SOBRE CIERTOS INVARIANTES DE GRUPOS FINITOS

por

ROBERTO FRUCHT
(Viña del Mar, Chile)

SUMMARY: After some remarks on a former paper of G. Fubini, the autor considers three types of "combinatorial invariants" which may be defined for every group of finite order; they represent a generalization of the well-known binomial coefficients which seems to be of some interest.

RESUMEN: Después de algunas consideraciones relativas a una nota anterior de G. Fubini, se consideran tres tipos de "invariantes combinatorios" que se pueden definir para cualquier grupo finito; representan una generalización de los coeficientes binomiales que parece ser de cierto interés.

§ 1. Observaciones sobre una nota de G. Fubini.

En una nota interesantísima (1), Guido Fubini ha considerado el menor número r de subgrupos cíclicos $G_1, G_2, G_3, \ldots, G_r$ (de un grupo finito G) tales que todo elemento del grupo G esté contenido por lo menos en uno de estos grupos G_i. Fubini demuestra que el número r —llamado por él el «orden cíclico» de G—, los grupos G_i y sus órdenes están completamente determinados por el grupo G, y determina los grupos cuyo orden cíclico r no es superior a 3. Además, en los §§ 3 y 5 de su nota, Fubini propone una generalización de los grupos abelianos consistente en los grupos tales que esos subgrupos G_i ($i=1, 2, \ldots, r$) satisfacen la ecuación: $v^{-1}G_iv=G_i$, para todos los elementos v de G; en otras palabras, los r subgrupos G_i han de ser subgrupos *normales* (o invariantes) de G. En el § 4 (pág. 58) de su nota, Fubini indica también ejemplos de grupos *no* abelianos que cumplen con esta condición, y en el último § de su nota, él estudia, pues, la cuestión de si es posible añadir

(1) GUIDO FUBINI: *Algunas propiedades de los grupos discontinuos finitos*, Vol. III, Nº 2, de estas "Publicaciones" (Rosario, 1941).

ulteriores condiciones que permitan afirmar que el grupo es abeliano, e indica algunas condiciones suficientes (pero no necesarias).

Sin embargo, esta «generalización de los grupos abelianos» propuesta por Fubini, conduce a una clase ya conocida y bien determinada de grupos, como ha observado R. Baer en una recensión de la nota de Fubini (2) (y como también el autor había comunicado al Dr. Fubini en una fecha anterior). En efecto, fácilmente se puede demostrar que *todos los subgrupos son normales* en un grupo en que los subgrupos G_1, G_2, ..., G_r (considerados por Fubini) son normales. Pero los grupos no abelianos que tienen sólo subgrupos normales, son conocidos bajo el nombre de grupos hamiltonianos y su estructura es la siguiente (3): *Cada grupo hamiltoniano es un producto directo*: $Q \times D \times J$, donde Q es el grupo de cuaterniones (del orden 8) (4), D es un grupo abeliano que (fuera de la unidad) contiene sólo elementos del orden 2, y J es un grupo abeliano de orden impar. (Los «factores» D y J pueden faltar).

Por consiguiente, si se desea obtener una condición necesaria y suficiente para que sea abeliano un grupo en que los «subgrupos de Fubini» G_1, G_2, ..., G_r son normales, basta postular que el grupo no ha de contener ningún subgrupo isomorfo al grupo de cuaterniones.

Resuelta así la cuestión planteada por Fubini, volvamos al caso de un grupo finito G cualquiera para observar aún que Fubini no aborda la cuestión de si el «orden cíclico» r y los órdenes γ_1, γ_2, ..., γ_r de los subgrupos G_1, G_2, ..., G_r considerados por él, sean tal vez ya suficientes para caracterizar la

---

(2) *Mathematical Reviews*, vol. 3 (1942), Nº 7, pág. 193.

(3) REINHOLD BAER: *Situation der Untergruppen und Struktur der Gruppe*, Sitzungsberichte der Heidelberger Akademie der Wissenschaften, Math. Nat. Klasse 1933 (2), pág. 14.

