Capitolul 10

Soluţiile exerciţiilor

1. Dacă $c \in M \setminus (A \cup B)$, atunci $f(\{c\}) = (\emptyset, \emptyset) = f(\emptyset)$. Reciproc, dacă $A \cup B = M$ şi $f(X) = f(Y)$, atunci $X = X \cap M = (X \cap A) \cup (X \cap B) = (Y \cap A) \cup (Y \cap B) = Y$.

Dacă f este surjectivă, atunci există X cu $f(W) = (A, \emptyset)$, deci $A \cap B \subseteq W \cap B = \emptyset$. Reciproc, dacă $A \cap B = \emptyset$, atunci pentru orice $(C, D) \in \mathcal{P}(A) \times \mathcal{P}(B)$, $f(C \cup D) = (C, D)$.

2. Se observă că f este injectivă (resp. surjectivă) $\Leftrightarrow$ $f^* f_* = I$ (resp. $f_* f^* = I$), sau se folosesc definiţiile.

3. Fie $a, b, p, q \in \mathbf{Z}$ cu $f(a, b) = f(p, q)$. Rezultă $2\sqrt{2}(a-p) \in \mathbf{Q}$, deci $a = p$; apoi $(b - q)(b + q - 2/3) = 0$, deci $b = q$, deoarece $2/3 \notin \mathbf{Z}$.

Cf. primei părţi, putem aşeza punctele de coordonate întregi într-un şir $(P_i)_{i \geq 1}$ astfel încât $d_1 < d_2 < d_3 ...$, unde d_i este distanţa de la P_i la C. Dacă $d_n < r_n < d_{n+1}$, cercul de centru C şi rază r_n conţine în interior exact n puncte cu coordonatele numere întregi.

4. Folosind egalităţile $4k = (2k + 1)^2 - (2k - 1)^2$ şi $2k + 1 = (k + 1)^2 - k$, se arată că $Im(f) = \mathbf{Z} \setminus (4\mathbf{Z} + 2)$.

5. $\{\emptyset$, $\{a\}$, $\{b\}$, $\{c\}$, $\{d\}$, $\{a, b\}$, $\{a, c\}$, $\{a, d\}$, $\{b, c\}$, $\{b, d\}$, $\{c, d\}$, $\{a, b, c\}$, $\{a, b, d\}$, $\{a, c, d\}$, $\{b, c, d\}$, $\{a, b, c, d\}\}$, unde $a = \emptyset$, $b = \{\emptyset\}$, $c = \{\{\emptyset\}\}$ şi $d = \{\emptyset, \{\emptyset\}\}$.

6. A_1 este finită şi $Im(f_1) \supseteq Im(f_1 f_2) \supseteq \cdots$, deci există $a_1 \in \cap_{n \geq 1} Im(f_1 \cdots f_n)$. A_2 este finită, deci există $a_2 \in \cap_{n \geq 2} Im(f_2 \cdots f_n)$ astfel încât $f_1(a_2) = a_1$ ş.a.m.d.

7. Dacă $b \in B$, atunci $f(B) = b \notin B$, contradicţie. Rezultă că $b \notin B$, adică există $C \subseteq A$ cu $b = f(C) \in C$. Deci $f(B) = f(C)$ şi $b \in C \setminus B$.

8. Injectivitatea lui g rezultă din injectivitatea lui f şi faptul că $f(C) \subseteq C$. Fie $y \in A$. Dacă $y \notin C$, atunci $g(y) = y$. Dacă $y \in C$, atunci există $x \in B \setminus A$ şi $n \geq 1$ astfel încât $y = f^n(x)$, deci $z = f^{n-1}(x) \in C$ şi $g(z) = y$.

Pentru cazul particular, $f : [0,1] \to [0,1)$, $f(x) = x/2$, rezultă bijecţia $g(x) = \begin{cases} 1/2^{n+1} & \text{dacă} \quad x = 1/2^n, \\ x & \text{altfel.} \end{cases}$

9. Aplicând exerciţiul anterior pentru $A = v(E)$, $B = D$ şi $f = vu$, obţinem $D \simeq v(E) \simeq E$.

10. Fie $p_B : B \times C \to B$ şi $p_C : B \times C \to C$ proiecţiile canonice. Fie funcţiile $\alpha : B^A \times C^A \to (B \times C)^A$, $\alpha(f,g)(a) = (f(a), g(a))$ pentru orice $(f,g) \in B^A \times C^A$, $a \in A$, şi $\beta : (B \times C)^A \to B^A \times C^A$, $\beta(h) = (p_B h, p_C h)$. Se arată că α, β sunt inverse una celeilalte.

Fie funcţiile $\gamma : (C^B)^A \to C^{A \times B}$, $(\gamma(f))(a,b) = f(a)(b)$, pentru orice $f \in (C^B)^A$, $a \in A$, $b \in B$, şi $\delta : C^{A \times B} \to (C^B)^A$, $(\delta(g))(a)(b) = g(a,b)$, $g \in C^{A \times B}$, $a \in A$, $b \in B$. Se arată că γ, δ sunt inverse una celeilalte.

11. Inducţie după n, cazul $n = 2$ fiind uşor. La pasul inductiv, scriem $|A_1 \cup A_2 \cup \cdots \cup A_n \cup A_{n+1}| = |A_1 \cup A_2 \cup \cdots \cup A_n| + |A_{n+1}| - |(A_1 \cap A_{n+1}) \cup (A_2 \cap A_{n+1}) \cup \cdots \cup (A_n \cap A_{n+1})|$ şi aplicăm ipoteza de inducţie.

Altfel. Fie $A = A_1 \cup A_2 \cup ... \cup A_n$ şi $B = X \setminus A$. Pentru $C \subseteq X$, fie $\chi_C : C \to \{0,1\}$ funcţia caracteristică a lui C în X; rezultă că $|C|$ este suma valorilor lui χ_C. Se arată că $\chi_A = 1 - \chi_B = 1 - (1 - \chi_{A_1}) \cdots (1 - \chi_{A_n})$.

12. (a), (b), (d). Reprezentăm o funcţie $f : A \to B$ sub forma

$$f = \begin{pmatrix} 1 & 2 & \ldots & a \\ f(1) & f(2) & \ldots & f(a) \end{pmatrix}$$

cu $f(1), f(2), ..., f(a) \in B$. Dacă f este oarecare, fiecare element $f(i)$ poate fi ales în b moduri. Deci $N = b^a$. Dacă f este injectivă (resp. strict crescătoare), atunci $f(1), f(2), ..., f(a)$ sunt distincte (resp. formează un şir strict crescător). Deci $N_i = A_b^a$ şi $N_r = C_b^a$.

