

Seminar 5

Subgrupuri

(G, \cdot) grup, $H \subseteq G$ submultime

$$H \leq G \text{ (subgrup)} \Leftrightarrow \begin{cases} a) 1 \in H \\ b) x, y \in H \Rightarrow xy \in H \\ c) x \in H \Rightarrow x^{-1} \in H \end{cases}$$

Obs. Condiția $1 \in H$ poate fi înlocuită cu $H \neq \emptyset$.

Într-adevăr dacă $1 \in H$ atunci $H \neq \emptyset$.

Reciproc dacă $H \neq \emptyset$ atunci $\exists x \in H$ și din condiția

c) de mai sus $x^{-1} \in H$. Atunci condiția b) aplicată pt.

x și x^{-1} ne spune că $1 = x \cdot x^{-1} \in H$.

Teoremă: Intersecția unei mulțimi de subgrupuri este subgrup.

Def. Subgrupul generat de o submultime $X \subseteq G$:

$$\langle X \rangle = \bigcap_{\substack{H \leq G \\ X \subseteq H}} H$$

Teoremă $\langle X \rangle = \{x_1^{\epsilon_1} x_2^{\epsilon_2} \dots x_n^{\epsilon_n} \mid n \in \mathbb{N}, x_i \in X, \epsilon_i = \pm 1\}$

Obs. Dacă $X = \emptyset$ atunci $\langle \emptyset \rangle = \{1\}$ (produsul fără factori este prin convenție elementul neutru).

1. Să se verifice dacă următoarele submultimi sunt subgrupuri în grupurile respective:

a) $S = \{a + ai \mid a \in \mathbb{R}\}$ în $(\mathbb{C}, +)$.

b) $T = \{a + ai \mid a \in \mathbb{R}^*\}$ în (\mathbb{C}^*, \cdot)

c) $n \in \mathbb{N}^*$ $H_n = \{\frac{a}{b} \in \mathbb{Q} \mid (a,b) = 1 \text{ și } b \mid n\}$ în $(\mathbb{Q}, +)$

d) $n \in \mathbb{N}^*$ $K_n = \{\frac{a}{b} \in \mathbb{Q}^* \mid (a,b) = 1 \text{ și } b \mid n\}$ în (\mathbb{Q}^*, \cdot)

e) $n \in \mathbb{N}^*$ $L_n = \{\frac{a}{b} \in \mathbb{Q} \mid (a,b) = 1 \text{ și } (b,n) = 1\}$ în $(\mathbb{Q}, +)$

f) $n \in \mathbb{N}^*$ $M_n = \{\frac{a}{b} \in \mathbb{Q}^* \mid (a,b) = 1 \text{ și } (b,n) = 1\}$ în (\mathbb{Q}^*, \cdot)

g) $L = \{a \in \mathbb{R}^* \mid a^2 \in \mathbb{Q}\}$ în (\mathbb{R}^*, \cdot)

h) $U = \{a \in \mathbb{R} \mid a^2 \in \mathbb{Q}\}$ în $(\mathbb{R}, +)$.

Soluție a) $0 = 0 + 0 \cdot i \in S$

Fie $x, y \in S \Rightarrow \exists a, b \in \mathbb{R} : x = a + ai, y = b + bi$.

Atunci $x - y = a + ai - (b + bi) = (a - b) + (a - b)i \in S$ pt. că $a - b \in \mathbb{R}$.

Deci $S \leq \mathbb{C}$.

b) $1 = 1 + 0i \notin T \Rightarrow T \not\subseteq \mathbb{C}^*$ (nu conține elementul neutru)

c) Observăm că $H_n = \{x \in \mathbb{Q} \mid \exists a, b \in \mathbb{Z}, b \neq 0 \text{ și } x = \frac{a}{b}\}$

Introducând incluziunea „ \subseteq ” este imediată prin definiția lui H_n .
„ \supseteq ”: Dacă $x = \frac{a}{b}$ cu $a, b \in \mathbb{Z}, b \neq 0$ atunci fie $d = (a, b)$ și
 $a = a'd, b = b'd$ cu $a', b' \in \mathbb{Z}$. Avem $x = \frac{a'd}{b'd} = \frac{a'}{b'}$ cu $(a', b') \neq 1$
și $b' \mid b$ deci $b' \neq 0$. Astfel $x = \frac{a'}{b'} \in H_n$.

