MULTIMI FINITE SI ELEMENTE DE COMBINATORICA

#

MULŢIMI FINITE ŞI ELEMENTE DE COMBINATORICĂ

de MIRCEA BECHEANU

0. INTRODUCERE

În această lecţie vom urmări două obiective :

a) să înţelegem ce este o problemă de Combinatorică,

b) să prezentăm unele metode de rezolvare a acestor probleme.

Lecţia cuprinde următoarele paragrafe :

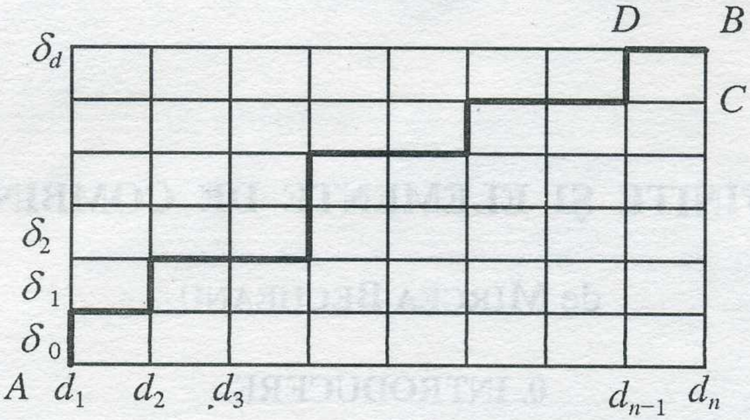
0. Introducere
1. Principiul includerii şi excluderii
2. Câteva probleme de combinatorică cu mulţimi finite
3. Combinatorica grupurilor finite. Grupuri de permutări

Combinatorica sau Analiza combinatorială este o ramură clasică a matematicii. Cu toate acestea, deşi mari matematicieni s-au ocupat de probleme de Combinatorică, ea pare să ocupe un loc singular între celelalte discipline matematice, în primul rând prin faptul că nu poate fi axiomatizată. Adoptând o clasificare bazată pe sisteme axiomatice ar trebui s-o încadrăm, poate, în marele capitol al Teoriei numerelor. Dar este clar că ea se ocupă de alte probleme decât Teoria numerelor.

Combinatorica se interferează cu disciplinele matematice axiomatizate din care extrage metode sau pe care le serveşte cu rezultate. O caracteristică a Combinatoricii, care o face atractivă atât pentru începători cât şi pentru profesionişti este faptul că ea abordează probleme concrete, al căror enunţ este în general uşor de înţeles şi care poate fi uneori chiar nematematic. Iar când înveţi matematică sau când înveţi pe cineva matematică asemenea probleme sunt cu deosebire potrivite şi atractive. Iată o asemenea problemă.

(0.1) *Un oraş are forma unui dreptunghi şi o reţea de străzi paralele formată din n străzi pe direcţia nord–sud şi d +1 străzi pe direcţia est–vest. În câte moduri poate ajunge un automobil din colţul de sud–vest în colţul de nord–est al oraşului, menţinând tot timpul direcţia de mers de la vest spre est şi de la sud către nord ?*

În figura de mai jos prezentăm un asemenea drum care uneşte punctele A şi B. Pe figură am notat :



cu $d_1, d_2,..., d_n$ cele n străzi verticale şi cu $\delta_0, \delta_1,..., \delta_d$ cele d+1 străzi orizontale. Să numim porţiunea cuprinsă între două străzi paralele consecutive un cvartal. O analiză atentă (chiar nematematică!) ne arată că un drum de la A la B este perfect determinat de numărul de cvartale parcurs pe fiecare din drumurile verticale $d_1, d_2,..., d_n$. Presupunând că numărul acestor cvartale este, respectiv, $k_1, k_2,..., k_n$ atunci $k_i \geq 0$ sunt numere naturale şi

(0.1.1) $$k_1 + k_2 + ... + k_n = d.$$

Aşadar, numărul drumurilor de la A la B coincide cu numărul sistemelor ordonate de numere naturale $(k_1, k_2,..., k_n)$ care verifică ecuaţia diofantică

$$x_1 + x_2 + ... + x_n = d.$$

Am regăsit astfel problema lui *Moivre*, o problemă clasică de combinatorică (sau de aritmetică!) : *în câte moduri se poate reprezenta un număr natural d ca sumă de n numere naturale* ?

Pentru algebrişti, această problemă este echivalentă cu următoarea :

Care este numărul monoamelor unitare $X_1^{k_1} X_2^{k_2} \dots X_n^{k_n}$ *în n nedeterminate şi de grad d conţinute în inelul polinoamelor* $\mathbf{R}[X_1, X_2, \dots, X_n]$ (de exemplu!) ? Este interesant de ştiut acest lucru căci numărul acestor monoame este dimensiunea spaţiului vectorial al polinoamelor omogene (formelor) de grad d.

În acest moment avem trei caracterizări echivalente ale numărului căutat, dar nu ştim care este acesta. Să încercăm o altă abordare !

Fie $N_{n,d}$ numărul căutat. Se vede uşor că $N_{n,1} = n$ şi că $N_{n,2} = \frac{1}{2}n(n+1)$. Deorece orice drum de la A la B trece obligatoriu prin C sau D, rezultă relaţia de recurenţă :

(0.1.2) $$N_{n,d} = N_{n-1,d} + N_{n,d-1}.$$

Aceeaşi formulă de recurenţă poate fi dedusă astfel : orice monom de grad d în $X_1,\dots, X_n$ este un monom de grad d în $X_1,\dots, X_{n-1}$ sau se obţine prin înmumlţire cu X_n dintr-un monom de grad $d-1$ în $X_1,\dots, X_n$.

Se prefigurează astfel o idee de recurenţă dublă ; exploatarea acesteia necesită însă unele calcule.

Vom regândi "problema drumurilor" astfel : presupunem că cele n drumuri verticale sunt n tuburi cilindrice d_1, d_2,..., d_n. în care trebuie să repartizăm d bile albe. Evident că dacă în tubul d_i repartizăm k_i bile avem relaţia (0.1.1). După repartizare adăugăm în fiecare tub o bilă roşie, în total n, bile roşii şi aşezăm tuburile orizontal, unul în prelungirea celuilalt , în ordinea iniţială. Se obţine în acest fel un şir de $n + d$ bile albe şi roşii. Repartizarea bilelor albe în tuburi este perfect descrisă de locurile în şir alese pentru a plasa bilele roşii. Cu observaţia că ultimul loc este ocupat întotdeauna de o bilă roşie, rezultă că numărul căutat este :

$$N_{n,d} = \binom{n+d-1}{n-1} = \binom{n+d-1}{d}.$$

Se vede uşor că numerele $N_{n,d}$ astfel obţinute verifică relaţia (0.1.2).

În concluzie, s-a obţinut următorul rezultat : numărul drumurilor de la A la B este egal cu numărul şirurilor ordonate de n numere naturale a căror sumă este d, este egal cu numărul monoamelor unitare în n nedeterminate şi de grad d, este egal cu numărul repartiţiilor a d bile în n tuburi şi este $N_{n,d}$. Analiza retrospectivă a modului în care s-a obţinut acest rezultat pune în evidenţă următorul principiu : pentru a număra elementele unei mulţimi, căutăm s-o înlocuim cu o altă mulţime, având acelaşi număr de elemente şi ale cărei elemente pot fi mai uşor numărate..

(0.2) *Fie n, $m \geq 2$ numere naturale, S o mulţime cu n elemente şi $A_1,\dots, A_m$ submulţimi ale lui S. Să se arate că dacă pentru orice două elemente x, $y\in S$ există o submulţime A_i astfel încât $x\in A_i$ şi $y\notin A_i$ sau $x\notin A_i$ şi $y\in A_i$, atunci $n \leq 2^m$.*

(Olimpiada Balcanică, 1997)

Imaginăm următorea construcţie : asociem fiecărui element $x\in S$ un şir de m numere binare $a(x) = (x_1, x_2,\dots, x_m)$ unde $x_i = 1$ dacă $x\in A_i$ şi $x_i = 0$ dacă $x\notin A_i$. Se obţine în acest fel o funcţie $a: S \to \{(x_1,\dots,x_m) \mid x_i \in \{0,1\}\}$ iar ipoteza spune că $x \neq y \Rightarrow a(x) \neq a(y)$, adică această funcţie este injectivă. Deci, $n \leq 2^m$.

Şi această problemă pune în evidenţă o metodă : pentru a demonstra inegalitatea, am transformat ipoteza privind familia de submulţimi $(A_i)_{1 \leq i \leq n}$ într-o metodă de comparare a mulţimii S cu mulţimea şirurilor binare de lungime m.

(0.3) *La o masă de formă circulară sunt aşezate un număr par de persoane. După o pauză, participanţii se aşează în jurul aceleiaşi mese, ocupând eventual locuri diferite. Să se arate că există cel puţin două persoane astfel încât numărul persoanelor aşezate între ele să fie acelaşi ca înainte de pauză.*

(O.I.M., 1988)

Problema este echivalentă cu următoarea : fiind dată o permutare $\sigma \in S_{2n}$, există o pereche de numere i, j astfel încât

$$|i-j| = |\sigma(i) - \sigma(j)|.$$

Vom imagina pentru aceasta următoarea situaţie : presupunem că cele $2n$ numere sunt vârfurile $P_0, P_1, \ldots, P_{2n-1}$ ale unui poligon regulat. Permutarea σ poate fi interpretată ca o rotaţie a fiecărui vârf P_i cu un unghi $t_i = k_i \cdot \frac{2\pi}{2n} = \frac{\pi k_i}{n}$, unde $k_i \in \{0,1,\ldots,2n-1\}$. Dacă numărul de vârfuri între P_i şi P_j rămâne neschimbat după rotaţie rezultă că cele două vârfuri s-au rotit cu aceleaşi unghiuri, deci $k_i = k_j$. Dacă, prin absurd, presupunem că toate unghiurile sunt diferite, rezultă că unghiurile de rotaţie sunt

$$0, \frac{\pi}{n}, \frac{2\pi}{n}, \ldots, \frac{(2n-1)\pi}{n}.$$

Suma acestor unghiuri este $\frac{\pi}{n}(0+1+\ldots+(2n-1)) = (2n-1)\pi$. Însă suma lor trebuie să fie de forma $2k\pi$ deoarece reprezintă suma după i, $i = 1,\ldots, 2n-1$, a unghiurilor $\angle P_0OP_i$, luată modulo 2π.

În această problemă, ideea principală a fost de a modela situaţia dată într-o situaţie mai clară din punct de vedere matematic, astfel încât un aparat adecvat să poată fi folosit.

Din analiza acestor exemple rezultă următoarea întrebare : *există metode generale prin care să se poată număra elementele unei mulţimi* ?

Combinatorica ne pune la dispoziţie asemenea metode dar ne şi învaţă cum să procedăm pentru a le găsi când întâlnim probleme ca cele de mai sus.

Back

#

1. PRINCIPIUL INCLUDERII ŞI EXCLUDERII. APLICAŢII

Spunem că o mulţime A este finită dacă există o funcţie bijectivă

$$f:\{1,2,\ldots,n\}\to A.$$

Atunci numărul n este unic şi spunem că A este finită cu n elemente sau că A este o mulţime de cardinal n. Vom nota cu $|A|$ cardinalul (sau numărul de elemente al) mulţimii A.

(1.1) Teoremă (principiul includerii şi excluderii). *Fie $A_1,\ldots,A_n$ o familie de mulţimii finite. Atunci cardinalul mulţimii $A_1\cup A_2\cup\ldots\cup A_n$ este dat de formula* :

$$\left|A_1\cup A_2\cup\ldots\cup A_n\right|=\sum_{i=1}^{n}|A_i|-\sum_{1\le i<j\le n}|A_i\cap A_j|+\ldots+(-1)^{k-1}\sum_{i_1<\ldots<i_k}|A_{i_1}\cap\ldots\cap A_{i_k}|+\ldots$$

$$\ldots+(-1)^{n-1}|A_1\cap A_2\cap\ldots\cap A_n|,$$

cunoscută ca formula lui Boole-Sylvester.

Demonstraţie. Procedăm prin inducţie după n. Pentru $n=2$ trebuie să demonstrăm formula :

$$|A_1\cup A_2|=|A_1|+|A_2|-|A_1\cap A_2|.$$

Aceasta rezultă din faptul că $A_1\cup A_2$ este reuniunea mulţimilor disjuncte A_1 şi $A_2\setminus(A_1\cap A_2)$, iar A_2 este reuniunea mulţimilor disjuncte $A_2\setminus(A_1\cap A_2)$ şi $A_1\cap A_2$. Din egalităţile :

$$|A_2|=|A_2\setminus(A_1\cap A_2)|+|A_1\cap A_2|$$

$$|A_1\cup A_2|=|A_1|+|A_2\setminus(A_1\cap A_2)|$$

rezultă egalitatea de demonstrat.

