1. Ordinul unui element al unui grup

1. 1. Proprietăți ale ordinului unui element al unui grup

Proprietățile noțiunii de ordin al unui element al unui grup sunt de multe ori foarte utile în probleme de concurs, facilitând deseori rezolvarea acestora.

Considerăm cunoscute noțiunile și rezultatele fundamentale ale teoriei grupurilor studiate în liceu (grup, subgrup, morfisme de grupuri).

În cele ce urmează, G este o mulțime nevidă, căreia o lege de compoziție notată multiplicativ îi conferă structură de grup.

Notăm cu ord(G) sau $|G|$ numărul elementelor grupului G, dacă G are un număr finit de elemente și spunem că $\text{ord}(G) = +\infty$ dacă G are o infinitate de elemente.

Reamintim următoarele concepte și proprietăți:

1.1.1. Definiție *Fie* $(G, \cdot)$ *un grup și X o submulțime nevidă a sa.*
Notăm cu $\langle X\rangle = \bigcap\{H \mid X \subseteq H,\ H \text{ subgrup al lui } G\}$.

1.1.2. Proprietate $(\langle X\rangle, \cdot)$ *este un subgrup al lui G (numit subgrupul generat de mulțimea X).*

1.1.3. Observații

a) $\langle X\rangle$ este cel mai mic subgrup (în raport cu relația de ordine „$\subseteq$") al lui G, astfel încât $X \subseteq \langle X\rangle$.

b) $\langle X\rangle = \left\{\alpha \in G \mid \exists n \in N^*, \exists x_1, x_2, ..., x_n \in G, \exists x_1, x_2, ..., x_n \in Z, \alpha = x_1^{k_1} \cdot x_2^{k_2} \cdot ... \cdot x_n^{k_n}\right\}$

c) Dacă $x \in G$, atunci subgrupul generat de elementul x este $\langle x\rangle = \{x^k \mid k \in \mathbf{Z}\}$.

1.1.4. Definiție *Grupul* $(G, \cdot)$ *se numește grup ciclic dacă există* $x \in G$ *astfel încât* $\langle x\rangle = G$. *În acest caz elementul x se numește generator al grupului G.*

1.1.5. Observație Dacă $(G, \cdot)$ este un grup ciclic de ordinul n, a este un generator al grupului G și $k \in \mathbf{Z}$, atunci a^k este un generator al lui G dacă și numai dacă $(n, k) = 1$.

1.1.6. Definiție *Grupul* $(G, \cdot)$ *se numește finit generat dacă există* $n \in N^*$ *și* $a_1, a_2, ..., a_n \in G$ *astfel încât* $\langle a_1, a_2, ..., a_n\rangle = G$.
În acest caz elementele $a_1, a_2, ..., a_n$ *se numesc generatori ai grupului G.*

1.1.7. Observații

a) Orice grup ciclic este comutativ.

b) Orice grup finit este finit generat.

Exemple de grupuri ciclice: $(\mathbf{Z}, +)$, $(\mathbf{Z}_n, +)$, $(U_n, \cdot)$, unde U_n este grupul rădăcinilor de ordinul n ale unității.

1.1.8. Definiție *Fie grupul $(G, \cdot)$ cu elementul neutru e.*

Elementul $x \in G$ este de ordin finit dacă $\exists\, m \in N^*$, $x^m = e$.

În acest caz, $\min\{m \in N^* / x^m = e\} \overset{not}{=} ord(x)$ se numește ordinul elementului x.

Elementul $x \in G$ este de ordin infinit dacă x nu este de ordin finit.

1.1.9. Teoremă *Fie grupul $(G, \cdot)$ și $x \in G$.*

a) *Dacă $ord(x) = n \in N^*$, atunci elementele $e, x, \ldots, x^{n-1}$ sunt distincte două câte două și $\forall k \in \mathbf{Z}$, $x^k = x^{k(mod\ n)}$*

b) *$ord(x) = +\infty \Leftrightarrow \forall k_1, k_2 \in \mathbf{Z}$, $k_1 \neq k_2$, avem $x^{k_1} \neq x^{k_2}$.*

1.1.10. Consecințe

C 1. Fie grupul $(G, \cdot)$. Dacă $x \in G$ și $ord(x) = n \in \mathbf{N}^*$, atunci $ord\langle x\rangle = n$ și $\langle x\rangle = \{e, x, \ldots, x^{n-1}\}$.

