)$ y es subgrupo. Otro ejemplo es D_n (grupo diédrico de orden n), que son los movimientos del plano que trasladan un n-polígono centrado en el origen en sí mismo.

Proposición 5. *Si $S_1 \leq G$ y $S_2 \leq G$, entonces $S_1 \cap S_2 \leq G$.*

Demostración. Si $s, t \in S_1 \cap S_2$, entonces por hipótesis $st \in S_1$, así como $st \in S_2$, de tal modo que $st \in S_1 \cap S_2$. Asimismo, como $e \in S_1$ y $e \in S_2$, se tiene $e \in S_1 \cap S_2$. Dado $s \in S_1 \cap S_2$, como $s^{-1} \in S_1$ y $s^{-1} \in S_2$, entonces $s^{-1} \in S_1 \cap S_2$. □

De hecho, un argumento completamente análogo permite ver que **toda intersección de subgrupos de G sigue siendo subgrupo de G** sin importar de cuántos conjuntos se trate.

Proposición 6. *Si G es un grupo finito, para que $H \subset G$ sea subgrupo basta con que se cumplan las 2 primeras propiedades.*

Demostración. Como es finito, dado $h \in H$, se tiene que h tiene orden r en G, de modo que h^{r-1} es su inverso, y $h^{r-1} \in H$ por la propiedad de cierre. □

Proposición 7. *Sea $(G, *)$ un grupo y $S \subset G$. Entonces $\exists \langle S \rangle$ tal que $\langle S \rangle < G$, $S \subset \langle S \rangle$ y, si $G' < G$, entonces $\langle S \rangle < G'$. Esto se denomina el **subgrupo generado por** S*

Demostración. Si $A = \{B : S \subset BB < G\}$, entonces definimos $\langle S\rangle := \bigcap A$. Ya sabemos que es subgrupo. Ahora, como S está en todos los intersecandos, $S \subset \langle S\rangle$. Asimismo, si $S \subset G'$, entonces $G' \in A$, por lo que $\langle S\rangle \subset G'$. □

¿Cómo podemos obtener $\langle S\rangle$ de una manera más explícita? La siguiente proposición lo indica:

Proposición 8. *Si $S = \{g_1, \dots, g_r\}$, definimos $\mathcal{F} = \{g_1, \dots, g_r, g_1^{-1}, \dots, g_r^{-1}\}$. Ahora, fijado $s \in \mathbb{N}$, sea $P_s = \{a_1a_2a_3 \dots a_s : a_i \in \mathcal{F}\}$. Se tiene que $\langle S\rangle = \bigcup_{s\in\mathbb{N}} P_s$.*

Demostración. Primero veamos que es un grupo. Está claro que dados $h_1, h_2 \in \bigcup_{s\in\mathbb{N}} P_s$, se tiene que $h_1 \in P_k$ y $h_2 \in P_l$ para enteros l, k adecuados. Así, $h_1h_2 \in P_{l+k}$ por lo que $h_1h_2 \in \bigcup_{s\in\mathbb{N}} P_s$, luego es cerrado. Asimismo, $e = g_1g_1^{-1} \in P_2$ luego $e \in \bigcup_{s\in\mathbb{N}} P_s$. Finalmente, si $h \in \bigcup_{s\in\mathbb{N}} P_s$, entonces $h \in P_k$ luego $h = a_1 \dots a_k$, pero entonces $h^{-1} = a_k^{-1} \dots a_1^{-1}$, de modo que $h^{-1} \in P_k$, luego $h^{-1} \in \bigcup_{s\in\mathbb{N}} P_s$.

Está claro que contiene a S, dado que $S \subset P_1$. Finalmente deberemos ver que se trata del menor de los que contienen a S. Si G' es subgrupo tal que $S \subset G'$, entonces, fijado $s \in \mathbb{N}$, se tiene que por cierre de G', $P_s \subset G'$. De este modo, $\bigcup_{s\in\mathbb{N}} P_s \subset G'$ y hemos acabado. □

Definición 8. El grupo $(G, *)$ es **cíclico** si $G = \langle\{g\}\rangle$. Al elemento g se lo denomina **generador**.

Observación 1. Si G es de orden n, finito, y tiene un elemento de orden n, entonces es cíclico y ese elemento es su generador.

De hecho, se trata de una equivalencia:

Proposición 9. *Si G es cíclico, finito, de orden n, entonces tiene un elemento de orden n, y por tanto es de la forma $G = \{g, g^2, \dots, g^n\}$.*

Demostración. Sea g el generador de G. Supongamos que su orden es $r < n$. Entonces, $\{g, g^2, \dots, g^r\}$ son r elementos distintos de G, y aplicar g más veces no da lugar a nuevos elementos, de modo que, por la proposición 8, los elementos faltantes tienen que venir de los inversos. No obstante, $g^{-k} = g^{r-k}$, que ya lo hemos listado arriba. Esto contradice que $r < n$. □

Observación 2. Un grupo cíclico es abeliano, dado que $g^ig^j = g^{i+j} = g^jg^i$.

1.2. Clases laterales y Teorema de Lagrange

Definición 9. Dado $(G, *)$ grupo con $T < G$, se define, dado $g \in G$, la **clase lateral izquierda de** g como $gT = \{gt : t \in T\}$.

Del mismo modo pueden definirse clases laterales derechas y, aunque si el grupo no es abeliano no se da $gT = Tg$, las propiedades que veremos a continuación valen tanto para clases izquierdas como para derechas, simplemente modificando las demostraciones para que todas las operaciones se hagan por la derecha.

Las clases laterales consisten en *subgrupos desplazados* por g. A continuación veremos ciertas propiedades que nos ayudan a verlo de esta manera, y nos permiten observar como se comportan estos conjuntos.

Proposición 10. $gT = T \iff g \in T$.

Demostración. Para $\implies$, veamos que como $e \in T$, entonces $g \in gT$. Por tanto, $g \in T$. Para $\impliedby$, se tiene que si $g \in T$, entonces $gT \subset T$ por cierre de T. Asimismo, dado $t \in T$, podemos escribirlo como $g(g^{-1}t)$, y como $g^{-1}t \in T$, se tiene que $t \in gT$. □

El siguiente resultado es de gran importancia: las clases laterales **particionan** el grupo G. Es decir, el grupo G lo podemos subdividir en el subgrupo T y desplazamientos de dicho subgrupo, de forma que no se solapan y recubren todo el grupo.

Proposición 11. *La familia $\{gT\}_{g\in G}$ forma una partición de G.*

Demostración. Primero tenemos que ver que $\bigcup gT = G$, es decir que todo elemento $g \in G$ pertenece a alguna clase lateral. Está claro que $g \in gT$, al ser $e \in T$. Ahora, si $gT \cap hT \neq \emptyset$, deben coincidir (es decir, son disjuntas). En ese supuesto, tomamos $c \in gT \cap hT$, de modo que $c = gt_1 = ht_2$ para $t_1, t_2 \in T$. De esto se deduce que $h^{-1}g = t_2 t_1^{-1} \in T$. En virtud de la proposición previa, se tiene que $h^{-1}gT = T$. Como son un subgrupo, se pueden considerar las clases laterales $h(h^{-1}gT) = hT$, es decir $gT = hT$. □

Ahora veremos que estos *bloques* que particionan el subgrupo son, de hecho, del mismo tamaño:

Proposición 12. *Existe una biyección entre T y gT para $g \in G$. Es decir, $card(T) = card(gT)$.*

Demostración. Sea $f_g : T \to gT$ dada por $t \to gt$. Sabemos que es inyección por la propiedad cancelativa. Obsérvese que $\exists f_g^{-1}$, la dada por $h \to g^{-1}h$, dado que $f_g^{-1}(f_g(t)) = g^{-1}gt = t$. Como tiene inversa, se trata de una biyección. (También se puede ver dado que f_g^{-1} es inyectiva también) □

Todo esto nos da un importantísimo resultado en relación a los posibles subgrupos de un grupo finito:

Teorema 1 (Lagrange)**.** *Si $(G, *)$ es un grupo finito y $T < G$, si $|T| = r$ y $|G| = n$, se tiene que $r|n$.*

Demostración. Tomamos la partición $\{gT\}_{g\in G}$. Como a lo sumo hay n elementos en G, dicha partición consta de $k \leq n$ clases laterales, digamos $\{g_i T\}_{1\leq i\leq k}$. Ahora bien, como $\biguplus_{j=1}^{k} g_j T = G$, se tiene que $\sum_{i=1}^{k} |g_k T| = |G|$, pero como $|g_k T| = |T|$, sigue que $k|T| = |G|$, como se quería. □

Definición 10. Se define el índice de H en G como $[G : H] = |G/H| = \frac{|G|}{|H|}$ el número de clases laterales (izquierdas o derechas) de H que existen.

Algunas consecuencias interesantes se muestran a continuación.

Proposición 13. *Si G es grupo finito con $|G| = p$ primo, no tiene subgrupos propios salvo el trivial.*

Demostración. Como p es primo, si T es subgrupo, debe darse que $|T||p$, es decir, $|T| = 1$ o $|T| = p$, o lo que es lo mismo, $T = G$ o $T = \{e\}$. □

Proposición 14. *Si G es finito y $g \in G$, sabemos que $o(g) \leq |G|$. Se tiene además que $o(g)||G|$, y por tanto además $g^{|G|} = e$.*

Demostración. Vimos con anterioridad que $|\langle g\rangle| = o(g)$. Como $\langle g\rangle < G$, debe darse que $o(g)||G|$. □

Proposición 15. *Si G es grupo finito que no tiene subgrupos propios no triviales, entonces es cíclico y por tanto abeliano. En particular, los grupos de orden primo son cíclicos y abelianos.*

Demostración. Tomamos $g \in G$. El subgrupo $\langle g\rangle$ tiene orden 1 o $|G|$, por hipótesis. Si tiene orden 1, $g = e$. Para cualquier otro $g \neq e$ está claro que $\langle g\rangle = G$, por tanto. □

1.3. Homomorfismos

En esta sección estudiaremos las aplicaciones que preservan la estructura de grupo.

Definición 11. Sean $(G, *)$ y $(H, \cdot)$ grupos. Se dice que $f : G \to H$ es **homomorfismo** de G en H si $f(g_1 g_2) = f(g_1)f(g_2)$ para cualesquiera $g_1, g_2 \in G$.

Proposición 16. *Si $f : G \to H$ es homomorfismo, entonces $f(e) = e$ y $f(g)^{-1} = f(g^{-1})$ $\forall g \in G$.*

Demostración. $f(e) = f(ee) = f(e)f(e)$, luego $e = f(e)$. Asimismo, $e = f(e) = f(gg^{-1}) = f(g)f(g^{-1})$, dando la segunda igualdad. □

Proposición 17. *Si $f : G \to H$ es homomorfismo, entonces $Im(f)$ es subgrupo de H.*

Demostración. Ya vimos que $e \in Im(f)$. Asimismo, si $h \in Im(f)$, entonces $h = f(g)$, luego $h^{-1} = f(g)^{-1} = f(g^{-1})$, con lo que $h^{-1} \in Im(f)$. Asimismo, si $h_1, h_2 \in Im(f)$, entonces $h_1 = f(g_1)$ y $h_2 = f(g_2)$ luego $h_1h_2 = f(g_1)f(g_2) = f(g_1g_2) \in Im(f)$. □

Proposición 18. *Supongamos que $g \in G$ tiene orden finito. Entonces $o(f(g))|o(g)$.*

Demostración. Está claro que $e = g^{o(g)}$ luego $e = f(e) = f(g^{o(g)}) = f(g)^{o(g)}$. Sabemos entonces que $o(f(g))|o(g)$. □

Ahora veremos que los homomorfismos lo siguen siendo tras composición:

Proposición 19. *Si $f : G \to H$ y $g : H \to T$ son homomorfismos, $g \circ f : G \to T$ también lo es.*

Demostración. Dados $g_1, g_2 \in G$, se tiene $g \circ f(g_1g_2) = g(f(g_1)f(g_2)) = g(f(g_1))g(f(g_2))$. □

Observación 3. Algunos ejemplos de homomorfismos son los siguientes:

- Si G es abeliano y $d \in \mathbb{N}$, entonces $\alpha_d : G \to G$ dado por $\alpha_d(g) = g^d$ es homomorfismo, dado que $(g_1g_2)^d = (g_1)^d(g_2)^d$ al ser abeliano.
- Si $g \in G$, con G cualquier grupo, entonces $\alpha_g : G \to G$ dado por $\alpha_g(x) = gxg^{-1}$ es homomorfismo. Si es abeliano está claro que es la identidad. Además, es biyectivo, dado que con $x \to g^{-1}xg$ se invierte.

Definición 12. Si $f : G \to H$ es un homomorfismo biyectivo, se denomina **isomorfismo**. Se dice entonces que G y H son **isomorfos**.

Proposición 20. *Si $f : G \to H$ es isomorfismo, entonces $f^{-1} : H \to G$ también lo es.*

Demostración. Solo hay que ver que es homomorfismo. Si $h_1, h_2 \in H$, con $h_1 = f(g_1)$, $h_2 = f(g_2)$, entonces $f^{-1}(h_1h_2) = f^{-1}(f(g_1)f(g_2)) = f^{-1}(f(g_1g_2)) = g_1g_2 = f^{-1}(h_1)f^{-1}(h_2)$. □

Los grupos isomorfos son, a nivel de estructura, idénticos. Vamos a ver algunos resultados en relación a esto:

Proposición 21. *Si G, H son isomorfos bajo α, dado $g \in G$ de orden finito, se tiene $o(g) = o(\alpha(g))$.*

Demostración. Ya sabemos que $o(\alpha(g))|o(g)$. Asimismo, sabemos que $o(\alpha^{-1}(\alpha(g)))|o(\alpha(g))$. Por tanto son iguales. □

Proposición 22. *Si G,H, son isomorfos bajo α, se tiene que G es abeliano $\iff$ H es abeliano.*

Demostración. Si H es abeliano, entonces $\alpha(g_1g_2) = \alpha(g_1)\alpha(g_2) = \alpha(g_2)\alpha(g_1) = \alpha(g_2g_1)$, y tomando inversos $g_1g_2 = g_2g_1$. Para G basta con intercambiar G con H y α con α^{-1}. □

Está claro que los isomorfismos definen una relación de equivalencia (y por tanto partición) entre los grupos.

Proposición 23. *Se puede definir una relación de equivalencia en la que $G \sim H \iff$ G y H son isomorfos.*

Demostración. Está claro que $G \sim G$ a través de $id : G \to G$. Asimismo, $G \sim H$ implica que $f : G \to H$ isomorfismo da lugar a $f^{-1} : H \to G$ isomorfismo luego $H \sim G$. Por otro lado, si $G \sim H$ y $H \sim T$, con $f : G \to H$ y $g : H \to T$ isomorfismos, entonces $g \circ f : G \to T$ es isomorfismo y $G \sim T$. □

Observación 4. Los grupos cíclicos G y H de orden n son isomorfos. Basta con mandar el generador de G en el de H, y el resto de asociaciones vienen dadas por la compatibilidad con la operación.

A continuación definiremos el núcleo de un homomorfismo como se hacía en aplicaciones lineales:

Definición 13. Dado $f : G \to H$ homomorfismo, se define su **núcleo** $Nuc(f) = \{x \in G : f(x) = e\}$.

Proposición 24. *$Nuc(f)$ es subgrupo de G.*

Demostración. Ya sabemos que $e \in Nuc(f)$. Si $g \in Nuc(f)$, entonces $f(g) = e$ luego $f^{-1}(g) = e^{-1} = e$ pero $f^{-1}(g) = f(g^{-1})$ luego $g^{-1} \in Nuc(f)$. Si $h, g \in Nuc(f)$, entonces $f(hg) = f(h)f(g) = ee = e$ luego $hg \in Nuc(f)$. □

Proposición 25. *$f : G \to H$ homomorfismo es inyectivo $\iff$ $Nuc(f) = \{e\}$.*

Demostración. Si f es inyectivo y $g \in Nuc(f)$, entonces $f(g) = e = f(e)$ luego no queda otra que $g = e$. Por otro lado, si $Nuc(f) = \{e\}$ y $f(g) = f(h)$, entonces $f(g)f(h^{-1}) = e$ luego $f(gh^{-1}) = e$. Como el núcleo es el trivial, $gh^{-1} = e$ luego $g = h$. □

Vamos a ver ahora dos resultados que nos permiten identificar los homomorfismos entre dos grupos, así como sus imágenes:

Proposición 26. *Si $f : G \to H$ es homomorfismo y $G = \langle\{g_1, \dots, g_r\}\rangle$, se tiene que $Im(f) = \langle\{f(g_1), \dots, f(g_r)\}\rangle$.*

Demostración. Si $h \in Im(f)$ es porque $h = f(g)$ con $g \in G$ luego $g = a_1 \dots a_k$ con cada $a_i \in \{g_1, \dots, g_r, g_1^{-1}, \dots, g_r^{-1}\}$. Entonces $h = f(a_1 \dots a_k) = f(a_1) \dots f(a_k)$ y, como $f(g_i^{-1}) = f^{-1}(g_i)$, se tiene lo que se quería. □

Proposición 27. *Si, en las condiciones de la proposición anterior, se tiene además que $h : G \to F$ es homomorfismo, entonces $f = h \iff f(g_i) = h(g_i)$, $\forall i \in \{1, \dots, k\}$.*

Demostración. $\implies$ es inmediata. Para $\impliedby$, si $\mathcal{F} = \{g_1, \dots, g_r, g_1^{-1}, \dots, g_r^{-1}\}$, está claro que $f(a) = h(a)$ si $a \in \mathcal{F}$. Por tanto, si $g \in G$, como $g = a_1 \dots a_k$, se tiene que $f(g) = f(a_1) \dots f(a_k) = h(a_1) \dots h(a_k) = h(g)$. □

Definición 14. Se define $Hom(G, H)$ como el conjunto de homomorfismos entre G y H. Asimismo, $Aut(G) \subset Hom(G, G)$ es el conjunto de **automorfismos** de G, es decir isomorfismos de G en G.