Acum este ușor să arătăm că $H_n \leq \mathbb{Q}$:

• $0 = \frac{0}{1} \in H_n$

• fie $x, y \in H_n \Rightarrow x = \frac{a}{b}, y = \frac{c}{d}$ cu $a, b, c, d \in \mathbb{Z}, b \neq 0$ și $d \neq 0$.
Notăm $m = [b, d]$ și avem $m = bk = dq$, iar $m \neq 0$. Atunci

$$x - y = \frac{a}{b} - \frac{c}{d} = \frac{ak}{bk} - \frac{cq}{dq} = \frac{ak}{m} - \frac{cq}{m} = \frac{ak - cq}{m} \in H_n.$$

d) $\frac{1}{n} \in K_n$ dar $\frac{1}{n} \cdot \frac{1}{n} = \frac{1}{n^2} \notin K_n$ deci $K_n \not\subseteq \mathbb{Q}^*$

e) Ca și în cazul lui H_n arătăm că

$$L_n = \{x \in \mathbb{Q} \mid \exists a, b \in \mathbb{Z} \quad (b, n) = 1 \text{ și } x = \frac{a}{b}\}$$

Atunci • $0 = \frac{0}{1} \in L_n$

• $x, y \in L_n \Rightarrow x = \frac{a}{b}, y = \frac{c}{d}$ cu $a, b, c, d \in \mathbb{Z}, (b, n) = (d, n) = 1$

$$\text{Avem } x - y = \frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd} \in L_n \text{ pt. că } (bd, n) = 1.$$

Deci $L_n \leq \mathbb{Q}$.

f) La fel ca în cazul e) se arată că $M_n \leq \mathbb{Q}^*$

g) Avem $1^2 = 1 \in \mathbb{Q}$ deci $1 \in L$

Dacă $a, b \in L$ atunci $a^2 \in \mathbb{Q}, b^2 \in \mathbb{Q}, a, b \neq 0$ deci $b \in \mathbb{R}$ și $(\frac{a}{b})^2 = \frac{a^2}{b^2} \in \mathbb{Q}$

Deci $a \cdot b^{-1} \in L$ pt. că $(a \cdot b^{-1})^2 = \frac{a^2}{b^2} \in \mathbb{Q}$ deci $L \leq \mathbb{R}^*$

h) $1, \sqrt{2} \in U$ pt. că $1^2 = 1 \in \mathbb{Q}$ și $(\sqrt{2})^2 = 2 \in \mathbb{Q}$. Dar

$(1 + \sqrt{2})^2 = 3 + 2\sqrt{2} \notin \mathbb{Q}$ deci $1 + \sqrt{2} \notin U$ și $U \not\subseteq \mathbb{R}$ (nu este parte stabilă)

Ob1. Cum justificăm că $3+2\sqrt{2} \notin \mathbb{Q}$?

Mai întâi arătăm că $\sqrt{2} \notin \mathbb{Q}$. Iată-adevar dacă presupunem $\sqrt{2} \in \mathbb{Q}$ atunci $\sqrt{2}$ se poate scrie ca o fracție ireductibilă deci

$$\sqrt{2} = \frac{a}{b} \text{ cu } a, b \in \mathbb{Z}, b \neq 0 \text{ și } (a, b) = 1.$$

Atunci $2 = \frac{a^2}{b^2}$ deci $2b^2 = a^2$ ceea ce implică faptul că a^2 este

par. Atunci a este par, deci $a = 2a'$, $a' \in \mathbb{Z} \Rightarrow a^2 = 4a'^2$

Atunci $2b^2 = 4a'^2 \Rightarrow b^2 = 2a'^2$ și b este de asemenea par,

ceea ce contrazice condiția ca $\frac{a}{b}$ să fie ireductibilă. Deci $\sqrt{2} \notin \mathbb{Q}$.