(c). Pentru $i \in B$, fie E_i mulţimea funcţiilor $f : A \to B$ cu $i \notin \mathrm{Im}(f)$. Atunci mulţimea non-surjecţiilor $f : A \to B$ este $E_1 \cup E_2 \cup \cdots \cup E_b$. Dacă

$1 \leq i_1 \leq i_2 \leq \cdots \leq i_k \leq b$, atunci $E_{i_1} \cap \cdots \cap E_{i_k}$ este practic mulţimea funcţiilor $h : A \to B \setminus \{i_1, ..., i_k\}$, deci are $(b-k)^a$ elemente. Pentru k fixat, sunt C_b^k astfel de intersecţii. Se aplică ex. 11.

(e). Fie $C = \{1, ..., a+b-1\}$. Dacă $f : A \to B$ este o funcţie crescătoare, atunci funcţia

$$f' : A \to C, f' = \begin{pmatrix} 1 & 2 & 3 & \dots & a \\ f(1) & f(2)+1 & f(3)+2 & \dots & f(a)+a-1 \end{pmatrix}$$

este strict crescătoare. Reciproc, dacă $g : A \to C$ este o funcţie strict crescătoare, atunci funcţia

$$g'' : A \to C, g'' = \begin{pmatrix} 1 & 2 & 3 & \dots & a \\ g(1) & g(2)-1 & g(3)-2 & \dots & g(a)-a+1 \end{pmatrix}$$

este crescătoare. Cum aplicaţiile $f \mapsto f'$, $g \mapsto g''$ sunt inverse una celeilalte, $N_c = C_{a+b-1}^a$, cf. (d).

13. Unui monom $X_1^{i_1} X_2^{i_2} \cdots X_n^{i_n}$ de grad k îi asociem şirul $0 \leq i_1 \leq i_1 + i_2 \leq ... \leq i_1 + \cdots + i_{n-1} \leq k$. Reciproc, unui şir $0 \leq j_1 \leq j_2 \leq ... \leq j_{n-1} \leq k$ îi asociem monomul de grad k, $X_1^{j_1} X_2^{j_2 - j_1} \cdots X_{n-1}^{j_{n-1} - j_{n-2}} X_n^{k - j_{n-1}}$. Cele două funcţii astfel definite sunt inverse una celeilalte. Se aplică punctul (e) al exerciţiului precedent.

14. Pentru $1 \leq i \leq n$, fie A_i mulţimea mulţimea permutărilor $\sigma \in S_n$ cu $\sigma(i) = i$. Atunci mulţimea permutărilor cu puncte fixe este $A_1 \cup A_2 \cup \cdots \cup A_n$. Dacă $1 \leq i_1 \leq i_2 \leq \cdots \leq i_k \leq n$, atunci $A_{i_1} \cap \cdots \cap A_{i_k}$ este practic mulţimea permutărilor mulţimii $\{1, ..., n\} \setminus \{i_1, ..., i_k\}$, deci are $(n-k)!$ elemente. Pentru k fixat, sunt C_n^k astfel de intersecţii. Se aplică ex. 11.

15. Pentru $1 \leq i \leq s$, fie A_i mulţimea numerelor $1 \leq q \leq n$ divizibile cu p_i. Atunci mulţimea numerelor pozitive $\leq n$ şi neprime cu n este $A_1 \cup A_2 \cup \cdots \cup A_s$. Dacă $1 \leq i_1 < i_2 < \cdots < i_k \leq s$, atunci $A_{i_1} \cap \cdots \cap A_{i_k}$ este mulţimea numerelor $1 \leq q \leq n$ divizibile cu $p_{i_1} \cdots p_{i_k}$, deci are $n/p_{i_1} \cdots p_{i_k}$ elemente. Se aplică ex. 11.

16. O relaţie de echivalenţă cu k clase de echivalenţă pe $\{1, 2, ..., n\}$ determină $k!$ surjecţii $\{1, 2, ..., n\} \to \{1, 2, ..., k\}$ obţinute din surjecţia canonică prin diverse numerotări ale claselor dechivalenţă. Deci numărul acestor relaţii este $s_{n,k}/k!$ unde $s_{n,k}$ este numărul surjecţiilor de la $\{1, 2, ..., n\}$ la $\{1, 2, ..., k\}$ (vezi ex. 12(c)). Numărul căutat este $s_{n,1}/1! + s_{n,2}/2! + \cdots + s_{n,n}/n!$.

17. Relaţia este reflexivă ($n|0 = a - a$), simetrică ($n|a - b$ implică $n|b - a$) şi tranzitivă ($n|a - b$ şi $n|b - c$ implică $n|a - c = a - b + b - c$).

18. (a). α este reflexivă ($0 = a - a \in \mathbf{Z}$), simetrică ($a - b \in \mathbf{Z}$ implică $b - a \in \mathbf{Z}$) şi tranzitivă ($a - b \in \mathbf{Z}$ şi $b - c \in \mathbf{Z}$ implică $a - c = a - b + b - c \in \mathbf{Z}$). Altfel: α este relaţia asociată funcţiei $f : \mathbf{R} \to \mathbf{C}$, $f(x) = \cos(2\pi x) + i\sin(2\pi x)$. $(b), (c)$. β nu este tranzitivă: $(0, 1), (1, 2) \in \beta$, $(0, 2) \notin \beta$, iar γ nu este reflexivă: $(1/3, 1/3) \notin \gamma$.

19. Simplificăm scrierea punând xy în loc de (x, y) şi suprimând acoladele. Fie $\Delta = 11, 22, 33$. Avem $g(12, 21, 13) = 0$, $g(\Delta, 12, 21, 23) = 1$, $g(12, 21) = 2$, $g(\Delta, 12, 21, 13, 31) = 3$, $g(12, 21, 11, 22, 13, 23) = 4$, $g(\Delta, 12, 21, 13, 23) = 5$, $g(12, 21, 11, 22) = 6$, $g(\{1, 2, 3\}^2) = 7$, $g(12, 23) = 8$, $g(\Delta, 12, 23) = 9$. $g(12) = 12$, $g(\Delta, 12) = 13$, $g(11) = 14$, $g(\Delta) = 15$. În plus, $10, 11 \notin \mathrm{Im}(g)$, deoarece o relaţie simetrică şi antisimetrică este $\subseteq \Delta$ deci tranzitivă.