Observación 5. Por las observaciones que realizamos anteriormente sobre la composición e inversión de isomorfismos, se tiene que $(Aut(G), \circ)$ es un grupo.

Una propiedad fundamental de los homomorfismos es que *preservan* la noción de subgrupo:

Proposición 28. *Si $f : G \to G'$ es un homomorfismo, entonces:*

1. *Si $H < G$, entonces $f(H) < G'$.*
2. *Si $H' < G'$, entonces $f^{-1}(H') < G$. Obsérvese además que $Nuc(f) < f^{-1}(H')$.*

Demostración. Para la primera, considérese la siguiente cadena: $H \xrightarrow{j} G \xrightarrow{f} G'$. Se tiene que j es la inclusión $j(h) = h$, que es claramente homomorfismo, por tanto esa aplicación, $f \circ j$ es homomorfismo e $Im(f \circ j) = f(H) < G'$. Por otra parte, si $g, g' \in f^{-1}(H')$, entonces $f(g), f(g') \in H'$ luego $f(gg') \in H$ luego $gg' \in f^{-1}(H')$. Está claro que $e \in f^{-1}(H')$ al estar $e \in H'$. Finalmente, si $h \in f^{-1}(H')$, entonces $f(h) \in H'$ luego $f(h)^{-1} = f(h^{-1}) \in H'$ luego $h^{-1} \in f^{-1}(f(H'))$, y hemos acabado. □

A continuación vamos a ver algunas propiedades para conocer mejor cómo construir homomorfismos que parten de un grupo cíclico. Bastará que veamos para $\mathbb{Z}_n$ dado que como sabemos todos los cíclicos de un mismo orden son isomorfos.

Proposición 29. *Se tiene un $f : \mathbb{Z}_n \to \mathbb{Z}_d$ sobreyectivo si $d|n$, dado por $f(1) = \frac{n}{d}$.*

Demostración. Sea $k = \frac{n}{d}$. Tomamos el morfismo $f_1 : \mathbb{Z}_n \to \mathbb{Z}_n$ dado por $f_1(g) = kg$. Como sabemos está bien definido al ser $\mathbb{Z}_n$ abeliano. Lo único que queda ver es que $Im(f_1) \simeq \mathbb{Z}_d$, pero sabemos que $Im(f_1) =< k >$ con orden d (al ser $kd = n$), luego hemos acabado. □

Proposición 30. *Si G es cíclico de orden n, y H es un subgrupo, $f : G \to H$ dado por $f(1) = h$ con $h \in H$ existe $\iff$ $o(h)|n$. Aquí 1 indica la el elemento que corresponde al generador de G, en analogía con $\mathbb{Z}_n$. Como los homomorfismos vienen determinados por la imagen del generador, se deduce que hay tantos como $h \in H$ tales que $o(h)|n$.*

Demostración. Si existe como homomorfismo, entonces $1^n = e \implies f(1)^n = e \implies g^n = e$ luego $o(g)|n$. Por otra parte, si $o(g) = d$ y $d|n$, estamos en el supuesto de la proposición anterior, y se tiene el homomorfismo deseado (tomando, si $n = kd$, el que manda el $f(1)$ al $\frac{n}{k}$) □

1.4. Subgrupos Normales

Anteriormente discutimos las clases laterales de un subgrupo, y vimos que las clases a izquierda no tienen por qué coincidir con las clases a derecha. Esta carencia impide que el cociente G/H sea un grupo en si mismo. Para solucionar esto, vamos a considerar los subgrupos cuyas particiones laterales son las mismas.

Definición 15. Sea $H < G$. Se dice que H es **normal**, y se denota $H \lhd G$, si $\forall g \in G$ se tiene $gH = Hg$.

Está claro que si G es abeliano todos sus subgrupos son normales. Otra observación clave es esta:

Observación 6. Si $[G : H] = 2$, entonces $H \lhd G$

Razón. Como H ha de estar en las particiones, tanto izquierdas como derechas, está claro que estas son ambas $\{H, H^c\}$. Por lo tanto, si $gH = H$, es porque $g \in H$ y $H = Hg$, y por otro lado, si $gH = H^c$, es porque $g \notin H$ y por tanto $Hg = H^c$. Luego $gH = Hg$ en todo caso.

Proposición 31. *Si $H \lhd G$, entonces $(G/H, *)$ es un grupo, con $aH * bH = (ab)H$.*

Demostración. Debemos ver en primer lugar que la operación está bien definida. Es decir, que si $aH = a'H$ y $bH = b'H$, vamos a tener que $(ab)H = (a'b')H$. Para ello, vamos a multiplicar los conjuntos $(aH)(bH) = \{cd : c \in aH \wedge d \in bH\} = aHbH = a(Hb)H = abHH = abH = (ab)H$. Hemos usado que $HH \subset H$ claramente al ser H grupo, y $H \subset HH$ tomando las combinaciones de la forma eh con $h \in H$. Esto quiere decir que, a nivel de conjunto, multiplicar aH y bH nos da la clase lateral $(ab)H$, si H es normal. Como $a'H = aH$ y $b'H = bH$, eso quiere decir que $(a'b')H = (a'H)(b'H) = (aH)(bH) = (abH)$ y hemos acabado. Por otro lado, el elemento neutro es H dado que $(aH)(eH) = (ae)H = aH$, y el inverso de gH es $g^{-1}H$ dado que $gHg^{-1}H = (gg^{-1})H = H$. □

Proposición 32. *La función natural $\pi : G \to G/H$ tal que $\pi(g) = gH$, es un homomorfismo si $H \lhd G$ y $Nuc(\pi) = H$.*

Demostración. $\pi(g)\pi(g') = gHg'H = gg'H = \pi(gg')$. Asimismo, $x \in Nuc(\pi) \iff xH = H \iff x \in H$. □

Acabamos de ver que existe un homomorfismo cuyo núcleo es un subgrupo normal. El recíproco, de hecho, es cierto:

Teorema 2. *Sea $f : G \to H$ un homomorfismo. Se tiene que $N = Nuc(f) \lhd G$. De hecho, el conjunto $gN = f^{-1}(f(g))$, es decir, desplazando N con g se obtienen todos los elementos que comparten imagen con g.*

Demostración. Veamos que $gN = f^{-1}(f(g))$. Si $gn \in gN$, entonces $f(gn) = f(g)f(n) = f(g)e = f(g)$, luego $gn \in f^{-1}(f(g))$. Por otro lado, si $g' \in f^{-1}(f(g))$, entonces $f(g') = f(g)$, lo que indica que $g^{-1}g' \in N$. Es decir, podemos expresar $g' = g(g^{-1}g')$, pero esto nos dice que $g' \in gN$.

Ahora observemos que la misma demostración sirve para ver que $Ng = f^{-1}(f(g))$, simplemente revirtiendo las operaciones para que sean a derecha. Entonces hemos probado que $gN = Ng$. □

Proposición 33. *Supongamos que $N < H < G$. Si $N \lhd G$, entonces $N \lhd H$.*

Demostración. Si $gN = Ng\ \forall g \in G$, en particular, para $h \in H \subset G$ se tiene $hN = Nh$. □

Lo que hemos visto aquí es que tiene sentido considerar también H/N para cualquier subgrupo de G, no solo G/N. El siguiente resultado los relaciona:

Proposición 34. *Si $N < H < G$ y $N \lhd G$, entonces $H/N < G/N$.*

Demostración. En primer lugar, si $hN, h'N \in H/N$, entonces $hNh'N = (hh')N \in H/N$ al ser $hh' \in H$, luego es cerrado. Al ser H subgrupo, se tiene $e \in H$ luego $eN \in H/N$, lo que nos da el neutro. Finalmente, si $hN \in H/N$, como $h^{-1} \in H$ al ser grupo, entonces $h^{-1}N \in H/N$ lo que nos da los inversos. □

A continuación veremos un importante resultado. Dado un f sobreyectivo, podemos identificar completamente los subgrupos del espacio de llegada con los del espacio de partida que contengan al núcleo mediante tomar preimágenes. De este modo, podremos calcular cuántos son/como se relacionan los subgrupos de un cierto espacio, construyendo un f sobreyectivo que parta de uno más sencillo y cuyo núcleo conozcamos.

Proposición 35. *Sea $f : G \to H$ homomorfismo sobreyectivo. Se tiene:*

1. *Si $ret'(G)$ son los subgrupos K de G tales que $Nuc(G) < K$ y $ret(H)$ son los subgrupos de H, entonces $\exists \varphi : ret(H) \to ret'(G)$ biyectiva, dada por $\varphi(L) = f^{-1}(L)$, que además preserva la estructura de retículo (las inclusiones entre los subgrupos).*
2. *$K \lhd H \iff f^{-1}(K) \lhd G$.*

Demostración. Sabemos que $\varphi' : ret(H) \to ret(G)$, dada por tomar preimágenes es inyectiva por ser f sobreyectiva. Entonces falta ver que $Im(\varphi') = ret'(G)$. Dado $L \in ret'(G)$, vamos a ver que de hecho $L = f^{-1}(f(L))$, y por tanto es preimagen de $f(L) \in ret(H)$. La inclusión $L \subset f^{-1}(f(L))$ es inmediata y aplica a cualquier conjunto L y función f. Por el contrario, si $g \in f^{-1}(f(L))$, como $f(g) \in f(L)$, entonces $f(g) = f(l)$ para cierto $l \in L$. Entonces, $gl^{-1} \in Nuc(f) \subset L$, luego $g = (gl^{-1})l \in L$ y hemos acabado. Está claro que preserva las inclusiones porque si $L \subset L_2$, entonces $f^{-1}(L) \subset f^{-1}(L_2)$ (esto ocurre para cualesquiera conjuntos y función).

Para la segunda afirmación, veamos que si $K \lhd H$, tiene sentido considerar $G \xrightarrow{f} H \xrightarrow{\pi} H/K$, de núcleo $f^{-1}(K)$, luego $f^{-1}(K) \lhd G$. Para la otra afirmación, si $gf^{-1}(K) = f^{-1}(K)g$ para todo $g \in G$, tenemos que $f(gf^{-1}(K)) = f(f^{-1}(K)g)$ luego $f(g)K = Kf(g)$ para todo $g \in G$, pero como es sobreyectiva, $hK = Kh$, $\forall h \in H$. □

Otra propiedad interesante de los subgrupos normales es que nos permiten generar otros subgrupos:

Proposición 36. *Sea $H \lhd G$ y $K < G$. Se tiene que $HK = KH$, y además $HK < G$.*

Demostración. $HK = \{hk : h \in H, k \in K\} = \bigcup_{k \in K} Hk = \bigcup_{k \in K} kH = \{kh : k \in K, h \in H\} = KH$. Es claramente cerrado, dado que si $hk, h'k' \in HK$, se tiene $hkh'k' = hh''kk' \in HK$ (hemos usado la normalidad para que $kh' = h''k$ para cierto $h'' \in H$). Por otra parte, $e \in HK$ al ser $e = e \cdot e$. Finalmente,

si $hk \in HK$, se tiene $(hk)^{-1} = k^{-1}h^{-1} = h'k^{-1} \in HK$. □

De hecho, el grupo descrito anteriormente es el menor que contiene a K y a H, dado que las operaciones por pares deben aparecer para garantizar el cierre. Se tiene una versión más restrictiva del resultado:

Proposición 37. *Si $H \lhd G$ y $K \lhd G$, se tiene que $HK \lhd G$.*

Demostración. Para ver la normalidad, basta con observar que $gHKg^{-1} = gHg^{-1}gKg^{-1} = (gHg^{-1})(gKg^{-1}) = HK$. □

Ahora vamos a ver un subgrupo normal de gran importancia:

Definición 16. El **centro** o **centralizador** de G es el grupo $C(G) = \{a \in G : ag = ga \forall g \in G\}$. Es decir, son los elementos que conmutan con todo el grupo. En ocasiones se denota $Z(G)$.

Proposición 38. *$Z(G) < G$. Además es abeliano.*

Demostración. Está claro que $e \in Z(G)$. Si $a, b \in Z(g)$, se tiene $abg = agb = gab$ luego $ab \in Z(G)$. Finalmente, si $a \in Z(G)$, entonces $a^{-1}g = (g^{-1}a)^{-1} = (ag^{-1})^{-1} = ga^{-1}$, luego $a^{-1} \in Z(G)$. Es abeliano porque si sus elementos conmutan con todo G, en particular lo hacen con $Z(G)$. □

Proposición 39. *Se tiene $Z(G) \lhd G$. Además, todo $K < Z(G)$ verifica $K \lhd Z(G)$.*

Demostración. Si $g \in G$, tenemos que $gZ(g) = Z(g)g$ dado que si $gz \in gZ(g)$, como $z \in Z(g)$, se tiene $gz = zg \in Z(g)g$. Del mismo modo, si $K < Z(g)$, todo $k \in K$ conmuta con G y por tanto $gK = Kg$. □

Vamos a ver un sencillo aunque potente resultado que nos ayudará a identificar el centro de un grupo:

Proposición 40. *Se tiene que $G/Z(G)$ es cíclico $\iff$ G es abeliano $\iff$ $G = Z(G)$.*

Demostración. El segundo $\iff$ es evidente. Por ello, demostraremos el primero. Está claro en $\impliedby$ que $G/Z(G) = G/G = \{\overline{e}\}$ luego es cíclico. Lo que queda probar es $\implies$. Supongamos que $G/Z(G) =< \overline{g} >$. Sea $\alpha \in G$. Entonces podemos decir que $\alpha \in g^iZ(g)$, luego $\alpha = g^ia$, con $a \in Z(g)$. Análogamente si $\beta \in G$, $\beta = g^jb$, con $b \in Z(g)$. Tenemos entonces que $\alpha\beta = g^iag^jb = g^ig^jab = g^{i+j}ab = g^jg^iab = g^jbg^ia = \beta\alpha$ donde hemos usado que a, b conmutan con todo. □

1.5. Teoremas de isomorfía

Teorema 3. *Sea $f : G_1 \to G_2$ homomorfismo sobreyectivo. Sea $H < Nuc(f)$ con $H \lhd G_1$. Entonces, $\exists \overline{f} : G_1/H \to G_2$, dada por $\overline{f}(aH) = f(a)$, bien definida, tal que:*

1. *$\overline{f} \circ \pi = f$, donde $\pi : G_1 \to G_1/H$ es el natural.*
2. *$Nuc(\overline{f}) = Nuc(f)/H$.*
3. *$\overline{f}$ es sobreyectiva.*

Demostración. Está bien definida dado que si $aH = bH$, entonces $a^{-1}b \in H \subset Nuc(f)$ luego $f(a^{-1}b) = e$ con lo que $f(a) = f(b)$. El punto (1) se tiene de inmediato dado que $\overline{f}(\pi(g)) = \overline{f}(gH) = f(g)$. Se tiene $\overline{g} \in Nuc(\overline{f}) \iff e = \overline{f}(\overline{g}) = f(g)$ luego hace falta que $g \in Nuc(f)$ pero esto ocurre $\iff \overline{g} \in Nuc(f)/H$. Finalmente, como $f = \overline{f} \circ \pi$ y tanto f como π son sobreyectivas, ha de serlo $\overline{f}$. □

Teorema 4 (Primer Teorema de Isomorfía)**.** *Si $f : G_1 \to G_2$ es homomorfismo sobreyectivo, entonces $G_1/Nuc(f) \simeq G_2$.*

Demostración. Aplicamos el teorema previo para $H = Nuc(f)$, luego $\overline{f}$ se vuelve inyectiva (su núcleo será $Nuc(f)/Nuc(f) = \{e\}$) y por tanto isomorfismo. □

Obsérvese que el teorema se puede reformular así: dado $f : G \to H$ un homomorfismo, entonces $G/Nuc(f) \simeq Im(f)$.

