Link-uri utile

- Grup tutoriat
- Cursurile de la Băețica
- Cursurile de anul acesta de la Mincu
- Cursurile de an trecut de la Mincu

Exerciții

Exercițiul 1. Fie $x \in \mathbb{Z}$. Notăm cu $\hat{a} \in \mathbb{Z}_3$ clasa de resturi modulo 3 corespunzătoare lui a. Fie corespondența $x \mapsto \widehat{x+1}$. Demonstrați că această corespondență definește o funcție.

Demonstrație. Pentru a fi funcție, corespondența trebuie să atribuie fiecărui x un singur rezultat, și să fie definită pentru orice $x \in \mathbb{Z}$.

Definim $f : \mathbb{Z} \to \mathbb{Z}_3$, $f(x) = \widehat{x+1}$. Pentru fiecare x, obținem o clasă de resturi. De asemenea, expresia $\widehat{x+1}$ este definită pentru orice număr întreg. □

Exercițiul 2. Fie $f : \mathbb{Z}_3 \to \mathbb{Z}$, $f(\hat{x}) = 3x + 2$. Demonstrați că această funcție nu este bine definită.

Demonstrație. Să calculăm funcția pentru un x anume:

$$f(\hat{1}) = 3 \cdot 1 + 2 = 5$$

Să calculăm funcția pentru un alt reprezentant din aceeași clasă de resturi:

$$f(\hat{7}) = 3 \cdot 7 + 2 = 23$$

Observăm că $\hat{1} = \hat{7}$, dar $f(\hat{1}) \neq f(\hat{7})$.

Valoarea expresiei depinde de ce reprezentant alegem pentru clasa de resturi. □

Exercițiul 3. Fie $f : \mathbb{R} \to \mathbb{R}$, $f(x) = x^2$. Această funcție nu este nici injectivă, nici surjectivă.

Propuneți o modificare (care ar putea fi aplicată pentru orice funcție) pentru ca aceasta să devină surjectivă, respectiv injectivă.

Demonstrație. Pentru surjectivitate, putem întotdeauna să **restrângem codomeniul** funcției la imaginea ei. Definim deci $f' : \mathbb{R} \to [0, +\infty)$, unde $f'(x) = x^2$.

Pentru injectivitate, am putea alege să **restrângem domeniul**, dar apar două probleme:

- în acest caz este ușor să determinăm la ce să restrângem domeniul, dar pe cazul general nu e clar cum am putea alege submulțimea pe care funcția ar fi injectivă
- vrem să putem cumva să continuăm să calculăm funcția pentru toate valorile din domeniul inițial

Putem rezolva ambele probleme prin *mulțimi factor*. Ne vom folosi de relația de echivalență asociată unei funcții.

Reamintim că relația ρ_f este definită ca

$$x \, \rho_f \, y \iff f(x) = f(y)$$

Pentru funcția noastră:

$$x \, \rho_f \, y \iff x^2 = y^2 \iff |x| = |y|$$

Să vedem care sunt clasele de echivalență pentru ρ_f:

$$\begin{aligned} \mathbb{R}/\rho_f &= \left\{ \left\{ y \in \mathbb{R} \;\middle|\; x \, \rho_f \, y \right\} \;\middle|\; x \in \mathbb{R} \right\} \\ &= \{ \{ y \in \mathbb{R} \mid |x| = |y| \} \mid x \in \mathbb{R} \} \\ &= \{ \{ x, -x \} \mid x \in \mathbb{R} \} \\ &= \{ \hat{x} \mid x \in [0, \infty) \} \end{aligned}$$

unde cu $\hat{x}$ am notat $\{ x, -x \}$.

Vom defini funcția $\tilde{f} : \mathbb{R}/\rho_f \to \mathbb{R}$, $\tilde{f}(\hat{x}) = x^2$. Fiind o funcție de la o mulțime factor la o mulțime obișnuită (adică o funcție în care „dăm jos căciula” lui x) ne punem problema dacă este bine-definită.

Pentru a demonstra asta mai ușor acest lucru ne putem folosi de *proprietatea de universalitate a mulțimii factor*.

