

Aurelian Claudiu VOLF

Structuri algebrice și aplicații

Universitatea „Al. I. Cuza” Iași

2004

(ultima modificare: 22 februarie 2007)

Cuprins

Cuprins	2
Către cititor	4
Prefață	5
I. Logică, mulțimi, axiome	8
I.1. Limbaj formal, logică	10
I.2. Axiomatica mulțimilor	15
I.3. Clase, relații, funcții	18
I.4. Ordinale, axioma infinității și mulțimea numerelor naturale.....	27
I.5. Comentarii și completări privind axiomatica mulțimilor	36
Exerciții.....	40
II. Mulțimi factor și construcții de structuri numerice fundamentale	42
II.1. Relații de echivalență și mulțimi factor.....	42
II.2. Inelul numerelor întregi.....	44
II.3. Corpul numerelor raționale. Inele și corpuri de fracții	46
Exerciții.....	51
II.4. Inele de clase de resturi $\mathbb{Z}_n$, inele factor	52
II.5. Corpul numerelor reale.....	59
Exerciții.....	66
III. Polinoame, corpul complex și extinderi de corpuri	68
III.1 Algebre. Algebre monoidale și algebre polinomiale	69

III.2 Corpul numerelor complexe construit ca inel factor.....	78
III.3 Corpuri finite și criptografie	85
Exerciții.....	90
III.4 Polinoame simetrice.....	91
IV. Aritmetică în inele și aplicații	96
IV.1 Divizibilitate	96
IV.2 Algoritmul lui Euclid, teorema fundamentală a aritmeticii	101
IV.3 Ireductibilitate în inele polinomiale.....	108
Exerciții.....	115
V. Spații liniare, matrice și aplicații.....	120
V.1 Algebre de matrice	120
V.2 Coduri liniare corectoare de erori	122
Exerciții.....	134
VI. Acțiuni ale grupurilor	136
VI.1. Acțiuni ale grupurilor pe mulțimi	136
Exerciții.....	142
Index	143
Bibliografie.....	148

Către cititor

Acest curs poate fi citit de un absolvent al anului I al Facultății de Matematică. Sînt presupuse cunoscute: noțiuni generale despre structuri algebrice (monoid, grup, inel, corp), construcția grupului factor, a inelului factor, noțiuni de bază despre spații vectoriale, matrice, polinoame, noțiuni elementare despre grupurile de permutări, aritmetica elementară a cardinalelor. Există un număr relativ mare de cărți și cursuri în literatura matematică românească în care se tratează aceste lucruri. Unele direcții de aprofundare sînt indicate prin referințe bibliografice.

Parcurgerea unui text matematic este un proces *activ* prin excelență. În primul rînd, toate definițiile nou introduse trebuie să capete rapid un suport intuitiv și să fie legate de noțiunile deja cunoscute prin căutarea de exemple (și contraexemple) de obiecte care să satisfacă definițiile. În plus, cititorul trebuie să *verifice* pe cazuri concrete și să *demonstreze* afirmațiile din text. În particular, toate aparițiile unor fraze de tipul „se verifică ușor că ...”, „evident, ...”, ... sînt o invitație la demonstrarea efectivă a afirmațiilor respective. Aceste exerciții intelectuale sînt un pas indispensabil spre asimilarea conceptelor și tehnicilor introduse și, totodată, o verificare a înțelegerii de către cititor a textului.

Paragrafele care au o bară la stînga sînt foarte importante pentru înțelegerea textului. Dacă merită reținută doar o singură frază dintr-o anumită secțiune, aceasta ar trebui să fie fraza marcată în acest mod.

Peste tot, în text:

- $|A|$ desemnează cardinalul mulțimii A (numărul elementelor lui A , dacă A este finită).
- $x := y$ înseamnă „ x este egal prin definiție cu y ” (unde y este deja definit) sau „notăm pe y cu x ”.
- $\square$ marchează sfîrșitul sau absența unei demonstrații.

Prefață

Matematica are o reputație de disciplină aridă, abstractă, greu de asimilat, cu aplicabilitate restrânsă. De multe ori, cei care o studiază – de voie sau de nevoie – (își) pun întrebări de genul „la ce folosesc toate aceste definiții, notații, axiome, teoreme, ...?”. Dintre ramurile matematicii, algebra excelează în această direcție, în special algebra „abstractă” (sau „axiomatică”, sau încă „modernă”), care se ocupă de *structurile algebrice*.

De unde provine această reputație? Convingerea noastră este că ea se formează din experiența contactelor cu algebra din cursul gimnaziului și liceului. Adesea, însuși profesorul de matematică nu este foarte convins de utilitatea studiului anumitor noțiuni și, în consecință, transmite elevilor doar o imagine formală și seacă, din care motivațiile, exemplele și aplicațiile sînt neglijate sau absente cu totul (uneori este „de vină” volumul mare de cunoștințe ce trebuie predat). Doar o cunoaștere aprofundată a conceptelor, care nu are cum să fie cantonată la nivelul unui manual de liceu, poate duce la conceperea unor lecții atractive, în care noțiunile nu sînt introduse în mod artificial, ci sînt însoțite permanent de exemple și aplicații.

Unul din scopurile rîndurilor ce urmează este de a aduce argumente în sprijinul ideii că structurile algebrice, departe de a fi creații teoretice și auto-suficiente, au apărut în mod natural, au un rol determinant în fundamentarea, simplificarea și unificarea matematicii și au aplicații consistente în practică și în matematica însăși.

Un alt scop al lucrării este de a oferi profesorilor de matematică un material care să arate că algebra este apropiată de realitate și să îi convingă de frumusețea și aplicabilitatea ei. De aceea, s-a avut în vedere și latura didactică, punîndu-se accentul pe noțiunile care au legătură directă cu matematica studiată în învățămîntul preuniversitar.

Lucrarea se adresează studenților Facultăților de Matematică, profesorilor de matematică și, în general, oricărui cititor interesat de algebră.

Titlul acestei lucrări face referire la Algebră. *Ce este însă algebra?* Încercăm să dăm un răspuns la această întrebare, după o argumentație a lui I.R. Shafarevich (KOSTRIKIN, SHAFAREVICH [1990]), care reia o idee a lui Hermann Weyl¹.

¹ Matematician german (1885-1955).

În procesul de cunoaștere a lumii fizice sînt esențiale procedee de *măsurare* și de *structurare*, care permit ca impresiile subiective ale indivizilor umani să fie traduse în entități obiective, cel mai adesea în *numere*. Aceste entități, cu toate că nu redau integral experiența subiectivă, pot fi păstrate și transmise nealterate. Mai mult, cu rezultatele măsurătorilor se pot face diverse *operații* (mai general, se pot *structura*), în scopul extragerii de noi informații, de a face predicții etc. Spre exemplu, structura matematică $\mathbb{N}$ a *numerelor naturale* este adecvată măsurării „mărimii” mulțimilor finite (făcînd abstracție de natura elementelor lor). *Numerele raționale*² au fost construite din motive evidente de măsurare a diverselor „mărimi fracționare”, dar s-au dovedit incapabile de a măsura obiecte geometrice simple, cum este diagonala unui pătrat de latură 1. Astfel a apărut necesitatea construcției *numerelor iraționale*³ și, ulterior, a *numerelor reale*. *Numerele complexe* au avut o geneză asemănătoare, între altele din nevoia de a rezolva ecuații algebrice care nu au soluții reale. S-au imaginat și alte extinderi ale conceptului de număr (*numerele cardinale* și *numerele ordinale* sînt generalizări ale numerelor naturale; *cuaternionii* generalizează numerele complexe etc.).

Structura matematică $\mathbb{R}$ (corpul total ordonat al numerelor reale) este folosită pentru exprimarea multor mărimi fizice (lungimi, intensități, ...). Cu ajutorul mulțimilor numerice (cel mai adesea $\mathbb{R}$) se pot construi structuri care pot măsura (un termen mai adecvat ar fi *coordonatiza*) multe obiecte și fenomene. De pildă, spațiul liniar $\mathbb{R}^3$ modelează (cu ajutorul coordonatelor carteziane) *spațiul fizic*.

Extinderile succesive ale conceptului de număr (mai bine zis, construcțiile de structuri numerice din ce în ce mai largi) nu pot însă fi adecvate tuturor nevoilor de coordonatizare care pot apărea. De exemplu, „măsurarea” *simetriei* figurilor plane este cel mai bine realizată prin structura algebrică de *grup*: fiecărei figuri i se atașează grupul său de simetrie (format din acele izometrii ale planului care invariază figura dată). Clasificarea *cristalelor* se realizează tot cu ajutorul grupurilor lor de simetrie. În mecanica cuantică, *spațiile Hilbert complexe* descriu sistemele cuantice: o stare a unui sistem cuantic este identificată cu un vector de normă 1 într-un astfel de spațiu.

Un alt exemplu este dat de *curbele plane*: o *curbă ireductibilă* C în $\mathbb{R}^2$ este mulțimea punctelor (x, y) din plan care satisfac ecuația $F(x, y) = 0$, unde $F \in \mathbb{R}[X, Y]$ este un polinom ireductibil fixat. Se presupune că curba C are o infinitate de puncte (se exclud deci curbe de tipul $x^2 + y^2 = 0$, care conține un singur punct). Atunci curbei C (polinomului F) i se asociază *corpul funcțiilor raționale pe C* , care în limbaj algebric modern poate fi descris ca fiind corpul de fracții al inelului integru $\mathbb{R}[X, Y]/(F)$. Acest corp reflectă proprietăți geometrice importante ale curbei C . În plus, prin schimbarea coordonatelor în care exprimăm ecuația curbei C , polinomul F se schimbă, însă noul corp al funcțiilor raționale este izomorf cu cel inițial. Iată

² De la *ratio*, care înseamnă raport (în latină).

³ Denumirea de număr *irațional* provine de la faptul că acel număr nu poate fi exprimat ca un raport (*ratio*).

un exemplu de proprietate a curbei care este reflectată în structura algebrică a corpului funcțiilor raționale pe curbă. Curbele care pot fi parametrizate prin funcții raționale (adică există două funcții raționale $f, g : \mathbb{R} \rightarrow \mathbb{R}$ astfel încât $F(f(t), g(t)) = 0$ pentru toți t , cu excepția unui număr finit și $\forall (x, y)$ cu $F(x, y) = 0$ (cu excepția unui număr finit), $\exists t \in \mathbb{R}$ cu $(x, y) = (f(t), g(t))$) sînt caracterizate de faptul că li se asociază un corp izomorf cu $\mathbb{R}(t)$ (corpul fracțiilor raționale cu coeficienți reali). Desigur, această construcție poate fi generalizată la alte corpuri decît $\mathbb{R}$ și dimensiuni mai mari decît 2.

Se poate concluziona că:

În studiul obiectelor fizice sau abstracte apare nevoia de măsurare (coordonatizare) a fenomenelor sau a anumitor proprietăți ale obiectelor. Procesul de coordonatizare asociază fiecărui obiect (fenomen, proprietate...) o structură matematică (grup, inel, corp, spațiu Hilbert...), care descrie, total sau parțial, obiectul respectiv sau unele caracteristici ale sale.

Aceste considerații conduc la enunțarea următoarei descrieri de natură generală - și inerent vagă - a Algebrei :

Obiectul de studiu al Algebrei este construcția și studiul structurilor matematice apărute în acest mod.

I. Logică, mulțimi, axiome

Includerea capitolului privind logica și teoria mulțimilor pornește de la premisa că un profesor de matematică nu se poate limita la punctul de vedere al unui manual de liceu, fiind necesară o viziune mai profundă asupra acestor tematici.

Mulțimile apar ca obiecte matematice foarte devreme în învățământul modern, sub o formă intuitivă (în varianta teoriei naive a mulțimilor). Este exclusă o tratare axiomatică a teoriei mulțimilor la nivel preuniversitar; totuși, un profesor de matematică trebuie să fie familiarizat cu conceptele ei de bază și să înțeleagă utilitatea, necesitatea și mecanismele teoriei axiomatică a mulțimilor.

Teoria modernă a mulțimilor începe odată cu lucrarea „Teoria rațională a infinității” a lui Georg Cantor⁴, în care se manevrează liber *mulțimile infinite* și se dezvoltă o tehnică de măsurare a lor (teoria cardinalelor). Până la Cantor, matematicienii adoptau punctul de vedere al filozofilor Greciei antice: există noțiunea de *infinit actual* (o infinitate de obiecte concepute ca existând simultan) și cea de *infinit potențial* (o mulțime sau o mărime finită, dar care se poate mări oricât de mult). Filozoful Zenon, prin faimoasele sale aporii (paradoxuri) a atras atenția asupra consecințelor absurde care par să apară introducând infinitul actual în raționamente. Se considera de aceea că infinitul actual nu este accesibil intuiției și doar infinitul potențial poate fi folosit în gândirea matematică.

Cantor are meritul de a fi spart această barieră mentală și de a fi încercat să „numere infinitul”. El a avut ideea de a compara mulțimile (finite sau nu) cu ajutorul *funcțiilor bijective*: două mulțimi sînt „la fel de mari” (echipotente) dacă există o bijecție între ele. Cantor a obținut rezultate precum: $\mathbb{N}$ este echipotent cu $\mathbb{Q}$ și cu mulțimea numerelor algebrice (numerele complexe care sînt rădăcini ale unui polinom nenul cu coeficienți raționali). Deja aceste afirmații nu sînt în acord cu percepția obișnuită și arată că uneori „partea este la fel de mare ca și întregul”. A mai arătat că $\mathbb{N}$ nu este echipotent cu $\mathbb{R}$; în general, o mulțime A nu este echipotentă cu mulțimea părților sale $\mathcal{P}(A)$. Există, deci, mai multe tipuri de infinitate. Alte rezultate contrazic și mai mult simțul comun: există tot atîtea puncte pe un segment cîte sînt pe o dreaptă sau în întregul plan sau în întregul spațiu!

⁴ Georg Ferdinand Ludwig Philipp Cantor (1845-1918), matematician german.

În cadrul teoriei lui Cantor a mulțimilor (astăzi numită „naivă”), prin *mulțime* se înțelege o colecție (un ansamblu, un set) de obiecte distincte (*elementele* mulțimii) bine determinată și considerată ca o entitate. Georg Cantor spunea „*Unter eine Menge verstehen wir jede Zusammenfassung M von bestimmten Wohlunterschiedenen Objekten m unseres Denkens zu einem Ganzen*”: „Prin *mulțime* înțelegem orice grupare într-un tot M a unor obiecte distincte și bine determinate m ale gândirii noastre”.

Însă teoria mulțimilor în forma descrisă de Cantor conducea la *paradoxuri* care provin din „definiția” foarte permisivă și vagă a conceptului de mulțime. Însuși Cantor în 1895 observă că nu se poate vorbi de „mulțimea tuturor ordinalelor” (paradox publicat de Burali-Forti în 1897); mai târziu, s-a constatat că există și alte „mulțimi contradictorii”: „mulțimea tuturor cardinalilor”, „mulțimea tuturor mulțimilor”, „mulțimea mulțimilor care nu se conțin ca element” (paradoxul lui Russel⁵). Prezentăm acest paradox: presupunem că există mulțimea mulțimilor care nu se conțin ca element și o notăm cu C (în notație modernă, $C = \{A \mid A \notin A\}$). Evident, are loc: sau $C \in C$, sau $C \notin C$. Dacă $C \in C$, atunci $C \notin C$ din definiția lui C , contradicție. Dacă $C \notin C$, atunci C nu satisface condiția de definiție a lui C , deci $C \in C$, contradicție.

Aceste paradoxuri au putut fi eliminate de *teoria axiomatică a mulțimilor*, care stabilește *reguli clare de construcție de mulțimi*. Printre altele, nu se permite considerarea mulțimilor „foarte mari”, care apar mai sus. O primă axiomatizare a fost dată de Zermelo⁶ în 1908. Una din axiomele sale (care evită apariția paradoxurilor de tipul de mai sus) este *Axioma selecției*, care în esență spune că, dată o „proprietate” P și o mulțime A , există „mulțimea elementelor din A care satisfac proprietatea P ”. Cu alte cuvinte, o proprietate nu determină o mulțime (ca în definiția originală a lui Cantor), ci, dată o mulțime A , se poate vorbi doar de existența *submulțimii* formată de elementele lui A care satisfac P .

În 1905 Richard construiește un paradox de alt tip (simplificat ulterior de Berry și publicat de Russel în 1906). Să considerăm următorul concept: „cel mai mic număr natural care nu poate fi definit cu mai puțin de 17 cuvinte”. Dacă acest număr ar exista, atunci el *poate fi definit cu 16 cuvinte*, chiar de enunțul anterior (care are 16 cuvinte, numărați). Contradicția obținută arată că nu există un astfel de număr. Pe de altă parte, mulțimea numerelor naturale care pot fi definite cu cel mult 16 cuvinte este finită (căci mulțimea frazelor cu cel mult 16 cuvinte care definesc un număr natural este finită) și deci *există* numere naturale care nu pot fi definite cu mai puțin de 17 cuvinte. Cel mai mic dintre acestea este un număr... care nu poate exista, conform celor de mai sus!

⁵ Bertrand Russel (1872-1970), matematician și filozof britanic.

⁶ Ernst Friedrich Ferdinand Zermelo (1871-1953), matematician german.

⁷ Mai precis, este vorba de un predicat cu o variabilă liberă.

Paradoxul de mai sus are altă sursă, și anume *ambiguitatea limbajului* natural, obișnuit. Ce înseamnă exact *a defini* un număr natural?

Din cele spuse reiese că, pe lângă o axiomatizare a teoriei mulțimilor, trebuie *restrîns limbajul natural* la cîteva modalități bine precizate și simple de exprimare. În același timp, posibilitățile trebuie să fie suficient de permissive pentru a putea formula orice enunț matematic. Aceste scopuri sînt realizate de un *limbaj formalizat*.

Vom prezenta intuitiv un astfel de limbaj (o prezentare riguroasă depășește cu mult cadrul și scopul acestei cărți). Cu această ocazie, vom sublinia anumite aspecte de logică matematică. În continuare vom descrie axiomele teoriei mulțimilor, aplicații (ordinale și numere naturale). Vom încerca să reliefăm și modul în care aceste axiome trebuie conștientizate în procesul didactic.