20. Pentru orice $f, g, h \in F$, avem $D_{ff} = \emptyset$, $D_{fg} = D_{gf}$ şi $D_{fh} \subseteq D_{fg} \cup D_{gh}$.

21. Clasele de echivalenţă sunt dreptele ce trec prin 0 şi un sistem de reprezentanţi este dat de un semicerc fără unul din capete al cercului unitate.

22. $\sim$ este relaţia asociată funcţiei $f : \mathbf{C} \to \mathbf{R}$, $f(z) = \mathrm{Re}(z)$. Clasele de echivalenţă sunt dreptele verticale, iar $\mathbf{R}$ este un sistem de reprezentanţi.

23. Relaţia este reflexivă ($fI = If$), simetrică ($fu = ug$ implică $gu^{-1} = u^{-1}f$) şi tranzitivă ($fu = ug$ şi $gv = vh$ implică $fuv = uvf$).

24. Relaţia este reflexivă ($a + b = b + a$), simetrică ($a + d = b + c$ implică $b + c = a + d$) şi tranzitivă ($a + d = b + c$ şi $c + f = d + e$ implică $a + f = b + e$). Avem bijecţia $[(a, b)] \mapsto a - b : \mathbf{N} \times \mathbf{N}/\sim \to \mathbf{Z}$.

25. Relaţia este reflexivă ($ab = ba$), simetrică ($ad = bc$ implică $bc = ad$) şi tranzitivă ($ad = bc$ şi $cf = de$ implică $af = be$). Avem bijecţia $[(a, b)] \mapsto a/b : \mathbf{Z} \times \mathbf{N}^*/\sim \to \mathbf{Q}$.

26. Relaţia este reflexivă ($\lim\limits_{n\to\infty}(a_n - a_n) = 0$), simetrică ($\lim\limits_{n\to\infty}(a_n - b_n) = 0$ implică $\lim\limits_{n\to\infty}(b_n - a_n) = 0$) şi tranzitivă ($\lim\limits_{n\to\infty}(a_n - b_n) = 0$ şi $\lim\limits_{n\to\infty}(b_n - c_n) = 0$ implică $\lim\limits_{n\to\infty}(a_n - c_n) = \lim\limits_{n\to\infty}(a_n - b_n + b_n - c_n) = 0$). Avem bijecţia $[(a_n)_{n\geq 1}] \mapsto \lim\limits_{n\to\infty}(a_n) : \mathcal{C}/\sim \to \mathbf{R}$.

27. Buna-definire înseamnă: $\hat{k} = \hat{l} \Rightarrow f(\hat{k}) = f(\hat{l})$. Rezultă că buna-definire este echivalentă cu $4 \mid n$.

28. Calculăm în câte moduri putem completa o tablă $n \times n$. Sunt n^{n^2} operaţii dintre care $n^{n(n+1)/2}$ sunt comutative deoarece elementele sub-diagonale sunt deja precizate. Sunt $n^{(n-1)^2+1}$ operaţii care au element neutru deoarece linia şi coloana elementului neutru sunt unic determinate şi elementul neutru poate fi oricare dintre cele n elemente.

29. Fie funcţiile $f_n : S \to S$, $f_n(x) = x^n$, $n \geq 1$. Cum S este finit, există $n > m \geq 1$ astfel încât $f_n = f_m$.

30. Se arată că $T_n = T_1 T_{n-1} + T_2 T_{n-2} + \cdots + T_{n-1} T_1$ (vezi [9, 3.23]).

31. (a) neasociativă, necomutativă, fără element neutru. (b) asociativă, necomutativă, fără element neutru. (c) neasociativă, comutativă, fără element neutru. (d) asociativă, comutativă, fără element neutru. (e) asociativă, comutativă, cu elementul neutru zero.

32. $f(x * y = x + 1) = 0$ deoarece $1 * (2 * 3) \neq (1 * 2) * 3$, $f(x * y = x) = 1$, $f(x * y = xy + 1) = 2$ deoarece $1 * (2 * 3) \neq (1 * 2) * 3$, $f(x * y = 0) = 3$, $f(x * y = x + 1$ pentru $x, y \geq 1$, $0 * x = x * 0 = x) = 4$, $f(x * y = x$ pentru $x, y \geq 1$, $0 * x = x * 0 = x) = 5$, $f(x * y = xy + 1$ pentru $x, y \geq 1$, $0 * x = x * 0 = x) = 6$, $f(x * y = x + y) = 7$. Deci f este surjecţie.

33. Vezi soluţia ex. precedent.

34. Necomutativă: $0 * (1/2) \neq (1/2) * 0$, asociativă: $x * (y * z) = x + [y] + [z] = (x * y) * z$, fără element neutru: $e * x = x$ implică $e = 0$, dar $0 * (1/2) \neq 1/2$.

35. $(x * y) * z - x * (y * z) = (ac + b - b^2)(x - z)$, deci $*$ asociativă $\Leftrightarrow b^2 = b + ac$. $x * e = x \Leftrightarrow (ae - 1 + b)x + be + c = 0$, deci $*$ are element neutru $\Leftrightarrow b \mid c$ şi $b = b^2 - ac$. Presupunem că $M_{a,b,c}$ este monoid. Rezultă că $d = c/b$ este întreg şi $b = 1 + ad$, $c = d(1 + ad)$; aşadar $x * y = axy + (1 + ad)(x + y) + d(1 + ad)$. Avem izomorfismele de monoizi $f : M_{a,b,c} \to M_{a,1,0}$, $f(x) = x + d$ şi $g : M_{a,1,0} \to K_a$, $g(x) = ax + 1$ (N. Beli).

36. Fie $a, b \geq 1$. Atunci $a + a \neq a$, dar $max(a, a) = min(a, a) = a$ şi $cmmmc(a, a) = a$, deci $(\mathbf{N}, +)$ nu este izomorf cu nici unul din ceilalţi trei monoizi. În plus, $max(a, b), min(a, b) \in \{a, b\}$, dar $cmmmc(2, 3) = 6$, deci al doilea monoid nu este izomorf cu al treilea sau cu al patrulea. În fine, ultimii doi nu sunt izomorfi deoarece în $(\mathbf{N} \cup \{\infty\}, min)$ ecuaţia $min(a, x) = a$ are o infinitate de soluţii.