Introducem acum și funcția numită *injecția canonică*, $i : \mathbb{R} \to \mathbb{R}/\rho_f$, unde $i(x) = \hat{x}$ (intuitiv, i îi „pune căciula” lui x). Pe cazul general, i e o funcție de la o mulțime la o mulțime factor obținută de la mulțimea inițială, care duce un element în clasa de echivalență corespunzătoare.

Putem rescrie f în funcție de celelalte funcții ca $f = \tilde{f} \circ i$.

$$\begin{tikzcd} \mathbb{R} \arrow[r, "f"] \arrow[d, "i"'] & \mathbb{R}^+ \\ \mathbb{R}/\rho_f \arrow[ur, "\tilde{f}"'] & \end{tikzcd}$$

Relația dintre funcțiile construite

Proprietatea de universalitate ne garantează că în acest caz $\tilde{f}$ este corect definită. $\square$

Exercițiul 4. Fie M o mulțime și $\cdot$ o lege de compoziție binară astfel încât $(M, \cdot)$ este monoid. Notăm cu e elementul neutru al acestui monoid.

Demonstrați că $(M, \odot)$ este tot monoid, unde am definit $x \odot y = y \cdot x$.

Demonstrație. Trebuie să arătăm că legea de compoziție „$\odot$”:

- este *asociativă*:

$$\begin{gathered} (x \odot y) \odot z = x \odot (y \odot z) \iff \\ (y \cdot x) \odot z = x \odot (z \cdot y) \iff \\ z \cdot (y \cdot x) = (z \cdot y) \cdot x \end{gathered}$$

  Ultima egalitate este adevărată deoarece „$\cdot$” este asociativă.

- admite *element neutru*, care este chiar elementul neutru pentru „·”:

$$x \odot e = e \odot x = x \iff e \cdot x \qquad\qquad = x \cdot e = x$$

□

Exercițiul 5. Fie $(M, \cdot)$ un monoid. Notăm cu $U(M)$ mulțimea *unităților* lui M, adică mulțimea elementelor inversabile în raport cu $\cdot$ din M.

Demonstrați că $(U(M), \cdot)$ formează un grup.

Demonstrație. Arătăm mai întâi că $(U(M), \cdot)$ este parte stabilă în raport cu „·”.

Fie $x, y \in U(M)$. Vrem să arătăm că și $xy \in U(M)$, deci că este inversabil.

Inversul lui xy este $y^{-1}x^{-1}$:

$$(xy)(y^{-1}x^{-1}) = x(yy^{-1})x^{-1} = xx^{-1} = e$$
$$(y^{-1}x^{-1})(xy) = y^{-1}(x^{-1}x)y = y^{-1}y = e$$

Observăm că $y^{-1}x^{-1}$ aparține lui $U(M)$ (inversul este xy).

Din faptul că este parte stabilă rezultă că $(U(M), \cdot)$ este monoid.

De asemenea, toate elementele din $U(M)$ sunt inversabile, din definiția acestei submulțimi.

Deci $(U(M), \cdot)$ formează un grup. □

Exercițiul 6. Fie un număr întreg $n > 1$. Lucrăm cu monoidul $(\mathbb{Z}_n, \cdot)$. Fie $0 \leq a < n$.

Demonstrați că a este inversabil în $\mathbb{Z}_n$ dacă și numai dacă $(a, n) = 1$.

Demonstrație. Implicația „ $\implies$ ”: Plecăm de la faptul că $\hat{a} \in \mathbb{Z}_n$ este inversabil. Deci există $\hat{b}$ pentru care

$$\hat{a}\hat{b} = \hat{1}$$

Înlocuind clasele de resturi cu reprezentanți în egalitate. Pentru $p, q, k \in \mathbb{Z}$ avem că:

$$\begin{aligned}(pn + a)(qn + b) &= kn + 1 \\ pqn^2 + qna + pnb + ab - kn &= 1 \\ ab + (pqn + q + p - k)n &= 1 \\ ab + k'n &= 1 && \text{(notăm coeficientul lui } n \text{ cu } k'\text{)}\end{aligned}$$

Notăm cu $d \in \mathbb{Z}$ c.m.m.d.c.-ul lui a și n. Deoarece d divide și pe a și pe n, avem că $d \mid ab + k'n$. Deci d divide și pe 1. Dar asta înseamnă că $d = 1$.