Acum dacă am presupune $3+2\sqrt{2} = q \in \mathbb{Q}$ atunci am avea

$$\sqrt{2} = \frac{q-3}{2} \in \mathbb{Q} \text{ ceea ce este fals. Deci } 3+2\sqrt{2} \notin \mathbb{Q}.$$

2. Verificați dacă următoarele submulțimi sunt subgrupuri:

a) $\{1, r^2, s, sr^2\}$ în D_4

b) $\{1, r, s, sr\}$ în D_4

c) $\{1, r^2, sr, sr^2\}$ în D_4

d) $\{1, -1, i, -i\}$ în \mathbb{Q} (grupul quaternionilor)

e) $\{1, i, j, k\}$ în \mathbb{Q} .

Soluție. a)

	1	r^2	s	sr^2
1	1	r^2	s	sr^2
r^2	r^2	1	sr^2	s
s	s	sr^2	1	r^2
sr^2	sr^2	s	r^2	1

grup izomorf cu grupul lui Klein

Deci $\{1, r^2, s, sr^2\}$ este subgrup.

b) $rs = sr^3 \notin \{1, r, s, sr\}$ deci nu este parte stabilă \Rightarrow nu este subgrup.

c), d) sunt subgrupuri (analog cu a))

e) $ji = -k \notin \{1, i, j, k\} \Rightarrow$ nu este subgrup.

3. a) Demonstrați că orice parte stabilă, nevidă și finită a unui grup (G, \cdot) este un subgrup al lui G .

b) Rămâne concluzia adevărată dacă renunțăm la ipoteza de finitudine?

Soluție a) Fie $\emptyset \neq H \subseteq G$ o parte stabilă finită. Cum $H \neq \emptyset$, există $x \in H$. Considerăm mulțimea puterilor $\{x^n \mid n \in \mathbb{N}^+\}$. Deoarece H este parte stabilă avem $\{x^n \mid n \in \mathbb{N}^+\} \subseteq H$. Dar H este finită deci $\exists k, m \in \mathbb{N}^+$, $k \neq m$ astfel încât $x^k = x^m$ (altfel, toate puterile pozitive ale lui x ar fi diferite și mulțimea acestor puteri ar fi infinită). Fără a restricționa generalitatea putem presupune că $k < m$. Obținem: $x^{m-k} = 1$ și $m-k \in \mathbb{N}^+$.

Cum H este parte stabilă rezultă că $1 = x^{m-k} \in H$.

Dacă $m-k=1$ atunci $x=1$ deci $x^{-1} \in H$

Dacă $m-k > 1$ atunci $1 = x^{m-k} = x \cdot x^{m-k-1} = x^{m-k-1} \cdot x$ deci

$x^{-1} = x^{m-k-1} \in H$ pt. că $m-k-1 \in \mathbb{N}^+$ și H este parte stabilă.

Priu în mare H este parte stabilă (din ipoteză) și am arădat că

$1 \in H$ și dacă $x \in H$ atunci $x^{-1} \in H$, deci H este subgrup.

b) Concluzia nu mai rămâne adeverată. Contrexemplu \mathbb{N} este parte stabilă, evidentă în $(\mathbb{Z}, +)$ dar nu este subgrup.

4. a) Arătați că $SL_3(\mathbb{Z}_3) = \{A \in M_3(\mathbb{Z}_3) \mid \det(A) = \hat{1}\} \subseteq GL_3(\mathbb{Z}_3)$

b) Determinați $\langle \begin{pmatrix} \hat{0} & -\hat{1} \\ \hat{1} & \hat{0} \end{pmatrix}, \begin{pmatrix} \hat{1} & \hat{1} \\ \hat{1} & -\hat{1} \end{pmatrix} \rangle$ în $SL_3(\mathbb{Z}_3)$ și arătați că este un grup izomorf cu grupul quaternionilor.