I.1. Limbaj formal, logică

Un minim de cunoștințe privind logica este indispensabil oricărui individ, cu atît mai mult profesorilor de matematică. În manualele de matematică există un capitol dedicat logicii, în clasa a IX-a. Noțiunile și tehnicile de logică sînt bine alese, în general bine prezentate, și ar trebui să fie cunoscute de toți elevii și profesorii. Din păcate, de multe ori acest capitol este privit drept ceva exotic, preferîndu-se o reducere a sa în favoarea unor teme precum funcția de gradul II, lângă care coexistă – cel puțin temporal. O asemenea alegere facilă este oarecum justificată: e mai ușor de predat o serie de formule și rețete care solicită mai mult memoria, decît de a încerca o adevărată *formare* a unei gândiri logice la elevi. Desigur, o astfel de formare nu se realizează doar prin cîteva lecții în clasa a IX-a, ci trebuie văzută ca un obiectiv permanent al lecțiilor de matematică. Existența unor deficiențe în gîndirea logică a elevilor este o chestiune serioasă, care se reflectă nu numai în matematică, ci în orice domeniu: apar dificultăți în înțelegerea legăturilor între diversele noțiuni, se confundă definițiile cu teoremele; în cele din urmă este compromisă însăși comunicarea coerentă și înțelegerea informațiilor uzuale.

În teoria axiomatică a mulțimilor (axiomatizarea Zermelo-Fraenkel-Skolem, acceptată în cvasitotalitatea matematicii moderne) *toate obiectele sînt mulțimi*. Altfel spus, *nu se face distincție între conceptele „element” și „mulțime”*. Acest punct de vedere este firesc, dacă ne gîndim că o mulțime poate fi element al altei mulțimi; în plus, o teorie axiomatică trebuie să pornească de la un minim de noțiuni primare, iar distincția între element și mulțime ar complica lucrurile inutil.

Pentru a putea enunța axiomele teoriei mulțimilor, avem nevoie de prezentarea (intuitivă) a limbajului formal al acestei teorii. Subliniem că nu este vorba de o formalizare propriu-zisă. Un limbaj formal prezentat riguros ar ocupa zeci de pagini (un exemplu de formalizare, în cadrul axiomatizării von Neumann-Gödel-Bernays a teoriei mulțimilor, poate fi găsit în REGHIȘ [1981]). Mai întâi descriem *sintaxa limbajului* (regulile după care putem forma expresii corecte ale limbajului formal).

1.1 Definiție. Un *enunț* al limbajului formal (numit și *expresie* a limbajului formal) este un șir finit de *simboluri*, format după anumite reguli descrise mai jos. Intuitiv, un enunț exprimă un fapt bine determinat despre obiectele la care se referă (în cazul nostru, toate obiectele sînt mulțimi).

Descriem acum tipurile de simboluri și construcția expresiilor limbajului formal :

i) Există simboluri de tip nume, care denumesc *mulțimi* (acestea sînt singurele obiecte pe care le considerăm!). Numele sînt de două feluri: un *nume constant* (pe scurt, *o constantă*) se referă la un obiect bine precizat, iar un *nume variabil* (pe scurt, *o variabilă*) notează un obiect generic (arbitrar, neprecizat). Se presupune că avem la dispoziție o colecție suficient de mare de nume constante și variabile. Exemple de nume: $x, y, a, b, c, A, B, \dots$

ii) Simbolurile care notează relații: relația de *egalitate*, notată cu simbolul $=$, și relația de apartenență, notată cu simbolul $\in$. Dacă x, y sînt nume (constante sau variabile), atunci următoarele șiruri de simboluri sînt *expresii* ale limbajului formal:

$x = y$ (citit „ x este egal cu y ”);

$x \in y$ (citit „ x aparține lui y ” sau „ x este element al lui y ”).

iii) Conectorii logici se folosesc pentru a exprima proprietăți mai complexe, pentru a combina mai multe expresii într-una nouă. Conectorii sînt: $\wedge$ (conjuncția, „și”), $\vee$ (disjuncția, „sau”), $\neg$ (negația, „non”). Dacă E, F sînt expresii (deja construite), atunci sînt expresii și următoarele șiruri de simboluri:

$E \wedge F$ (citită „ E și F ”);

$E \vee F$ (citită „ E sau F ”);

$\neg E$ (citită „non E ”).

iv) Cuantificatorii logici sînt: $\forall$ (cuantificatorul universal, „oricare”), $\exists$ (cuantificatorul existențial, „există”). Cu ajutorul cuantificatorilor (numiți uneori și *cuantori*) se precizează dacă, într-o expresie, o variabilă se referă la *toate obiectele* sau la *măcar un obiect*. Dacă E este o expresie a limbajului și x este o variabilă, atunci:

$(\forall x)E$ este expresie (citită „pentru orice x are loc E ” sau „pentru orice x , E este adevărată”);

$(\exists x)E$ este expresie (citită „există x astfel încît are loc E ” sau „există x astfel încît E este adevărată”).

v) Parantezele rotunde (și) au rolul de a elimina ambiguitățile. Astfel, în construcțiile precedente, se scrie de exemplu $(E) \wedge (F)$ în loc de $E \wedge F$, sau $(\forall x)(E)$ în loc de $(\forall x)E$ dacă pot

apărea confuzii. Uneori, pentru un plus de claritate, se folosesc și parantezele pătrate [] sau acoladele { }.

Singurele expresii (enunțuri) admise ale limbajului formal sînt cele construite respectînd regulile de mai sus.

Variabilele unei expresii pot fi *libere* sau *legate*. Spunem că *variabila x este liberă în expresia E* dacă x apare în E , dar E nu conține nici o cuantificare a lui x (adică nici $\forall x$, nici $\exists x$ nu apar în E). Spunem că *variabila x este legată în E* dacă E conține un subșir de simboluri de forma $(\forall x)F$ sau $(\exists x)F$ (unde F este o expresie).

Dacă expresia E conține variabilele *libere* $x_1, \dots, x_n$, vom sublinia uneori acest lucru scriind $E(x_1, \dots, x_n)$. Fiind date constantele $c_1, \dots, c_n$, prin înlocuirea peste tot în E a variabilei x_1 cu c_1 , a lui x_2 cu c_2 , ..., a lui x_n cu c_n se obține o nouă expresie (demonstrați!), notată cu $E(c_1, \dots, c_n)$. Dacă $x_1, \dots, x_n$ sînt *toate* variabilele libere din E , atunci $E(c_1, \dots, c_n)$ este o *propoziție* (adică o expresie care nu are variabile libere). O expresie care are variabile libere se mai numește *predicat*.

Vom reveni asupra problemei variabilelor libere sau legate, care are o mare importanță în modul de scriere a enunțurilor matematice.

1.2 Exemple. Presupunem că x, y, z sînt variabile și a, b sînt constante. Arătați că următoarele șiruri de simboluri sînt expresii: $x \in y$; $(\forall x)(x \in y)$; $(a \in b) \wedge (x = y)$; $\neg((a \in b) \wedge (x = y))$; $(\forall z)(\exists y)(x \in y)$. Care sînt variabilele libere din fiecare? Șirurile de simboluri: $x(\forall y)$; $x = \in$; $\forall y$ nu sînt expresii corecte ale limbajului formal (de ce?).

Să trecem acum la **interpretarea sensului expresiilor (semantica limbajului)**. Reamintim că o expresie care nu conține variabile libere se numește *propoziție*. Oricărei *propoziții* îi asociem o unică *valoare de adevăr*. Valorile de adevăr sînt: 0 (sau *fals*), și 1 (sau *adevărat*). O propoziție cu valoarea de adevăr 0 se numește *propoziție falsă*; o propoziție cu valoarea de adevăr 1 se numește *propoziție adevărată*. O propoziție nu poate fi simultan falsă și adevărată). Descriem acum *regulile* prin care se determină valoarea de adevăr a unei propoziții⁸ date.

Fie a, b constante și x, y variabile.

- i) Propozițiile de forma $a = b$ sînt adevărate exact atunci cînd a și b denumesc același obiect.
- ii) Valoarea de adevăr a propozițiilor de forma $a \in b$ nu poate fi precizată acum; acest lucru este descris de axiome (în paragraful următor). Evident, intuitiv, $a \in b$ este

⁸ Subliniem că doar *propozițiile* au valori de adevăr. Unei expresii cu variabile libere nu i se dă nici o valoare de adevăr.

adevărată dacă și numai dacă obiectul numit de a este un element al obiectului numit de b .

- iii) O propoziție de forma $E \wedge F$ (unde E și F sînt propoziții) este adevărată dacă și numai dacă E și F sînt *ambele* adevărate.
- iv) O propoziție de forma $E \vee F$ este adevărată dacă și numai dacă *măcar una* din propozițiile E și F este adevărată (adică sau E , sau F , sau atît E cît și F sînt adevărate).
- v) O propoziție de forma $\neg E$ este adevărată dacă și numai dacă propoziția E este *falsă*.
- vi) O propoziție de forma $(\forall x)E(x)$ (unde variabila x este liberă în E) este adevărată dacă și numai dacă pentru *orice* obiect c propoziția $E(c)$ este adevărată.
- vii) O propoziție de forma $(\exists x)E(x)$ (unde variabila x este liberă în E) este adevărată dacă și numai dacă *există măcar un obiect* c astfel încît propoziția $E(c)$ să fie adevărată.

1.3 Observație. Valoarea de adevăr a propozițiilor de tipul $E \wedge F$, $E \vee F$, $\neg E$ se poate defini prin *tabele de adevăr*. Iată tabelul de adevăr pentru $E \vee F$, construit după regula iv):

E	F	$E \vee F$
1	1	1
1	0	1
0	1	1
0	0	0

S-au scris pe linii toate combinațiile posibile de valori de adevăr pentru E și F . Tabelul se citește pe linii: de exemplu, linia 3 a tabelului spune, că, dacă E are valoarea de adevăr 0, iar F are valoarea de adevăr 1, atunci $E \vee F$ are valoarea de adevăr 1.

1.4 Definiție. a) Două propoziții E și F se numesc *echivalente* dacă au aceeași valoare de adevăr. Scriem aceasta sub forma $E \equiv F$.

b) Definiția se poate extinde la expresii oarecare. Două expresii E și F ce conțin aceleași constante și aceleași variabile (fie $x_1, \dots, x_n$ variabilele din E și F) sînt numite *echivalente* dacă: orice variabilă care este liberă în E este liberă în F (și reciproc) și *propozițiile* $(\forall x_1)(\forall x_2)\dots(\forall x_n)E(x_1, \dots, x_n)$ și $(\forall x_1)(\forall x_2)\dots(\forall x_n)F(x_1, \dots, x_n)$ au aceeași valoare de adevăr. Scriem atunci $E \equiv F$, sau $E(x_1, \dots, x_n) \equiv F(x_1, \dots, x_n)$ dacă vrem să evidențiem variabilele libere.

1.5 Exercițiu. Dacă E , F și G sînt expresii, avem echivalențele :

$$\begin{aligned} \neg(E \wedge F) &\equiv (\neg E) \vee (\neg F); & \neg(E \vee F) &\equiv (\neg E) \wedge (\neg F); & (\text{legile lui DeMorgan}) \\ (E \wedge F) \vee G &\equiv (E \vee G) \wedge (F \vee G); & & & (\text{distributivitatea lui } \vee \text{ față de } \wedge) \\ (E \vee F) \wedge G &\equiv (E \wedge G) \vee (F \wedge G); & & & (\text{distributivitatea lui } \wedge \text{ față de } \vee) \end{aligned}$$

$\neg((\forall x)E) \equiv (\exists x)(\neg E)$; $\neg((\exists x)E) \equiv (\forall x)(\neg E)$ (legile de negare a cuantificatorilor).

De exemplu, $\neg(E \wedge F) \equiv (\neg E) \vee (\neg F)$ se poate demonstra cu următorul tabel de adevăr:

E	F	$E \wedge F$	$\neg(E \wedge F)$	$\neg E$	$\neg F$	$(\neg E) \vee (\neg F)$
1	1	1	0	0	0	0
1	0	0	1	0	1	1
0	1	0	1	1	0	1
0	0	0	1	1	1	1

Identitatea coloanelor $\neg(E \wedge F)$ și $(\neg E) \vee (\neg F)$ demonstrează echivalența cerută.

Legile lui DeMorgan arată că am fi putut reduce setul de conectori logici și cuantificatori, de exemplu la $\forall$, $\neg$, $\wedge$.

Introducem următoarele *prescurtări* uzuale. Fie E, F expresii. Atunci scriem:

$E \rightarrow F$ în loc de $(\neg E) \vee F$ și citim „ E implică F ” sau „dacă E , atunci F ”;

$E \leftrightarrow F$ în loc de $(E \rightarrow F) \wedge (F \rightarrow E)$ și citim „ E este echivalent cu F ”.

1.6 Exercițiu. Scrieți tabelele de adevăr pentru conectorii $\rightarrow$ și $\leftrightarrow$. Demonstrați că, dacă E și F sînt propoziții, $E \leftrightarrow F$ este adevărată dacă și numai dacă E și F au aceeași valoare de adevăr.

Insistăm asupra *implicației*, $\rightarrow$. Se justifică intuitiv că $E \rightarrow F$ este același lucru cu $(\neg E) \vee F$, astfel: „ $E \rightarrow F$ ” înseamnă „dacă E este adevărată, atunci F este adevărată”. Altfel spus, sau E este falsă (adică are loc $\neg E$), sau E este adevărată și atunci automat F este adevărată (adică are loc F); pe scurt, $(\neg E) \vee F$. Este important de conștientizat această echivalență logică, utilă mai ales cînd trebuie negată o implicație (lucru care intervine frecvent, de exemplu în cazul demonstrațiilor prin reducere la absurd). Astfel, faptul că $E \rightarrow F$ este falsă înseamnă că are loc $(E \rightarrow F) \equiv \neg(\neg E) \vee F \equiv E \wedge (\neg F)$ (ipoteza este adevărată și totuși concluzia este falsă). Această interpretare este conformă cu intuiția („bunul-simț”). De altfel, concluziile bazate pe un calcul logic formal trebuie totdeauna interpretate intuitiv, proces absolut necesar în înțelegerea unor demonstrații (sau în găsirea unor soluții la o problemă dată).

Vom mai folosi și alte prescurtări, larg utilizate, de exemplu $x \neq y$ pentru $\neg(x = y)$ sau $x \notin y$ în loc de $\neg(x \in y)$.

Dacă propoziția $E \rightarrow F$ este adevărată, scriem atunci $E \Rightarrow F$. Analog, scrierea $E \Leftrightarrow F$ înseamnă că propoziția $E \leftrightarrow F$ este adevărată.

1.7 Observație. Orice teoremă matematică (propoziție, leamă etc.) poate fi scrisă în limbaj formal. Expresia obținută trebuie să fie din punct de vedere logic o *propoziție* (nu trebuie să aibă variabile libere). De exemplu, teorema împărțirii cu rest în $\mathbb{N}$ se poate scrie formal:

$$(\forall a)(\forall b)[(a \in \mathbb{N} \wedge b \in \mathbb{N} \wedge b \neq 0) \Rightarrow (\exists q)(\exists r)(q \in \mathbb{N} \wedge r \in \mathbb{N} \wedge a = bq + r \wedge r < b)].$$

I.2. Axiomatica mulțimilor

Prezentăm câteva elemente din teoria axiomatică Zermelo-Fraenkel-Skolem (ZFS) a mulțimilor. Pentru o tratare mai detaliată, incluzînd multe teme interesante (ordinali, cardinali, axioma alegerii etc.), vezi SCORPAN [1996].

Nu putem *defini* un obiect fără a face referire la alte obiecte, presupuse cunoscute. Aceste obiecte "cunoscute" trebuie la rîndul lor definite... Se vede că acest proces nu poate continua la infinit.

Așadar, trebuie să considerăm în cele din urmă *noțiuni care nu se definesc (noțiuni primare)*; cu ajutorul lor vom putea defini alte obiecte. Aceasta este un principiu de bază în orice teorie axiomatică.

În axiomatizarea teoriei mulțimilor, noțiunile de *mulțime* și de *relație de apartenență* se consideră *noțiuni primare* (nu se definesc) și *toate obiectele teoriei sînt mulțimi* (în particular, toate elementele unei mulțimi sînt tot mulțimi!). Aceste noțiuni satisfac un set de *axiome* (care, într-un anumit sens, *definesc* obiectele respective). Altfel spus, nu ne interesează *ce sînt* mulțimile, ci *cum se comportă* unele față de altele și față de relația de apartenență. Axiomele stabilesc regulile care se aplică obiectelor abstracte numite mulțimi și relației de apartenență.

Axiomele nu sînt decît *propoziții* (din limbajul formal construit anterior) care sînt *declarat* și *acceptate ca adevărate*. Orice altă afirmație despre mulțimi trebuie *demonstrată* pornind de la axiome. În acest mod se deduc toate proprietățile „uzuale” ale teoriei mulțimilor.

Deși, după cum am spus, în teoria axiomatică *elementele unei mulțimi sînt tot mulțimi*, vom adopta (pe cît posibil), pentru a nu crea confuzii cititorului, distincția tradițională în notație: în general, se notează *mulțimile cu majuscule* ($A, B, \dots$), iar *elementele mulțimilor cu minuscule* ($a, b, \dots$). Dacă A este o mulțime și a este un element al lui A , atunci scriem $a \in A$ (citit „ a aparține lui A ” sau „ A conține pe a ”). Dacă a nu este element al mulțimii A , scriem $a \notin A$.

2.1 Axioma extensibilității: Pentru orice două mulțimi A și B , avem :

$$[(\forall a) (a \in A \leftrightarrow a \in B)] \rightarrow A = B.$$

Mai riguros spus, propoziția următoare este adevărată:

$$(\forall A) (\forall B) \{[(\forall a) (a \in A \leftrightarrow a \in B)] \rightarrow A = B\}.$$

Această axiomă nu spune decît că *o mulțime este determinată de elementele sale*. Cu alte cuvinte, *dacă două mulțimi au aceleași elemente, atunci mulțimile coincid*.

