L'AXIOMA DE L'ELECCIÓ I LA PARADOXA DE BANACH-TARSKI

Josep Pla Carrera
Universitat de Barcelona

1.- L'AXIOMA DE L'ELECCIÓ. INTRODUCCIÓ.

Des del moment mateix que hom s'inicia a l'estudi de les matemàtiques -en tant que ciència en ella mateixa- es troba amb l'anomenat AXIOMA DE L'ELECCIÓ: A. C.

L'A. C. ens diu

> "si $\mathcal{A} = \{A_i : i \in I\}$ és una família de conjunts no buits i disjunts dos a dos, existeix un conjunt $M = \{x_i : i \in I\}$ que té exactament un element x_i en comú amb cada A_i, $i \in I$, $A_i \in \mathcal{A}$",

que podem enunciar de forma, potser més intuitiva, dient:

> "donada una partició $\mathcal{P}$ d'un conjunt A, existeix un conjunt M que conté exactament un element de cadescuna de les parts de la partició $\mathcal{P}$".

Es ben conegut que la restricció que hem imposat als $A_i \in$ d'ésser disjunts dos a dos és supèrflua.

Aquest axioma és *existencial* i hom havia pensat que, en matemàtiques, *existir* havia de ser equivalent a *ésser construible* i amb aquest axioma això no és pas així. Sembla doncs que aquest axioma és *essencialment diferent* dels altres axiomes existencials de la teoria axiomàtica de conjunts, ja que en ells -en els altres axiomes existencials s'estableix la *manera de construir* el conjunt, l'existència del qual es garanteix. Així, a tall d'exemple, l'axioma de la *unió* ens diu que, per cada conjunt X, *existeix* el conjunt $\cup X$ que *conté com elements els elements dels elements d'*X.

L'Axioma de l'elecció s'usa de forma inconscient al llarg del segle XIX i el mateix G. CANTOR l'usa de forma absolutament inconscient, per exemple, quan estableix una demostració alternativa a la de LIOUVILLE de *l'existència de nombres trascendents* [15] i també quan conjectura en 1883 el principi de la bona ordenació [11]. Qui en donarà la primera al.lusió *explícita* serà G. PEANO en una prova d'existència de solucions per a un sistema d'equacions diferencials ordinàries [40]. En 1902 B. LEVI, en voler calcular el cardinal del conjunt reunió d'una família de conjunts disjunts, observa que la demostració depèn de l'A.C. [35].

En 1904 E. ZERMELO, seguint una suggerència d'E. SCHMIDT, formula l'A. C. de forma explícita i l'usa per a establir l'antiga conjectura de G. CANTOR; és a dir, per a establir el principi del bon ordre [56]. En 1906 B. RUSSELL estableix el principi multiplicatiu [44] i en 1908 E. ZERMELO veu que d'ell s'en segueix l'A. C. [58] .

Malgrat l'èxit que aquest axioma té al sí de l'*aritmètica transfinita*, no és ben rebut per tota la collectivitat matemàtica. Així H. POINCARÉ, ja a partir de 1905, a la vista de les paradoxes de la teoria *naîve* de conjunts de G. CANTOR ataca l'admissió de l'*infinit actual en matemàtiques*, puix que és la causa de les definicions *impredicatives*.

E. BOREL analitza la demostració d'E. ZERMELO de 1904 i observa que ZERMELO usa l'A. C. per tal de ben ordenar un conjunt X i BOREL argumenta que, si acceptem l'A. C., bé podiem haver elegit el primer element, després un primer element de la resta, etc. ... I diu:

> "cal refusar tot raonament en el qual hom utilitza una elecció arbitrària realitzada una infinitat no numerable de vegades; aquests raonaments no formen part de les matemàtiques". [7]

Així E. BOREL posa en qüestió l'A. C. per a famílies no numerables. Però BAIRE i LEGESGUE no comprenen la raó per la qual BOREL opina que el cas numerable és admissible. Per BAIRE "cal reduir-se al cas finit" [23] i per LEBESGUE és una qüestió a convenir, però hom no pot construir *sòlidament a menys que no demostri l'existència d'un ésser definint-lo* i definir, diu, té el significat següent:"nomenar una propietat característica del definit -propietat definible amb un nombre finit de paraules que s'apliqui a l'ésser que volem definir i solament a ell". [34]

E. ZERMELO surt al pas d'aquestes objeccions replicant que l'A. C. cal acceptar-lo *fora* de l'aritmètica transfinita, ja que és *indispensable* per a demostrar que un conjunt infinit admet un subconjunt propi equipotent i per poder citar solucions discontínues de l'equació funcional $f(x + y) = f(x) + f(y)$ i també les bases de HAMEL d'$\mathbb{R}$ com $\mathbb{Q}$-espai vectorial [24] .

Malgrat tot l'A.C. i la seva necessitat en matemàtiques no queden ben afermats fins 1910 quan E. STEINITZ en un treball sobre cossos algebraics posa de manifest el *paper indispensable* que juga a l'A. C. a l'hora de demostrar la unicitat, a menys d'isomorfisme, de l'extensió algebraicament tancada d'un cos. Diu textualment E. STEINITZ:

> "... per tal de garantir la puresa del mètode, sembla que cal evitar aquest principi sempre que la seva aplicació no sigui exigida per la naturalesa del problema". [47]

Des de 1920-1930 tot el món matemàtic ha acceptat com a base formalista del *quefer matemàtic* la teoria axiomàtica de ZERMELO-FRAENKEL, S.F., [56, 57, 58 i 21] i l'única discussió important sorgeix a rel de l'A. C. Però aquesta discussió es va apagant a mesura que els resultats *matemàtics* de l'A. C. esdevenen cada vegada més *importants i més desitjables* (veure & 3 i & 4). Això fa que la balança de l'opinió matemàtica s'inclini cap a l'acceptació de l'A. C. Refusar-lo portaria àdhuc a haver de refusar alguns d'aquests resultats matemàtics importants, puix que li són equivalents (veure & 4).

Abans però d'entrar més de ple en la qüestió dels resultats posituis i negatius de l'A. C., analitzarem una mica més a poc a poc aquest axioma.

L'A. C. en diu, en definitiva, que

> "si $\mathcal{A} = \{A_i : i \in I\}$ és una família de conjunts no buits, aleshores $\prod_{i \in I} A_i$ és no buit" [36]

Si I és finit, no cal en absolut l'A. C. per tal de poder garantir que $\Pi A_i \neq \emptyset$ [55] . És a dir, hom pot provar l'existència del conjunt M que conté exactament un element de cada A_i , $i \in I$, I finit, usant solament els axiomes usuals de ZF , ja que hom pot *descriure formalment la manera d'elegir cada* x_i *a cada* A_i *, si* i *varia en un* conjunt *finit* I .

Però la possibilitat de *descriure la manera d'elegir* desapareix quan $\mathcal{A}$ és infinit.

Suposem ara, com a segon exemple, que cada A_i és un conjunt, no buit, d'ordinals o àdhuc que cada A_i mateix és un ordinal no buit (en realitat és suficient que hom pugui distingir usant ZF un element concret a cada A_i , de manera simultània). Aleshores

$$M = \{\alpha \in \cup \mathcal{A} : \exists A \quad \alpha \text{ és el primer element d'A}\}$$

existeix gràcies als axiomes de la unió i de selecció.

Què passa, però, en el cas general? Per l'axioma de les parts sabem que *existeixen tots els subconjunts de* $\cup\mathfrak{A}$. La teoria ZF no és pas restrictiva. Així doncs el mot "tots" *no inclou també el conjunt M ?* Doncs bé, la resposta és: "no, aquest "tots" no inclou pas, en absolut, el conjunt M " . En realitat quan diem que, amb cada conjunt, disposen de *tots els seus subconjunts* diem molt poc puix que, en realitat, *no sabem quins són els seus subconjunts*; no sabem quins són els subconjunts *concrets* del conjunt de partida. I no ho sabem perquè, en realitat, desconeixem qui és conjunt i qui no ho és. Una primera precissió que fa la teoria ZF en relació amb aquesta qüestió l'estableix l'anomenat *axioma de selecció* que garanteix l'existència - en tant que conjunt - dels *subconjunts* d'un conjunt X que *hom pot descriure usant el llenguatge formal* (L_{set}). No disposàvem ja d'aquest subconjunt d'X en disposar de *tots els subconjunts d'X* ? La resposta és que no puix que no sabem -a menys que ho imposem axiomàticament- si la família

$$\{x \in X : \varphi(x)\}$$

és un conjunt. És clar que, si no és un conjunt, no pot ésser subconjunt d'X. L'*axioma de selecció* ens diu precisament que, donat un conjunt X , els objectes Y de la forma

$$Y = \{x \in X : \varphi(x)\}$$

són conjunts i , per tant, són subconjunts d'X i, en conseqüència, $Y \in P(X)$.

Per tot això, si hom *pot descriure una propietat de tria* , no li caldrà, és clar!, l'A. C. En els atres casos, sí, puix que haurà d'imposar la seva naturalesa de conjunt.

Recordem el famós exemple de B. RUSSELL (citat a [5]). Sigui $\mathcal{A}$ una col.lecció de parelles de guants, hom pot descriure fàcilment un cojunt que tingui exactament un element de cada parella:

"agafem, a cada parella, el guant de la ma dreta";

què passarà, però, si $\mathcal{A}$ és una família de parelles de mitjons? Si la família és finita és possible de construir efectivament el conjunt que cerquem: "d'ací agafo aquest, d'allà, aquell, etc..." i acabo; però com *podem donar una descripció explícita de la tria quan* $\mathcal{A}$ *és una família infinita?*

Acabarem amb un exemple molt simple i instructiu; és usual quan hom s'inicia a l'estudi de les matemàtiques, de plantejar-se i resoldre amb facilitat els següents problemes:

P1.- si $f : X \to Y$ és *injectiva* construir una funció $g : Y \to X$ tal que $g \circ f = 1_X$;

p2.- si $f : X \to Y$ és *exhaustiva* construir una funció $g : Y \to X$ tal que $f \circ g = 1_Y$.

Ambdós problemes són, però, *essencialment diferents*: el primer és trivial puix que la pròpia funció f ens facilita la tria a l'hora de construir la funció g ; en canvi el segon problema precisa de l'A. C. i, de fet, *és equivalent amb l'A. C.* Cal precisar *com elegir a cada conjunt antiimatge* $f^{-1}(y)$ *exactament un* x *que faci d'imatge de la* y *via la funció* g .

Amb aquestes notes introductòries hem vist prou clarament el significat de l'A. C. així com el seu desenvolupament històric i també la seva necessitat al sí de ZF .

NOTA BIBLIOGRAFICA

Hom pot ampliar aquestes observacions amb FRAENKEL, A.A. , BAR-HILLEL, Y. i LÉVY, A. [22] , BERNAYS, P. i FRAENKEL, A.A. [6] i GUILLAUME, M. [19] pel que fa a notes històriques i metodològiques de l'A. C. A l'obra de DEVLIN, K.J.[17, 8] hom trobarà una exposició clara i precisa sobre la necessitat al sí de la teoria ZF de l'A. C. També són d'interès els articles de JECH, T.J. i SHOENFIELD, J.R. a [5] .

2.- LA PARADOXA DE BANACH-TARSKI

Hem indicat de forma somera algunes de les crítiques relatives a l'A. C. però podem afegir, seguint JECH:

> "Algunes objeccions a l'A.C. es basen en el fet que l'axioma té conseqüències paradoxals. Usant l'A.C. poden establir-se resultats que xoquen amb la nostra intuició. L'exemple més famós és el següent: PARADOXA DE BANACH-TARSKI: *Usant l'A.C. és possible descomposar una bola en un cert nombre finit de peces que hom pot reagrupar de manera que s'obtinguin dues boles de la mateixa mida que la bola original*". [5]

I també:

> "L'exemple més popular d'una conseqüència 'poc desitjable' de l'A.C. és l'existència d'un conjunt de nombres reals que *no és pas mesurable en el sentit de LEBESGUE*". [29]

En primer lloc veurem com, usant l'A. C., és possible de construir un cert subconjunt d'$\mathbb{R}$ que *no és mesurable de LEBESGUE*.