Soluție. a) $I_2 = \begin{pmatrix} \hat{1} & \hat{0} \\ \hat{0} & \hat{1} \end{pmatrix} \in SL_3(\mathbb{Z}_3)$ pt. că $\det(I_2) = \hat{1}$

Dacă $A, B \in SL_3(\mathbb{Z}_3)$ atunci $\det(A) = \det(B) = \hat{1} \neq \hat{0}$

deci $B \in GL_3(\mathbb{Z}_3)$ adică $\exists B^{-1} \in GL_3(\mathbb{Z}_3)$ și avem

$$\det(A \cdot B^{-1}) = \det(A) \cdot \det(B^{-1}) = \det(A) \cdot \det(B)^{-1} = 1 \cdot 1^{-1} = 1$$

Asadar $A \cdot B^{-1} \in SL_3(\mathbb{Z}_3)$ ceea ce arată că $SL_3(\mathbb{Z}_3) \subseteq GL_3(\mathbb{Z}_3)$

b) Notăm $I = \begin{pmatrix} \hat{0} & -\hat{1} \\ \hat{1} & \hat{0} \end{pmatrix}$, $J = \begin{pmatrix} \hat{1} & \hat{1} \\ \hat{1} & -\hat{1} \end{pmatrix}$. Se observă mai

întâi că $\det(I) = \hat{1}$, $\det(J) = -\hat{2} = \hat{1}$ deci $I, J \in SL_3(\mathbb{Z}_3)$.

Fie $K = IJ = \begin{pmatrix} -\hat{1} & \hat{1} \\ \hat{1} & \hat{1} \end{pmatrix}$. Verificăm atunci egalitățile:

$$I^2 = J^2 = K^2 = -I_2; \quad JI = -K, \quad JK = I = -KJ, \quad KI = J = -IK$$

și apoi completăm tabla cauză ea a grupului quaternion.

3. Determinați următoarele subgrupuri ale lui $(\mathbb{Q}, +)$:

a) $\langle \frac{1}{2} \rangle$

b) $\langle \frac{1}{2}, \frac{1}{3} \rangle$

c) $\langle \frac{1}{2}, \frac{1}{3}, \frac{1}{5}, \dots, \frac{1}{p}, \dots \rangle$ p este prim

d) $\langle \{ \frac{1}{n!} \mid n \in \mathbb{N} \} \rangle$

Soluție. a) $\langle \frac{1}{2} \rangle = \{ k \cdot \frac{1}{2} \mid k \in \mathbb{Z} \}$

(dacă înlocuim în formula de la începutul seminarului $X = \{x\}$ atunci

$$\langle x \rangle = \{ x^{\epsilon_1} x^{\epsilon_2} \dots x^{\epsilon_n} \mid \epsilon_i = \pm 1 \} = \{ x^k \mid k \in \mathbb{Z} \}.$$

b) $\langle \frac{1}{2}, \frac{1}{3} \rangle = \{ k \cdot \frac{1}{2} + n \cdot \frac{1}{3} \mid k, n \in \mathbb{Z} \}$ (tot cu formula de dinaintea)

Dar aici putem arăta uai mult:

$$\langle \frac{1}{2}, \frac{1}{3} \rangle = \langle \frac{1}{6} \rangle = \{ k \cdot \frac{1}{6} \mid k \in \mathbb{Z} \}.$$

Într-adevăr $\frac{1}{6} = \frac{1}{2} - \frac{1}{3} \in \langle \frac{1}{2}, \frac{1}{3} \rangle$ deci $\langle \frac{1}{6} \rangle \subseteq \langle \frac{1}{2}, \frac{1}{3} \rangle$.

Reciproc $\frac{1}{2} = \frac{1}{6} + \frac{1}{6} + \frac{1}{6} \in \langle \frac{1}{6} \rangle$ și $\frac{1}{3} = \frac{1}{6} + \frac{1}{6} \in \langle \frac{1}{6} \rangle$ deci

$$\langle \frac{1}{2}, \frac{1}{3} \rangle \subseteq \langle \frac{1}{6} \rangle.$$

c) $\langle \{ \frac{1}{p} \mid p \text{ prim} \} \rangle = \{ \frac{a}{b} \in \mathbb{Q} \mid (a,b)=1 \text{ și } b \text{ liber de pătrate} \}.$

Ca și în cazul exercitiului 1 putem arăta că

$$\{ \frac{a}{b} \in \mathbb{Q} \mid (a,b)=1 \text{ și } b \text{ liber de pătrate} \} = \{ x \in \mathbb{Q} \mid \exists a, b \in \mathbb{Z}, b \neq 0 \text{ liber de pătrate} \}$$

și $x = \frac{a}{b}$

Idea este că $x \in \mathbb{Q}$ și poate scrie ca o fracție cu numitorul liber de pătrate (sau relativ prim cu $n \in \mathbb{N}$) etc. Ca

în exercitiul 1) să-l scrie ca o fracție ireductibilă

cu aceeași proprietate. Prin urmare notăm

$$H = \{ x \in \mathbb{Q} \mid \exists a, b \in \mathbb{Z}, b \neq 0 \text{ liber de pătrate și } x = \frac{a}{b} \}$$

și avem $0 = \frac{0}{1} \in H$

• $x, y \in H \Rightarrow x = \frac{a}{b}, y = \frac{c}{d}$, cu b, d libere de pătrate.