Presupunem că formula din enunţ este adevărată pentru familii de $n-1$ mulţimi şi o vom demonstra pentru familii de n mulţimi :

$$\left|\bigcup_{i=1}^{n}A_i\right|=\left|\bigcup_{i=1}^{n-1}A_i\cup A_n\right|=\left|\bigcup_{i=1}^{n-1}A_i\right|+|A_n|-\left|\left(\bigcup_{i=1}^{n-1}A_i\right)\cap A_n\right|=$$

$$=\sum_{i=1}^{n-1}|A_i|+|A_n|-\sum_{1\le i<j\le n-1}|A_i\cap A_j|+\ldots+(-1)^{k-1}\sum_{1\le i_1<\ldots<i_k\le n-1}|A_{i_1}\cap\ldots\cap A_{i_k}|+\ldots$$

$$\ldots+(-1)^{n-2}|A_1\cap\ldots\cap A_{n-1}|-\left|\bigcup_{i=1}^{n-1}(A_i\cap A_n)\right|=$$

$$=\sum_{i=1}^{n}|A_i|-\sum_{1\le i<j\le n-1}|A_i\cap A_j|+\ldots+(-1)^{k-1}\sum_{1\le i_1<\ldots<i_k\le n-1}|A_{i_1}\cap\ldots\cap A_{i_k}|+\ldots$$

$$\ldots+(-1)^{n-2}\left|A_1\cap\ldots\cap A_{n-1}\right|-\sum_{i=1}^{n-1}\left|A_i\cap A_n\right|+\sum_{1\le i<j\le n-1}\left|A_i\cap A_j\cap A_n\right|-\ldots$$

$$\ldots+(-1)^{n-1}\left|A_1\cap\ldots\cap A_{n-1}\cap A_n\right|.$$

Grupând sumele cu acelaşi număr de factori în intersecţie se obţine formula din enunţ.

Observaţie. Formula lui *Boole-Sylvester* se mai scrie sintetic astfel :

$$\left|\bigcup_{i=1}^{n} A_i\right| = \sum_{I\subset\{1,2,\ldots,n\}} (-1)^{|I|+1}\left|\bigcap_{i\in I} A_i\right|. \tag{1.1.1}$$

O formă mai generală a principiului includerii şi excluderii este următoarea. Fie A o mmulţime finită şi $f: B\to[0,\infty)$ o funcţie. Pentru orice submulţime $B\subset A$ notăm :

$$f(B)=\sum_{x\in B} f(x),$$

iar $f(\varnothing)=0$. În aceste ipoteze, dacă $A=\bigcup_{i=1}^{n} A_i$ atunci are loc egalitatea :

$$f(A)=\sum_{I\subset\{1,2,\ldots,n\}} (-1)^{|I|+1} f\left(\bigcap_{i\in I} A_i\right). \tag{1.1.2}$$

Dacă f este funcţia constantă $f(x)=1, \forall x\in A$, atunci se obţine (1.1.1).

Demonstraţia formei generale se face exact ca în cazul (1.1).

În continuare vom prezenta câteva exemple clasice de utilizare a principiului includerii şi excluderii urmate de câteva probleme utilizate în concursuri.

Back

#

(1.2) Indicativul lui *Euler*

Fie $n>1$ un număr natural. Mulţimea $\{0,1,2,\ldots, n-1\}$ constituie un sistem complet de resturi modulo n, cu alte cuvinte, dacă notăm

$$R_i=\{nk+i \mid k\in\mathbf{Z}\}$$

atunci $R_0, R_1, \ldots, R_{n-1}$ sunt toate elementele inelului $\mathbf{Z}/(n)$ al claselor de resturi modulo n. Elementele inversabile ale inelului $\mathbf{Z}/(n)$ sunt clasele R_i pentru care i este prim cu n. Mulţimea

$$U_n=\{i \mid 0\le i\le n-1, (i,n)=1\}$$

se numeşte un sistem redus de resturi modulo n. Cardinalul mulţimii U_n se notează cu $\varphi(n)$ iar funcţia aritmetică $\varphi: \mathbf{N}^*\to\mathbf{N}$ obţinută în acest mod şi adăugând $\varphi(1)=1$ se numeşte funcţia lui *Euler* sau indicatorul lui *Euler*.

Dacă $p > 1$ este număr prim atunci numerele 1, 2, ..., $p-1$ sunt prime cu p, deci $\varphi(p) = p-1$. Dacă $p > 1$ este număr prim şi $r \geq 1$ atunci un sistem redus de resturi modulo p^r este format din toate numerele şirului

$$1, 2, 3, \ldots, p, p+1, \ldots, 2p, \ldots, p^r$$

care sunt nedivizibile cu p. Numerele divizibile cu p în acest şir sunt p, $2p$, $3p$,..., $p^{r-1}\cdot p$, deci numărul numerelor nedivizibile cu p este

$$\varphi\left(p^r\right) = p^r - p^{r-1} = p^r\left(1 - \frac{1}{p}\right)$$

Să dăm o *formulă generală de calcul pentru* $\varphi(n)$.

Fie $n = p_1^{r_1} \ldots p_m^{r_m}, p_i > 1$ numere prime şi $r_i > 0$. Un număr i din mulţimea $A = \{1, 2, \ldots, n\}$ este prim cu n dacă şi numai dacă a nu este divizibil cu nici unul din numerele prime $p_1, p_2, \ldots, p_m$. Pentru $i = 1, 2,\ldots, m$ notăm

$$A_i = \{a \mid 1 \leq a \leq n, p_i \mid a\}.$$

Rezultă că un sistem redus de resturi modulo n este dat de mulţimea $A \setminus \bigcup_{i=1}^{m} A_i$, iar $\varphi(n) = n - \left|\bigcup_{i=1}^{m} A_i\right|$. Aplicând principiul includerii şi excluderii rezultă că :

$$\varphi(n) = n - \sum_{i=1}^{m}|A_i| + \sum_{1 \leq i < j \leq m}|A_i \cap A_j| - \ldots + (-1)^k \sum_{i_1 < \ldots < i_k}|A_{i_1} \cap \ldots \cap A_{i_k}| + \ldots$$
$$\ldots + (-1)^m |A_1 \cap \ldots \cap A_m|.$$

Dar $|A_i| = \frac{n}{p_i}$, $|A_i \cap A_j| = \frac{n}{p_i p_j}$, etc. Deci :

$$\varphi(n) = n - \sum_{i=1}^{m}\frac{n}{p_i} + \sum_{i<j}\frac{n}{p_i p_j} + \ldots + (-1)^k \sum_{i_1 < \ldots < i_k}\frac{n}{p_{i_1}\ldots p_{i_k}} + \ldots + (-1)^m \frac{n}{p_1 \ldots p_m} =$$
$$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\ldots\left(1 - \frac{1}{p_m}\right).$$

Am obţinut aşadar formula : *dacă* $n = p_1^{r_1} \ldots p_m^{r_m}$ *atunci*

(1.2.1) $$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\ldots\left(1 - \frac{1}{p_m}\right).$$

Din această formulă rezultă următoarea proprietate importantă a indicatorului lui *Euler* : *dacă* $(m, n) = 1$ *atunci*

(1.2.3) $$\varphi(mn) = \varphi(m)\varphi(n).$$

Spunem în acest caz că *funcția lui Euler este o funcție aritmetică multiplicativă.*

Ca aplicație a proprietății lui φ de a fi funcție multiplicativă vom demonstra următoarea proprietate clasică a funcției lui *Euler* :

Pentru orice n

(1.2.4) $$\sum_{d|n} \varphi(d) = n .$$

Demonstrație. Presupunem că $n = p_1^{i_1} \dots p_m^{i_m}$, $i_k > 0$. După o idee a lui *Gauss* vom demonstra afirmația prin inducție după suma $s = i_1 + \dots + i_m$.

Dacă $s = 1$ rezultă că n este număr prim și are doar divizorii 1 și n ; prin urmare suma devine :

$$\varphi(1) + \varphi(n) = 1 + (n-1) = n .$$

Presupunând proprietatea adevărată pentru numerele în care suma exponenților este mai mică decât s, o vom demonstra pentru s. Împărțim mulțimea D a divizorilor lui n în două clase disjuncte : D_1 este mulțimea divizorilor în care p_1 apare la puteri mai mici decât i_1 iar D_2 este mulțimea divizorilor în care p_1 apare la puterea i_1. Avem $D = D_1 \bigcup D_2$ și $D_1 \bigcap D_2 = \varnothing$.

Prin urmare :

$$\sum_{d \in D} \varphi(d) = \sum_{d \in D_1} \varphi(d) + \sum_{d \in D_2} \varphi(d) =$$

$$= \sum_{d | \frac{n}{p_1}} \varphi(d) + \varphi\left(p_1^{i_1}\right) \sum_{d | \frac{n}{p_1^{i_1}}} \varphi(d) =$$

$$= \frac{n}{p_1} + p_1^{i_1}\left(1 - \frac{1}{p_1}\right)\frac{n}{p_1^{i_1}} = \frac{n}{p_1} + n - \frac{n}{p_1} = n.$$

Back

#

(1.3) Calculul numărului numerelor prime dintr-o mulțime

Fie $n > 1$ un număr natural și ne propunem să calculăm numărul numerelor prime din mulțimea $A = \{1, 2, \dots, n\}$. Ideea este de a proceda ca în ciurul lui *Eratostene* ; se șterge 1 care nu este prim, se reține 2 și se șterg multiplii lui 2, se reține 3 și se șterg multiplii lui 3 ș.a.m.d. Pentru numere n mici se poate proceda efectiv ca mai sus, dar pentru numere mari avem nevoie de o analiză mai atentă. Se observă că orice număr compus din A este multiplu al unuia din numerele prime cel mult egale cu $\left[\sqrt{n}\right]$. Fie $p_1 = 2, p_1 = 3, \dots, p_k$ șirul numerelor prime cel mult egale cu $\left[\sqrt{n}\right]$. Pentru fiecare număr p din acest şir notăm $A_p = \{a \mid 1 \le a \le n, p \mid a\}$. Atunci numărul numerelor prime cel mult egale cu n este

$$(1.3.1) \qquad n + k - 1 - \left|\bigcup_{i=1}^{k} A_{p_i}\right|.$$

De exemplu, să calculăm numărul numerelor prime mai mici decât 250. Deoarece $\left[\sqrt{250}\right] = 15$ rezultă că şirul de numere prime cu care vom lucra este

$$2, 3, 5, 7, 11, 13$$

şi avem de calculat cardinalul unei reuniuni de 6 mulţimi :

$$|A_2 \cup A_3 \cup A_5 \cup A_7 \cup A_{11} \cup A_{13}| = \sum |A_i| - \sum |A_i \cap A_j| + \sum |A_i \cap A_j \cap A_k| -$$

$$- \sum |A_i \cap A_j \cap A_k \cap A_l|$$, indicierea fiind evidentă.

Formula se opreşte aici deoarece din inegalitatea

$$2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 > 250$$

rezultă că intersecţia a cinci mulţimi este vidă.

Ţinând seama de faptul că $|A_{p_i}| = \left[\frac{n}{p_i}\right], |A_{p_i} \cap A_{p_j}| = \left[\frac{n}{p_i p_j}\right]$ ş.a.m.d.

obţinem :

$$\left|\bigcup A_i\right| = \left[\frac{250}{2}\right] + \left[\frac{250}{3}\right] + \left[\frac{250}{5}\right] + \left[\frac{250}{7}\right] + \left[\frac{250}{11}\right] + \left[\frac{250}{13}\right] -$$

$$- \left[\frac{250}{6}\right] - \left[\frac{250}{10}\right] - \left[\frac{250}{14}\right] - \left[\frac{250}{22}\right] - \left[\frac{250}{26}\right] - \left[\frac{250}{15}\right] - \left[\frac{250}{21}\right] -$$

$$- \left[\frac{250}{33}\right] - \left[\frac{250}{39}\right] - \left[\frac{250}{35}\right] - \left[\frac{250}{55}\right] - \left[\frac{250}{65}\right] - \left[\frac{250}{77}\right] - \left[\frac{250}{91}\right] -$$

$$- \left[\frac{250}{143}\right] + \left[\frac{250}{30}\right] + \left[\frac{250}{42}\right] + \left[\frac{250}{66}\right] + \left[\frac{250}{78}\right] + \left[\frac{250}{70}\right] + \left[\frac{250}{110}\right] +$$

$$+ \left[\frac{250}{130}\right] + \left[\frac{250}{154}\right] + \left[\frac{250}{182}\right] + \left[\frac{250}{286}\right] + \left[\frac{250}{105}\right] + \left[\frac{250}{165}\right] + \left[\frac{250}{195}\right] +$$

$$+ \left[\frac{250}{231}\right] + \left[\frac{250}{273}\right] - \left[\frac{250}{210}\right] = 125 + 83 + 50 + 35 + 22 + 19 - 41 -$$

$$-25 - 17 - 11 - 9 - 16 - 11 - 7 - 6 - 7 - 4 - 3 - 3 - 2 - 1 + 8 + 5 + 3 + 3 + 3 +$$

$$2 + 1 + 1 + 1 + 0 + 2 + 1 + 1 + 1 + 0 - 1 = 202.$$

Din formula (1.3.1) rezultă că în mulţimea $\{1, 2, 3, \ldots, 250\}$ sunt $250 + 6 - 1 - 202 = 53$ numere prime.