Teorema 5 (Segundo Teorema de Isomorfía)**.** *Sean $H \lhd L \lhd G$. Sabemos entonces que $L/H \lhd G/H$ al ser L, G sus preimágenes por el epimorfismo π. Se tiene que $(G/H)/(L/H) \simeq G/L$.*

Demostración. Consideramos los epimorfismos naturales $\pi : G/H \to (G/H)/(L/H)$ y $\pi' : G \to G/H$. La composición es $f = \pi \circ \pi'$. Está claro que es epimorfismo, y además $g \in Nuc(f) \iff \pi'(g) \in (L/H) \iff g \in L$. Aplicando el primer teorema de isomorfía se tiene el resultado. □

Teorema 6 (Tercer Teorema de Isomorfía)**.** *Sea G un grupo y $K < G$, $H \lhd G$. Sabemos que $HK < G$ en ese caso, pero entonces $H \lhd HK$. Se tiene que, además, $H \cap K \lhd K$ y que $K/(H \cap K) = HK/H$.*

Demostración. Sea $j : K \to KH$ la inclusión y $\pi : KH \to KH/H$ el epimorfismo natural. Sea $\beta = \pi \circ j$. En primer lugar, es sobreyectivo, dado que si $(kh)H \in KH/H$, tenemos que como $khH = kH$, entonces $\beta(k) = (kh)H$. Por otro lado, $k \in Nuc(f) \iff k \in H \wedge k \in K \iff k \in K \cap H$. De aquí se deduce que $Nuc(f) = K \cap H \lhd K$ y aplicando el primer teorema de isomorfía, el resultado se tiene. □

1.6. Clases de conjugación. Centralizador. Normalizador. Teorema de Cauchy.

Proposición 41 (Relación de conjugación)**.** *Fijado G grupo, la relación $xRx' \iff gxg^{-1} = x'$ para cierto $g \in G$ es de equivalencia, y por tanto induce una partición en G.*

Demostración. Está claro que xRx dado que $exe = e$. Por otra parte, si xRy, entonces $gxg^{-1} = y$ luego $g^{-1}yg = (g^{-1})y(g^{-1})^{-1} = x$. Finalmente, si $gxg^{-1} = y$ y además $hyh^{-1} = z$, sustituyendo se tiene que $z = ghxh^{-1}g^{-1} = ghx(gh)^{-1}$. □

Definición 17. Las clases de equivalencia de la relación anterior son, por tanto, $[x] = \{gxg^{-1} : g \in G\} := F_x$ y se denominan **clases de conjugación**.

Observación 7. Las clases de conjugación tienen tamaño variable, y si $x \in Z(G)$, de hecho se tiene que $F_x = \{x\}$ dado que conmuta con g y g^{-1}. La implicación inversa es cierta: si $gxg^{-1} = x$ siempre, entonces $gx = xg$. Es decir: $F_x = \{x\} \iff x \in Z(G)$.

La siguiente definición nos permitirá saber exactamente cuántos elementos tiene cada clase de conjugación:

Definición 18. El **centralizador** de $x \in G$ es el conjunto $C(x) = \{g \in G : gxg^{-1} = x\}$. Es decir, son los elementos que lo dejan fijo.

Proposición 42. $C(x) < G$.

Demostración. Está claro que $e \in C(x)$. Asimismo, si $h \in C(x)$, como $hxh^{-1} = x$, se tiene $h^{-1}xh = x$ luego $h^{-1} \in C(x)$. Finalmente, si $a, b \in C(x)$, entonces como $axa^{-1} = x$ y $bxb^{-1} = x$. Por lo tanto, $abxb^{-1}a^{-1} = x$ luego $ab \in C(x)$. □

Proposición 43. *Se tiene que $axa^{-1} = bxb^{-1} \iff a \in bC(x)$. Es decir, F_x tiene tantos elementos como clases laterales haya en $C(x)$. Por tanto: $|F_x| = [G : C(x)]$.*

Demostración. Si $a \in bC(x)$, entonces $a = bh$ con $h \in C(x)$, luego $hxh^{-1} = x$ y por tanto $axa^{-1} = bhxh^{-1}b^{-1} = bxb^{-1}$. Por otro lado, si $axa^{-1} = bxb^{-1}$, entonces $b^{-1}axa^{-1}b = x$ luego $b^{-1}a \in C(x)$ y por tanto $a \in bC(x)$. □

Observación 8 (Ecuación de Clases). Supongamos que $\{x_1, \ldots, x_s\}$ son representantes de las clases de conjugación en G de tamaño 2 o superior. Entonces:

$$|G| = |Z(G)| + \sum_{j=1}^{s} [G : C(x_s)]$$

Debido a que sumamos los elementos del centro, cuyas clases tienen 1 solo elemento, y después, en virtud de la proposición anterior, sumamos los tamaños de las cajas restantes.

El siguiente teorema es de inmensa utilidad para clasificar los subgrupos de un grupo:

Teorema 7 (Cauchy)**.** *Sea G finito tal que el primo p verifica $p||G|$. En ese caso, G tiene un elemento de orden p.*

Demostración. Comenzamos primero con el caso de que G sea abeliano y procedemos por inducción en $|G|$. Si $|G| = 2$, se verifica de inmediato. Pongamos ahora que $|G| = n > 2$ y asumamos que se cumple si $|G| < n$. En ese caso podemos tomar un $g \in G$, $g \neq e$. Si $p|o(g)$ hemos acabado, ya que $g^{\frac{o(g)}{p}}$ tiene orden p. Si no, entonces podemos definir $G/ < g >$ al ser abeliano, y como $|G| = |G/ < g > | \cdot | < g > |$, debe darse que $p||G/ < g > |$. Como $< g > \neq \{e\}$, entonces ese grupo cociente tiene orden menor a G y por hipótesis de inducción, $\overline{x} \in G/ < g >$ tiene orden p. Pero sabemos que $o(\pi(x))|o(x)$, luego $o(\overline{x})|o(x)$, y por tanto $p|o(x)$ y estamos en el caso primero.

Ahora supongamos que G es un grupo arbitrario. Procedemos por inducción en $|G|$. El caso base ya se ha mostrado. Supongamos que se cumple para todos los grupos de orden $k < |G|$. Supongamos que $p||C(x_i)|$ para algún x_i representante de clase de conjugación de más de 1 elemento. Bajo este supuesto, $[G : C(x_i)] > 1$ lo que nos dice que $|C(x_i)| < |G|$, de tal modo que por hipótesis de inducción hemos acabado. Ahora imaginemos que no se verifica lo anterior. Entonces como $|G| = |C(x_i)|[G : C(x_i)]$, es necesario que $p|[G : C(x_i)]$, para todo x_i con la propiedad mencionada. Nos valemos de la observación previa: $|G| = |Z(G)| + \sum_{j=1}^{s} [G : C(x_s)]$, que módulo p se vuelve: $0 = |Z(G)| + 0$, luego $p||Z(G)|$, y como $Z(G)$ es abeliano hemos acabado. □

Otra utilidad de la ecuación de clases es un resultado acerca de los denominados p-grupos.

Definición 19. Sea p primo. G es un p-grupo si es finito y $|G| = p^k$ para algún $k \geq 0$.

Teorema 8. *Sea G un p-grupo. Entonces $|Z(G)| \neq 1$, es decir, su centro es no trivial.*

Demostración. Consideramos la ecuación de clases del grupo: $|G| = |Z(G)| + \sum_{j=1}^{s} [G : C(x_s)]$. Como $|G| = |C(x_i)|[G : C(x_i)]$ y $|G| = p^k$, sigue inmediatamente que $[G : C(x_i)] = p^t$ para cierto $t > 0$ porque $[G : C(x_i)] \geq 2$. Tomando clases módulo p en la ecuación de clases, tenemos que $0 = |Z(G)| + 0$, de lo que sigue que $p||Z(G)|$ y por tanto no puede ser el trivial. □

Al igual que considerabamos el isomorfismo $x \to gxg^{-1}$ para elementos, podemos hacerlo para subgrupos. Es decir, vamos a estudiar cual es la acción del isomorfismo en los subgrupos de G. Naturalmente, pueden quedar fijos o ir a parar a otro subgrupo del mismo tamaño. Esto se explora de manera similar a los elementos:

Definición 20. Sea G un grupo y $K < G$. El **normalizador** de K es el conjunto: $N(K) = \{g \in G : gKg^{-1} = K\}$.

Observación 9. Por definición se tiene que $N(K) = G \iff K \lhd G$.

Proposición 44. *Se tiene que $N(K) < G$.*

Demostración. Está claro que $e \in N(K)$. Asimismo, si $h \in N(K)$, como $hKh^{-1} = K$, se tiene $h^{-1}Kh = K$ luego $h^{-1} \in N(K)$. Finalmente, si $a, b \in N(K)$, entonces como $aKa^{-1} = K$ y $bKb^{-1} = K$. Por lo tanto, $abKb^{-1}a^{-1} = K$ luego $ab \in N(K)$. □

Proposición 45. *Se tiene que $K \lhd N(K)$.*

Demostración. Para ver que $K \subset N(K)$, está claro que si $g \in K$, $gKg^{-1} = Kg^{-1} = K$. Además por definición todo $g \in N(K)$ verifica $gKg^{-1} = K$. □

Proposición 46. *El conjunto $F_K = \{gKg^{-1} : g \in G\}$ de posibles desplazamientos del subgrupo verifica $|F_K| = [G : N(K)]$*

Demostración. El argumento es el mismo que para las clases de conjugación, es decir, $gKg^{-1} = hKh^{-1} \iff h^{-1}gKg^{-1}h = K \iff h^{-1}g \in N(K) \iff h \in gN(K)$. □

1.7. Notación Cíclica para Permutaciones

Para estudiar los grupos S_n de permutaciones de n elementos, o lo que es lo mismo, de biyecciones de $\mathbb{N}_n = \{1, \dots, n\}$ en sí mismo, conviene hablar del concepto de **ciclo**, tanto por motivos de notación, como por motivos de entendimiento de las permutaciones y facilidad en su operación.

Definición 21. La permutación $\sigma \in S_n$ es un **ciclo de longitud r** si existe una partición $\mathbb{N}_n = F \cup C$, tal que $\forall x \in F$, tenemos $\sigma(x) = x$, y además $C = \{x_0, \sigma(x_0), \sigma^2(x_0), \dots, \sigma^{r-1}(x_0)\}$, y se tiene $\sigma^r(x_0) = x_0$.

Es decir, σ fija una serie de puntos, y el resto se obtienen aplicando σ sucesivas veces. Se denota $\sigma = (x_0, \sigma(x_0), \sigma^2(x_0), \dots, \sigma^{r-1}(x_0))$.

Por ejemplo, la permutación $\sigma \in S_3$ dada por $\sigma(1) = 1$, $\sigma(2) = 3$ y $\sigma(3) = 2$ es un ciclo y se denota $\sigma = (23)$.

Definición 22. Dos ciclos σ_1, $\sigma_2 \in S_n$ son **disjuntos** si los conjuntos C_1 y C_2 de puntos que no quedan fijos lo son.

Proposición 47. *Toda $\sigma \in S_n$ es composición de ciclos disjuntos.*

Demostración. Ponemos $1 = x_1$. Supongamos que $\sigma(x_1) = x_2$ para otro $x_2 \in S_n$, e, iterando este proceso, que $\sigma(x_k) = x_{k+1}$. En cierto punto r se tendrá que $\sigma(x_r) = x_1$, completando un ciclo, dado que el grupo es finito y la función es biyectiva. Entonces el primer ciclo viene dado por $\sigma_1(x_k) = \sigma(x_k)$ con $k \in \{1, \dots, r\}$ y fijando el resto. Continuando a partir de x_{r+1} se extraen sucesivos ciclos hasta agotar los elementos de $\mathbb{N}_n$ y esos son todos los ciclos. □

Por ejemplo, la permutación $\sigma \in S_6$ dada por $\begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 2 & 3 & 1 & 5 & 4 & 6 \end{pmatrix}$ se puede expresar como $\sigma = (123)(45)$. Esto se conoce como **notación cíclica**. Presenta enormes ventajas en el tratamiento de permutaciones:

Proposición 48. *Los ciclos disjuntos $\sigma_1, \sigma_2 \in S_n$ conmutan.*

Demostración. Sea $x \in \mathbb{N}_n$. Si ambos ciclos fijan x, está claro que $\sigma_1(\sigma_2(x)) = \sigma_2\sigma_1(x)$. Si alguno no lo fija, sin perder en generalidad suponemos que es el σ_1. Por ser disjuntos, entonces el σ_2 lo fija, así como a $\sigma_1(x)$. Pero entonces $\sigma_1(\sigma_2(x)) = \sigma_1(x) = \sigma_2(\sigma_1(x))$. □

Proposición 49. *Un ciclo de longitud r tiene orden r. Por tanto, $\sigma \in S_n$ tiene como orden el mínimo común múltiplo de las longitudes de su expresión en ciclos disjuntos.*

Demostración. Observamos de la definición de ciclo que si $x \in C$, entonces $x = \sigma^t(x_0)$ y entonces $\sigma^r(x) = \sigma^{(r+t)}(x_0) = \sigma^t(x_0) = x$. Por otro lado si $x \in F$ está claro que $\sigma^r(x) = x$ luego tiene orden r. No es difícil convencerse de que es el mínimo dado que si el orden fuese $\alpha < r$ no se tiene la propiedad $\alpha + t \neq t, \mod r$ que hemos utilizado. La afirmación acerca del mínimo común múltiplo sigue de manera evidente por la conmutatividad de los ciclos disjuntos. □

A continuación estudiaremos cómo actúan los isomorfismos de conjugación en S_n.

Proposición 50. *Si $\sigma \in S_n$ es el ciclo de longitud r, $\sigma = (i_1, i_2, \dots, i_r)$, entonces, dado $g \in S_n$, $g\sigma g^{-1} = (g(i_1), \dots, g(i_r))$ y por lo tanto es otro ciclo de su misma longitud.*

Demostración. Primero estudiamos el comportamiento de $g\sigma g^{-1}$ en los puntos de la forma $g(i_t)$. Se tiene que $g\sigma g^{-1}(g(i_t)) = g\sigma(i_t) = g(i_{t+1})$, luego como vemos $g\sigma g^{-1}$ hace ciclar estos puntos. Por otro lado, si $k \in \mathbb{N}_n \backslash \{i_1, \dots, i_r\}$, tenemos que, en $g(k)$, $g\sigma g^{-1}(g(k)) = g\sigma(k) = g(k)$, luego efectivamente es el ciclo propuesto. □

Proposición 51. *Sean en S_n los elementos $\sigma_1 = (i_1^1, i_2^1, \dots, i_{r_1}^1)(i_1^2, i_2^2, \dots i_{r_2}^2) \dots (i_1^k, i_2^k, \dots, i_{r_k}^k)$ y $\sigma_2 = (j_1^1, j_2^1, \dots, j_{r_1}^1)(j_1^2, j_2^2, \dots j_{r_2}^2) \dots (j_1^k, j_2^k, \dots, j_{r_k}^k)$ que, como se observa, constan del mismo número de ciclos y con las mismas longitudes. Entonces $\exists \sigma \in S_n$ tal que $\sigma\sigma_1\sigma^{-1} = \sigma_2$, y es todo aquel que verifique $\sigma(i_t^s) = j_t^s$ en todos t, s.*

Demostración. Siempre podemos construir un σ como el propuesto en la proposición, decidiendo las imágenes del resto de los puntos arbitrariamente. Tenemos que:

$$\sigma\sigma_1\sigma^{-1} = \sigma(i_1^1, i_2^1, \dots, i_{r_1}^1)\sigma^{-1}\sigma(i_1^2, i_2^2, \dots i_{r_2}^2)\sigma^{-1}\sigma \dots \sigma^{-1}\sigma(i_1^k, i_2^k, \dots, i_{r_k}^k)\sigma^{-1}$$

Y por la proposición previa resulta ser σ_2. □

Observación 10. Si dos permutaciones se descomponen en ciclos disjuntos con las mismas longitudes, como en el enunciado anterior, entonces están relacionadas por conjugación, y como aplicar composición preserva las longitudes de ciclos, se trata, de hecho, de una equivalencia. Es decir, **la clase de conjugación de una permutación son todas las que se descomponen en ciclos con misma longitud que ella**.

Definición 23. Una **trasposición** $\tau \in S_n$ es un ciclo de longitud 2. Es decir, $\tau = (ab)$.

Teorema 9. *S_n está generado por sus trasposiciones. Es decir, toda $\sigma \in S_n$ es producto de trasposiciones.*

Demostración. Por lo que sabemos ya, basta con probarlo para ciclos $\sigma = (i, \sigma(i), \dots, \sigma^{r-1}(i))$. Se afirma que se tiene $\sigma = (i, \sigma^{r-1}(i))(i, \sigma^{r-2}(i)) \dots (i, \sigma(i))$. Está claro que si k queda fijo por el ciclo, entonces no figura en ninguna de esas trasposiciones y por ello queda fijo. Si tomamos $\sigma^t(i)$, veamos que: $(i, \sigma^{r-1}(i))(i, \sigma^{r-2}(i)) \dots (i, \sigma(i))\sigma^t(i) = (i, \sigma^{r-1}(i)) \dots (i, \sigma^t(i))\sigma^t(i) = (i, \sigma^{r-1}) \dots (i, \sigma^{t+1}(i))i = (i, \sigma^{r-1}) \dots (i, \sigma^{t+2})\sigma^{t+1}(i) = \sigma^{t+1}(i)$, luego lo cicla, como queríamos ver. □

Teorema 10 (De paridad)**.** *Todas las formas de expresar $\sigma \in S_n$ como k trasposiciones mantienen la paridad de k. Es decir, si se puede expresar como un número par (resp. impar) de trasposiciones, entonces siempre que se exprese como producto de trasposiciones habrá un número par (resp. impar) de ellas.*

Por tanto, podemos distinguir entre permutaciones **pares e impares**. Las **pares** forman un grupo, $A_n < S_n$, de índice 2, llamado **grupo alternado**.

Definición 24. Un grupo G es **simple** si $H \lhd G \implies H = G \vee H = \{e\}$. Es decir, no tiene subgrupos normales propios no triviales.