(4) Grupo de cuaterniones llámase al grupo de multiplicación de tres unidades "imaginarias" i_1, i_2, i_3, según las reglas siguientes:

$$i_1^2 = i_2^2 = i_3^2 = -1, \qquad i_2 i_3 = -i_3 i_2 = i_1,$$

$$i_3 i_1 = -i_1 i_3 = i_2, \qquad i_1 i_2 = -i_2 i_1 = i_3;$$

véase p. ej. pág. 495 del libro: *Elementos de Análisis Algebraico* (5ª ed., Madrid 1939) de JULIO REY PASTOR, a cuyo 25º aniversario de su labor pedagógica en la Argentina se dedica el presente volumen de las "Publicaciones"

estructura de un grupo G — de manera análoga como los «invariantes» de un grupo abeliano caracterizan completamente la estructura del grupo.

La respuesta que hay que dar a la pregunta que acabamos de formular, es negativa: los «invariantes» r, γ_1, γ_2, ..., γ_r no son suficientes para describir la estructura de un grupo, pues puede haber varios grupos con los mismos valores numéricos de esos invariantes. Lo demuestra el siguiente ejemplo de dos grupos distintos que tienen los mismos «invariantes» de Fubini:

I) el producto directo de 3 grupos cíclicos del orden 3;

II) el grupo *no* abeliano, del mismo orden 27, que es engendrado por dos elementos a y b, ambos del orden 3, y cuyo elemento conmutador $a^{-1}b^{-1}ab$ es conmutable con a y b. Se ve fácilmente que todos los elementos de este grupo (con excepción de la unidad) tienen el mismo orden 3; esta afirmación se puede comprobar también usando la siguiente representación del grupo por permutaciones en 9 cifras:

$$a=(1,2,3)\,(4,5,6)\,(7,8,9); \qquad b=(1,4,7)\,(2,8,5).$$

El hecho de que los grupos I) y II) tienen los mismos «invariantes»:

$$r=13, \qquad \gamma_i=3 \qquad (i=1,\ 2,\ \ldots,\ 13),$$

es una consecuencia inmediata del teorema siguiente (para $p=3$, $n=3$).

Teorema 1. Si en un grupo del orden p^n ($n\geqq 2$, p un número primo) todos los elementos (con excepción de la unidad) tienen el mismo orden p, el «orden cíclico» r del grupo es igual a

$$r=\frac{p^n-1}{p-1}=1+p+p^2+\cdots\pm p^{n-1}$$

y cada número γ_i (orden del grupo cíclico G_i) es igual a p ($i=1,\ 2,\ \ldots,\ r$).

Dem. Si x e y son dos elementos del orden p, los grupos cíclicos $\{x\}$ e $\{y\}$, engendrados por x e y, si no son idénticos, tienen sólo la unidad en común. Por consiguiente, con los p^n-1

elementos del orden p de un grupo que cumple con las condiciones del teorema, se pueden formar $\frac{p^n-1}{p-1}$ grupos cíclicos del orden p, y dos de éstos tienen sólo la unidad en común, de modo que ninguno de estos grupos es «superfluo»; es decir que $r=\frac{p^n-1}{p-1}$ y $\gamma_1=\gamma_2=\ldots=\gamma_r=p$.

§ 2. Los «invariantes combinatorios» de un grupo: una generalización de los números combinatorios (coeficientes binomiales).

Fubini considera en su nota (pág. 53) también el grupo de permutaciones (5) de sus subgrupos cíclicos G_1, G_2, ..., G_r, que resulta cuando se someten los elementos de G a todos los automorfismos interiores posibles, es decir, a todos los automorfismos de la forma

$$x \longrightarrow v^{-1}xv \qquad \text{(siendo } v \text{ un elemento de } G\text{)}.$$

De la misma manera se pueden considerar las permutaciones, no sólo de los subgrupos G_1, G_2, ..., G_r, sino también de otros subgrupos (p. ej. de *todos* los subgrupos cíclicos) y hasta de conjuntos cualesquiera de elementos — permutaciones que en todos los casos se obtienen aplicando los automorfismos interiores del grupo G.

Para los elementos mismos de un grupo se trata de una consideración bien conocida que conduce al concepto de las clases de elementos conjugados; y se sabe que k, el número total de clases, es otro importantísimo «invariante» de un grupo finito (que desempeña un papel decisivo en la representación de los grupos finitos por matrices). De manera análoga diremos que dos *conjuntos* de elementos de un grupo finito G son *conjugados*, cuando hay en G un elemento v tal que el automorfismo producido por v transforma uno de los conjuntos en el otro; y el *número* de los conjuntos no conjugados da origen a la definición de otros «invariantes» de un grupo finito, los que parecen

(5) Con postular que este grupo contenga sólo la unidad, FUBINI llega a su "generalización de grupos abelianos" de la que hablamos en el § 1.

ser de cierto interés por representar, en el caso de grupos no abelianos, una generalización de los coeficientes binomiales.

