Curs VII
ELEMENTE DE TEORIA GRUPURILOR

§ 5. SUBGRUPURI NORMALE

Definiţia 5.1. Un subgrup N al unui grup G se spune că este subgrup *normal* dacă oricare ar fi $x \in G$ şi $h \in N$, avem $xhx^{-1} \in N$.

Notaţie. $N \lhd G$

Observaţie. Pentru un grup G şi $x \in G$ am definit automorfismul interior $\varphi_x : G \to G$, $\varphi_x(g) = xgx^{-1}$. Din definiţie rezultă că un subgrup N al lui G este subgrup normal dacă şi numai dacă $\varphi_x(N) \subseteq N$, oricare ar fi $x \in G$.

Propoziţia 5.2. Dacă N este un subgrup al grupului G, afirmaţiile următoare sunt echivalente:

1) N este subgrup normal;
2) Relaţiile de congruenţă modulo N, adică R_N^s şi R_N^d coincid;
3) $xN = Nx$, oricare ar fi $x \in G$;
4) $G / R_N^s = G / R_N^d$.

Demonstraţie. 1) $\Rightarrow$ 2) Dacă $x \; R_N^s \; y$, atunci $x^{-1}y \in N$. Fie $h = x^{-1}y \in N$. Atunci $xh = y$. Dar cum N este subgrup normal, avem $xhx^{-1} \in N$, adică $yx^{-1} \in N$, deci şi $(yx^{-1})^{-1} = xy^{-1} \in N$, adică $x \; R_N^d \; y$.

Analog se demonstrează că dacă $x \; R_N^d \; y$, atunci $x \; R_N^s \; y$, deci relaţiile R_N^s şi R_N^d coincid.

2) $\Rightarrow$ 3) Dacă $y \in xN$, atunci $y = xh$ cu $h \in N$, deci $x^{-1}y = h \in N$, adică $x \; R_N^s \; y$. Deci $x \; R_N^d \; y$, adică $yx^{-1} \in N$ sau $yx^{-1} = h' \in N$, de unde $y = h'x \in Nx$; deci $xN \subseteq Nx$. Analog se demonstrează că $Nx \subseteq xN$.

3) $\Rightarrow$ 4) Evident.

4) $\Rightarrow$ 3) Fie $x \in G$. Avem $xN \in G / R_N^s$ şi cum $G / R_N^s = G / R_N^d$ rezultă că există $y \in G$ cu proprietatea că $xN = Ny$. Dar $x \in xN$, deci $x \in Ny \Rightarrow x \; R_N^d \; y \Rightarrow Ny = Nx$, deci $xN = Nx$.

3) $\Rightarrow$ 2) Fie $x, y \in G$ cu $x \; R_N^s \; y$. Atunci $xN = yN$ şi cum $xN = Nx$ şi $yN = Ny$ rezultă că $Nx = Ny$, de unde $x \; R_N^d \; y$. Reciproc se arată la fel.

3) $\Rightarrow$ 1) Dacă $x \in G$ şi $h \in N$, atunci $xh \in xN = Nx$ şi deci $xh = h'x$ cu $h' \in N$, de unde $xhx^{-1} = h' \in N$, adică N este subgrup normal.

Exemple.
1) G şi $\{e\}$ sunt subgrupuri normale ale grupului G.
2) Dacă G este un grup abelian, este clar că orice subgrup al său este normal.

3) Orice subgrup de indice 2 al unui grup oarecare G este normal.

Într-adevăr, dacă H este subgrup al lui G astfel încât [G : H] = 2, atunci

$$G/R_H^s = \{H, G \setminus H\} \text{ şi } G/R_H^d = \{H, G \setminus H\}.$$

Deci $G/R_H^s = G/R_H^d$.

4) Fie grupul $\mathbf{S}_3$ al permutărilor de 3 elemente şi permutarea $\tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$.

Submulţimea H = {e, τ} este un subgrup al lui $\mathbf{S}_3$ care nu este normal. Într-adevăr, dacă

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}, \text{ atunci } \sigma\tau\sigma^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} \notin H.$$

(Această afirmaţie rezultă şi din paragraful precedent, unde am arătat că mulţimile factor la stânga şi la dreapta ale lui $\mathbf{S}_3$ în raport cu H sunt diferite.)

Propoziţia 5.3. Fie f : G → G' un morfism de grupuri. Avem:

1) Dacă N este subgrup normal al lui G, iar f este surjectiv, atunci f(N) este subgrup normal al lui G'.