(2.1) TEOREMA (A.C.) [G. VITALI [54]]

Existeix un subconjunt $M \subseteq \mathbb{R}$ que no és me-
surable de LEBESGUE.

En efecte:

Sabem que la mesura de LEBESGUE μ de $\mathbb{R}$ és σ-additiva, $\mu(|a,b|) = b - a$ per cada interval amb $a < b$ i *invariant per traslacions.*

A l'interval $[0,1]$ definim

$$x \sim y \quad \text{sii} \quad x - y \in Q \; .$$

És una relació d'equivalència. Sigui

$$[x] = \{y \in [0,1] : y \sim x\} \quad , \quad x \in [0,1] \; .$$

L'A, C. ens permet d'elegir un element *exactament* de cada classe $[x]$, $x \in [0,1]$; així obtenim un conjunt $M \subseteq [0,1]$.

Suposem ara que M és mesurable de LEBESGUE i que $\mu M = m \in [0,1]$. considerem els conjunts $M_q = \{x + q : x \in M\}$ per cada $q \in Q$.

Es compleix:

1.- si $q_1, q_2 \in Q$ i $q_1 \neq q_2$ i $M_{q_1} \cap M_{q_2} = \emptyset$;

2.- $\mathbb{R} = \bigcup\limits_{q \in Q} M_q$.

Per la σ-additivitat, la invariància de μ per traslacions resulta de 1 i 2 que $\mu \mathbb{R} = 0$ si $\mu M = m = 0$. Però com que

3.- $\bigcup_{q \in [0,1]} M_q \subseteq [0,2]$,

per les mateixes raons resulta que $\mu[0,2] = \infty$, si $\mu M = m > 0$. Impossible. El conjunt M no és doncs mesurable de LEBESGUE.

Hom pot veure que és suficient l'A. C. per a famílies de parelles. Aquest resultat és de W. SIERPINSKI i podem trobar-lo a [46] i [29] .

Ara veurem el teorema de BANACH-TARSKI [3, 9, 41, 48] que, a l'engròs, diu: *"si X i Y són dos subconjunts de $\mathbb{R}^3$ suficientment petits per tal d'ésser continguts en una bola suficientment gran i suficientment grans per tal de contenir alguna bola suficientment petita, aleshores X es pot partir en un número finit de peces que poden ésser reagrupades de manera que s'obtingui Y".* Aquest teorema és fals, en canvi, per n = 1 o n = 2 .

L'anterior teorema pot sorprendre'ns si pensem en objectes reals: un mil.lió de pilotes de futbol poden ésser reagrupades de manera que s'obtingui una estatua de l'actual president de la *Secció de Matemàtiques de l'Institut d'Estudis Catalans*. Impossible!

Fins i tot, però, en el món de les matemàtiques aquest resultat és sorprenent. La seva demostració és, en canvi, absolutament rigurosa, si bé, com veurem, no és trivial en absolut.

(2.2) DEFINICIÓ

Per cada $x \in \mathbb{R}^3$, la *norma d'x* és

$|x| = (\sum_{k-1}^{3} x_k^2)^{1/2}$. La *bola tancada de radi* $r > 0$ *i centre en* $a \in \mathbb{R}^3$ és el conjunt de punts de $\mathbb{R}^3$

$$\{x \in \mathbb{R}^3 : |x - a| \leq r\} .$$

Un subconjunt $X \subseteq \mathbb{R}^3$ *està acotat* sii està ficat en una certa bola; *té interior no buit* sii conté una bola.

(2.3) DEFINICIÓ

Una matriu 3×3 A és *ortogonal* sii $A^{-1} = {}^tA$.

Un *gir* de $\mathbb{R}^3$ és una matriu 3×3 ortogonal ρ tal que $\det \rho = +1$.

Un *moviment rígid (euclidià)* és una aplicació

$$r : \mathbb{R}^3 \rightarrow \mathbb{R}^3 , \quad x \rightarrow r(x) = \rho(x) + a ,$$

on ρ és un gir d'$\mathbb{R}^3$ i $a \in \mathbb{R}^3$.

(2.4) DEFINICIÓ (BANACH-TARSKI [3]).

Dos conjunts X i Y d'$\mathbb{R}^3$ són *congruents* ($X \simeq Y$) sii existeix un moviment rígid r tal que

$$Y = r\langle X\rangle = \{r(x) : x \in X\} .$$

Dos conjunts X i Y d'$\mathbb{R}^3$ són *con--gruents per peces* ($X \sim Y$) sii, per un cert nombre natural $n \geqslant 1$, existeix una partició $\{X_j : 1 \leqslant j \leqslant n\}$ d'X en $\underline{n}$ peces i una col.lecció d'$\underline{n}$ moviments rígids $\{r_j : 1 \leqslant j \leqslant n\}$ tals que

$$\{Y_j : 1 \leqslant j \leqslant n\}, \quad \text{on} \quad Y_j = r_j\langle X_j\rangle,$$

es una partició d'$\underline{Y}$ en $\underline{n}$ peces.

Si X és congruent per peces a un cert subconjunt d'Y, escriurem $X < Y$. La relació de congruència per peces compleix les propietats següents:

(2.5) LEMA (BANACH-TARSKI [3])

1. $\sim$ és una relació d'equivalència; és la induida pel preordre $<$ i $\subseteq$ està contingut en $<$.

2. $\sim$ és de CANTOR-BERNSTEIN: si $Z \subseteq Y \subseteq X$ i $Z \sim X$ aleshores $Z \sim Y$ i $Y \sim X$.

3. $\sim$ és compatible amb les unions disjuntes finites: si $X_k \sim Y_k$, $1 \leqslant k \leqslant n$ i $X_k \cap X_{k'} = \emptyset$, $Y_k \cap Y_{k'} = \emptyset$, $k \neq k'$, aleshores

$$X = \bigcup_{k=1}^{n} X_k \qquad Y = \bigcup_{x=1}^{n} Y_k \ .$$

4. Si $X \sim Y$, a cada subconjunt $X_1 \subseteq X$ li correspon un $Y_1 \subseteq Y$ tal que

   i) $X_1 \sim Y_1$,

   ii) si $X_1 \neq X$, aleshores $Y_1 \neq Y$.

5. Si $X \sim X \cup Y_k$, $1 \leqslant k \leqslant n$, aleshores $X \sim X \cup Y$, on $Y = \bigcup_{k=1}^{n} Y_k$.

La demostració d'aquest lema la donarem detalladament a l'apèndix. Veure Lema (A.2)

El lector pot observar l'analogia que existeix entre l'equivalència i la congruència o equipotència de conjunts (sobretot els infinits).

Ara admetrem de forma provisòria una *hipòtesi suplementària* i usant-la demostrarem el teorema de BANACH-TARSKI.

Designarem per S l'esfera unitat: $S = \{x \in \mathbb{R}^3 : |x| = 1\}$.

HIPÒTESI SUPLEMENTÀRIA:

Existeix una partició $\{P, S_1, S_2, S_3\}$ *de l'esfera unitat* S *d'*$\mathbb{R}^3$ *en quatre conjunts tals que*

i) P *és comptamble*

ii) existeixen girs ρ_1 *i* ρ_2 *tals* *que*

$$\rho_1\langle S_1\rangle = S_2 \ , \ \rho_2\langle S_1\rangle = S_3 \ ;$$

iii) existeix un gir ρ *tal que*

$$\rho\langle S_1\rangle = S_2 \cup S_3 \ .$$

Ara estem ja en situació de demostrar el tant anomenat teorema de BANACH-TARSKI de 1924.

(2.6) TEOREMA (BANACH-TARSKI [3]).

1. Tota bola U descomposa en dos subconjunts X i Y tals que $X \sim U$ i $Y \sim U$.

2. Si U_1 i U_2 són dues boles tals que $U_1 \sim U_2$, aleshores $U_1 \sim U_1 \cup U_2$.

3. Si X és un subconjunt d'$\mathbb{R}^3$ acotat amb interior no buit, aleshores $X \sim U$.

4. Si X, Y són dos subconjunts d'$\mathbb{R}^3$, acotats i que no són frontera, aleshores $X \sim Y$.

En efecte:

Si la hipòtesi suplementària val, tenim que $S = P \cup S_1 \cup S_2 \cup S_3$ i, per cada $X \subseteq S$, considerem el conjunt

$$\bar{X} = \{\lambda x : x \in X \ \text{ i } \ 0 < \lambda \leqslant 1\} \ .$$

Tenim doncs que la bola U descomposa en cinc conjunts disjunts

$$U = \bar{P} \cup \bar{S}_1 \cup \bar{S}_2 \cup \bar{S}_3 \cup \{0\}.$$

on $0 = (0, 0, 0)$. De la hipòtesi suplementària i de les propietats dels girs (Lema A.1 de l'apèndix) resulta que

$$\bar{S}_1 \simeq \bar{S}_2 \simeq \bar{S}_3 \simeq \bar{S}_2 \cup \bar{S}_3 .$$

Una altra observació fàcil és la següent: existeix un subconjunt Q de $S_1 \cup S_2 \cup S_3$ comptable tal que $P \simeq Q$ (Lema A.5 de l'apèndix).

1. Sigui ara $X = \bar{S}_1 \cup \bar{P} \cup \{0\}$, $Y = \bar{S}_2 \cup \bar{S}_3 = U - X$.
   Tenim que

$$\bar{S}_3 \sim \bar{S}_2 \cup \bar{S}_3, \ \bar{S}_1 \cup \bar{S}_3 \sim \bar{S}_1 \cup \bar{S}_2 \cup \bar{S}_3, \ \bar{S}_1 \cup \bar{S}_2 \sim \bar{S}_3 \cup \bar{S}_2 \sim \bar{S}_3 \cup \bar{S}_1$$

   i, per tant,

$$\bar{S}_1 \sim \bar{S}_1 \cup \bar{S}_2 \cup \bar{S}_3$$

   i finalment: $X \sim U$.
   Ara bé; $\bar{S}_2 \sim \bar{S}_1 \cup \bar{S}_2 \cup \bar{S}_3$ i $\bar{S}_3 \sim \bar{S}_1 \cup \bar{S}_2 \cup \bar{S}_3$ (*)
   i existeix un Q comptable $\subsetneq S_1 \cup S_2 \cup S_3$ i, per tant,

$$\bar{Q} \subsetneq \bar{S}_1 \cup \bar{S}_2 \cup \bar{S}_3$$

i pel lema (2.5) i la primera relació d'(*) existeix un $Q^* \subsetneq \bar{S}_2$ tal que

$$Q^* \sim \bar{Q} \sim \bar{P} \quad .$$

Sigui ara $x \in \bar{S}_2 - Q^*$ i fem $Y^* = \bar{S}_3 \cup Q^* \cup \{x\}$.
És clar que S_3, $Q^* \subseteq S_2$ i $\{x\} \subseteq S_2 - Q^*$ són disjunts .
Per la segona part d'(*) tenim:

$$Y^* = \bar{S}_3 \cup Q^* \cup \{x\} \sim \bar{S}_1 \cup \bar{S}_2 \cup \bar{S}_3 \cup \bar{P} \cup \{0\} = U \; .$$

Ara bé: $Y^* = \bar{S}_3 \cup Q^* \cup \{x\} \subseteq \bar{S}_2 \cup \bar{S}_3 = Y \subseteq U$ i $Y^* \sim U$.
El lema (2.5) (2) ens diu finalment que $Y \sim U$ i això acaba la demostració.