Definición. Un conjunto formado por μ elementos a_1, a_2, ..., a_μ (todos distintos entre sí) llámese conjugado a otro conjunto formado por μ elementos b_1, b_2, ..., b_μ del mismo grupo G, si G contiene un elemento v tal que los μ elementos «transformados»

$$v^{-1}a_1v,\ v^{-1}a_2v,\ \ldots,\ v^{-1}a_\mu v$$

representan una permutación de los elementos b_1, b_2, ..., b_μ. El número de los conjuntos *no* conjugados entre sí que se puedan formar, de μ elementos distintos de un grupo finito G del orden γ, llámese $N_i(\mu)$ (para $\mu=1, 2, \ldots, \gamma$).

Ejemplo. Para el grupo simétrico de tres variables tenemos $N_i(1)=3$, pues la identidad, una transposición cualquiera y un «ciclo», p. ej. (1, 2, 3), forman los únicos elementos no conjugados; $N_i(2)=5$, pues hay los siguientes 5 conjuntos «binarios» no conjugados (6):
identidad $+(1,2)$; identidad $+(1,2,3)$; $(1,2)+(1,3)$;

$$(1,2)+(1,2,3);\ (1,2,3)+(1,3,2);$$

$N_i(3)=6$, pues tenemos los siguientes 6 conjuntos «ternarios» no conjugados:

identidad $+(1,2)+(1,3)$; ident. $+(1,2)\pm(1,2,3)$;

» $+(1,2,3)+(1,3,2)$; $(1,2)+(1,3)\pm(2,3)$;

$(1,2)+(1,3)+(1,2,3)$; $(1,2)+(1,2,3)+(1,3,2)$;

de manera análoga se determinan: $N_i(4)=5$; $N_i(5)=3$; $N_i(6)=1$.

Teorema 2. Para los «invariantes combinatorios» $N_i(1)$, $N_i(2)$, ..., $N_i(\gamma)$ de un grupo finito G del orden γ rigen las fórmulas siguientes:

1) $N_i(1)=k$ (=número de clases de elementos conjugados); $N_i(\gamma)=1$;

(6) Usaremos el signo + en este ejemplo (y en otros que siguen) únicamente para indicar cuales son los elementos que componen un conjunto.

2) $N_i(\mu)=N_i(\gamma-\mu)$, para $\mu=1, 2, \ldots, \gamma-1$; la igualdad rige también para $\mu=0$ y $\mu=\gamma$, si definimos todavía $N_i(0)=1$, lo que conviene también para la fórmula siguiente;

3) $\sum_{k=0}^{\gamma} N_i(k) \equiv 0 \pmod 2$;

4) $\frac{\zeta}{\gamma}\binom{\gamma}{\mu} \leqq N_i(\mu) \leqq \binom{\gamma}{\mu}$, donde ζ es el orden del grupo central de G, $(\mu=0,1,2,\ldots,\gamma)$.

Dem. 1) se deduce inmediatamente de la definición.

2) A cada conjunto de μ elementos (distintos) $a_1, a_2, \ldots, a_\mu$ corresponde *un* conjunto «complementario», formado por los $\gamma-\mu$ demás elementos del grupo, distintos de los a_i; y a dos conjuntos conjugados (resp. no conjugados) de μ elementos corresponden dos conjuntos complementarios conjugados (resp. no conjugados). Por lo tanto: $N_i(\mu)=N_i(\gamma-\mu)$.