2) Dacă N' este subgrup normal al lui G', atunci $f^{-1}(N')$ este subgrup normal al lui G. În particular, Ker f este subgrup normal al lui G.

Demonstraţie. 1) Fie g' ∈ G' şi h ∈ N. Vrem să arătăm că $g'f(h)(g')^{-1} \in f(N)$. Deoarece f este surjectivă există g ∈ G astfel încât f(g) = g'. Atunci $g'f(h)(g')^{-1} = f(g)f(h)f(g)^{-1} = f(ghg^{-1}) \in f(N)$, deoarece N este subgrup normal.

2) Fie g ∈ G şi $h \in f^{-1}(N')$. Vrem să arătăm că $ghg^{-1} \in f^{-1}(N')$, adică $f(ghg^{-1}) \in N'$. Dar f(h) ∈ N' şi cum N' este normal în G' rezultă că $f(g)f(h)f(g)^{-1} \in N'$, adică $f(ghg^{-1}) \in N'$.

Exerciţiu. Daţi un exemplu de subgrup normal a cărui imagine printr-un morfism de grupuri să nu fie subgrup normal.

Teorema 5.4. (Teorema de corespondenţă pentru subgrupuri normale) Fie f : G → G' un morfism *surjectiv* de grupuri. Există o corespondenţă bijectivă între mulţimea subgrupurilor normale ale lui G care conţin Ker f şi mulţimea tuturor subgrupurilor normale ale lui G', dată prin N → f(N).

Demonstraţie. Corespondenţa N → f(N) este corect definită după cum rezultă din propoziţia 5.3. Restul este la fel ca în demonstraţia teoremei 2.6 din cursul 5.

§ 6. GRUP FACTOR

Fie G un grup şi N un subgrup normal al său. După cum rezultă din cele de mai înainte, relaţiile de congruenţă R_N^s şi R_N^d (la stânga şi la dreapta modulo N) coincid. În acest caz vom spune, pe scurt, congruenţa modulo N, iar dacă x, y ∈ G, faptul că x este congruent cu y modulo N îl vom scrie $x \equiv y$ (mod N). Cele două mulţimi factor G / R_N^s şi G / R_N^d coincid, mulţimea factor fiind notată cu G/N.

Propoziţia 6.1. Dacă G este un grup şi N un subgrup normal al său, atunci pe mulţimea factor G/N se poate defini o operaţie algebrică împreună cu care G/N devine grup, iar funcţia surjectivă $p: G \to G/N$, $p(x) = [x]$ este morfism de grupuri cu Ker p = N.

Demonstraţie. Dacă $x, y \in G$, definim

$$[x][y] = [xy].$$

Să arătăm că în acest mod se defineşte o operaţie algebrică pe G/N, împreună cu care G/N devine grup.

Să demonstrăm mai întâi că operaţia este bine definită, adică nu depinde de alegerea reprezentanţilor. Într-adevăr, dacă $[x] = [x']$ şi $[y] = [y']$, atunci avem $x^{-1}x' \in N$ şi $y^{-1}y' \in N$, adică există $h_1, h_2 \in N$ astfel încât $x^{-1}x' = h_1$ şi $y^{-1}y' = h_2$, adică $x' = xh_1$ şi $y' = yh_2$. Deci $x'y' = (xh_1)(yh_2) = x(h_1y)h_2$. Dar cum N este subgrup normal, există $h_3 \in N$ astfel încât $h_1y = yh_3$ (deoarece Ny = yN), de unde se obţine $x'y' = x(yh_3)h_2 = (xy)(h_3h_2)$, iar $h_3h_2 \in N$. Deci $(xy)^{-1}(x'y') = h_3h_2 \in N$, adică xy este congruent modulo N cu x'y', de unde $[xy] = [x'y']$. Deci operaţia algebrică este bine definită.

Operaţia este asociativă, deoarece dacă $[x], [y], [z] \in G/N$, atunci

$$[x]([y][z]) = [x][yz] = [x(yz)] = [(xy)z] = [xy][z] = ([x][y])[z].$$

Operaţia admite ca element neutru $[e] \in G/N$ (unde e este elementul neutru din G), deoarece oricare ar fi $[x] \in G/N$ avem, în mod evident,

$$[x][e] = [e][x] = [x].$$

Orice element $[x] \in G/N$ are un invers care este $[x^{-1}] \in G/N$, deoarece

$$[x][x^{-1}] = [xx^{-1}] = [e] \text{ şi } [x^{-1}][x] = [x^{-1}x] = [e].$$

Astfel am demonstrat că G/N este un grup.

