Seminar 1 – Recapitulare

1 Grupuri - Definiții

Definiţie 1.1: Se numește *grup* orice monoid cu toate elementele inversabile.

Mai precis, fie G o mulțime nevidă și $*$ o operație binară pe G. Perechea $(G,*)$ formează un grup dacă:

(1) Operația $*$ este *internă*;

(2) Operația $*$ este *asociativă*;

(3) Operația $*$ admite *element neutru*;

(4) Orice element din G este inversabil față de $*$.

Dacă, în plus, operația $*$ este *comutativă*, atunci grupul se numește *comutativ* sau *abelian*.

În continuare, cînd nu există riscul de confuzie, vom desemna un grup doar prin mulțimea subiacentă, iar notația pentru operație va fi multiplicativă, cu juxtapunere.

Substructura unui grup este definită ca mai jos:

Definiţie 1.2: Fie G un grup și $H \subseteq G$ o submulțime. Spunem că H este un *subgrup* al lui G, notat $H \leq G$ dacă H la rîndul său devine grup, cu operația indusă. În plus, $1_G \in H$.

Există o teoremă care caracterizează într-o ecuație definiția subgrupului.

Teoremă 1.1: *În notațiile și contextul din definiție,* $H \leq G \iff xy^{-1} \in H, \forall x, y \in H$.

Mai departe, funcțiile "speciale" între grupuri (compatibile cu structura de grup) se definesc mai jos.

Definiţie 1.3: Fie $(G,*)$ și $(H,\circ)$ două grupuri. O funcție $f : G \to H$ se numește *morfism de grupuri* dacă:

$$f(g_1 * g_2) = f(g_1) \circ f(g_2).$$

Dacă f este injectiv, se numește *monomorfism*, dacă este surjectiv, se numește *epimorfism*, iar dacă este bijectiv, se numește *izomorfism*. Mai mult, dacă $G = H$, morfismul f se numește *endomorfism*, iar dacă este bijectiv, se numește *automorfism*.

Ca notații, pentru mulțimea morfismelor de grupuri $G \to H$ se folosește $\mathrm{Hom}(G,H)$, iar mulțimea endomorfismelor unui grup G se notează $\mathrm{End}(G)$, respectiv mulțimea automorfismelor, $\mathrm{Aut}(G)$.

Din definiția morfismului de grupuri rezultă imediat următoarele proprietăți:

Propoziţie 1.1: *Fie $f : G \to H$ un morfism de grupuri. Atunci:*

(a) f este unitar, i.e. $f(1_G) = 1_H$;

(b) $\Big(f(x)\Big)^{-1} = f(x^{-1})$;

Pentru un morfism de grupuri $f : G \to H$, se definesc următoarele mulțimi:

$$\mathrm{Ker} f = \{x \in G \mid f(x) = 1\} \subseteq G \qquad \text{și} \qquad \mathrm{Im} f = \{y \in H \mid \exists x \in G \text{ a.î. } f(x) = y\} \subseteq H.$$

Ele se numesc *nucleul* (engl. *kernel*) și *imaginea* morfismului.

Putem construi *grupul liber* generat de o submulțime a unui grup, $A = \{a_1, a_2, a_3, \ldots, a_n, \ldots\} \subseteq G$, ca fiind:

$$\langle A \rangle = \{a_1^{\pm 1} a_2^{\pm 1} \cdots a_p^{\pm 1} \mid a_i \in A, p \geq 0\}$$

Dacă $A = \{\bullet\}$, atunci grupul generat de A se numește *ciclic*.

Definiţie 1.4: Fie G un grup și $x \in G$ un element. Cel mai mic număr natural n astfel încît $x^n = 1$ se numește *ordinul elementului* x. Dacă n nu există, se pune prin definiție $ord(x) = \infty$.

A nu se confunda cu:

Definiţie 1.5: Ordinul unui grup G înseamnă cardinalul mulțimii subiacente.