Observăm că are loc și implicația inversă: dacă $A = B$, atunci orice element a care aparține lui A aparține și lui B . Acest fapt este evident: A și B denumesc același obiect, deci orice enunț referitor la A este adevărat și pentru B (și reciproc).

Dacă A și B sînt două mulțimi, vom scrie $A \subseteq B$ (și citim A *inclus în* B sau A *este submulțime a lui* B) dacă orice element al lui A aparține și lui B : $(\forall a) [(a \in A) \rightarrow (a \in B)]$. În caz contrar, notăm $A \not\subseteq B$.

Cu această notație, avem: $(\forall A) (\forall B) [(A = B) \leftrightarrow (A \subseteq B \wedge B \subseteq A)]$.

Pe această proprietate se bazează majoritatea demonstrațiilor de egalitate de mulțimi: pentru a demonstra că $A = B$, arătăm că orice element al lui A aparține și lui B (adică $A \subseteq B$) și reciproc ($B \subseteq A$).

Axiomele care urmează sînt toate de următorul tip: *fiind date una sau mai multe mulțimi, se garantează existența unei noi mulțimi cu anumite proprietăți* (construită cu ajutorul mulțimilor inițiale). Cu alte cuvinte, axiomele descriu *construcții permise în cadrul teoriei*. Se regăsește astfel motivul pentru care a fost construită teoria: evitarea paradoxurilor generate de construcții de mulțimi „prea mari”.

2.2 Axioma mulțimii părților unei mulțimi. $(\forall M) (\exists P) ((\forall A)(A \in P \leftrightarrow A \subseteq M))$.

În cuvinte: *fiind dată o mulțime M , există o mulțime P astfel încît elementele lui P sînt exact submulțimile lui M .*

Mulțimea P a cărei existență este postulată mai sus este unic determinată de mulțimea M . Într-adevăr, dacă și Q satisface condiția $(\forall A) (A \in Q \leftrightarrow A \subseteq M)$, atunci avem, pentru orice mulțime A : $A \in Q \leftrightarrow A \subseteq M \leftrightarrow A \in P$. Din axioma extensionalității obținem că $P = Q$.

Notația tradițională pentru P este $\mathcal{P}(M)$ (mulțimea părților lui M).

2.3 Axioma reuniunii. *Pentru orice mulțime A (subînțeles: avînd ca elemente tot mulțimi), se admite existența unei mulțimi ale cărei elemente sînt elementele mulțimilor din A , adică:*

$$(\forall A) (\exists U) (\forall x) [(x \in U) \leftrightarrow (\exists a) (a \in A \wedge x \in a)].$$

Pentru înțelegerea acestei axiome, este util să privim A ca pe o *familie de mulțimi*. Axioma de mai sus nu face decît să postuleze existența *reuniunii* acestei familii de mulțimi.

Mulțimea U – a cărei existență este garantată de axiomă – este unic determinată de A (demonstrați!) și se notează $\bigcup A$ sau $\bigcup_{x \in A} x$ sau $\bigcup \{x \mid x \in A\}$. A se remarca în acest context futilitatea distincției dintre element și mulțime.

2.4 Axioma-schemă a substituției

Nu este vorba de o simplă axiomă, ci de o *schemă* de axiome. Mai precis, pentru orice expresie (de un anumit tip) a limbajului formal se obține o axiomă. Așadar, avem de a face cu o infinitate de axiome.

Pentru enunț, avem nevoie de o **definiție**. O expresie $E(x, y)$ cu exact două variabile libere x și y se numește *relație funcțională* dacă pentru orice x există cel mult un y astfel încît $E(x, y)$ să fie adevărată:

$$(\forall x)(\forall y)(\forall z) ((E(x, y) \wedge E(x, z)) \rightarrow y = z).$$

Intuitiv, putem privi o relație funcțională ca pe o „funcție parțial definită”: pentru anumiți x există un unic y astfel încât $E(x, y)$ să aibă loc; se notează uneori chiar „funcțional”, $y = \tilde{E}(x)$ în loc de $E(x, y)$. Observăm că nu este neapărat adevărat că $(\forall x)(\exists y)E(x, y)$.

În termeni mai puțin formali, axioma-schemă a substituției afirmă că: *Pentru orice relație funcțională $E(x, y)$ și pentru orice mulțime a , există „imaginea prin E a mulțimii a ”.*

Evident, trebuie să definim formal conceptul de „imagine a unei mulțimi printr-o relație funcțională”. Spunem că mulțimea b este *imaginea mulțimii a prin relația funcțională $E(x, y)$* dacă „elementele lui b sînt de forma $\tilde{E}(x)$, cu $x \in a$ ”, adică:

$$(\forall y)[y \in b \leftrightarrow (\exists x)(x \in a \wedge E(x, y))].$$

Axioma-schemă a substituției este: *pentru orice relație funcțională $E(x, y)$, are loc:*

$$(\forall a)(\exists b)(\forall y)[y \in b \leftrightarrow (\exists x)(x \in a \wedge E(x, y))].$$

Subliniem din nou că *se obține cîte o axiomă pentru fiecare alegere a unei relații funcționale E* . Nu se pot condensa toate aceste enunțuri într-unul singur, de tipul

$$(\forall E \text{ relație funcțională})(\forall a)(\exists b)(\forall y)[y \in b \leftrightarrow (\exists x)(x \in a \wedge E(x, y))],$$

deoarece acesta *nu* este o expresie a limbajului formal: E nu denumește un *obiect* legitim (o mulțime), ci o *expresie*.

Folosind axioma extensionalității, se demonstrează imediat că *imaginea unei mulțimi printr-o relație funcțională este unic determinată* (mulțimea b a cărei existență este postulată de axioma schemă a substituției este unic determinată de E și b).

2.5 Consecință (Schema de comprehensiune). *Pentru orice mulțime A și pentru orice expresie cu o variabilă liberă $P(x)$, există submulțimea elementelor din A pentru care P este adevărată. Formal, $(\forall A)(\exists B)(\forall x)[x \in B \leftrightarrow (x \in A \wedge P(x))]$.⁹*

Demonstrație. Fie expresia $E(x, y) : "(x = y) \wedge P(y)"$. Afirmăm că E este o relație funcțională. Într-adevăr, fie x, y, z cu $E(x, y)$ și $E(x, z)$ adevărate. Atunci $x = y$ și $x = z$, deci $y = z$.

Conform axiomei substituției, pentru mulțimea A există o mulțime B astfel încît:

$$(\forall y)[y \in B \leftrightarrow (\exists x)(x \in A \wedge E(x, y))],$$

adică $y \in B \leftrightarrow (\exists x)(x \in A \wedge (x = y) \wedge P(y))$, ceea ce revine la a spune că $y \in B \leftrightarrow (y \in A \wedge P(y))$, ceea ce trebuia demonstrat. $\square$

Iarăși, axioma extensionalității asigură că A și $P(x)$ determină *unic* mulțimea B din enunț. Această mulțime se notează tradițional:

$$\{x \in A \mid P(x)\} \quad (\text{citit „mulțimea elementelor din } A \text{ care satisfac } P”).$$

2.6 Observație. Dacă se presupune că există măcar o mulțime¹⁰ A , rezultatul de mai sus asigură existența unei (unice) mulțimi ce nu conține nici un element, numită *mulțimea vidă* și

⁹ În axiomatizarea lui Zermelo din 1908, acest rezultat era enunțat ca axiomă și era numit *Axioma selecției*.

notată cu $\emptyset$.¹¹ Într-adevăr, fie $P(x) : "x \neq x"$. Din schema de comprehensiune, există $\emptyset := \{x \in A \mid x \neq x\}$. Pentru orice x , avem $x \notin \emptyset$ (dacă $x \in \emptyset$, atunci $x \neq x$, absurd). Unicitatea lui $\emptyset$ este o consecință a axiomei extensionalității. Notăm deci $\emptyset := \{x \in A \mid x \neq x\}$.

Pentru orice mulțime M are loc $\emptyset \subseteq M$. Este instructiv să prezentăm în detaliu acest argument. Conform definiției, avem $\emptyset \subseteq M$ dacă și numai dacă $\forall x (x \in \emptyset \rightarrow x \in M)$. Dar expresia $x \in \emptyset \rightarrow x \in M$ este, conform definiției, o prescurtare pentru $\neg(x \in \emptyset) \vee (x \in M)$, care este adevărată, căci $\neg(x \in \emptyset)$ este adevărată.

Termenul de *comprehensiune* descrie modalitatea de a preciza o mulțime prin enunțarea unei proprietăți pe care o au doar elementele mulțimii și numai ele. S-a văzut că acest concept, care a stat la baza teoriei naive a mulțimilor, duce la paradoxuri; schema de comprehensiune restrânge această modalitate doar la posibilitatea următoare: pentru orice mulțime dată M și orice „proprietate” P , există *submulțimea* elementelor lui M care satisfac P .

Cealaltă modalitate de a da o mulțime este prin *extensiune*, adică prin enumerarea tuturor elementelor sale. Astfel, fiind date elementele distincte $x_1, \dots, x_n$, există mulțimea X ale cărei elemente sînt exact $x_1, \dots, x_n$. Acest lucru este asigurat de schema de comprehensiune; scrierea $X = \{x_1, \dots, x_n\}$ este o prescurtare a scrierii $(\forall x)(x \in X \leftrightarrow (x = x_1 \vee x = x_2 \vee \dots \vee x = x_n))$.

2.7 Observație. Putem acum defini și alte „operații cu mulțimi”. Astfel, pentru orice două mulțimi A și B , arătați că există mulțimile:

$$\{x \in A \mid x \in B\} \text{ (notată } A \cap B \text{ și numită } \textit{intersecția} \text{ lui } A \text{ și } B)$$

$$\{x \in A \mid x \notin B\} \text{ (notată } A \setminus B \text{ și numită } \textit{diferența} \text{ lui } A \text{ și } B).$$

Demonstrați că $A \cap B = B \cap A$.

I.3. Clase, relații, funcții

Nu există o „mulțime a tuturor mulțimilor”, căci acest concept conduce la paradoxuri. Dacă ar exista mulțimea tuturor mulțimilor, fie aceasta A , atunci, conform schemei de comprehensiune, ar exista și mulțimea $C = \{B \in A \mid B \notin B\}$. Se vede că regăsim paradoxul lui Russel. Astfel de colecții „foarte mari” de obiecte apar însă frecvent în matematică (dorim de exemplu să vorbim de o proprietate pe care o au „toate” grupurile) și este necesară precizarea unui cadru riguros pentru aceste situații. O rezolvare rezonabilă este dată de conceptul de *clasă*.

¹⁰ Acest fapt este postulat de axioma infinității, enunțată mai jos.

¹¹ Nu este litera grecească majusculă *phi*, Φ , ci un simbol matematic derivat dintr-o literă norvegiană, $\emptyset$.

În cadrul teoriei Gödel-Bernays (GB), *clasa* este o noțiune primară (nu se definește clasa, ci este dat un set de axiome referitoare la clase; mulțimile vor fi un tip particular de clase – cele care sînt elemente ale altor clase). Teoria astfel dezvoltată este însă considerabil mai complicată decît ZFS¹².

În teoria ZFS, prin *clasă* se înțelege o expresie cu o variabilă liberă (un predicat cu o variabilă)¹³. Cu alte cuvinte, o proprietate nu mai definește o *mulțime* de obiecte, ci este privită ea însăși ca o entitate și o numim *clasă*. O clasă *nu* este însă un obiect al teoriei ZFS, ci este o expresie a limbajului formal (cf. comentariul de la axioma-schemă a substituției). De exemplu, predicatul $P(x) : „x = x”$ este evident satisfăcut de orice mulțime x ; acest predicat definește „clasa tuturor mulțimilor”. Abuzînd de limbajul de la mulțimi, fiind dată o clasă $P(x)$, în loc să se spună ca un anumit x satisface P sau „ $P(x)$ este adevărată”, se spune „ x aparține clasei P ” sau „ x este un element al clasei P ”.

Observăm că orice mulțime a definește o clasă, anume „ $x \in a$ ”.

Reciproc, spunem că o clasă $P(x)$ *corespunde* unei mulțimi M dacă are loc $\forall x (P(x) \leftrightarrow x \in M)$: obiectele care satisfac P sînt exact elementele lui M . Uneori spunem în acest caz chiar că P este o mulțime.

În acest sens, *clasa tuturor mulțimilor nu corespunde unei mulțimi*. Demonstrația a fost dată chiar la începutul acestui paragraf!

Se pot defini și *operații cu clase*, prin analogie cu cele de la mulțimi. Astfel, dacă $P(x)$ și $Q(x)$ sînt clase, definim *reuniunea* claselor P și Q ca fiind clasa $P(x) \vee Q(x)$; *intersecția* lor este clasa $P(x) \wedge Q(x)$. Cum s-ar defini *diferența* lor? Dar faptul că clasa P este *inclusă* în clasa Q ?

În această terminologie, schema de comprehensiune nu spune altceva decît că *intersecția dintre o clasă și o mulțime este o mulțime*.

Apare acum destul de clar că exprimări de genul „mulțimea tuturor grupurilor” nu sînt legitime, o exprimare corectă fiind „clasa tuturor grupurilor”. Noțiunea de clasă este esențială în *teoria categoriilor*.

Să trecem la un alt concept fundamental, anume la cel de *funcție*. Pentru aceasta, avem nevoie de noțiunea de *cuplu* (*pereche ordonată*). Începem cu un rezultat interesant și prin sine.

3.1 Propoziție (Teorema perechii). Fie a și b două mulțimi. Atunci există o mulțime c care are ca elemente pe a și pe b și numai pe ele. Formal:

$$(\forall a)(\forall b)(\exists c)(\forall x) [(x \in c) \leftrightarrow (x = a \vee x = b)]$$

Mulțimea c de mai sus este unic determinată de a și b și se notează $\{a, b\}$.

¹² În plus, s-a arătat că orice enunț despre mulțimi demonstrabil în GB este demonstrabil în ZFS.

¹³ Această interpretare pentru clase a fost prezentată de W. Quine în 1963.

Demonstrație. Ideea este de a construi o mulțime cu două elemente D și de a obține $\{a, b\}$ ca imaginea lui D printr-o relație funcțională bine aleasă (se aplică deci axioma substituției).

Știm că există mulțimea vidă $\emptyset$. Construim (cu axioma mulțimii părților) mulțimea $\mathcal{P}(\emptyset)$, care are un element (avem $\emptyset \subseteq \emptyset$, deci $\emptyset \in \mathcal{P}(\emptyset)$; $\emptyset$ este chiar unicul element al lui $\mathcal{P}(\emptyset)$, deci $\mathcal{P}(\emptyset) = \{\emptyset\}$). Cum $\emptyset$ nu are nici un element, deducem că $\mathcal{P}(\emptyset) \neq \emptyset$. Construim acum $\mathcal{P}(\mathcal{P}(\emptyset)) = \mathcal{P}(\{\emptyset\})$. Unicele mulțimi incluse în $\{\emptyset\}$ sînt $\emptyset$ și $\{\emptyset\}$, deci $\mathcal{P}(\{\emptyset\}) = \{\emptyset, \{\emptyset\}\}$ are două elemente (cum am dorit).

Fie $E(x, y)$: " $(x = \emptyset \wedge y = a) \vee (x = \{\emptyset\} \wedge y = b)$ " (verificați că este o relație funcțională) Imaginea prin E a lui $\mathcal{P}(\{\emptyset\})$ este chiar mulțimea căutată c .

Unicitatea lui c rezultă din axioma extensionalității. □

3.2 Exercițiu. Fie a și b mulțimi. Demonstrați că există reuniunea lor $a \cup b$ (adică unica mulțime cu proprietatea $\forall x[(x \in a \cup b) \leftrightarrow (x \in a \vee x \in b)]$).

Intuitiv, noțiunea de *cuplu* (*pereche ordonată*) format de elementele a și b diferă de $\{a, b\}$, prin faptul că avem o „ordine”: a este primul, iar b este al doilea. Această distincție între a și b se realizează prin:

3.3 Definiție. Fie a și b mulțimi. Aplicînd propoziția de mai sus mulțimilor a și a , există mulțimea $\{a\}$; există și $\{a, b\}$. Aplicînd din nou propoziția, există mulțimea $\{\{a\}, \{a, b\}\}$, care se notează cu (a, b) și se numește *perechea ordonată* (*cuplul*) format de a și b . Observați că, dacă $a = b$, atunci $(a, b) = \{\{a\}\}$.

Această idee de introducere a noțiunii de cuplu este atribuită lui Kuratowski. Are loc proprietatea fundamentală următoare (demonstrați!):

3.4 Propoziție. Fie a, b, a', b' mulțimi. Atunci are loc: $(a, b) = (a', b') \leftrightarrow a = a' \text{ și } b = b'$. □

Astfel, spre deosebire de mulțimea $\{a, b\}$, în cuplul (a, b) contează ordinea elementelor a și b ; dacă $a \neq b$, atunci $(a, b) \neq (b, a)$, însă $\{a, b\} = \{b, a\}$.

Avînd definită noțiunea de cuplu, definim noțiunea de *triplet*:

$$(a, b, c) := ((a, b), c)$$

și, prin recurență, n -uplu, $\forall n \geq 3$ (pentru o tratare riguroasă a inducției și recurenței, vezi I.4.20)

$$(a_1, \dots, a_n) := ((a_1, \dots, a_{n-1}), a_n).$$

Are loc: $(a_1, \dots, a_n) = (b_1, \dots, b_n) \leftrightarrow a_1 = b_1 \wedge \dots \wedge a_n = b_n$.

În manualele de liceu (și în multe alte cărți de matematică), o *funcție* definită pe o mulțime A cu valori într-o mulțime B este „definită” (mai bine spus descrisă) ca fiind „un procedeu (lege), prin care oricărui element din A i se asociază un unic element din B ”. Intuitiv, descrierea este corectă (dar vagă, deoarece folosește noțiunea nedefinită de *procedeu (lege)*); în plus, se subînțelege că pentru orice funcție se poate descrie un *procedeu (algoritm)* de

obținere a imaginii oricărui element prin funcția dată. Acest lucru nu este necesar și în matematică se întâlnesc exemple de funcții pentru care acest fapt nu are loc.