Back

#

(1.4) Calculul permutărilor fără puncte fixe

O permutare $\sigma \in S_n$ se numeşte deranjament dacă $\sigma(i) \neq 0$ oricare ar fi i, $1 \leq i \leq n$. Dacă $\sigma(i) = i$ spunem că i este punct fix al lui σ.

Ne propunem *să calculăm numărul D_n al deranjamentelor din S_n.* Pentru orice i, $1 \leq i \leq n$, notăm cu F_i mulţimea permutărilor care au pe i drept punct fix. Deci :

$$D_n = n! - \left| \bigcup_{i=1}^{n} F_i \right| .$$

Ţinând seama de formulele : $|F_i| = (n-1)!, |F_i \cap F_j| = (n-2)!$ etc. şi aplicând principiul includerii şi excluderii se obţine :

$$D_n = n! - \sum_{1}^{n} |F_i| + \sum_{1 \leq i < j \leq n} |F_i \cap F_j| - \ldots + (-1)^k \sum_{1 \leq i_1 < \ldots < i_k \leq n} |F_{i_1} \cap \ldots \cap F_{i_k}| + \ldots$$

$$+ (-1)^{n-1} \sum_{1 \leq i_1 < \ldots < i_{n-1} \leq n} |F_{i_1} \cap \ldots \cap F_{i_{n-1}}| + (-1)^n |F_1 \cap \ldots \cap F_n| =$$

$$= n! - n(n-1)! + \binom{n}{2}(n-2)! - \ldots + (-1)^k \binom{n}{k}(n-k)! + \ldots$$

$$\ldots + (-1)^{n-1} \binom{n}{n-1} 1! + (-1)^n \cdot 1 \Rightarrow$$

(1.4.1) $$D_n = n!\left(1 - \frac{1}{1!} + \frac{1}{2!} - \ldots + (-1)^k \frac{1}{k!} + \ldots + (-1)^n \frac{1}{n!}\right).$$

Şirul de numere $(D_n)_{n \geq 1}$ satisface relaţiile de recurenţă :

(1.4.2) $$D_{n+1} = (n+1)D_n + (-1)^{n+1}$$

(1.4.3) $$D_{n+1} = n(D_n + D_{n-1}).$$

Relaţia (1.4.2) rezultă din (1.4.1) iar (1.4.3) din (1.4.2) prin calcule directe.

Numărul permutărilor pare din S_n fără puncte fixe este dat de formula :

(1.4.4) $$E_n = \frac{1}{2}\left(D_n + (-1)^{n+1}(n-1)\right).$$

Această formulă se demonstrează analog, dar se ţine seama că numărul permutărilor pare cu k puncte fixe este $\frac{1}{2}(n-k)!$.

Back

#

(1.5) Numărul funcţiilor surjective

Fie A, B două mulţimi finite cu $|A| = n$ şi $|B| = m$, unde $n \geq m$. Ne propunem *să calculăm numărul* $s_{n,m}$ *al funcţiilor surjective* $f : A \to B$. Putem presupune că $B = \{1,2,\ldots,m\}$. Pentru orice i, $1 \leq i \leq m$, notăm cu B_i mulţimea funcţiilor $f : A \to B$ cu proprietatea $i \notin f(A)$. Mulţimea funcţiilor surjective $f : A \to B$ este

$$B^A \setminus \bigcup_{i=1}^{m} B_i .$$

În general, $|B^A| = m^n, |B_i| = (m-1)^n, |B_i \cap B_j| = (m-2)^n$ etc.

Aplicând principiul includerii şi excluderii rezultă formula :

$$s_{n,m} = m^n - \binom{m}{1}(m-1)^n + \binom{m}{2}(m-2)^n - \ldots + (-1)^k \binom{m}{k}(m-k)^n + \ldots \quad (1.5.1)$$
$$\ldots + (-1)^{m-1}\binom{m}{m-1} \cdot 1^n .$$

În cazul $m = n$, funcţiile $f : A \to B$ surjective sunt exact funcţiile bijective, şi din (1.5.1) se obţine identitatea (netrivială !)

$$n! = n^n - \binom{n}{1}(n-1)^n + \binom{n}{2}(n-2)^n - \ldots \quad (1.5.2)$$
$$\ldots + (-1)^k \binom{n}{k}(n-k)^n + \ldots + (-1)^{n-1}\binom{n}{n-1}.$$

Back

#

(1.6) Numărul partiţiilor unei mulţimi. Numerele Stirling şi Bell

Fie A o mulţime cu n elemente. O partiţie a lui A cu m clase, $m \geq 1$, este o descompunere a lui A ca o reuniune disjunctă de m submulţimi :

$$A = A_1 \cup A_2 \cup \ldots \cup A_m .$$

Două partiţii ale lui A se consideră identice dacă diferă doar prin ordinea termenilor reuniunii.

Orice asemenea descompunere defineşte o funcţie surjectivă

$$f : A \to \{1,2,\ldots,m\}$$

unde $f(a) = i$, dacă $a \in A_i$. Se observă că dacă schimbăm numerotarea mulţimilor A_i după o permutare $\sigma \in S_n$, se obţine o altă funcţie f_σ unde $f_\sigma = \sigma f$ iar $f = \sigma^{-1} f_\sigma$. Reciproc, oricărei funcţii surjective $f : A \to \{1,2,\ldots,m\}$ îi corespunde o partiţie a lui A cu m clase, ale cărei submulţimi sunt

$$f^{-1}(1), f^{-1}(2), \ldots, f^{-1}(m).$$

În plus, dacă $\sigma \in S_n$ atunci f şi $f_\sigma = \sigma f$ definesc aceeaşi partiţie. Rezultă că există o funcţie surjectivă Φ de la mulţimea funcţiilor surjective $f: A \to \{1, 2, \ldots, m\}$ la mulţimea partiţiilor lui A cu m clase prin care pentru orice funcţie surjectivă f, funcţiile σf, $\sigma \in S_m$, au aceeaşi imagine.

Cum $\left|\left\{\sigma f \mid \sigma \in S_m\right\}\right| = m!$ rezultă că numărul partiţiilor lui A cu m clase este dat de formula

(1.6.1)
$$S(n,m) = \frac{1}{m!} s_{n,m} = \frac{1}{m!} \sum_{k=0}^{m-1} (-1)^k \binom{m}{k} (m-k)^n.$$

Numerele $S(m, n)$ se numesc *numerele lui Stirling de speţa a doua.*

Deoarece există o bijecţie între mulţimea partiţiilor lui A cu m clase şi mulţimea relaţiilor de echivalenţă pe A care dau m clase de echivalenţă rezultă că $S(n, m)$ coincide cu numărul relaţiilor de echivalenţă cu m clase de echivalenţă. Atunci, numărul total al relaţiilor de echivalenţă pe o mulţime cu n elemente este

(1.6.2)
$$B_n = S(n,1) + S(n,2) + \ldots + S(n,n).$$

Numerele B_n astfel definite se numesc *numerele lui Bell.* Prin definiţie

$$B_0 = 1.$$

(1.6.3) Propoziţie. *Numerele lui Stirling de speţa a doua verifică relaţia de recurenţă*

(1.6.4)
$$S(n+1,m) = \sum_{k=m-1}^{n} \binom{n}{k} S(k, m-1).$$

Demonstraţie. Fie $A = \{a_1, a_2, \ldots, a_{n+1}\}$ o mulţime cu $n+1$ elemente şi fie $A = A_1 \cup A_2 \cup \ldots \cup A_m$ o partiţie a sa cu m clase, astfel încât $a_{n+1} \in A_i$. Dacă înlăturăm clasa A_i obţinem o partiţie a mulţimii $B = A \setminus A_i$:

$$B = A_1 \cup \ldots \cup A_{i-1} \cup A_{i+1} \cup \ldots \cup A_m.$$

Cardinalul mulţimii B este limitat de inegalităţile :

$$m-1 \le |B| \le n,$$

deoarece $1 \le |A_i| \le n-m+2$. Partiţiile astfel obţinute sunt distincte deoarece se obţin din partiţii distincte ale lui A. Am definit astfel o funcţie injectivă de la mulţimea partiţiilor lui A cu m clase la mulţimea partiţiilor cu $m-1$ clase ale unei submulţimi B, $B \subset A$, cu $m-1 \le |B| \le n$. Este evident că această funcţie este bijectivă.

Deoarece mulţimea $B \subset A \setminus \{a_{n+1}\}$ cu $|B| = k$ şi $m-1 \le k \le n$ poate fi aleasă în $\binom{n}{k}$ moduri rezultă formula (1.6.4).

(1.6.5) Propoziţie. *Numerele lui Bell verifică relaţia de recurenţă :*

(1.6.6) $$B_{n+1} = \sum_{k=0}^{n} \binom{n}{k} B_k .$$

Demonstraţie. Vom folosi formulele (1.6.2) şi (1.6.4)

$$B_{n+1} = \sum_{m=1}^{n+1} S(n+1,m) = 1 + \sum_{m=2}^{n+1} S(n+1,m) = 1 + \sum_{m=2}^{n+1} \sum_{k=m-1}^{n} \binom{n}{k} S(k,m-1) =$$

$$= 1 + \sum_{k=1}^{n} \binom{n}{k} \sum_{m=2}^{i+1} S(k,m-1) = 1 + \sum_{k=1}^{n} \binom{n}{k} B_k = \sum_{k=0}^{n} \binom{n}{k} B_k .$$

Back
#

(1.7) O egalitate a lui Szegö şi Pólya.

O aplicaţie interesantă a formei generale a principiului includerii şi excluderii o constituie următorul rezultat datorat lui *Szegö* şi *Pólya* (1925) :

Dacă $n > 1$ este un număr natural cu divizorii primi $p_1, p_2, \ldots, p_k$ şi $a_1, a_2, \ldots, a_{\varphi(n)}$ este un sistem redus de resturi modulo n din mulţimea $A = \{1,2,\ldots,n\}$ atunci

(1.7.1) $$a_1^2 + a_2^2 + \ldots + a_{\varphi(n)}^2 = \frac{1}{6}\varphi(n)\left(2n^2 + (-1)^k p_1 \ldots p_k\right).$$

Demonstraţie. Considerăm funcţia $f : A \to \mathbf{N}$, $f(x) = x^2$ şi fie $A_i = \{a \in A \mid p_i \mid a\}, 1 \le i \le k$. Atunci

$$f(A) = \sum_{i=1}^{n} i^2 = \frac{n(n+1)(2n+1)}{6} = \alpha n^3 + \beta n^2 + \gamma n + \delta ,$$

unde $\alpha = \frac{1}{3}, \beta = \frac{1}{2}, \gamma = \frac{1}{6}$ şi $\delta = 0$.

$$f(A_i) = p_i^2 + (2p_i)^2 + \ldots + \left(\frac{n}{p_i} p_i\right)^2 = p_0^2 \left[\alpha\left(\frac{n}{p_i}\right)^3 + \beta\left(\frac{n}{p_i}\right)^2 + \gamma\left(\frac{n}{p_i}\right)\right].$$

În mod asemănător avem :

$$f(A_i \cap A_j) = (p_i p_j)^2 \left[\alpha\left(\frac{n}{p_i p_j}\right)^3 + \beta\left(\frac{n}{p_i p_j}\right)^2 + \gamma\left(\frac{n}{p_i p_j}\right)\right], \forall i \ne j ,$$

şi celelalte intersecţii.