Funcţia surjectivă $p: G \to G/N$, unde $p(x) = [x]$, este un morfism de grupuri. Într-adevăr,

$$p(xy) = [xy] = [x][y] = p(x)p(y).$$

Arătăm acum că Ker p = N. Dacă $x \in$ Ker p, atunci $p(x) = [e]$, deci $[x] = [e]$, de unde $x \equiv e$ (mod N) sau $xe^{-1} \in N$, adică $x \in N$. Reciproc, dacă $x \in N$, atunci $x \equiv e$ (mod N), adică $[x] = [e]$, de unde $p(x) = [x] = [e]$ şi deci $x \in$ Ker p.

Definiţia 6.2. Grupul G/N construit în propoziţia precedentă se numeşte *grupul factor (cât)* al lui G în raport cu subgrupul normal N. Morfismul $p: G \to G/N$, $p(x) = [x]$ se numeşte *proiecţia* (*surjecţia*) *canonică* a lui G pe grupul factor G/N.

Observaţii.

1) Dacă G este un grup comutativ, atunci orice subgrup al său este normal şi deci putem vorbi de grupul factor al lui G în raport cu orice subgrup al său. Mai mult, dacă G este comutativ, orice grup factor al său este comutativ.

2) Proiecţia canonică $p: G \to G/\{e\}$ este izomorfism de grupuri.

Exemplu. Să determinăm grupurile factor ale grupului aditiv (**Z**, +).

Fie $H \subseteq \mathbf{Z}$ un subgrup al lui **Z**. Atunci $H = n\mathbf{Z}$, unde $n \geq 0$.

Dacă $n = 0$, adică $H = \{0\}$, avem $\mathbf{Z}/\{0\} \cong \mathbf{Z}$.

Dacă $n \geq 1$, atunci pentru $x, y \in \mathbf{Z}$, avem $x \equiv y \pmod{n\mathbf{Z}}$ dacă şi numai dacă $x - y \in n\mathbf{Z}$, dacă şi numai dacă $n \mid x - y$, dacă şi numai dacă $x \equiv y \pmod{n}$. Aşadar, relaţia de echivalenţă pe **Z** modulo subgrupul $n\mathbf{Z}$ coincide cu relaţia de congruenţă modulo n. Mai mult, operaţia algebrică pe grupul factor $\mathbf{Z}/n\mathbf{Z}$ coincide cu adunarea claselor de resturi modulo n. Deci grupul factor ($\mathbf{Z}/n\mathbf{Z}$, +) al lui **Z** în raport cu subgrupul $n\mathbf{Z}$ este izomorf cu grupul aditiv al claselor de resturi modulo n, adică $\mathbf{Z}/n\mathbf{Z} \cong \mathbf{Z}_n$.

Din teorema de corespondenţă pentru subgrupuri (normale) obţinem:

Propoziţia 6.3. Fie G un grup şi N un subgrup normal al lui G. Există o corespondenţă bijectivă între mulţimea subgrupurilor (normale) ale lui G care conţin pe N şi mulţimea tuturor subgrupurilor (normale) ale lui G/N, dată prin $H \to H/N$.

Exemplu. Să determinăm subgrupurile grupului factor ($\mathbf{Z}/n\mathbf{Z}$, +), unde $n \geq 2$.

Fie $K \subseteq \mathbf{Z}/n\mathbf{Z}$ un subgrup al lui $\mathbf{Z}/n\mathbf{Z}$. Atunci $K = H/n\mathbf{Z}$, unde H este un subgrup al lui **Z** care-l conţine pe $n\mathbf{Z}$. Ţinând seama de forma subgrupurilor lui **Z** deducem că există un $d \in \mathbf{N}$ astfel ca $H = d\mathbf{Z}$. Dar $n\mathbf{Z} \subseteq H$ dacă şi numai dacă $n\mathbf{Z} \subseteq d\mathbf{Z}$ dacă şi numai dacă $d \mid n$. În concluzie, $K = d\mathbf{Z}/n\mathbf{Z}$ cu $d \mid n$. (Dacă ţinem cont de izomorfismul dintre $\mathbf{Z}/n\mathbf{Z}$ şi $\mathbf{Z}_n$ putem scrie $K = [d]\mathbf{Z}_n$ cu $d \mid n$.)