Se observă însă că o funcție $f: A \rightarrow B$ este perfect determinată de *graficul* său, adică de mulțimea cuplurilor $\{(a, f(a)) \mid a \in A\}$. Aceasta este și ideea definiției conceptului de funcție în cadrul unei tratări riguroase. Începem cu alte două noțiuni, și ele fundamentale:

3.5 Definiție. Fie A și B mulțimi. Numim *produsul cartezian*¹⁴ al mulțimilor A și B mulțimea $A \times B := \{(a, b) \mid a \in A \wedge b \in B\}$.

Avem dreptul de a defini o astfel de mulțime? Ar trebui să arătăm că ne încadrăm în schema de comprehensiune, adică să indicăm o mulțime a cărei existență este certă, care să conțină toate perechile de forma (a, b) cu $a \in A$ și $b \in B$. Dar $(a, b) = \{\{a\}, \{a, b\}\}$. Observăm că avem $\{a\} \in \mathcal{P}(A \cup B)$ și $\{a, b\} \in \mathcal{P}(A \cup B)$, deci $\{\{a\}, \{a, b\}\} \in \mathcal{P}(\mathcal{P}(A \cup B))$. Astfel, putem defini, respectând schema de comprehensiune:

$$A \times B := \{c \in \mathcal{P}(\mathcal{P}(A \cup B)) \mid (\exists a)(\exists b)[c = (a, b) \wedge a \in A \wedge b \in B]\}.$$

Folosind produsul cartezian putem defini noțiunile de *relație* și de *funcție*:

3.6 Definiție. Fie A și B două mulțimi.

a) Numim *relație binară între A și B* (sau *de la A la B*) orice triplet de forma (A, B, ρ) , unde $\rho \subseteq A \times B$. Uneori vom exprima acest fapt sub forma „ ρ este o relație între A și B ”. Dacă $A = B$, scriem (A, ρ) și spunem că ρ este o *relație pe A* . Adeseori, în loc de $(x, y) \in \rho$ se scrie $x\rho y$. Dacă sînt subînțelese mulțimile A și B , se spune, simplu, relația ρ în loc de (A, B, ρ) .

b) O relație binară f de la A la B se numește *funcție* (sau *aplicație*) *definită pe A cu valori în B* dacă pentru orice $a \in A$ există un unic $b \in B$ astfel încît $(a, b) \in f$. Formal, tripletul (A, B, f) este funcție de la A la B dacă:

$$(f \subseteq A \times B) \wedge (\forall a) \{(a \in A) \rightarrow (\exists b)[(b \in B) \wedge (a, b) \in f]\} \wedge$$

$$(\forall a)(\forall b)(\forall b') \{(a \in A) \wedge (b \in B) \wedge (b' \in B) \wedge (a, b) \in f \wedge (a, b') \in f \rightarrow (b = b')\} \quad (*)$$

Întrucît pentru orice $a \in A$ există un unic $b \in B$ astfel încît $(a, b) \in f$, se scrie:

$$„f(a) = b” \text{ în loc de } „(a, b) \in f”.$$

Se mai spune „ f este o funcție (aplicație) de la A la B ” și se notează aceasta prin $f: A \rightarrow B$ sau $A \xrightarrow{f} B$. Notăția $f: A \rightarrow B$ nu este decît o prescurtare a expresiei (*).

Mulțimea A se numește *domeniul* funcției f și B se numește *codomeniul* lui f . Orice element a din domeniul lui f se numește *argument* al funcției f . Dacă $a \in A$ și $b \in B$ astfel încît $f(a) = b$, b se numește *valoarea funcției f în a* .

Pentru orice mulțime A , notăm cu $\mathbf{1}_A$ sau cu id_A *funcția identitate* a mulțimii A , anume: $id_A(a) = a, \forall a \in A$.

¹⁴ În onoarea lui René Descartes (1596-1650), al cărui nume latinizat era Cartesius.

Dacă adoptăm punctul de vedere naiv: o funcție $f: A \rightarrow B$ este o „lege de corespondență” prin care oricărui element a din A i se asociază un unic element $f(a)$ din B , atunci mulțimea $\{(a, f(a)) \mid a \in A\} \subseteq A \times B$ se numește *graficul* lui f . Astfel, definiția 3.6.b) identifică o funcție cu graficul ei.

3.7 Observație. Condiția (*) se scrie, mai puțin formalizat:

$$(f \subseteq A \times B) \text{ și } \forall a \in A, \exists b \in B \text{ astfel încât } (a, b) \in f \text{ și } \\ \forall a \in A, \forall b, b' \in B, (a, b) \in f \text{ și } (a, b') \in f \text{ implică } b = b'.$$

Observăm că, în expresii, șirurile de forma " $(\forall a)(a \in A)$ " se scriu adesea prescurtat " $\forall a \in A$ ". Această convenție, larg răspândită, ascunde o capcană: o implicație, de genul $(\forall a)[(a \in A) \rightarrow P(a)]$, se scrie adesea " $\forall a \in A, P(a)$ ", în care implicația $\rightarrow$ nu apare explicit. Trebuie conștientizat acest fapt, mai ales când apare necesitatea negării unei astfel de expresii: negația ei este $(\exists a)\{(a \in A) \wedge \neg P(a)\}$, lucru care nu este clar din scrierea prescurtată (dar este destul de clar din punct de vedere intuitiv).

3.8 Observație. O expresie cu exact două variabile libere se numește *relație*. Pentru orice relație $R(x, y)$ putem defini "*domeniul*" D_R și "*imagea*" I_R ca fiind clasele:

$$D_R(x): "(\exists y)R(x, y)" \\ I_R(y): "(\exists x)R(x, y)"$$

Demonstrați că, dacă clasele D_R și I_R sînt mulțimi, atunci relației $R(x, y)$ i se asociază o relație ρ între D_R și I_R (în sensul definiției 3.6.a), $\rho := \{(x, y) \in D_R \times I_R \mid R(x, y) \text{ adevărată}\}$. Mai mult, această relație este *funcție* (în sensul definiției 3.6.b) dacă și numai dacă R este *relație funcțională*. Invers, unei funcții $f: A \rightarrow B$ i se asociază o relație funcțională $F(x, y): "x \in A \wedge y = f(x)"$.

Demonstrați că, dacă R este relație funcțională și D_R este mulțime, atunci I_R este mulțime. Reciproca este adevărată?

3.9 Exercițiu. Fie A o mulțime. Cîte funcții $\varphi: \emptyset \rightarrow A$ (respectiv $\varphi: A \rightarrow \emptyset$) există?

3.10 Definiție. Fie $f: A \rightarrow B$ o funcție. Dacă $A' \subseteq A$, se definește *imagea lui A' prin f* ca fiind imagea mulțimii A' prin relația funcțională asociată lui f . Cu alte cuvinte, definim

$$f[A'] = \{y \in B \mid (\exists x)(x \in A' \wedge f(x) = y)\}$$

Notăția tradițională pentru imagea lui A' prin f este $f(A')$; nu se poate folosi o astfel de notație în teoria axiomatică a mulțimilor, pentru că A' poate fi simultan submulțime a lui A și element al lui A (puteți da exemplu de un astfel de caz?) și este foarte posibil ca $f(A')$ (valoarea în A' a lui f) să difere de $f[A']$ (imagea submulțimii A' prin f).

3.11 Definiție. Fie I o mulțime (interpretată ca mulțime de „indici”). O funcție $b: I \rightarrow M$, unde M este o mulțime, se numește *familie de mulțimi indexată după I* . Notății tradiționale pentru această noțiune: $(B_i)_{i \in I}$ (unde $B_i := b(i)$), sau $\{B_i \mid i \in I\}$.

Dacă $(B_i)_{i \in I}$ este o familie de mulțimi ca mai sus, *reuniunea familiei* $\{B_i\}_{i \in I}$ este reuniunea imaginii funcției b :

$$\bigcup A = \bigcup_{i \in I} B_i := \{x \in M \mid \exists i \in I \text{ astfel încât } x \in B_i\}.$$

Intersecția familiei $\{B_i\}_{i \in I}$ este, prin definiție

$$\bigcap_{i \in I} B_i := \{x \mid \forall i \in I, x \in B_i\}.$$

De exemplu, dacă $I = \{1, 2\}$ și $\{B_i\}_{i \in I} = \{B_1, B_2\}$,

$$\bigcup \{B_1, B_2\} = \bigcup_{i \in I} B_i = B_1 \cup B_2; \text{ la fel, } \bigcap \{B_1, B_2\} = \bigcap_{i \in I} B_i = B_1 \cap B_2.$$

Se spune că *reuniunea familiei* $\{B_i\}_{i \in I}$ este *disjunctă* dacă $\{B_i\}_{i \in I}$ sînt disjuncte două cîte două: $B_i \cap B_j = \emptyset$ dacă $i \neq j$.

3.12 Propoziție. Pentru orice mulțimi A, B, C , au loc egalitățile:

$$i) \emptyset \cap A = \emptyset, \emptyset \cup A = A, A \setminus \emptyset = A, A \setminus A = \emptyset;$$

$$ii) A \cap B \subseteq A, A \cap B \subseteq B, A \subseteq A \cup B, B \subseteq A \cup B;$$

$$iii) A \cap B = B \cap A, A \cup B = B \cup A;$$

$$iv) A \cap (B \cap C) = (A \cap B) \cap C, A \cup (B \cup C) = (A \cup B) \cup C;$$

$$v) A \cap (B \cup C) = (A \cap B) \cup (A \cap C), A \cup (B \cap C) = (A \cup B) \cap (A \cup C);$$

$$vi) A \cup A = A = A \cap A.$$

□

3.13 Definiție. Se numește *inversă a unei relații* (A, B, ρ) relația (B, A, ρ^{-1}) unde $\rho^{-1} = \{(b, a) \mid (a, b) \in \rho\} \subseteq B \times A$.

Fie relațiile (A, B, ρ) și (B, C, τ) . Relația $(A, C, \tau \circ \rho)$, unde

$$\tau \circ \rho = \{(a, c) \in A \times C \mid (\exists b)(b \in B \wedge a \rho b \wedge b \tau c)\}$$

este numită *compusa* (sau *compunerea*) *relațiilor* τ și ρ .

3.14 Propoziție. a) Fiind date funcțiile $u : A \rightarrow B$, $v : B \rightarrow C$, compusa $v \circ u$ este tot o funcție, $v \circ u : A \rightarrow C$, și, $\forall a \in A$, are loc:

$$(v \circ u)(a) = v(u(a)).$$

b) Pentru orice relații (A, B, ρ) , (B, C, τ) , (C, D, η) , avem $(\eta \circ \tau) \circ \rho = \eta \circ (\tau \circ \rho)$ (compunerea relațiilor este asociativă). În particular, compunerea funcțiilor este asociativă. □

Se disting următoarele tipuri remarcabile de funcții:

3.15 Definiție. Fie $f : A \rightarrow B$ o funcție. Spunem că f este:

$$i) \text{ funcție injectivă dacă } \forall x, y \in A, f(x) = f(y) \Rightarrow x = y;$$

$$ii) \text{ funcție surjectivă dacă } \forall y \in B, \exists x \in A \text{ astfel încât } f(x) = y;$$

$$iii) \text{ funcție bijectivă dacă este injectivă și surjectivă;}$$

$$iv) \text{ funcție inversabilă dacă } \exists g : B \rightarrow A \text{ (numită inversa lui } f) \text{ astfel încât } (g \circ f)(x) = x, \forall x \in A \text{ și } (f \circ g)(y) = y, \forall y \in B.$$

Notînd, pentru o mulțime M , prin $\mathbf{1}_M : M \rightarrow M$ funcția $\mathbf{1}_M(x) = x$, $\forall x \in M$ (numită și *funcția identitate* a lui M , notată și cu id_M sau id), condițiile ce definesc funcțiile inversabile pot fi rescrise în modul următor: $g \circ f = \mathbf{1}_A$, $f \circ g = \mathbf{1}_B$. Dacă există, inversa lui f se notează f^{-1} .

3.16 Propoziție. Fie $f : A \rightarrow B$ și $g : B \rightarrow C$ funcții. Atunci:

a) f este inversabilă $\Leftrightarrow f$ este bijectivă;

b) $g \circ f$ este bijectivă $\Rightarrow g$ este surjectivă și f este injectivă;

c) Compunerea a două funcții injective (surjective) este funcție injectivă (surjectivă). $\square$

Definiția produsului cartezian poate fi extinsă prin recurență la o familie de trei sau mai multe mulțimi, sau, mai general, la o familie oarecare de mulțimi:

3.17 Definiție. a) Fiind date mulțimile A_1, A_2, A_3 ¹⁵, definim produsul lor cartezian:

$$A_1 \times A_2 \times A_3 := (A_1 \times A_2) \times A_3.$$

Astfel, $\forall a_1 \in A_1, \forall a_2 \in A_2, \forall a_3 \in A_3$, notăm $((a_1, a_2), a_3)$, mai simplu, cu (a_1, a_2, a_3) .

b) Pentru orice $n \geq 3$ și orice familie de n mulțimi $A_1, A_2, \dots, A_n$, definim (prin recurență¹⁶):

$$A_1 \times A_2 \times \dots \times A_n := (A_1 \times A_2 \times \dots \times A_{n-1}) \times A_n.$$

$A_1 \times A_2 \times \dots \times A_n$ se mai notează cu $\prod_{i=1}^n A_i$ sau $\prod_{1 \leq i \leq n} A_i$. Dacă $\forall i \in \{1, 2, \dots, n\}$, $a_i \in A_i$, se

notează $((a_1, a_2, \dots, a_{n-1}), a_n) \in \prod_{i=1}^n A_i$ cu $(a_1, a_2, \dots, a_n)$. Astfel,

$$A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, \dots, a_n) \mid a_i \in A_i, i = \overline{1, n}\}$$

În cazul $A_1 = A_2 = \dots = A_n = A$, $A \times A \times \dots \times A$ (de n ori) se notează cu A^n .

c) Este necesară și o definiție în cazul general al unei familii de mulțimi $(A_i)_{i \in I}$ indexată după o mulțime de indici I . Se definește produsul cartezian $\prod_{i \in I} A_i$:

$$\prod_{i \in I} A_i := \{\varphi : I \rightarrow \bigcup_{i \in I} A_i \mid \varphi(i) \in A_i, \forall i \in I\}.$$

3.18 Observație. Produsul cartezian definit ca la c), în cazul unei familii finite de mulțimi, nu este același cu cel definit la a) și b) și la 3.5. Există însă o bijecție naturală între mulțimile obținute prin cele două definiții. De exemplu, dacă $I = \{1, 2\}$, avem funcția bijectivă β , definită pe $\{\varphi : \{1, 2\} \rightarrow A_1 \cup A_2 \mid \varphi(i) \in A_i, \forall i \in I\}$ cu valori în $A_1 \times A_2$, dată de $\beta(\varphi) = (\varphi(1), \varphi(2))$. Se pot astfel identifica noțiunile de produs cartezian definite mai sus.

Definim următoarele *tipuri remarcabile de relații pe o mulțime*:

3.19 Definiție. Fie o mulțime nevidă A și ρ o relație pe A . Spunem că ρ este:

- *reflexivă* dacă $a\rho a$, $\forall a \in A$. Formal: $(\forall a)(a \in A \rightarrow a\rho a)$;

¹⁵ În această ordine! De fapt, se dă o familie de mulțimi indexată după $\{1, 2, 3\}$.

¹⁶ Folosim deocamdată o accepție intuitivă a noțiunii de definiție prin recurență. Pentru o tratare riguroasă, vezi 4.20 și următoarele.

- *ireflexivă* dacă $\forall a \in A$, nu are loc apa ;
- *simetrică* dacă $\forall a, b \in A$, $apb \rightarrow bpa$;
- *asimetrică* dacă $\forall a, b \in A$, $apb \rightarrow \neg bpa$;
- *antisimetrică* dacă $\forall a, b \in A$, apb și $bpa \rightarrow a = b$;
- *tranzitivă* dacă $\forall a, b, c \in A$, apb și $bpc \rightarrow apc$;
- *relație de echivalență* dacă este reflexivă, simetrică și tranzitivă. Pentru relații de echivalență se folosesc notații de tipul $a \equiv b$, $a \sim b$ în loc de apb .
- *relație de preordine* dacă este reflexivă și tranzitivă;
- *relație de ordine* dacă este reflexivă, tranzitivă și antisimetrică. Pentru relații de (pre)ordine se folosesc în general notații de tipul $a \leq b$ în loc de apb .
- *relație de ordine strictă* dacă este ireflexivă și tranzitivă. Pentru relații de ordine strictă se folosesc în general notații de tipul $a < b$ în loc de apb .

Relațiile de *ordine* și de *echivalență* sînt deosebit de importante în toată matematica și este esențială o bună cunoaștere a proprietăților lor.

3.20 Exercițiu. a) Scrieți formal condițiile de mai sus referitoare la o relație ρ .

b) Cum se generalizează definițiile anterioare la *relații* (în sensul de expresii cu două variabile libere)? De exemplu, o relație $R(x, y)$ se numește reflexivă dacă $(\forall x)R(x, x)$.

c) Exprimați definițiile de mai sus în termeni de incluziuni și compuneri de relații (și eventual de inverse). De exemplu, ρ este reflexivă înseamnă că $id_A \subseteq \rho$; ρ este simetrică înseamnă că $\rho^{-1} \subseteq \rho$.

Dacă $\leq$ este o relație de ordine pe A , scriem $(A, \leq)$ și spunem că $(A, \leq)$ este *mulțime ordonată*. Dacă pentru orice $a, b \in A$ avem $a \leq b$ sau $b \leq a$, atunci $(A, \leq)$ se numește mulțime *total ordonată* (sau *lanț*) și relația $\leq$ se numește relație de *ordine totală*. Uneori, pentru a sublinia că o anumită relație de ordine nu este totală, se spune *relație de ordine parțială*. În loc de $a \leq b$ se scrie și $b \geq a$. Se observă că, dacă $\leq$ este o relație de ordine pe A , atunci $\geq$ este tot o relație de ordine.