37. Dacă M este monoid, morfismele $(\mathbf{N}, +) \to M$ au forma $n \mapsto a^n$, a fixat (cf. teoremei 22). Endomorfismele lui $(\mathbf{N}, max)$ sunt funcţiile crescătoare. Singurul morfism $f : (\mathbf{N}, max) \to (\mathbf{N}, +)$ este cel nul, deoarece $x \leq y$ implică $f(y) = f(x) + f(y)$.

38. $f(n) = \{1, 2, ..., n\}$.

39. Fie $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbf{Z})$ cu $A^3 = 0$. Rezultă că $|A| = 0$, apoi $A^2 = (a + d)A$ şi $(a + d)A^2 = 0$, deci $A^2 = 0$. Există $B \in M_3(\mathbf{Z})$ cu $B^3 = 0$ şi $B^2 \neq 0$, de exemplu $B = \begin{pmatrix} 0 & 0 & 0 \\ 1 & 0 & 0 \\ 0 & 1 & 0 \end{pmatrix}$.

40. Prima parte este imediată. Pentru partea a doua, pornim cu un grup cu a elemente şi iterăm construcţia $M \mapsto M'$.

41. $(\mathbf{N}^n, +)$ are n atomi: $(1, 0, ..., 0)$,...,$(0, ..., 0, 1)$. Doi monoizi izomorfi au acelaşi număr de atomi.

42. Monoidul $(\mathbf{N}^2, +)$ are atomii $(1, 0)$ şi $(0, 1)$, iar $(\mathbf{N} \setminus \{1\}, +)$ are atomii 2 şi 3. Dacă $f : (\mathbf{N}^2, +) \to (\mathbf{N} \setminus \{1\}, +)$ este un izomorfism şi $f(1, 0) = a$, $f(0, 1) = b$, atunci $bf(1, 0) = af(0, 1)$, deci $(b, 0) = (a, 0)$, contradicţie.

43. Atomii unui monoid liber sunt literele, deci $W(S)$ are s atomi. Dacă monoizii sunt izomorfi, ei au acelaşi număr de atomi, deci $s = t$. Reciproc, dacă $s = t$, orice bijecţie $S \to T$ se extinde la un izomorfism $W(S) \to W(T)$.

44. Fie $n \neq 5, 8$. Orice element neinversabil din M_n este $\geq n + 1$, deci $p = (n - 1)^2$ este atom. $n + 1$ nu divide $(2n - 1)^2$, deoarece $n \neq 8$. Deci $q = (2n - 1)^2$ este atom, altfel $(2n - 1)^2 = ab$ cu $a, b \geq 2n + 1$, imposibil. Analog se arată că $r = (n - 1)(2n - 1)$ este atom. Pentru $n = 5$, putem lua $p = 4^2$, $q = 14^2$ şi $r = 56$. Pentru $n = 8$, putem lua $p = 7^2$, $q = 23^2$ şi $r = 161$. Altfel. Cf. teoremei lui Dirichlet, progresia aritmetică $(an - 1)_{a \geq 1}$ conţine o infinitate de numere prime. Fie $p \neq q$ două dintre acestea. Rezultă că p^2, q^2 şi $(pq)^2$ sunt atomi (O.I.M. 1977).

45. Atomii lui M_2 sunt numerele prime impare, iar atomii lui M_3 sunt numerele prime de forma $3k+1$ şi produsele pq cu p, q numere prime de forma $3k+2$. În M_3 sunt numere ce se scriu în mai multe moduri ca produs de atomi (e.g., $55^2 = 25 \cdot 121$).

46. $xy = (xy)^{-1} = y^{-1}x^{-1} = yx$.

47. Notând $0 = (\hat{0}, \hat{0})$, $a = (\hat{1}, \hat{0})$, $b = (\hat{0}, \hat{1})$ şi $c = (\hat{1}, \hat{1})$ avem

$+$	0	a	b	c
0	0	a	a	c
a	a	0	c	b
b	b	c	0	a
c	c	b	a	0

48. $(13) = ab$, $(23) = a^2b$, $(132) = a^2$.

	I	a	a^2	b	ab	a^2b
I	I	a	a^2	b	ab	a^2b
a	a	a^2	I	ab	a^2b	b
a^2	a^2	I	a	a^2b	b	ab
b	b	a^2b	ab	I	a^2	a
ab	ab	b	a^2b	a	I	a^2
a^2b	a^2b	ab	b	a^2	a	I

49. Fie G un grup cu 4 elemente. Elementele lui G au ordinul divizor al lui 4. Dacă G conţine un element x de ordin 4, atunci G este ciclic generat de x, deci $G \simeq \mathbf{Z}_4$. Presupunem că $G = \{1, a, b, c\}$ cu $a^2 = b^2 = c^2 = 1$. Dacă $ab = 1$ (resp., $ab = a$, $ab = b$), atunci $a = b$ (resp., $b = 1$, $a = 1$), contradicţie. Deci $ab = c$, şi analog $ba = c$, $ac = ca = b$, $bc = cb = a$. Comparând tablele de înmulţire (vezi exerciţiului 47), vedem că $G \simeq \mathbf{Z}_2 \times \mathbf{Z}_2$.

50. Fie $k \geq 1$ cu $(ab)^k = 1$. Rezultă că $a^k = b^{-k}$, apoi $a^{nk} = (b^n)^{-k} = 1$, deci m divide nk, şi cum $(m, n) = 1$, rezultă că m divide k. Din simetrie rezultă că n divide k, deci mn divide k, deoarece $(m, n) = 1$.

51. Fie G un grup cu 6 elemente. G conţine un element a de ordin 3 şi un element b de ordin 2, cf. teoremei lui Cauchy. Deci $G = \{1, a, a^2, b, ab, ab^2\}$. Dacă $ba = 1$ (resp., $ba = b$, $ba = b^2$, $ba = a$), atunci $a = b$ (resp., $a = 1$, $a = b$, $b = 1$), contradicţie. Deci $ba = ab$ sau $ba = a^2b$. Dacă $ba = ab$, atunci ab are ordinul 6 (cf. ex. 50), deci G este ciclic generat de ab, aşadar $G \simeq \mathbf{Z}_6$. Dacă $ba = a^2b$, atunci comparând tablele de înmulţire (vezi ex. 48), se vede că $G \simeq S_3$.