Proposición 52. *Si G es abeliano, entonces G es simple $\iff |G| = p$.*

Demostración. Claramente, si $|G| = p$ entonces directamente no tiene subgrupos propios no triviales, luego es simple. Si suponemos que $|G| = pq$ con p primo y $q > 2$, por el contrario, entonces el teorema de Cauchy asegura que $\exists a \in G$ con $o(a) = p$, de tal modo que $\langle a \rangle \subset G$ es propio y no trivial, y como G es abeliano, entonces es normal y no puede ser simple. □

Para estudiar el comportamiento de $A_n < S_n$ conviene preguntarse qué ocurre con los subgrupos de S_n cuando los intersecamos en A_n. En general se observa el siguiente resultado:

Proposición 53. *Supongamos que G es un grupo con $N < G$ y $[G : N] = 2$. Entonces dado otro $K < G$, se tiene que $K \cap N = K$ o bien $[K : K \cap N] = 2$. Es decir, o bien K está entero en N o bien K tiene la mitad en N y la mitad fuera.*

Demostración. Consideramos la cadena de morfismos $f : K \to G \to G/N$, donde de K a G vamos por inclusión y de G a G/N vamos de manera natural tomando clases. Está claro que $Nuc(f) = N \cap K$. El teorema de isomorfía indica que $K/(K \cap N) \simeq Im(f)$. Pero $Im(f) < G/N$, que tiene dos elementos. Si es todo G/N entonces $K/(K \cap N) \simeq G/N$ y entonces $[K : K \cap N] = 2$. Si por el contrario es el trivial, entonces $K = K \cap N$. □

1.8. Productos semidirectos

Proposición 54. *Sea G finito, $K_1 \lhd G$ y $K_2 < G$. Entonces $|K_1K_2| = \frac{|K_1||K_2|}{|K_1 \cap K_2|}$*

Demostración. Tenemos que $|K_1K_2| = |K_1||\frac{K_1K_2}{K_1}|$, pero el tercer teorema de isomorfía nos asegura que $K_1K_2/K_1 \simeq K_2/(K_1 \cap K_2)$ luego tienen los mismos elementos y hemos acabado. □

Observación 11. En particular, si $K_1 \cap K_2 = \{e\}$, entonces $|K_1K_2| = |K_1||K_2|$.

Es decir, en el caso anterior $|K_1K_2| = |K_1 \times K_2|$, y cabría preguntarse si son isomorfos.

Proposición 55. *En los supuestos anteriores, la aplicación $p : K_1 \times K_2 \to K_1K_2$ con $p((k_1, k_2)) \to k_1k_2$ es biyectiva.*

Demostración. Claramente es sobreyectiva: por definición los elementos de K_1K_2 son aquellos de la forma k_1k_2, con $k_1 \in K_1$ y $k_2 \in K_2$. Además, la observación anterior indica que va entre grupos del mismo orden, luego es biyección. □

No obstante, si tomamos el grupo $D_5 = \langle A, B | A^5, B^2, BAB^{-1}A \rangle$, y los subgrupos $K_1 = \langle A \rangle$ y $K_2 = \langle B \rangle$, nos damos cuenta de que estamos en los supuestos anteriores, con $K_1K_2 = D_5$ y sin embargo $K_1 \times K_2 \simeq \mathbb{Z}_{10}$ cíclico. Luego, en general, la biyección anterior **NO** es un homomorfismo de grupos. Solo bajo ciertas condiciones adicionales. Primero, un lema previo:

Lema 1. *Si $K_1 \lhd G$, $K_2 \lhd G$ y $K_1 \cap K_2 = \{e\}$, entonces $k_1k_2 = k_2k_1 \forall k_1 \in K_1$, $k_2 \in K_2$.*

Demostración. Consideramos $k_2^{-1}k_1k_2$. Por normalidad de K_1, se tiene que ese elemento está en K_1, luego $k_1^{-1}k_2^{-1}k_1k_2 \in K_1$. Si consideramos ahora $k_1^{-1}k_2^{-1}k_1$, por normalidad de K_2, está en K_2 luego $k_1^{-1}k_2^{-1}k_1k_2 \in K_2$. Como la intersección es nula, se da que $k_1^{-1}k_2^{-1}k_1k_2 = e$ lo que implica que $k_1k_2 = k_2k_1$. □

Proposición 56. *Si $K_1 \lhd G$, $K_2 \lhd G$, $K_1 \cap K_2 = \{e\}$, entonces la aplicación del resultado anterior, $p : K_1 \times K_2 \to K_1K_2$ con $p((k_1, k_2)) \to k_1k_2$ es además un homomorfismo y por tanto un isomorfismo.*

Demostración. Tenemos $p((k_1, k_2))p((k_1', k_2')) = k_1k_2k_1'k_2' = k_1k_1'k_2k_2' = p((k_1, k_2)(k_1', k_2'))$, donde hemos usado el lema previo. □

Si aplicamos el teorema varias veces llegamos a la conclusión de que:

Observación 12. Si $N_1, \ldots, N_r$ son subgrupos normales de G ($N_i \lhd G$) y $N_i \cap (N_1 \ldots N_{i-1} N_{i+1} \ldots N_r) = \{e\}$, entonces $p : N_1 \times \cdots \times N_r \to N_1 \ldots N_r$ dado por $p(a_1, \ldots, a_r) = a_1 \ldots a_r$ es un isomorfismo.

Para que se tuviese ese isomorfismo hemos necesitado que ambos subgrupos sean normales, pero, puesto que basta con que uno lo sea para considerar el producto, conviene plantearse cómo hacer para que se tenga ese isomorfismo en caso de que uno de ellos no sea normal.

Definición 25. Cuando $K < G$, $N \lhd G$, $K \cap N = \{e\}$ y $KN = G$, se dice que $G = N \rtimes K$, es decir, que G es **producto semidirecto (interno)** de N y K.

Lo que nos preguntamos es si $N \times K$ puede ser isomorfo a $N \rtimes K$. Para ello vamos a dotar de otra estructura a $N \times K$.

Definición 26. Fijamos grupos G_1, G_2, y un homomorfismo $\varphi : G_2 \to Aut(G_1)$. El conjunto $G_1 \times G_2$ se dota de la operación:
$(a, b) \times_\varphi (c, d) = (a\varphi(b)(c), bd)$
Lo que da lugar a un grupo que se suele denotar $G_1 \rtimes_\varphi G_2$, y se denomina **producto semidirecto (externo)** dado que es isomorfo a un producto semidirecto (interno) de ciertos subgrupos ($G_1 \times e$ y $e \times G_2$).

Un sencillo cálculo muestra que esa operación es asociativa, tiene como neutro al (e_1, e_2), donde e_i es el neutro de G_i, y tiene como inverso del (a, b) al $(a, b)^{-1} = (\varphi(b^{-1})(a^{-1}), b^{-1})$.

Teorema 11. *En caso de que $N \rtimes K$, con $NK = G$, y $\varphi : K \to Aut(N)$ está dada por $k \to \varphi_k$ donde $\varphi_k \in Aut(N)$ es la conjugación: $\varphi_k(n) = knk^{-1}$, bien definida por ser N normal, entonces $p : N \rtimes_\varphi K \to G$ dada por $p(a, b) = ab$ es isomorfismo de grupos.*

Demostración. Por un lado, $p(n, k)p(n'k') = nkn'k'$. Por otro, $(n, k)(n', k') = (n\varphi(k)(n'), kk') = (nkn'k^{-1}, kk')$, luego $p((n, k)(n', k')) = nkn'k^{-1}kk' = nkn'k'$, como se quería. Como $N \rtimes K$ es el mismo conjunto que $N \times K$, ya sabemos que la aplicación es una biyección. □

Proposición 57. *En $G_1 \rtimes_\varphi G_2$, la aplicación $j : G_1 \to G_1 \rtimes_\varphi G_2$ dada por $j(g) = (g, e)$, y la aplicación $j_2 : G_2 \to G_1 \rtimes_\varphi G_2$ dada por $j_2(g) = (e, g)$ son homomorfismos inyectivos, y sus imágenes ($G_1 \times e$ y $e \times G_2$) son subgrupos de $G_1 \rtimes_\varphi G_2$. El primero de ellos, $G_1 \times e$, es además un subgrupo normal. Finalmente, se tiene $(G_1 \times e) \times_\varphi (e \times G_2) = G_1 \rtimes_\varphi G_2$.*

La demostración sigue de un cálculo rutinario. Esto indica que el producto semidirecto externo es un producto interno de esos subgrupos, y por tanto, junto con el teorema anterior, se marca una **equivalencia** entre ambos conceptos y en adelante hablaremos simplemente de producto semidirecto.

1.9. Acciones, órbitas e isotropía

Vamos a generalizar los conceptos que tratamos en las clases de conjugación. Para ello, recordemos que considerabamos el isomorfismo $x \to gxg^{-1}$, pero realmente basta con asociar una biyección cualquiera a cada elemento de un grupo, de manera que preserve la estructura, para obtener la mayoría de resultados al respecto.

Definición 27. Dado un conjunto X y un grupo G, una **acción** de G en X es un homomorfismo $\alpha : G \to Biy(X)$.

Es decir, permite imaginar los elementos de G actuando sobre X.

Proposición 58. *Una acción induce una partición en X dada por la relación $x \sim y \iff \alpha(g)(x) = y$ para cierto $g \in G$.*

Demostración. Por ser homomorfismo, $\alpha(e)(x) = Id(x) = x$. Por otro lado, si $\alpha(g)(x) = y$, se tiene $x = \alpha^{-1}(g)(y) = \alpha(g^{-1})(y)$. Finalmente, para la transitividad, si $\alpha(g)(x) = y$ y $\alpha(h)(y) = z$, entonces $\alpha(h)(\alpha(g)(x)) = z$ luego $\alpha(hg)(x) = z$. □

Definición 28. A la clases de equivalencia de $x \in X$ con esta relación, es decir, a todos los puntos posibles alcanzables desde x mediante la acción de G, se le denomina **órbita** de x. $O(x) = \{\alpha(g)(x) : g \in G\}$.

Definición 29. Se define el **subgrupo de isotropía** de x como $G_x = \{g \in G : \alpha(g)(x) = x\}$, es decir, los elementos cuya acción deja invariante a x.

Proposición 59. *Se tiene $G_x < G$.*

Demostración. $e \in G_x$ trivialmente. Si $\alpha(g)(x) = x$ entonces $x = \alpha(g^{-1})(x)$, y finalmente, si $\alpha(g)(x) = \alpha(h)(x) = x$, entonces $\alpha(gh)(x) = x$ componiendo ambas, y por tanto es cerrado. □

Proposición 60. *Si G, X son finitos entonces se tiene $|O(x)| = [G : G_x]$.*

Demostración. Es análoga a cuando se hizo para las clases de conjugación (que son las órbitas bajo la acción de conjugación). Vamos a demostrar que elementos en la misma clase de G/G_x actúan igual sobre x, y elementos en distinta clase actúan distinto, con lo que habrá tantos elementos en la órbita como clases en el cociente. Efectivamente, se tiene $g_1G_x = g_2G_x \iff g_2^{-1}g_1G_x = G_x \iff \alpha(g_2^{-1}g_1)(x) = x \iff \alpha(g_1)(x) = \alpha(g_2)(x)$. □

1.10. Teoremas de Sylow

Los teoremas de Sylow nos permiten obtener mucha información sobre la estructura de subgrupos de un grupo finito dado.

Teorema 12 (De Sylow (1º))**.** *Sea G un grupo con $|G| = p^a m$, donde p es primo y $(p, m) = 1$. Entonces G tiene un subgrupo H con $|H| = p^a$.*

Demostración. Por inducción en $|G|$. Si $|G| = 2$, la afirmación es trivial. Supongamos que se tiene para todo grupo de orden $k < n$. Sea G con $|G| = n = p^a m$, con $(p, m) = 1$. Tenemos dos opciones:

- Si $p|Z(G)$, el teorema de Cauchy asegura que $\exists x \in Z(G)$ con $|\langle x \rangle| = p$, de tal modo que $G/\langle x \rangle$ es un grupo de orden $p^{a-1}m$, y por hipótesis de inducción, sea $Q < G/\langle x \rangle$ con $|Q| = p^{a-1}$. Si π es el epimorfismo natural que lleva cada elemento a su clase, entonces $\pi^{-1}(Q)$ verifica que $Q = \pi(\pi^{-1}(Q)) = \pi^{-1}(Q)/\langle x \rangle$, luego $|\pi^{-1}(Q)| = p \cdot p^{a-1} = p^a$ y hemos acabado.
- Si $p \nmid Z(G)$, observamos la ecuación de clases módulo p: $0 = |Z(G)| + \sum_j [G : C(x_j)]$. Como $|Z(G)| \neq 0$, entonces hay un j_0 con $[G : C(x_{j_0})] \neq 0$ en módulo p. Es decir, tenemos que $[G : C(x_{j_0})]|C(x_{j_0})| = |G|$ y además $p \nmid [G : C(x_{j_0})]$, de tal modo que ha de ser $|C(x_{j_0})| = p^a t$, donde $t < m$ o de otro modo $[G : C(x_{j_0})] = 1$ y no sería término de la ecuación de clases. Pero entonces, por hipótesis de inducción, hay un $Q < C(x_{j_0}) < G$ con $|Q| = p^a$ y hemos acabado.

□

Definición 30. En un grupo finito G con $|G| = p^a m$ y $(p, m) = 1$, si $H < G$ y $|H| = p^a$, se dice que H es un **p-subgrupo de Sylow**.

Con el fin de de enunciar y demostrar el segundo teorema, necesitamos un resultado previo:

Lema 2. *Supongamos que $Q, P < G$, donde Q es un p-subgrupo y P es un p-subgrupo de Sylow con $|P| = p^a$. Entonces, $N_Q(P) = \{q \in Q : qPq^{-1} = P\} = N_G(P) \cap Q$ verifica que $N_Q(P) = Q \cap P$.*

Demostración. Está claro que $P\cap Q \subset N_G(P)\cap Q = N_Q(P)$. Por otra parte, $N_Q(P) \subset Q$ por definición, luego basta ver que $N_Q(P) \subset P$, o lo que es lo mismo, $N_G(P)\cap Q \subset P$. Pero $P \lhd N_G(P)$ y $N_G(P)\cap Q < N_G(P)$, luego su producto libre es un subgrupo, y tenemos que: $N_G(P)\cap Q \subset P \iff [N_G(P)\cap Q]P = P$, con lo que solo tenemos que centrarnos en probar esta última afirmación. Como $P \subset [N_G(P)\cap Q]P$, lo que haremos será probar que tienen el mismo número de elementos. Efectivamente:

$$|[N_G(P)\cap Q]P| = \frac{|N_G(P)\cap Q|\cdot|P|}{|N_G(P)\cap Q\cap P|} = \frac{|N_G(P)\cap Q|\cdot|P|}{|Q\cap P|}$$

Pero como los 3 enteros que aparecen en esa expresión son potencias de p (por ser subgrupos de P o de Q), tenemos que $|[N_G(P)\cap Q]P| = p^b$ para cierto b. La cadena de inclusiones: $P \subset [N_G(P)\cap Q]P \subset G$ nos indica que de hecho, $p^a \leq p^b \mid p^a m$ con $(m,a)=1$, luego ha de ser $b=a$ y por tanto hemos acabado. □

Teorema 13 (De Sylow (2º))**.** *Sea G un grupo finito y P un p-subgrupo de Sylow suyo. Sea Q cualquier p-subgrupo (subgrupo de orden potencia de p). Entonces, $\exists g \in G$ con $Q < gPg^{-1}$. En particular, si Q es p-subgrupo de Sylow, entonces $\exists g \in G$ con $Q = gPg^{-1}$.*

Demostración. Sea $X = \{gPg^{-1} : g \in G\} = \{P_i\}_{i=1}^r$ la órbita de P por la acción de conjugación de G. Como hemos indicado, ponemos $|X| = r$, y, en el listado anterior, $P_1 = P$. En primer lugar, vamos a probar que $r \equiv 1 \mod p$. Para ello, vamos a considerar la acción por conjugación de P en X, bien definida dado que como $P < G$, entonces si $P' \in X$, tenemos que $pP'p^{-1} \in X$ siempre que $p \in P$. Si $\{P_{i_j}\}_{j=1}^s$ son representantes de las clases de conjugación por esta acción, con $i_1 = 1$, entonces sus clases particionan X:

$$X = \bigsqcup_{j=1}^{s} \{pP_{i_j}p^{-1} : p \in P\} = \{P\} \sqcup \bigsqcup_{j=2}^{s} \{pP_{i_j}p^{-1} : p \in P\}$$

Dado que $pPp^{-1} = P$ si $p \in P$. Aquí $\sqcup$ denota la unión disjunta. Atendiendo a los cardinales:

$$|X| = 1 + \sum_{j=2}^{s} \left|\{pP_{i_j}p^{-1} : p \in P\}\right|$$

Pero como cada uno de los P_{i_j} con $j \geq 2$ verifica que $P_{i_j}\cap P \subsetneq P$ (de otro modo $P_{i_j} = P$ al tener la misma cantidad de elementos), entonces, como $|\{pP_{i_j}p^{-1} : p \in P\}| = [P : P\cap P_j]$ por el lema previo, cada $[P : P\cap P_j] > 1$ y es potencia de primo, luego, módulo p, se tiene $|X| = 1 + 0 = 1$, como se quería.