Deci $\quad a_1^2 + a_2^2 + \ldots + a_{\varphi(n)}^2 = f(A) - f\left(\bigcup_{i=1}^{k} A_k\right) =$

$$= \alpha n^3 + \beta n^2 + \gamma n - \sum_{i=1}^{k} p_i^2 \left[\alpha\left(\frac{n}{p_i}\right)^3 + \beta\left(\frac{n}{p_i}\right)^2 + \gamma\left(\frac{n}{p_i}\right)\right] +$$

$$+ \sum_{1 \le i < j \le k} \left(p_i p_j\right)^2 \left[\alpha\left(\frac{n}{p_i p_j}\right)^3 + \beta\left(\frac{n}{p_i p_j}\right)^2 + \gamma\left(\frac{n}{p_i p_j}\right)\right] - \ldots$$

$$\ldots + (-1)^k \left(p_1 \ldots p_k\right)^2 \left[\alpha\left(\frac{n}{p_1 \ldots p_k}\right)^3 + \beta\left(\frac{n}{p_1 \ldots p_k}\right)^2 + \gamma\left(\frac{n}{p_1 \ldots p_k}\right)\right].$$

Se observă că $a_1^2 + a_2^2 + \ldots + a_{\varphi(n)}^2$ este un număr de forma $\alpha_0 n^3 + \beta_0 n^2 + \gamma_{0n}$ unde :

$$\alpha_0 = \alpha\left(1 - \sum_{i=1}^{k} \frac{1}{p_i} + \sum_{i<j} \frac{1}{p_i p_j} - \ldots + (-1)^k \frac{1}{p_1 \ldots p_k}\right),$$

$$\beta_0 = \beta\left(1 - \sum_{i=1}^{k} 1 + \sum_{i<j} 1 - \ldots + (-1)^k 1\right),$$

$$\gamma_0 = \gamma\left(1 - \sum_{i=1}^{k} p_i + \sum_{i<j} p_i p_j - \ldots + (-1)^k p_1 \ldots p_k\right).$$

Deci $\alpha_0 = \dfrac{1}{3}\left(1 - \dfrac{1}{p_1}\right)\left(1 - \dfrac{1}{p_2}\right) \ldots \left(1 - \dfrac{1}{p_k}\right) = \dfrac{1}{3}\dfrac{\varphi(n)}{n}$,

$$\beta_0 = \frac{1}{2}(1-1)^k = 0,$$

$$\gamma_0 = \frac{1}{6}(1 - p_1)(1 - p_2)\ldots(1 - p_k) = \frac{(-1)^k}{3} p_1 \ldots p_k \frac{\varphi(n)}{n}.$$

În acest fel (1.7.1) este demonstrată.

Back

#

(1.8) O problemă de numărare de matrice. *Fie p, m, n numere naturale nenule. Să se determine numărul matricelor* $A = (a_{ij})$ *cu m linii, n coloane şi elemente din mulţimea* $\{1, 2, \ldots, p\}$ *şi cu proprietatea că suma elementelor pe fiecare linie şi fiecare coloană este nedivizibilă cu p.*

(*Mircea Becheanu*, Gazeta Matematică, nr.10-11, 1997)

Fie M mulţimea tuturor matricelor cu m linii, n coloane şi cu elemente din $\{1,2,\ldots,p\}$. Notăm cu A_i mulţimea matricelor din M în care suma elementelor de pe linia i este divizibilă cu p şi cu B_j mulţimea matricelor din M în care suma elementelor de pe coloana j este divizibilă cu p. Deoarece $|M| = p^{mn}$, rezultă că numărul căutat este

$$N = p^{mn} - \left|\left(\bigcup_{i=1}^{m} A_i\right) \cup \left(\bigcup_{j=1}^{n} B_j\right)\right|.$$

Conform principiului includerii şi excluderii avem :

$$\left|\left(\bigcup_{i=1}^{m} A_i\right) \cup \left(\bigcup_{j=1}^{n} B_j\right)\right| = |A_1 \cup \ldots \cup A_m \cup B_1 \cup \ldots \cup B_n| =$$

$$= \sum_{i=1}^{m} |A_i| + \sum_{i=1}^{n} |B_i| + \sum_{k=1}^{m} \sum_{l=1}^{n} \sum_{\substack{1 \le i_1 < \ldots < i_k \le m \\ 1 \le j_1 < \ldots < j_l \le n}} (-1)^{k+l-1} \left|A_{i_1} \cap \ldots \cap A_{i_k} \cap B_{j_1} \cap \ldots \cap B_{j_l}\right|.$$

Pentru orice i, j avem $|A_i| = |B_j| = p^{mn-1}$. Oricare ar fi indicii $i_1 < \ldots < i_k, j_1 < \ldots < j_l$, avem

$$\left|A_{i_1} \cap \ldots \cap A_{i_k} \cap B_{j_1} \cap \ldots \cap B_{j_l}\right| = |A_1 \cap \ldots \cap A_k \cap B_1 \cap \ldots \cap B_l|.$$

Va rezulta pentru numărul căutat formula :

$$N = p^{mn} - mnp^{mn-1} + \sum_{k=1}^{m} \sum_{l=1}^{n} (-1)^{k+l} \binom{m}{k} \binom{n}{l} |A_1 \cap \ldots \cap A_k \cap B_1 \cap \ldots \cap B_l|.$$

În cazul în care $k < m$ sau $l < n$ avem :

$$|A_1 \cap \ldots \cap A_k \cap B_1 \cap \ldots \cap B_l| = p^{mn-k-l}.$$

Într-adevăr, dacă o matrice $A = (a_{ij})$ aparţine lui $|A_1 \cap \ldots \cap A_k \cap B_1 \cap \ldots \cap B_l|$ toate elementele a_{ij} sunt alese în mod arbitrar, cu excepţia elementelor $a_{1n}, a_{2n}, \ldots, a_{kn}, a_{m1}, \ldots, a_{ml}$ care sunt alese în mod unic, astfel încât să avem congruenţele

$$\sum_{j=1}^{n} a_{ij} \equiv 0 (\text{mod}\, p),\ \forall i = 1, \ldots, k$$

$$\sum_{i=1}^{m} a_{ij} \equiv 0 (\text{mod}\, p),\ \forall j = 1, \ldots, l.$$

În cazul $k = m$ şi $l = n$ mulţimea $A_1 \cap \ldots \cap A_m \cap B_1 \cap \ldots \cap B_n$ are cardinalul $p^{(m-1)(n-1)}$ deoarece este în corespondenţă bijectivă cu mulţimea matricelor cu $m-1$ linii şi $n-1$ coloane şi cu elemente din $\{1, 2, \ldots, p\}$. Revenind la formula de mai sus obţinem :

$$N = p^{mn} - \binom{m}{1}\binom{n}{1} p^{mn-1} + \sum_{k=1}^{m}\sum_{l=1}^{n}(-1)^{k+l}\binom{m}{k}\binom{n}{l} p^{mn-k-l} +$$

$$+(-1)^{m+n}\binom{m}{m}\binom{n}{n} p^{mn-m-n} + (-1)^{m+n}\binom{m}{m}\binom{n}{n} p^{mn-m-n+1} =$$

$$= (-1)^{0+0}\binom{m}{0}\binom{n}{0} p^{mn-0-0} + \sum_{k=1}^{m}(-1)^{1+0}\binom{m}{1}\binom{n}{0} p^{mn-1} + \sum_{l=1}^{n}(-1)^{0+1}\binom{m}{0}\binom{n}{1} p^{mn-1} +$$

$$+\sum_{k=1}^{m}\sum_{l=1}^{n}(-1)^{k+l}\binom{m}{k}\binom{n}{l} p^{mn-k-l} + (-1)^{m+n} p^{mn-m-n}(p-1) =$$

$$= \sum_{k=0}^{m}\sum_{l=0}^{n}(-1)^{k+l}\binom{m}{k}\binom{n}{l} p^{mn-k-l} + (-1)^{m+n} p^{mn-m-n}(p-1) =$$

$$= \sum_{s=0}^{m+n}(-1)^{s} p^{mn-s} \sum_{k+l=s}\binom{m}{k}\binom{n}{l} + (-1)^{m+n} p^{mn-m-n}(p-1) =$$

$$= p^{mn}\sum_{s=0}^{m+n}\left(-\frac{1}{p}\right)^{s}\binom{m+n}{s} + (-1)^{m+n} p^{mn-m-n}(p-1) =$$

$$= p^{mn}\left(1-\frac{1}{p}\right)^{m+n} + (-1)^{m+n} p^{mn-m-n}(p-1) =$$

$$= p^{mn-m-n}(p-1)^{m+n} + (-1)^{m+n} p^{mn-m-n}(p-1) =$$

$$= p^{mn-m-n}\left[(p-1)^{m+n} + (-1)^{m+n}(p-1)\right].$$

Back

#

2. CÂTEVA PROBLEME DE COMBINATORICĂ CU MULŢIMI FINITE

În acest paragraf prezentăm câteva probleme neclasice de combinatorică, cu scopul de a pune în evidenţă noi metode de abordare.

(2.1) *Fie A o mulţime şi* $A_1, A_2, \ldots, A_{n+1}$ *submulţimi nevide ale lui A. Să se arate că există două mulţimi disjuncte de indici* $I, J \subset \{1, 2, \ldots, n\}$ *astfel încât*

$$\bigcup_{i\in I} A_i = \bigcup_{j\in J} A_j .$$

Soluţie. Presupunem că $A = \{a_1, a_2, \dots, a_n\}$. Definim "matricea de incidenţă" a familiei de mulţimi $A_1, A_2, \dots, A_{n+1}$ ca fiind matricea $M = (\alpha_{ij}) \in M(n, n+1; \mathbf{R})$, unde

$$\alpha_{ij} = \begin{cases} 1 \text{ dacă } a_i \in A_j \\ 0 \text{ dacă } a_i \notin A_j . \end{cases}$$

Considerăm sistemul de ecuaţii liniare

$$\text{(2.1.1)} \qquad \sum_{j=1}^{n+1} \alpha_{ij}\xi_j = 0 \; ; \; i = 1, \dots, n .$$

Fiind un sistem de n ecuaţii cu $n+1$ necunoscute, el admite o soluţie netrivială $(x_1, x_2, \dots, x_{n+1})$. Considerăm mulţimile de indici

$$I = \{ j | 1 \le j \le n+1, x_j > 0 \},$$
$$J = \{ j | 1 \le j \le n+1, x_j < 0 \}.$$

Este evident, din definiţia lui M şi din faptul că $(x_1, x_2, \dots, x_{n+1})$ este o soluţie netrivială a sistemului (3.1.1), că $I \cap J = \varnothing$ şi $I \ne \varnothing, J \ne \varnothing$. Să notăm $y_j = -x_j$ pentru $j \in J$; evident $y_j > 0$. Faptul că $(x_1, x_2, \dots, x_{n+1})$ este o soluţie se exprimă acum astfel :

$$\text{“}\sum_{j\in I} \alpha_{ij} x_j = \sum_{j\in J} \alpha_{ij} y_j \text{, oricare ar fi } i \in \{1, 2, \dots, n\}\text{”.}$$

Fie i, $1 \le i \le n$, un indice fixat. Au loc echivalenţele :

$$\sum_{j\in I} \alpha_{ij} x_j > 0 \Leftrightarrow \exists j \in I, \alpha_{ij} = 1 \Leftrightarrow \exists j \in I, \text{ a.î. } a_i \in A_j \Leftrightarrow a_i \in \bigcup_{j\in I} A_j .$$

Rezultă că $a_i \in \bigcup_{j\in I} A_j \Leftrightarrow a_i \in \bigcup_{j\in J} A_j$, oricare ar fi $i \in \{1, 2, \dots, n\}$.

Cu aceasta, rezultă că cele două reuniuni sunt egale.

(2.2) *Fie A o mulţime cu n elemente şi* $B_1, B_2, \dots, B_{n+1}$ *submulţimi ale lui A, fiecare având* 3 *elemente. Să se arate că există două mulţimi* B_i *şi* B_j *astfel încât* $|B_i \cap B_j| = 1$.

Soluţie. Presupunem prin absurd că nu există două mulţimi cu proprietatea cerută. Rezultă că oricare ar fi i, j cu $i \ne j$ avem $B_i \cap B_j = \varnothing$ sau $|B_i \cap B_j| = 2$. Fie $\mathcal{B} = \{B_1, B_2, \dots, B_{n+1}\}$. Definim pe $\mathcal{B}$ relaţia de echivalenţă :

$$X \sim Y \Leftrightarrow X = Y \text{ sau } |X \cap Y| = 2 .$$

Trebuie demonstrată doar proprietatea de tranzitivitate : $X \sim Y$ şi $Y \sim Z$ $\Rightarrow X \sim Z$. Din $X \sim Y$ rezultă $X = \{a,b,x\}$ şi $Y = \{a,b,y\}$. Deoarece $|Y \cap Z| = 2$ rezultă că Z conţine a sau b, deci $X \cap Z \neq \emptyset$. Atunci $|X \cap Z| = 2$.