52. Fie G un grup cu 8 elemente. Dacă G conţine un element de ordin 8, atunci G este ciclic, deci $G \simeq \mathbf{Z}_8$. Dacă toate elementele $\neq 1$ au ordinul 2, atunci $G \simeq \mathbf{Z}_2^3$. Presupunem că G conţine un element a de ordin 4 şi fie $b \in G\setminus < a >$. Rezultă că $G = \{1, a, a^2, a^3, b, ab, ab^2, a^3b\}$. Deducem că $G \simeq \mathbf{Z}_2 \times \mathbf{Z}_4$ dacă $ab = ba$, $G \simeq D_4$ dacă $ba = a^3b$ şi $b^2 = 1$, şi $G \simeq Q$ dacă $ba = a^3b$ şi $b^2 = a^2$.

53. Fie $f : A \to B$ o bijecţie. Se arată că $\sigma \mapsto f\sigma f^{-1} : S_A \to S_B$ este izomorfism.

54. Bijecţia $f : (0, \infty) \to (-1, 1)$, $f(x) = (x - 1)/(x + 1)$, verifică condiţia $f(xy) = f(x) * f(y)$ pentru $x, y > 0$.

55. (a). 1 este elementul neutru, $1 = ac = ca = b^2 = d^2 = e^2 = f^2 = g^2$ şi $ad \neq da$, deci G grup neabelian. $G =< a, d >$ deoarece $b = a^2$, $c = a^3$, $e = ad$, $f = a^2d$, $g = ad$. (b). Clasele de conjugare sunt $\{1\}$, $\{b\}$, $\{a, c\}$, $\{d, f\}$, $\{e, g\}$. $Z(G) = \{1, b\}$. (c). 1 are ordinul 1, a şi c au ordinul 4, celelalte au ordinul 2. (d). Subgrupurile sunt $\{1\}$, G, $\{1, b, d, f\}$, $\{1, b, e, g\}$, $\{1, a, b, c\}$ $\{1, b\}$, $\{1, d\}$, $\{1, e\}$, $\{1, f\}$, $\{1, g\}$, normale, adică reuniune de clase de conjugare, fiind primele 6. (e). $G/ < b >= \{\hat{1}, \hat{a}, \hat{d}, \hat{e}\}$ este izomorf cu grupul lui Klein, cf. exerciţiului 49, deoarece elementele $\neq \hat{1}$ au ordinul doi.

56. Realizăm pe D_4 ca grup de permutări, ca în ex. 89. Se compară tablele de înmulţire.

57. Fie T un triunghi echilateral cu centrul cercului circumscris O. Grupul D_3 constă din rotaţiile decentru O şi unghi 0, $2\pi/3$, $4\pi/3$ radiani şi cele 3 simetrii faţă de axele de mediatoarele lui T. Privind aceste transformari ca permutări ale vârfurilor triunghiului se obţine un izmorfism $D_3 \simeq S_3$.

58. D_{12} are elemente de ordin 12 în timp ce S_4 nu are.

59. Cu excepţia elementelor 1 care are ordinul 1 şi a lui -1 care are ordinul 2, toate celelalte au ordinul 4. Subgrupurile de ordin 4 sunt $\{\pm 1, \pm i\}$, $\{\pm 1, \pm j\}$, $\{\pm 1, \pm k\}$ şi sunt normale deoarece sunt de indice 2. Există un singur subgrup de ordin 2, $\{\pm 1\}$. Normalitatea acestuia se verifica cu definiţia sau observăm că $Z(Q) = \{\pm 1\}$.

60. Elementul neutru este $(0, 1)$ şi $(x, a)^{-1} = (-ax, a)$. Elementele $(2, -1)$ şi $(1, -1)$ au ordinul 2 şi produsul lor $(1, 1)$ are ordin infinit.

61. Fie $f : \mathbf{Q} \to \mathbf{Z}$ un morfism şi $x, n \in \mathbf{Z}$, $n \neq 0$. Atunci $f(x) = nf(x/n)$, deci $f(x) = 0$ deoarece se divide cu orice n.

62. $(\mathbf{Q}^*, \cdot)$ are un element de ordinul 2, pe -1, celelalte grupuri nu au. Apoi se aplică ex. precedent.

63. Pentru orice $a_1, ..., a_n, s \in \mathbf{Z} \setminus \{0\}$, $< a_1/s, ..., a_n/s >$ este subgrup al grupului ciclic $< 1/s >$, deci ciclic.

64. Putem lua grupurile aditive $G = \mathbf{Q}^{\mathbf{N}}$ şi $H = \mathbf{Z} \times \mathbf{Q}^{\mathbf{N}}$. H este subgrup al lui G iar $(a_1, a_2, ...) \mapsto (0, a_1, a_2, ...) : G \to H$ este morfism injectiv. Grupurile nu sunt izomorfe deoarece $x \mapsto 2x$ este automorfism al lui G dar nu este automorfism al lui H.

65. G este produsul direct al grupurilor $\mathbf{Z}$ şi $(\{\pm 1\}, \cdot)$. G nu este ciclic deoarece are şi elemente de ordin finit > 1 (e.g. $(0, -1)$) şi elemente de ordin infinit (e.g. $(1, 0)$).

66. Fie H un subgrup nenul al lui $(\mathbf{Q}, +)$. Înmulţind cu un anumit $q \in \mathbf{Q}^*$, putem presupune că $H \supseteq \mathbf{Z}$. Folosim următoarele două observaţii. Dacă $a/b \in H$ cu $a, b \in \mathbf{N}^*$ prime între ele, atunci $1/b \in H$ (din $1 = aa' + bb'$, rezultă $1/b = b' + a'a/b \in H$). Dacă $b, c \in \mathbf{N}^*$ sunt prime între ele, atunci $1/b, 1/c \in H \Leftrightarrow 1/b, 1/c \in H$ (dacă $1/(bc) \in H$ şi $1 = bb' + cc'$, atunci $1/(bc) = b'/c + c'/b \in H$).

