Seminar 5

Subgrupuri

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

$H \leq G$ (subgrup) $\iff$ a) $1 \in H$
b) $x,y \in H \Rightarrow x \cdot y \in H$
c) $x \in H \Rightarrow x^{-1} \in H$

Obs. Conditia $1 \in H$ poate fi inlocuita cu $H \neq \emptyset$.
Intr-adevar daca $1 \in H$ atunci $H \neq \emptyset$.
Reciproc daca $H \neq \emptyset$ atunci $\exists x \in H$ si din conditia
c) de mai sus $x^{-1} \in H$. Atunci conditia b aplicata pt.
x si x^{-1} ne spune ca $1 = x \cdot x^{-1} \in H$.

Teorema: Intersectia unei multimi de subgrupuri este subgrup.

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

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

Teorema $\langle X \rangle = \{x_1^{\varepsilon_1} x_2^{\varepsilon_2} \dots x_n^{\varepsilon_n} \mid n \in \mathbb{N},\ x_i \in X,\ \varepsilon_i = \pm 1\}$

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

1. Să se verifice dacă următoarele submulțimi 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) $n \in \mathbb{N}^*$ $H_n = \{\frac{a}{b} \in \mathbb{Q} \mid (a,b) = 1$ și $b \mid n\}$ în $(\mathbb{Q}, +)$
d) $n \in \mathbb{N}^*$ $K_n = \{\frac{a}{b} \in \mathbb{Q}^* \mid (a,b) = 1$ și $b \mid n\}$ în $(\mathbb{Q}^*, \cdot)$
e) $n \in \mathbb{N}^*$ $L_n = \{\frac{a}{b} \in \mathbb{Q} \mid (a,b) = 1$ și $(b,n) = 1\}$ în $(\mathbb{Q}, +)$
f) $n \in \mathbb{N}^*$ $M_n = \{\frac{a}{b} \in \mathbb{Q}^* \mid (a,b) = 1$ 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) $1 = 1+0i \notin T \Rightarrow T \not\leq \mathbb{C}^*$ (nu conține elementul neutru)

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

Întâi arătăm incluziunea „$\subseteq$" este imediată prin definiția lui H_n

- „$\supseteq$": Fie $x = \frac{a}{b}$ cu $a, b \in \mathbb{Z}$, $b \mid n$ 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 $(a', b') = 1$ și $b' \mid b$ deci $b' \mid n$. Așadar $x = \frac{a'}{b'} \in H_n$.

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 $a, b, c, d \in \mathbb{Z}$, $b \mid n$ și $d \mid n$.

Notăm $m = [b, d]$ și avem $m = bk = dq$, iar $m \mid n$. 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 $K_n \not\leq \mathbb{Q}^*$

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 • $0 = \frac{0}{1} \in L_n$

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

Avem $x - y = \frac{a}{b} - \frac{c}{d} = \frac{ad - bc}{bd} \in L_n$ 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 $b^2 \in \mathbb{R}$ și $(b^{-1})^2 = (b^2)^{-1} \in \mathbb{Q}$

Deci $a \cdot b^{-1} \in L$ pt. că $(a \cdot b^{-1})^2 = a^2 \cdot (b^{-1})^2$ 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 $U \not\leq \mathbb{R}$ (nu este parte stabilă

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

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

$\sqrt{2} = \frac{a}{b}$ cu $a, b \in \mathbb{Z}$, $b \neq 0$ 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 $\sqrt{2} = \frac{q-3}{2} \in \mathbb{Q}$ 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) $\{1, r^2, sr, sr^3\}$ în D_4

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

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.
Prin urmare H este parte stabilă (deci închisă) și are arătat că $1 \in H$ și dacă $x \in H$ atunci $x^{-1} \in H$, deci H este subgrup.

b) Concluzia nu mai rămâne adevărată. Contraexemplu $\mathbb{N}$ este parte stabilă, nevidă în $(\mathbb{Z}, +)$ dar nu este subgrup

4. a) Arătați că $SL_n(\mathbb{Z}_3) = \{A \in M_3(\mathbb{Z}_3) \mid \det(A) = \hat{1}\} \leq GL_3(\mathbb{Z}_3)$
b) Determinați $\left\langle \begin{pmatrix} \hat{0} & -\hat{1} \\ \hat{1} & \hat{0} \end{pmatrix}, \begin{pmatrix} \hat{1} & \hat{1} \\ \hat{1} & -\hat{1} \end{pmatrix} \right\rangle$ 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
$\det(A \cdot B^{-1}) = \det(A) \cdot \det(B^{-1}) = \det(A) \cdot \det(B)^{-1} = 1 \cdot 1^{-1} = 1$
Așadar $A \cdot B^{-1} \in SL_3(\mathbb{Z}_3)$ ceea ce arată că $SL_3(\mathbb{Z}_3) \leq GL_3(\mathbb{Z}_3)$

b) Notăm $I = \begin{pmatrix} \hat{0} & -\hat{1} \\ \hat{1} & \hat{0} \end{pmatrix}$, $J = \begin{pmatrix} \hat{1} & \hat{1} \\ \hat{1} & -\hat{1} \end{pmatrix}$. Să observăm 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:
$I^2 = J^2 = K^2 = -I_2$; $JI = -K$, $JK = I = -KJ$, $IKI = J = -IK$
și apoi completăm tabla care este cea a grupului quaternionilor.

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

(dacă înlocuim în formula de la începutul seriei anterioare $X = \{x\}$ atunci $\langle x \rangle = \{x^{\varepsilon_1} x^{\varepsilon_2} \dots x^{\varepsilon_n} \mid \varepsilon_i = \pm 1\} = \{x^k \mid k \in \mathbb{Z}\}$).