C 2. Grupul finit G de ordinul $n \in \mathbf{N}^*$ este ciclic $\Leftrightarrow$ G are un element ordinul n.

C 3. Fie grupul $(G, \cdot)$. Dacă $x \in G$, $ord(x) = n \in \mathbf{N}^*$ și $k \in \mathbf{Z}$, $x^k = e$, atunci n/k.

Demonstrație: Conform teoremei împărțiri cu rest, $\exists!\ q, r \in \mathbf{Z}$. $0 \leq r < ord(x)$, astfel încât $k = ord(x) \cdot q + r$.

Atunci $x^k = x^{nq+r} = (x^n)^q \cdot x^r$ și cum $x^n = e$, rezultă că $x^k = x^r$ și deci $x^r = e$.

Dar $n = ord(x) = \min\{m \in \mathbf{N}^* \mid x^m = e\}$ și rezultă $r = 0$, deci $k = n \cdot q$, adică n / k.

C 4. Orice element al unui grup finit are ordinul finit.

C 5. Orice două grupuri ciclice de același ordin sunt izomorfe. Dacă G este un grup ciclic de ordinul n, atunci $(G, \cdot) \approx (\mathbf{Z}, +)$

C 6. Orice subgrup al unui grup ciclic este ciclic.

C 7. Dacă $x, y \in G$, atunci

a) $\text{ord}(x) = \text{ord}(x^{-1})$

b) $\text{ord}(x \cdot y) = \text{ord}(y \cdot x)$

Demonstrație:

a) <u>I. Dacă $\text{ord}(x) = n \in \mathbf{N}^*$</u> avem $x^n = e$ și $\left(x^{-1}\right)^n = \left(x^n\right)^{-1} = e^{-1} = e$.

Fie $k = \text{ord}(x^{-1})$. Din **C3.** rezultă k / n.

Cum $e = \left(x^{-1}\right)^k = \left(x^k\right)^{-1}$, rezultă că $x^k = e$ și cum $\text{ord}(x) = n$, din **C3.** rezultă că n / k. Așadar $n = k$.

<u>II. Dacă $\text{ord}(x) = +\infty$</u> să presupunem că $\text{ord}(x^{-1}) = k \in \mathbf{N}^*$. Atunci din cazul anterior rezultă că $\text{ord}(x) = \text{ord}(x^{-1})^{-1} = k$, fals. Așadar $\text{ord}(x^{-1}) = +\infty$.

b) <u>I. Dacă $\text{ord}(x \cdot y) = n \in \mathbf{N}^*$</u> avem $(x \cdot y)^k = e \Leftrightarrow x \cdot (y \cdot x)^{k-1} \cdot y = e \Leftrightarrow$ $(y \cdot x)^k \cdot y = y \Leftrightarrow (y \cdot x)^k = e$, așadar $\text{ord}(y \cdot x) = k' \in \mathbf{N}^*$ și k' / k.

Dar $(y \cdot x)^{k'} = e \Leftrightarrow y \cdot (x \cdot y)^{k'-1} \cdot x = e \Leftrightarrow (x \cdot y)^{k'} = e$ și cum $\text{ord}(x \cdot y) = k$ rezultă și k / k' și deci $k = k'$.

<u>II. Dacă $\text{ord}(x \cdot y) = +\infty$</u>, presupunând că $\text{ord}(y \cdot x) = k \in \mathbf{N}^*$ rezultă ca mai înainte că $\text{ord}(x \cdot y) = k$, fals. Așadar $\text{ord}(y \cdot x) = +\infty$.

C 8. Dacă $f : G \to G'$ este un morfism injectiv de grupuri multiplicative și $a \in G$, atunci $\text{ord}(a) = \text{ord}(f(a))$.

Demonstrație:

<u>I. Dacă $\text{ord}(a) = k \in \mathbf{N}^*$</u> avem $e' = f(a^k) = (f(a))^k$ și deci și ordinul elementului $f(a) \in G'$ este finit. Fie $t = \text{ord}(f(a)$. Rezultă că t / k.

