1. Mulțimi

$C_B A$ = complementara lui A în raport cu B

De Morgan: $C_M(A \cup B) = C_M A \cap C_M B$

$C_M(A \cap B) = C_M A \cup C_M B$

Principiul includerii și excluderii:

$|A_1 \cup A_2 \cup A_3| = |A_1| + |A_2| + |A_3| - |A_1 \cap A_2| - |A_2 \cap A_3|$
$- |A_1 \cap A_3| + |A_1 \cap A_2 \cap A_3|$

Mulțimea părților (submulțimile)

Notație $P(A) \Rightarrow |P(A)| = 2^n$

n = nr. elemente

Pentru orice mulțimi A, B:

$A \cap B \subset A \subset A \cup B$

Două mulțimi cu același cardinal se numesc mulțimi echipotente ($|A| = |B|$)

! O mulțime echipotentă cu $\mathbb{N}$ s.n. numărabilă

2. Funcții

f atr. unui el. din A un unic el. în B

C_b^a = nr. fct. s. cresc.

C_{b+a-1}^a = nr. fct. cresc.

Compunerea funcțiilor e asociativă

$f: A \to B,\ g: B \to C \Rightarrow g \circ f: A \to C$

injectivă: $x, y \in A$ cu $f(x) = f(y) \Rightarrow x = y$
sau $f(x)$ continuă și monotonă

surjectivă: $\forall y \in B, \exists x \in A$ a.î. $f(x) = y$
sau $f(x)$ continuă și codomeniul = im(f)

nr. funcții = n^m
nr. bijecții = $n!$
nr. surjecții = $n^m - C_n^1 (n-1)^m + C_n^2 (n-2)^m + \dots + (-1)^{n-1} C_n^{n-1}$

pentru $f: M \to N$
card M = m, card N = n

! Dacă f, g sunt inj. / surj. / bij. $\Rightarrow g \circ f$ e inj. / surj. / bij.

$g \circ f$ injectivă $\Rightarrow$ f injectivă

$g \circ f$ surjectivă $\Rightarrow$ g surjectivă

3. Relații de echivalență

1) reflexivă : $a \sim a, \forall a \in A$
2) simetrică : $a \sim b \Rightarrow b \sim a$
3) tranzitivă: $a \sim b$ și $b \sim c \Rightarrow a \sim c$

Relația de congruență modulo n:

$$a \equiv b \pmod{n} \Leftrightarrow n \mid a-b$$

Avem 2^{n^2} relații binare pe mulțimea A

Partițiile unei mulțimi sunt familii de submulț. nevide și disjuncte a căror reuniune este mulțimea

$A = A_1 \cup A_2 \cup \ldots \cup A_n$
$A_1 \cap A_2 \cap \ldots \cap A_n = \emptyset$ partiții

! nr. clase de echivalență = nr. partiții

Un sistem complet de reprezentanți (SCR) cuprinde un element din fiecare clasă de echival.

! Orice $\sim$ partiționează mulțimea și invers

4. Operații algebrice

Perechea $(M, *)$ se numește monoid dacă "$*$" e:
asociativă, are element neutru și parte st.
$(M, *)$ este monoid comutativ dacă e și com.
1_A = element neutru (identitate)

Perechea $(G, \circ)$ se numește grup dacă "$\circ$" e:
asociativă, are parte stabilă, el. neutru și el. inversabil sau simetriz.
$(G, \circ)$ este grup abelian dacă e și comutativ

$U(M)$ = mulțimea elementelor inversabile din M

Monoizi: $(\mathbb{N}, +)$, $(\mathbb{N}, \cdot)$, $(\mathbb{Z}, \cdot)$, $(\mathbb{Q}, \cdot)$, $(\mathbb{R}, \cdot)$, $(\mathbb{C}, \cdot)$,
comutativi: $(P(A), \cup)$, $(P(A), \cap)$