A continuación, vamos a repetir lo mismo pero bajo la acción de conjugación de Q, para obtener:

$$X = \bigsqcup_{j=1}^{l} \{qP_{i_j}q^{-1} : q \in Q\} \qquad (i)$$

$$|X| = \sum_{j=1}^{l} \left|\{qP_{i_j}q^{-1} : q \in Q\}\right| \qquad (ii)$$

Donde esta vez los $\{P_{i_j}\}_{j=1}^l$ son los representantes de las clases bajo esta nueva acción. Seguimos eligiendo $i_1 = 1$. Pero ahora supongamos que ningún P_{i_j} verifica que $Q < P_{i_j}$. Entonces, usando de nuevo el lema previo:

$$\left|\{qP_{i_j}q^{-1} : q \in Q\}\right| = [Q : N_Q(P_{i_j})] = \frac{|Q|}{|Q\cap P_{i_j}|} > \frac{|Q|}{|Q|} = 1$$

Hemos utilizado que $|Q\cap P_{i_j}| < |Q|$, dado que si fuesen iguales, se tendría que $Q\cap P_{i_j} \subset Q$ que hemos supuesto que no ocurre. Además observemos que $\frac{|Q|}{|Q\cap P_{i_j}|}$ es potencia de primo por serlo numerador y

denominador. Por lo tanto, tomando en (ii) módulo p, llegamos a que $r \equiv 0 \mod p$, contradiciendo lo anterior, y por tanto $Q < P_{i_j}$ para algún $P_{i_j} \in X$. □

Finalmente, el tercer teorema nos ayuda a contar los p-subgrupos:

Teorema 14 (De Sylow (3^o))**.** *Sea G un grupo finito con $|G| = p^a m$, $(p, m) = 1$. Sea P un p-subgrupo de Sylow suyo, y $\{gPg^{-1} : g \in G\} = \{P = P_1, \ldots, P_r\}$ todos los p-subgrupos de Sylow. Se tienen:*

1. $r \equiv 1 \mod p$
2. $r \mid m$

Demostración. En la demostración del teorema 2 ya hemos mostrado 1, luego falta por mostrar 2. Tenemos que $|P|[G : P] = |G| = r|N(p)| = r|P|[N(P) : P] \implies m = [G : P] = r|P|[N(P) : P] \implies r \mid m$. □

Esto no solo ayuda a contarlos, sino que en muchas ocasiones obtendremos información adicional. Veamos la fuerza de estos teoremas en el ejemplo siguiente:

Observación 13 (Grupos de orden 10). Consideramos G con $|G| = 10 = 2^1 \cdot 5^1$. La información del teorema 3 nos dice que, si n_2 y n_5 son los números de 2-grupos y 5-grupos de Sylow, tenemos $n_5 \equiv 1$ mód 5 y $n_5|2$ luego $n_5 = 1$, y, del mismo modo, $n_2 = 1$ o bien $n_2 = 5$.

- Si $n_2 = n_5 = 1$, sean P_2 y P_5 esos subgrupos. P_5 es normal por ser de índice 2, y, de acuerdo al segundo teorema de Sylow: $gP_2g^{-1} = P_2$ dado que $n_2 = 1$. Por tanto ambos son normales, al ser sus ordenes coprimos tenemos $P_2 \cap P_5 = \{e\}$ y $P_2P_5 = G$, es decir: $G \simeq P_2 \times P_5 \simeq \mathbb{Z}_2 \times \mathbb{Z}_5 \simeq \mathbb{Z}_{10}$.
- Si $n_2 = 5$, entonces P_2 no es normal. Aun así tenemos $G = P_5 \rtimes_\varphi P_2 \simeq \mathbb{Z}_5 \rtimes_\varphi \mathbb{Z}_2$, donde $\varphi : \mathbb{Z}_2 \to Aut(\mathbb{Z}_5) \simeq \mathcal{U}(\mathbb{Z}_5)$. Vemos que $\varphi(0) = Id$, luego falta escoger $\varphi(1) = \alpha_k$ con $\alpha_k(\overline{a}) = \overline{ka}$, pero hace falta que $o(\alpha_k) \mid 2$ para que φ sea homomorfismo. Si $k = 1$ estamos en el caso trivial y el producto sería directo, lo que sabemos no pasa. Luego $k = 4$, lo que da un $\varphi(1)$ que actúa invirtiendo en $\mathbb{Z}_5$, y en este caso $G \simeq D_5$.

Por tanto los únicos grupos de orden 10 son $\mathbb{Z}_{10}$ y D_5.

Otra observación es la siguiente:

Proposición 61. *Sea G abeliano, con $|G| = p_1^{a_1} \ldots p_n^{a_n}$, cada p_i primo y distinto de los demás. Entonces, si P_i es un p_i-subgrupo de Sylow, es único. Además, se tiene $G \simeq P_1 \times \cdots \times P_n$*

Demostración. Para empezar, por ser G abeliano, se tiene $P_i \lhd G$, pero sabemos que todos los p_i-subgrupos de Sylow son $\{gP_ig^{-1} : g \in G\} = \{P_i\}$, de ahí la unicidad. Para la descomposición, primero veamos que por ser sus órdenes coprimos, $P_1 \cap P_2 = \{e\}$. Por ser ambos normales, $P_1P_2 \lhd G$ y por ser abeliano G, $P_1 \lhd P_1P_2$ y $P_2 \lhd P_1P_2$ luego $P_1P_2 \simeq P_1 \times P_2$. Ahora supongamos que hemos demostrado que $P_1 \ldots P_k \simeq P_1 \times \cdots \times P_k$. Como $P_1P_2 \ldots P_k \cap P_{k+1} = \{e\}$, y ambos son normales, tenemos que $P_1 \ldots P_kP_{k+1} \simeq (P_1 \ldots P_k) \times P_{k+1} \simeq P_1 \times \cdots \times P_k \times P_{k+1}$ por hipótesis. Luego por inducción hemos probado: $G = P_1 \ldots P_n \simeq P_1 \times \cdots \times P_n$. □

Por lo tanto, si queremos clasificar **todos** los grupos abelianos, basta con conocer la estructura de los p-grupos abelianos, dado que los demás se descomponen en producto de estos (de sus subgrupos de Sylow). Lo que se afirma es que **los p-grupos abelianos son producto directo de cíclicos**. Y por tanto, **todo grupo abeliano es producto de cíclicos**. Para probar ese resultado comenzaremos con una serie de resultados previos, para los que usaremos **notación aditiva** en vez de multiplicativa.

Observación 14. Si G es abeliano y $\alpha_p : G \to G$ es el homomorfismo dado por $\alpha_p(g) = pg$, entonces $Nuc(\alpha_p) = \{g \in G : o(g)|p\}$. Es decir, son los de orden p y el neutro.

Razón. $g \in Nuc(\alpha_p) \iff pg = e \iff o(g)|p$.

Lema 3. *Sea G un p-grupo abeliano tal que $\exists! H$ con $H < G$ tal que $|H| = p$. Entonces dado $K < G$ no trivial, $H < K$ y es el único con orden p.*

Demostración. $|K| = p^s$ para cierto s. Por el teorema de Cauchy, $\exists k \in K$ con $o(k) = p$. Entonces $\langle k \rangle < G$ luego $\langle k \rangle = H$. Si hubiese otro de orden p en K, también estaría en G contradiciendo la unicidad de H. □

Lema 4. *Sea G un p-grupo abeliano tal que $\exists! H$ con $H < G$ tal que $|H| = p$. Entonces es cíclico, es decir, $G \simeq \mathbb{Z}/p^n\mathbb{Z}$.*

Demostración. Por inducción en n. Si $n = 1$ entonces $|G| = p$ primo luego es cíclico. Si $n \geq 2$, nos valemos de la observación 14 para ver que $Nuc(\alpha_p) = H$. Efectivamente, si $g \in G$ tiene $o(g) = p$, como $< g >= H$ por unicidad, debe darse que $g \in H$, luego $Nuc(\alpha_p) \subset H$, y el recíproco es evidente. Entonces $|Im(\alpha_p)| = p^{n-1}$ y el lema anterior nos indica que $H < Im(\alpha_p)$ y es el único de orden p, luego aplicamos la hipótesis de inducción y $Im(\alpha_p) \simeq \mathbb{Z}/p^{n-1}\mathbb{Z}$. Pongamos $Im(\alpha_p) = \langle \overline{g} \rangle$. Se tiene que g no es el neutro porque si no $Im(\alpha_p)$ sería el trivial. Entonces $H < \langle g \rangle$ y sabemos entonces que, como $\pi : G \to G/H$ es sobreyectivo, $\exists K < G/H$ con $\pi^{-1}(K) = \langle g \rangle$. Aplicamos π para ver que (por sobreyectividad), se tiene: $K = \pi(\langle g \rangle) = \langle \overline{g} \rangle = Im(\alpha_p)$ y por tanto $\langle g \rangle = \pi^{-1}(Im(\alpha_p)) = G$ y es cíclico. □

El recíproco de este lema es inmediato. Ahora vamos a tratar de partir un p-grupo abeliano en uno cíclico y otro cualquiera, más pequeños, con el fin de que, reiterando este procedimiento, el subgrupo resultante que a priori no es cíclico verifique las hipótesis del lema previo y podamos afirmar que todos los trozos son cíclicos.

Lema 5. *Sea G un p-grupo abeliano, con $|G| = p^n$ y sea $p^e = \text{máx}\{o(g) : g \in G\} \geq p$. Entonces $\exists C < G$, $K < G$ con C cíclico, $|C| = p^e$ y tal que $C + K = G$ y $C \cap K = \{e\}$, es decir, $G = C \times K$.*

Demostración. Por inducción en n. Si $|G| = p$, está claro que $G = \langle g \rangle \times \{e\}$ con $g \in G$ no trivial. Ahora, si $n \geq 2$, y G no es cíclico (puesto que de serlo hemos acabado), sea $g \in G$ con $o(g) = p^e$. Sea $C = \langle g \rangle$. Como es cíclico, $\exists! H < C$ con $|H| = p$. Como G no es cíclico, debe haber otro $H' \neq H$ con $|H'| = p$. Si consideramos $\pi : G \to G/H'$ el natural, entonces $C \simeq \pi(C)$ dado que $Nuc(\pi|_C) = H' \cap C = \{e\}$ porque si no se tendría $H' < C$ contradiciendo el Lema 3. Por lo tanto $|\pi(C)| = p^e$ luego como $\pi(C) = \langle \overline{g} \rangle$, tenemos que $\text{máx}\{o(g) : g \in G/H'\} = p^e$ (recordemos que no puede haber elementos en G/H' que superen en orden a los de G, dado que $o(\pi(g))|o(g)$). Es decir, G/H' entra en las hipótesis del lema y, por inducción, tenemos que $G/H' \simeq \pi(C) \times \overline{K}$ para cierto $\overline{K} \subset G/H'$ (dado que el cíclico de orden p^e que daría el lema es isomorfo a $\pi(C)$).

A continuación definimos $C' = \pi^{-1}(\pi(C))$ y $K = \pi^{-1}(\overline{K})$ que, dado que $\pi(C) \cap \overline{K} = \{e\}$ y $\pi(C) + \overline{K} = G/H'$, sabemos que se tiene $C' \cap K = H'$ y $C' + K = G$. Recordemos por ser $\pi(C)$ las clases de los elementos de C en el cociente G/H, entonces $C' = C + H'$, luego como $H' < K$ (es preimagen por π que tiene núcleo H'), tenemos que $C + K = C + H' + K = C' + K = G$ y por otro lado, como $C \cap K < C' \cap K = H'$, entonces $C \cap K = C \cap K \cap H' = C \cap H' = \{e\}$. Por tanto C y K son los grupos buscados. □

Teorema 15. *Si G es un p-grupo abeliano finito, entonces $\exists a_1 \geq a_2 \geq \cdots \geq a_s \geq 1$ tales que*

$$G \simeq \mathbb{Z}/p^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_s}\mathbb{Z}.$$

Además, tanto s como $a_1, \ldots, a_s$ están bien definidos, es decir, no hay otra descomposición de este tipo con distinto valor de s o distintos valores de a_i.

Demostración. Por inducción en n si $|G| = p^n$. Está claro que $|G| \simeq \mathbb{Z}/p\mathbb{Z}$ si $n = 1$. Ahora, si $n \geq 1$, sabemos por el lema previo que $G \simeq \mathbb{Z}/p^e\mathbb{Z} \times K$ con $p^e \geq p$. Si $|K| = 1$ hemos acabado, y si no, es un p-grupo abeliano finito de orden $|K| = p^m$ con $m < n$ luego se aplica la hipótesis de inducción y hemos acabado.

Ahora falta ver que la expresión está bien definida. Supongamos que $G \simeq \mathbb{Z}/p^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_s}\mathbb{Z} \simeq \mathbb{Z}/p^{b_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{b_r}\mathbb{Z}$ para ciertos r, s y $a_1 \geq \cdots \geq a_s \geq 1$ y $b_1 \geq \cdots \geq b_r \geq 1$. Vamos a ver que entonces $r = s$ y $a_i = b_i$ en todo i. Para ello consideramos el morfismo $\alpha_p : G \to G$ con $\alpha_p(g) = pg$. Si vemos los elementos de G como en la primera expresión, entonces $\alpha_p(g_1, \ldots, g_s) = (pg_1, \ldots, pg_s) = 0 \iff \forall i\ pg_i = 0 \iff \forall i\ o(g_i)|p$ luego $Nuc(\alpha_p) = \left\langle p^{a_1-1} \right\rangle \times \cdots \times \left\langle p^{a_s-1} \right\rangle$, dado que cada $\left\langle p^{a_i-1} \right\rangle$ es el subgrupo de elementos de $\mathbb{Z}/p^{a_i}\mathbb{Z}$ de orden p, puesto que al ser cíclico, solo hay un subgrupo de orden p (y es ese). Esto nos dice que $|Nuc(\alpha_p)| = p^r$. Aplicando la misma lógica pero viendo a G como en su segunda expresión, sigue que $|Nuc(\alpha_p)| = p^s$, de donde $r = s$.

Para la unicidad de cada exponente, veamos que cada $Im(\alpha_p) = \langle p \rangle$ en cada uno de los $\mathbb{Z}/p^{a_i}\mathbb{Z}$, dado que sabemos tiene p^{a_i-1} elementos por el teorema de isomorfía. Una observación similar a la anterior nos permite darnos cuenta de que $Im(\alpha_p) = \langle p \rangle \times \langle p \rangle \times \cdots \times \langle p \rangle$, es decir, que $Im(\alpha_p) \simeq \mathbb{Z}/p^{a_1-1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{a_{s'}-1}\mathbb{Z} \simeq \mathbb{Z}/p^{b_1-1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p^{b_{r'}-1}\mathbb{Z}$, donde s' y r' están tomados para que no haya elementos nulos, es decir, que $a_i \geq 2$ si $i \leq s'$, así como que $b_i \geq 2$ si $i \leq r'$, y son los más grandes que lo cumplen. Por lo que hemos visto anteriormente pero aplicado a estas imágenes, que son p-grupos, debe ser que $s' = r'$, luego sabemos que $a_j = b_j = 1$ para todo $j > s'$. Ahora basta con repetir inductivamente el argumento con este p-grupo $(Im(\alpha_p))$, de modo que iremos reduciendo el número de grupos cíclicos que forman la expresión, y estableciendo la igualdad de los exponentes que se desvanecen en cada paso. □

2. Anillos

Definición 31. Sea $A \neq \emptyset$ dotado de 2 operaciones binarias, $+ : A \times A \to A$ y $\cdot : A \times A \to A$ tales que:

1. $(A, +)$ es un grupo abeliano.
2. La operación $\cdot$ es asociativa.
3. $\forall a, b, c \in A$ vale la **propiedad distributiva** por ambos lados, es decir:
   3.1. $a \cdot (b + c) = a \cdot b + a \cdot c$
   3.2. $(b + c) \cdot a = b \cdot a + c \cdot a$

Entonces la terna $(A, +, \cdot)$ se denomina **anillo**.

Denotaremos al neutro de $(A, +)$ como 0, y $a \cdot b \equiv ab$. Asimismo, el inverso de $a \in A$ en $(A, +)$ se denotará $-a$ y se denominará **inverso aditivo**. Un ejemplo de anillo son las matrices reales de $n \times n$ con las operaciones usuales.

Proposición 62. *En un anillo $(A, +, \cdot)$ se tiene que $\forall a \in A$, se verifica $0a = 0$.*

Demostración. $0a + 0a = (0 + 0)a = 0a$ y aplicando la propiedad cancelativa del grupo $(A, +)$, sigue que $0a = 0$. □

Definición 32. Un anillo $(A, +, \cdot)$ es **conmutativo** si $\forall a, b \in A$, se tiene $ab = ba$.
Una anillo es **unitario** si $\exists e \in A$ tal que $\forall a \in A$ se tiene $ea = ae = a$.

Proposición 63. *En un anillo unitario A, $\exists! e \in A$ tal que $\forall a \in A$ se tiene $ea = ae = a$.*

Demostración. La existencia es por definición, y la unicidad es porque si $e' \in A$ verifica esa propiedad, entonces $e'e = e'$ (por la propiedad de e) y $e'e = e$ (por la propiedad de e'), de tal modo que $e = e'$. □

Ese elemento característico de los anillos unitarios se denota generalmente por 1.

En lo que sigue se usará el término **anillo** para hablar de **anillos conmutativos unitarios**.