3.21 Observație. Dacă $\leq$ este o relație de ordine pe A , atunci relația $<$ pe A , definită prin: $x < y \leftrightarrow (x \leq y \wedge x \neq y)$ este o relație de *ordine strictă* pe A . Reciproc, dacă $<$ este o ordine strictă pe A , atunci, definind $x \leq y \leftrightarrow (x < y \vee x = y)$ se obține o relație de ordine pe A . Verificați! Așadar, există o bijecție între relațiile de ordine pe A și relațiile de ordine strictă pe A . De aceea, orice definiție sau rezultat aplicabil unei relații de ordine se aplică și relației de ordine strictă asociate (și reciproc). Cum trebuie adaptate aceste considerații la *relațiile* văzute în sensul de la 3.8?

3.22 Definiție. Fie $(A, \leq)$ o mulțime ordonată și B o submulțime a lui A . Un element $m \in A$ se numește *minorant* al lui B dacă $m \leq b$, $\forall b \in B$. Un element $M \in A$ se numește *majorant* al lui B dacă $b \leq M$, $\forall b \in B$. Submulțimea B se numește *minorată* (resp. *majorată*) dacă are un

minorant (resp. majorant). Dacă B conține un minorant m pentru B , spunem că m este *cel mai mic element* (sau *primul element*) al lui B . Dacă B conține un majorant M pentru B , M se numește *cel mai mare element* (sau *ultimul element*) al lui B .

Dacă B are un prim element $m \in B$, acesta este unic: $\forall m' \in B$, avem $m \leq m'$ (m este prim element) și $m' \leq m$, deci $m = m'$ din antisimetrie. La fel, *ultimul element al lui B este unic* (dacă există).

Ca exercițiu, exprimați definițiile și proprietățile de mai sus (date pentru relații de ordine) pentru relații de ordine *strictă*.

3.23 Exemplu. Relația de divizibilitate " $|$ " pe $\mathbb{N}$, dată de:

$$\forall a, b \in \mathbb{N} \quad (a|b \leftrightarrow \exists c \in \mathbb{N} \text{ astfel încât } b = ac)$$

este o relație de ordine, care *nu este totală* (nu are loc nici $2|3$, nici $3|2$); 0 este *ultimul element* al lui $(\mathbb{N}, |)$ și 1 este *primul element* al lui $(\mathbb{N}, |)$. Relația uzuală de ordine " $\leq$ " pe $\mathbb{N}$ este *totală*, 0 este primul element al lui $(\mathbb{N}, \leq)$; nu există ultimul element al lui $(\mathbb{N}, \leq)$.

O mulțime $(A, \leq)$ cu proprietatea că orice submulțime nevidă B a lui A are un prim element se numește mulțime *bine ordonată* (caz în care relația $\leq$ pe A se numește *relație de bună ordine*). Mulțimile bine ordonate sînt foarte importante: pe o mulțime bine ordonată se poate aplica un raționament prin *inducție*.

Orice mulțime bine ordonată este total ordonată (demonstrați!).

3.24 Definiție. Un element m al unei mulțimi ordonate $(A, \leq)$ se numește *element maximal* al lui A dacă, $\forall b \in A$ cu $m \leq b$ rezultă $m = b$. Un element m se numește *element minimal* al lui A dacă, $\forall b \in A$ cu $b \leq m$ rezultă $m = b$. De exemplu, în mulțimea ordonată $\mathbb{N} \setminus \{0, 1\}$ cu divizibilitatea, 2 este element minimal. Care sînt toate elementele sale minimale?

3.25 Definiție. Fie $(A, \leq)$ o mulțime ordonată și B o submulțime a sa. Fie $Maj(B)$ mulțimea majoranților lui B . Dacă există cel mai mic element al lui $Maj(B)$, acest element se numește *supremumul* (sau *marginea superioară* a) lui B și se notează $\sup B$. Dacă există $\sup B = c$, atunci c este „*cel mai mic majorant al lui B* ”, adică satisface condițiile:

- $\forall b \in B, b \leq c$ (c este majorant al lui B).
- $\forall c' \in A$ astfel încît $\forall b \in B, b \leq c'$, rezultă $c \leq c'$ (c este mai mic decît orice alt majorant c' al lui B).

„Dual” (considerînd relația de ordine $\geq$) se obține noțiunea de *infimum* (sau *margine inferioară*) al submulțimii B a lui $(A, \leq)$, notat (dacă există!) cu $\inf B$.

O mulțime ordonată $(A, \leq)$ cu proprietatea că orice submulțime cu două elemente a sa are supremum și infimum se numește *latice*. Dacă orice submulțime a lui A are $\sup$ și $\inf$, A se numește *latice completă*.

De exemplu, pentru o mulțime nevidă oarecare M , mulțimea $\mathcal{P}(M)$ a părților lui M este ordonată de relația de incluziune; dacă $A, B \in \mathcal{P}(M)$, atunci $\sup\{A, B\} = A \cup B$, $\inf\{A, B\} = A \cap B$. $(\mathcal{P}(M), \subseteq)$ este chiar o latice completă. La fel, $(\mathbb{N}, |)$ este o latice.

În $\mathbb{R}$, ordonat cu ordinea uzuală, orice submulțime nevidă majorată are supremum (aceasta este o proprietate fundamentală a lui $\mathbb{R}$, esențială în Analiză). În $\mathbb{Q}$, nu orice submulțime nevidă are supremum (justificați!).

I.4. Ordinale, axioma infinității și mulțimea numerelor naturale

În toată matematica este esențială mulțimea numerelor naturale $\mathbb{N}$. Se pune problema unui mod de a construi această mulțime (sau, fiind vorba de un concept care poate apărea drept primar, de a axiomatiza $\mathbb{N}$). Vom arăta că, în cadrul teoriei axiomatice a mulțimilor, se poate da o construcție satisfăcătoare a lui $\mathbb{N}$. Mai mult, modul de construcție duce la o generalizare posibilă a mulțimii $\mathbb{N}$, sub forma *clasei ordinalelor*.

O modalitate de abordare a introducerii lui $\mathbb{N}$ este dată de *axiomatica Dedekind-Peano*. Noțiunile primare sînt cele de *număr natural* și *funcție succesor*¹⁷. Limbajul acestei teorii axiomatice este format din:

- simbolul $=$ (notează egalitatea a două obiecte);
- simbolul 0 (notează un număr natural privilegiat fixat);
- nume variabile, constante, conectorii logici (ca la limbajul teoriei axiomatice a mulțimilor), cu deosebirea că numele denumesc acum obiectele acestei teorii, adică *numere naturale*.

Axiomele acestei teorii sînt:

1. Există un număr natural notat 0 .
2. Pentru orice număr natural n , există un număr natural unic determinat, numit *succesorul lui n* și notat $s(n)$ sau n^+ : $(\forall n)(\exists n^+)$.
3. Orice două numere naturale cu același succesori sînt egale: $(\forall m)(\forall n)(m^+ = n^+ \rightarrow m = n)$.
4. 0 nu este succesori nici unui număr natural: $(\forall n)(n^+ \neq 0)$.
5. (**Axioma inducției**) Pentru orice predicat cu o variabilă $A(n)$ are loc:

$$[A(0) \wedge (\forall n)(A(n) \rightarrow A(n^+)) \rightarrow (\forall m)A(m)].$$

¹⁷ Întrucît este vorba de o teorie axiomatică, funcția succesori nu este a priori o *funcție* în sensul teoriei mulțimilor (ci este o noțiune primară); este adevărat însă că în *modelul* pe care îl construim, rolul funcției succesori va fi jucat de o funcție în sens uzual.

Observăm că axioma **5** (binecunoscutul *principiu de demonstrație prin inducție*) este de fapt o *schemă de axiome*.

Introducerea operațiilor cu numere naturale, a relației de ordine și deducerea principalelor proprietăți ale acestora folosind axiomaticele Dedekind-Peano sînt interesante și instructive. Aceste aspecte fiind însă destul de cunoscute (vezi de ex. BECHEANU et al. [1983]), nu insistăm în această direcție. Vom arăta, în schimb, că se poate *modela* sistemul axiomatic de mai sus în cadrul teoriei mulțimilor, dacă mai introducem o axiomă (de fapt, acest *model* se expune în general, cînd se vorbește de axiomaticele Peano). Mai precis, vom construi o *mulțime* $\mathbb{N}$, un *element* $0 \in \mathbb{N}$ și o *funcție* (în sens uzual) $s : \mathbb{N} \rightarrow \mathbb{N}$, $s(n) = n^+$, care să satisfacă axiomele de mai sus.

Începem cu o abordare intuitivă. Instrumentele oferite pînă acum de axiomele teoriei mulțimilor permit considerarea următorului „șir de mulțimi”:

$$\emptyset; \{\emptyset\}; \{\emptyset, \{\emptyset\}\}; \{\emptyset, \{\emptyset\}, \{\emptyset, \{\emptyset\}\}\}; \dots \quad (1)$$

Se observă că, pentru fiecare termen x al șirului, următorul termen este $x \cup \{x\}$. Primul termen are 0 elemente, al doilea are 1 element ș.a.m.d. Ar fi tentant să considerăm drept mulțime a numerelor naturale „mulțimea tuturor termenilor acestui șir”, $\emptyset$ să joace rolul lui 0, iar funcția succesor să fie $s(x) = x \cup \{x\}$. Apar două probleme: *definirea riguroasă* a „mulțimii tuturor termenilor șirului (1)” și garantarea *existenței* unei astfel de mulțimi. Faptul că există o mulțime care *include* toți termenii șirului (1) este asigurat de o nouă axiomă:

4.1 Axioma infinității. $(\exists M) [\emptyset \in M \wedge (\forall y)(y \in M \rightarrow y \cup \{y\} \in M)]$.

Intuitiv, este clar că axioma de mai sus garantează existența unei mulțimi M care să conțină toate mulțimile șirului (1); aceasta nu înseamnă că M conține *doar* aceste mulțimi. Vom adopta următoarea strategie: definim riguros *clasa* mulțimilor din șirul (1) (aceasta va fi *clasa ordinalelor finite*, noțiune pe care o vom defini în cele ce urmează); atunci mulțimea $\mathbb{N}$ a numerelor naturale va fi obținută prin comprehensiune, ca fiind mulțimea acelor elemente din M (dată de axioma infinității) care sînt în plus *ordinale finite*. Apoi demonstrăm că toate aceste obiecte satisfac axiomele Dedekind-Peano.

4.2 Definiție. O mulțime α se numește *ordinal* dacă are următoarele proprietăți:

- i) α este *tranzitivă*, adică $(\forall x)(x \in \alpha \rightarrow x \subseteq \alpha)$.
- ii) relația de apartenență definește o relație de *ordine strictă* pe α , care este o *bună ordine* pe α . Detaliind, această condiție este echivalentă cu:

- $\forall x, y, z \in \alpha$, din $x \in y$ și $y \in z$ rezultă că $x \in z$ (*tranzitivitatea* relației $\in$);
- $\forall x, y \in \alpha$, din $x \in y$ rezultă că $y \notin x$ (*ireflexivitatea* relației $\in$);
- orice submulțime nevidă a lui α are un prim element (față de relația $\in$):

$$\forall \beta \{(\beta \subseteq \alpha \wedge \beta \neq \emptyset) \rightarrow \exists x [x \in \beta \wedge \forall y(y \in \beta \rightarrow (x = y \vee x \in y))]\}.$$

4.3 Exemplu. Orice element din șirul (1) este ordinal.

Clasa ordinaletor se notează cu *On*. Astfel, scrierea $On(\alpha)$ înseamnă „mulțimea α este un ordinal”.¹⁸

Înainte de a defini ordinalele *finite*, avem nevoie de unele pregătiri.

4.4 Definiție. Fie $(A, \leq)$ o mulțime ordonată. O submulțime S a lui A se numește *segment inițial* al lui A dacă are proprietatea că, odată cu un element x , conține toate elementele mai mici decât x : $\forall x [x \in S \rightarrow (\forall y (y \in A \wedge y \leq x) \rightarrow y \in S)]$.

De exemplu, dacă fixăm $a \in A$, mulțimea $S_a(A) := \{x \in A \mid x < a\}$ este un segment inițial în A . Este remarcabil că în mulțimi *bine ordonate*, toate segmentele inițiale sînt de acest tip:

4.5 Propoziție. Fie $(A, \leq)$ o mulțime *bine ordonată* și S un segment inițial al lui A . Atunci: sau $S = A$, sau există $a \in A$ astfel încît $S = S_a(A) := \{x \in A \mid x < a\}$.

Demonstrație. Presupunem că $S \neq A$. Atunci $A \setminus S$ este nevidă și (A fiind bine ordonată) are un prim element a . Afirmăm că $S_a(A) = S$. Într-adevăr, fie $x \in S$. Dacă $a \leq x$, atunci $a \in S$, din definiția segmentului inițial. Cum A este total ordonată, rezultă că $x < a$, adică $x \in S_a(A)$. Incluziunea cealaltă o lăsăm cititorului. $\square$

4.6 Propoziție. Fie α un ordinal și s un segment inițial în α . Atunci $s = \alpha$ sau există $\beta \in \alpha$ astfel încît $s = \beta = S_\beta(\alpha)$.

Demonstrație. Reamintim că relația de ordine strictă pe α este $\in$, față de care α este bine ordonată. Din propoziția precedentă rezultă că $s = \alpha$ sau există $\beta \in \alpha$ astfel încît $s = S_\beta(\alpha)$. Dar $S_\beta(\alpha) = \{x \in \alpha \mid x \in \beta\} = \alpha \cap \beta$. Cum α este ordinal, din $\beta \in \alpha$ rezultă $\beta \subseteq \alpha$, deci $\alpha \cap \beta = \beta$. $\square$

4.7 Propoziție. Orice element al unui ordinal este tot un ordinal.

Demonstrație. Fie α un ordinal și $\beta \in \alpha$. Atunci $\beta = S_\beta(\alpha)$, care este un segment inițial în α . În general, orice submulțime nevidă a unei mulțimi bine ordonate A este bine ordonată de relația de ordine de pe A (demonstrați!), deci $\beta = S_\beta(\alpha)$ este bine ordonat de $\in$. Avem și că β este tranzitivă: dacă $x \in \beta$, iar $y \in x$, atunci $x \in \alpha$ (căci $\beta \in \alpha$ și α este tranzitivă). Acum, din $x \in \alpha$ și $y \in x$ deducem că $y \in \alpha$. Am obținut că $y, x, \beta \in \alpha, y \in x$ și $x \in \beta$. Relația $\in$ este tranzitivă pe α , deci $y \in \beta$. $\square$

4.8 Propoziție. Dacă α este un ordinal, atunci $\alpha \notin \alpha$.

Demonstrație. Relația de apartenență $\in$ este de ordine strictă pe α , deci este ireflexivă: $\forall x \in \alpha$, avem $x \notin x$. Dacă presupunem că $\alpha \in \alpha$, obținem astfel că $\alpha \notin \alpha$, absurd. $\square$

¹⁸ Ideea de a defini ordinalele în această manieră îi aparține lui John von Neumann. Un ordinal se poate defini și ca o *clasă de izomorfism de mulțimi bine ordonate*. În această abordare însă, clasa ordinaletor ar fi o "clasă de clase", o complicare tehnică evitată de prezentarea aleasă aici.

4.9 Propoziție. Pentru orice ordinale α și β , are loc una și numai una din afirmațiile: $\alpha \in \beta$, $\alpha = \beta$ sau $\beta \in \alpha$.

Demonstrație. Fie $\gamma = \alpha \cap \beta = \{x \in \alpha \mid x \in \beta\}$. Se verifică imediat că γ este un segment inițial în mulțimea ordonată $(\alpha, \in)$ (vezi def. 4.4). Din 4.6 rezultă că $\gamma = \alpha$ sau $\gamma \in \alpha$. Simetric, avem $\gamma = \beta$ sau $\gamma \in \beta$. Analizăm toate posibilitățile: 1) $\gamma = \alpha$ și $\gamma = \beta$. Atunci $\alpha = \beta$. 2) $\gamma = \alpha$ și $\gamma \in \beta$. Atunci $\alpha \in \beta$. 3) $\gamma \in \alpha$ și $\gamma = \beta$. Atunci $\beta \in \alpha$. 4) $\gamma \in \alpha$ și $\gamma \in \beta$. Atunci $\gamma \in \alpha \cap \beta = \gamma$, imposibil: γ este ordinal și s-ar contrazice 4.8.

Cele trei situații din enunț sînt mutual incompatibile: dacă $\alpha \in \beta$, atunci $\alpha = \beta$ ar contrazice 4.8, iar $\beta \in \alpha$ implică (pentru că α este tranzitivă) $\alpha \in \alpha$, aceeași contradicție. $\square$

Putem enunța proprietatea de mai sus sub forma: *Clasa ordinaletor este total ordonată de relația de ordine strictă $\in$.*

Mai mult, *clasa ordinaletor este bine ordonată de relația de apartenență*. Acest enunț necesită precizări: nu am definit încă noțiunea de *clasă* bine ordonată. O analogie directă cu *mulțimile* bine ordonate ar conduce la următoarea „definiție”: o clasă $C(x)$ ordonată de o relație (în sensul de la 3.8) de ordine $R(x, y)$ este bine ordonată dacă *orice subclasă* nevidă a sa are un prim element. Sintagma „*orice subclasă*” inclusă în definiție conduce de fapt la a da o *schemă* de definiții, căci clasele nu sînt obiecte ale teoriei, ci expresii ale limbajului formal (cf. comentariul de la Axioma-schemă a substituției). Se adoptă următoarea definiție, mai restrictivă, dar care nu are dezavantajul descris anterior:

4.10 Definiție. O clasă $C(x)$ se numește *bine ordonată* de o relație de ordine strictă $R(x, y)$ dacă este total ordonată de R și orice segment inițial al lui C în raport cu relația R este o mulțime bine ordonată de R . Mai precis, au loc afirmațiile:

- R este o relație ireflexivă pe C : $\forall x(C(x) \rightarrow \neg R(x, x))$.
- R este o relație tranzitivă pe C : $\forall x \forall y \forall z(C(x) \wedge C(y) \wedge C(z) \wedge R(x, y) \wedge R(y, z) \rightarrow R(x, z))$.
- R este o relație totală pe C : $\forall x \forall y(C(x) \wedge C(y) \rightarrow (R(x, y) \vee R(y, x) \vee x = y))$.
- Pentru orice mulțime t , segmentul inițial al clasei C determinat de t în raport cu relația R , adică clasa $S_t(C)(\text{mod } R) := C(x) \wedge R(x, t)$, este o *mulțime* bine ordonată de R :

$$(\forall t)(\exists s)[(\forall x)(x \in s \leftrightarrow (C(x) \wedge R(x, t))) \wedge (\forall u)[(u \neq \emptyset \wedge u \subseteq s) \rightarrow \exists p(p \text{ primul element al lui } u)]]$$

Dacă C este bine ordonată de R în sensul definiției anterioare, atunci *orice clasă nevidă inclusă în C are prim element*. Într-adevăr, fie D o clasă nevidă inclusă în C și fie t un element din D (adică $D(t)$ adevărată). Dacă t este prim element în D în raport cu R , atunci am terminat. Dacă nu, există q în D mai mic strict decît t : $D(q) \wedge R(q, t)$. Dar segmentul inițial $S_t(C)(\text{mod } R)$ este o mulțime; deci intersecția clasei D cu $S_t(C)(\text{mod } R)$, adică clasa $D(x) \wedge (x \in S_t(C)(\text{mod } R))$ este o submulțime S a lui $S_t(C)(\text{mod } R)$ (nevidă, căci conține q). Din buna ordonare a lui $S_t(C)(\text{mod } R)$ deducem că există primul element m al mulțimii S . Acesta este primul element al clasei D : dacă ar exista n în D , mai mic decît m , atunci n este mai mic

decît t și deci $n \in S_t(C)(\text{mod } R)$. Astfel, $n \in S$ și obținem o contradicție cu faptul că m este primul element al lui S .