3) Según la fórmula que acabamos de demostrar, tenemos que

$$\sum_{k=0}^{\gamma} N_i(k) = \{N_i(0)+N_i(\gamma)\}+\{N_i(1)+N_i(\gamma-1)\}+$$

$$\{N_i(2)+N_i(\gamma-2)\}+\ldots = 2N_i(0)+2N_i(1)+2N_i(2)+\ldots,$$

y este desarrollo terminna, si γ es un número impar, con $2N_i\left(\frac{\gamma-1}{2}\right)$ de manera que en este caso es

$$\sum_{k=0}^{\gamma} N_i(k) = 2\sum_{k=0}^{\frac{\gamma-1}{2}} N_i(k) \equiv 0 \pmod 2;$$

en cambio, si γ es un número par, obtenemos

$$\sum_{k=0}^{\gamma} N_i(k) = 2\left\{N_i(0)+N_i(1)+N_i(2)+\ldots \pm N_i\left(\frac{\gamma}{2}-1\right)\right\}+N_i\left(\frac{\gamma}{2}\right),$$

de modo que hay que demostrar todavía que $N_i\left(\frac{\gamma}{2}\right)$ es un número par (si γ es par). Para ver eso basta dividir los conjuntos

relativos en dos «clases», según contienen o no la unidad del grupo, y hacer una consideración análoga a la hecha en el Nº. 2, esta vez para $\mu=\frac{\gamma}{2}$. En otras palabras, hay que tener presente que a los conjuntos formados por $\frac{\gamma}{2}$ elementos y que contienen la unidad, corresponden igual número de conjuntos complementarios que no la contienen, y viceversa. Por consiguiente, $N_i\left(\frac{\gamma}{2}\right)$ es igual a la suma de dos números iguales entre sí, pues cada una de las dos «clases» consideradas contiene igual número de conjuntos no conjugados entre sí.

4) La desigualdad $N_i(\mu)\leqq\binom{\gamma}{\mu}$ se deduce del hecho de que el número de *todos* los conjuntos que se pueden formar eligiendo μ elementos entre los γ elementos de G, es igual al número combinatorio

$$\binom{\gamma}{\mu}=\frac{\gamma!}{\mu!(\gamma-\mu)!}.$$

Por otra parte, si tenemos $N_i(\mu)$ conjuntos, entre los cuales no hay dos conjugados, podemos someterlos a todos los distintos automorfismos interiores, cuyo número (7) es igual a $\frac{\gamma}{\zeta}$. De esta manera obtenemos, formalmente, $\frac{\gamma}{\zeta}.N_i(\mu)$ conjuntos, los que en parte pueden ser iguales entre sí; pero, de ninguna manera puede faltar entre ellos uno cualquiera de todos los posibles $\binom{\gamma}{\mu}$ conjuntos que existen. Por consiguiente rige la desigualdad:

$$\frac{\gamma}{\zeta}N_i(\mu)\geqq\binom{\gamma}{\mu},\ \text{o sea}\ N_i(\mu)\geqq\frac{\zeta}{\gamma}\binom{\gamma}{\mu}.$$

En grupos abelianos es $\zeta=\gamma$; por lo tanto:

Teorema 3. En grupos abelianos rige la igualdad: $N_i(\mu)=\binom{\gamma}{\mu}$ $(\mu=0, 1, 2, \ldots, \gamma)$.

De esta manera se presentan los «invariantes combinatorios» $N_i(0), N_i(1), \ldots, N_i(\gamma)$ de un grupo no abeliano como generaliza-

ción interesante de los coeficientes binomiales $\binom{\gamma}{0}, \binom{\gamma}{1}, \ldots, \binom{\gamma}{\gamma}$, a los cuales son iguales en el caso de un grupo abeliano.

Aun mayor interés ofrecen, tal vez, los números análogos $N_a(0)$, $N_a(1)$, $N_a(2)$, ..., $N_a(\gamma)$, que se pueden definir para cada grupo finito, incluyendo en la consideración también los (eventuales) automorfismos exteriores que admite el grupo.

Definición. Dos conjuntos (formados cada uno por μ elementos distintos entre sí): $a_1, a_2, \ldots, a_\mu$ y $b_1, b_2, \ldots, b_\mu$, llámense *del mismo tipo* (8), si el grupo G admite un automorfismo (interior o exterior) tal que los elementos $a'_1, a'_2, \ldots, a'_\mu$ (los que corresponden a los $a_1, a_2, \ldots, a_\mu$ en virtud de dicho automorfismo) representan una permutación de los elementos $b_1, b_2, \ldots, b_\mu$. El número de conjuntos distintos que se pueden formar de μ elementos de G, sin que dos de estos conjuntos sean del mismo tipo, llámese $N_a(\mu)$ (para $\mu = 1, 2, \ldots, \gamma$).