67. Fie H un subgrup nenul al lui $\mathbf{Z}_{p^\infty}$. Dacă $a \in \mathbf{Z}^*$ nu se divide cu p, atunci $\widehat{a/p^n} \in H \Leftrightarrow \widehat{1/p^n} \in H$ (din $1 = ab + p^n c$, rezultă $\widehat{1/p^n} = b\widehat{a/p^n} \in H$). Fie $M = sup\{n | \ \widehat{1/p^n} \in H\}$. Dacă $M = \infty$, atunci $H = \mathbf{Z}_{p^\infty}$, altfel $H =< \widehat{1/p^M} >$. În încheiere se aplică teorema fundamentală de izomorfism epimorfismului $x \mapsto x^{p^n} : \mathbf{Z}_{p^\infty} \to \mathbf{Z}_{p^\infty}$.

68. Prima parte se verifică prin calcul. $\{u((2+i)^n)|\ n \geq 1\} = \{(\widehat{4}, \widehat{0}), (\widehat{1}, \widehat{0})\}$, $\{u((2-i)^n)|\ n \geq 1\} = \{(\widehat{0}, \widehat{4}), (\widehat{0}, \widehat{1})\}$.

69. (a). $\widehat{1+i}$ are ordinul 4 deoarece $\widehat{1+i}^2 = \widehat{2i} \neq \widehat{1}$ şi $\widehat{1+i}^4 = \widehat{-4} = \widehat{1}$. Dacă există $n \geq 1$ cu $(2+i)^n \in \mathbf{Q}^*$, atunci $(2+i)^n = (2-i)^n$, imposibil cf. exerciţiului precedent. (b). Avem $2+i = \sqrt{5}(cos\ \theta + i\ sin\ \theta)$ cu $\theta = arctg(1/2)$. Din (a) rezultă că $arctg(1/2)/\pi \notin \mathbf{Q}^*$. Subgrupul generat de $\widehat{1+i}$ şi $\widehat{2+i}$ nu este ciclic deoarece conţine un element de ordin 4 şi un altul de ordin infinit. (c). Dacă G este finit generat, atunci el este numărabil, deci $\mathbf{C}^*$ ar fi numărabil, ca reuniunea claselor sale modulo $\mathbf{Q}^*$, contradicţie.

70. Se adaptează demonstraţia teoremei 25 astfel. Fie H un subgrup neciclic al lui $\mathbf{Z}^2$. Atunci H nu este conţinut în $\mathbf{Z} \times \{0\}$ sau $\{0\} \times \mathbf{Z}$ deoarece acestea sunt izomorfe cu $\mathbf{Z}$. Există atunci elementele $(a, b) \in H$ cu $a > 0$ minim şi $(0, c) \in H$ cu $c > 0$ minim. Se arată că $< (a, b), (0, c) >= H$

71. Putem lua $G = (\mathbf{Z}[X], +)$ şi izomorfismul $u : G \times G \to G$, $u(f, g) = f(X^2) + Xg(X^2)$.

În următoarele patru exerciţii, $\mathbf{Z}[[X]]$ (resp. $\mathbf{Z}[X]$) desemnează grupul aditiv al seriilor formale (resp. polinoamelor).

72. Fie A mulţimea morfismelor $\mathbf{Z}[X] \to \mathbf{Z}$. Se arată că aplicaţia $u \mapsto u(1) + u(X)X + u(X^2)X^2 + \cdots : A \to \mathbf{Z}[[X]]$ este bijectivă.

73. Negăm. Putem presupune că $u(X^n) \neq 0$ pentru orice $n \geq 0$. Punem $q_0 = 1$ şi $q_n = (|u(1)| + 1)(|u(X)| + 1) \cdots (|u(X^{n-1})| + 1)$, pentru $n \geq 1$. Mulţimea seriilor de forma $\sum_n r_n X^n$ cu $r_n \in \{0, q_n\}$ este nenumărabilă, deci există două serii de acest tip distincte cu aceeaşi imagine prin u. Scăzându-le, găsim o serie $f = a_m X^m + a_{m+1} X^{m+1} + \cdots$ cu $a_m \neq 0$ şi $a_n \in \{0, \pm q_n\}$ pentru $n \geq m$ astfel încât $u(f) = 0$. Deci

$$\pm q_m u(X^m) = u(a_m X^m) = -q_{m+1} u(a'_{m+1} X^{m+1} + a'_{m+2} X^{m+2} + \cdots)$$

unde $a'_i = a_i / q_{m+1}$. Deci q_{m+1} divide $\pm q_m u(X^m)$, de unde rezultă că $|u(X^m)| + 1$ divide $u(X^m)$, contradicţie.

74. Presupunem că există $f = \sum_n a_n X^n$ cu $u(f) \neq 0$. Atunci aplicaţia $v : \mathbf{Z}[[X]] \to \mathbf{Z}$, $v(\sum_n b_n X^n) = u(b_0 a_0 + (b_0 + b_1) a_1 X + (b_0 + b_1 + b_2) a_2 X^2 + \cdots)$, este morfism de grupuri. Cum u se anulează pe $\mathbf{Z}[X]$, rezultă că $v(X^n) = u(f) \neq 0$, pentru orice n, contradicţie, cf. ex. 73.

75. Cf. ex. 73, există N cu $u(X^n) = 0$ pentru $n \geq N+1$. Atunci morfismul $u - u(1)\pi_0 - u(X)\pi_1 - \cdots - u(X^N)\pi_N$ se anulează pe $\mathbf{Z}[X]$, deci este nul, cf. ex. 74.

76. (a). $\widehat{na/b} = \widehat{0} \Leftrightarrow na/b \in \mathbf{Z} \Leftrightarrow b$ divide n. (b). Pentru orice $a_1, ..., a_n, s \in \mathbf{N}^*$, $< \widehat{a_1/s}, ..., \widehat{a_n/s} >$ este subgrup al grupului ciclic cu s elemente $< \widehat{1/s} >$. (c). G nu este finit deoarece are elemente de orice ordin (cf. (a)), deci G nu este nici finit generat, cf. (b).

77. Fie $f : \mathbf{Z}_m \to \mathbf{Z}_n$ morfism. Pentru $x \in \mathbf{Z}$, $f(\widehat{x}) = f(x\widehat{1}) = \overline{ax}$ cu $\overline{a} = f(\widehat{1})$.

În plus, $\overline{0} = f(\widehat{m}) = \overline{am}$, deci $n \mid ma$, adică n/d divide a unde $d = (m, n)$. Reciproc, dacă n/d divide a, f definit prin $f(\widehat{x}) = \overline{ax}$ este morfism.