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

Dar aici putem arăta mai mult.

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

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

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

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 exercițiului 1 putem arăta că

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

Ideea este că $x \in \mathbb{Q}$ se poate scrie ca o fracție cu numitorul liber de pătrate (sau relativ prim cu $n \in \mathbb{N}^*$ etc. ca în exercițiul 1) deci că x se scrie ca o fracție ireductibilă cu această proprietate. Prin urmare notăm

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

și avem $\cdot\ 0 = \frac{0}{1} \in H$

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

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

ca o fracție cu numitorul nr. Deci $x-y \in H$.

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

G este un subgrup al lui $(\mathbb{Q}, +)$ care conține toate elem. de forma $\frac{1}{p}$, p prim avem $H \subseteq G$. Mai rămâne de arătat că pentru $\frac{a}{b} \in H$ (adică b liber de pătrate) avem $\frac{a}{b} = \underbrace{\frac{1}{b} + \frac{1}{b} + \dots + \frac{1}{b}}_{a\text{-ori}}$ pt. $a \geq 0$ sau $\frac{a}{b} = -\left(\underbrace{\frac{1}{b} + \frac{1}{b} + \dots + \frac{1}{b}}_{|a|\text{-ori}}\right)$ pt. $a < 0$, deci este suficient să arătăm că $\frac{1}{b} \in G$. Dar b liber de pătrate $\Rightarrow b = p_1 p_2 \dots p_k$ cu p_i $1 \leq i \leq k$ prime diferite. Vom proceda prin inducție după k.

Pentru $k = 1$ avem $b = \frac{1}{p} \in G$.

Presupunem că afirmația 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 coeficienții Bezout $s, t \in \mathbb{Z}$ a.i $s p_1 p_2 \dots p_k + t \cdot p_{k+1} = 1$ atunci

$$\frac{1}{b} = \frac{1}{p_1 \dots p_k p_{k+1}} = s \frac{p_1 p_2 \dots p_k}{p_1 p_2 \dots p_k p_{k+1}} + t \cdot \frac{p_{k+1}}{p_1 \dots p_k p_{k+1}} =$$

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

$\in G$ (ipoteza de inducție).

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

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

Incluziunea „$\subseteq$" este evident adevărată și pt. „$\supseteq$" considerăm o fracție $\frac{a}{b} \in \mathbb{Q}$ oarecare. Atunci

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

6. Fie $(G,\cdot)$ un grup cu proprietatea că $g^2=1$ $\forall$ oricare $g\in G$.
a) Arătați că $\forall$ oricare $H\leq G$ avem $HUgH\leq G$ $\forall$ oricare $g\in G$.
b) Dacă G este finit atunci $|G|=2^k$, $k\in\mathbb{N}$.

Soluție a). Se știe că G este comutativ (v. seminarul 1). Avem
- $1\in H \Rightarrow 1\in HUgH$
- fie $x,y\in HUgH$.
  Dacă $x,y\in H$ atunci $x\cdot y\in H\subseteq HUgH$
  Dacă $x\in H$, $y\in gH$ atunci $y=g\cdot y'$ cu $y'\in H \Rightarrow xy=gxy'\in gH\subseteq HUgH$
  Dacă $x\in gH$, $y\in H$ atunci $xy\in HUgH$ din comutativitate
  Dacă $x,y\in gH$ atunci $x=gx'$, $y=gy'$ cu $x'\cdot y'\in H$ deci
  $$xy=g^2\cdot x'y'=x'\cdot y'\in H$$
- fie $x\in HUgH$.
  Dacă $x\in H$ atunci $x^{-1}\in H\subseteq HUgH$
  Dacă $x\in gH$ atunci $x=gx'$ cu $x'\in H$ deci $x^{-1}=g^{-1}\cdot x'^{-1}=gx'^{-1}$ ($\forall$ oricare $g^{-1}=g$) deci $x^{-1}\in gH\subseteq HUgH$.

Deci $HUgH\leq G$.

Obs Dacă $g\in H$ atunci $gH\subseteq H$ (chiar $gH=H$) deci $HUgH=H$.

b). Mai întâi vom arăta că dacă H este finit și $g\in G\setminus H$ atunci
$$|HUgH|=2|H|. \quad (*)$$
Între-adevăr funcția $f:H\to gH$, $f(x)=gx$ 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 $x=g\cdot h$ $\forall$ oricare $h\in H$ deci $g=x\cdot h^{-1}\in H$ ceea ce contrazice $g\notin H$.

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

Dacă procesul nu s-ar opri niciodată, atunci

$$\{1\} = H_0 \subsetneq H_1 \subsetneq H_2 \subsetneq \dots$$

ar fi un șir infinit de subgrupuri ale lui G. Dar G era finit și asta era exact imposibil. Deci procesul trebuie să se termine, deci e important că $\exists k \geq 0$ a.i.

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

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. orice $g \in G$. Ca și mai înainte știm că $(G, +)$ este comutativ. Definim o înmulțire cu scalari luați din $\mathbb{Z}_2 = \{\hat{0}, \hat{1}\}$. Prin

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

Atunci este clar că putem scrie $\hat{n}x = n \cdot x$ 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

$$\hat{n}(x+y) = \hat{n}x + \hat{n}y$$
$$(\hat{n} + \hat{m})x = \hat{n}x + \hat{m}y \quad \text{pt orice } n, m \in \mathbb{Z} \text{ și orice } x, y \in G.$$
$$\hat{n} \cdot (\hat{m}x) = (\hat{n} \cdot \hat{m})x$$
$$\hat{1}x = x$$

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 fie $k = \dim_{\mathbb{Z}_2} G$. Tot cursul de algebră liniară (sau corolar al proprietății de universalitate) ne spune că

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

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