Atunci $m = [b, d]$ este liber de pătrate și x, y se scrie

ca o fracție cu numitorul un. Deci $x, y \in H$.

Mai mult $\frac{1}{p} \in H$ pt. orice p prim și dacă

G este un subgrup al lui $(\mathbb{Q}, +)$ care conține toate elem. de

forma $\frac{1}{p}$, p prim avem $H \subseteq G$. Într-adevăr pentru

$\frac{a}{b} \in H$ (adică b liber de pătrate) avem $\frac{a}{b} = \frac{1}{b} + \frac{1}{b} + \dots + \frac{1}{b}$

pt. $a \geq 0$ sau $\frac{a}{b} = -\left(\frac{1}{b} + \frac{1}{b} + \dots + \frac{1}{b}\right)$ pt. $a < 0$, deci este

suficient să arătăm că $\frac{1}{b} \in G$. Dacă b liber de pătrate

$\Leftrightarrow b = p_1 p_2 \dots p_k$ cu p_i $1 \leq i \leq k$ prime diferite. Vom

proceda prin inducție după k .

Pentru $k=1$ avem $b = p \in G$.
Presupunem că afirmația e adevărată pt. orice b care se scrie

ca un produs de k numere prime distincte și fie

$b = p_1 p_2 \dots p_k \cdot p_{k+1}$ cu p_i $1 \leq i \leq k+1$ prime distincte.

Pb. că $(p_1 p_2 \dots p_k, p_{k+1}) = 1$ există coeficienți Bezout

$$\Delta, t \in \mathbb{Z} \text{ a.i. } \Delta p_1 p_2 \dots p_k + t \cdot p_{k+1} = 1 \text{ atunci}$$
$$\frac{1}{b} = \frac{1}{p_1 \dots p_k p_{k+1}} = \Delta \frac{p_1 p_2 \dots p_k}{p_1 p_2 \dots p_k p_{k+1}} + t \cdot \frac{p_k}{p_1 \dots p_k p_{k+1}}$$

$$= \Delta \cdot \frac{1}{p_{k+1}} + t \cdot \frac{1}{p_1 \dots p_k}$$

\uparrow \uparrow
 G G (ipoteza de inducție).

Deci $\frac{1}{b} \in G$ și afirmația este demonstrată.

Arătăm că $\langle \frac{1}{n!} \mid n \in \mathbb{N} \rangle = \mathbb{Q}$.

Incluziunea „ \subseteq ” este evident adevărată și pt. „ \supseteq ” considerăm

o fracție $\frac{a}{b} \in \mathbb{Q}$ oarecare. Atunci

$$\frac{a}{b} = \frac{a \cdot (b-1)!}{b!} = \frac{k}{b!} = k \cdot \frac{1}{b!} \in \langle \frac{1}{n!} \mid n \in \mathbb{N} \rangle.$$

6. Fie (G, \cdot) un grup cu proprietatea că $g^2 = 1$ pt orice $g \in G$.
- Arătați că pt. sau $H \leq G$ avem $H \cup gH \leq G$ pt. orice $g \in G$.
 - Dacă G este finit atunci $|G| = 2^k$, $k \in \mathbb{N}$.

Soluție a). Se știe că G este comutativ (v. seminarul 1). Avem

- $x \in H \Rightarrow x \in H \cup gH$

- fie $x, y \in H \cup gH$.