78. Grupul $(\mathbf{R}, +)/\mathbf{Z}$ are un singur element de ordinul doi $1/2 + \mathbf{Z}$. Grupul $(\mathbf{R}, +)/ < \sqrt{2}, \sqrt{3} >$ are trei elemente de ordinul doi: $\sqrt{2}/2 + H$, $\sqrt{3}/2 + H$ şi $\sqrt{2}/2 + \sqrt{3}/2 + H$, unde $H =< \sqrt{2}, \sqrt{3} >$.

79. Funcţia $f : \mathbf{Z} \to \mathbf{Z}^2/ < (2,3) >$, $f(m) = \widehat{(m, m)}$ este un izomorfism de grupuri, deoarece $(m, m) \notin < (2,3) >$ pentru orice m nenul şi $(a, b) = (b-a)(2,3) + (3a-2b)(1,1)$ pentru $a, b \in \mathbf{Z}$. În $(\mathbf{Z}^2, +)/ < (2,2) >$, $\widehat{(1,1)}$ are ordinul 2 iar $\widehat{(1,0)}$ are ordin infinit.

80. Fie $p : G \to G/H$ morfismul canonic şi fie elementul nenul $x = p(1, 2, ..., 2^n, 2^{n+1}, ...)$. Pentru orice n, $x = p(0, 0, ..., 0, 2^n, 2^{n+1}, ...) = 2^n p(0, 0, ..., 0, 1, 2, ...)$. Un element $y \in G$ care se scrie sub forma $2^n y_n$ pentru orice n este obligatoriu nul.

81. Prima afirmaţie se verifică uşor. Fie $K = \{0, a, b, c\}$ grupul lui Klein (vezi soluţia ex. 47). Se arată că orice permutare $\sigma \in S_K$ cu $\sigma(0) = 0$ este endomorfism al lui K.

82. $x^{ka} = 1 \Leftrightarrow n$ divide $ka \Leftrightarrow n/(n, k)$ divide a.

83. Se foloseşte ultima parte a demonstraţiei corolarului 45. Subgrupurile lui $\mathbf{Z}_{12} = \mathbf{Z}/12\mathbf{Z}$ sunt $\mathbf{dZ}/12\mathbf{Z}$ cu d divizor al lui 12: $\{\widehat{0}\}$, $\{\widehat{0}, \widehat{6}\}$, $\{\widehat{0}, \widehat{4}, \widehat{8}\}$, $\{\widehat{0}, \widehat{3}, \widehat{6}, \widehat{9}\}$, $\{\widehat{0}, \widehat{2}, \widehat{4}, \widehat{6}, \widehat{8}, \widehat{10}\}$, $\mathbf{Z}_{12}$. Pentru grupurile factor se aplică corolarul 45 şi teorema 44, de exemplu $\mathbf{Z}_{12}/\{\widehat{0}, \widehat{3}, \widehat{6}, \widehat{9}\} \simeq \mathbf{Z}_3$.

84. Fie $n \geq 1$. Subgrupul $U_n = \{z \in \mathbf{C} | \ z^n = 1\} = \{cos\ 2k\pi/n + i\ sin\ 2k\pi/n |\ k = 0, 1, ..., n-1\}$ este ciclic generat de $cos\ 2\pi/n + i\ sin\ 2\pi/n$. Dacă H este un subgrup cu n elemente, atunci $H \subseteq U_n$ (cf. teoremei lui Lagrange), deci $H = U_n$.

85. Fie C_n subgrupul lui G generat de $f_n = D^{-n}TD^n$. Deoarece $f_n(x) = x+1/2^n$, subgrupurile C_n alcătuiesc un lanţ strict ascendent a cărui reuniune este un subgrup care nu este finit generat.

86. H este subgrup normal deoarece $\sigma(ij)(kl)\sigma^{-1} = (\sigma(i)\sigma(j))(\sigma(k)\sigma(l))$. Grupul S_3/H are $4!/4 = 6$ elemente. Deoarece $(12)(13)(12)^{-1}(13)^{-1} = (123) \notin H$, rezultă că $\widehat{(12)}$ şi $\widehat{(13)}$ nu comută în S_3/H. Aplicăm exerciţiul 51.

87. Permutarea identică are ordinul 1, cele 10 de transpoziţii sunt impare şi au ordinul 2, cele 20 de cicluri de lungime 3 sunt pare şi au ordinul 3, cele 30 de cicluri de lungime 4 sunt impare şi au ordinul 4, cele 24 de cicluri de lungime 5 sunt pare şi au ordinul 5, cele 15 produse de câte două transpoziţii disjuncte sunt pare şi au ordinul 2, cele 20 produse de câte o transpoziţie şi un ciclu de lungime 3 disjuncte sunt impare şi au ordinul 6.

88. Fie $f : S_3 \to \{\pm 1, \cdot\}$ un morfism. Elementele de ordin 3 din S_3, adică ciclurile de lungime 3, sunt duse de f în 1. Cum un produs de două transpoziţii distincte este un ciclu de lungime 3, f duce toate transpoziţiile în 1 (morfismul trivial) sau toate în -1 (morfismul signatură).

89. $D = \{I, (1234), (13)(24), (1432), (13), (24), (12)(34), (14)(23)\}$, adică grupul diedral D_4, vezi şi exerciţiul 55.

90. $H = \{I, (1234)(5678), (1537)(2846), (1836)(2745), (1638)(2547), (1432)$ $(5876), (1735)(2648), (13)(24)(57)(68)\}$. Se foloseşte teorema 47 sau se compară tablele de înmulţire ale lui H şi Q.

91. (a). S_n este generat de toate transpoziţiile şi $(ij) = (1i)(1j)(1i)$. (b). $(23)(12)(23) = (13)$, $(34)(13)(34) = (14)$, etc. şi aplicăm (a). (c). $(12...n)(12)\ (12...n)^{-1} = (23)$, $(12...n)(23)(12...n)^{-1} = (34)$, etc. şi aplicăm (b).

92. Fie $\sigma \in A_n$. (a). Cf. ex. precedent, σ este un produs de un număr par de transpoziţii de forma $(1i)$ şi $(1i)(1j) = (1ji)$. (b). Cf. ex. precedent, σ este un produs de un număr par de transpoziţii de forma $(i\ i+1)$ şi $(12)(23) = (123)$, $(12)(34) = (123)(234)$, $(12)(45) = (123)(234)(345)$, etc.