În particular, grupul ($\mathbf{Z}_6$, +) are 4 subgrupuri şi anume: $\langle[0]\rangle = \{[0]\}$; $\langle[1]\rangle = \mathbf{Z}_6$; $\langle[2]\rangle = \{[0], [2], [4]\}$; $\langle[3]\rangle = \{[0], [3]\}$.

Teorema 6.4. (Proprietatea de universalitate a grupurilor factor) Fie $f : G \to G'$ un morfism de grupuri şi N un subgrup normal al lui G. Dacă $N \subseteq \operatorname{Ker} f$, atunci există un morfism de grupuri $\overline{f} : G/N \to G'$ unic cu proprietatea că $\overline{f} \circ p = f$, unde $p : G \to G/N$ este proiecţia canonică. Mai mult:

1) $\overline{f}$ este injectiv $\Leftrightarrow N = \operatorname{Ker} f$;
2) $\overline{f}$ este surjectiv $\Leftrightarrow$ f este surjectiv.

Am observat mai înainte că dacă $f : G \to G'$ este un morfism de grupuri, atunci nucleul său, Ker f, este subgrup normal al lui G şi deci putem vorbi de grupul factor G/Ker f. De asemenea, am arătat că Im f este un subgrup al lui G'.

Teorema 6.5. (Teorema fundamentală de izomorfism pentru grupuri) Fie $f : G \to G'$ un morfism de grupuri. Atunci există un izomorfism de grupuri

$$\overline{f} : G/\operatorname{Ker} f \to \operatorname{Im} f.$$

Demonstraţie. Definim $\overline{f} : G/\operatorname{Ker} f \to \operatorname{Im} f$, prin $\overline{f}([x]) = f(x)$.

Funcţia $\overline{f}$ este bine definită, adică nu depinde de alegerea reprezentanţilor. Într-adevăr, dacă [x] = [y], rezultă $x^{-1}y \in \mathrm{Ker}\, f$, adică $f(x^{-1}y) = e'$. Dar $f(x^{-1}y) = f(x^{-1})f(y) = (f(x))^{-1}f(y)$, de unde $(f(x))^{-1}f(y) = e'$, adică $f(x) = f(y)$ şi deci $\overline{f}([x]) = \overline{f}([y])$.

Faptul că $\overline{f}$ este surjectivă este clar, deoarece orice element din Im f se scrie sub forma f(x), cu $x \in G$, iar $\overline{f}([x]) = f(x)$.

Să demonstrăm injectivitatea funcţiei $\overline{f}$. Într-adevăr, dacă $\overline{f}([x]) = \overline{f}([y])$, atunci $f(x) = f(y)$ şi deci $(f(x))^{-1}f(y) = e'$, adică $f(x^{-1}y) = e'$, de unde $x^{-1}y \in \mathrm{Ker}\, f$, ceea ce înseamnă că [x] = [y].

Ţinând seama că f este morfism de grupuri, rezultă

$$\overline{f}([x][y]) = \overline{f}([xy]) = f(xy) = f(x)f(y) = \overline{f}([x])\ \overline{f}([y]),$$

adică $\overline{f}$ este morfism de grupuri.

Deci $\overline{f}$ este un izomorfism de grupuri.

Observaţie. Existenţa unui (izo)morfism de grupuri $\overline{f} : G/\mathrm{Ker}\, f \to \mathrm{Im}\, f$ se poate arăta folosind proprietatea de universalitate a grupurilor factor astfel: fie $f' : G \to \mathrm{Im}\, f$ corestricţia lui f la Im f. Deoarece Ker f' = Ker f, din proprietatea de universalitate a grupurilor factor există un morfism de grupuri $\overline{f} : G/\mathrm{Ker}\, f \to \mathrm{Im}\, f$ unic cu proprietatea că $\overline{f} \circ p = f'$, unde $p : G \to G/\mathrm{Ker}\, f$ este proiecţia canonică. Cum f' este surjectiv, rezultă că $\overline{f}$ este izomorfism.

Exemple.

Fie $\mathbf{R}^*_+$ grupul multiplicativ al numerelor reale strict pozitive, $\mathbf{C}^*$ grupul multiplicativ al numerelor complexe nenule, iar S subgrupul numerelor complexe de modul 1. Atunci:

1) Grupul factor $\mathbf{C}^*/S$ este izomorf cu $\mathbf{R}^*_+$.