Împărţim mulţimea $\mathcal{B}$ în clase de echivalenţă după această relaţie de echivalenţă : $\mathcal{B} = B_1 \cup B_2 \cup \ldots \cup B_m$. Deoarece mulţimile din două clase distincte sunt disjuncte rezultă că

$$(2.2.1) \qquad \left|\bigcup_{i=1}^{n+1} B_i\right| = \sum_{i=1}^{m} \left|\bigcup_{B_j \in \mathcal{B}_i} B_j\right|.$$

Presupunem că $\mathcal{B}_i = \{B_{i_1}, B_{i_2}, \ldots, B_{i_k}\}$ şi fie $\overline{B_i} = B_{i_1} \cup B_{i_2} \cup \ldots \cup B_{i_k}$. Dacă $\mathcal{B}_i$ conţine o singură mulţime atunci $\overline{B_i} = 3 = |\mathcal{B}_i| + 2$. Dacă $|\overline{B_i}| = 4$, rezultă că $\mathcal{B}_i$ conţine cel puţin două mulţimi. Deoarece o mulţime cu 4 elemente conţine 4 mulţimi cu 3 elemente rezultă că $\mathcal{B}_i$ conţine cel mult 4 mulţimi adică $|\mathcal{B}_i| \in \{2, 3, 4\}$. Deci în acest caz $|\overline{B_i}| \geq |\mathcal{B}_i|$. Presupunem că $|\overline{B_i}| > 4$. Vom arăta că în acest caz toate mulţimile din $\mathcal{B}_i$ au în comun două elemente şi atunci va rezulta

$$(2.2.2) \qquad |\overline{B_i}| = |\mathcal{B}_i| + 2.$$

Fie $B_{i_1} = \{a,b,x\}$ şi $B_{i_2} = \{a,b,y\}$ mulţimi din $\mathcal{B}_i$. Luăm un element $z \in \overline{B_i}, z \neq a,b,x,y$. Există un indice i_3 a.î. $z \in B_{i_3}$. Atunci $B_{i_3} = \{a,b,z\}$ deoarece $B_{i_3} = \{a,x,z\}$ implică $B_{i_2} \cap B_{i_3} = \{a\}$ şi aceasta contrazice ipoteza. În consecinţă (2.2.2) este adevărată.

În concluzie, în toate cazurile avem :

$$(2.2.3) \qquad |\mathcal{B}_i| \leq |\overline{B_i}|,\ i = 1,\ldots,m.$$

Adunând toate aceste relaţii şi folosind (3.2.1) obţinem :

$$n+1 = \sum_{i=1}^{m} |\mathcal{B}_i| \leq \sum_{i=1}^{m} |\overline{B_i}| = \left|\bigcup_{i=1}^{n+1} B_i\right| \leq n.$$

Aceasta este o contradicţie.

(2.3) *Fie A o mulţime cu n elemente. Să se demonstreze egalitatea :*

$$\sum_{\substack{(A_1,A_2) \\ A_1 \subset A \\ A_2 \subset A}} |A_1 \cap A_2| = n \cdot 4^{n-1}.$$

Soluţie. Mulţimea A are 2^n submulţimi, deci avem $2^n \cdot 2^n = 4^n$ perechi ordonate (A_1, A_2) de submulţimi ale lui A. Pentru orice pereche ordonată (A_1, A_2) se consideră perechile

$$(A_1, A_2),\ \left(A_1, \overline{A_2}\right), \left(\overline{A_1}, A_2\right) \text{ şi } \left(\overline{A_1}, \overline{A_2}\right)$$

unde $\overline{A_1}$ este complementara lui A_1 etc. Reuniunea

$$A = \left(A_1 \cap A_2\right) \cup \left(A_1 \cap \overline{A_2}\right) \cup \left(\overline{A_1} \cap A_2\right) \cup \left(\overline{A_1} \cap \overline{A_2}\right)$$

este o partiţie a lui A. Adunând toate cardinalele obţinute obţinem $n \cdot 4^n$. Deoarece fiecare intersecţie $A_1 \cap A_2$ apare în acest fel de patru ori, se obţine că suma cerută este $n \cdot 4^{n-1}$.

(2.4) *Fie A o mulţime cu n elemente. O familie $\mathcal{A}$ de submulţimi ale lui A, $\mathcal{A} = \{A_1, A_2, \ldots, A_m\}$, se numeşte separantă dacă pentru orice pereche de elemente din A, $\{x, y\} \subset A$, există o mulţime $A_j \in \mathcal{A}$ astfel încât $A_j \cap \{x, y\}$ conţine un singur element. Familia $\mathcal{A}$ se numeşte acoperitoare dacă $A = \bigcup_{j=1}^{m} A_j$.*

Să se determine cel mai mic număr de mulţimi dintr-o familie separantă şi acoperitoare de submulţimi ale lui A.

Soluţie. Trebuie deci să calculăm funcţia :

$$f(n) = \min\left\{|\mathcal{A}| \,\middle|\, \mathcal{A} \text{ familie acoperitoare pentru } A\right\}.$$

Fie $A = \{x_1, x_2, \ldots, x_n\}$ o numerotare a elementelor lui A.

Pentru orice familie acoperitoare $\mathcal{A}$ considerăm matricea de incidenţă a lui $\mathcal{A}$, $I_{\mathcal{A}} = (\alpha_{ij}), 1 \le i \le n, 1 \le j \le m$, unde

$$\alpha_{ij} = \begin{cases} 1 \text{ dacă } x_i \in A_j \\ 0 \text{ dacă } x_i \notin A_j. \end{cases}$$

Din condiţia de separare rezultă că funcţia

$$A \to \{0,1\}^m$$

$$x_i \mapsto \left(\alpha_{i_1}, \alpha_{i_2}, \ldots, \alpha_{i_m}\right).$$

este injectivă. Într-adevăr, dacă x_i şi x_k sunt elemente diferite şi $x_i \in A_j, x_k \notin A_j$ atunci $\alpha_{ij} = 1$ şi $\alpha_{kj} = 0$, deci liniile i şi k diferă pe coloana j. Din aceasta rezultă că $n \le 2^m$.

Presupunem că $2^p \le n < 2^{p+1}$, unde $p = \left[\log_2 n\right]$. Din inegalitatea de mai sus rezultă că $m \ge p$ şi deci $f(n) \ge p$. Vom arăta că $f(n) = p+1$. Pentru aceasta distingem două cazuri.

Cazul I : $n = 2^p$. Mai întâi observăm că $m > p$. Într-adevăr, dacă $m = p$, aplicaţia de mai sus este bijectivă, deci orice cuvât de lungime m din $\{0,1\}^m$ apare ca o linie în matricea de incidenţă. Dar cuvântul (0, 0,…, 0) nu poate să apară în $I_{\mathcal{A}}$ deoarece familia $\mathcal{A}$ este acoperitoare. În consecinţă $m > p$ şi deci, $m \ge p+1$. Vom arăta că există o familie acoperitoare şi separantă cu $p+1$ mulţimi. Este suficient să considerăm familia $A_1,\ldots,A_{p+1}$ definită de matricea de incidenţă $I = (\alpha_{ij}), 1 \le i \le n, 1 \le j \le p+1$, unde $(\alpha_{i1},\alpha_{i2},\ldots,\alpha_{ip+1})$ sunt cifrele reprezentării binare ale numărului i.

Cazul II : $2^p < n < 2^{p+1}$. Deoarece funcţia de mai sus este injectivă şi linia (0, 0, …, 0) nu apare în matricea de incidenţă rezultă că $n < 2^m - 1 \Rightarrow 2^p < 2^m - 1 \Rightarrow 2^p + 1 < 2^m \Rightarrow p < m$. Pentru a arăta că există o familie acoperitoare şi separantă cu $p+1$ mulţimi este suficient să considerăm aceeaşi construcţie ca la cazul I.

Back

#

3. COMBINATORICA GRUPURILOR FINITE

GRUPURI DE PERMUTĂRI

Presupunem cunoscută noţiunea de grup (la nivelul manualului de clasa a XII-a). Vom adopta, pentru un grup general G, notaţia multiplicativă iar elementul neutru va fi notat cu 1. O submulţime nevidă H a lui G se numeşte subgrup dacă îndeplineşte condiţiile :

(s1) $\forall\, x, y \in H \Rightarrow xy \in H$

(s2) $\forall\, x \in H \Rightarrow x^{-1} \in H$.

Rezultă că $1 \in H$ şi că H este, la rândul său, un grup în raport cu operaţia de înmulţire din G, restricţionată la H.

Este interesant de observat că în cazul subgrupurilor finite, condiţia (s2) este superfluă ; cu alte cuvinte, dacă H este o submulţime finită a lui G atunci H este subgrup dacă şi numai dacă îndeplineşte condiţia (s1). Într-adevăr, dacă $g \in H$, funcţia $\tau_g : H \to H$ definită prin $\tau_g(x) = gx, \forall x \in H$, are sens conform (s1) şi este injectivă (din proprietăţile grupurilor !). Deci τ_g este bijectivă, căci H este finită. Din surjectivitate, rezultă că există $x_0 \in H$ astfel încât $gx_0 = g$. Deci $1 \in H$. Tot din surjectivitatea lui τ_g rezultă că există $g' \in H$ a. î. $gg' = 1$; deci $g^{-1} \in H$.

Back

#

(3.1) Relaţii de congruenţă pe un grup. Reamintim că dacă G este un grup finit, numărul elementelor sale se numeşte ordinul grupului G şi se notează $|G|$.

(3.1.1) Teorema lui Lagrange. *Fie G un grup finit şi H un subgrup al său. Atunci $|G|$ este divizibil cu $|H|$.*

Demonstraţie. Se introduce pe G relaţia de echivalenţă :

$$x \equiv y(\operatorname{mod} H) \Leftrightarrow x^{-1}y \in H,$$

numită congruenţa la stânga modulo H. Pentru orice $g \in G$ clasa de echivalenţă a lui g este mulţimea :

$$gH = \{gh | h \in H\}$$

Deoarece gH este imaginea lui H prin funcţia bijectivă $\tau_g : G \to G, \quad \tau_g(x) = gx$ rezultă că gH şi H sunt cardinal echivalente (au acelaşi număr de elemente). Din proprietăţile relaţiei de echivalenţă, rezultă că $G = g_1H \cup g_2H \cup \ldots \cup g_nH$, unde $g_1, g_2, \ldots g_n$ este un sistem complet de reprezentanţi pentru relaţia de echivalenţă, reuniunea fiind disjunctă. Prin urmare, trecând la cardinale avem :

$$|G| = |g_1H| + |g_2H| + \ldots + |g_nH| = n|H|.$$

(3.2) Definiţie. *Numărul* $n = \dfrac{|G|}{|H|}$ *se numeşte indicele lui H în G.*

Se poate introduce pe G o relaţie de congruenţă la dreapta modulo H astfel :

$$x \overset{d}{\equiv} y(\operatorname{mod} H) \Leftrightarrow xy^{-1} \in H.$$

Clasa de echivalenţă a unui element $g \in G$ prin această relaţie de congruenţă este

$$Hg = \{hg | h \in H\}.$$

În general cele două relaţii de congruenţă nu coincid. Este clar că ele coincid atunci când pentru orice $g \in G$ are loc egalitatea :

$$gH = Hg.$$

În mod echivalent, aceasta înseamnă că oricare ar fi $g \in G$ şi $h \in H$ are loc proprietatea $ghg^{-1} \in H$. Spunem în acest caz că H este subgrup normal în G şi vom nota $H \triangleleft G$. Într-un grup abelian orice subgrup este normal. Există subgrupuri care nu sunt normale. Cu toate acestea este adevărată proprietatea : *pentru orice subgrup $H < G$, numărul claselor de congruenţă la stânga modulo H şi numărul claselor de congruenţă la dreapta modulo H coincid.* Cu alte cuvinte, indicele unui subgrup nu depinde de relaţia de congruenţă ci numai de H. Demonstraţia afirmaţiei de mai sus este următoarea : funcţia $gH \to Hg^{-1}$

este o bijecţie între cele două mulţimi de clase de congruenţă la stânga şi la dreapta.