Grupuri: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Z}_n, +)$
com. $(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$

5. Subgrupuri

Fie H o submulțime nevidă a lui G; H este subgrup dacă este parte stabilă și $\forall x \in H$ atunci x^{-1} (invers) $\in H$

Un subgrup ciclic este un subgrup generat de un singur element. Prin definiție: $\langle \emptyset \rangle = \{1_G\}$

! Subgrupurile lui $(\mathbb{Z}, +)$ sunt $n\mathbb{Z}$, $n \in \mathbb{N}$
Toate submulțimile $n\mathbb{Z}$ sunt ciclice

! Un subgrup generat cuprinde și inversele în raport cu operația grupului

! Un grup ciclic este comutativ

- H este subgrup normal al grupului G dacă $x \cdot H = H \cdot x$ $\forall x \in G$ (notăm $H \trianglelefteq G$)

Dacă H e comutativ atunci e normal (nu și invers)

Dacă G e comutativ atunci $\forall$ subgrup e normal

6. Grupul factor

Fie $(G, \cdot)$ un grup și H un subgrup normal atunci $(G/H, \cdot)$ este un grup factor

G/H = mulțimea claselor de echivalență (m. factor)

! Grupul factor $\mathbb{Z}/n\mathbb{Z} = (\mathbb{Z}_n, +)$

Orice grup ciclic infinit este izomorf cu $(\mathbb{Z}, +)$

Orice grup ciclic finit este izomorf cu $(\mathbb{Z}_n, +)$

- Ordinul unui element:

pentru înmulțire

$$\text{ord}(x) = \begin{cases} \infty, & \text{dacă } x^n \neq 1_G \\ t, & \text{dacă } x^t = 1_G, t \text{ minim} \end{cases}$$

$\text{ord}(x) = n < \infty$ atunci $\text{ord}(x^k) = \frac{n}{(n,k)}$, $\text{ord}(\hat{b}) = \frac{n}{(n,b)}$

! Fie p nr. prim atunci orice grup finit de ordin p (lungime p) este ciclic deci izomorf cu $(\mathbb{Z}_p, +)$

! $(\hat{a}, \bar{b}) \in \mathbb{Z}_n \times \mathbb{Z}_m \Rightarrow \text{ord}(\hat{a}, \bar{b}) = [\text{ord}(\hat{a}), \text{ord}(\bar{b})]$
c.m.m.m.c

Pentru $(G, \cdot)$ grup $\text{ord}(G) = |G|$ (cardinalul)

1) $x \in G$, $\text{ord}(x) = n \Rightarrow |\langle x \rangle| = n$

2) $(G, \cdot)$ grup finit $\Rightarrow \text{ord}(x) < \infty$ și $\text{ord}(x) \mid |G|$
(Lagrange)

$Ker(f) = \{x \mid f(x) = 1_G, x \in G\}$

- Teorema fundamentală de izomorfism:
  dacă avem $f : G \to G'$ morfism atunci
  $\exists\ G/Ker(f) \simeq Im f$
- indicele lui H în G, $H \le G$: $[G:H] = \frac{ord(G)}{ord(H)}$

  $ord(1_G) = 1$

! Teorema lui Euler: $a, n \in \mathbb{N}^*$, $(a,n) = 1$ atunci
$a^{\varphi(n)} \equiv 1 \pmod n$ unde $\varphi(n) = n(1-\frac{1}{p_1})\dots(1-\frac{1}{p_k})$
$n = p_1^{a_1} \dots p_k^{a_k}$

! Teorema lui Fermat: p prim, $a \in \mathbb{N}$, $(a,p) = 1$
$a^{p-1} \equiv 1 \pmod p$