Dacă $x, y \in H$ atunci $x \cdot y \in H \subseteq H \cup gH$

Dacă $x \in H, y \in gH$ atunci $y = g \cdot y'$ cu $y' \in H \Rightarrow xy = g \cdot xy' \in gH \subseteq H \cup gH$

Dacă $x \in gH, y \in H$ atunci $xy \in H \cup gH$ din comutativitate

Dacă $x, y \in gH$ atunci $x = gx', y = gy'$ cu $x', y' \in H$ deci
 $xy = g^2 \cdot x' \cdot y' = x' \cdot y' \in H$

- fie $x \in H \cup gH$.

Dacă $x \in H$ atunci $x^{-1} \in H \subseteq H \cup gH$

Dacă $x \in gH$ atunci $x = gx'$ cu $x' \in H$ deci $x^{-1} = g^{-1} \cdot x'^{-1} = gx'^{-1}$
 (pt. că $g^{-1} = g$) deci $x^{-1} \in gH \subseteq H \cup gH$.

Deci $H \cup gH \leq G$.

Ob Dacă $g \in H$ atunci $gH \subseteq H$ (chiar $gH = H$) deci $H \cup gH = H$.

b). Mai întâi vom arăta că dacă H este finit și $g \in G \setminus H$ atunci

$$|H \cup gH| = 2|H|. \quad (*)$$

Într-adevar funcția $f: H \rightarrow gH$, $f(x) = gx$ este injectivă și surjectivă (justificare temă) deci $|H| = |gH|$. Mai mult

$H \cap gH = \emptyset$ deoarece din $x \in H \cap gH$ am obține $x \in H$ și $x = g \cdot h$ pt. un $h \in H$ deci $g = x \cdot h^{-1} \in H$ ceea ce contrazică $g \notin H$.

Acum luăm $H_0 = \{1\}$ și dacă presupunem că $H_i, i \geq 0$ este dat atunci fie $H = G$ sau $H \subsetneq G$. În primul caz

pe opinia în al doilea considerăm $g_i \in G \setminus H_i$ și construim $H_{i+1} = H_i \cup g_i H_i$. Prin urmare egalitatea (*) ne asigură că $|H_i| = 2^i$ pt. orice $i \geq 0$, pt. care am construit H_i .

Dacă procesul nu s-ar opri niciodată, atunci

$$\{H_k = H_0 \subsetneq H_1 \subsetneq H_2 \subsetneq \dots$$

ar fi un sm infinit de subgrupuri ale lui G . Dar G este finit și așa ceva este imposibil. Deci procesul trebuie să se termine, ceea ce înseamnă că $\exists k \geq 0$ a.i.

$$G = H_k \quad \text{și} \quad |G| = |H_k| = 2^k.$$

Altă metodă (pt. b): Să modificăm notația folosită pt. operația din G și să spunem că $(G, +)$ este un grup în care $g+g=0$, pt. oricui $g \in G$. Ca și mai înainte știm că $(G, +)$ este comutativ. Definim o înmulțire cu scalari cuantă din $\mathbb{Z}_2 = \{0, 1\}$. Prin

$$\mathbb{Z}_2 \times G \rightarrow G, \quad \hat{0} \cdot x = 0 \quad \text{și} \quad \hat{1} \cdot x = x, \quad \forall x \in G.$$

Atunci este clar că putem scrie $\hat{n} \cdot x = n \cdot x$ pt. orice $n \in \mathbb{Z}$ (pt. că dacă n este par atunci rezultatul este 0 iar dacă n este impar atunci rezultatul este x)

Se verifică acum ușor că

$$\hat{n}(x+y) = \hat{n}x + \hat{n}y$$

$$(\hat{n} + \hat{m})x = \hat{n}x + \hat{m}y$$

$$\hat{n}(\hat{m}x) = (\hat{n} \cdot \hat{m})x$$

$$\uparrow x = x$$

pt. orice $n, m \in \mathbb{Z}$
și orice $x, y \in G$.

Deci G este un \mathbb{Z}_2 -spațiu vectorial. Din cursul de algebră liniară știm că G are o bază care trebuie să fie finită și $k = \dim_{\mathbb{Z}_2} G$. Tot cursul de algebră liniară (cu corolar al proprietății de universalitate) ne spune că

$$G \cong \mathbb{Z}_2^k \quad (\text{isomorfism de } \mathbb{Z}_2\text{-sp. vectoriale)}$$

$$\text{Atunci} \quad |G| = |\mathbb{Z}_2^k| = 2^k.$$