93. Fie α o transpoziţie şi β un ciclul de lungime 5. Schimbând numerotarea şi luând o putere a lui β, ne reducem la cazul $\alpha = (12)$ şi $\beta = (12345)$. Se aplică ex. 91.

94. Fie H un subgrup de indice 2. Atunci $|H| = 6$. Cum A_4 nu are elemente de ordin 6, rezultă că $H \simeq S_3$, cf. ex. 51. Atunci H conţine toate cele trei elemente de ordin 2 din A_4. Deci H conţine subgrupul $\{I, (12)(34), (13)(24),$ $(14)\ (23)\}$, în contradicţie cu teorema lui Lagrange.

95. Fie H un subgrup normal diferit de $\{I\}$ şi A_5. Conform teoremei lui Cauchy, H conţine un element de ordin prim p. Deci $p = 2, 3$ sau 5. Dacă H conţine un ciclu de lungime 3, atunci $|G/H|$ nu se divide cu 3, deci H conţine toate ciclurile de lungime 3, şi rezultă că $H = A_5$, contradicţie. Cazul când H conţine un ciclu de lungime 5 se tratează similar. Putem presupune că $(12)(34) \in H$. Atunci $(123)(12)(34)(123)^{-1} = (23)(14) \in H$, deci H conţine subgrupul $\{I, (12)(34), (13)(24), (14)(23)\}$. Rezultă că $|G/H|$ nu se divide cu 2, deci H conţine toate elementele de ordin 2 din A_5. Rezultă că H constă din I şi cele 15 elemente de ordinul 2, contradicţie (G. Pollack, 1955).

96. Se foloseşte formula de conjugare a unui ciclu $\sigma(a_1, ..., a_k)\sigma^{-1} = (\sigma(a_1),$ $..., \sigma(a_k))$. Se ţine seama că ciclurile disjuncte comută iar un ciclu de lungime k se poate scrie în k moduri. Numărul permutările de tip $(k_1, k_2, ..., k_n)$ este $n!/(1^{k_1}2^{k_2} \cdots n^{k_n} k_1!k_2! \cdots k_n!)$.

97. Se foloseşte teorema 47. $H = \{I, (12)(36)(45), (13)(25)(46), (14)(26)(35),$ $(165)(243), (156)(234)\}$.

98. $Sim(B)$ constă din rotaţiile de unghi 0, $\pi/2$, π, $3\pi/2$ în jurul lui 0.

99. Fixăm o faţă a a tetraedrului. Stabilizatorul lui a, adică mulţimea $S := \{g \in G |\ g(a) = a\}$ este un subgrup al lui G cu 3 elemente. Oricare ar fi o faţă b a tetraedrului, există $g \in G$ cu $g(a) = b$. În plus, dacă $g, h \in G$, atunci $g(a) = h(a)$ dacă şi numai dacă $gh^{-1} \in S$. Deci numărul feţelor este egal cu $[G : S]$. Rezultă că $|G| = |S|[G : S] = 3 \cdot 4 = 12$.

În afară de transformarea identică, sunt $4 \cdot 2 = 8$ rotaţii cu axa trecând printr-un vârf al tetraedrului şi centrul feţei opuse, şi $3 \cdot 1 = 3$ rotaţii cu axa trecând prin mijlocul a două muchii opuse. Fiecare rotaţie permută feţele tetraedrului. Obţinem astfel un morfism injectiv $f : G \to S_4$. Prin f primele 8 rotaţii se corespund cu ciclurile de lungime 3, iar ultimele 3 rotaţii se corespund cu produsele de câte două transpoziţii disjuncte, deci imaginea lui f este A_4.

100. Adaptând raţionamentul din ex. 99 se obţine $|G| = 24$. G acţionează tranzitiv asupra celor 6 feţe ale cubului şi stabilizatorul unei feţe are ordinul 4. Deci G are $6 \cdot 4 = 24$ de elemente. În afară de transformarea identică, sunt $3 \cdot 3 = 9$ rotaţii cu axa trecând prin centrul a două feţe opuse, $4 \cdot 2 = 8$ rotaţii cu axa trecând prin două vârfuri opuse şi $6 \cdot 1 = 3$ rotaţii cu axa trecând prin mijlocul a două muchii opuse. Fiecare rotaţie permută diagonalele cubului. Obţinem astfel un morfism injectiv $G \to S_4$ care este izomorfism deoarece grupurile au 24 de elemente. Prin acest izomorfism primele 9 rotaţii se corespund cu ciclurile de lungime 4 şi produsele de câte două transpoziţii disjuncte, următoarele 8 rotaţii se corespund cu ciclurile de lungime 3, iar ultimele 6 rotaţii se corespund cu tranpoziţiile.

101. Adaptând raţionamentul din ex. 99 se obţine $|G| = 60$. În afară de transformarea identică, sunt $6 \cdot 4 = 24$ rotaţii cu axa trecând prin centrul a două feţe opuse, $10 \cdot 2 = 20$ rotaţii cu axa trecând prin două vârfuri opuse şi $15 \cdot 1 = 15$ rotaţii cu axa trecând prin mijlocul a două muchii opuse. Fiecare rotaţie permută cele 5 cuburi înscrise în dodecaedru. Obţinem astfel un morfism injectiv $G \to S_5$. Prin acest izomorfism primele 24 rotaţii, care sunt elemente de ordinul 5, se corespund cu ciclurile de lungime 5, următoarele 20 rotaţii, care sunt elemente de ordinul 3, se corespund cu ciclurile de lungime 3, iar ultimele 15 rotaţii se corespund cu produsele de câte două transpoziţii disjuncte.

102. Presupunem că $G/Z(G) =< \hat{x} >$ şi fie $y, z \in G$. Putem scrie $y = ax^m$ şi $z = bx^n$ cu $a, b \in Z(G)$ şi m, n întregi. Atunci $yz = ax^m bx^n = abx^{m+n} = bx^n ax^m = zy$.

Fie G un grup cu p^2 elemente neabelian. Cum $|Z(G)|$ divide $|G| = p^2$ rezultă că $|Z(G)| = 1$ (cf. primei părţi, $|G/Z(G)| \neq p$). Fie $|G| = |Z(G)| + [G : C(x_1)] + \cdots + [G : C(x_n)]$ ecuaţia claselor lui G. Cum p divide $|G|$ şi fiecare termen $[G : C(x_i)]$, rezultă că p divide $|Z(G)|$, contradicţie.