2. Per 1 existeixen X_1, Y_1 tals que $U_1 = X_1 \cup Y_1$, $X_1 \cap Y_1 = \emptyset$ i $X_1 \sim U_1$ i $Y_1 \sim U_1$.
Però $U_1 \sim U_2$ i, per tant, $U_2 \sim Y_1$.
Pel lema (2.5) (4) existeix $Z \subseteq Y_1$ i $Z \sim U_2 - U_1 \subseteq U_2$ i per (2.5) (3)

$$X_1 \cup Z \sim U_1 \cup (U_2 - U_1) = U_2 \cup U_1 \; ,$$

però $X_1 \cup Z \subseteq U_1 \subseteq U_1 \cup U_2$ i el lema (2.5) (2) acaba la demostració.

3. Sabem que $X = \bigcup_{k=1}^{n} X_k$, on $X_k \subseteq U_k$ i $U_k \simeq U$ i, per (2)

$U \sim U \cup U_k$ per $1 \leqslant k \leqslant n$ i pel lema (2.5) (5):

$U \sim U \sim \bigcup_{k=1}^{n} U_k$ però, com que,

$$U \subseteq X \subseteq U \cup \bigcup_{k=1}^{n} U_k$$

el lema (2.5) (2) ens diu de nou que $X \sim U$.

4. Siguin $U_1 \subseteq X$ i $U_2 \subseteq Y$. Podem suposar, és clar! , que $U_1 \simeq U_2$. Per (3) tenim que

$$X \sim U_1 \simeq U_2 \sim Y$$

i el lema (2.5). (1) acaba la demostració.

Abans de seguir endavant farem unes consideracions:

A. Dues boles de radis diferents són equivalents per peces.

B. Aquest resultat és fals per a discs. En aquest cas solament són equivalents per peces si els seus radis són iguals (veure l'Apèndix, Lema (A.9)).

C. Donat que la mesura de LEBESGUE és *invariant per girs* és absolutament clar que els subconjunts $\bar{S}_k$, k = 1, 2, 3 d'abans *no són mesurables de LEBESGUE.*

C. En el pla val una conjectura més feble que la que hem imposat en el cas d'$\mathbb{R}^3$. La demostració es fa al sí de la teo ria ZF de conjunts. (Veure Lema (A.8)).

E. Si U_1 és una bola de radi r_1 i U_2 és una bola de radi r_2, $r_1 \neq r_2$, existeix un $n \in \mathbb{N}$ tal que

$$U_1 = \bigcup_{k=1}^{n} X_k \quad i \quad U_2 = \bigcup_{k=1}^{n} Y_k \quad i \quad X_k \sim Y_k \quad i \quad X_k, Y_k \subseteq \mathbb{R}^3 .$$

Per tant cap dels X_k ni dels Y_k no és mai mesurable de LEBESGUE a $\mathbb{R}^3$.

F. Cal observar que

ZF + la hipòtesi suplementària

implica

el teorema de BANACH-TARSKI

sense fer ús de l'A. C.

Ara veurem el teorema de HAUSDORFF [1914] que diu

ZF + l'A.C. implica ZF + la hipòtesi suplementària .

(2.7) TEOREMA [HAUSDORFF][1914]] (A.C.) [26]

Existeix una partició $\{P, S_1, S_2\ S_3\}$ de l'esfera unitat S en quatre conjunts tals que

i) P és comptable

ii) $S_1 \simeq S_2 \simeq S_3$

iii) $S_2 \cup S_3 \simeq S_k$, $k = 1, 2, 3.$

Aquest teorema es basa en certs resultats purament algebraics - que enunciarem a continuació i dels quals en donarem, si s'escau, una breu notícia de la demostració, postposant els detalls complets a l'apèndix.

(2.8) LEMA [26]

Existeixen dos girs de $\mathbb{R}^3$ ψ i ϕ tals que $\phi^2 = 1 = \psi^3$ són les úniques relacions del grup G generat per ϕ i ψ.

La demostració pot trobar-se a l'apèndix, lema (A.6). □

(2.9) LEMA [26]

Existeix una partició B_1, G_2, G_3 de G en tres subconjunts no buits tal que

i) $\phi G_1 = G_2 \cup G_3$ (i.e.: $\rho \in G_1 \Leftrightarrow \phi\rho \in G_2 \cup G_3$)

ii) $\psi G_1 = G_2$

iii) $\psi^2 G_1 = G_3$

En efecte:

L'assignació dels elements de G es fa d'acord amb les longituds dels mots del grup G formats a partir de les lletres ϕ, ψ, ψ^2. (Cf. l'apèndix).

$$\iota \in G_1, \quad \phi \in G_2, \quad \psi \in G_2 \quad \text{i} \quad \psi^2 \in G_3$$

i, per inducció sobre la longitud del mot, tenim la taula següent:

$$\rho \text{ comença amb } \begin{cases} \psi \ \dot{-}\ \rho\in G_1,G_2,G_3 \ \text{, aleshores } \phi\rho\in G_2,G_1,G_1 \text{ respectiv.} \\ \psi^2 \ \dot{-}\ \rho\in G_1,G_2,G_3 \ \text{, aleshores } \phi\rho\in G_2,G_1,G_1 \text{ respectiv.} \\ \phi \ \dot{-}\ \rho\in G_1,\ _2\, G_3 \ \text{, aleshores } \psi\rho\in G_2,G_3,G_1 \text{ respectiv.} \\ \phi \ \dot{-}\ \rho\in G_1,G_2,G_3 \ \text{, aleshores } \psi^2\rho\in G_3,G_1,G_2 \text{ respectiv.} \end{cases}$$

Exemple: $\rho = \psi\phi\psi\phi\psi^2\phi\psi^2$ i) $\psi^2\in G_3$, ii) $\phi\psi^2\in G_1$, iii) $\psi^2\phi\psi^2 \in G_3$ iv) $\phi\psi^2\phi\psi^2 \in G_1$, v) $\psi\phi\psi^2\phi\psi^2 \in G_2$, vi) $\phi\psi\phi\psi^2\phi\psi^2 \in G_1$ i vii) $\rho\in G_2$).

Així obtenim la partició buscada. (Els detalls a l'apèndix, Lema (A.7)). □

Ara estem ja en situació de demostrar el teorema de HAUSDORFF.

Fem $P = \{x \in S: \rho(x) = x$ per un $\rho \in G, \rho \neq \iota\}$.

G és numerable i cada ρ deixa fixos solament dos punts d'S (els pols del gir) (Cf. Apèndix, Lema (A.1) (iv)). Així obtenim (i).

Per cada $x \in S - P$, l'*òrbita* d'x és $G(x) = \{\rho(x):\rho \in G\}$. És un subconjunt de $S - P$ (En efecte: si $\rho(x) \in P$ per un $x \in S - P$, aleshores $\rho_1\rho(x) = \rho(x)$ oer un $\rho_1 \in G$, $\rho_1 \neq \iota$;

per tant $\rho^{-1}\rho_1\rho(x) = x$ i $\rho^{-1}\rho_1 \neq \iota$ i $x \in P$. Impossible).

$G(x) \neq \emptyset$ ja que $x \in G(x)$.

$G(x) \cap G(y) = \emptyset$ o bé coincideixen (En efecte : sigui $t \in G(x) \cap G(y)$, aleshores $t = \rho(x) = \rho_1(y)$; sigui $z \in G(x)$, aleshores $z = \tilde{\rho}(x)$ i $x = \rho^{-1}\rho_1(y)$ i $z = \tilde{\rho}\rho^{-1}\rho_1(y)$ i $z \in G(y)$.)

La família $\mathcal{P} = \{G(x) : x \in S - P\}$ és una *partició* d'S-P.

Per l'A. C. podem elegir un punt de cada classe i així obtenir un conjunt M que satisfà:

1. $M \subseteq S - P$;
2. $x_1, x_2 \in M$, $x_1 \neq x_2$, aleshores $G(x_1) \cap G(x_2) = \emptyset$;
3. per cada $z \in S - P$, existeix un $x \in M$ tal que $z \in G(x)$.

Ara definim, par cada $j = 1, 2, 3$:

$$S_j = G_j\langle M\rangle = \{\rho(x) : \rho \in G_j, x \in M\} = \bigcup_{x \in M} G_j(x) \subseteq S - P ,$$

Si $i \neq j$, aleshores $S_1 \cap S_j = \emptyset$ (ja que de no ésser així, existiria un z de $S_i \cap S_j$; és a dir: $z = \rho(x_1) = \rho_1(x_2)$, $\rho \in G_i$, $\rho_1 \in G_j$ i $x_1, x_2 \in M$; d'on, per (2), $x_1 = x_2 = x$ i $\rho_1^{-1}\ \rho(x) = x \in P$; d'on $\rho_1^{-1}\ \rho = \iota$ i $\rho = \rho_1$ i $G_j \cap G_i \neq \emptyset$. Impossible.)

D'aquesta forma hem partit S en els conjunts P, S_1, S_2 i S_3. Aplicant ara el lema (2.9) resulta que

$$\phi\langle S_1\rangle = \{\phi\rho(x) : \rho \in G_1, x \in M\} = \{\tau(x) : \tau \in \phi G_1, x \in M\}$$
$$= \{\tau(x) : \tau \in G_2 \cup G_3, x \in M\} = S_2 \cup S_3 ,$$

$$\psi\langle S_1\rangle = \{\psi\rho(x) : \rho \in G_1, x \in M\} = \{\tau(x) : \tau \in G_2, x \in M\} = S_2 ,$$

$$\psi^2\langle S_1\rangle = \{\psi^2\rho(x) : \rho \in G_1, x \in M\} = \{\tau(x) : \tau \in G_2, x \in M\} = S_3 .$$

□

Notes.

1.- Al teorema de VITALI agafem $M \subsetneq [0,1] - \mathbb{Q} \subsetneq \mathbb{R} - \mathbb{Q}$, si volem, i $G(x) = \{x + q : q \in \mathbb{Q}\} = M_q$ i l'analogia entre ambdós teoremes és clara.

2.- El teorema de HASDORFF val per a tota esfera S_r de radi $r > 0$, no necessàriament unitària.

NOTA BIBLIOGRÀFICA

Al final de l'apèndix.

APÈNDIX

(A.1) LEMA

Sigui ρ un gir. Tenim

i) la imatge d'una recta és una recta;

ii) ρ conserva el producte escalar i , per tant, la norma;

iii) si $\rho \neq \iota$, aleshores $A = \{x \in \mathbb{R}^3 : \rho(x) = x\}$ és una línia recta que passa per l'orígen; és l'*eix* de gir de ρ . Existeix un vector $v \in \mathbb{R}^3$ amb $|v| = 1$ tal que $A = \{tv : t \in \mathbb{R}\}$.

iv) Si $w \in \mathbb{R}^3$ és tal que $A = \{tw : t \in \mathbb{R}\}$ i $|w| = 1$, aleshores $v = \pm w$. v i $-v$ són els *pols* de ρ .

En efecte:

i) per la linealitat;

ii) pel fet que la matriu de ρ és ortogonal;

iii) el polinomi característic de ρ té una arrel real i, si els valors propis són λ_1, λ_2 i λ_3 , aleshores $\det\rho = +1 = \lambda_1 . \lambda_2 . \lambda_3$.

Sigui λ_1 la més gran de les arrels reals. Si λ_3 i λ_2

són complexes, són conjugades i $\lambda_1 |\lambda_2|^2 = 1$ que implica $\lambda_1 = 1$ i $|\lambda_2|^2 = 1$.

Si $\lambda_2 = \lambda_3$ són reals, aleshores $\lambda_1 . \lambda_2^2 = 1$ i $\lambda_1 = 1$; si les tres són reals però diferents, existeix un vector propi $v \neq 0$, per cada una d'elles; $\rho(v) = \lambda_k . v$, $k = 1, 2, 3$, però $<\rho(v) , \rho(v)> = <\lambda_k . v, \lambda_k . v> =$ $= |\lambda_k|^2 . <v,v>$ i, en consequüència, $|\lambda_k|^2 = 1$. Per tant $\lambda_k = \pm 1$.

Podem cercar un vector propi $|v|$ de valor propi $\lambda_1 = 1$ amb $|v| = 1$. Aleshores $\rho(v) = v$ i $t.v \in A$.