Într-adevăr, fie $\varphi : \mathbf{C}^* \to \mathbf{R}^*_+$ definită prin $\varphi(z) = |z|$. Avem că φ este morfism surjectiv de grupuri, adică $\mathrm{Im}\, \varphi = \mathbf{R}^*_+$ şi $\mathrm{Ker}\, \varphi = S$. Din teorema fundamentală de izomorfism pentru grupuri rezultă că $\mathbf{C}^*/S \cong \mathbf{R}^*_+$.

2) Grupul factor $\mathbf{C}^*/\mathbf{R}^*_+$ este izomorf cu S.

Fie $\psi : \mathbf{C}^* \to \mathbf{C}^*$ definită prin $\psi(z) = z/|z|$. Avem că ψ este morfism de grupuri, $\mathrm{Ker}\, \psi = \mathbf{R}^*_+$ şi $\mathrm{Im}\, \psi = S$. Din teorema precedentă rezultă că $\mathbf{C}^*/\mathbf{R}^*_+ \cong S$.

3) Grupurile factor ale lui $\mathbf{Z}/n\mathbf{Z}$.

Fie $K = d\mathbf{Z}/n\mathbf{Z}$, $d \mid n$, un subgrup al lui $\mathbf{Z}/n\mathbf{Z}$. Din proprietatea de universalitate a grupurilor factor deducem că există un morfism surjectiv de grupuri $f : \mathbf{Z}/n\mathbf{Z} \to \mathbf{Z}/d\mathbf{Z}$. Ţinând seama de modul în care se defineşte f rezultă că $\mathrm{Ker}\, f = d\mathbf{Z}/n\mathbf{Z}$. Atunci, din teorema fundamentală de izomorfism pentru grupuri, obţinem că grupul factor $(\mathbf{Z}/n\mathbf{Z})/K$ este izomorf cu $\mathbf{Z}/d\mathbf{Z}$. (Dacă ţinem cont de izomorfismul dintre $\mathbf{Z}/n\mathbf{Z}$ şi $\mathbf{Z}_n$ putem scrie astfel: $\mathbf{Z}_n/[d]\mathbf{Z}_n \cong \mathbf{Z}_d$.)

Mai rezultă că $|d\mathbf{Z}/n\mathbf{Z}| = n/d$.

Exerciţiu. Fie G_1, G_2 două grupuri şi H_1, respectiv H_2 subgrupuri normale. Arătaţi că $H_1 \times H_2$ este subgrup normal al lui $G_1 \times G_2$. Mai mult, avem că

$$(G_1 \times G_2)/(H_1 \times H_2) \cong G_1/H_1 \times G_2/H_2.$$

(Generalizaţi la un produs arbitrar de grupuri.)

Din teorema fundamentală de izomorfism pentru grupuri se obţin încă două teoreme de izomorfism foarte utile.

Teorema 6.6. (A doua teoremă de izomorfism pentru grupuri) Fie G un grup şi H, K subgrupuri ale lui G. Dacă K este subgrup normal, atunci HK este un subgrup al lui G, $H \cap K$ este subgrup normal al lui H şi $HK/K \cong H/H \cap K$.

Demonstraţie. Se consideră morfismul $f : H \to HK/K$ definit prin $f(h) = hK$, se observă că f este surjectiv şi $\mathrm{Ker}\, f = H \cap K$ iar apoi se aplică teorema fundamentală de izomorfism pentru grupuri.

Teorema 6.7. (A treia teoremă de izomorfism pentru grupuri) Fie G un grup şi H, K subgrupuri normale ale lui G cu $H \le K$. Atunci K/H este subgrup normal al lui G/H şi $(G/H)/(K/H) \cong G/K$.

Demonstraţie. Se consideră morfismul $f : G/H \to G/K$ definit prin $f(xH) = xK$, se observă că f este surjectiv şi $\mathrm{Ker}\, f = K/H$ iar apoi se aplică teorema fundamentală de izomorfism pentru grupuri.

§ 7. GRUPURI CICLICE

Am observat anterior că grupurile aditive $\mathbf{Z}$ şi $\mathbf{Z}_n$, $n \ge 1$, sunt ciclice. Următoarea teoremă arată că acestea sunt singurele tipuri de grupuri ciclice.