Proposición 64. *Si A es un anillo tal que $1 = 0$, entonces $A = \{0\}$.*

Demostración. Dado $a \in A$, tenemos que $0 = 0a = 1a = a$. □

Si bien el 1 actúa como *neutro para el producto*, la definición de anillo en ningún momento exige la existencia de inversos multiplicativos. Los elementos que posean dichos inversos serán de relevante importancia:

Definición 33. Si $(A, +, \cdot)$ es un anillo, se define el conjunto $\mathcal{U}(A) = \{a \in A : \exists b \in A : ab = ba = 1\}$, y se denomina conjunto de **unidades de** A.

Proposición 65. *Si $a \in \mathcal{U}(A)$, entonces, $\exists! b \in A$ tal que $ab = ba = 1$. Asimismo, $b \in \mathcal{U}(A)$. Si a este elemento lo denotamos $b \equiv a^{-1}$, entonces $(a^{-1})^{-1} = a$.*

Demostración. Supuesto que $b' \in A$ también verifique $ab = ba = 1$, entonces $ab = ab'$, y por tanto $bab = bab' \implies 1b = 1b' \implies b = b'$. Como $ab = ba = 1$, sigue inmediatamente que $b^{-1} = a$ y que $b \in \mathcal{U}(A)$. □

Observación 15. Dado el anillo $(A, +, \cdot)$, se tiene que $(\mathcal{U}(A), \cdot)$ es un grupo. Si el anillo es conmutativo, es abeliano.

Esto es porque sabemos que se verifica asociatividad por ser A anillo, el $1 \in \mathcal{U}(A)$ (porque $1 \cdot 1 = 1$) es neutro, y por definición de $\mathcal{U}(A)$, cada elemento tiene inverso.

Definición 34. Dado el anillo $(A,+,\cdot)$, se dice que $A' \subset A$ es un **subanillo** si $(A', +|_{A'\times A'}, \cdot|_{A'\times A'})$ es anillo y cerrado por $+$ y $\cdot$. Si A es unitario pediremos asimismo que $1 \in A'$.

Definición 35. Si A y B son anillos, $f : A \to B$ es un **homomorfismo de anillos** si $\forall a, a' \in A$ se verifica:

1. $f(a+a') = f(a) + f(a')$.
2. $f(aa') = f(a)f(a')$.
3. $f(1_A) = 1_B$.

Proposición 66 (Algunas propiedades habituales)**.** *Si $f : A \to B$ y $g : B \to C$ son homomorfismos de anillos, entonces $g \circ f : A \to C$ también lo es. Si $f : A \to B$ es un homomorfismo de anillos biyectivo, entonces $f^{-1} : B \to A$ también lo es.*

La demostración es análoga al caso de los grupos en ambas situaciones.

Definición 36. El homomorfismo de anillos $f : A \to B$ se denomina **isomorfismo** si $\exists g : B \to A$ homomorfismo tal que $f \circ g = Id_B$ y $g \circ f = Id_A$. En virtud de la proposición anterior, es equivalente pedir que f sea homomorfismo y biyectivo.

Los anillos $(A,+,\cdot)$ y $(B,+,\cdot)$ son **isomorfos**, y se denota $A \simeq B$, si $\exists f : A \to B$ isomorfismo.

Observación 16. El único homorfismo de anillos $h : \mathbb{Z} \to \mathbb{Z}$ es la identidad. Esto es porque como $h(1) = 1$, y sabemos que en particular es homomorfismo de grupos, entonces $h(k) = h(k \times 1) = k \times h(1) = k \times 1 = k$.

Observación 17. $h : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ es homomorfismo de anillos $\iff$ h verifica $h(\overline{k}) = \overline{\overline{k}}$ y $m|n$.

Demostración. Para $\implies$, veamos que como $h(\overline{1}) = \overline{\overline{1}}$, ha de verificarse que $o(\overline{\overline{1}})|o(\overline{1})$ en tanto grupo, es decir que $m|n$. Además $h(\overline{k}) = h(k\overline{1}) = k\overline{\overline{1}} = \overline{\overline{k}}$.

Para $\impliedby$, sabemos que una aplicación así formada (que envía el $\overline{1}$ a un elemento de orden que divida a n) es homomorfismo de grupos. Además es inmediato comprobar la compatibilidad con el producto y que envía el 1 en el 1. □

Es decir, únicamente hay 1 homomorfismo de anillos en caso de que $m|n$, y ninguno en caso contrario.

Proposición 67. *Si $f : A \to B$ es un homomorfismo de anillos, entonces $Im(f)$ es subanillo de B.*

Demostración. Ya sabemos que $(Im(f),+)$ es grupo. Como $f(1) = 1$, entonces $1 \in Im(f)$. Además $f(a)f(b) \in Im(f)$ al ser $f(ab)$. □

Definición 37. Dados $(A,+,\cdot)$ y $(B,+,\cdot)$ anillos, se define un nuevo anillo, el **producto directo**, por $A \times B$, bajo las operaciones $(a,b) + (a',b') = (a+a', b+b')$ y $(a,b)(a'b') = (aa', bb')$.

Es fácil comprobar que es un anillo y que la proyección $\pi_A : A \times B \to A$ dada por $\pi(a,b) = a$ es homomorfismo, así como la equivalente natural π_B.

Observación 18. Se tiene que $\mathcal{U}(A \times B) = \mathcal{U}(A) \times \mathcal{U}(B)$.

Esto es así porque si $(a,b) \in \mathcal{U}(A \times B)$, entonces $\exists (a',b')$ con $(a,b)(a',b') = (1,1)$. Pero esto indica que $aa' = 1$ y $bb' = 1$ luego $a \in \mathcal{U}(A)$ y $b \in \mathcal{U}(B)$. El recíproco funciona de la misma manera. □

Proposición 68. *Si $\alpha : H \to A$ es homomorfismo de anillos, y $\beta : H \to B$ es otro homomorfismo, entonces $H \to A \times B$ dado por $h \to (\alpha(h), \beta(h))$ también es homomorfismo de anillos.*

Demostración. $1 \to (1,1)$, $h+h' \to (\alpha(h+h'), \beta(h+h')) = (\alpha(h)+\alpha(h'), \beta(h)+\beta(h')) = (\alpha(h), \beta(h)) + (\alpha(h'), \beta(h'))$, y $hh' \to (\alpha(hh'), \beta(hh')) = (\alpha(h)\alpha(h'), \beta(h)\beta(h')) = (\alpha(h), \beta(h))(\alpha(h'), \beta(h'))$. □

Observación 19 (Una aplicación: Número de unidades). Vamos a calcular cuántas unidades hay en $\mathbb{Z}/n\mathbb{Z}$. Pongamos que $n = p_1^{a_1} \dots p_r^{a_r}$ primos distintos. Como cada $p_j^{a_j} | n$, damos los únicos morfismos de anillos $\alpha_j : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/p_j^{a_j}\mathbb{Z}$, que recordemos verifican $\alpha_j(1) = 1$. Esto nos permite dar el homomorfismo de anillos:

$$\alpha : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{a_r}\mathbb{Z}.$$

Dado por $\alpha(1) = (1, 1, \dots, 1)$. Sabemos además que $o(1, 1, \dots, 1) = mcm(p_1^{a_1}, \dots, p_r^{a_r}) = n$ por ser primos distintos. Es decir, que $Im(\alpha) = \langle (1, 1, \dots, 1) \rangle = \mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{a_r}\mathbb{Z}$. Pero entonces, como ambos conjuntos tienen el mismo número de elementos, α es una biyección y por tanto un isomorfismo de anillos. Esto quiere decir que ambos anillos son isomorfos y tienen el mismo número de unidades.

Por tanto $\varphi(n) = |\mathcal{U}(\mathbb{Z}/n\mathbb{Z})| = |\mathcal{U}(\mathbb{Z}/p_1^{a_1}\mathbb{Z} \times \cdots \times \mathbb{Z}/p_r^{a_r}\mathbb{Z})| = |\mathcal{U}(\mathbb{Z}/p_1^{a_1}\mathbb{Z}) \times \cdots \times \mathcal{U}(\mathbb{Z}/p_r^{a_r})| = \prod_1^r |\mathcal{U}(\mathbb{Z}/p_i^{a_i}\mathbb{Z})|$.

Esto nos indica entonces que $\varphi(n) = \prod_1^r \varphi(p_i^{a_i})$. Un argumento similar sirve para ver que si $n = ab$ con a, b coprimos, entonces $\varphi(ab) = \varphi(a)\varphi(b)$. Volviendo al problema principal, solo hay que darse cuenta de que $\varphi(p_i^{a_i})$ es el número de enteros hasta $p_i^{a_i}$ que no son múltiplos de p_i. Es decir, todos excepto los de la forma kp_i, donde $k \in \{1, \dots, p^{a_i - 1}\}$, dado que si k es mayor, el número supera a $p_i^{a_i}$.

Por lo tanto, $\varphi(p_i^{a_i}) = p_i^{a_i} - p_i^{a_i - 1}$, y por tanto:

$$\varphi(n) = |\mathcal{U}(\mathbb{Z}/n\mathbb{Z})| = \prod_{i=1}^{r} \left(p_i^{a_i} - p_i^{a_i - 1}\right).$$

Definición 38 (Anillo de polinomios)**.** Dado A un anillo, se define el conjunto $A[X] = \bigcup_{r=0}^{\infty} \{a_0 + a_1 X + \cdots + a_r X^r : a_0, \dots, a_r \in A\}$ con las operaciones suma y producto habituales. Dicho $A[X]$ es un anillo.

Observación 20. En un anillo, si $1 \neq 0$, entonces $0 \notin \mathcal{U}(A)$. Esto es así dado que $0b = 0 \neq 1$ sin importar $b \in A$.

Definición 39. El anillo A es un **cuerpo** si $\mathcal{U}(A) = A \backslash \{0\}$.

Proposición 69. *Si $u \in \mathcal{U}(A)$, entonces $ua = ub \implies a = b$.*

Demostración. Basta con multiplicar a izquierda por u^{-1}. □

En particular, en todo cuerpo vale la propiedad cancelativa del producto (siempre y cuando no sea nulo el elemento).

Definición 40. El elemento $a \in A$, $a \neq 0$ es **divisor de cero** si $\exists b \in A$, $b \neq 0$, tal que $ab = 0$.

Por ejemplo en $\mathbb{Z}/4\mathbb{Z}$, tenemos que $\overline{2} \cdot \overline{2} = \overline{0}$. El $\overline{2}$ es un divisor de cero.

Proposición 70. *Un cuerpo A no tiene divisores de 0.*

Demostración. Si $a \neq 0$ y $ab = 0$, entonces $ab = a0$ y por la cancelativa, $b = 0$. □

Definición 41. El anillo A es un **dominio** si no tiene divisores de cero, es decir, si $\forall a, b \in A$, $a \neq 0$ y $b \neq 0$, se tiene $ab \neq 0$.

Por ejemplo, $\mathbb{Z}$ es un dominio a pesar de no ser un cuerpo.

Proposición 71. *Si $a \in A$ no es divisor de cero y $a \neq 0$, entonces se tiene $ab = ac \implies b = c$, $\forall b, c \in A$.*

Demostración. Tenemos, si $ab = ac$, que $a(b - c) = 0$, pero como a no es divisor de cero, entonces $b - c = 0$ luego $b = c$. □

En particular, en todo dominio vale la propiedad cancelativa del producto siempre y cuando no sea nulo el elemento.

Proposición 72. *Si el anillo A es finito, entonces A es dominio $\iff$ A es cuerpo.*

Demostración. $\impliedby$ ocurre siempre, como hemos visto previamente. Por otro lado, si A es un dominio, esto indica que, fijado $a \in A$ no nulo, la aplicación $h_a : A \to A$ dada por $h_a(b) = ab$ es inyectiva. Efectivamente, si $ab = ac$, como A es dominio, vale la propiedad cancelativa y $b = c$. Pero eso quiere decir que es una biyección entre A y A, por ser A finito, de tal modo que $\exists b \in A$ tal que $h_a(b) = 1$ y por tanto $a \in \mathcal{U}(A)$. □

Proposición 73. *Si A es un dominio, el anillo $A[X]$ es un dominio.*

Demostración. Dados dos polinomios no nulos, podemos expresarlos $P(X) = \sum_{i=0}^{r} a_i X_i$ y $Q(X) = \sum_{i=0}^{s} b_i X^i$ donde $a_r \neq 0$ y $b_s \neq 0$. Pero entonces el coeficiente de X^{r+s} en $P(X)Q(X)$ es $a_r b_s$, y como $a_r \neq 0$, $b_s \neq 0$ y A es un dominio, se sigue que $a_r b_s \neq 0$ y el polinomio producto es no nulo. □

Definición 42. Si A es dominio y $f(X) \in A[X]$ es no nulo, es decir, se expresa como $f(X) = \sum_{i=0}^{r} a_i X_i$, con $a_r \neq 0$, definimos su **grado** por $Gr(f(X)) = r$.

Observación 21. Si $P(X)$ y $Q(X)$ son no nulos en $A[X]$ con A un dominio, entonces $Gr(P(X)Q(X)) = Gr(P(X)) + Gr(Q(X))$.

2.1. Cocientes e ideales

Con el fin de definir correctamente anillos cociente y generar nuevos anillos a partir de otros, definimos:

Definición 43. Dado el anillo $(A, +, \cdot)$, el subconjunto $I \subset A$ es un **ideal** si:

1. $(I, +) < (A, +)$.
2. $\forall a \in A$ y $f \in I$, se tiene $af \in I$.

Obsérvese que la segunda condición no solo pide que sea cerrado por el producto, sino que además todo elemento del anillo dejar invariante al ideal. Por ejemplo, en $\mathbb{Z}$, tenemos que los subgrupos son los de la forma $k\mathbb{Z}$, y es fácil ver que todos ellos son ideales: si tomamos $k' \in \mathbb{Z}$ y $ka \in k\mathbb{Z}$, el valor $k'ka = k(k'a)$ está en $k\mathbb{Z}$.

Todo anillo A admite los ideales $\{0\}$ y A. Cabe observar que un ideal no tiene por qué ser un subanillo, dado que estamos exigiendo que el 1 esté en el subanillo, pero no tiene por qué pertenecer a un ideal (como profundizaremos en la proposición siguiente). Si no consideramos esto, sí que es cerrado bajo suma y producto trivialmente (por ello, algunos autores lo consideran subanillo).

Proposición 74 (Caracterización de Ideales Propios)**.** *Dado I un ideal de A, se tiene:*

$$I = A \iff 1 \in I \iff I \cap \mathcal{U}(A) \neq \emptyset$$

es decir, $I \subsetneq A \iff 1 \notin I \iff I \cap \mathcal{U}(A) = \emptyset$.

Demostración. Si $I = A$ es evidente que $1 \in I$. Si $1 \in I$, entonces $1 \in I \cap \mathcal{U}(A)$ y por tanto es no vacío. Finalmente, dado $a \in I \cap \mathcal{U}(A) \neq \emptyset$, nos damos $b \in A$ y entonces, como $a \in I$, y $ba^{-1} \in A$, tenemos que $b = (ba^{-1})a \in I$. □

Definición 44. Dado el anillo A y un ideal $I \subset A$, definimos el **anillo cociente** como A/I el conjunto de clases de equivalencia bajo la relación $a \sim b \iff a - b \in I$, o, lo que es lo mismo, los elementos de la forma $\{a + I\}_{a \in A}$, dotado de la operación de grupo: $(a + I) + (b + I) = (a + b) + I$, y de la siguiente operación producto: $(a + I)(b + I) = (ab + I)$.

Ya sabemos que, como A es un grupo e I es un subgrupo normal (A es abeliano), entonces ese conjunto, relación y operación están bien definidas. Basta ver que la operación producto lo está. Dado $a' \in a+I$ y $b' \in b+I$, con $a' = a+i$ y $b' = b+j$ con $i, j \in I$, tenemos que $a'b' = ab+aj+bi+ij$, y como I es ideal, $aj+bi+ij \in I$ luego $a'b' \in ab+I$. Es decir, independientemente de los representantes a', b' tomados, el resultado es la clase $ab+I$, luego está bien definida. Lo que estamos diciendo es que:

Observación 22. $\pi : A \to A/I$ es homomorfismo de anillos bajo las operaciones definidas anteriormente. Esto es así porque además $\pi(1) = 1+I$ verifica $(1+I)(a+I) = 1a+I = a+I$ luego es neutro multiplicativo.

Conviene que $I \neq A$, es decir, que sea propio, para que el anillo resultante no sea trivial (y por tanto $1+I \neq 0+I$).

Vimos con anterioridad que la imagen de un homomorfismo de anillos es un subanillo. Se tiene también lo siguiente:

Proposición 75. *Dado $\alpha : A \to B$ un homomorfismo de anillos, se tiene que $Nuc(\alpha)$ es un ideal.*

Demostración. Ya sabemos que es un subgrupo por ser el homomorfismo de anillos también de grupos. Por otro lado, si $a \in Nuc(\alpha)$ y damos $b \in A$, tenemos que $\alpha(ab) = 0\alpha(b) = 0$. □

Definición 45 (Ideal Generado)**.** Dado el conjunto $C = \{f_1, \ldots, f_r\} \subset A$, definimos el **ideal generado por** C como $\langle C\rangle = \{\sum_{i=1}^{r} a_i f_i : a_1, \ldots, a_r \in A\}$.