Ejemplos. En el grupo cíclico del orden $\gamma = 4$, engendrado por un elemento a (con $a^4 = 1$), tenemos $N_a(1) = 3$, pues a y a^3 son dos elementos del mismo tipo; $N_a(2) = 4$, pues tenemos los siguientes conjuntos «binarios»:

$$1+a,\ 1+a^2,\ a+a^2,\ a+a^3;$$

$N_a(3) = 3$, por haber 3 conjuntos de distinto tipo, p. ej.:

$$1+a+a^2,\ 1+a+a^3,\ a+a^2+a^3;$$

$N_a(4) = 1$, pues para cualquier grupo es $N_a(\gamma) = 1$.

Para el otro grupo del orden $\gamma = 4$ que existe, es decir para el producto directo de dos grupos cíclicos del orden 2 («grupo de Klein»), se encuentra fácilmente que $N_a(1) = N_a(2) = N_a(3) = 2$.

En analogía a los invariantes $N_i(\mu)$, conviene definir todavía: $N_a(0) = 1$ (para cualquier grupo).

Obsérvese que $N_a(1)$ es, por definición, el número de elementos de «distinto tipo» que posee un grupo; este número ya ha

---

(7) Véase p. ej. el teorema Nº 105 en el libro de A. SPEISER: *Die Theorie der Gruppen von endlicher Ordnung* (2ª ed., Berlín, 1927).

(8) Para elementos de grupos abelianos, este concepto de "isotipía" es bien conocido; véase R. BAER: *Gruppen mit vom Zentrum wesentlich verschiedenen Kern und abelscher Faktorgruppe nach dem Kern*, Compositio Mathematica, Vol. 4, fasc. 1 (1936), pág. 46.

sido considerado por I. Schur, quien demostró (9) que los únicos grupos finitos que tienen $N_a(1)=2$, son productos directos de (cualquier número de) grupos cíclicos de un mismo orden p (= número primo). Un problema interesante, pero difícil, parece ser el de encontrar *todos* los grupos finitos con $N_a(1)=3$; pertenecen a estos grupos, por ejemplo, el grupo cíclico del orden p^2, el grupo simétrico en tres variables ($\gamma=6$), el grupo de cuaterniones ($\gamma=8$), el grupo no abeliano (del orden 27) indicado en el § 1, y muchos otros grupos más.

Teorema 4. Para los números $N_a(0), N_a(1), N_a(2), \ldots, N_a(\gamma)$ de un grupo G (del orden γ), cuyo grupo de automorfismos tiene el orden α, rigen las fórmulas siguientes (siempre para $\mu=0, 1, 2, \ldots, \gamma$):

1) $N_a(\mu)=N_a(\gamma-\mu)$;

2) $\sum_{k=0}^{\gamma} N_a(k) \equiv 0 \pmod 2$;

3) $\frac{1}{\alpha}\binom{\gamma}{\mu} \leqq N_a(\mu) \leqq N_i(\mu) \leqq \binom{\gamma}{\mu}$.

La *demostración* es completamente análoga a la de las fórmulas 2), 3) y 4) del teorema N°. 2, de modo que no vale la pena repetirla.

Cabe observar que, en lugar de una desigualdad, tendremos la igualdad:

$$N_a(\mu)=N_i(\mu) \qquad (\mu=0,\ 1,\ 2,\ \ldots,\ \gamma)$$

para grupos que no admiten automorfismos exteriores, como el grupo simétrico de 3, 4, 5 o más de 6 variables — de manera que p. ej. para el grupo simétrico de tres variables rigen los mismos valores ya antes calculados como $N_i(\mu)$:

$$N_a(1)=N_a(5)=3,\ N_a(2)=N_a(4)=5,\ N_a(3)=6.$$

Se sabe, en cambio, que todos los grupos abelianos (con $\gamma \geqq 3$) admiten automorfismos exteriores, y mientras que los

(9) en: *Zur Theorie der einfach transitiven Permutationsgruppen*, Sitzungsberichte der Preussichen Akademie der Wissenschaften, Physikalisch-Mathematische Klasse 1933, XVIII, § 6.

invariantes $N_i(\mu)$ de los grupos abelianos son completamente determinados por el teorema Nº. 3, el cálculo numérico de los invariantes $N_a(\mu)$ para los mismos grupos no es de ninguna manera fácil, sino que puede conducir a problemas difíciles de la teoría de los números.