Să demonstrăm acum:

4.11 Propoziție. *Clasa ordinaledor On este bine ordonată de relația de apartenență.*

Demonstrație. Am văzut (4.9) că relația de apartenență este totală pe clasa ordinaledor. Fie α un ordinal și segmentul inițial $S_\alpha(On)(\text{mod } \in) = On(t) \wedge (t \in \alpha)$. Evident, această clasă este o mulțime, anume α (orice element t al lui α este ordinal). Din definiția ordinaledor, α este bine ordonat de apartenență. $\square$

Ordonarea „nstrictă” pe clasa On este *incluziunea*. Mai precis, pentru două ordinale α și β , $(\alpha \in \beta \vee \alpha = \beta)$ este echivalent cu $\alpha \subseteq \beta$. Cel mai mic ordinal este $\emptyset$. Care este însă cel mai mic ordinal mai mare decît un ordinal α dat?

4.12 Propoziție. *Pentru orice ordinal α , $\alpha \cup \{\alpha\}$ este tot ordinal (numit succesorul lui α) și este cel mai mic ordinal, mai mare decît α .*

Demonstrație. Propunem spre demonstrație afirmația: α ordinal implică $\alpha \cup \{\alpha\}$ ordinal. Fie acum β un ordinal mai mare decît α . Atunci $\alpha \in \beta$ (adică $\{\alpha\} \subseteq \beta$). Deci $\alpha \subseteq \beta$ (căci β ordinal), și astfel $\alpha \cup \{\alpha\} \subseteq \beta$. Aceasta demonstrează că orice ordinal mai mare decît α este mai mare sau egal cu $\alpha \cup \{\alpha\}$. Pe de altă parte, este evident că $\alpha \in \alpha \cup \{\alpha\}$. $\square$

4.13 Definiție. Dacă pentru ordinalul β există α astfel încît $\beta = \alpha \cup \{\alpha\}$ (β este succesorul lui α), atunci α este ordinal, unic determinat de β (de ce?) și se numește *predecesorul* lui β . Un ordinal α se numește *ordinal finit* dacă: sau $\alpha = \emptyset$, sau orice element al lui α și α însuși au un predecesor. Un ordinal care nu este finit se numește *ordinal infinit*.

Se observă că toate mulțimile din șirul (1) sînt ordinale finite. De altfel, șirul a fost construit plecînd de la $\emptyset$ și luînd succesorul fiecărui ordinal construit deja.

Dacă α este ordinal finit, atunci se verifică imediat că:

- orice ordinal $\beta \subseteq \alpha$ este ordinal finit.
- succesorul lui α , $\alpha \cup \{\alpha\}$, este ordinal finit.

4.14 Propoziție. *Axioma infinității este echivalentă cu afirmația:*

Ordinalele finite formează o mulțime (notată cu ω).

Demonstrație. Presupunem axioma infinității adevărată și considerăm *mulțimea* $\omega := \{\alpha \in M \mid \alpha \text{ ordinal finit}\}$, unde M este dată de 4.1. Să arătăm că ω conține orice ordinal finit. Dacă nu ar fi așa, ar exista un ordinal finit β , cu $\beta \notin M$. Cum clasa ordinaledor finite este bine ordonată, există cel mai mic ordinal finit μ cu proprietatea că $\mu \notin M$. Cum $\emptyset \in M$, $\mu \neq \emptyset$. Însă atunci μ are un predecesor λ , care (din modul de alegere al lui μ) este în M . Însă atunci succesorul lui λ (adică μ) aparține lui M , contradicție.

Invers, dacă ordinalementele finite formează o mulțime ω , atunci ω satisface proprietățile din axioma 4.1: $\emptyset \in \omega$ și $\forall \alpha \in \omega$, avem $\alpha \cup \{\alpha\} \in \omega$. $\square$

Acum se poate da următorul **model** (în cadrul teoriei axiomatice a mulțimilor) pentru axiomele Dedekind-Peano:

- numerele naturale sînt *ordinalementele finite*;
- numărul natural 0 este *mulțimea vidă* $\emptyset$;
- funcția succesor este funcția $s : \omega \rightarrow \omega$ care *asociază fiecărui ordinal finit α succesorul său $\alpha \cup \{\alpha\}$* .

Clar, axiomele 1-4 sînt verificate. Să verificăm și axioma inducției:

4.15 Propoziție. (*Teorema inducției pe mulțimea ordinalementelor finite*) Fie P o clasă de ordinalemente finite astfel încît $P(\emptyset)$ este adevărată și, $\forall \alpha$ ordinal finit cu $P(\alpha)$ adevărată, rezultă că $P(\alpha \cup \{\alpha\})$ adevărată. Atunci $P(\alpha)$ adevărată pentru orice ordinal finit α .

Demonstrație. Clasa P corespunde unei submulțimi (notată tot P) a lui ω . Dacă $P \neq \omega$, atunci $\omega \setminus P \neq \emptyset$ și deci $\omega \setminus P$ are un prim element β , cu $\beta \neq \emptyset$ din ipoteza $P(\emptyset)$ adevărată. Fie α predecesorul lui β . Avem $\alpha \notin \omega \setminus P$, deci $P(\alpha)$ adevărată, de unde rezultă $P(\alpha \cup \{\alpha\}) = P(\beta)$ adevărată, adică $\beta \in P$, contradicție cu $\beta \in \omega \setminus P$. $\square$

4.16 Observație. Mulțimea ω a ordinalementelor finite este un ordinal (demonstrați!), care nu este finit.

Alte rezultate despre ordinalemente sînt propuse ca exerciții. Detalii și dezvoltări ale teoriei ordinalementelor pot fi găsite de exemplu în SCORPAN [1996].

În continuare vom identifica mulțimea ordinalementelor finite ω cu mulțimea numerelor naturale $\mathbb{N}$. Notăm cu $\leq$ relația de ordine pe $\mathbb{N}$ (numită relația de ordine uzuală) și cu $n + 1$ succesorul numărului natural (ordinalului finit) n . Prin această identificare, 0 corespunde lui $\emptyset$, 1 lui $\{\emptyset\}$, ș.a.m.d.; $n + 1$ corespunde lui $n \cup \{n\}$. Observăm că atunci $n = \{0, 1, \dots, n - 1\}$.

Prin analogie cu $\mathbb{N}$, se notează cu $<$ relația de ordine strictă pe On (pentru orice ordinalemente α, β , $\alpha < \beta$ înseamnă deci $\alpha \in \beta$) și cu $\alpha + 1$ succesorul ordinalului α (deci $\alpha + 1 = \alpha \cup \{\alpha\}$).

Este deosebit de important următorul enunț, care stă la baza raționamentelor prin inducție:

Mulțimea numerelor naturale $\mathbb{N}$ este bine ordonată în raport cu relația de ordine uzuală.

Considerăm utile cîteva remarci și rezultate privind tehnica de *demonstrație prin inducție*, respectiv de *definire prin recurență*. Mai întîi dăm un rezultat care este cunoscut uneori ca o „variantă a principiului de inducție”:

4.17 Propoziție. Fie $P(x)$ o expresie cu proprietatea că, pentru orice număr natural n , dacă $P(k)$ este adevărată pentru orice $k < n$, rezultă că $P(n)$ este adevărată. Atunci $P(n)$ este

adevărată pentru orice număr natural n . Mai precis, are loc (subînțelegem că toate variabilele sînt în $\mathbb{N}$):

$$\{\forall n [(\forall k (k < n \rightarrow P(k)) \rightarrow P(n)]\} \rightarrow (\forall n)(P(n)).$$

Demonstrație. Mai întîi observăm că, în condițiile din enunț, $P(0)$ este adevărată. Într-adevăr, pentru $n = 0$ are loc implicația: $[\forall k(k < 0 \rightarrow P(k)) \rightarrow P(0)]$. Dar $\forall k(k < 0 \rightarrow P(k))$ este adevărată, deoarece $k < 0$ este falsă pentru orice $k \in \mathbb{N}$ (o expresie de forma $p \rightarrow q$ este adevărată dacă p este falsă!). Deci $P(0)$ adevărată.¹⁹

Presupunem prin absurd că există $n \in \mathbb{N}$ astfel încît $P(n)$ să fie falsă. Atunci mulțimea nevidă $\{n \in \mathbb{N} \mid P(n) \text{ falsă}\}$ are un prim element a . Deci $P(k)$ este adevărată, $\forall k < a$, din modul de alegere a lui a . Cum are loc implicația $(\forall k(k < a \rightarrow P(k)) \rightarrow P(a)$, rezultă că $P(a)$ este adevărată, absurd. $\square$

Este remarcabil faptul că acest rezultat are loc în orice mulțime bine ordonată. Propunem cititorului să reia ideea demonstrației de mai sus pentru a arăta :

4.18 Propoziție. Fie $(A, \leq)$ o mulțime bine ordonată și fie $P(x)$ o expresie cu proprietatea că, pentru orice $n \in A$, dacă $P(k)$ este adevărată pentru orice $k < n$, $k \in A$, rezultă că $P(n)$ adevărată. Atunci $P(n)$ adevărată pentru orice $n \in A$. Mai precis, are loc (subînțelegem că toate variabilele sînt în A):

$$\{\forall n [(\forall k (k < n \rightarrow P(k)) \rightarrow P(n)]\} \rightarrow (\forall n)(P(n)).$$

$\square$

Un exemplu de aplicare a acestei propoziții este demonstrația teoremei polinoamelor simetrice (unde mulțimea bine ordonată este $\mathbb{N}^n$, cu ordinea lexicografică).

Mai mult, se poate face inducție pe clase bine ordonate. Dacă $R(x, y)$ este o relație de ordine, vom scrie, mai sugestiv, $x < y \pmod{R}$ în loc de $R(x, y) \wedge (x \neq y)$. Demonstrația rezultatului ce urmează este similară cu cea de la mulțimi bine ordonate.

4.19 Propoziție. Fie $A(x)$ o clasă bine ordonată de o relație $R(x, y)$ și fie $P(x)$ o expresie cu proprietatea că, pentru orice n din clasa A , dacă $P(k)$ este adevărată pentru orice k din A , cu $k < n \pmod{R}$, rezultă că $P(n)$ adevărată. Atunci $P(n)$ adevărată pentru orice n din A . Mai precis, dacă are loc:

$$\forall n \{[A(n) \wedge (\forall k (A(k) \wedge k < n \pmod{R}) \rightarrow P(k)) \rightarrow P(n)\},$$

atunci are loc $(\forall n)(A(n) \rightarrow P(n))$. $\square$

În general, astfel de raționamente se fac pe clasa ordinalelor On și se numesc raționamente prin inducție transfinită.

Strîns legat de principiul demonstrației prin inducție este *definirea șirurilor prin recurență* (numită uneori *definire prin inducție*, denumire improprie, căci inducția este o metodă de

¹⁹ Așadar, nu are rost să se arate că $P(0)$ este adevărată cînd se folosește acest raționament prin inducție!

demonstrație). De exemplu, este clar că relațiile $x_0 = 1, x_{n+1} = 2x_n + 1, \forall n \in \mathbb{N}$, definesc unic șirul de numere naturale: $x_0 = 1, x_1 = 3, x_2 = 7, x_3 = 15, \dots$.

4.20 Definiție. Fie A o mulțime nevidă. Se numește *șir* (indexat după ω)²⁰, cu valori în A , orice funcție $s : \omega \rightarrow A$ (ω este ordinalul tuturor ordinalelor finite). Mai general, dacă α este un ordinal oarecare, vom numi *șir* (indexat după α) cu valori în A orice funcție definită pe α cu valori în A .

Pentru un șir $s : \alpha \rightarrow A$ se folosesc notații de tipul $(s_i)_{i \in \alpha}$ sau $\{s_i \mid i \in \alpha\}$. Pentru orice $\beta \in \alpha$ (β este deci ordinal!), notăm cu $s|_\beta$ restricția lui s la β ($s|_\beta$ este atunci șir indexat după β). De exemplu, dacă $(s_n)_{n \in \omega}$ este un șir indexat după ω , atunci:

$$\begin{aligned} s|_0 &= s|_\emptyset = \emptyset; & s|_1 &= s|_{\{0\}} = \{(0, s(0))\}; & s|_2 &= s|_{\{0,1\}} = \{(0, s(0)), (1, s(1))\}, \dots, \\ s|_n &= s|_{\{0,1, \dots, n-1\}} = \{(0, s(0)), (1, s(1)), \dots, (n-1, s(n-1))\}. \end{aligned}$$

Ce înseamnă a *defini prin recurență* un șir $(s_n)_{n \in \omega}$? Intuitiv, pentru orice $n \in \omega$, termenul s_n „depinde de termenii precedenți $s_0, \dots, s_{n-1}$ ”, adică este dată o „relație de recurență” de forma $s_n = f(s_0, \dots, s_{n-1})$. Observăm că putem rescrie aceasta sub forma $s_n = f(s|_n)$, folosind notațiile de mai sus. Deci f este o funcție cu domeniul format de mulțimea șirurilor (cu valori în A), indexate după un $n = \{0, 1, \dots, n-1\}$. Mai general, putem da următoarea:

4.21 Definiție. Fie A o mulțime nevidă și α un ordinal. Pentru fiecare $\beta \in \alpha$ notăm cu

$$S_\beta(A) = \{b \mid b : \beta \rightarrow A\}$$

mulțimea șirurilor cu valori în A , indexate după β . Fie

$$S(A, \alpha) = \bigcup_{\beta \in \alpha} S_\beta(A) = \{b \mid (\exists \beta) (\beta \in \alpha \text{ și } b \text{ este funcție de la } \beta \text{ la } A)\}$$

mulțimea șirurilor cu valori în A , indexate după ordiale din α . Dacă $s : \alpha \rightarrow A$ și $\beta \in \alpha$, atunci $s|_\beta \in S_\beta(A) \subseteq S(A, \alpha)$, deci există $f(s|_\beta) \in A$.

O *relație de recurență* este o funcție $f : S(A, \alpha) \rightarrow A$. Spunem că șirul $s : \alpha \rightarrow A$ este *definit recurent de relația de recurență* f dacă, $\forall \beta \in \alpha$, avem :

$$s(\beta) = f(s|_\beta).$$

4.22 Teoremă. Fie α un ordinal și A o mulțime. Pentru orice relație de recurență $f : S(A, \alpha) \rightarrow A$ există un unic șir $s : \alpha \rightarrow A$ care este definit recurent de f .

Demonstrație. Unicitatea: presupunem că există două șiruri $s : \alpha \rightarrow A$ și $t : \alpha \rightarrow A$, definite recurent de f , astfel încât $s \neq t$. Deci mulțimea $\{\beta \in \alpha \mid s(\beta) \neq t(\beta)\}$ este nevidă și are un prim element π . Atunci $s(\gamma) = t(\gamma), \forall \gamma \in \pi$, adică $s|_\pi = t|_\pi$. Dar $s(\pi) = f(s|_\pi) = f(t|_\pi) = t(\pi)$, contradicție.

²⁰ Reamintim că am identificat $\mathbb{N}$ cu ordinalul ω .

Existența: Notăm cu δ mulțimea ordinalelor β din α pentru care există un șir s_β indexat după β , definit recurent de f , adică: $\delta := \{\beta \in \alpha \mid \exists s_\beta : \beta \rightarrow A \wedge (\forall \gamma \in \beta \rightarrow s_\beta(\gamma) = f(s_\beta|_\gamma))\}$. Evident, $\delta \subseteq \alpha$. Avem de arătat că $\delta = \alpha$.

Afirmăm că δ este un ordinal. E suficient să demonstrăm că δ este segment inițial (vezi 4.6). Observăm că $\emptyset \in \delta$ (funcția $\emptyset : \emptyset \rightarrow A$ este definită recurent de f !), deci δ este nevidă. Fie $\beta \in \delta$. Vrem să arătăm că $\gamma \in \delta$, $\forall \gamma < \beta$. Cum $\beta \in \delta$, există $s : \beta \rightarrow A$ definit recurent de f . Pentru $s|_\gamma$ avem, $\forall \lambda \in \gamma$: $s|_\gamma(\lambda) = s(\lambda) = f(s|_\lambda) = f((s|_\gamma)|_\lambda)$, deci $s|_\gamma$ este definit pe γ și este definit recurent de f . Astfel, $\gamma \in \delta$.

Cum δ este ordinal și $\delta \subseteq \alpha$, avem $\delta = \alpha$ sau $\delta \in \alpha$. Dacă $\delta = \alpha$, am terminat. Presupunem prin absurd că $\delta \in \alpha$.