Sigui $u \in A$ i $u \neq t.v$, $t \in \mathbb{R}$. Sigui $w \perp u$ i $w \perp v$ i $|w| = 1$. Com que $\rho(u) = u$ i $\rho(v) = v$, resulta que $\rho(w) \perp u$ i $\rho(w) \perp v$, per (ii) i aleshores $\rho(w) = \lambda . w$. Però $|\rho(w)| = 1$, d'on resulta que $\rho(w) = \pm w$.

Per tot $x \in \mathbb{R}$, $x = \alpha . u + \beta . v + \gamma . w$, $\alpha, \beta, \gamma \in \mathbb{R}^3$ i $\rho(x) = \alpha . u + \beta . v \pm \gamma . w$ i $\rho \neq \sim$; per tant $\rho(w) \neq w$. En conseqüència: $\rho(w) = -w$. Si la matriu d'u, v i w li diem σ , aleshores la matriu de u, v, -w és $\rho\sigma$ i $\det \rho\sigma = -\det \sigma$ i $\det \rho\sigma = \det \rho . \det \sigma = \det \sigma$, d'on: $\det \sigma = 0$. Així arribem a contradicció i acabem la prova.

$\square$

(A.2) LEMA

La relació de congruència per peces satisfà les condicions del lema (2.5).

En efecte:

1) a) $X \sim X$: és obvi puix que la identitat és un moviment rígid;

b) $X \sim Y$ implica $Y \sim X$: és obvi puix que l'invers d'un moviment rígid és un moviment rígid;

c) $X \subseteq Y$ implica $X < Y$; és obvi ja que $X \sim X \subseteq Y$;

d) $X \sim Y$ implica $X < Y$: és obvi puix que $X \sim Y \subseteq Y$;

e) $X < Y,\ Y < Z$ implica $X < Z$:

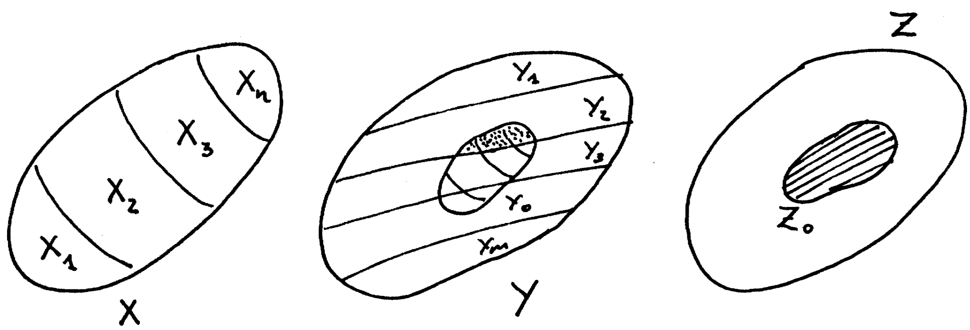
sigui $X \sim Y_o \subseteq Y$ i $Y \sim Z_o \subseteq Z$ i

$\{X_j : 1 \leqslant j \leqslant n\}$ i $\{r_j : 1 \leqslant j \leqslant n\}$ tals que

$X = \cup X_j$ i $Y_o = \cup r_j\langle X_j\rangle$

$\{Y_k : 1 \leqslant k \leqslant m\}$ i $\{s_k : 1 \leqslant k \leqslant m\}$ tals que

$Y = \cup Y_k$ i $Z_o = \cup s_k\langle Y_k\rangle$



Els conjunts $A_{kj} = X_j \cap r_j^{-1}\langle Y_k \rangle$ formen una partició d'X (per cada j fix $A_{1j},\ldots,A_{mj}$ és una partició d'X_j) .

Els conjunts $r_j\langle A_{kj}\rangle = r_j\langle X_j\rangle \cap Y_k$ $(1 \leqslant j \leqslant n)$ és una partició d'$Y_k \cap Y_\circ$. Per tant

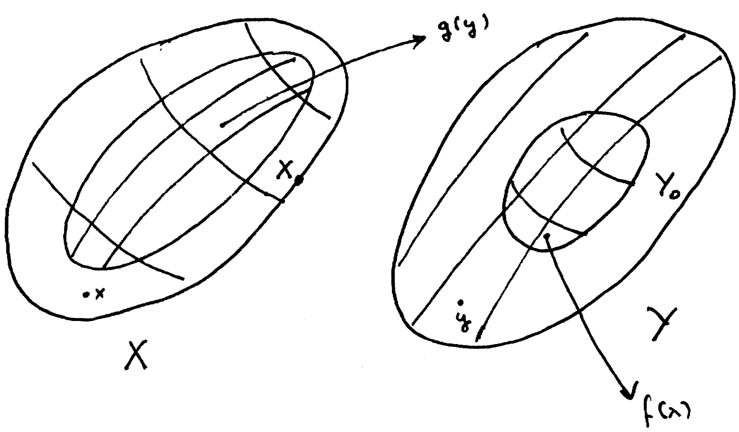
$$\{s_k r_j\langle A_{kj}\rangle : 1 \leqslant k \leqslant m,\ 1 \leqslant j \leqslant n\}$$

és una partició d'un cert subconjunt Z_1 de $Z_\circ$ i els $s_k r_j$ són moviments rígids i, per tant, $X \sim Z_1 \subseteq Z_\circ \subseteq Z$; d'on $X < Z$.

f) $X \sim Y$ i $Y \sim Z$ implica $X \sim Z$: fem $Y_\circ = Y$ i $Z_\circ = Z$ en (e) .

g) $X < Y$ i $Y < X$ implica $X \sim Y$ (CANTOR-BERSTEIN)

Tenim $X \sim Y_\circ \subseteq Y$ i $Y \sim X_\circ \subseteq X$.
Tenim doncs el mateix que en (e) , si fem $X_\circ = Z_\circ$ i $X = Z$, en la segona desigualtat.



Definim $f(x) = r_j(x)$, si $x \in X_j$ i $g(y) = s_k(y)$, si $y \in Y_k$. Per $E \subseteq X$, definim $E' \subseteq X$ per:

$$E' = X - g\langle Y - f\langle E\rangle\rangle .$$

Si $E \subseteq F \subseteq X$, aleshores $E' \subseteq F'$.

Sigui $\mathfrak{D} = \{E \subseteq X : E \subseteq E'\}$. És clar que $\phi \in \mathfrak{D}$. Sigui $D = \cup\mathfrak{D}$. Si $E \in \mathfrak{D}$, aleshores $D \supseteq E$ i $D' \supseteq E' \supseteq E$. D'on: $D \subseteq D'$ i, en conseqüència $D' \subseteq (D')'$. Així doncs $D' \in \mathfrak{D}$ i $D' \subseteq D$. Per tant $D = D'$.

Però

$$D = D' = X - g\langle Y - f\langle D\rangle\rangle$$

i

$$X - D = g\langle Y - f\langle D\rangle\rangle \subseteq X_0 .$$

Ara definim, per $1 \leqslant k \leqslant m$, $1 \leqslant j \leqslant n$,

$$A_j = D \cap X_j, \quad h_j = r_j$$

$$A_{n+k} = s_k\langle Y_k - f\langle D\rangle\rangle, \quad h_{n+k} = s_k^{-1}$$

Es clar que $A_1, \ldots, A_n$ constitueix una partició de D i que $A_{n+1}, \ldots, A_{n+m}$ una de $X - D$. A més, $\{h_j\langle A_j\rangle : j = 1, \ldots, n\}$ parteix $f\langle D\rangle$ i $\{h_{k+n}\langle A_{k+n}\rangle : 1 \leqslant k \leqslant m\}$ parteix $Y - D$. Per tant $X \sim Y$

2) És immediat aplican 1c, 1f i 1g : $Z \sim Y_0 \subseteq Y \sim X_0 \subseteq X \sim Z$, d'on:

$Z < Y$ i $Y < X$ i $Z \sim X$, d'on: $Z < Y$ i $Y < X$ i $X < Z$,

d'on finalment: $Z < Y$ i $Y < Z$.

3) Sigui $X = \overset{n}{\underset{1}{\cup}} X_k$ i $Y = \overset{n}{\underset{1}{\cup}} Y_k$ i $X_k \cap X_{k'} = \emptyset = Y_j \cap Y_j$ i $X_k \sim Y_k$.

Existeixen

$$X_k = \bigcup_{j=1}^{m_z} X_{kj} \ , \quad Y_k = \bigcup_{j=1}^{m_k} Y_{kj} \quad \text{i} \quad X_{kj} \simeq Y_{kj} \ ,$$

d'on

$$X = \bigcup_{k=1}^{n} \bigcup_{j=1}^{m_k} X_{kj} \quad \text{i} \quad Y = \bigcup_{k=1}^{n} \bigcup_{j=1}^{m_k} Y_{kj} \quad \text{i} \quad X_{kj} \simeq Y_{kj}$$

4) És conseqüència immediata del lema que seguix:

(A.3) LEMA

Si $X \sim Y$, aleshores existeix una bijecció $\varphi : X \to Y$ tal que, per cada $Z \subseteq X$, $\varphi\langle Z\rangle \sim Z$.

En efecte:

Sigui $X = \bigcup_{j=1}^{n} X_j$ i $Y = \bigcup_{j=1}^{n} r_j\langle X_j\rangle$. Fem $\varphi(x) = r_j(x)$, si $x \in X_j$, $1 \leqslant j \leqslant n$. Es clarament bijectiva. Sigui ara $Z \subseteq X$ i fem $Z_j = Z \cap X_j$, $1 \leqslant j \leqslant n$.

$\{Z_j : 1 \leqslant j \leqslant n\}$ és una partició de Z tal que $Z_j \subseteq X_j$.

A més: $\varphi\langle Z\rangle = \bigcup_{j=1}^{n} \varphi\langle Z_j\rangle$ i $\varphi\langle Z_j\rangle$ constitueixen una partició de $\varphi\langle Z\rangle$.

A més: $Z_j \simeq \varphi\langle Z_j\rangle$, $1 \leqslant j \leqslant n$, ja que $\varphi|_{X_j} = r_j$.

(A.4) COROL.LARI.

1. Si $X \sim Y$ i existeix una descomposició d'X en conjunts disjunts $\{X_j : 1 \leqslant j \leqslant n\}$, n'existeix una d'Y, $\{Y_j : 1 \leqslant j \leqslant n\}$ tal que $X_j \sim Y_j$.
2. La part 4) del lema (A.2). La segona part és deguda al fet que φ sigui una bijecció.

5) Suposarem dos casos:

i) Els conjunts $X, Y_1, \dots, Y_n$ són disjunts dos a dos.

Per $n = 1$ és obvi.

Suposem-ho doncs cert per un cert k i veiem-ho per $k + 1 \leqslant n$.

$$X \sim X \cup \bigcup_{j=1}^{k} Y_j$$

$$X \sim X \cup Y_{k+1}.$$

Però $X \cap Y_{k+1} = \emptyset = Y_{k+1} \cap \bigcup_{j=1}^{k} Y_j$ i aplicant 3) :

$$X \cup Y_{k+1} \sim X \cup \bigcup_{j=1}^{k} Y_j \cup Y_{k+1} = X \cup \bigcup_{j=1}^{k+1} Y_j$$

i per la propietat transitiva, hem acabat la demostració.

ii) En general. Fem $Y'_1 = Y_1 - X$ i $Y'_{k+1} = Y_{k+1} - (X \cup \bigcup_{j=1}^{k} Y_j)$, $1 \leqslant k \leqslant n$.

Tenim

$$X \cup \bigcup_{k=1}^{n} Y'_k = X \cup \bigcup_{k=1}^{n} Y_k$$

i $\qquad X \subseteq X \cup Y'_k \subseteq X \cup Y_k$ i aplicant 2) resulta que $X \sim X \cup Y'_k$ i, per consegüent, podem aplicar i).

(A.5) LEMA.

Si $S = P \cup S_1 \cup S_2 \cup S_3$, on P és comptable, existeix un $Q \subseteq S_1 \cup S_2 \cup S_3$ tal que $P \simeq Q$.