Ejemplo. Trátese de un grupo cíclico del orden p (=número primo >2) engendrado por un elemento a (de modo que $a^p=1$). Por supuesto que $N_a(1)=2$. Para determinar $N_a(2)$ hay que considerar todos los conjuntos de la forma a^k+a^λ, con $k \not\equiv 0$, $\lambda \not\equiv 0$ (mód p), manteniendo siempre sólo uno, cuando hay varios de unn mismo tipo. Si $k=0$, todos esos conjuntos que resultan para $\lambda=1, 2, 3, \ldots, p-1$, son del mismo tipo; consideremos entonces, el caso $k \not\equiv 0$, $\lambda \not\equiv 0$ (mód p). Existe un número $k' \not\equiv 0$ (mód p) tal que $kk' \equiv 1$ (mód p), y empleando el automorfismo del grupo que reemplaza cada elemento por su potencia con el exponente k', el conjunto a^k+a^λ será transformado en $a+a^{k'\lambda}$. Bastará, por lo tanto, considerar los $p-2$ conjuntos de la forma $a+a^\nu$ (con $\nu=2, 3, \ldots, p-1$). ¿Cuándo son dos de ellos, por ejemplo $a+a^\rho$ y $a+a^\sigma$, del mismo tipo? Empleando el automorfismo que reemplaza cada elemento por su potencia con el exponente σ, vemos que los conjuntos $a+a^\rho$ y $a^{\rho\sigma}+a^\sigma$ son del mismo tipo, de modo que será necesario y suficiente tomar σ como solución de la ecuación de congruencia:

$$\sigma\rho \equiv 1 \pmod{p},$$

para obtener dos conjuntos $a+a^\rho$ y $a+a^\sigma$ del mismo tipo. Si $\rho=p-1$, resulta $\sigma \equiv \rho$ (mód p), pero si $\rho=2, 3, \ldots, p-2$, resulta $\sigma \not\equiv \rho$ (mód p), de modo que hay $1+\frac{p-3}{2}=\frac{p-1}{2}$ conjuntos a^k+a^λ de distinto tipo, con $k \not\equiv 0$, $\lambda \not\equiv 0$ (mód p); añadiendo el caso $k=0$ (considerado ya antes), tendremos, por fin, que

$$N_a(2)=\frac{p+1}{2}. \quad (^{10})$$

(^{10}) La desigualdad 3) del teorema Nº 4 nos habría dado tan sólo:

$$\frac{p}{2} \leqq N_a(2) \leqq \frac{p(p-1)}{2}$$

Aun más difícil resultaría el cálculo de $N_a(3)$, $N_a(4)$, ..., para el grupo considerado, o el cálculo de los invariantes $N_a(\mu)$ para grupos más «complicados».

§ 3. *Una tercera clase de invariantes combinatorios de un grupo.*

Si el concepto de conjuntos conjugados y, respectivamente, de conjuntos del mismo tipo, nos ha conducido a los números $N_i(\mu)$ y $N_a(\mu)$, obtendremos otros «invariantes combinatorios» $P(\mu)$ de un grupo finito, si introducimos el siguiente concepto de la *proporcionalidad* de dos conjuntos de elementos de un grupo finito.

Definición. Dos conjuntos (cada uno formado por μ elementos distintos entre sí): $a_1, a_2, \ldots, a_\mu$ y $b_1, b_2, \ldots, b_\mu$ llámense *proporcionales*, si el grupo G contiene un elemento v tal que los productos: $a_1v, a_2v, \ldots, a_\mu v$ representan una permutación de los elementos $b_1, b_2, \ldots, b_\mu$ [11]. El número de conjuntos distintos que se puedan formar de μ elementos de G, sin que dos de estos conjuntos sean proporcionales entre sí, llámese $P(\mu)$ (para $\mu = 1, 2, \ldots, \gamma - 1$).

Evidentemente es $P(1) = 1$, porque dos *elementos* de un grupo son siempre proporcionales, en el sentido de la definición que acabamos de introducir. Determinemos ahora, por ejemplo, el número $P(2)$ para el grupo cíclico del orden $\gamma = 4$, engendrado por un elemento a (con $a^4 = 1$). El conjunto $1 + a$ es proporcional a los conjuntos $a + a^2$, $a^2 + a^3$ y $a^3 + a^4 = 1 + a^3$: pero no es proporcional al conjunto $1 + a^2$, el que, a su vez, es proporcional tan sólo al conjunto $a + a^3$. Por consiguiente es $P(2) = 2$ (para el grupo considerado) [12].