(3.1.3) Exemplu de subgrup normal. Dacă G este mulţimea matricelor inversabile de ordinul n cu coeficienţi reali şi $H < G$ este subgrupul matricelor de acelaşi ordin şi cu determinantul 1 atunci $H \triangleleft G$. Într-adevăr, $g \in G$ şi $h \in H \Rightarrow ghg^{-1} \in H$ deoarece :

$$\det\left(ghg^{-1}\right) = \det(g)\det(h)\det\left(g^{-1}\right) = \det(g)\det(g)^{-1}\det(h) = 1 .$$

(3.1.4) Exemplu de subgrup care nu este normal. În grupul S_n cu $n \geq 3$, subgrupul $H = \left\{ f \in S_n \middle| f(n) = n \right\}$ (vezi (4.3.1)), nu este normal. Într-adevăr, dacă $g \in S_n \setminus H$ şi $f \in H$, nu rezultă în mod necesar că $gfg^{-1} \in H$. Pentru aceasta considerăm exemplul următor : f este o permutare cu $f(1) = 2, f(2) = 1$ şi $f(n) = n$, g este o permutare cu $g(1) = 2, g(2) = n$ şi $g(n) = 1$. Atunci $g\left(f\left(g^{-1}(n)\right)\right) = g(f(2)) = g(1) = 2 \neq n$.

Back

#

(3.2) Ordinul unui element într-un grup. Fie G un grup şi $g \in G$. Şirul puterilor pozitive ale elementului g în G este :

$$g^0 = 1, g, g^2, \ldots, g^n, \ldots$$

Dacă acest şir conţine elemente distincte două câte două, el este infinit. Spunem în acest caz că g este element de ordin infinit. Dacă elementele şirului nu sunt distincte, există $i > j \geq 0$ astfel încât $g^i = g^j$. Înmulţind cu g^{-j} obţinem $g^{i-j} = 1$; deci există $k > 0$ a.î. $g^k = 1$.

Fie $n = \min\left\{k \middle| k > 0, g^k = 1\right\}$. Vom arăta că elementele şirului puterilor întregi ale lui g se reduc la : $g^0 = 1, g, g^2, \ldots, g^{n-1}$.

Într-adevăr, din teorema împărţirii cu rest avem pentru orice întreg m,

$$m = nq + r \text{ şi } 0 \leq r < n .$$

Atunci $g^m = g^{nq} \cdot g^r = \left(g^n\right)^q \cdot g^r = g^r$. În plus, puterile $g^0 = 1, g, g^2, \ldots, g^{n-1}$ sunt distincte căci :

$$g^i = g^j \Rightarrow g^{i-j} = 1 \text{ cu } 0 < i - j < r.$$

Spunem în acest caz că *elementul g este de ordin finit şi că ordinul său este n*. Cu alte cuvinte, ordinul unui element g (de ordin finit) este cel mai mic număr întreg pozitiv n astfel încât $g^n = 1$, sau este numărul elementelor distincte din şirul puterilor întregi ale lui g. În plus, pentru orice număr întreg m astfel încât $g^m = 1$ rezultă $n \mid m$.

Vom nota cu $\operatorname{ord}(g)$ ordinul unui element g (finit sau infinit).

(3.2.1) Propoziţie. *Fie G un grup şi* $g \in G$ *un element de ordin n. Mulţimea* $\langle g \rangle = \{1, g, \ldots, g^{n-1}\}$ *este subgrup al lui G.*

Demonstraţia este evidentă ; este suficient să verificăm condiţia $(s1)$ şi aceasta se verifică din cele de mai sus.

În condiţiile de la (3.2.1) spunem că *mulţimea* $\langle g \rangle = \{1, g, \ldots, g^{n-1}\}$ *este grupul ciclic generat de g în G.* Rezultă că ordinul grupului ciclic generat de g coincide cu ordinul lui g. Din aceste consideraţii şi teorema lui *Lagrange* obţinem următorul rezultat :

(3.2.2) Corolar. *Într-un grup finit G, orice element g este de ordin finit şi ordinul (unui element) este un divizor al ordinului grupului.*

(3.2.3) Lemă. *Fie G un grup şi x, y* $\in G$. *Atunci*

$$\operatorname{ord}(xy) = \operatorname{ord}(yx).$$

Demonstraţie. Din egalitatea $xy = x(yx)x^{-1}$ rezultă că pentru orice număr întreg n are loc echivalenţa :

$$(xy)^n = 1 \Leftrightarrow (yx)^n = 1.$$

(3.2.4) Lemă. *Fie G un grup şi x, y* $\in G$ *elemente de ordin finit astfel încât* $xy = yx$, $\operatorname{ord}(x) = m, \operatorname{ord}(y) = n$ şi $(m,n) = 1$. Atunci

$$\operatorname{ord}(xy) = mn.$$

Demonstraţie. Avem $(xy)^{mn} = (x^m)^n (y^n)^m = 1$. Fie p un număr întreg astfel încât $(xy)^p = 1$. Rezultă $x^p \cdot y^p = 1$. Ridicând la puterea m obţinem $x^{pm} \cdot y^{pm} = 1 \Rightarrow y^{pm} = 1$; de aici rezultă $n \mid pm$ şi din $(m,n) = 1$ rezultă $n \mid p$. Ridicând aceeaşi egalitate la puterea n avem $x^{pn} y^{pn} = 1 \Rightarrow x^{pn} = 1$; în mod analog deducem $m \mid p$. Deoarece $(m,n) = 1$ rezultă $mn \mid p$.

(3.2.5) Lemă. *Fie G un grup şi x, y* $\in G$ *astfel încât* $xy = yx$, $\langle x \rangle \cap \langle y \rangle = 1$ *şi* $\operatorname{ord}(x) = m, \operatorname{ord}(y) = n$*: Atunci*

$$\operatorname{ord}(x, y) = [m, n].$$

Demonstraţie. Pentru uşurinţă, fie $M = [m, n]$ şi $d = (m, n)$. Atunci $m = dm', n = dn'$ şi $M = dm'n' = mn' = m'n$. Avem evident :

$$(xy)^M = x^{mn'} \cdot y^{m'n} = (x^m)^{n'} (y^n)^{m'} = 1.$$

Fie p un număr întreg astfel încât $(xy)^p = 1$. Atunci $x^p = y^{-p} \Rightarrow$ $\Rightarrow x^p \in \langle x \rangle \cap \langle y \rangle \Rightarrow x^p = y^{-p} = 1$. Rezultă că $m \mid p$, $n \mid p$ şi prin urmare $M \mid p$.

(3.2.6) Exemplu. *Este posibil ca într–un grup G produsul a două elemente de ordin finit să fie un element de ordin infinit.*

Fie $G = GL_2(\mathbf{Z})$ grupul matricelor pătratice de ordinul 2, cu coeficienţi întregi şi inversabile. Matricele

$$X = \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} \text{ şi } Y = \begin{pmatrix} 0 & 1 \\ -1 & -1 \end{pmatrix}$$

au ordinele $\operatorname{ord}(X) = 4$ şi $\operatorname{ord}(Y) = 3$ iar

$$XY = \begin{pmatrix} -1 & -1 \\ 0 & -1 \end{pmatrix}$$

are ordinul infinit. Deoarece în acest exemplu $\langle X \rangle \cap \langle Y \rangle = 1$ şi

$$YX = \begin{pmatrix} -1 & 0 \\ 1 & -1 \end{pmatrix},$$

rezultă că ipoteza de comutare din lema precedentă este necesară.

Back

#

(3.3) Grupuri de permutări. Permutări pare şi permutări impare.

Fie N o mulţime finită cu n elemente. Mulţimea funcţiilor bijective $f : N \to N$ formează un grup în raport cu operaţia de compunere a funcţiilor. Acest grup se numeşte grupul simetric al mulţimii N şi se notează cu S_N.

O funcţie $f \in S_N$ se numeşte permutare a mulţimii N. Dacă notăm elementele mulţimii N cu numerele 1, 2, ..., n atunci o permutare a mulţimii $N = \{1,2,\ldots,n\}$ se numeşte permutare de grad n iar S_N se va nota cu S_n. În mod tradiţional, o permutare de grad n se notează matriceal, sub forma unei matrice cu 2 linii şi n coloane în care pe linia întâi sunt elementele 1, 2, ..., n iar pe linia a doua sunt imaginile lor prin f, în această ordine :

$$f = \begin{pmatrix} 1 & 2 & \ldots & i & \ldots & n \\ f(1) & f(2) & \ldots & f(i) & \ldots & f(n) \end{pmatrix}.$$

De exemplu, permutarea identică se notează :

$$1 = \begin{pmatrix} 1 & 2 & \ldots & i & \ldots & n \\ 1 & 2 & \ldots & i & \ldots & n \end{pmatrix}.$$

Matricea

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 1 & 7 & 2 & 3 & 6 & 5 & 9 & 7 & 4 \end{pmatrix}$$

nu desemnează o permutare deoarece $f(2) = f(8)$ şi prin urmare f nu este injectivă.

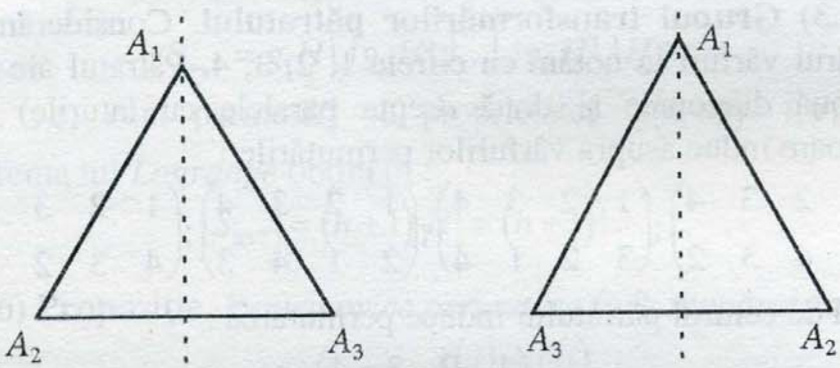
Permutările apar frecvent în matematică şi organizarea lor ca grup este extrem de utilă. Vom prezenta în acest sens câteva exemple.

(3.3.1) Grupurile transformărilor planului. Dacă Π este planul geometric, considerat ca mulţime de puncte, orice bijecţie $t : \Pi \to \Pi$ se numeşte transformare geometrică. Aceste transformări nu pot fi descrise în totalitate dar printre elemenetele lui S_Π apar rotaţiile, translaţiile, omotetiile de raport nenul, transformările liniare nesingulare de coordonate, inversiunile, simetriile etc.

(3.3.2) Grupul transformărilor unui triunghi. Fie $A_1A_2A_3$ un triunghi echilateral. Anumite transformări ale planului păstrează triunghiul $A_1A_2A_3$ invariant : i.e. dacă $f : \Pi \to \Pi$ atunci

$$\{A_1, A_2, A_3\} = \{f(A_1), f(A_2), f(A_3)\}.$$

De exemplu, simetria faţă de înălţimea din vârful A_1 stabileşte între vârfuri bijecţia $A_1 \to A_1, A_2 \to A_3, A_3 \to A_2$.



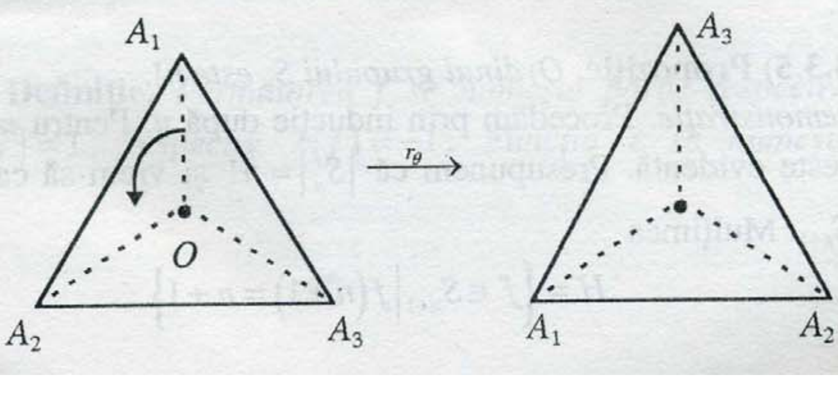
Putem reprezenta această transformare ca o permutare a vârfurilor triunghiului astfel :

$$t_{23} = \begin{pmatrix} A_1 & A_2 & A_3 \\ A_1 & A_3 & A_2 \end{pmatrix}.$$

În mod analog, simetriile faţă de înălţimile din A_2, A_3 induc respectiv permutările

$$t_{13} = \begin{pmatrix} A_1 & A_2 & A_3 \\ A_3 & A_2 & A_1 \end{pmatrix}, \; t_{12} = \begin{pmatrix} A_1 & A_2 & A_3 \\ A_2 & A_1 & A_3 \end{pmatrix}.$$

Dacă O este centrul triunghiului $A_1A_2A_3$ rotaţia în sens trigonometric de centru O şi unghi $\theta = 120°$, în planul Π, induce asupra vârfurilor triunghiului permutarea



$$r_\theta = \begin{pmatrix} A_1 & A_2 & A_3 \\ A_2 & A_3 & A_1 \end{pmatrix}.$$

În mod asemănător, rotaţia de unghi $2\theta = 240°$ induce permutarea

$$r_{2\theta} = \begin{pmatrix} A_1 & A_2 & A_3 \\ A_3 & A_1 & A_2 \end{pmatrix}.$$

Ţinând seama şi de permutarea identică, am obţinut toate permutările posibile ale celor trei vârfuri ale triunghiului. Deci transformarea identică, cele trei simetrii şi cele două rotaţii sunt şase transformări ale planului care induc transformări distincte (deci şase !) ale triunghiului. Alte transformări ale triunghiului nu mai există. În Geometrie se demonstrează că orice transformare a planului care păstrează distanţele şi invariază triunghiul este una din cele şase.