Dar $e' = f(a^t) = (f(a))^t$ și pentru că f este o funcție injectivă rezultă că $a^t = e$ și cum $\text{ord}(a) = k$ avem și k / t, deci $k = t$.

<u>II. Dacă $\text{ord}(a) = +\infty$</u>, presupunem că $\text{ord}(f(a)) = k \in \mathbf{N}^*$.

Atunci $(f(a))^k = e = f(a^k)$ și din injectivitatea lui f rezultă că $a^k = e$, ceea ce este fals. Așadar $\text{ord}(f(a)) = +\infty$.

Să observăm că afirmația anterioară este adevărată și în cazul izomorfismelor de grupuri, ceea ce întărește imaginea intuitivă că elementele asociate printr-un izomorfism „au aceleași proprietăți"

C 9. Fie grupul $(G, \cdot)$ și $a, b \in G$ cu $\text{ord}(a) = m \in \mathbf{N}^*$, $\text{ord}(b) = n \in \mathbf{N}^*$, astfel încât $a \cdot b = b \cdot a$. Notăm cu $d = (m, n)$, $p = [m, n]$. Atunci:

a) $\text{ord}(a \cdot b) / p$

b) $\dfrac{p}{d} / \text{ord}(a \cdot b)$

Demonstrație: Se știe că dacă $a\cdot b = b\cdot a$, atunci $\forall\ k\in\mathbf{Z}$, $(a\cdot b)^k = a^k b^k$

a) Avem $m = d\cdot m_1$ și $n = d\cdot n_1$, cu $m_1, n_1\in\mathbf{N}$, $(m_1, n_1) = 1$, iar $p = d\cdot m_1\cdot n_1$.

$(a\cdot b)^p = (a\cdot b)^{d\cdot m_1\cdot n_1} = a^{m\cdot n_1}\cdot b^{n\cdot m_1} = \left(a^m\right)^{n_1}\cdot\left(b^n\right)^{m_1} = e \overset{1.1.10, C3}{\Rightarrow} k / p$,

unde $\mathrm{ord}(a\cdot b) = k$ (este evident că $\mathrm{ord}(a\cdot b)\in\mathbf{N}^*$).

b) $\dfrac{p}{d} = m_1\cdot n_1$. Demonstrăm că $m_1\cdot n_1 / k$.

$(a\cdot b)^k = e \Rightarrow a^k = b^{-k} \Rightarrow a^{k\cdot n} = b^{-k\cdot n} = e \overset{1.1.10, C3}{\Rightarrow} m / k\cdot n \Leftrightarrow d\cdot m_1 / k\cdot d\cdot n_1 \Rightarrow$

$\Rightarrow \left.\begin{array}{l} m_1 / k\cdot n_1 \\ (m_1, n_1) = 1 \end{array}\right\} \Rightarrow m_1 / k.$

Analog rezultă că n_1 / k și cum $(m_1, n_1) = 1$ obținem $m_1\cdot n_1 / k$

Observații:

a) $\mathrm{ord}(a\cdot b) / m\cdot n$

b) Dacă $a, b\in G$, $a\cdot b = b\cdot a$, $\mathrm{ord}(a) = m$, $\mathrm{ord}(b) = n$ și $(m, n) = 1$, atunci $\mathrm{ord}(a\cdot b) = [m, n] = m\cdot n$.

c) Există situații când $\mathrm{ord}(a, b) = \dfrac{[m, n]}{(m, n)} = m_1\cdot n_1$.

De exemplu, în grupul $(\mathbf{Z}_{12}, +)$, $\mathrm{ord}\left(\hat{6}\right) = 2$, $\mathrm{ord}\left(\hat{2}\right) = 6$ și $\mathrm{ord}\left(\hat{2}+\hat{6}\right) = 3$.

d) Există situații când $\mathrm{ord}(a\cdot b) = [m, n]$, chiar dacă $(m, n) \neq 1$.

De exemplu, în grupul $(\mathbf{Z}_{24}, +)$, $\mathrm{ord}\left(\hat{6}\right) = 4$, $\mathrm{ord}\left(\widehat{12}\right) = 6$ și $\mathrm{ord}\left(\widehat{12}+\hat{6}\right) = 4$.