Antes de establecer relaciones generales para los números $P(\mu)$ de un grupo cualquiera, conviene demostrar el siguiente teorema auxiliar:

---

[11] Para grupos no abelianos podría introducirse también una "proporcionalidad izquierda", postulando la existencia de un elemento w tal que los productos $wa_1, wa_2, \ldots wa_\mu$ formen sólo una permutación de $b_1, b_2, \ldots, b_\mu$. Sin embargo, para cuestiones de carácter combinatorio no se obtendría nada de nuevo.

[12] Conoceremos una fórmula general para $P(2)$ en el teorema Nº 10.

Teorema 5. Para cada conjunto de μ elementos distintos de un grupo ($1 \leqq \mu \leqq \gamma - 1$) se puede encontrar otro conjunto que es proporcional al primero, pero distinto de él.

Dem. El conjunto dado contenga los elementos a_1, a_2, a_3, ..., a_μ. Siendo $\mu < \gamma$, hay (por lo menos) un elemento b que no pertenece al conjunto dado. El conjunto formado por los elementos:

$$b,\ a_2 a_1^{-1} b,\ a_3 a_1^{-1} b,\ \ldots,\ a_\mu a_1^{-1} b$$

será proporcional al conjunto dado (con $v = a_1^{-1} b$), pero distinto de él, por contener el elemento b que no figura entre $a_1, a_2, \ldots, a_\mu$.

Teorema 6. Para los números $P(1)$, $P(2)$, ..., $P(\gamma - 1)$ de un grupo finito G del orden $\gamma \geqq 2$ rigen las relaciones de simetría

$$P(\mu) = P(\gamma - \mu)$$

y las desigualdades

$$\frac{1}{\gamma}\binom{\gamma}{\mu} \leqq P(\mu) \leqq \frac{1}{2}\binom{\gamma}{\mu}$$

(siempre para $\mu = 1, 2, \ldots, \gamma - 1$).

Dem. Las relaciones de simetría se demuestran de la misma manera como lo hicimos para la fórmula análoga 2) del teorema N°. 2. En cuanto a las desigualdades indicadas para $P(\mu)$, hay que observar que nada hay por demostrar cuando $\mu = 1$ o $\mu = \gamma - 1$, pues $P(\gamma - 1) = P(1) = 1$. Sea entonces μ un número de la serie 2, 3, ..., $\gamma - 2$. Hay, por definición, $P(\mu)$ conjuntos de μ elementos, entre los cuales no hay dos proporcionales. Multiplicando todos estos conjuntos sucesivamente a la derecha por todos los γ elementos del grupo, obtendremos, formalmente, $\gamma . P(\mu)$ conjuntos — algunos tal vez iguales entre sí; pero, de todos modos, entre ellos será representado, por lo menos una vez, cada uno de todos los $\binom{\gamma}{\mu}$ conjuntos que existen. Por consiguiente será $\gamma . P(\mu) \geqq \binom{\gamma}{\mu}$, es decir $\frac{1}{\gamma}\binom{\gamma}{\mu} \leqq P(\mu)$.

Para demostrar ahora la otra desigualdad: $P(\mu) \leqq \frac{1}{2}\binom{\gamma}{\mu}$,

(siendo μ siempre un número de la serie 2, 3, ..., $\gamma-2$) basta aplicar el teorema Nº. 5; éste enseña que a lo sumo la mitad de todos los $\binom{\gamma}{\mu}$ conjuntos puede dar conjuntos no proporcionales entre sí, porque para cada conjunto hay (por lo menos un) otro proporcional.

La misma consideración da una desigualdad «mejor» para grupos cuyo orden es un número impar, si en lugar del teorema Nº. 5, aplicamos el siguiente teorema auxiliar:

Teorema 7. Si C_1 es un conjunto formado por μ elementos distintos de un grupo del orden γ (con $\mu<\gamma$) y si formamos *todos* los conjuntos $C_2, C_3, \ldots, C_\delta$ (distintos de C_1 y distintos entre sí) que son proporcionales a C_1, su número δ es un divisor de γ. Además rige $\delta \geqq \pi$, si π es el *menor* número primo contenido en γ.

