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 $P(A)$ $\Rightarrow |P(A)| = 2^m$

m = 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.m. numărabilă

2. Funcții

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

C_b^a = nr. fcț. s. crescătoare

C_{b+a-1}^{a} = nr. fcț. crescătoare

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 = $\text{im}(f)$

nr. funcții = n^m

nr. bijecții = $n!$

nr. surjecții = $n^m - C_n^1 (n-1)^m + C_n^2 (n-2)^m + \ldots + (-1)^{n-1} C_n^{n-1}$

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

! 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:

$$a \equiv b \pmod n \iff n \mid a-b$$

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

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

$$A = A_1 \cup A_2 \cup \dots \cup A_m$$
$$A_1 \cap A_2 \cap \dots \cap A_m = \varnothing \quad \text{partiții}$$

! nr. clase de echivalență = nr. partiții

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

! Orice ~ 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: $(\mathbb{Z}, +)$, $(\mathbb{Q}, +)$, $(\mathbb{R}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Z}_n, +)$ comm.
$(\mathbb{Q}^*, \cdot)$, $(\mathbb{R}^*, \cdot)$, $(\mathbb{C}^*, \cdot)$

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 conține 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

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

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

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

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

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

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

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

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

- Teorema fundamentală de izomorfism:
  dacă avem $f: G \to G'$ morfism atunci
  $\exists\ G/\ker(f) \cong \text{im } f$

- indicele lui H în G, $H \leq G$: $[G:H] = \frac{ord(G)}{ord(H)}$

$ord(1_G) = 1$

! **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(ciclu) = lungimea ciclu — ord(τ) | $n!$

ord(τ) = cmmmc lungimilor ciclilor din descompunere

Signatura sau **semnul**: $sgn(\tau) = \varepsilon(\tau) = (-1)^{m(\tau)}$
$m(\tau)$ = lungime(τ) − 1
= câte numere sunt mai mari decât primul

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

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

! Signatura lui τ 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

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

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

! $x^2 = \tau \cdot \sigma$ are soluție dacă τ și σ 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. Imcle și corpuri $(a_1 a_2 \dots a_n)^d$ cu $n:d \Rightarrow d$ cicli de lung. n/d

Imcl $(A, +, \cdot)$ 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 înmult.

imcl comutativ = are înmulțirea comutativă

Un imcl $(A, +, \cdot)$ este corp ddacă $(A, \cdot)$ grup (d. inv.)

imcle 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

Divizori ai lui zero: $a \in A$ imcl a. î. $a \cdot x = 0$, $x \in A, \neq 0$ ($D(A)$ mult.)

! 0 e divizor al lui 0 în orice imcl nenul

! un element inversabil nu e div. al lui 0

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

Orice corp este domeniu de integritate (d. 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 subimcl 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 imcl are 2 ideale: $\{0\}$ și A (cl însuși)

Un imcl e corp dacă are exact 2 ideale

! Fie i, J 2 ideale ale lui A $\Leftrightarrow$ $i \cap J$ 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 dirct a două inele $A \times B$:

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

$(a,b) \cdot (c,d) = (a \cdot c, b \cdot d)$! $(A \times B, +, \cdot)$ 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 idcal 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: $F(\hat{x}) = f(x)$

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

Corolar: Lema chinezească a resturilor (**LCR**)

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

Aplicație: **sistem de forma**

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

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

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

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

t_i = inversul lui m_i' mod m_i

soluție unică:

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

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

$A[X] = \{ a_0 + a_1 X + \dots + a_m X^m \mid m \in \mathbb{Z}, a_0, \dots a_m \in A \}$

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

! gradul polinomului nul este $-\infty$

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

2) grad $(f \cdot g) \leq$ grad (f) + grad (g) f, g nenule

= dacă $a_m \cdot b_n \neq 0$

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 $f(X) : (X-a) \Rightarrow f(a) = 0$

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

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

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

$$m = m_1 + m_2 + \dots + m_r = m \text{ rădăcini}$$

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:

$$a_0 + a_1 X + \dots + a_{m-1} X^{m-1} \pmod f$$

$K[X] / X^m$ = mult. tuturor resturilor pos. la împ. cu X^m
SCR = mult. tuturor polinoamelor de grad. max. $m-1$

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

T. F. I (aplicație): $\mathbb{Z}[X]/(X^2-p) \overset{\varphi}{\cong} \mathbb{Z}[\sqrt{p}]$, p prim
$\ker \varphi = (X^2-p)$ ↖ incl

Relațiile lui Viete:

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

$$f(X) = a_m (X-x_1)\dots(X-x_m)$$

$x_1, x_2, \dots x_m$ rădăcini

$$S_1 = x_1 + x_2 + x_3 = (-1)^1 \frac{a_2}{a_3}$$

$$S_2 = x_1x_2 + x_1x_3 + x_2 \cdot x_3 = \frac{a_1}{a_3} \cdot (-1)^2$$

$$S_3 = x_1 \cdot x_2 \cdot x_3 = (-1)^3 \frac{a_0}{a_3}$$

$$S^* = S_1^2 - 2S_2$$

$S^* < 0 \Rightarrow$ 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