Teorema 7.1. (Teorema de structură a grupurilor ciclice) Orice grup ciclic G este izomorf fie cu grupul $\mathbf{Z}$ al numerelor întregi, fie cu un anumit grup $\mathbf{Z}_n$, $n \ge 1$, de clase de resturi modulo n.

Demonstraţie. Dacă $G = \langle a \rangle$, considerăm funcţia $\varphi: \mathbf{Z} \to G$, $\varphi(n) = a^n$, definită mai înainte. Avem

$$\varphi(m + n) = a^{m+n} = a^m a^n = \varphi(m)\varphi(n)$$

şi deci φ este morfism de grupuri. Mai mult, φ este evident morfism surjectiv, deci $\mathrm{Im}\, \varphi = G$. Considerând nucleul lui φ, $\mathrm{Ker}\, \varphi$, distingem două cazuri:

1) $\mathrm{Ker}\, \varphi = \{0\}$;
2) $\mathrm{Ker}\, \varphi \ne \{0\}$.

În primul caz, conform teoremei fundamentale de izomorfism, avem

$$\mathbf{Z}/\{0\} \cong \mathrm{Im}\, \varphi, \text{ adică } \mathbf{Z} \cong G;$$

În cazul al doilea, $\mathrm{Ker}\, \varphi$ este de forma $n\mathbf{Z}$ cu $n \ge 1$ un număr întreg şi deci

$$\mathbf{Z}/n\mathbf{Z} \cong \mathrm{Im}\, \varphi, \text{ adică } \mathbf{Z}_n \cong G.$$

Observaţie. Din teorema de mai sus rezultă că dacă G este un grup ciclic şi $a \in G$ un generator al său, atunci:

1) Dacă *a* este de ordin infinit, atunci G este izomorf cu grupul aditiv **Z** al numerelor întregi.

2) Dacă *a* este de ordin n (finit), atunci G este izomorf cu grupul aditiv $\mathbf{Z}_n$ al claselor de resturi modulo n.

Propoziţia 7.2. Orice subgrup şi orice grup factor al unui grup ciclic este ciclic.

Demonstraţie. Dacă G = <a> este un grup ciclic, iar H un subgrup al său, atunci grupul factor G/H este ciclic generat de [a], clasa lui a modulo H, adică G/H = <[a]>.

Să arătăm acum că orice subgrup al unui grup ciclic este ciclic. Într-adevăr, dacă G este izomorf cu **Z**, am arătat că subgrupurile lui **Z** sunt de forma n**Z**, adică sunt ciclice; deci şi subgrupurile lui G sunt ciclice. Dacă G este izomorf cu $\mathbf{Z}_n$, am arătat că subgrupurile lui $\mathbf{Z}_n$ sunt de forma $[d]\mathbf{Z}_n$, cu d | n, adică sunt ciclice; deci şi subgrupurile lui G sunt ciclice.

Observaţie. Dacă G = <a> este un grup ciclic de ordin n, izomorfismul dintre G şi grupul aditiv $\mathbf{Z}_n$ este dat de funcţia $\varphi : \mathbf{Z}_n \to G$, definită prin $\varphi([k]) = a^k$. Aşadar, având în vedere caracterizarea generatorilor grupului aditiv $\mathbf{Z}_n$ dată în secţiunea 2, avem că elementul a^k este generator al lui G dacă şi numai dacă k este prim cu n.

Fie acum $n \geq 1$ un număr natural şi U_n grupul multiplicativ al rădăcinilor de ordinul n ale unităţii, adică

$$U_n = \{z \in \mathbf{C} \mid z^n = 1\}.$$

Avem că $U_n = \{\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_{n-1}\}$, unde

$$\varepsilon_k = \cos(2k\pi/n) + i\sin(2k\pi/n),\ \ 0 \leq k \leq n-1.$$

Din formula lui Moivre avem că $\varepsilon_k = \varepsilon_1^k$ şi deci U_n este grup ciclic de ordinul n, un generator al său fiind ε_1.

Definiţia 7.3. Un generator al grupului U_n se numeşte *rădăcină primitivă de ordinul n a unităţii*.

Conform celor de mai înainte rezultă că ε_k este rădăcină primitivă de ordinul n a unităţii dacă şi numai dacă k este relativ prim cu n.

Exerciţiu. Arătaţi că grupurile (**Q**, +), (**R**, +) şi (**C**, **+)** nu sunt ciclice.