Enumerem $P = \{x_n : n \in \omega\}$. Sigui e_p un eix de gir que no passi per cap punt de P . Sigui $A_k = \{\theta \in [0,2\pi] : \varphi_\theta(x_k) \in P\}$ És comptable com a màxim. Per tant $A = \bigcup_{k\in\omega} A_k$ és comptable i, en conseqüència, existeix un $\theta_\circ \in [0,2\pi]$ i $\theta_\circ \notin A$. Sigui ara $\rho = \rho_{\theta_\circ}$. Aleshores $P \cap \rho\langle P\rangle = \emptyset$ i, per tant, $Q = \rho\langle P\rangle \simeq P$ i $Q \subseteq S_1 \cup S_2 \cup S_3$.

(A.6) LEMA

Existeixen dos girs d'$\mathbb{R}^3$ ϕ i ψ tals que $\phi^2 = 1 = \psi^3$ són les úniques relacions del grup generat per ϕ i ψ .

En efecte:

La rotació ψ és la rotació d'$\mathbb{R}^3$ d'eix OZ i angle 120° i la ϕ és la rotació d'$\mathbb{R}^3$ d'angle 180° i d'eix la recta del pla XZ d'equació

$$x.\cos\frac{1}{2}\theta = z.\sin\frac{1}{2}\theta ,$$

on θ es determinarà més endavant. Aleshores

$$\psi = \begin{pmatrix} -1/2 & -\sqrt{3}/2 & 0 \\ \sqrt{3}/2 & -1/2 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

$$\phi = \begin{pmatrix} -\cos\theta & 0 & \sin\theta \\ 0 & -1 & 0 \\ \sin\theta & 0 & \cos\theta \end{pmatrix}$$

És clar que ψ^2 s'obté de ψ canviant $\sqrt{3}$ per $-\sqrt{3}$ i $\psi^3 = \phi^2 = \iota$.

Sigui G el conjunt de totes les matrius que s'obtenen per productes finits, essent els factors ψ i ϕ .

G és un grup.

A més, si $\rho \in G$ i $\rho \neq \iota$, aleshores ρ es pot expressar d'una manera almenys en la forma

$$\rho = \sigma_1.\sigma_2 \ldots \sigma_n, \quad n \geqslant 1 ,$$

on cada σ_j és ϕ, ψ ó ψ^2 i, si $1 \leqslant j \leqslant n$, un exactament dels σ_j, σ_{j+1} és ϕ.
Són paraules reduïdes de lletres ϕ, ψ, ψ^2.

Tot element de G, diferent de la identitat, i de ϕ, ψ i ψ^2, es pot escriure en una almenys de les formes:

$$\alpha : \psi^{p_1}.\phi.\psi^{p_1}.\phi \ \ldots \ \psi^{p_m}.\phi \ , \quad m \geqslant 1 \ \text{ i } \ p_j = 1,2,$$

$$\beta : \phi.\psi^{p_1}.\phi.\psi^{p_2} \ \ldots \ \psi^{p_m} \ , \quad m \geqslant 1 \ \text{ i } \ p_j = 1,2,$$

$$\gamma : \phi.\psi^{p_1}.\phi.\psi^{p_2} \ \ldots \ \psi^{p_m}\phi \ , \quad m \geqslant 1 \ \text{ i } \ p_j = 1,2,$$

$$\delta : \psi^{p_1}.\phi.\psi^{p_2}.\phi \ \ldots \ \phi.\psi^{p_m}, \quad m \geqslant 1 \ \text{ i } \ p_j = 1,2$$

Ara la qüestió és: *dues paraules reduïdes diferents poden tenir la mateixa matriu?* És clar que sí: per $\theta = \pi$, $\psi.\phi = \phi.\psi^2$ i $\psi\phi\psi\phi = \iota$.

HAUSDORFF [26] observarà, però, que, si $\cos\theta$ és un nombre *trascendent*, aleshores tot gir diferent de la identitat té una única expressió en tant que paraula reduïda en les lletres ϕ, ψ, ψ^2. És a dir: si

$$\sigma_1.\sigma_2. \ \ldots \ .\sigma_m = \sigma_1^*.\sigma_2^*. \ \ldots \ .\sigma_n^* \ ,$$

on cada membre de l'equació és una paraula reduïda, aleshores $m = n$ i $\sigma_i = \sigma_i^*$, $1 \leqslant i \leqslant m$.

Hem de veure que cap paraula reduïda no és mai igual a la identitat, ja que aleshores, de donar-se una igualtat com l'anterior amb n tan petit com sigui possible, tindrem $n = 1$ i $\sigma = \sigma^*$.

Si la paraula reduïda és de la forma α, aleshores $\alpha \neq \iota$. Tenim

$$\alpha = \sigma_m \sigma_{m-1} \cdots \sigma_2 \sigma_1 \quad , \text{ on cada } \sigma_i \text{ és } \psi\phi \text{ ó } \psi^2\phi \quad .$$

Així doncs cada σ_i és una matriu de la forma

$$\begin{pmatrix} 1/2.\cos\theta & \pm\sqrt{3}/2 & -1/2.\sin\theta \\ \pm\sqrt{3}/2\cos\theta & 1/2 & \pm\ 3/2.\sin\theta \\ \sin\theta & 0 & \cos\theta \end{pmatrix}$$

Per inducció sobre m hom constata que, si $v = (0,0,1)$, aleshores

$$\alpha\,(v) = (\sin\theta.P_{m-1}(\cos\theta)\ ,\ \sqrt{3}.\sin\theta.Q_{m-1}(\cos\theta)\ ,\ R_m(\cos\theta)).$$

On P, Q i R són polinomis a coeficients racionals, de grau l'indicat pel subíndex i de coeficients principals:

$$-\frac{1}{2}.\left(\frac{3}{2}\right)^{m-1}, \quad \pm\,\frac{1}{2}\left(\frac{3}{2}\right)^{m-1}, \quad \left(\frac{3}{2}\right)^{m-1}$$

respectivament. (Veure [48] .) Fent càlculs, tenim:

$$P_0(x) = -1/2, \quad Q_0(x) = \pm 1/2, \quad R_1(x) = x\ ,$$

$$P_m(x) = \frac{1}{2}.x.P_{m-1}(x) \pm\frac{3}{2}.Q_{m-1}(x) - \frac{1}{2}.R_m(x),$$

$$Q_m(x) = \mp\frac{1}{2}.x.P_{m-1}(x) + \frac{1}{2}.Q_{m-1}(x) \pm \frac{1}{2}.R_m(x),$$

$$R_{m+1}(x) = (1 - X^2).P_{m-1}(x) + x.R_m(x).$$

- Si $\cos\theta$ és trascendent és impossible que $R_m(\cos\theta)=1$ i, per tant, $\alpha v \neq v$ i $\alpha \neq \iota$.

- Tampoc β no és igual a la identitat; si ho fós

$$\alpha = \phi\beta\phi = \phi\iota\phi = \phi = \iota$$

- tampoc no ho és γ , ja que si ho fós

$$\delta = \phi\gamma\phi = \phi\iota\phi = \phi = \iota$$

Per tant hem de veure que $\delta \neq \iota$.

- Suposem el contrari; és a dir, que $\delta = \iota$ i que m és mínim amb aquesta propietat i que $m > 1$.

- si $p_1 = p_m$, aleshores $\psi^{p_1+p_m}$ és o bé ψ^2 o bé $\psi^4 = \psi$; d'on :

$$\iota = \psi^{-p_1}\delta.\psi^{p_1} = \phi\,\psi^{p_2} \dots \phi.\psi^{p_1+p_m}$$

que és de la forma β . Impossible.

- si $p_1 + p_3 = 3$ i $m > 3$ tenim $\imath = \phi\psi^{p_m}\delta.\psi^{p_1} =$
$= \psi^{p_2}.\phi \ldots \phi.\psi^{p_{m-1}}$ que és la forma δ , però m és més curt. Impossible!

- si $p_1 + p_m = 3$ i $m = 2$, $\imath = \psi^{p_2}.\delta.\psi^{p_1} = \phi$. Impossible.
i $m = 3$, $\imath = \phi.\psi.^{p_3}\delta.\psi^{p_1}.\phi = \psi^{p_2}$. Impossible.

Elegim $\cos\theta$ *trascendent* i hem acabat. Tots els angles θ , llevat una quantitat numerable tenen aquesta propietat. Per exemple $\cos 1$.

(A.7) LEMA

Els conjunts G_1, G_2 i G_3 construits al lema (2.10) compleixen i), ii) i iii) .

En efecte:
Són disjunts claramente per construcció.

Pel resultat de HAUSDORFF els elements de G tenen longitud que és la *longitud* de la paraula reuida i $l(\imath) = 0$.

Si σ té longitud zero, aleshores $\sigma = \imath \in G_1$ i $\phi.\sigma =$ $= \phi \in G_2 \subseteq G_2 \cup G_3$ i $\phi.\sigma = \psi \in G_2$ i $\psi^2.\sigma = \psi^2 \in G_3$. Compleix i), ii) i iii).

Si σ té longitud un, aleshores

$$\sigma = \begin{cases} \phi \in G_2 \quad i \quad \psi.\phi \in G_3 \quad i \quad \psi^2\phi \in G_1 \\ \psi \in G_2 \quad i \quad \phi\psi \in G_3 \\ \psi^2 \in G_2 \quad i \quad \phi\psi^2 \in G_1 \ . \end{cases}$$

i i)-iii) valen per a la longitud un.

Si val per tot ρ de longitud $< n$, valdrà pels $\rho \in G$ amb longitud n :

CAS 1. ρ comença amb ϕ i $\rho \in G_1$, aleshores $\psi.\rho \in G_2$ i $\psi^2.\rho \in G_3$;
i $\rho \notin G_1$, aleshores $\phi.\rho$ té longitud n-1 i
$\rho = \phi(\phi.\rho) \in G_2 \cup G_3$ si, i només
si, (per hipòtesi d'inducció)
$\phi.\rho \in G_1$ si, i només si, $\phi\rho \notin G_2 \cup G_2$

CAS 2. ρ comença amb ψ i $\rho \in G_1$ si, i només si $\phi\rho \in G_2 \subseteq G_2 \cup G_3$.
$\psi\cdot\rho = \psi\,\sigma$ amb $(\sigma) \leqslant n-1$ i σ comença amb ϕ
$\psi.\rho \in G_2$ si, i només si, $\psi^2\sigma \in G_2$ si, i només si,
$\sigma = \psi^2\rho \in G_3$ si, i només si, $\rho = \psi.\sigma \in G_1$
(puix que σ comença amb ϕ)

CAS 3. ρ comença amb ψ^2 i $\rho \in G_1$ si, i només si, $\phi.\rho \in G_2$.
$\psi\rho = \sigma$ i $(\sigma) = n-1$ i σ comença amb ϕ
$\psi\phi = \sigma \in G_2$ si, i només si, $\rho = \psi^2.\sigma \in G_1$
si, i només si, $\sigma \in G_2$ si, i només si,
$\psi\sigma = \psi^2\rho \in G_3$.

□

Veiem ara de nou el teorema de VITALI. De $[0,1] - Q$ i, per cada $x \in [0,1] - Q$, considerem $G(x) = \{x + q \in [0,1] : q \in Q\}$

$G(x) \subseteq [0,1] - Q$;

$G(x) \cap G(y) = \emptyset$ o bé coincideixen;

$G(x) \neq \emptyset$.

Així doncs $\mathcal{P} = \{G(x) : x \in [0,1] - Q\}$ és una partició de $[0,1] - Q$ i per l'A. C. podem elegir un punt de cada classe i obtenim així un conjunt M tal que

$$M \subseteq [0,1] - Q \; ; \quad x_1, x_2 \in M, \; x_1 \neq x_2, \; G(x_1) \cap G(x_2) = \emptyset \; ;$$

$$z \in [0,1] - Q, \text{ existeix un } x \in M \text{ i } z \in G(x) \; .$$

En el cas d'espais euclidians de dimensió 1 ó 2, què passa?