(3.3.3) Grupul transformărilor pătratului. Considerăm în plan un pătrat ale cărui vârfuri le notăm cu cifrele 1, 2, 3, 4. Pătratul are patru axe de simetrie (două diagonale şi două drepte paralele cu laturile) şi simetriile corespunzătoare induc asupra vârfurilor permutările :

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 4 & 3 & 2 \end{pmatrix}; \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 2 & 1 & 4 \end{pmatrix}; \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}; \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix}.$$

Simetria faţă de centrul pătratului induce permutarea :

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}$$

Rotaţiile pătratului în jurul centrului său, cu unghiurile $\frac{\pi}{2}, \pi, \frac{3\pi}{2}, 2\pi$ induc permutările

$$\begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 3 & 4 & 1 \end{pmatrix}; \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}; \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 1 & 2 & 3 \end{pmatrix}; \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 2 & 3 & 4 \end{pmatrix}$$

Se observă că simetria faţă de centru şi rotaţia de unghi π coincid. Rămân opt transformări care formează un grup. Acest grup se notează cu D_4 şi se numeşte grupul diedral al pătratului. Se verifică uşor că este un grup neabelian.

(3.3.4) Definiţie. *Orice subgrup H al grupului S_n se numeşte grup de permutări.*

(3.3.5) Propoziţie. *Ordinul grupului S_n este $n!$.*

Demonstraţie. Procedăm prin inducţie după n. Pentru $n = 1$ sau $n = 2$ afirmaţia este evidentă. Presupunem că $|S_n| = n!$ şi vrem să calculăm ordinul grupului S_{n+1}. Mulţimea

$$H = \left\{ f \in S_{n+1} \middle| f(n+1) = n+1 \right\}$$

este un subgrup în S_{n+1} (se verifică uşor condiţiile (s_1) şi (s_2) sau se verifică numai (s_1) ştiind că $|S_{n+1}| < \left((n+1)^{n+1}!\right)$. Subgrupul H este în corespondenţă bijectivă cu S_n prin funcţia $\varphi : H \to S_n$, $\varphi(f) = \bar{f}$, unde $\bar{f}$ este restricţia lui f la $\{1, 2, ..., n\}$:

$$f = \begin{pmatrix} 1 & 2 & \dots & n & n+1 \\ f(1) & f(2) & \dots & f(n) & n+1 \end{pmatrix} \xrightarrow{\varphi} \bar{f} = \begin{pmatrix} 1 & 2 & \dots & n \\ f(1) & f(2) & \dots & f(n) \end{pmatrix}.$$

Deci $|H| = n!$. Considerăm în S_{n+1} relaţia de congruenţă modulo H:

$$f \equiv g(\operatorname{mod} H) \Leftrightarrow f^{-1}g \in H \Leftrightarrow f(n+1) = g(n+1).$$

Rezultă că mulţimea cât S_{n+1}/H are $n+1$ clase de echivalenţă şi anume:

$$S_{n+1} = g_1H \bigcup g_2H \bigcup \dots \bigcup g_nH \bigcup H$$

unde $g_1, g_2, \dots, g_n$ sunt permutări cu proprietatea $g(n+1) = i, \forall i = 1,2,\dots,n$. Aplicând teorema lui *Lagrange* obţinem :

$$|S_{n+1}| = (n+1)|H| = (n+1)!.$$

(3.3.6) Propoziţie. *Pentru orice permutare $f \in S_n$ numărul raţional*

$$\varepsilon(f) = \prod_{1 \le i < j \le n} \frac{f(j) - f(i)}{j - i}$$

ia numai una din valorile ± 1.

Demonstraţie. Produsul are $\frac{1}{2}n(n-1)$ factori şi este indexat după perechile (i, j) cu $1 \le i < j \le n$. Dacă în această familie de indici dubli se schimbă (i, j) cu (j, i), produsul nu se schimbă. Deci putem scrie

$$\varepsilon(f) = \prod_{\{i,j\}} \frac{f(j) - f(i)}{j - i}.$$

Rezultă că la numărătorul produsului avem aceeaşi factori ca la numitor, mai puţin semnul deoarece când $\{i, j\}$ parcurge mulţimea submulţimilor cu 2 elemente din $\{1, 2, ..., 3\}$, $\{f(i), f(j)\}$ parcurge aceeaşi mulţime de submulţimi.

(3.3.7) Definiţie. *Permutarea f se numeşte pară, respectiv impară, după cum $\varepsilon(f) = 1$, respectiv $\varepsilon(f) = -1$. Funcţia ε se numeşte funcţia signatură.*

(3.3.8) Propoziţie. *Oricare ar fi permutările f, g∈S_n are loc egalitatea :*

$$\varepsilon(fg) = \varepsilon(f)\varepsilon(g),$$

Demonstraţie.

$$\varepsilon(fg) = \prod_{\{i,j\}} \frac{f(g(j)) - f(g(i))}{j-i} = \prod_{\{i,j\}} \frac{f(g(j)) - f(g(i))}{g(j) - g(i)} \cdot \frac{g(j) - g(i)}{j-i} =$$

$$= \prod_{\{i,j\}} \frac{f(g(j)) - f(g(i))}{g(j) - g(i)} \cdot \prod_{\{i,j\}} \frac{g(j) - g(i)}{j-i} = \varepsilon(f) \cdot \varepsilon(g).$$

(3.3.9) Propoziţie. *În grupul S_n numărul permutărilor pare este egal cu numărul permutărilor impare şi este $\frac{1}{2}n!$. Mulţimea permutărilor pare formează un subgrup normal $A_n \triangleleft S_n$, numit grupul altern de grad n.*

Demonstraţie. Este clar că $A_n < S_n$, deoarece $\varepsilon(f) = 1$, $\varepsilon(g) = 1 \Rightarrow \varepsilon(fg) = 1$. De asemenea se vede uşor că $A_n \triangleleft S_n$. Deoarece pentru orice permutare $g \in S_n$ avem $\varepsilon(g) = \varepsilon(g^{-1})$ rezultă că :

$$f \in A_n \Rightarrow \varepsilon(gfg^{-1}) = \varepsilon(g)\varepsilon(f)\varepsilon(g^{-1}) = 1.$$

Considerând în S_n congruenţa modulo A_n şi ţinând seama că $A_n \neq S_n$ rezultă că S_n se împarte în două clase : A_n este clasa permutărilor pare şi $S_n \setminus A_n$ este clasa permutărilor impare. Ele au acelaşi cardinal : $\frac{1}{2}n!$.

(3.3.10) Propoziţie. *Oricare ar fi i, j cu $1 \le i < j \le n$, permutarea*

$$t = \begin{pmatrix} 1 & 1 & \dots & i & \dots & j & \dots & n \\ 2 & 2 & \dots & j & \dots & i & \dots & n \end{pmatrix}$$

este o permutare impară.

Demonstraţie. Din definiţia signaturii rezultă că $\varepsilon(f) = \pm 1$ după cum pentru un număr par, respectiv impar, de perechi (i, j) cu $1 \le i < j \le n$ avem $f(i) > f(j)$. Vom spune că o pereche cu această proprietate este o pereche inversată. O cercetare atentă ne arată că permutarea t de mai sus inversează $2(j-i)-1$ perechi. Deci $\varepsilon(t) = -1$.

Back

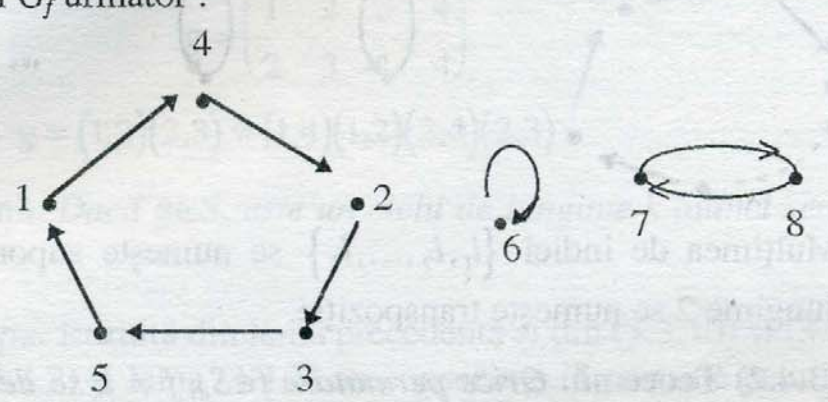
#

(3.4) Graful unei permutări. Descompunerea permutărilor în cicli

Fie $f \in S_n$ o permutare. Putem asocia lui f un graf orientat G_f cu n vârfuri 1, 2, ..., n ale cărui muchii sunt $(i, f(i))$. Deoarece funcţia f este bijectivă rezultă că fiecare vârf este originea unei muchii şi adresa unei muchii, deci fiecare vârf are gradul 2 şi că în total avem n muchii. De exemplu, permutării f din S_8

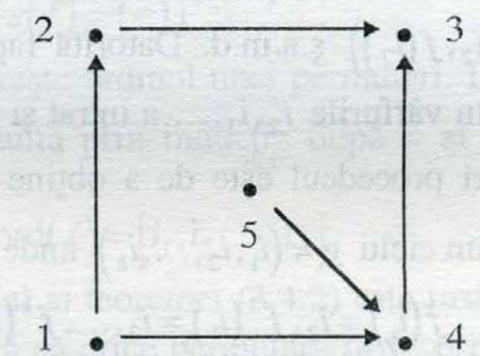
$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 3 & 5 & 2 & 1 & 6 & 8 & 7 \end{pmatrix}$$

i se asociază graful G_f următor :



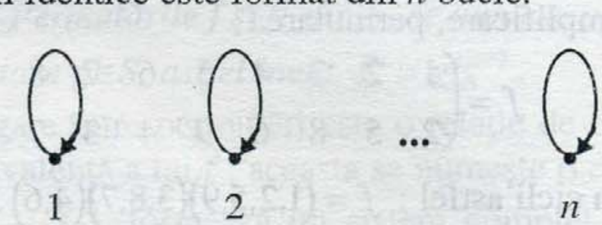
Reciproc, orice graf orientat cu n vârfuri în care orice vârf este originea unei muchii şi capătul unei muchii este graful unei permutări.

De exemplu graful de mai jos



nu este graful unei permutări deoarece 5 nu este adresa unei muchii, 3 este adresa a două muchii şi nu este sursa unei muchii, etc.

Graful permutării identice este format din n bucle.

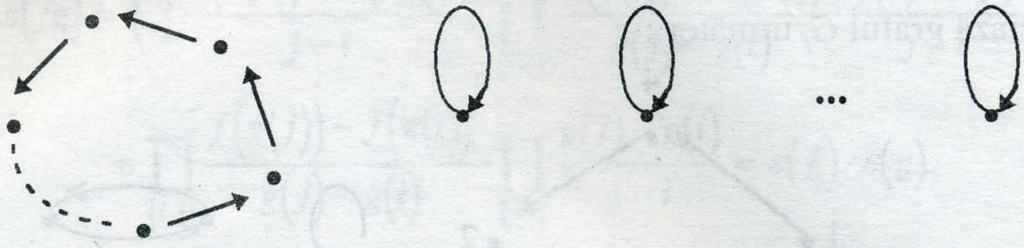


Se observă că buclele grafului asociat unei permutări sunt date de vârfurile care sunt puncte fixe ale permutării.