7. Permutări

$|S_n| = n!$ permutări de gradul n

dim S_n

$ord(\text{ciclu}) =$ lungime ciclu $\qquad ord(\sigma) \mid n!$

$ord(\sigma) =$ cmmmc lungimilor ciclilor din descompunere

Signatura sau semnul: $sgn(\sigma) = \varepsilon(\sigma) = (-1)^{m(\sigma)}$

$m(\sigma) =$ lungime $(\sigma) - 1$

i câte numere sunt mai mari decât primul

$m(\sigma) =$ nr. de inversiuni

Mulțimea permutărilor pare (A_n) are $|A_n| = \frac{n!}{2}$

! Signatura lui σ este egală cu produsul signaturilor ciclilor din descompunere

! Fie p un număr prim și o permutare de ordin p, aceasta are în descompunere doar cicli de lungime p

! Când ridicăm la puterea k se face pasul k pornind de la primul element iar când nu se poate face pasul se închide ciclul

$ord(\sigma) = n \Rightarrow ord(\sigma^k) = \frac{n}{(n,k)}$

S_n e generat de: $(1\,2), (1\,3), \dots (1\,n)$

$(1\,2), (2\,3), \dots (n-1\ n)$

$(1\,2), (1\,2 \dots n)$ orice $(i\,j)$ și n-ciclu

! $(1\,i)(1\,j) = (1\,j\,i)$

S_n e ciclic dacă $n = 2$ deoarece S_n e necomutativ

! $x^2 = \sigma \cdot \tau$ are soluție dacă σ și τ sunt cicli de lungime pară și egală

nr. de m-cicli din S_n este: $\frac{n(n-1)\dots(n-m+1)}{m}$

8. Inele și corpuri $(a_1 a_2 \dots a_n)^d$ cu $n \vdots d \Rightarrow d$ cicli de lung. n/d

inel $(A, +, \cdot)$ are $(A, +)$ grup abelian, $(A, \cdot)$ monoid și $a(b+c) = a \cdot b + a \cdot c = (b+c) \cdot a$ (distributiv.)

element inversabil = are invers față de înmulț.

inel comutativ = are înmulțirea comutativă

Un inel $(A, +, \cdot)$ este corp ddacă $(A, \cdot)$ grup (el. inv.)

inele comutative: $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Q}, +, \cdot)$, $(\mathbb{R}, +, \cdot)$, $(\mathbb{C}, +, \cdot)$

$U(\mathbb{Z})$, $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ corpuri

($D(A)$ mulț.)

Divizori ai lui zero: $a \in A$ inel a. î. $a \cdot x = 0$, $x \in A, \neq 0$

! 0 e divizor al lui 0 în orice inel nenul

! un element inversabil nu e div. al lui 0

Un inel cu $D(A) = \{0\}$ s.n. domeniu de integritate

Orice corp este domeniu de integritate (el. inv.)

exemple: $(\mathbb{Z}, +, \cdot)$, $(\mathbb{Z}[i], +, \cdot)$ dom. de int., nu corpuri

! orice domeniu de integritate finit e corp

- $B \subseteq A$ submulțime e subinel a lui A dacă: $(B, +) \leq (A, +)$ subgrup, $a \cdot b \in B$, $a, b \in B$, $1 \in B$
- $I \subseteq A$ submulțime e ideal al lui A dacă: $(I, +) \leq (A, +)$ subgrup, $a \cdot x \in I$, $a \in A$, $x \in I$

idealele lui $(\mathbb{Z}, +, \cdot)$ sunt $n\mathbb{Z}$

Orice inel are 2 ideale: $\{0\}$ și A (el însuși)

Un inel e corp dacă are exact 2 ideale

! Fie I, J 2 ideale ale lui $A \Leftarrow$ $I \cap J$ și $I \cap J$ ideale

! Dacă I, J ideale atunci $I \cup J$ ideal $\Leftrightarrow I \subseteq J$ sau $J \subseteq I$

ideal principal = generat de un singur el.