(A.8) LEMA. [48]

A $\mathbb{R}^2$ també val un cert teorema afeblit de HAUSDORFF.

En efecte:

Sigui $c \in \mathbb{C}$ trascendent amb $|c| = 1$ (N'hi ha: $c = e^i$.)

Sigui $X = \{z \in \mathbb{C} : z = \sum_{k=o}^{n} a_k . c^k, \; n \in \omega$ i $a_o, \ldots, a_n \in \omega\}$.

Cada z té una expressió única per la trascedència de c.

Sigui $X_0 \subseteq X$ el subconjunt dels x d'X tals que $a_0 = 0$ i $X_1 = X - X_0$.

Es clar que $\{X_0, X_1\}$ divideix X.

Sigui ara la rotació del pla complex $\rho(z) = cz$ i la tras lació τ donada per $\tau(z) = z + 1$. És clar que $\rho(X) = X_\circ$ i $\tau(X) = X_1$ i cada un dels conjunts $X_\circ$, X_1 és congruent amb X .

S'empobreix puix que X és no acotat i comptable. No cal, però, l'elecció.

(A.9) LEMA. [3]

Si X i Y són conjunts de $\mathbb{R}$ ó $\mathbb{R}^2$ ambdós acotats i mesurables de LEBESGUE, aleshores, si $X \sim Y$, $\mu(X) = \mu(Y)$.

En efecte:

És conseqüencia immediata d'un resultat de BANACH [1] que diu: "a cada subconjunt acotat A d'$\mathbb{R}$ ó d'$\mathbb{R}^2$ li podem associar un nombre real no negatiu $f(A)$ de forma que

i. $A \simeq B$ implica $f(A) \quad f(B)$;

ii. $A \cap B \quad \emptyset$ implica $f(A \cup B) \quad f(A) + f(B)$

iii. si A és mesurable, $f(A) = \mu(A)$.

De la hipòtesi, tenim que:

$$X = \bigcup_{k=1}^{n} X_k , \quad Y = \bigcup_{k=1}^{n} Y_k , \quad \text{amb} \quad X_k \cap X_{k'} = \emptyset = Y_k \cap Y_{k'} , \quad \text{i} \quad X_k \simeq Y_k$$

Per i) $f(X_k) = f(Y_k)$ i, per ii), $f(X) = \sum_{k\,1}^{n} f(X_k)$ i $f(Y) = \sum_{k\,1}^{n} f(Y_k)$ i, per tant, $f(X) = f(Y)$. Però, si X i Y són mesurables de LEBESGUE resulta que $\mu(X) = \mu(Y)$.

$\square$

A més BANACH-TARSKI [3] veuen que aquest resultat no és pas invertible ja que, si X és arreu no dens i $X \sim Y$, Y també ho és. Existeixen conjunts l'un arreu no dens i l'altre que no té pas aquesta propietat amb la mateixa mesura de LEBESGUE. Si hom tracta amb polígons, però, el resultat és invertible.

NOTA BIBLIOGRÀFICA

A JECH [5, 29] hom pot trobar indicacions mínimes del teorema de BANACH-TARSKI. Nosaltres hem seguit al peu de la lletra el treball original de BANACH-THARSKI [3]. D'altres presentacions diferents poden trobar-se a BRUCKNER, A.M. i CEDER,J. [9] i a STROMBERG, K. [48], així com també a M. ROBINSON [91].

3.- L'AXIOMA DE L'ELECCIO AL SÍ DE LA TEORIA DE CONJUNTS ZERMELO-FRAENKEL

Tothom coneix les equivalències més importants de l'A. C. Malgrat tot no ens sembla pas excessiu de repassar les més importants.

L'AXIOMA DE L'ELECCIO (A. C.) (RUSELL [1906][41]):

"si $\mathcal{A} = \{A_i : i \in I\}$ és una família de conjunts no buits, existeix un conjunt X que conté exactament un element amb comú amb cada A_i, $i \in I$" ;

LEMA DE ZORN (L. Z.) (HAUSDORFF [1914] i ZORN [1935][26,59]):

"si $(X,<)$ és un conjunt parcialment ordenat tal que tota cadena té cota superiors, aleshores $(X,<)$ té elements maximals" ;

PRINCIPI DEL BON ORDRE (P. B. O.) (CANTOR) [1883] i ZERMELO [1904][11, 56]):

"tot conjunt X admet una bona ordenació";

PRINCIPI DE TRICOTOMIA (P. T.) (HARTOGS) [1915][25]):

"donats dos conjunts X, Y sempre és possible d'injectar almenys un d'ells en l'altre".

PRINCIPI D'EPIJECCIÓ (P. E.):

"donats dos conjunts X, Y sempre és possible trobar una epijecció almenys d'un d'ells en l'altre" ;

LEMA DE TUKEY (L. T.) (TEICHMÜLLER [1939] i TUKEY [1940] [51, 52]):

"tot conjunt $\mathfrak{F}$ de caràcter finit té elements maximals".

Hom diu que $\mathfrak{F}$ és de caràcter finit sii $E \in \mathfrak{F}$ sii tota part finita F d'E pertany a $\mathfrak{F}$.

(3.1) TEOREMA

Les proposicions anteriors són totes equivalents.

Hom pot donar demostracions senzilles usant els ordinals que, parlant a l'engròs, no són altre cosa que la generalització (la continuació) dels nombres naturals.

Serveixen per a caracteritzar els *bons ordres*.
Un conjunt $(X, <)$ és *ben ordenat* sii tot subconjunt $Y \subseteq X$, $Y \neq \emptyset$, té $<$-primer element.
Un conjunt X és *transitiu* sii tot $x \in X$ satisfà $x \subseteq X$.
Un conjunt α és un *ordinal* sii és transitiu i, per tot, $x, y \in \alpha$, $x \in y$ ó $y \in x$ ó $x = y$.

A Z.F. valen les següents proposicions:

1. α és un ordinal sii $\alpha = \{x : x$ és un ordinal $\in \alpha\}$;
2. si α és un ordinal, $(\alpha, \in)$ és ben ordenat;
3. per tot $x, y \in \alpha$, $x \in y$ sii $x \subsetneq y$;
4. la classe Ord de tots els ordinals és una classe pro pia.
5. tot conjunt ben ordenat $(W, <)$ és ordre-isoform a un únic ordinal.

Un ordinal k és *inicial* (o *número cardinal*) sii, per tot $\beta < k$ $\beta \not\sim k$ (on $x \sim y$ significa que existeix una bijecció d'x en y).

La classe Card de tots els cardinals és una classe pròpia.

Hom escriu $x \leqslant y$ sii existeix una injecció $f : x \to y$.

Tothom coneix el famós teorema de CANTOR [12] : $X < P(X)$:

Ara estem en situació de demostrar el teorema (3.1) .

Veurem

$$\begin{tikzcd}[column sep=small]
\text{A.C.} \arrow[r, Rightarrow] & \text{L.Z.} \arrow[r, Rightarrow] \arrow[d, Rightarrow, shift left] & \text{P.O.B.} \arrow[r, Rightarrow] & \text{P.T.} \arrow[r, Rightarrow] & \text{P.E.} \arrow[r, Rightarrow] & \text{P.B.O.} \arrow[r, Rightarrow] & \text{A.C.} \\
& \text{L.T.} \arrow[ul, Rightarrow] & & & & &
\end{tikzcd}$$

A.C. $\Rightarrow$ L.Z.

Sigui $(X, <)$ un conjunt parcialment ordenat i supo sem que tota cadena té cotes superiors, però, en can vi, X no té maximals. Definim

$$G : P(X) \to X$$
$$Y \to G(Y) = \begin{cases} \text{una cota superior estricta d'}Y, \\ \text{si } Y \text{ és una cadena;} \\ x_0 \ X, \text{ altrament} \end{cases}$$

Considerem $f: Ord \to X; \alpha \to f(\alpha)=G<f]\alpha,\alpha[>=G<f(\xi): \xi\in\alpha>$.
És clar que $f(\alpha) > f(\xi)$ per tot $\alpha \ni \xi$ i, per tant, f és injectiva. Aleshores $f < Ord >$ és una classe pròpia $\subseteq X$ i això no és possible a Z.F.

L.Z. $\Rightarrow$ L.T.

Si $\mathcal{C}$ té caràcter finit i $(X_i)_{i \in I}$ és una cadena d'elements de $\mathcal{C}$, aleshores $\bigcup_{i\in I} X_i \in \mathcal{C}$ (puig que tota part finita d' $\bigcup_{i\in X} X_i$ estarà en un X_i i, per tant, serà de $\mathcal{C}$ i $\mathcal{C}$ té caràcter finit). Aleshores té elements maximals.

L.T. $\Rightarrow$ A.C.

Sigui $(X_i)_{i\in I}$ una família de conjunts disjunts no buits. Sigui $\mathcal{C} = \{K :$ existeix $f : K \to \bigcup_{i\in I} X_i$, $f(k) \in X_k$ i $K \subseteq I$ i $k \in K\}$
Té caràcter finit. Si K hi pertany, les seves parts finites també. Si les parts finites de K hi pertanyen tenim

$$f_k : \{k\} \to \bigcup_{i\in I} X_i, \quad f_k(k) \in X_k$$

i, si fem $f : K \to \bigcup_{i\in I} X_i$ per $f(k) = f_k(k)$, K hi pertany.
Existeix un maximal $K \subseteq I$ a $\mathcal{C}$. Necessàriament $K = I$.

L.Z. $\Rightarrow$ P.B.O

Donat X considerem $\mathcal{J} = \{(Y,R) : Y \subseteq X$ i R ben ordena $Y\}$.

Definim la relació $\lhd$ a $\mathcal{J}$:

$$(Y,R) \lhd (Z.Z) \text{ sii } Y \subseteq Z \text{ i } S|_Y = R \text{ i}$$
$$\text{per tot } y \in Y \text{ i } z \in Z-Y \ (y,z) \in S$$

$\lhd$ és un ordre parcial no estricte a $\mathcal{J}$ i tota cadena $(X_i, R_i)_{i \in I}$ té cotes superiors (en particular; $(\cup X_i, \cup R_i)$). Existeixen maximals de la forma (X,R), on R ben ordena naturalment X.

P.B.O. $\Rightarrow$ P.T.

Si X i Y admeten bones ordenacions aleshores $X \simeq \alpha$, $Y \simeq \beta$ per certs ordinals α i β i $\alpha \subseteq \beta$ ó $\beta \subseteq \alpha$. D'on: $X \leqslant Y$ ó $Y \leqslant X$.

P.T. $\Rightarrow$ P.E.

Donats X i Y tenim $X \leqslant Y$ ó $Y \leqslant X$ i aleshores és possible de construir una epijecció d'X en Y de Y en X.

P.E. $\Rightarrow$ P.B.O.

Sigui X un conjunt i k un cardinal. Si existeix una epijecció $f : k \to X$, aleshores X es pot ben ordenar; si $x_1, x_2 \in X$, fem $x_1 < x_2$ sii el primer element de $f^{-1}(x_1)$ és més petit que el primer element de $f^{-1}(x_2)$.

Suposem ara que, per tot cardinal k, no existeix cap epijecció sobre X. Aleshores X s'espijectarà sobre tots els cardinals. En X tenim doncs tantes particions diferents com cardinals. Però una partició $\mathcal{G} \subseteq P(X)$ i, per tant, el conjunt.

$$\{\mathcal{G} : \mathcal{G} \text{ particions d'X induides}\} \subseteq P^3(X) .$$

Aleshores tenim una aplicació injectiva de Card en $P^3(X)$. Impossible!

P.B.O. $\Rightarrow$ A.C.

Ja ho hem indicat a la introducció. Donada una família $\mathcal{A} = \{A_i : i \in I\}$ ben ordenem $\bigcup_{i \in I} A_i$ i, a a cada A_i, $i \in I$, li associem el $<_i$-primer element.