Observăm că, $\forall \beta \in \delta$, șirul s_β definit recurent de f este unic determinat, din prima parte a demonstrației. Mai mult, $\forall \beta \in \delta$ și $\forall \gamma \in \beta$, restricția lui s_β la γ coincide cu s_γ (tot din unicitate). Definim atunci $s : \delta \rightarrow A$ prin: $\forall \beta \in \delta$, $s(\beta) = f(s_\beta)$. Definiția are sens: s_β este un șir indexat după β (unicul șir definit recurent pe β de f) și există $f(s_\beta) \in A$.

Să demonstrăm că $s : \delta \rightarrow A$ este definit recurent pe δ de f , adică: $\forall \beta \in \delta$ are loc $s(\beta) = f(s|_\beta)$. Comparînd cu definiția lui s , aceasta revine la a arăta că $\forall \beta \in \delta$, avem $s|_\beta = s_\beta$.

Fie $\beta \in \delta$ și fie $\gamma \in \beta$. Avem, din cele de mai sus: $s(\gamma) = f(s_\gamma) = f(s_\beta|_\gamma) = s_\beta(\gamma)$, $\forall \gamma \in \beta$. Deci $s|_\beta(\gamma) = s_\beta(\gamma)$, $\forall \gamma \in \beta$, adică $s|_\beta = s_\beta$.

Deci $\delta \in \alpha$ și există $s : \delta \rightarrow A$ definit recurent de f . Din definiția lui δ , avem $\delta \in \delta$; absurd. $\square$

Definițiile prin recurență pe un ordinal oarecare sînt cunoscute ca definiții prin *recurență transfinită*. Acest tip de definiții se utilizează, între altele, în teoria dimensiunii laticelor și a modulelor (vezi de exemplu NĂSTĂSESCU [1983]).

Prezentăm o proprietate foarte importantă a lui $\mathbb{N}$, a cărei demonstrație ilustrează principiul de demonstrație prin inducție. Se presupun cunoscute operațiile de adunare și înmulțire în $\mathbb{N}$ și proprietățile lor.

4.23 Teoremă (Teorema împărțirii cu rest în $\mathbb{N}$). *Pentru orice numere naturale a , b , cu $b \neq 0$, există $q, r \in \mathbb{N}$ astfel încît $a = bq + r$ și $r = 0$ sau $r < b$ (q se numește cîtuș iar r restul împărțirii lui a la b). În plus, q și r sînt unic determinate cu aceste proprietăți.*

Demonstrație. Fie $b \neq 0$ fixat. Demonstrăm prin inducție după a , aplicînd 4.17. Mai precis, considerăm $P(a)$: $\exists q \exists r (q \in \mathbb{N} \wedge r \in \mathbb{N} \wedge a = bq + r \wedge r < b)$.

Pentru orice $a < b$, $P(a)$ este adevărată, luînd $q = 0$, $r = a$. Presupunem acum că $a \geq b$ și $P(k)$ este adevărată, $\forall k \in \mathbb{N}$, $k < a$. Să demonstrăm $P(a)$. Cum $a \geq b$ avem $a - b \in \mathbb{N}$ și $a - b < a$. Deci are loc $P(a - b)$: $\exists q, r$ astfel încît $a - b = bq + r$ și $r < b$, adică $a = b(q + 1) + r$, cu $r < b$.

Unicitatea: presupunem că $a = bq + r = bt + s$, cu $r < b$ și $s < b$. Pentru a face o alegere, fie $q \geq t$, adică $q - t \geq 0$. Atunci $b(q - t) = s - r$. Cum $s < b$, rezultă că $s - r < b$. Astfel, $b(q - t) < b$, de unde obținem $q - t = 0$ și $s - r = 0$. $\square$

Teorema împărțirii cu rest este de o importanță covârșitoare în matematică. O primă aplicație a ei este *reprezentarea numerelor naturale într-o bază dată* (vezi Exerciții).

Un alt punct de vedere privind ordinalele este descris în continuare.

4.24 Definiție. Fie $(A, \leq)$ și $(B, \leq)$ mulțimi ordonate. O aplicație $\varphi: A \rightarrow B$ se numește *morfism de ordine* (sau *aplicație crescătoare*) dacă $\forall x, y \in A$, din $x \leq y$ rezultă $\varphi(x) \leq \varphi(y)$. Morfismul φ se numește *izomorfism de ordine* dacă φ este bijectivă și inversa sa φ^{-1} este tot morfism. Mulțimile ordonate $(A, \leq)$ și $(B, \leq)$ se numesc *izomorfe* dacă există măcar un izomorfism de ordine $\varphi: A \rightarrow B$, caz în care scriem $A \cong B$.

4.25 Observație. Dacă $(A, \leq)$ și $(B, \leq)$ sînt *total* ordonate, atunci orice morfism bijectiv $\varphi: A \rightarrow B$ este și izomorfism. Demonstrați! Pentru mulțimi ordonate în general, nu orice morfism bijectiv este izomorfism, după cum arată exemplul aplicației identitate $\text{id}: (\mathbb{N}^*, |) \rightarrow (\mathbb{N}^*, \leq)$, unde $(\mathbb{N}^*, |)$ este mulțimea numerelor naturale nenule înzestrată cu relația de ordine divizibilitatea, iar $\leq$ este relația de ordine uzuală.

Comparați rezultatul următor cu 4.9:

4.26 Propoziție. Fie A și B mulțimi bine ordonate. Atunci are loc exact una din situațiile: $A \cong B$; A izomorf cu un segment inițial al lui B ; B izomorf cu un segment inițial al lui A . $\square$

Clasa mulțimilor ordonate izomorfe cu o mulțime ordonată dată $(A, \leq)$ se numește *tipul de ordine* al lui $(A, \leq)$. Orice mulțime bine ordonată este izomorfă cu un unic ordinal:

4.27 Propoziție. Fie $(A, \leq)$ o mulțime bine ordonată. Atunci există un unic ordinal $(\alpha, \in)$ izomorf cu $(A, \leq)$. $\square$

Astfel, pentru orice tip de *bună ordine*, există un unic ordinal în acel tip (și, evident, orice ordinal se află într-un unic tip de bună ordine). Din acest motiv, uneori prin *ordinal* se înțelege *un tip de ordine de mulțimi bine ordonate*. Rezultatele enunțate arată echivalența celor două abordări.

I.5. Comentarii și completări privind axiomatizarea mulțimilor

În această secțiune vom discuta cu titlu informativ anumite aspecte ale teoriei axiomatice a mulțimilor. Pentru detalii, se pot consulta lucrări precum SCORPAN [1996], MANIN [1977].

Sistemul ZF propriu-zis conține 4 axiome și o schemă de axiome: *axioma extensivității*, *axioma reuniunii*, *axioma mulțimii părților*, *schema de axiome a substituției* și *axioma infinității*.

Este de dorit ca orice teorie axiomatică (deci și ZF) să satisfacă următoarele proprietăți:

Consistența (sau *necontradictorialitatea*) teoriei: din axiomele teoriei nu se poate deduce simultan o propoziție și negația ei (adică nu se poate obține o *contradicție*). O teorie care nu este consistentă nu are nici o valoare științifică: *dacă există o propoziție p astfel încât p și $\neg p$ sînt adevărate, atunci orice propoziție q este adevărată* (ceea ce elimină orice interes în stabilirea adevărului unei propoziții). Într-adevăr, este clar că, dacă p și $p \rightarrow q$ sînt adevărate, atunci q este adevărată. Însă p e adevărată din ipoteză, iar $p \rightarrow q$ este $\neg p \vee q$, adevărată căci $\neg p$ este adevărată.

Independența axiomelor: nici o axiomă nu este o consecință a celorlalte. O teorie în care axiomele nu sînt independente nu este însă lipsită de interes (poate fi, cel mult, acuzată de redundanță).

Problemele stabilirii consistenței și independenței unui sistem axiomatic sînt dificile și profunde.

Strîns legată de problema consistenței este *modelarea* unui sistem axiomatic. Se numește *model* al unei teorii axiomatice o structură de obiecte care satisfac axiomele teoriei. Se pot da exemple numeroase: un model al axiomelor geometriei plane este $\mathbb{R} \times \mathbb{R}$, un model pentru axiomele inelului este $(\mathbb{Z}, +, \cdot)$ etc. Are loc următorul rezultat: *o teorie axiomatică este consistentă dacă și numai dacă are un model*.

Se observă că, în exemplele de mai sus, modelele teoriilor sînt obiecte construite în cadrul teoriei (axiomatice) a mulțimilor (care este mai largă decît teoriile respective). O teoremă a lui Gödel afirmă, într-o exprimare neriguroasă, că un model pentru o teorie axiomatică poate fi construit doar într-o teorie mai largă. Așadar, un eventual model pentru ZF (care i-ar demonstra consistența) nu ar putea fi construit decît într-o teorie mai largă. Însă ZF este suficient de cuprinzătoare pentru a putea servi drept fundament al întregii matematici; pe de altă parte, verificarea consistenței unei ipotetice teorii mai largi revine la construcția unei teorii și mai largi ș.a.m.d. Se vede că această cale nu conduce la o demonstrație a consistenței teoriei ZF. Se poate doar presupune că teoria ZF nu conduce la apariția de contradicții (de fapt, am văzut că a fost creată tocmai pentru a elimina contradicțiile apărute în teoria naivă a mulțimilor). În acest sens, este grăitor următorul citat din MANIN [1977], p. 102:

Problema consistenței formale a axiomelor Zermelo-Fraenkel trebuie să rămînă o chestiune de credință, cu excepția cazului cînd o eventuală inconsistență formală este demonstrată. Pînă acum toate demonstrațiile bazate pe aceste axiome nu au dus niciodată la o contradicție; dimpotrivă, au deschis în fața noastră bogata lume a matematicilor clasice și moderne. Această lume are o anumită realitate și o viață proprii, care depind în mică măsură de formalismele alese pentru a le descrie. O descoperire a unei contradicții în oricare din diversele formalisme, chiar dacă ar apărea, ar servi doar la clarificarea, rafinarea și poate reconstrucția unor anumite idei, dar nu ar conduce la falimentul lor, cum s-a întîmplat de mai multe ori în trecut.

Independența axiomelor are și ea legătură cu consistența. Să exemplificăm aceasta pe cazul unei noi axiome, *axioma fundării*.

Axioma fundării (AF). *Orice mulțime nevidă conține un element de care este disjunctă:*

$$(\forall a)[a \neq \emptyset \rightarrow (\exists b)(b \in a \wedge b \cap a = \emptyset)].$$

Acest enunț implică: *Nici o mulțime nu este element al ei însăși.* Într-adevăr, dacă avem o mulțime x astfel încât $x \in x$, atunci $\{x\}$ contrazice axioma fundării: singurul element al lui $\{x\}$ este x și avem $x \cap \{x\}$ nevidă, căci conține pe x . Mai mult, nu există „lanțuri de mulțimi” de forma $x_0 \in x_1 \in x_2 \in \dots \in x_n \in x_0$. Dacă ar exista un asemenea lanț, atunci mulțimea $\{x_0, x_1, \dots, x_n\}$ contrazice AF (de ce?). La fel, nu poate exista un șir $(x_n)_{n \in \omega}$ astfel încât $x_{n+1} \in x_n, \forall n \in \omega$. AF își datorează numele faptului că, pentru orice mulțime x , orice lanț de forma $x \ni x_0 \ni x_1 \ni \dots \ni x_n \ni \dots$ este finit și se termină cu $\emptyset$: $\exists n$ astfel încât $x \ni x_0 \ni x_1 \ni \dots \ni x_n \ni \emptyset$: orice șir descrescător (față de relația $\in$) este finit și „fundat” pe $\emptyset$.²¹

S-a demonstrat că, dacă acceptăm că ZF este consistentă, atunci ZF + AF (sistemul ZF la care se adaugă AF) nu conduce la contradicții. Această probare a *consistenței relative* a AF s-a realizat prin construirea unui model (în cadrul ZF) care satisface ZF + AF. În plus, s-a construit un alt model (tot în cadrul ZF) care satisface ZF și *negația AF*. Din aceste două rezultate se vede că AF este independentă de ZF (nu poate fi dedusă din axiomele ZF).

Un alt rezultat în această direcție este demonstrarea *independenței axiomei infinității față de restul axiomelor ZF*, printr-un procedeu principal asemănător cu cel de mai sus.

Axioma alegerii (AC)²² este o nouă axiomă care joacă un rol deosebit în matematică, datorită faptului că, pe de o parte, are un enunț aparent „evident”; pe de altă parte, are un caracter neconstructiv care i-a atras multe critici. Există multe enunțuri echivalente cu această axiomă. În formularea lui Zermelo, AC se enunță:

Pentru orice mulțime A în care elementele sînt disjuncte două cîte două²³, există o mulțime care conține exact un element din fiecare mulțime nevidă din A :

$$(\forall A)[(\forall x)(\forall y)(x \in A \wedge y \in A \wedge x \neq y) \rightarrow x \cap y = \emptyset] \rightarrow$$

$$(\exists c)[(\forall x)(x \in A \wedge x \neq \emptyset) \rightarrow (\exists z)(c \cap x = \{z\})].$$

Altfel spus, putem „alege” cîte un element din fiecare mulțime nevidă din A și forma cu ele o nouă mulțime. Controversele privind această axiomă provin și din faptul că se postulează existența unei astfel de mulțimi și implicit a unui „procedeu de alegere” a unui element dintr-o mulțime nevidă. În 1963 s-a demonstrat că AC nu poate fi dedusă din ZF. În majoritatea matematicilor contemporane, AC este acceptată alături de ZF, în sistemul numit ZFC.

Există numeroase enunțuri echivalente cu Axioma Alegerii. Iată cîteva:

²¹ Astfel, întregul univers descris de ZF și AF este "creat" pornind de la $\emptyset$ (universul "von Neumann", vezi MANIN [1977], p. 95-102).

²² Acronimul expresiei Axiom of Choice.

²³ Reamintim că elementele lui A sînt tot mulțimi.

Principiul bunei ordonări (Zermelo 1904). *Orice mulțime nevidă A poate fi bine ordonată (există o relație de bună ordine pe A).*

Produsul cartezian al unei familii de mulțimi nevide este nevid.

*Pentru orice mulțime a , există o funcție de alegere $f: a \rightarrow \bigcup a$ (adică f are proprietatea că, $\forall x \in a, x \neq \emptyset \rightarrow f(x) \in x$).*²⁴

Pentru orice funcție surjectivă $\phi: E \rightarrow F$ există $\psi: F \rightarrow E$ astfel încât $\phi\psi = id_F$.

Lema lui Zorn. *Fie $(A, \leq)$ o mulțime ordonată nevidă în care orice submulțime total ordonată este majorată (mulțime „inductiv ordonată”). Atunci A conține un element maximal.*

Lema lui Zorn este folosită în algebră în demonstrarea unor teoreme importante: existența unei baze într-un spațiu vectorial oarecare, existența idealelor maximale într-un inel, existența închiderii algebrice a unui corp comutativ.

În continuare prezentăm câteva noțiuni de *teoria cardinalilor*. Pentru o tratare mai în detaliu, vezi MIRON, NĂSTĂSESCU [1974], SCORPAN.

5.28 Definiție. Fie A și B două mulțimi. Spunem că A și B sînt *echipotente* (sau că sînt *cardinal echivalente*, sau că *au același cardinal*) dacă există o bijecție $f: A \rightarrow B$. Scriem atunci $A \sim B$ sau $|A| = |B|$.

Pentru orice mulțimi A, B, C , au loc:

- a) $A \sim A$ (reflexivitate);
- b) Dacă $A \sim B$, atunci $B \sim A$ (simetrie);
- c) Dacă $A \sim B$ și $B \sim C$, atunci $A \sim C$ (tranzitivitate).

Astfel, putem spune că relația de echipotență " $\sim$ " este o relație de echivalență pe clasa mulțimilor. Clasa²⁵ tuturor mulțimilor echipotente cu o mulțime dată A se numește *cardinalul mulțimii A* și se notează $\text{card } A$ sau $|A|$. Spunem că A este o mulțime *finită* cu n elemente ($n \in \mathbb{N}$) dacă $A \sim \{1, \dots, n\}$ și atunci notăm $|A| = |\{1, \dots, n\}| =: n$. O mulțime care nu este finită se numește *infinită*. Se poate demonstra că: *mulțimea A este infinită $\Leftrightarrow$ există o funcție injectivă $\phi: A \rightarrow A$ care nu este surjectivă $\Leftrightarrow$ există o funcție injectivă $\psi: \mathbb{N} \rightarrow A$.*

Dacă $|A| = |\mathbb{N}|$, spunem că A este o mulțime *numărabilă*.

Se introduce o *relație de ordine* între cardinali: spunem că $|A| \leq |B|$ dacă există o funcție injectivă $\phi: A \rightarrow B$. Definiția este corectă: dacă $A \sim A', B \sim B'$ și există o funcție injectivă $\phi: A \rightarrow B$, atunci există o funcție injectivă $\phi': A' \rightarrow B'$ (demonstrați!).

Se verifică imediat că, pentru orice mulțimi A, B, C are loc:

- a) $|A| \leq |A|$ (reflexivitate);
- b) $|A| \leq |B|$ și $|B| \leq |C|$ implică $|A| \leq |C|$ (tranzitivitate);

²⁴ Altfel spus, funcția f "alege" câte un element $f(x)$ din fiecare mulțime nevidă $x \in a$.

²⁵ Nu putem vorbi de "mulțimea tuturor mulțimilor echipotente cu A ".

Are loc următoarea teoremă importantă, care arată că $\leq$ este și *antisimetrică* (deci are într-adevăr aceleași proprietăți ca o relație de ordine).

5.29 Teoremă. (Cantor-Schröder-Bernstein) *Fie A și B două mulțimi. Dacă $|A| \leq |B|$ și $|B| \leq |A|$, atunci $|A| = |B|$.*

Demonstrație. Idee: să găsim $D \subseteq A$ astfel încât $A \setminus D \subseteq \text{Img}$ și $\alpha: A \rightarrow B$, dată de:

$$\alpha(a) = \begin{cases} f(a) & \text{dacă } a \in D \\ g^{-1}(a) & \text{dacă } a \notin D \end{cases}$$

să fie o bijecție (faceți un desen!). Trebuie să avem atunci $A \setminus D = g(B \setminus f(D))$, adică $D = A \setminus g(B \setminus f(D))$.