Implicația „ $\impliedby$ ”: Știm din ipoteză că $(a, n) = 1$. Ne folosim de identitatea lui Bézout, care ne spune că există $p, q \in \mathbb{Z}$ astfel încât

$$pa + qn = (a, n) = 1$$

Trecând totul la clase de resturi modulo n obținem că:

$$\begin{gathered}\widehat{pa + qn} = \hat{1} \iff \widehat{pa} + \widehat{qn} = \hat{1} \\ \iff \hat{p}\hat{a} + \hat{q}\hat{n} = \hat{1} \iff \hat{p}\hat{a} + \hat{q}\hat{0} = \hat{1} \\ \iff \hat{p}\hat{a} = \hat{1}\end{gathered}$$

Din ultima egalitate rezultă că $\hat{p}$ din identitatea lui Bézout este inversul lui $\hat{a}$.

Importanța teoretică a acestui rezultat este că avem un mod de a găsi inverse modulare folosind algoritmul lui Euclid extins (care ne ajută să calculăm p, q din identitatea lui Bézout). □

Exercițiul 7. Fie $(G, \cdot)$ un grup în care $(ab)^2 = a^2b^2$, $\forall a, b \in G$.

Demonstrați că $(G, \cdot)$ este abelian (comutativ).

Demonstrație. Un grup este comutativ dacă $ab = ba, \forall a, b \in G$.

Plecând de la relație, și folosindu-ne de faptul că toate elementele dintr-un grup sunt inversabile, obținem echivalențele:

$$\begin{aligned}(ab)^2 = a^2b^2 &\iff \\ abab = aabb &\iff \\ (a^{-1}a)ba(bb^{-1}) = (a^{-1}a)ab(bb^{-1}) &\iff \\ ba = ab\end{aligned}$$

□

Exercițiul 8. Fie $(\mathbb{Z}, +)$ grupul numerelor întregi cu adunarea. Arătați că toate subgrupurile acestuia sunt de forma $n\mathbb{Z}$ pentru un $n \in \mathbb{Z}$, adică multiplii de n.

Demonstrație. Un **subgrup** al unui grup $(G, \cdot)$ este

- o **submulțime** H a lui G
- la rândul ei **grup**, în raport cu aceeași operație

În mod echivalent, un subgrup este o submulțime care:

- este **parte stabilă** în raport cu operația „$\cdot$": dacă $a, b \in H$, atunci $a \cdot b \in H$
- conține **elementul neutru** al lui G
- pentru orice element x din H, și **inversul** x^{-1} este în H

Observăm că $n\mathbb{Z} = \{ kn \mid k \in \mathbb{Z} \}$ formează un subgrup.

Fie H un subgrup al lui $n\mathbb{Z}$. Lucrând pe cazul general, nu știm ce elemente conține.

Fiind subgrup, cu siguranță conține elementul neutru 0. Dacă îl conține doar pe 0, atunci $H = \{ 0 \} = 0\mathbb{Z}$. Dacă nu, observăm că trebuie să conțină cel puțin un număr pozitiv și un număr negativ (dacă îl conține pe x îl conține și pe inversul său la adunare $-x$).

Îl notăm cu a pe cel mai mic număr din H care este strict pozitiv. Deoarece H este subgrup, trebuie să îl conțină și pe $a + a$, $a + a + a$, ..., adică $ka, \forall k \in \mathbb{Z}$.

Să presupunem că mai există un $b \in H, b > 0$, care nu este multiplu de a. Deoarece a este cel mai mic număr strict pozitiv din H, avem că $b > a$. Putem împărți cu rest pe b la a. Atunci relația din teorema împărțirii cu rest se scrie ca

$$b = p \cdot a + r$$

Deoarece r este restul la împărțire, avem că $0 \leq r < a$.

Putem rescrie formula ca

$$r = b - p \cdot a$$

Am plecat de la faptul că $b \in H$, $p \cdot a$ este multiplu de a deci este în H, și deoarece un subgrup este parte stabilă avem că și $r \in H$.

Deci avem în H un număr strict pozitiv r care este mai mic decât a. Asta contrazice presupunerea că a ar fi cel mai mic număr din H. Deci b nu poate să fie în H; toate elementele din H trebuie să fie multiplii de a. □