(Nota: elegim un bon ordre en el conjunt de tots els bons ordres d' $\bigcup_{i \in I} A_i$ que, per hipòtesis, és no buit. Això no necessita pas l'A.C.)

$\square$

L'A.C. permet d'associar a cada cojunt X un número *cardinal* -si bé aquest concepte pot introduir-se també a Z.F. però d'una forma molt més sofisticada (veure nota bibliogràfica).

Si disposem de l'A.C. disposem del P.B.O. i, per tant, per cada conjunt X,

$$\{\alpha : \alpha \in \mathrm{Ord}: \alpha \sim X\}$$

és no buit. Anomenarem *cardinal d'X, car (X) , el primer element de l'anterior conjunt* i és fàcil de constatar que és un ordinal inicial.

El concepte de cardinal, degut a CANTOR [10] , data de 1878, i mesura la grandària dels conjunts i aquesta grandària es pot mesurar usant un cert tipus de nombre ordinal, si hom disposa de l'A.C.

NOTA BIBLIOGRÀFICA

El concepte de cardinal és de CANTOR 1878 [10] , així com també el concepto d'ordinal [13,14] . Aquests conceptes els milloraria sensiblement von NEUMANN. La conjectura de la bona ordenació també és presentada per CANTOR en 1883 [11] . Els diferents teoremes d'equivalència que hem donat porten adjunta la seva nota bibliogràfica.

Una exposició detallada de l'equivalència de l'A.C. pot trobar-se a D.J. MONK [37] , a A. LEVY [36] i d'altres. L'excel.lent obra de RUBIN i RUBIN [48] és, però, encara avui un text força exhaustiu d'equivalències de l'A.C. També és digne de menció l'obra de T. JECH [29] .

A aquesta darrera així com a RUBIN i RUBIN hom podrà trobar un tractament del concepte de cardinal d'un conjunt sense A.C., si bé on podem trobar-ho exposat més sistemàticament , donant els teoremes de A.TARSKI [50] que impliquen l'A.C., és a l'obra de A. LEVY [36] .

A les obres de JECH [28,29,30] el lector realment interessat en el tema podrà assabentar-se de la *independència lògica* de l'A.C. respecte dels altres axiomes de Z.F. (Això, àdhuc una breu notícia, s'escapa dels propòs its d'aquesta xerrada).

Finalment, el lector interessat en axiomes *més febles* que l'A.C., com són l'axioma de l'ideal principal, d'elecció per a col.leccions numerables, o de les eleccions depenents, pot consultar JECH [29] i A. LEVY, op. cit.

Una lleugera informació sobre l'axioma de *determinació* , incompatible amb l'axioma de l'elecció, però que permet d'establir que tot subconjunt d'$\mathbb{R}$ és mesurable de LEBESGUE, pot trobar-se a [5,29] i una anàlisi més aprofundida a [30] .

4.- L'AXIOMA DE L'ELECCIÓ I EL QUEFER MATEMÀTIC

Hem vist que, si bé l'A.C. por ésser en certa forma nefast en teoria de la mesura, és molt bo al sí de la teoria Z.F. de conjunts. Però què aporta al quefer matemàtic?

Farem un repàs ràpid i, en absolut, exhaustiu de l'A.C. en la matemàtica bàsica que hom troba els primers anys de llicenciatura.

A. Usant el *principi del bon ordre* tenim

A1. "Tot conjunt X és ordre isomorf a un únic ordinal"

A1'. "Tot conjunt X és equipotent a un ordinal al menys".

A1" "Existeix cardinal d'X"

A2. "Un conjunt X és infinit sii és infinit de DEDEKIND"

Un conjunt X és *finit* sii $X \sim n$ per un cert nombre natural n; altrement es *infinit*.

Un conjunt X és *infinit de DEDEKIND* sii existeix $Y \subsetneq X$, $Y \sim X$.

Es fàcil veure que

"si X és infinit de DEDEKIND és infinit" (ja que cap nombre natural <u>n</u> no és infinit de DEDEKIND, per inducció);

"si X conté un subconjunt equipotent a ω és infinit de DEDEKIND" (obviament);

Per veure A2 ben ordenem X i aleshores existeix un cardinal $k \sim X$ i, si X és infinit, $k \geqslant \omega$ i, per tant, X conté un subconjunt equipotent a ω.

A3. "Existeix clausura algebraica d'un cos K" (tal com ho establí STEINITZ en 1910).

B. Usant l'*axioma de l'elecció* tal com l'hem introduit a la pàgina 1.

B1. "La unió numerable de conjunts numerables és numerable".

B1' "Els racionals són numerables", "els trascendents existeixen".

Si $\mathcal{A} = \{A_n : n \in \omega\}$ és una col.lecció numerable de conjunts numerables

$$A_n = \{a_{n0}, a_{n1}, \ldots, a_{nm}, \ldots\}$$

aleshores hem d'enumerar $A = \bigcup_{n \in \omega} A_n$. El mètode usual diu que enumerem seguint les fletxes

$$\begin{array}{cccccc}
a_{00} & \overset{\downarrow}{a_{01}} & \overset{\downarrow}{a_{02}} & \ldots & \overset{\downarrow}{a_{0m}} & \ldots \\
\leftarrow a_{10} \leftarrow & \overset{\downarrow}{a_{11}} & \overset{\downarrow}{a_{12}} & \ldots & \overset{\downarrow}{a_{1m}} & \ldots \\
\leftarrow a_{20} \leftarrow & a_{21} \leftarrow & \overset{\downarrow}{a_{22}} & \ldots & \overset{\downarrow}{a_{2m}} & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots \\
\leftarrow a_{m0} \leftarrow & a_{m1} \leftarrow & a_{m2} \leftarrow & \ldots \leftarrow & \overset{\downarrow}{a_{mm}} & \ldots \\
\ldots & \ldots & \ldots & \ldots & \ldots & \ldots
\end{array}$$

i obtenim

$$a_{oo}\ a_{01}\ a_{11}\ a_{1o}\ a_{o2}\ a_{22}\ a_{21}\ a_{2o}\ \cdots$$

On s'usa l'elecció? Donada una col.lecció *enumerem els seus elements*. Ara disposem d'una col.lecció de conjunts numerables que cal *enumerar*. Sigui E_n el conjunt de *totes* les enumeracions possibles d'A_n ; disposem d'una col.lecció $\mathcal{E} = \{E_n : n \in \omega\}$ i hem de triar un element a cada E_n *simultàniament*. Cal doncs elecció.

Tenim, per cada $n \in \omega$, una funció $f_n \in E_n$ tal que

$$f_n\,(m) = a_{nm}$$

i construïm

$$f(n,m) = f_n(m)\ .$$

B2. "Per calcular el cardinal de $\bigcup_{i \in I} A_i$ en funció dels cardinals dels A_i, $i \in I$".

B3. "Tota epijecció $\pi : X \to Y$ admet una inversa parcial $f : Y \to X$ tal que $\pi \circ f = Id_Y$".

B3' "card $Y \leqslant$ card X, si existeix una epi jecció d'X en Y".

B4. "Un punt $x_o \in \mathbb{R}$ és d'acumulació de K sii és punt límit de K ".

Un punt $x_o \in \mathbb{R}$ és un punt d'*acumulació de K* sii tot entorn d'X conté punts de K diferents d'x .

Un punt $x_o \in \mathbb{R}$ és un punt *límit de K* sii existeix una successió $(x_n)_{n \in \omega}$ de punts diferents de K tal que $\lim_{\pi \to \infty} x_n = x_o$.

Els punts límits de K són clarament d'acumulació de K .

El recíproc necessita l'A.C.: per cada $n \in \omega$ considerem l'entorn E_n de centre x i radi 1/n . Elegim *simultàniament* un punt a cada E_n i hem acabat.

Nota.
Pensem el teorema de BOLZANO-WEIERSTRASS: "tot conjunt acotat i infinit té un punt d'acumulació o un punt límit".

No hi ha diferència entre un teorema i l'altre si infinit significa "infinit" (veure A.2); en canvi, si infinit significa "infinit de DEDEKIND", aleshores , pels punts límits, cal l'A.C.

B5. "Una funció $f : (a,b) \to \mathbb{R}$ és contínua en x sii ho és per successions".

Sigui $f : (a,b) \to \mathbb{R}$ i $x_0 \in (a,b)$.
f és *contínua en* x_0 sii, per cada $\epsilon > 0$, existeix un $\delta > 0$ tal que

$$|x - x_0| < \delta \quad \text{implica} \quad |f(x) - f(x_0)| < \epsilon$$

f és *contínua en* x_0 *per successions* sii per tota successió $(x_n)_{n \in \omega}$, $x_n \in (a,b)$ convergent cap a x_0

$$\lim_{n \to \infty} x_n = x_0 \quad \text{implica} \quad \lim_{n \to \infty} f(x_n) = f(x_0).$$

La continuitat implica la continuitat per successions.

Si f és contínua per successions en x_0 i *no és contínua* aleshores existeix un $\epsilon > 0$ tal que, per cada $1/n$,

existeix un $x_n \in (x_0 - 1/n, x_0 + 1/n)$ i $|f(x) - f(x_0)| \geq \epsilon$.

Agafem simultàniament a cada I_n $(x_0 - 1/n, x \cdot 1/n)$ un punt x_n .
Tindrem $x_n \to x_0$ i $f(x_n) \not\to f(x_0)$.

B6. "Un espai mètric és separable sii la seva topologia admet una base comptable".

B6'. "Tot subespai d'un espai mètric separable és separable".

B7. El teorema de NIELSEN-SCHREIER: "tot subgrup d'un grup lliure és lliure".

C. En la forma de *lema de ZORN* s'estableix fàcilment:

C1. "tot anell amb unitat té un ideal maximal"

Els ideals d'un anell amb la inclusió satisfan la premissa del L.Z.; per tant existeixen elements maximals.

C1'. "Tot ideal d'un anell amb unitat està contingut en un ideal maximal";

C1''. "Tot cos K admet una clausura algebraica única".

A cada $p(x) \in K[x]$ de grau n li associem n indeterminades $y_1^{(p)}, \ldots, y_n^{(p)}$; sigui $K[x][y]$, on $y = \{y_i^{(p)} : p \in K[x], i = 1, \ldots, \text{grau } p\}$.

Sigui I l'ideal engendrat pels elements de la forma

$p(x) - (x - y_1^{(p)}) \ldots (x - y_n^{(p)})$

$p(y_i^{(p)})$

i agafem l'ideal maximal J de $K[x][y]$ que conté I . Aleshores $K^* = K[x][y]/J$ és l'extensió buscada.

La unicitat s'obté usant també el lema de ZORN. Hom considera la família

$\mathfrak{F} = \{f : f$ és un isomorfisme de H_1 en H_2, on H_1 és un cos intremig entre K i K_1 i H_2 entre K i $K_2\}$.

on K_1 i K_2 són dues extensions. A $\mathfrak{F}$ hi definim una relació d'ordre per extensió i veiem que podem aplicar el lema de ZORN. L'element maximal és el buscat.

Cl"! "Tot ideal d'una àlgebra de BOOLE pot submergir-se en un ideal maximal".

Cl"" Teorema de STONE. "Tota àlgebra de BOOLE és una àlgebra de parts d'un conjunt".

C2. Els teoremes de completesa i de compacitat de la lògica del càlcul de predicats de primer ordre.
El mateix pel càlcul de proposicions.

En realitat cal veure que tot conjunt consistent es pot submergir en un conjunt consistent maximal i això és una conseqüència immediata del lema de ZORN.

C3. El teorema de HANH-BANACH: "si M és un subespai d'un espai lineal normat E i φ és un funcional lineal acotat en M, podem estendre'l a un funcional lineal acotat f sobre E de manera que $\|\varphi\| = \|f\|$."

Hom considera la col.lecció de totes les parelles ordenades (M',f'), on M' és un subespai vectorial d'E que conté M i f' és una extensió lineal de φ a M' amb $\|f'\| = \|\varphi\|$. Aleshores s'ordena aquesta família de forma natural i s'aplica el lema de ZORN. L'element maximal resol la qüestió.