Cu acestea, putem formula și demonstra următoarele:

Teoremă 1.2: *Fie G un grup și $x \in G$, cu $ord(x) = n$. Atunci $x^k = 1 \Leftrightarrow n \mid k$, pentru $k \in \mathbb{Z}$. În plus, dacă $ord(G) = g$, avem $n \mid g$ (Lagrange).*

Folosind teoria grupurilor în cazul claselor de resturi, putem obține următoarele:

Teoremă 1.3 (Euler)**:** *Fie $a, n \geq 1$, cu $(a, n) = 1$. Atunci:*

$$a^{\varphi(n)} \equiv 1 \ (mod\ n).$$

Teoremă 1.4 (Mica Teoremă a lui Fermat)**:** *Fie p un număr prim și a un număr natural nedivizibil cu p. Atunci:*

$$a^{p-1} \equiv 1 \ (mod\ p).$$

2 Subgrupuri normale, grup factor

Pornind cu un grup arbitrar și un subgrup al lui, putem defini o relație de echivalență asociată datelor, iar mulțimea factor să aibă o importanță deosebită. Avem nevoie de următoarele:

Definiţie 2.1: Fie G un grup și H un subgrup al său. Mulțimile de forma $xH = \{xh \mid h \in H\}$, cu x un element fixat din G se numesc mulțimi de echivalență la stînga (*coset-uri stîngi*) ale lui H în G. Similar, mulțimile de forma $Hx = \{hx \mid h \in H\}$ se numesc *coset-uri drepte*, iar $xHx = \{xhx \mid h \in H\}$ se numesc *coset-uri duble*.

Definiţie 2.2: Fie G un grup și H un subgrup al său. Pentru un element fixat $x \in G$, mulțimile de forma xHx^{-1} se numesc *clase de conjugare* ale lui x. Elementele din ele se numesc *elemente conjugate* cu x.

Un caz particular de subgrupuri ne interesează.

Definiţie 2.3: Fie G un grup și H un subgrup al său. H se numește *subgrup normal*, notat $H \trianglelefteq G$ dacă $xH = Hx, \forall x \in G$. Echivalent, $xHx^{-1} \subseteq H, \forall x \in G$.

În acest caz particular, coset-urile stîngi și drepte coincid (modulo o permutare), așa că putem introduce o nouă noțiune, care este bine definită:

Definiţie 2.4: Fie $H \trianglelefteq G$. *Indicele* subgrupului H în G, notat $[G : H]$ este mulțimea coset-urilor stîngi (drepte) ale lui H în G.

Putem formula și demonstra un rezultat simplu, care ne va folosi pentru a obține teorema lui Lagrange într-o nouă prezentare.

Lemă 2.1: *Fie $H \leq G$ și $a, b \in G$. Atunci:*

(a) $aH = bH \Leftrightarrow b^{-1}a \in H$. *În particular,* $aH = H \Leftrightarrow a \in H$;

(b) $aH \cap bH = \emptyset \Rightarrow aH = bH$;

(c) $card(aH) = card(H), \forall a \in G$.

Folosind această lemă, putem da o nouă formulare și demonstrație pentru teorema lui Lagrange, anume:

Teoremă 2.1 (Lagrange)**:** *Fie $H \trianglelefteq G$. Atunci $ord(G) = ord(H) \cdot [G : H]$.*

Acum putem defini relația de echivalență anunțată, folosind cele de mai sus.

Definiţie 2.5: Fie $H \trianglelefteq G$ și $a, b \in G$. Pe G definim următoarea relație:

$$a \sim b \Leftrightarrow a \in bH \quad (\Leftrightarrow ab^{-1} \in H).$$

Aceasta este o relație de echivalență, iar mulțimea factor, notată G/H, se numește *grupul factor* G modulo H.

Motivul pentru care G/H se numește chiar *grup* și nu doar mulțime este că, într-adevăr, se obține o structură de grup, cu operația:

$$aH \cdot bH = (a \cdot b)H, \forall a, b \in G.$$

3 Teorema fundamentală de izomorfism pentru grupuri

Acest rezultat, descoperit de Emmy Noether, ne arată puterea grupurilor factor și, practic, principala lor utilizare, felul în care apar în uz. Puterea teoremei rezidă în faptul că datele de intrare sînt foarte simple, spre deosebire de puterea rezultatului.