9. ideale

$a\mathbb{Z} \cap b\mathbb{Z} = [a,b]\mathbb{Z}$ cmmmc

$a\mathbb{Z} + b\mathbb{Z} = (a,b)\mathbb{Z}$ cmmdc $\quad a \cdot b = (a,b)\cdot[a,b]$

Produsul direct a două inele $A \times B$:

$(a,b) + (c,d) = (a+c, b+d)$

$(a,b)\cdot(c,d) = (a\cdot c, b\cdot d)$ $\quad$! $(A\times B, +, \cdot)$ inel

cu ideale de forma $I \times J$, I ideal A, J ideal B

Morfism de inele $f: A \to B$ dacă: $f(x+y) = f(x) + f(y)$, $f(x\cdot y) = f(x)\cdot f(y)$, $f(1_A) = 1_B$ (unitar)

inel factor

Fie $(A,+,\cdot)$ un inel și I un ideal al lui A. Cum $(I,+) \trianglelefteq (A,+)$ considerăm grupul factor $(A/I, +)$

cu $\hat{a} + \hat{b} = \widehat{a+b}$, $\hat{a}\cdot\hat{b} = \widehat{a\cdot b}$ $\Rightarrow (A/I, +, \cdot)$ inel factor

T.F.I: $f: A \to B$ morfism de inele atunci: $F(\hat{x}) = f(x)$

$A/\ker f \simeq \operatorname{im} f$ și $F: A/\ker f \to \operatorname{im} f$ izomorf.

Corolar: Lema chineză a resturilor (LCR)

$\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n \quad (m,n) = 1$

Aplicație: sistem de forma

$$\begin{cases} x \equiv a_1 \bmod m_1 \\ x \equiv a_2 \bmod m_2 \\ \dots \\ x \equiv a_k \bmod m_k \end{cases}$$

$m_i \in \mathbb{N}, m_i \geq 2$, $(m_i, m_j) = 1, \forall i \neq j$

$m = m_1 \cdot m_2 \cdot \ldots \cdot m_k$

$m_i' = \dfrac{m}{m_i}$, $i = \overline{1,k}$

t_i = inversul lui m_i' mod m_i

soluție unică:

$x = (a_1 t_1 m_1' + a_2 t_2 m_2' + \ldots + a_k t_k m_k') \bmod m$

10. inele de polinoame $\quad (A[x], +, \cdot)$

$A[x] = \{ a_0 + a_1 x + \ldots + a_n x^n \mid n \in \mathbb{Z}, a_0, \ldots a_n \in A \}$

grad(f) = cel mai mare nr. k a.î. $a_k \neq 0$ ← coeficient dominant

! gradul polinomului nul este $-\infty$

1) $\text{grad}(f+g) \leq \max\{\text{grad}(f), \text{grad}(g)\}$ $\quad f, g$ nenule

2) $\text{grad}(f\cdot g) \leq \text{grad}(f) + \text{grad}(g)$

= dacă $a_n \cdot b_n \neq 0$

Dacă A e corp comutativ atunci $A[x]$ e domeniu de integritate și $U(A[x]) = A \setminus \{0\}$ (polinoame const.)

T.Î.R: $f(x), g(x) \in K[x]$, $g(x) \neq 0$ atunci: $f(x) = g(x) \cdot q(x) + r$ unde $q(x), r(x) \in K[x]$ și $grad(r(x)) < grad(g(x))$

Teorema lui Bezout: $f(x) = q(x) \cdot (x-a) + f(a)$ = rest

sau $f(x) \vdots (x-a) \Rightarrow f(a) = 0$

Rădăcina multiplă a de ordin l: dacă $f(x) = (x-a)^l \cdot g(x)$
$g(\ ) \neq 0$

Pentru $f(x) \in K[x]$, $grad(f) = n$, rădăcini $\alpha_1, \dots, \alpha_r$ cu ord. de multiplicitate $m_1, \dots, m_r$

$$f(x) = (x-\alpha_1)^{m_1} \cdot (x-\alpha_2)^{m_2} \cdot \dots \cdot (x-\alpha_r)^{m_r}$$