Dem. Usando la abreviatura «$C_i v$» para el conjunto que se obtiene al multiplicar los elementos del conjunto C_i, a la derecha, por el elemento v del grupo G, podemos ver fácilmente que los conjuntos

$$C_1 v,\ C_2 v,\ \ldots,\ C_\delta v$$

representan una permutación de $C_1, C_2, \ldots, C_\delta$. Tomando ahora para v sucesivamente *todos* los elementos del grupo G, obtenemos de esta manera un grupo transitivo de permutaciones en las δ «variables» C_i. δ es, por lo tanto, índice de un subgrupo de G [13], y como tal es un divisor de γ. Pero no puede ser $\delta=1$, pues ya sabemos que $\delta \geqq 2$ (éste es el contenido del teorema Nº. 5); por consiguiente, δ debe ser un divisor de γ distinto de 1, y el más pequeño de éstos es π.

Teorema 8. Si π es el menor número primo contenido en el orden γ de un grupo G, rigen, para $\mu=1, 2, 3, \ldots, \gamma-1$, las desigualdades:

$$\frac{1}{\gamma}\binom{\gamma}{\mu} \leqq P(\mu) \leqq \frac{1}{\pi}\binom{\gamma}{\mu}.$$

(13) Véase p. ej. el teorema Nº 95 en el libro ya citado de Speiser.

Dem. Basta repetir el raciocinio de la demostración del teorema N°. 6, aplicando el teorema N°. 7, en lugar del teorema N°. 5.

Teorema 9. Para un grupo cíclico cuyo orden es un número primo p, es $P(\mu)=\frac{1}{p}\binom{p}{\mu}$ (para $\mu=1, 2, \ldots, p-1$).

Dem. Aplíquense las desigualdades del teorema N°. 8, con $\gamma=p$ (y, por consiguiente, también $\pi=p$).

Teorema 10. Si un grupo del orden $\gamma\geqq 3$ contiene ν_2 elementos del orden 2, rige la igualdad:

$$P(2)=\frac{\gamma-1+\nu_2}{2}$$

(Si el grupo no contiene ningún elemento del orden 2, por ser γ un número impar, póngase $\nu_2=0$).

Dem. Sea C_1 el conjunto formado por la unidad y un elemento x cualquiera del grupo G:

$$C_1=1+x;$$

el conjunto:

$$C_1 . x^{-1}=1+x^{-1}$$

es proporcional a C_1 y, evidentemente, es el único conjunto proporcional a C_1 que contiene la unidad. Ahora bien, si $x^2=1$, será $x=x^{-1}$, y los dos conjuntos C_1 y $C_1 . x^{-1}$ no son distintos entre sí; en cambio, si $x^2\neq 1$, será $x\neq x^{-1}$ y $C_1\neq C_1 . x^{-1}$, es decir que en este caso entre los «conjuntos binarios» que contienen la unidad, hay siempre dos proporcionales entre sí. Vemos, por lo tanto, que los ν_2 elementos del orden 2 que contiene el grupo, conducen a igual número de conjuntos no proporcionales entre sí; en cambio, los $(\gamma-1-\nu_2)$ elementos del grupo cuyo orden es superior a 2, dan origen sólo a $\frac{\gamma-1-\nu_2}{2}$ conjuntos no proporcionales entre sí (y los que contienen la unidad). Los conjuntos que *no* contienen la unidad no es necesario considerarlos, porque para cada uno de ellos habrá siempre uno proporcional que

contiene la unidad; de modo que

$$P(2) = \nu_2 + \frac{\gamma - 1 - \nu_2}{2} = \frac{\gamma - 1 + \nu_2}{2} \ (^{14}).$$

De manera análoga se podría obtener para $P(3)$ la fórmula siguiente:

$$P(3) = \frac{(\gamma-1)(\gamma-2)}{6} + \frac{\nu_3}{3},$$

donde ν_3 es el número de elementos del orden 3 que contiene el grupo G del orden $\gamma \geqq 4$; pero omitimos la demostración (bastante larga) de esta fórmula y la consideración del próximo número $P(4)$, donde ya no rige más una fórmula tan sencilla (debido evidentemente al hecho de que 4 no es número primo).

(14) La fórmula que acabamos de demostrar tiene cierto interés en un problema de topología combinatoria que trataremos en otra publicación.