Proposición 76. *Se tiene, si C es un conjunto en el anillo A, que:*

1. $C \subset \langle C\rangle$
2. $\langle C\rangle$ *es ideal.*
3. *Dado otro ideal J con $C \subset J$, entonces $\langle C\rangle \subset J$.*

Demostración. 1 es trivial asignando uno de los coeficientes a 1 y el resto a 0. Para 2, tenemos que $\sum_j 0f_j = 0 \in \langle C\rangle$, también $\sum_j a_j f_j + \sum_j b_j f_j = \sum_j (a_j+b_j) f_j \in \langle C\rangle$, y además $\sum_j -a_j f_j = -\sum_j a_j f_j$ luego es subgrupo. Dado $c \in A$ tenemos que $c\sum_j a_j f_j = \sum_j c a_j f_j$ luego es ideal. Para 3, veamos que como J es ideal, se tiene por definición que toda combinación $\sum a_j f_j \in J$, como se quería. □

Definición 46. Un ideal es **principal** si es generado por un único elemento, es decir, si es de la forma $I = \langle f\rangle = \{af : a \in A\}$.

El siguiente resultado nos permite generar ideales propios:

Proposición 77. *Se tiene que $f \in \mathcal{U}(A) \iff \langle f\rangle = A$.*

Demostración. $\Longrightarrow$ ya está visto: como $f \in \langle f\rangle \cap \mathcal{U}(A)$, sigue que $\langle f\rangle = A$. Para $\Longleftarrow$, si $\langle f\rangle = A$, entonces $1 \in \langle f\rangle$, o lo que es lo mismo, $\exists a \in A$ tal que $af = 1$. □

Proposición 78. *A es un cuerpo $\iff$ el retículo de ideales de A es el trivial (es decir, solo admite los ideales A y $\{0\}$)*

Demostración. $\Longrightarrow$. Dado J un ideal no nulo, tomamos $a \in J$ no nulo. Como $\langle a\rangle \subset J$, y $a \in \mathcal{U}(A)$ al ser cuerpo, entonces $\langle a\rangle = A$, es decir, $A \subset J$ y por tanto $J = A$. Para $\Longleftarrow$, tenemos que si no fuese un cuerpo, tomamos $a \in A$ no nulo ni unidad y por el resultado anterior $\langle a\rangle \subsetneq A$ y no es trivial.

2.1.1. Isomorfía de anillos

Vamos a probar los teoremas de isomorfía en anillos. Requerimos el siguiente lema previo:

Lema 6. *Si I es un ideal de A, y J es otro ideal que verifica $I \subset J$, tenemos que el subgrupo $J/I < A/I$ es un ideal del anillo A/I.*

Demostración. Ya sabemos que $(J/I,+) < (A/I,+)$ de teoría de grupos (es $\pi(J)$), luego queda ver que dado $(a+I) \in A/I$ y $(b+I) \in J/I$, su producto sigue en J/I. Pero $(a+I)(b+I) = (ab+I)$, y como $ab \in J$ por ser J ideal, $a \in A$ y $b \in J$, tenemos que $ab+I \in J/I$. □

Podemos enunciar el habitual primer lema de isomorfía:

Teorema 16. *Sea $\alpha : A \to B$ homomorfismo de anillos sobreyectivo. Sea $I \subset A$ un ideal con $I \subset Nuc(\alpha)$. Entonces, $\exists \overline{\alpha} : A/I \to B$, homomorfismo de anillos, dado por $\overline{\alpha}(a+I) = \alpha(a)$, bien definido, tal que:*

1. *$\overline{\alpha} \circ \pi = \alpha$, donde $\pi : A \to A/I$ es el natural.*
2. *$Nuc(\overline{\alpha}) = Nuc(\alpha)/I$.*
3. *$\overline{\alpha}$ es sobreyectiva.*

Demostración. Está bien definida dado que si $a+I = b+I$, entonces es porque $b = a+i$, con $i \in I$, luego $\alpha(b) = \alpha(a+i) = \alpha(a)+\alpha(i) = \alpha(a)$ dado que $I \subset Nuc(\alpha)$. Que $\overline{\alpha}$ es homomorfismo de anillos sigue de que $\overline{\alpha}((a+I)(b+I)) = \overline{\alpha}(ab+I) = \alpha(ab)$, y $\overline{\alpha}(1+I) = \alpha(1) = 1$ (y ya sabemos de la parte de grupos que es homomorfismo de grupos). El punto (1) se tiene de inmediato dado que $\overline{\alpha}(\pi(a)) = \overline{\alpha}(a+I) = \alpha(a)$. Se tiene $\overline{a} \in Nuc(\overline{\alpha}) \iff 0 = \overline{\alpha}(\overline{a}) = \alpha(a)$ luego hace falta que $a \in Nuc(\alpha)$ pero esto ocurre $\iff$ $\overline{a} \in Nuc(\alpha)/I$. Finalmente, como $\alpha = \overline{\alpha} \circ \pi$ y tanto α como π son sobreyectivas, ha de serlo $\overline{\alpha}$. □

Lo que nos lleva al teorema de isomorfía:

Teorema 17 (1^o de isomorfía)**.** *Sea $\alpha : A \to B$ un homomorfismo de anillos. Entonces $A/Nuc(\alpha) \simeq Im(B)$.*

Demostración. Aplicamos el lema de isomorfía previo a $\alpha : A \to Im(\alpha)$ que es homomorfismo de anillos al ser $Im(\alpha)$ anillo, y para el ideal $I = Nuc(\alpha)$. Esto nos da $\overline{\alpha} : A/Nuc(\alpha) \to Im(\alpha)$ homomorfismo sobreyectivo de anillos, con $Nuc(\overline{\alpha}) = Nuc(\alpha)/Nuc(\alpha) \simeq \{0\}$, luego como $\overline{\alpha}$ es en particular homomorfismo de grupos, es también inyectivo y se tiene el isomorfismo. □

Otro importante resultado de teoría de grupos era la identificación, dado $f : A \to B$ homomorfismo sobreyectivo, entre el retículo de B y el de subgrupos de A que contienen al núcleo. Un resultado similar se tiene en teoría de anillos:

Proposición 79. *Sea A un anillo y sea $I \subset A$ un ideal. Existe una identificación biyectiva entre el retículo de ideales de A/I y el subretículo de ideales de A que contienen a I. Esta identificación viene dada por π^{-1} (es decir, tomar la preimagen del ideal por π da el ideal asociado), es biyectiva y preserva las inclusiones.*

Demostración. Dado $\overline{J} \in A/I$ ideal, veamos que $J = \pi^{-1}(\overline{J})$ es un ideal de A que contiene al núcleo. Como $0 \in \overline{J}$, está claro que $Nuc(\pi) \subset J$. Para ver que es un ideal, construimos la aplicación $\tilde{\pi} : A/I \to (A/I)/\overline{J}$, y entonces $Nuc(\tilde{\pi} \circ \pi) = \pi^{-1}(\overline{J})$ luego es ideal. Si $\overline{J} \subset \overline{J}'$, se tiene $\pi^{-1}(\overline{J}) \subset \pi^{-1}(\overline{J}')$, preservando además la inclusión estricta si lo fuese, al ser sobreyectivo. Finalmente hay que ver que dado un ideal $J \subset A$ tal que $I \subset J$, existe un ideal de A/I que va a parar a él. Se afirma que tal ideal es J/I. Está claro que $J \subset \pi^{-1}(J/I)$, dado que si $a \in J$, entonces $\pi(a) \in J/I$ por definición de J/I. Para la inclusión opuesta, dado $b \in \pi^{-1}(J/I)$, se tiene que la clase $b+I \in J/I$, es decir, $\exists a \in J$ tal que $b+I = a+I$, de donde $b-a \in I$ luego $b = a+i$, con $i \in I$, $a \in J$, lo que indica que $b \in J$ y hemos

acabado. □

Como vemos, esto nos permite dado un homomorfismo cualquiera de anillos sobreyectivo $f : A \to B$, identificar el retículo de ideales de B con el de ideales de A que contienen a $Nuc(f)$, dado que $B \simeq A/Nuc(f)$.

Teorema 18 (2º de isomorfía)**.** *Sean $I \subset J \subset A$ ideales. Sabemos que $J/I \subset A/I$ es ideal. Se tiene que $(A/I)/(J/I) \simeq A/J$*

Demostración. Sabemos $\pi : A \to A/J$ es sobreyectivo con $Nuc(\pi) = J$, luego $I \subset Nuc(\pi)$. El lema de isomorfía nos indica que $\exists \overline{\pi} : A/I \to A/J$ sobreyectivo tal que $Nuc(\overline{\pi}) = Nuc(\pi)/I = J/I$. Aplicando el primer teorema de isomorfía a $\overline{\pi}$, se tiene finalmente que $(A/I)/(J/I) \simeq A/J$. □

Definición 47. Sea $I \subset A$ un ideal propio. Se dice que I es **maximal** si A/I es un cuerpo.

Obsérvese que esto es lo mismo que pedir que no existan ideales entre I y A, dado que si A/I es cuerpo, su retículo solo consta de $\{0\}$ y A/I, y a través de la identificación mencionada anteriormente, tenemos únicamente los ideales I y A que contienen a I.

Definición 48. Sea $I \subset A$ un ideal propio. Se dice que I es **primo** si A/I es un dominio.

Por lo que sabemos, si I es maximal también será primo. Los ideales primos se pueden interpretar como aquellos tales que si $a, b \notin I$, entonces $ab \notin I$.

Proposición 80. *Sea $I \subset A$. En la identificación entre el retículo de ideales de A/I y el de ideales de A que contienen a I, dada por tomar la preimagen por π, se preserva la primalidad y la maximalidad. Es decir, $\overline{J} \in A/I$ es maximal (resp. primo) $\iff$ $\pi^{-1}(\overline{J}) \in A$ es maximal (resp. primo).*

Demostración. Dado un ideal $J \in A$ sabemos que su correspondiente es $J/I \in A/I$ (vimos que $\pi^{-1}(J/I) = J$ en la demostración de la identificación de retículos). No obstante, $A/J \simeq (A/I)/(J/I)$, luego se tiene lo que se quería. (Por ejemplo, si J es maximal, $A/J \simeq (A/I)/(J/I)$ es cuerpo y por tanto J/I es maximal. La clave está en que los dos cocientes de la definición de primo/maximal de cada uno son isomorfos). □

Definición 49. Sea D un dominio. Dados $f, g \in D$, se dice que f **divide a** g si $g = af$ para algún $a \in D$.

Proposición 81. *Dados $f_1, f_2 \in D$ elementos no nulos de un dominio, se tiene que $\langle f_1 \rangle = \langle f_2 \rangle \iff f_1 = uf_2$ para un $u \in \mathcal{U}(D)$. En este caso se dice que f_1 y f_2 son **asociados**.*

Demostración. $\Longleftarrow$ es inmediato y no requiere que D sea un dominio: dado $a \in \langle f_1 \rangle$, tenemos que $a = bf_1$ y por tanto $a = buf_2 \in \langle f_2 \rangle$. Si $c \in \langle f_2 \rangle$, tenemos que $c = df_2 = du^{-1}f_1 \in \langle f_1 \rangle$. Para $\Longrightarrow$, tendríamos que $f_1 = af_2$ y $f_2 = bf_1$, con lo que $f_1 = abf_1$. Como en un dominio vale la propiedad cancelativa, sigue que $ab = 1$ luego el $a \in \mathcal{U}(D)$. □

Definición 50. Sea D un dominio, $f \in D$ no nulo y no unidad. Se dice que **f es irreducible** si $f = f_1 f_2 \implies f_1$ o f_2 es unidad. Es decir, si toda vez que descomponga como producto de dos elementos, alguno sea unidad.

Un elemento $f \in D$ no nulo y no unidad es **reducible** si $\exists f_1, f_2 \notin \mathcal{U}(D)$ tales que $f_1 f_2 = f$, es decir, si descompone como producto de dos elementos no unidad.

Proposición 82 (Caracterización de irreducibles en términos de ideales)**.** *Sea $f \in D$ con D dominio, f no nulo y no unidad. Se tiene f irreducible $\iff \nexists f_1 \in D$ con $\langle f \rangle \subsetneq \langle f_1 \rangle \subsetneq D$.*

Demostración. $\implies$. Pongamos que $\langle f\rangle \subset \langle f_1\rangle \subsetneq D$. Entonces se puede expresar $f = af_1$. Como $\langle f_1\rangle \neq D$, sigue que f_1 no es unidad, luego por irreducibilidad debe darse que a sea unidad y por tanto $\langle f\rangle = \langle f_1\rangle$. Para $\impliedby$, si f fuese reducible, podríamos poner $f = f_1f_2$ no unidades, y por tanto $f \in \langle f_2\rangle \subsetneq D$, luego $\langle f\rangle \subset \langle f_2\rangle \subsetneq D$. Para ver que la inclusión es estricta, si se pudiese poner $f = uf_2$ con $u \in \mathcal{U}(D)$, seguiría por cancelativa que $u = f_1$ lo cual sabemos no ocurre. □

Definición 51. Sea $f \in D$ con D dominio tal que f es irreducible y $\langle f\rangle$ es primo. Entonces se dice que f **es primo**.

Definición 52. Sea D un dominio. Se dice que es un **dominio de factorización única** si $\forall a \in D$ con $a \neq 0$, $a \notin \mathcal{U}(D)$, se tiene una factorización $a = f_1 \dots f_r$ con cada f_i primo.

Proposición 83. *En un dominio de factorización única, si $a = f_1 \dots f_r = g_1 \dots g_s$, todos los f_i y g_i primos, entonces $r = s$ y además $f_i = u_ig_i$ para unidades $u_i \in \mathcal{U}(D)$, y cierta ordenación de los g.*

Demostración. Como $a \in \langle g_1\rangle$, que es un ideal primo, debe ser que algún $f_i \in \langle g_1\rangle$ (de no ser así, sabemos que su producto, que es a, estaría fuera del ideal primo $\langle g_1\rangle$). Sin perder generalidad sea f_1 tal elemento. Entonces $\langle f_1\rangle \subset \langle g_1\rangle$, pero como son irreducibles y g_1 no es unidad (lo que indica que $\langle g_1\rangle \subsetneq D$), debe darse que $\langle f_1\rangle = \langle g_1\rangle$. Es decir, $f_1 = u_1g_1$ para una unidad u_1. Pero entonces $a = f_1 \dots f_r = u_1^{-1}f_1g_2 \dots g_s$, luego $f_2 \dots f_r = u^{-1}g_2 \dots g_s$, donde $u^{-1}g_2$ es otro primo (su ideal principal es el mismo que el de g_2 luego sigue satisfaciendo la definición). Podemos continuar de esta manera, eliminando de uno en uno los factores y se tiene lo que se quería inductivamente. □

Definición 53. El dominio D es un **dominio de ideales principales** si todo ideal en D es principal.

Proposición 84. *En un dominio de ideales principales D, se tiene que f es irreducible $\iff$ $\langle f\rangle$ es maximal. Sigue que f irreducible $\implies$ f primo.*

Demostración. f irreducible $\iff \nexists f_1 : \langle f\rangle \subsetneq \langle f_1\rangle \subsetneq D \iff \nexists J$ ideal con $\langle f\rangle \subsetneq J \subsetneq D \iff \langle f\rangle$ es maximal. Hemos usado que todos los ideales son principales, luego que no exista un principal entre $\langle f\rangle$ y D equivale a que no exista ningún ideal entre ellos. □

Teorema 19. *Sea D un dominio de ideales principales. Entonces, todo elemento no nulo ni unidad se expresa como producto de irreducibles, y, en virtud de la proposición anterior, D es un dominio de factorización única.*

Observación 23. $\mathbb{Z}$ es un dominio de ideales principales. Dado un ideal no trivial $J \subset Z$, sabemos que $A = \{a \in J : a > 0\}$ es no vacío (porque el ideal no es el trivial). Sea $b = \min A$. Entonces $\langle b\rangle = J$. Que $\langle b\rangle \subset J$ es inmediato porque $b \in A$. Ahora, dado $a \in J$, lo expresamos mediante división euclídea como $a = bq + r$, con $0 \leq r < b$. Como $r = a - bq \in J$, debe ser que $r = 0$ (si no contradice la minimalidad de b), luego $a = bq \in \langle b\rangle$ y hemos acabado.

A continuación vamos a definir la característica de un anillo, para lo cual necesitamos la siguiente observación:

Observación 24. Sea A un anillo. La aplicación $h : \mathbb{Z} \to A$ dada por $h(n) = n \cdot 1_A = 1_A + \dots + 1_A$ n veces, es un homomorfismo de anillos (de hecho, el único). Es fácil comprobar que lo es, y, si hubiese otro, como $h(1) = 1_A$, sigue que esta sería su definición. Sabemos que $Nuc(h) = n\mathbb{Z}$ para algún $n \geq 0$ natural, dado que debe ser un ideal.

Definición 54. El anillo A tiene **característica** n si, siendo $h : \mathbb{Z} \to A$ es homomorfismo de la observación anterior, se tiene $Nuc(h) = n\mathbb{Z}$.