C 10. Fie grupul $(G, \cdot)$ și $x\in G$, $\mathrm{ord}(x) = n\in\mathbf{N}^*$. Atunci:

a) $\forall\ k\in\mathbf{Z}$, $\mathrm{ord}(x^k) / n$

b) $\forall\ k\in\mathbf{Z}$, $\mathrm{ord}(x^k) = \dfrac{n}{(k, n)}$

Demonstrație: a) $\left(x^k\right)^n = e \overset{1.1.10, C3}{\Rightarrow} \mathrm{ord}(x^k) / n$.

b) Fie $d = (k, n)$. Atunci există $n_1, k_1\in\mathbf{Z}$ astfel încât $n = d\cdot n_1$, $k = d\cdot k_1$, $(n_1, k_1) = 1$.

Cum $\left(x^k\right)^{n_1} = x^{n\cdot k_1} = e \overset{1.1.10, C3}{\Rightarrow} \mathrm{ord}(x^k) / n_1$ (1)

Fie $s = \mathrm{ord}(x^k)$. Avem $x^{k\cdot s} = e$ şi cum $\mathrm{ord}(x) = n \overset{1.1.10,C3}{\Rightarrow} n / k\cdot s \Rightarrow$ $d\cdot n_1 / d\cdot k_1\cdot s \Rightarrow n_1 / k_1\cdot s$ şi deoarece $(n_1, k_1) = 1$ rezultă că n_1 / s.

Ținând cont de (1) obținem $n_1 = s$, adică $\mathrm{ord}(x^k) = n_1 = \dfrac{n}{d} = \dfrac{n}{(k, n)}$.

C 11. Fie $(G, \cdot)$ un grup ciclic de ordinul n, $G = \langle a \rangle$ şi $k \in \mathbf{Z}$.
Atunci: a^k este generator al grupului $\Leftrightarrow (k, n) = 1$.

Demonstrație: Reamintim următoarea

Lemă *Fie $k, n \in \mathbf{Z}$. Atunci: $(k, n) = 1 \Leftrightarrow \exists\, t, s \in \mathbf{Z},\ k\cdot t + n\cdot s = 1$*

„$\Rightarrow$" Cum $\langle a^k \rangle = G$, există $t \in \mathbf{Z}$ astfel încât $\left(a^k\right)^t = a$ şi deci $a^{k\cdot t-1} = e$ $\overset{1.1.10,C3}{\Rightarrow}$ $\mathrm{ord}(a) = n / (k\cdot t - 1) \Rightarrow \exists\, s \in \mathbf{Z},\ k\cdot t - 1 = s\cdot n \Leftrightarrow n\cdot(-s) + k\cdot t = 1 \overset{\text{Lemă}}{\Leftrightarrow}$ $(k, n) = 1$.

„$\Leftarrow$" $(k, n) = 1 \overset{\text{Lemă}}{\Leftrightarrow} \exists\, t, s \in \mathbf{Z},\ k\cdot t + n\cdot s = 1$.

Atunci $a = a^{k\cdot t + n\cdot s} = \left(a^k\right)^t \cdot \left(a^n\right)^s = \left(a^k\right)^t$ şi deci $a \in \langle a^k \rangle$ şi cum grupul G este generat de a, rezultă că $G \subseteq \langle a^k \rangle$. Dar $\langle a^k \rangle \subseteq G$ şi deci $G = \langle a^k \rangle$.
Să observăm că există $\varphi(n)$ generatori ai lui G.

Consecință Dacă $(G, \cdot)$ este un grup ciclic de ordinul p, cu $p \in \mathbf{N}$ număr prim, atunci: **a)** orice element al lui G este generator al grupului
b) G nu are subgrupuri proprii.