Teoremă 3.1 (Teorema fundamentală de izomorfism - Emmy Noether)**:** *Fie $f : G \to H$ un morfism de grupuri. Atunci există un izomorfism de grupuri indus de f:*

$$\varphi : G/\mathrm{Ker} f \to \mathrm{Im} f, \quad \varphi(\widehat{x}) = f(x).$$

În particular, dacă f este injectiv, obținem $G \simeq f(G)$. Spunem, în acest caz, că un morfism injectiv este *un izomorfism pe imagine*. Iar dacă f este surjectiv, obținem $G/\mathrm{Ker} f \simeq H$. În cazul în care f este izomorfism, teorema lui Noether nu ne spune nimic, obținem din nou $G \simeq H$.

Iată cîteva utilizări ale teoremei fundamentale de izomorfism.

1. Putem arăta că $\mathbb{Z}/n\mathbb{Z} \simeq \mathbb{Z}_n$, în felul următor. Fie $f : \mathbb{Z} \to \mathbb{Z}$ un morfism dat de $f(x) = x \bmod n$. Atunci $\mathrm{Ker} f = n\mathbb{Z}$ și $\mathrm{Im} f = \mathbb{Z}_n$.

2*. Putem da o nouă descriere pentru inelul întregilor lui Gauss, anume $\mathbb{Z}[i] \simeq \mathbb{Z}[X]/(X^2 + 1)$. Demonstrația este: considerăm $f : \mathbb{Z}[X] \to \mathbb{Z}$ dată de $f(p) = p(i)$. Atunci $\mathrm{Ker} f = (X^2+1)$ și $\mathrm{Im} f = \mathbb{Z}[i]$. Prin această metodă putem obține, de fapt, toate inelele de forma $\mathbb{Z}[i\sqrt{d}]$.

În teoria inelelor, teorema fundamentală de izomorfism ne va fi de folos într-un context special, deoarece există caracterizări folosind inele factor pentru cazuri speciale de ideale (e.g. ideale prime și ideale maximale).

4 Inele

Definiţie 4.1: Fie A o mulțime nevidă și $+, \cdot$ două operații pe A. Tripletul $(A, +, \cdot)$ se numește *inel* dacă

- $(A, +)$ este grup comutativ;
- $(A, \cdot)$ este monoid;
- $a \cdot (b + c) = a \cdot b + a \cdot c$ și $(b + c) \cdot a = b \cdot a + c \cdot a, \forall a, b, c \in A$ (distributivitatea $\cdot$ față de $+$).

Dacă, în plus, monoidul $(A, \cdot)$ este comutativ, inelul A se numește *comutativ*.

Pentru un inel A, notăm cu $U(A)$ mulțimea elementelor inversabile față de înmulțire. Așadar, $U(A)$ este grup multiplicativ și, luat împreună și cu adunarea, $U(A)$ este un corp.

Cîteva elemente speciale din inele sînt următoarele.

Definiţie 4.2: Fie A un inel. Elementul $a \in A$ se numește *divizor al lui zero* (sau *zero-divizor*) dacă $a \neq 0$ și există $b \neq 0$ în A cu $ab = 0$. Un inel care nu are divizori ai lui zero se numește *integru*. Iar dacă este și comutativ, se numește *domeniu (de integritate)*.

Elementul $a \in A$ se numește *inversabil* sau *unitate* dacă există $b \in A$ cu $a \cdot b = b \cdot a = 1$.

Elementul $a \in A$ se numește *idempotent* dacă $a^2 = a$ și *nilpotent* dacă există $n \in \mathbb{N}$ astfel încît $a^n = 0$. Cel mai mic astfel de n se numește *indice de nilpotență*.