Proposición 85. *Si D es un dominio, entonces su característica es 0 o p un primo.*

Demostración. Todo subanillo de D es un dominio también, en particular $h(\mathbb{Z}) \simeq \mathbb{Z}/Nuc(h)$. Si D tiene característica n, entonces estamos diciendo que $\mathbb{Z}/n\mathbb{Z}$ es dominio, lo cual ocurre si $n = 0$ ($\mathbb{Z}$ es dominio), o si $n > 0$, ocurre si y solo si n es primo (dado que en anillos finitos como $\mathbb{Z}/n\mathbb{Z}$, dominio equivale a cuerpo). □

Vamos a seguir analizando los anillos de polinomios:

Proposición 86. *Si D es un dominio, se tiene $\mathcal{U}(D[X]) = \mathcal{U}(D)$.*

Demostración. Está claro que $\mathcal{U}(D) \subset \mathcal{U}(D[X])$. Para la otra inclusión, sea $g \in \mathcal{U}(D[X])$. Como D es dominio, la aplicación $gr : D\backslash\{0\} \to \mathbb{N} \cup \{0\}$ que da el grado de cada polinomio, está bien definida y $0 = gr(1) = gr(gg^{-1}) = gr(g) + gr(g^{-1})$, de donde sigue que $gr(g) = 0$, es decir $g \in \mathcal{U}(D)$. □

Esto nos indica que:

Observación 25. En $D[X]$, f es irreducible si $\nexists g_1, g_2$ tales que $f = g_1 g_2$ y $gr(g_1), gr(g_2) < gr(f)$, dado que es irreducible si en toda descomposición de este tipo hay una unidad (y por tanto uno tiene grado 0 y otro grado $gr(f)$).

Proposición 87. *Si K es un cuerpo, se tiene que $K[X]$ es un dominio de ideales principales.*

Demostración. Sea $I \subset K[X]$ un ideal. Si $I = \{0\}$ hemos acabado. Si no, sea $f \in I$ no nulo con grado mínimo (se puede escoger porque los grados son naturales). Está claro que $\langle f \rangle \subset I$. Dado $h \in I$, tenemos que como K es un cuerpo, vale la división euclídea en $K[X]$ (no vale en general), de tal forma que $h = fg + r$, con $gr(r) < gr(f)$ o bien $r = 0$. Como $r = h - fg \in I$, debe darse que $r \neq 0$ por minimalidad en el grado de f, de tal modo que $h = fg$, luego de hecho $I = \langle f \rangle$. □

Observación 26. Si K es cuerpo, en $K[X]$, $\langle f \rangle = \langle f' \rangle \iff f = uf'$, con $u \in K\backslash\{0\}$. Esto es así porque las unidades de $K[X]$ son las mismas que las de K, y por tanto los elementos no nulos (al ser cuerpo). Esto indica que **los ideales de $K[X]$ se pueden pensar como los generados por un polinomio mónico**, dado que serán principales, y además multiplicar por una constante no nula da lugar al mismo ideal.

Observación 27. En $K[X]$ todo polinomio de grado 1 es irreducible. Esto es así porque si $f \in K[X]$ es de grado 1 y $f = f_1 f_2$, debe ser $gr(f_1) + gr(f_2) = 1$ con lo que uno de ellos es 0 y por tanto es una unidad.

Proposición 88. *Sea $I = \langle a_1 X + a_0 \rangle = \langle X - \alpha \rangle$, con $\alpha = \frac{-a_0}{a_1}$. Este ideal son exactamente los polinomios $p(x) \in K[X]$ tales que $p(\alpha) = 0$.*

Demostración. Está claro que si $p \in I$, como $p = g \cdot (x - \alpha)$, se tiene $p(\alpha) = g(\alpha) \cdot 0 = 0$. Por otra parte, si $p \in K[X]$ verifica que $p(\alpha) = 0$, entonces tenemos $p = q \cdot (x - \alpha) + r$ por división euclídea, pero evaluando en α sigue que $0 = r(\alpha)$. Si $r \neq 0$, como $gr(r) < gr(x - \alpha) = 1$, entonces $r \in K\backslash 0$ lo cual es contradictorio, luego en definitiva $p = q \cdot (x - \alpha)$ y hemos acabado. □

De esta manera, si $p(x)$ se anula en puntos distintos $\alpha_1, \ldots, \alpha_n$, podemos irlo expresando como $p(x) = (x - \alpha_1)(x - \alpha_2) \ldots (x - \alpha_n)q(x)$. Sigue de aquí que a lo sumo se anula en $gr(p)$ puntos distintos.

Teorema 20 (Fundamental del álgebra)**.** *En $\mathbb{C}[X]$, todo irreducible tiene grado 1. Es decir, $f = u(x - \alpha_1) \ldots (x - \alpha_n)$ con $u \in \mathcal{U}(\mathbb{C}[X]) = \mathbb{C}\backslash\{0\}$.*

Lema 7. *Sea $P \in \mathbb{R}[X]$, y $z \in \mathbb{C}$ una raíz de P considerado en $\mathbb{C}[X]$. Entonces también es raíz $\overline{z}$.*

Demostración. Está claro que $0 = \sum_{i=1}^n a_i z^i$, donde $P(X) = \sum_{i=1}^n a_i X^i$. Tomando conjugados, $\overline{0} = 0 = \overline{\sum_{i=1}^n a_i z^i} = \sum_{i=1}^n \overline{a_i z^i} = \sum_{i=1}^n a_i \overline{z}^i$ dado que los a_i son reales luego sus conjugados son ellos mismos. □

Como consecuencia, las raíces complejas no reales de P aparecen por pares, luego todas las raíces son $\alpha_1, \alpha_2, \ldots \alpha_m \in \mathbb{R}$, y $\beta_1, \overline{\beta_1}, \ldots \beta_r, \overline{\beta_r} \in \mathbb{C}\backslash\mathbb{R}$. Como se tiene que $\forall \beta \in \mathbb{C}$, $(X - \beta)(X - \overline{\beta}) = X^2 - 2XRe(\beta) + |\beta|^2$, entonces:

Lema 8. *Sea $P \in \mathbb{R}[X]$, con las raíces indicadas arriba, entonces $P = c\prod_{i=1}^{m}(X-\alpha_i)\prod_{i=1}^{r}(X^2 - 2Re(\beta_i)+|\beta_i|^2)$ es su descomposición en factores irreducibles. Por tanto, todo irreducible en $\mathbb{R}[X]$ tiene grado 1 o 2.*

Esto es así dado que, como se ha visto, los factores se pueden escribir de esta manera, y ademas los factores cuadráticos son irreducibles en $\mathbb{R}$ porque como se ha visto sus 2 raíces son complejas no-reales. Por tanto, **los polinomios irreducibles en $\mathbb{R}[X]$ son los de grado 1 y los de grado 2 sin raíces reales**, es decir, los de forma aX^2+bX+c con $a \neq 0$ y $b^2 < 4ac$.

Estos criterios funcionan en $\mathbb{R}$ y $\mathbb{C}$, pero aquí hay uno mucho más general:

Proposición 89. *Sea $p \in K[X]$ con K un cuerpo y p de grado 2 o 3. Entonces p es reducible $\iff$ $\exists \alpha \in K$ tal que $p(\alpha)=0$.*

Demostración. p es reducible $\iff$ $p = fg$ con $gr(f), gr(g) < gr(p)$. Como p tiene grado 2 o 3, esto ocurre si y solo si $gr(f)=1$ o $gr(g)=1$, luego esto equivale a decir que $p=(a_1X+a_0)h$, y esto equivale a que tenga una raíz. □

Obsérvese que es necesario que sea de grado 2 o 3. Hay polinomios de grados mayores que son reducibles pese a no tener raíces.

Lema 9. *Si $f \in \mathbb{Z}[X] \subset \mathbb{Q}[X]$ es reducible en $\mathbb{Q}[X]$, de tal modo que $f = f_1f_2$ con $gr(f_1) = r < gr(f)$ y $gr(f_2) = s < gr(f)$, entonces también lo es en $\mathbb{Z}[X]$, es decir, $\exists g_1, g_2 \in \mathbb{Z}[X]$ con $f = g_1g_2$ y además $gr(g_1) = r$ y $gr(g_2) = s$.*

Teorema 21 (Eisenstein)**.** *Si $f(x) = a_nX^n + a_{n-1}X^{n-1} + \cdots + a_0 \in \mathbb{Z}[X]$, $a_n \neq 0$ y $p \in \mathbb{Z}$ es un primo tal que $p \nmid a_n$, $p \mid a_i$ $\forall i \in \{1,\dots,n-1\}$, y además $p^2 \nmid a_0$, entonces f es irreducible en $\mathbb{Q}[X]$ (y por tanto en $\mathbb{Z}[X]$).*

Demostración. Si fuese reducible en $\mathbb{Q}$, lo sería en particular en $\mathbb{Z}$, es decir $f = f_1f_2$ con $f_1 = b_sX^s + \cdots + b_0$ y $f_2 = c_rX^r + \cdots + c_0$, con $r < n$, $s < n$. El homomorfismo $\pi : \mathbb{Z} \to \mathbb{Z}/p\mathbb{Z}$ induce otro $\tilde{\pi} : \mathbb{Z}[X] \to \mathbb{Z}/p\mathbb{Z}[X]$ natural (aplicándolo en cada coeficiente). Es decir, $\tilde{\pi}(f) = \tilde{\pi}(f_1)\tilde{\pi}(f_2)$, luego por las hipótesis, $\overline{a_n}X^n = (\overline{b_s}X^s + \cdots + \overline{b_0})(\overline{c_r}X^r + \cdots + \overline{c_0})$. Pero como $\mathbb{Z}/p\mathbb{Z}[X]$ es de factorización única (por ser asimismo de ideales principales), y $\overline{a_n}X^n = \overline{a_n}X^sX^r$, debe darse que $\overline{b_s}X^s + \cdots + \overline{b_0} = \overline{b_s}X^s$ y que $\overline{c_r}X^r + \cdots + \overline{c_0} = \overline{c_r}X^r$, de donde sigue en particular que $\overline{b_0} = \overline{c_0} = 0$, luego $p \mid b_0$, $p \mid c_0$ pero entonces $p^2 \mid b_0c_0 = a_0$ lo cual es una contradicción. □

Como corolario se tiene que en $Q[X]$ el polinomio $X^n - p$ es irreducible (p es un primo arbitrario), de tal modo que hay irreducibles de grado arbitrario.

A continuación vamos a estudiar los posibles cocientes en $K[X]$.

Observación 28. En $K[X]/\langle p(X)\rangle$ hay tantos ideales como haya en $K[X]$ que contengan a $\langle p(X)\rangle$. Es decir, hay uno por cada divisor mónico de $\langle p(X)\rangle$. Los generados por polinomios irreducibles, además, son los primos (equivalentemente, los maximales, al ser un dominio de ideales principales).

Por ejemplo, en $Q[X]/\langle (X^2-4)^2\rangle$, como $(X^2-4)^2 = (X+2)^2(X-2)^2$, eso indica que tiene 9 divisores (correspondientes a los polinomios 'de la forma $(X+2)^i(X-2)^j$ con $0 \leq i,j \leq 2$), y por tanto $Q[X]/\langle (X^2-4)^2\rangle$ tiene 9 ideales. 2 de ellos son maximales (equivalentemente, primos) porque solo hay dos divisores irreducibles: $X+2$ y $X-2$.

Proposición 90. *Dado $f \in K[X]$ con $gr(f) = n \geq 1$, el anillo $K[X]/\langle f(x)\rangle$ es un espacio vectorial sobre K, de dimensión n y con base $\{\overline{1},\dots,\overline{X}^{n-1}\}$.*

Demostración. Por división euclídea, dado $g \in K[X]$ tenemos que $g = fq + a_0 + a_1X + \cdots + a_{n-1}X^{n-1}$, luego $\overline{g} = a_0 \cdot \overline{1} + a_1\overline{X} + \cdots + \overline{a_{n-1}}\overline{X}^{n-1}$. Falta ver que son linealmente independientes. Si $\lambda_0 + \lambda_1\overline{X} + \cdots + \lambda_{n-1}\overline{X}^{n-1} = 0$, eso es porque $\lambda_0 + \lambda_1 X + \cdots + \lambda_{n-1}X^{n-1} = fg$ para $g \in K[X]$, pero como f tiene grado n, o bien $g = 0$ o bien $gr(fg) \geq n$, lo que es contradictorio, luego $g = 0$ y por tanto $\lambda_0 + \lambda_1 X + \cdots + \lambda_{n-1}X^{n-1} = 0$ y cada escalar es nulo. □

Esto permite construir anillos finitos. Por ejemplo, para construir un anillo de p^k elementos, basta tomar $(\mathbb{Z}/p\mathbb{Z}[X])/\langle X^k \rangle$, dado que es k-dimensional y los escalares van del 0 al $p-1$, luego hay p^k. Si lo que queremos es un **cuerpo** de p^k elementos, deberemos usar el ideal generado por un irreducible de grado k en $\mathbb{Z}/p\mathbb{Z}$. Vamos a estudiar a continuación cuerpos finitos y de dimensión finita.

Proposición 91. *Sea K un cuerpo. Si $\alpha : K \to A$ es un homomorfismo de anillos, entonces ha de ser inyectivo, y por tanto $K \simeq Im\alpha \subset A$ y A es un K-espacio vectorial.*

Demostración. Sabemos que $Nuc(\alpha)$ es un ideal en K y no es todo K porque $\alpha(1) = 1$. Sigue que $Nuc(\alpha) = \{0\}$, porque K es un cuerpo. □

Definición 55. Si $\alpha : K \to F$ es un homomorfismo de anillos, por la proposición anterior, F es un K-espacio vectorial. Si es de dimensión finita, F se dice **extensión finita** de K.

Por ejemplo, $\mathbb{C}$ es extensión finita de $\mathbb{R}$ dado que es un $\mathbb{R}$-espacio vectorial de dimensión 2. Como $X^3 + X + 1$ es irreducible en $\mathbb{Z}/3\mathbb{Z}$, tenemos que $(\mathbb{Z}/3\mathbb{Z})/\langle X^3 + X + 1 \rangle$ es un espacio de dimensión 3, y por tanto una extensión finita, sobre $\mathbb{Z}/3\mathbb{Z}$.

Teorema 22. *Sea F un cuerpo finito. Entonces es una extensión finita de $\mathbb{Z}/p\mathbb{Z}$, para p primo de $\mathbb{N}$. En particular, $|F| = p^n$ donde n es la dimensión de F como $\mathbb{Z}/p\mathbb{Z}$-espacio vectorial.*

Demostración. Consideramos $\alpha : \mathbb{Z} \to F$ el único homomorfismo de anillos (recordemos que viene dado por $\alpha(1) = 1$). Como F es finito, $Nuc(\alpha)$ es un ideal no trivial en $\mathbb{Z}$, e $Im(\alpha) \simeq \mathbb{Z}/Nuc(\alpha)$. Como $Im(\alpha) \subset F$ que es un cuerpo, debe ser que $Im(\alpha)$ sea un dominio y por tanto $Nuc(\alpha) = p\mathbb{Z}$ para p primo, y tenemos lo que queremos: $\mathbb{Z}/p\mathbb{Z} \simeq Im(\alpha) \subset F$. □

Obsérvese también que en esas condiciones la característica de F es precisamente p ($Nuc(\alpha) = p\mathbb{Z}$).

Teorema 23. *Sea F un cuerpo finito. Entonces el grupo abeliano $\mathcal{U}(F)$ ha de ser cíclico.*

Demostración. Sabemos que $|F| = p^n$, y como es cuerpo, $|\mathcal{U}(F)| = p^n - 1 = q_1^{\alpha_1} \dots q_r^{\alpha_r}$, cada q_i primo. Entonces, como es abeliano, $\mathcal{U}(F) \simeq P_1 \times \cdots \times P_r$, con P_i el subgrupo de Sylow de orden $q_i^{\alpha_i}$. Vamos a ver que cada P_i es cíclico, y, como sus órdenes son coprimos dos a dos, el producto será cíclico. Fijado el i, sabemos que $P_i \simeq \mathbb{Z}/q_i^{r_1} \times \cdots \times \mathbb{Z}/q_i^{r_s}$, con $r_1 \geq r_2 \geq \cdots \geq r_s \geq 1$. Lo que queremos probar es que de hecho $s = 1$. Como r_1 es el mayor de todos, $\beta^{q^{r_1}} = 1$ si $\beta \in P_i$. Pero esto indica que $X^{q^{r_1}} - 1$ es un polinomio en F que se anula en todo elemento isomorfo a $\beta \in P_i$, es decir, en $q_i^{\alpha_i}$ elementos. Como el número de raíces de un polinomio no puede superar a su grado, se tiene que $q_i^{r_1} \geq q_i^{\alpha_i}$, de donde $\alpha_i \leq r_1$, y por tanto $r_1 = \alpha_i$ dado que $\alpha_i = r_1 + \cdots + r_s$, y hemos acabado. □

Proposición 92. *Si K es un cuerpo finito de característica p ($|K| = p^n$), el **morfismo de Frobenius** $f : K \to K$ con $f(x) = x^p$ es un isomorfismo de anillos.*

Demostración. $f(1) = 1^p = 1$. $f(ab) = (ab)^p = a^p b^p = f(a)f(b)$. Asimismo, $f(a+b) = (a+b)^p = \sum_{i=0}^{p} \binom{p}{i} a^{p-i}b^i$. No obstante, $\binom{p}{i} = \frac{p!}{i!(p-i)!}$ siempre es múltiplo de p si p es primo, luego $\binom{p}{i}a^{p-i}b^i = (p \times k)a^{p-i}b^i = ka^{p-i}b^i(1 + \cdots + 1) = 0$ por ser p la característica (en la suma hay p unos). Además como K es cuerpo debe ser inyectivo, y como es finito es biyección. □