Bibliografie

1. Gh. Andrei, C-tin Caragea, V. Ene – *Algebră – Culegere de probleme pentru examene de admitere şi olimpiade şcolare*, Ed. Scorpion 7, Bucureşti 1995
2. M. Burtea, G. Burtea – *Matematică – clasa a XII-a – Elemente de analiză matematică. Algebră superioară*, Ed. Carminis 2001
3. I. Purdea, Gh Pic – *Tratat de algebră modernă*, vol I, Ed Academiei, Bucureşti, 1977
4. D. Andrica, N. Bişboacă, I. Şerdean, M. Andronache, M. Piticari, D. Zaharia - *Matematică – Manual pentru clasa a XII-a*, M1, Ed. Plus, 2002
5. Colecția „Gazeta Matematică"

Probleme rezolvate

R1.2.1. *Fie $(G, \cdot)$ un grup şi $g \in G$, cu $ord(g) = m \cdot n$, unde $m, n \in N^*$, $(m, n) = 1$. Să se demonstreze că există şi sunt unice $a, b \in G$ astfel încât $g = a \cdot b = b \cdot a$ şi $ord(a) = m$, $ord(b) = n$.*

Soluţie: <u>Existenţa</u> Cum $(m, n) = 1$, există $k, t \in \mathbf{Z}$ astfel încât $m \cdot k + n \cdot t = 1$ (1)

Fie $a = g^{n \cdot t}$ şi $b = g^{m \cdot k}$. Observăm că $a^m = \left(g^{n \cdot t}\right)^m = \left(g^{m \cdot n}\right)^t = e$ şi analog $b^n = e$.

Cum $a^m = e$, din 1.1.10, C 3. rezultă că $ord(a) = p \in \mathbf{N}^*$ şi p / m (2)

Presupunem că $p \neq m$. Atunci $a^p = \left(g^{n \cdot t}\right)^p = g^{n \cdot t \cdot p}$ şi cum $ord(g) = m \cdot n$, din 1.1.10, C 3, rezultă că $m \cdot n / n \cdot t \cdot p$ şi deci $m / t \cdot p$. Din (1) rezultă că $(m, t) = 1$ şi obţinem $m/p \overset{(2)}{\Rightarrow} p = m \Leftrightarrow ord(a) = m$. Analog se demonstrează că $ord(b) = n$.

<u>Unicitatea</u> Fie $a, b \in G$ astfel încât $g = a_1 \cdot b_1 = b_1 \cdot a_1$ şi $ord(a_1) = m$, $ord(b_1) = n$.

Atunci $g^n = (a_1 \cdot b_1)^n = a_1^n \cdot b_1^n = a_1^n$. Fie k, t din relaţia (1).

Avem $n \cdot t = 1 - m \cdot k$ şi $a_1^{n \cdot t} = g^{n \cdot t}$, deci $a_1 \cdot \left(a_1^m\right)^{-k} = g^{n \cdot t}$ şi cum $a_1^m = e$, rezultă $a_1 = g^{n \cdot t} = a$ (a este cel din demonstraţia existenţei)

Analog rezultă că $b_1 = g^{m \cdot k} = b$.

R1.2.2. *Fie $(G, \cdot)$ un grup şi $x \in G$, un element de ordin finit. Dacă $m, n \in \mathbf{Z}$ astfel încât $(m, n) = 1$, $ord(x^m) = n$ şi $ord(x^n) = m$, să se demonstreze că $ord(x) = m \cdot n$.*

Soluţie: Fie $d = ord(x)$. Din 1.1.10, C 10, cum x^m şi x^n comută, avem că $ord(x^{m+n}) / ord(x)$, deci $m \cdot n / d$ (1)

Din $ord(x^m) = n$ rezultă că $x^{m \cdot n} = e$ şi deci (1.1.10, C 3.) $d / m \cdot n$.

Folosind şi relaţia (1) rezultă că $d = m \cdot n$.

R1.2.3. *Fie $(G, \cdot)$ un grup. Să se demonstreze că următoarele afirmaţii sunt echivalente:*

1) Orice submulţime H a sa care este parte stabilă în raport cu operaţia grupului, este subgrup al lui G.

2) Toate elementele grupului G sunt de ordin finit.

Marian Andronache

Soluţie: „1 ⇒ 2" Fie $x \in G$. Cum $(G, \cdot)$ este grup, rezultă că $\forall\, t \in \mathbf{N}^*$, $x^t \in G$ şi deci mulţimea $H = \{x^t \mid t \in \mathbf{N}^*\}$ este parte stabilă a lui G în raport cu operaţia grupului. Aşadar, conform ipotezei, H este subgrup al lui G şi deci H conţine elementul neutru e al lui G. În consecinţă, există $k \in \mathbf{N}^*$ astfel încât $x^k = e$ şi deci afirmaţia (2) este adevărată.