(3.4.1) Definiţie. *O permutare $g \in S_n$ se numeşte ciclu sau permutare ciclică dacă există o mulţime de indici $i_1, i_2, \ldots, i_k \in \{1,2,\ldots,n\}$ astfel încât :*

$$f(i_1) = i_2, f(i_2) = i_3, \ldots, f(i_{k-1}) = i_k, f(i_k) = i_1 \text{ şi } f(j) = j \text{ pentru } j \neq i_1, i_2, \ldots, i_k .$$

Acest ciclu se notează $g=(i_1,i_2,\ldots,i_k)(j)(l)\ldots(q)$ sau pur şi simplu $g=(i_1,i_2,\ldots,i_k)$. Numărul k se numeşte lungimea ciclului. Graful G_g al unei permutări ciclice este un poligon convex cu k laturi şi, eventual, $n-k$ bucle :



Mulţimea de indici $\{i_1,i_2,\ldots,i_k\}$ se numeşte suportul ciclului g. Un ciclu de lungime 2 se numeşte transpoziţie.

(3.4.2) Teoremă. *Orice permutare $f\in S_n$, $f\neq 1$ se descompune într–un produs finit de permutări ciclice cu suporţii multimi disjuncte. Produsul acestor cicli disjuncţi este unic până la o permutare a factorilor.*

Demonstraţie. Se consideră un vârf $i=i_1$ al grafului asociat lui f şi se trasează muchia $(i_1,f(i_1))$ care pleacă din i_1. Se notează $i_2=f(i_1)$ şi se consideră muchia $(i_2,f(i_2))$ ş.a.m.d. Datorită faptului că obţinem tot timpul vârfuri distincte şi din vârfurile $i_2,i_3,\ldots$ a intrat şi a ieşit câte o muchie, singura posibilitate de a opri procedeul este de a obţine o muchie $(i_k,f(i_k)=i_1)$. În acest fel s-a obţinut un ciclu $g=(i_1,i_2,\ldots,i_k)$ unde

$$f(i_1)=i_2,\, f^2(i_1)=i_3,\ldots,f^k(i_1)=i_1 .$$

Se continuă în acest mod cu vârfurile rămase, obţinându-se în astfel descompunerea grafului în componente conexe şi a permutării în cicli. Este evident că ciclii disjuncţi comută şi deci că avem unicitatea din enunţ.

Spre exemplificare, permutarea

$$f=\begin{pmatrix}1&2&3&4&5&6&7&8&9\\2&5&8&6&9&4&3&7&1\end{pmatrix}$$

se descompune în cicli astfel : $f=(1,2,5,9)(3,8,7)(4,6)$.

(3.4.3) Lemă. *Orice permutare ciclică $g=(i_1,i_2,\ldots,i_k)$ este un produs de $k-1$ transpoziţii. Descompunerea nu este unică.*

Demonstraţie. Se verifică direct prin calcule că are loc egalitatea :

$$(i_1,i_2,\ldots,i_k)=(i_1,i_k)(i_1,i_{k-1})\ldots(i_1,i_3)(i_1,i_2) .$$

Deoarece $(i_1,i_2,\ldots,i_k)=(i_2,i_3,\ldots,i_k,i_1)$ rezultă că avem şi descompunerea $(i_1,i_2,\ldots,i_k)=(i_2,i_1)(i_2,i_k)\ldots(i_2,i_3)$. Înseamnă că descompunerea nu este unică. Mai mult, nici numărul de transpoziţii dintr-o descompunere nu este unic. De exemplu, permutarea $g\in S_4$

$$g=\begin{pmatrix}1 & 2 & 3 & 4\\ 2 & 3 & 1 & 4\end{pmatrix}$$

are descompunerile $g=(1,2)(2,3)=(1,4)(1,2)(2,4)(2,3)$.

(3.4.4) Lemă. *Dacă $g\in S_n$ este un ciclu de lungime k atunci semnul său este $\varepsilon(g)=(-1)^{k-1}$.*

Demonstraţie. Rezultă din lema precedentă şi din (3.3.10) şi (3.3.8).

Teorema (3.4.2) şi lema (3.4.3) au consecinţe importante pentru studiul grupurilor de permutări. Orice permutare $f\in S_n$ se poate scrie ca un produs de transpoziţii. Dacă $f\in S_n$ este un produs de cicli, $f=g_1g_2\ldots g_p$, de lungimi $l_1,l_2,\ldots l_p$ atunci

$$\varepsilon(f)=(-1)^{l_1+\ldots+l_p-p}.$$

O altă consecinţă priveşte ordinul unei permutări. Dacă $f=g_1\ldots g_p$, g_i fiind cicli de lungime l_i, rezultă prin inducţie după p şi aplicând (3.2.5) că ordinul lui f este

$$\operatorname{ord}(f)=[l_1,l_2,\ldots,l_p].$$

Aspectul combinatorial al teoremei (3.4.2) este însă pus în evidenţă de următorul rezultat : se observă că orice permutare $f\in S_n$, prin descompunerea sa în cicli, pune în evidenţă o partiţie a lui n ale cărui elemente sunt lungimile ciclilor care intră în compunerea lui f. Vom aprofunda această asociere.

(3.4.5) Definiţie. *Permutările f şi f' din S_n se numesc permutări conjugate dacă există o permutare $g\in S_n$ astfel încât $f'=gfg^{-1}$.*

Relaţia de conjugare între permutări este o relaţie de echivalenţă. Vom nota cu $C(f)$ clasa de echivalenţă a lui f ; aceasta se numeşte o *clasă de elemente conjugate*. Dacă $\{f_1,f_2,\ldots,f_k\}$ formează un sistem complet de reprezentanţi pentru clasele de elemente conjugate, rezultă că avem partiţia :

$$S_n=C(f_1)\cup C(f_2)\cup\ldots\cup C(f_k).$$

De exemplu, dacă $f=1$ atunci $C(1)=\{1\}$. Deci în partiţia de mai sus figurează şi clasa $C(1)$ care conţine un singur element. Putem preciza acest lucru : $C(1)$ este singura clasă de conjugare care conţine un singur element.

Într-adevăr, dacă $f \in S_n$ şi $C(f) = \{f\}$ înseamnă că $f' = gfg^{-1}$, $\forall\ g \in S_n$. Deci $fg = gf\ \ \forall\ g \in S_n$, adică f permută cu toate permutările lui S_n. Este uşor de demonstrat că dacă $n > 2$, rezultă $f = 1$.

Pentru a preciza descompunerea lui S_n de mai sus vom da următoarea :

(3.4.6) Teoremă. *Permutările f şi f' sunt conjugate în S_n dacă şi numai dacă descompunerile lor conţin acelaşi număr de cicli şi pentru fiecare număr natural $l > 0$, acelaşi număr de cicli de lungime l.*

Demonstraţie. Presupunem că $f' = gfg^{-1}$ şi că f conţine p cicli de lungimi $n_1 \geq n_2 \geq \ldots \geq n_p$. Atunci avem descompunerea lui f (într-o notaţie aproximativă !) :

$$f = \left(a_1, a_2, \ldots, a_{n_1}\right)\left(b_1, b_2, \ldots, b_{n_2}\right)\ldots\left(v_1, v_2, \ldots, v_{n_p}\right).$$

Evident că avem egalitatea de mulţimi

$$\{1,2,\ldots,n\} = \left\{a_1, a_2, \ldots, a_{n_1}, b_1, \ldots, \ldots, v_{n_p}\right\}.$$

Deci putem scrie pe g sub forma :

$$g = \begin{pmatrix} a_1 & a_2 & \ldots & a_{n_1} & b_1 & b_2 & \ldots & b_{n_2} & \ldots & v_1 & v_2 & \ldots & v_{n_1} \\ a_1' & a_2' & \ldots & a_{n_p}' & b_1' & b_2' & \ldots & b_{n_2}' & \ldots & v_1' & v_2' & \ldots & v_{n_p}' \end{pmatrix},$$

unde avem din nou : $\{1,2,\ldots,n\} = \left\{a_1', a_2', \ldots, a_{n_1}', b_1', \ldots, \ldots, v_{n_p}'\right\}$.

Un calcul simplu cu permutări ne arată că

$$f' = \left(a_1', a_2', \ldots, a_{n_1}'\right)\left(b_1', b_2', \ldots, b_{n_2}'\right)\ldots\left(v_1', v_2', \ldots, v_{n_p}'\right).$$

Reciproc, dacă $f = \left(a_1, a_2, \ldots, a_{n_1}\right)\left(b_1, b_2, \ldots, b_{n_2}\right)\ldots\left(v_1, v_2, \ldots, v_{n_p}\right)$ şi $f' = \left(a_1', a_2', \ldots, a_{n_1}'\right)\left(b_1', b_2', \ldots, b_{n_2}'\right)\ldots\left(v_1', v_2', \ldots, v_{n_p}'\right)$ atunci $f' = gfg^{-1}$, unde

$$g = \begin{pmatrix} a_1 & a_2 & \ldots & a_{n_1} & b_1 & b_2 & \ldots & b_{n_2} & \ldots & v_1 & v_2 & \ldots & v_{n_1} \\ a_1' & a_2' & \ldots & a_{n_p}' & b_1' & b_2' & \ldots & b_{n_2}' & \ldots & v_1' & v_2' & \ldots & v_{n_p}' \end{pmatrix}.$$

Cu aceasta teorema este demonstrată.

Este clar acum că şirul descrescător al lungimilor ciclilor unei permutări din S_n este o partiţie a lui n. Rezultă că numărul claselor de permutări conjugate ale lui S_n este numărul $P(n)$ al partiţiilor lui n.

(3.4.7) Teoremă (formula lui Cauchy). *Fie $\pi = 1^{\lambda_1}2^{\lambda_2}\ldots n^{\lambda_n}$ o partiţie a numărului natural n. (i.e π conţine λ_1 părţi egale cu 1, λ_2 părţi egale cu 2 etc.). Clasa de permutări conjugate corespunzătoare partiţiei π conţine*

$$h(\lambda_1, \lambda_2, \ldots, \lambda_n) = \frac{n!}{\lambda_1!\lambda_2!\ldots\lambda_n!1^{\lambda_1}2^{\lambda_2}\ldots n^{\lambda_n}}$$

Demonstraţie. Conform teoremei precedente, trebuie să numărăm toate permutările $f \in S_n$ care conţin λ_1 cicli de lungime 1, λ_2 cicli de lungime 2 etc. Fie f o asemenea permutare şi fie descompunerea lui f ca un produs de cicli :

$$f = (a_1)\ldots(a_{\lambda_1})(b_{11}, b_{21})\ldots(b_{1\lambda_2}, b_{2\lambda_2})\ldots(v_{1\lambda_k}, \ldots, v_{k\lambda_k}),$$

unde lungimea maximă a unui ciclu este k, $k \le n$. Dacă se şterg parantezele în descompunerea de mai sus, se obţin numerele 1, 2,..., n scrise într-o ordine care defineşte o permutare g a lui S_n. Vom arăta că permutarea f de la care am plecat defineşte $\lambda_1!\lambda_2!\ldots\lambda_n!1^{\lambda_1}2^{\lambda_2}\ldots n^{\lambda_n}$ permutări diferite, $g \in S_n$. Într-adevăr, în expresia lui f putem permuta cei λ_i cicli de lungime i în $\lambda_i!$ moduri, fără că f să se schimbe, dar schimbându-se permutarea $g \in S_n$ asociată acestei descompuneri. În plus, orice ciclu de lungime i poate fi scris în i moduri diferite luând ca prim element al ciclului oricare din elementele sale componente, de unde rezultă în total $1^{\lambda_1}2^{\lambda_2}\ldots n^{\lambda_n}$ posibilităţi. În acest mod putem fabrica toate cele $n!$ permutări ale lui S_n înmulţind numărul $h(\lambda_1, \lambda_2, \ldots \lambda_n)$ cu $\lambda_1!\lambda_2!\ldots\lambda_n!1^{\lambda_1}2^{\lambda_2}\ldots n^{\lambda_n}$. De aici rezultă formula lui *Cauchy*.

Comentariu. Combinatorica grupurilor finite este unul din capitolele cele mai interesante ale teoriei grupurilor şi combinatoricii, în acelaşi timp. Noţiunile introductive pe care le-am prezentat aici pot servi ca un punct de plecare în probleme de colorare, teoria acţiunilor grupurilor pe mulţimi finite, metoda de numărare a lui *Pólya – de Bruijn* etc.

Back