$n = m_1 + m_2 + \dots + m_r$ = nr. rădăcini

T.F.A: un polinom $f(x) \in \mathbb{C}[x]$ are exact $grad(f(x))$ rădăcini (nu $\mathbb{Q}$ sau $\mathbb{R}$)

Fie K un corp și $f(x) \in K[x]$ un polinom neconstant inelul factor $K[x]/f(x)$ are forma:

$$a_0 + a_1 x + \dots + a_{n-1} x^{n-1} \ (\text{mod } f)$$

$K[x]/x^n$ = mult. tuturor resturilor pos. la împ. cu x^n

SCR = mult. tuturor polinoamelor de grad. max. $n-1$

! Dacă $K = \mathbb{Z}_p$ (prim) atunci $K[x]/f$ are p^n elemente

T.F.i (aplicație): $\mathbb{Z}[x]/(x^2-p) \overset{\varphi}{\simeq} \mathbb{Z}[\sqrt{p}]$, p prim

$Ker\ \varphi = (x^2 - p)$ inele

Relațiile lui Viete:

$f(x) = a_n(x-\alpha_1)\dots(x-\alpha_n)$

$\alpha_1, \alpha_2, \dots \alpha_n$ rădăcini

$a_3 x^3 + a_2 x^2 + a_1 x + a_0 = 0$

$s_1 = x_1 + x_2 + x_3 = (-1)^1 \frac{a_2}{a_3}$

$s_2 = x_1 x_2 + x_1 x_3 + x_2 \cdot x_3 = \frac{a_1}{a_3} \cdot (-1)^2$

$s_3 = x_1 \cdot x_2 \cdot x_3 = (-1)^3 \frac{a_0}{a_3}$

$S^* = s_1^2 - 2s_2$

$S^* < 0 \Rightarrow$ cel puțin 2 sol. complexe

Pentru $f(x) \in K[X]$ un SCR este:

$$\{a_0 + a_1 x + \dots + a_{m-1} x^{m-1} \mid a_0, a_1, \dots, a_{m-1} \in K\}$$

- Orice ideal al lui $K[x]$ e principal
- $U(K[x])$ e domeniu de integritate : $U(K[x]) = K^*$
- LCR: $K[x]/_{(f \cdot g)} \simeq K[x]/f \times K[x]/g$

Algoritmul lui Euclid:

$a, b \in \mathbb{Z}$, $b \neq 0$

$a = b \cdot q_1 + r_1$

$b = r_1 \cdot q_2 + r_2$

...

$r_{t-1} = r_t \cdot q_{t+1} + r_{t+1}$

$r_t = r_{t+1} \cdot q_{t+2} + 0$

cmmdc $(a,b) = r_{t+1}$

$r_{t+1} = a \cdot k + b \cdot l$

$(a,b) = 1 \Rightarrow \exists\, a', b' \in \mathbb{Z}$

a.î. $a \cdot a' + b \cdot b' = 1$

11. Polinoame ireductibile

$f(x) \in K[x]$ ireduct. dacă nu se poate scrie ca produs de 2 polinoame neconstante

! Polinoamele de gradul 1 sunt ireductibile

Un polinom de grad ≥ 2 ireduct. nu are rădăcini în K

Teorema lui Euclid: orice polinom neconstant se poate scrie ca produs de polinoame ireductibile

sau

orice număr întreg se poate scrie ca produs de numere prime în mod unic

1) Polinoamele ireductibile din $\mathbb{C}[x]$ sunt de gr. 1
2) Polinoamele ired. din $\mathbb{R}[x]$ sunt cele de gradul 1 și cele de gradul 2 fără soluții reale
3) în $\mathbb{Q}[x]$ polinoamele ireduc. sunt de orice grad

Mulțimea polinoamelor ireductibile e infinită

Mulțimea nr. prime este infinită