„$2 \Rightarrow 1$" Fie $H \subset G$, H parte stabilă a lui G în raport cu operația lui G.
Fie $x \in H$. Din ipoteză rezultă că $\exists\, k \in \mathbf{N}^*$, $x^k = e$.
Cum H este parte stabilă, avem $x^h \in H$, $\forall\, h \in \mathbf{N}^*$ și deci $e \in H$.
$x^k = e \Rightarrow x^{-1} = x^{k-1}$ și cum H este parte stabilă avem că și x^{k-1} (adică x^{-1}) se află în H. Așadar H este subgrup al lui G.

Observații

1. Există grupuri infinite cu toate elementele de ordin finit.
De exemplu $(\mathbf{Z}_p[X], +)$, dacă p este un număr prim.

2. Dacă $(G, \cdot)$ este un grup finit, atunci $\forall\, H \subset G$, avem:
H e parte stabilă a lui G în raport cu operația lui $G \Leftrightarrow H$ e subgrup al lui G.

3. Dacă impunem condiția de finitudine doar asupra lui H obținem rezultatul cunoscut:
Pentru grupul $(G, \cdot)$ și mulțimea finită $H \subset G$,
H e parte stabilă a lui G în raport cu operația lui $G \Leftrightarrow H$ e subgrup al lui G.

R1.2.4. *Să se demonstreze că orice subgrup al unui grup ciclic este ciclic.*

Soluție: Fie $(G, \cdot)$ un grup ciclic.
I. Dacă $\mathrm{ord}(G) = +\infty$ și $G = \langle a \rangle$, atunci grupul G este izomorf cu $(\mathbf{Z}, +)$ (un izomorfism este $f : G \to \mathbf{Z}$, $f(a^k) = k$, $\forall\, k \in \mathbf{Z}$) și cum subgrupurile lui $\mathbf{Z}$ sunt de forma $n\mathbf{Z} = \langle n \rangle$, cu $n \in \mathbf{Z}$, rezultă că și subgrupurile lui G sunt ciclice, pe baza următorului rezultat cunoscut:

***Lemă** dacă grupurile $(G, \cdot)$ și $(G', \cdot)$ sunt izomorfe și $f : G \to G'$ este un izomorfism, atunci: H este subgrup al lui $G \Leftrightarrow f(H)$ este subgrup al lui G'.*

II. Dacă $\mathrm{ord}(G) = n \in \mathbf{N}^*$ și $G = \langle a \rangle$, subgrupurile improprii ale lui G fiind evident ciclice, fie H un subgrup propriu al lui G, $H = \{a^{k_1}, a^{k_2}, \ldots, a^{k_t}\}$, cu $k_1 < k_2 < \ldots < k_t$ numere naturale nenule.
Demonstrăm, prin inducție după s, că $H = \langle a^{k_1} \rangle$, deci că $\forall\, s \in \mathbf{N}^*$, $a^{k_s} \in \langle a^{k_1} \rangle$.
Pentru $s = 2$, $a^{k_1}, a^{k_2} \in H$. Cum H e subgrup al lui G obținem $\left(a^{k_1}\right)^{-1} \cdot a^{k_2} \in H$ și deci $a^{k_2 - k_1} \in H$ și din $k_2 - k_1 < k_2$ rezultă că avem $k_2 = 2 \cdot k_1$ și $a^{k_2} \in \langle a^{k_1} \rangle$.
Presupunem că avem $k_{s-1} = (s-1) \cdot k_1$ și demonstrăm că și $k_s = k_1 \cdot s$.

Avem: $k_s - k_1 > k_s - k_2 > \ldots > k_s - k_{s-1}$ și $a^{k_s - k_1}, a^{k_s - k_2}, \ldots, a^{k_s - k_{s-1}} \in H$ iar $k_s - k_1, k_s - k_2, \ldots, k_s - k_{s-1} \in \{k_1, k_2, \ldots, k_{s-1}\}$ și deci $k_s - k_{s-1} = k_1$ și folosind ipoteza de inducție obținem $k_s = s \cdot k_1$ și $a^{k_s} = \left(a^{k_1}\right)^s \in \langle a^{k_1} \rangle$, așadar H este ciclic, generat de a^{k_1}.