Definiţie 4.3: Fie A un inel și $B \subseteq A$ o submulțime a sa. B se numește *subinel* dacă B este subgrup aditiv al lui $(A, +)$, B este parte stabilă față de $\cdot$ și $1 \in B$.

B se numește *ideal* dacă este subgrup aditiv al lui $(A, +)$ și $\forall a \in A, aB \subseteq B (\Leftrightarrow a \cdot b \in A, \forall a \in A, b \in B)$. Se notează $B \trianglelefteq A$.

Definiţie 4.4: Fie A, B două inele. O funcție $f : A \to B$ se numește *morfism de inele* dacă este unitară, aditivă și multiplicativă, adică $f(1_A) = 1_B$, $f(a + b) = f(a) + f(b)$ și $f(a \cdot b) = f(a) \cdot f(b), \forall a, b \in A$.

Definiţie 4.5: Fie A un inel. Se numește *caracteristica inelului* numărul natural $car(A)$ definit prin ordinul aditiv al elementului 1. Dacă acesta nu este finit, se definește $car(A) = 0$.

În general, caracteristica unui inel integru este zero sau un număr prim.

Definiţie 4.6: Fie A un inel și I un ideal al său. Putem defini grupul (aditiv) factor A/I și, în plus, îi putem da o structură de inel. Astfel, A/I devine inel, numit *inel factor*, cu operațiile: $(a + I) + (b + I) = (a + b) + I$ și $(a + I) \cdot (b + I) = (a \cdot b) + I$.

De asemenea, pentru inele are loc și teorema fundamentală de izomorfism.

5 Exemple și exerciții

1. Fie G, H două grupuri și $f : G \to H$ un morfism de grupuri. Arătați că:

(a) $\mathrm{Ker} f$ este subgrup al lui G;

(b) $\mathrm{Im} f$ este subgrup al lui H;

(c) f este injectiv dacă și numai dacă $\mathrm{Ker} f = \{1_G\}$;

(d) f este surjectiv dacă și numai dacă $H/f(G) = \{\widehat{1}_H\}$;

(e) f este injectiv dacă și numai dacă $G \simeq f(G)$.

2. Arătați că un grup G în care orice element are ordinul 2 este comutativ.

3. Descrieți grupul lui Klein $\mathcal{K}$ și arătați că este izomorf cu $\mathbb{Z}_2 \times \mathbb{Z}_2$.

4. Fie G un grup, $a \in G$ un element arbitrar și $f_a : G \to G$ un morfism definit prin $f_a(g) = a^{-1}ga$ (se numește *automorfismul de conjugare*).

(a) Arătați că $f_a \in \mathrm{Aut}(G)$.

(b) Fie $\mathrm{Int}(G) = \{f_g \mid g \in G\}$ (*grupul automorfismelor interioare*). Arătați că $\mathrm{Int}(G) \trianglelefteq \mathrm{Aut}(G)$.

5. Arătați că $\mathrm{Hom}(\mathbb{Z}, \mathbb{Z}) \simeq \mathbb{Z}$, izomorfism de grupuri.

6. Fie subgrupul aditiv $\mathbb{Z}$ al grupului aditiv $\mathbb{Q}$. Descrieți construcția grupului factor $\mathbb{Q}/\mathbb{Z}$ și arătați că orice element al său are ordin finit.

7. Arătați că următoarele afirmații sînt echivalente:

(a) p este număr prim;

(b) Orice morfism nenul de grupuri abeliene $f : \mathbb{Z}_p \to G$ este injectiv;

(c) Orice morfism nenul de grupuri abeliene $g : G \to \mathbb{Z}_p$ este surjectiv.

8. Pe mulțimea $G = (0,1) \cup (1,\infty)$ definim operația $x * y = x^{lg\sqrt{y}}$. Arătați că $(G, *)$ este un grup.

9. Arătați că într-un inel finit R, orice element este inversabil sau zero-divizor.

10. Arătați că în orice inel R are loc $\mathcal{U}(R) \cap \mathcal{ZD}(R) = \emptyset$.