D. Usant el *lema de TUKEY* tenim:

D1. "Tot espai vectorial E té una base"

La família de subconjunts linealment independents d'E té caràcter finit i qualsevol dels seus elements maximals és una base d'E.

Hom pot usar tanmateix el lema de ZORN.

D2. El teorema de TYCHONOFF: "El producte d'una família d'espais compactes és compacte".

Sigui $\mathcal{G} = \{X_i : i \in I\}$ una família d'espais compactes i $X = \prod_{i \in I} X_i$.

Hem de veure que, si β és una família de tancats d' X que té la p.i.f. (propietat de les interseccions finites que diu que les interseccions de les subfamílies finites és $\neq \emptyset$, aleshores $\cap\beta \neq \emptyset$.

Sigui $\mathcal{C}$ la classe de totes les famílies de tancats amb la p.i.f. Aquesta classe té caràcter finit i conté un element maximal que conté la classe β . Suposem ara, sense perdre generalitat, que β és maximal i que β satisfà la p.i.f. Sigui

$$\beta_i = \{\pi_i < B > : B \in \beta\} \quad .$$

β_i satisfà la p.i.f. i X_i és compacta. Per tant

$$H_i = \cap \overline{\pi_i < B >} \neq \emptyset \quad .$$

Sigui finalment $x_i \in H_i$ i $x = (x_i)_{i \in I} \in X$. Hom constata que $x \in B$ per cada $B \in \beta$.

Podem indicar, per acabar, que el teorema de TYCHONOFF i l'existència d'ideals maximal per a reticles són equivalents a l'A. C.

D'altres resultats, com són B1, B4, i B5, depenen solament de l'A. C. numerable.

C1"' i C2 depenen, i de fet són equivalents, a C1'.

Sorprèn, a la vista de la gran utilitat de l'A. C., llegir FRAENKEL quen en la nota històrica que apareix a l'obra de BERNAYS [6] , diu:

> "... alguns autors com BOREL i DENJOY creuen més acceptable l'axioma quan <u>t</u> és numerable, mentre que l'escepticisme de LEBESGUE i d'altres no fa distincions entre numerable i no numerable. L'oposició a l'axioma es basa, en part, sobre certes paradoxes que d'ell s'en segueixen, com el teorema de BANACH-TARSKI ..."

Els matemàtics, però, no poden ja avui dia renunciar a l'A. C. Així doncs cal acceptar l'existència de subconjunts d'$\mathbb{R}$ no mesurables de LEBESGUE i l'anomenada paradoxa de BANACH-TARSKI a canvi de disposar en el quefer matemàtic d'aquesta eina potent i irrenunciable de la matemàtica que és l'A. C.

<u>NOTA BIBLIOGRÀFICA</u>

Les demostracions de A1 i B2 poden trobar-se a qualsevol llibre de teoria de conjunts, com [33,36,37] . A2 podem trobar-lo a DEDEKIND [16] i a SUPPES [49] . A3 a STEINITS [47] . B1 a CANTOR [10] i B1' també a CANTOR [15]. Veure així mateix JECH [29] i BARWISE [5] . B2 es troba a [35] . B4 i B5 estan desenvolupats a [22] , B6 a [29,36] i B7 a [42] . C1 i C1' i C1" podem trobar-los a [20] i [29] mentres que C1''' i C1'$^{\nu}$ a MONK [38] . C2 també a [38] i [4].

C3 a [2,32 i 39] . A [39] MUNROE fa servir a la demostració el P.B.O.

D1 podem trobar-lo a [29] , si bé cal dir que històricament el primer en adonar-se de la necessitat de l'A. C. en aquest fe fou HAMEL [24] .

D2 podem trobar-lo a [53,36,8,27] . L'equivalència de D2 amb l'A. C. és troba a KELLEY [31] i l'equivalència entre l'A. C. i l'existència d'ideals maximals d'un reticle es de D.SCOTT [45]. Tota aquesta informació i d'altre pot trobar-se en definitiva a JECH [29].

BIBLIOGRAFIA

[1] BANACH, S. *Sur le problème de mesure.* Fund. Mat. 4 1923, pp. 30-37.

[2] BANACH, S. *Théorie des operations linéaires.* 1932, Monographic Math., Tom 1.

[3] BANACH, S. TARSKI, A. *Sur les décompositions des ensembles de points en parties respectivement congruents.* Fund. Math. 6, 1924, pp. 224-277.

[4] BARNES, MACK, *An Algebraic Introduction to Mathematical Logic.* 1975, GTM 25, Springer-Verlag.

[5] BARWISE, J. *Handbook of Mathematical Logic.* Editor. Studies in Logic. Vol. 90, 1977, North-Holland.

[6] BERNAYS, P. FRAENKEL, A.A. *Axiomatic Set Theory.* Studies in Logic, 1958. North-Holland.

[7] BOREL, E. *Quelques remarques sur les principes de la théorie des ensembles.* Math. Ann., 60, 1904, pp. 194-195.

[8] BOURBAKI, N. *Topologie Général.* Actualités Sci. Ind. 858 (1940), 916 (1942).

[9] BRUCKNER, A. M. CEDER, J. *On improving Lebesgue measures.* Nord. Math. Tidsk. 23 II, 1975, pp. 59-68.

[10] CANTOR, G. *Ein Beitrag zur Mannigfaltigkeitslehre* . Jour. F. Math., 84, 1878, pp. 119-138.

[11] CANTOR, G. *Über unendliche lineare Punktmannigfaltigkeiten.* Nr. 5, Math. Ann., 21, 1883, pp. 545-586.

[12] CANTOR, G. *Über eine elementare Frage der Mannigfaltigkeitslehre* . Jahresber. Deutsch. Math. Verein 1, 1982, pp. 75-78.

[13] CANTOR, G. *Beiträge zur Begründug der transfiniten Mengenlehre 1* . Math. Ann., 46, 1895, pp. 481-512.

[14] CANTOR, G. *idem, 2* . Math. Ann., 46, 1897, pp.207-246.

[15] CANTOR, G. *Letters to DEDEKIND.*

[16] DEDEKIND, R. *Was sind und was sollen die Zahlen?* Gas. Math. Works, t. III, 1972, pp. 335-391.

[17] DEVLIN, K.J. *Fundamentals of Contemporary Set Theory.* Universitext, 1979, Springer-Verlag.

[18] DEVLIN, K.J. *The axiom of Constructability.* Lecture Notes in Math., 617, 1970. Springer-Verlag.

[19] DIEUDONNÉ, J. et autres. *Avégé d'histoire des mathématiques 1700-1900*, vol. II, 1978, Hermann.

[20] DUBREIL, JACOTIN. *Leçons d'âlgebre moderne.* 1964, Dunod.

[21] FRAENKEL, A.A. *Zu den Grundlagen der Cantor-Zermeloschen Mengenlehre.* Math. Ann., 86, 1922, pp. 230-237.

[22] FRAENKEL, A.A. BAR-HILLEL, Y. LEVY, A. *Foundations of set Theory.* Studies in Logic 1973, North-Holland.

[23] HARDAMARD, J. BAIRE, R. LEBESGUE, H. et BOREL, E. *Cinq lettres sur la théorie des ensembles.* Bull . Soc. Math. France, 1905, pp. 261-273.

[24] HAMEL, G. *Eine Basis aller Zahlen und die unstetige Lösungen der Funktionalgleichung f(x+y)=f(x)+f(y)* Math. Ann., 60, 1905, pp. 459-462.

[25] HARTOG, F. *Über das Problem der Wohlordnung.* Math. Ann., 76, 1915, pp. 438-443.

[26] HAUSDORFF, F. *Grundzüge der Mengenlehre.* Lipzig 1914.

[27] HU, S.T. *Introduction to General Topology.* 1966 Holden-Day.

[28] JECH, T. *Lectures in Set Theory.* Lecture Notes No. 217, 1977, Springer-Verlag.

[29] JECH, T. *The axiom of choice.* Studies in Logic, 1973, North-Holland.

[30] JECH, T. *Set Theory* . 1978. Academic Press.

[31] KELLEY, J.L. *The Thychonoff product theorem implies the axiom of choice.* Fund. Math., 37,1950, pp. 75-76.

[32] KOLMOGORV, FOMIN. *Elementos de la teoría de funciones y del análisis funcional.* 1972. Editorial MIR.

[33] KUNEN, K. *Set Theory. An Introduction to Independence Proofs.* Studies in Logic 102, 1980, North-Holland.

[34] LEBESGUE, H. *Sur les fonctions représentables analytiquement.* Jour. Math. Pures et App., 1905, pp. 139-216.

[35] LEVI, B. *Intorno alla teoria degli aggregati.* Rend. Inst. Lombardo de Science e Lettere. Rendic. (2) 35, 1902, pp. 863-868.

[36] LEVY, A. *Basic Set Theory.* Persp. Math. Logic.,1979 Springer-Verlag.

[37] MONK, K. *Introduction to Set Theory.* McGraw Hill. 1969.

[38] MONK, D. *Mathematical Logic.* G.T.M., No. 37, 1976. Springer-Verlag.

[39] MUNROE. *Introduction to Measure and Integration.* 1959. Addison-Wesley.

[40] PEANO, G. *Démostration de l'integrabilité des équations différencielles ordinaires.* Math. Ann., 37, 1890, pp. 182-228.

[41] ROBINSON, R.M. *On the descomposition of the sphere.* Fund. Math., 34, 1947, pp. 246-260.

[42] ROTMAN, J.J. *The Theory of Groups. An Introduction.* Allyn and Bacon, Inc. 19-65.

[43] RUDIN, H. RUDIN, J. *Equivalents of the Axiom of Choice.* Studies in Logic 1970. North-Holland.

[44] RUSSELL, B. *On some difficulties in the theory of transfinite numbers and order types.* Proc. London Math. Soc., (2) 4, 1906, pp.29-53.

[45] SCOTT, D. *The theorem on maximal ideals in lattices and the axiom of choice.* Bull.Am.Math.Soc. 60, 1954, p. 83.

[46] SIERPINSKI,W. *Fonctions additives non completement additives et fonctions non mesurables.* Fund. Math., 30, 1938, pp. 96-99.

[47] STEINITZ, E. *Algebraische Theorie der Körper.* J. Fur die Reine und Angew.Math., 137, 1910, pp. 167-309.

[48] STROMBERG, K. *The Banach-Tarski Paradox.* Am. Math. Monthly. 86, No. 3, 1979. pp. 151-167.

[49] SUPPES, P. *Axiomatic Set Theory.* 1960. Van Nostrand.

[50] TARSKI, A. *Sur quelques théoremes qui equivalent a l'axiome de choice.* Fund. Math., 5, 1923, pp. 147-154.

[51] TEICHMULLER,J.W. *Braucht der Algebraiken das Auswahlaxiom?* Deutsche Zeit. Math., 4, 1939, pp. 567-577.

[52] TUKEY, J.W. *Convergence and uniformity in topology.* Ann. Math. Studies, No. 2, 1940, Princeton.

[53] TYCHONOFF, A. *Über eine Functionenraum.* Math. Ann., 111, 1935, pp. 762-682.

[54] VITALI, G. *Sul Problema della Mesura dei Gruppi di Punti di una Retta.* 1905. Bolonia.

[55] WHITEHEAD, A.N. *Principia Mathematica.* Vol. II, 1912.
RUSSELL, B.

[56] ZERMELO, E. *Beweis, das jede Menge wohlgeordent werden kann.* Math. Ann., 59, 1904, pp.514-516.

[57] ZERMELO, E. *Untersuchungen über die Grundlagen der Mengenlehere* . Math. Ann., 65, 1908, pp. 261-281.

[58] ZERMELO, E. *Neuer Beweis für die Wohlordnung.* Math. Ann., 65, 1908, pp. 107-128.

[59] ZORN, M. *A remark on method in transfinite algebra.* Bull. Am. Math. Soc. 41, 1935, pp.667-670.