Pentru a găsi D ca mai sus, definim $\varphi: \mathcal{P}(A) \rightarrow \mathcal{P}(A)$, $\varphi(E) := A \setminus g(B \setminus f(E))$, $\forall E \in \mathcal{P}(A)$. Noi căutăm un D cu $\varphi(D) = D$.

Se arată ușor că φ este *crescătoare*: dacă $E \subseteq F$, atunci $\varphi(E) \subseteq \varphi(F)$.

Definim $M := \{E \subseteq A \mid E \subseteq \varphi(E)\}$. Evident, M este nevidă căci, de exemplu, $\emptyset \in M$.

Fie $D := \bigcup \{E \mid E \in M\}$. Să arătăm că $\varphi(D) = D$. Avem $\varphi(D) = \varphi(\bigcup \{E \mid E \in M\}) = \bigcup \{\varphi(E) \mid E \in M\} \supseteq \bigcup \{E \mid E \in M\} = D$. Deci $D \subseteq \varphi(D)$. Aplicând φ acestei incluziuni, obținem $\varphi(D) \subseteq \varphi(\varphi(D))$ adică $\varphi(D) \in M$. De aici, $D = \bigcup \{E \mid E \in M\} \supseteq \varphi(D)$. Astfel, $\varphi(D) = D$. Lăsăm cititorului verificarea faptului că α este bijecție. $\square$

Relația de ordine $\leq$ este și *totală* (demonstrația face apel la Axioma Alegerii):

5.30 Teoremă. *Oricare ar fi două mulțimi A, B , are loc $|A| \leq |B|$ sau $|B| \leq |A|$.* $\square$

Această ultimă proprietate este echivalentă cu Axioma Alegerii.

Exerciții

1. Fie A, B mulțimi. Scrieți o expresie a limbajului formal care să semnifice că:
 - a) Mulțimea A nu este inclusă în mulțimea B .
 - b) $A \neq B$ (folosiți doar relația de apartenență).
 - b) Dacă $f: A \rightarrow B$ este o funcție, iar $C, D \subseteq A$, scrieți că $f(C) = f(D)$.
2. Demonstrați că axioma infinității este echivalentă cu enunțul: *Există un ordinal infinit*.
3. Demonstrați că clasa ordinarilor On nu este mulțime („paradoxul Burali-Forti”).
4. Demonstrați că reuniunea unei mulțimi A de ordinale este un ordinal și este marginea superioară a lui A în On .
5. Un ordinal se numește *ordinal limită* dacă nu are un predecesor. Arătați că ω este cel mai mic ordinal limită și că axioma infinității este echivalentă cu afirmația: *Există un ordinal limită*. Care este succesorul lui ω ?

6. Arătați că ordinalul α este ordinal limită dacă și numai dacă $\alpha = \sup \{\beta \mid \beta \in \alpha\}$ (margine superioară în On).

7. Inducția transfinită (pe clasa ordinaletor On) se face adesea distingînd cazul ordinaletor limită. Mai precis, demonstrați că dacă o expresie $P(x)$ are proprietățile:

a) $P(\emptyset)$ adevărată;

b) $\forall \alpha [(On(\alpha) \wedge P(\alpha)) \rightarrow P(\alpha + 1)]$;

c) Pentru orice ordinal limită λ , dacă $P(\beta)$ adevărată, $\forall \beta < \lambda$, atunci $P(\lambda)$ adevărată, atunci $P(\alpha)$ adevărată pentru orice ordinal α .

8. Axioma infinității face referire la mulțimea vidă $\emptyset$, a cărei existență rezultă din existența măcar a unei mulțimi. Dar acest lucru este asigurat de axioma infinității. Cum se poate ieși din acest (aparent) cerc vicios?

9. Arătați că, pentru orice mulțime A , are loc $|\mathcal{P}(A)| > |A|$.

10. (Reprezentarea unui număr în baza b) Fie b un număr natural nenul fixat (numit *bază de numerație*). Demonstrați că, $\forall a \in \mathbb{N}$, există și sînt unice $n \in \mathbb{N}^*$ și $c_0, \dots, c_{n-1} \in \{0, 1, \dots, b-1\}$, astfel încît

$$a = c_{n-1}b^{n-1} + \dots + c_1b + c_0 \quad (R)$$

În cazul în care are loc egalitatea (R) de mai sus, se mai scrie $a = \overline{c_{n-1} \dots c_1 c_0}$, scriere numită *reprezentarea lui a în baza b* . Numerele naturale $0, 1, \dots, b-1$ se numesc *cifre*²⁶ în baza b (pentru scrierea concretă se dau b simboluri care reprezintă aceste cifre și nu se folosește bara superioară, scrisă aici pentru a evita confuzia cu produsul $c_{n-1} \dots c_1 c_0$). Uneori, în notație, se mai specifică baza b , ca indice. De exemplu, $105_7 = 54_{10}$. (Ind. Din teorema împărțirii cu rest aplicată lui a și b , $\exists!$ $q, r \in \mathbb{N}$ astfel încît $a = bq + r$. Se pune $c_0 = r$ și se repetă procedeul pentru q – sau, mai riguros, se aplică o inducție după a . Pentru unicitate, se observă că c_0 este restul împărțirii lui a la b și se aplică o inducție după cel mai mic număr de cifre din ipoteticele reprezentări ale lui a în baza b).

11. Reprezentați în baza 10 numerele 1011_2 , 1212_3 . Scrieți în bazele 2, 7, 16, numerele 129_{10} , 1152_{10} .

²⁶ A se remarca distincția între *număr* și *cifră* (într-o bază fixată). De exemplu, cifrele în baza 16 (sistem *hexadecimal*) sînt 0, 1, 2, 3, 4, 5, 6, 7, 8, 9, A, B, C, D, E, F, unde A reprezintă pe 10 (scris în baza zece), B pe 11, ...

II. Mulțimi factor și construcții de structuri numerice fundamentale

Presupunând cunoscută mulțimea $\mathbb{N}$ a numerelor naturale, înzestrat cu operațiile de adunare și înmulțire (cu proprietățile cunoscute) și cu structura sa de ordine uzuală ($\mathbb{N}$ este o mulțime *bine ordonată*), se pune problema *construirii celorlalte structuri numerice de bază*: $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, la care putem adăuga inelele de clase de resturi $\mathbb{Z}_n$.

Se impune un comentariu privind noțiunea de „număr”. În multe cărți se pun întrebări (probleme) de genul „ce este *numărul* (eventual rațional sau real sau complex)”, urmînd ca autorul să dea un răspuns de natură filozofică sau matematică. Noțiunea de *număr* (privit ca element individual, izolat) nu are o semnificație deosebită în matematică, mult mai importantă fiind cea de *structură pe o mulțime numerică*. Astfel, de pildă mulțimea $\mathbb{R}$ a numerelor reale este importantă prin *structurile* cu care este înzestrată: structura *algebrică* de corp comutativ, cea de *ordine* (este total ordonată și orice submulțime majorată are supremum), cea *topologică* derivată din acestea (este spațiu metric complet); un număr real, luat ca element individual al lui $\mathbb{R}$, nu poate fi pus nicidecum în legătură cu astfel de proprietăți. Insistăm asupra acestei distincții pentru că o conștientizare a ei își poate pune amprenta și asupra stilului de predare a acestor concepte fundamentale.

II.1. Relații de echivalență și mulțimi factor

Relațiile de echivalență sînt un instrument esențial în matematică, mai ales în problemele de *construcții* de obiecte (structuri) noi. Vom descrie un procedeu general, *construcția mulțimii factor (cît) în raport cu o relație de echivalență*, care, aplicat în diverse cazuri particulare, duce la construcții importante. Trebuie subliniat că mulțimea factor obținută se înzestrează cu o structură care este de obicei legată de structura mulțimii inițiale (ceea ce presupune o *compatibilitate între relația de echivalență și structura inițială*). Această metodă permite construcția unor structuri matematice importante: $\mathbb{Z}$ (construit ca mulțime factor a lui $\mathbb{N} \times \mathbb{N}$), $\mathbb{Q}$ (mulțime factor a lui $\mathbb{Z} \times \mathbb{Z}^*$; același procedeu dă în general inele și corpuri de fracții), $\mathbb{R}$ (mulțime factor a mulțimii șirurilor Cauchy de numere raționale), $\mathbb{C}$ (mulțime factor

a inelului de polinoame $\mathbb{R}[X]$). Remarcăm că majoritatea construcțiilor în matematică sînt mulțimi factor în raport cu o anumită relație de echivalență: produsul tensorial a două module, grupul liber pe o mulțime, spațiile proiective din geometrie, spațiile L^p din analiză, ... și lista este departe de a fi completă.

Fie A o mulțime și ρ o relație de echivalență pe A . Mulțimea

$$\{x \in A \mid x\rho a\}$$

poartă numele de *clasa de echivalență* a elementului a relativ la relația ρ și se notează cu $\hat{a}$. Se folosesc adesea multe alte notații, depinzînd de cazul particular ales și de dorința de a include sau nu relația ρ în notație. De exemplu, clasa lui a se mai notează C_a , $\bar{a}$, $\hat{a}_\rho$, $[a]_\rho$ etc.

Dacă pentru elementele a și b are loc $a\rho b$, mai spunem că a și b sînt *echivalente modulo ρ* .

1.1 Definiție. Mulțimea claselor de echivalență în raport cu relația ρ se numește *mulțimea cît* (sau *factor*) a lui A în raport cu ρ și se notează cu A/ρ . Deci $A/\rho := \{\hat{a} \mid a \in A\}$.

1.2 Propoziție. Fie ρ o relație de echivalență pe A . Atunci:

- a) $\forall a \in A$ are loc $a \in \hat{a}$ (deci $\hat{a}$ este nevidă).
- b) $\forall a, b \in A$, avem: $\hat{a} = \hat{b} \Leftrightarrow a\rho b$.
- c) $\forall a, b \in A$, are loc fie $\hat{a} = \hat{b}$, fie $\hat{a} \cap \hat{b} = \emptyset$.
- d) $\bigcup_{a \in A} \hat{a} = A$. □

O mulțime P de submulțimi nevide ale lui A , disjuncte două cîte două, a căror reuniune este A , este numită *partiție* a lui A . Mai precis, avem:

- a) $\forall B (B \in P) \rightarrow B \neq \emptyset$;
- b) $\forall B [(B \in P) \wedge (C \in P) \wedge (B \neq C)] \rightarrow (B \cap C = \emptyset)$;
- c) $\bigcup \{B \mid B \in P\} = A$.

Propoziția anterioară nu spune altceva decît că *mulțimea factor a lui A în raport cu o relație de echivalență este o partiție a lui A* . Reciproc, orice partiție poate fi obținută dintr-o relație de echivalență:

1.3 Propoziție. Fie P o partiție a mulțimii A . Atunci relația ρ definită prin:

$$\forall a, b \in A, a\rho b \Leftrightarrow \exists B \in P \text{ astfel încît } a \in B \text{ și } b \in B$$

este o relație de echivalență pe A și P este chiar mulțimea cît A/ρ . □

În aplicații, mulțimea inițială are de obicei o *structură* (algebrică, topologică, de ordine,...), iar relația de echivalență este *compatibilă* cu structura dată (sensul precis al acestei compatibilități fiind definit în fiecare caz în parte; în general, definiția este „naturală”). Atunci mulțimea factor obținută va moșteni o structură de același tip ca mulțimea inițială. Vom prezenta exemple de aplicare în algebră a acestei construcții fundamentale (trecerea de la o mulțime la mulțimea factor în raport cu o relație de echivalență) în paragrafele următoare.

Un concept important este cel de *sistem de reprezentanți*.

1.4 Definiție. Fie ρ o relație de echivalență pe mulțimea A . Spunem că submulțimea $S \subseteq A$ este un *sistem de reprezentanți*²⁷ pentru clasele de echivalență (modulo ρ) dacă orice element din A este echivalent modulo ρ cu exact un element din S . Intuitiv, un sistem de reprezentanți se obține „alegînd” din fiecare clasă de echivalență cîte un element („reprezentantul” clasei respective). Astfel S este sistem de reprezentanți dacă și numai dacă:

$$(\forall a \in A)(\exists s \in S)(a \rho s) \wedge (\forall s, t \in S)(s \rho t \rightarrow s = t).$$

1.5 Exerciții. a) Fie relația de echivalență definită pe $\mathbb{R}^2$ (identificat cu un plan în care s-a ales un sistem de coordonate Oxy): $(x, y) \sim (z, t) \Leftrightarrow x = z$. Clasele de echivalență sînt dreptele paralele cu Oy . Un sistem de reprezentanți este (de exemplu) $\{(x, 0) \mid x \in \mathbb{R}\}$. Mulțimea factor $\mathbb{R}^2 / \sim$ este în bijecție cu $\mathbb{R}$. Cum se poate defini o relație de echivalență pe $\mathbb{R}^2$ astfel încît clasele de echivalență să fie dreptele paralele cu o dreaptă fixată ce trece prin origine, de ecuație $y = \alpha x$?

b) Puteți defini o relație de echivalență pe $\mathbb{R}^2$ astfel încît clasele de echivalență să fie cercurile concentrice cu centrul în origine? Dar pătrate centrate în origine, cu laturile paralele cu axele? Dar pătrate centrate în origine, cu laturile paralele cu bisectoarele sistemului de axe?

c) Pe $\mathbb{R}$ definim relația de „congruență modulo $\mathbb{Z}$ ”: pentru $x, y \in \mathbb{R}$, spunem că $x \equiv y \pmod{\mathbb{Z}}$ dacă $x - y \in \mathbb{Z}$. Un sistem de reprezentanți este dat de intervalul $[0, 1)$. Acesta este un caz particular de grup factor (în cazul nostru $\mathbb{R}/\mathbb{Z}$).

d) *Închiderea tranzitivă a unei relații.* Fie ρ o relație pe mulțimea A . Definim o nouă relație τ_ρ pe A , astfel: $\forall a, b \in A, a \tau_\rho b \Leftrightarrow \exists n \in \mathbb{N}$ și $x_1, \dots, x_n \in A$ astfel încît $a = x_1, b = x_n$ și $x_i \rho x_{i+1}, i = 1, \dots, n-1$. Atunci τ_ρ este o relație *tranzitivă* pe A . Mai mult, τ_ρ este cea mai mică (în sensul incluziunii) relație tranzitivă pe A care include relația ρ .

II.2. Inelul numerelor întregi

Necesitatea considerării numerelor negative apare din considerente practice, binecunoscute cititorilor (pentru a modela situații precum: temperaturi negative, datorii în conturi bancare etc.), dar și din considerente matematice: diferența a două numere naturale nu este întotdeauna definită ca un număr natural. Formulată altfel, nu pentru orice $a, b \in \mathbb{N}$ ecuația $x + a = b$ are soluții $x \in \mathbb{N}$.

De aici apare și ideea de a concepe un „număr întreg negativ” ca o *diferență* de numere naturale. Bineînțeles, pentru o „diferență” dată există mai multe (chiar o infinitate de) perechi de numere naturale care au aceeași diferență: de exemplu perechile $(0, 1), (1, 2), (2, 3), \dots$ au

²⁷ O denumire mai corectă, dar mai greu de manipulat, este *sistem complet și independent de reprezentanți*.

aceeași diferență (numărul întreg -1). Ar trebui deci să vedem un număr întreg ca pe o pereche de numere naturale (de forma (a, b)), cu convenția că „se consideră egale” două perechi (a, b) și (c, d) dacă $a - b = c - d$. Cum scăderea nu este definită pentru orice pereche de numere naturale, rescriem această condiție sub forma $a + d = b + c$. Exprimăm riguros aceste considerații euristice:

Pe mulțimea $\mathbb{N} \times \mathbb{N}$ se consideră relația $\sim$, definită prin:

$$\forall (a, b), (c, d) \in \mathbb{N} \times \mathbb{N} : (a, b) \sim (c, d) \Leftrightarrow a + d = b + c$$

Se demonstrează (verificați!) că aceasta este o relație de echivalență. O clasă de echivalență în raport cu această relație o numim *număr întreg*, iar mulțimea factor $\mathbb{N} \times \mathbb{N} / \sim$ se numește *mulțimea numerelor întregi* și se notează cu $\mathbb{Z}$.

Notăția $\mathbb{Z}$ provine de la cuvântul german *zahl* (pronunțat *țal*, cu un *a* lung), care înseamnă *număr*. A se observa grafia ($\mathbb{Z}$ și nu Z), litera $\mathbb{Z}$ scrisă astfel fiind rezervată exclusiv notării mulțimii numerelor întregi (după cum $\mathbb{N}$ este folosită exclusiv pentru mulțimea numerelor naturale).

Nu ne putem opri aici cu construcția. Trebuie arătat că obiectul pe care l-am construit (riguros) satisface toate proprietățile pe care ne-am aștepta să le aibă mulțimea numerelor întregi: „include” mulțimea $\mathbb{N}$, orice număr întreg este sau număr natural, sau opusul unui număr natural, este definită o adunare și o înmulțire în raport cu care este inel, este o mulțime total ordonată, iar ordinea este compatibilă cu adunarea și înmulțirea.

Mai întâi să determinăm un sistem de reprezentanți. Mulțimea

$$Z := \{(a, 0) \mid a \in \mathbb{N}\} \cup \{(0, a) \mid a \in \mathbb{N}^*\}$$

este sistem de reprezentanți: dacă $a \geq b$, atunci $(a, b) \sim (a - b, 0)$, iar dacă $a < b$, atunci $(a, b) \sim (0, b - a)$. Vom *identifica* numărul natural a cu clasa de echivalență a lui $(a, 0)$ (lucru permis de faptul că aplicația care duce a în $(a, 0)$ este injectivă de la $\mathbb{N}$ la $\mathbb{N} \times \mathbb{N} / \sim$, demonstrați!) și vom nota cu $-a$ clasa de echivalență a lui $(0, a)$. Ce mai trebuie verificat pentru a demonstra că Z , definit mai sus, este sistem de reprezentanți?

Cu aceste identificări, putem scrie:

$$\mathbb{Z} = \{a \mid a \in \mathbb{N}\} \cup \{-a \mid a \in \mathbb{N}^*\}.$$

Să definim *operațiile de adunare și înmulțire* pe $\mathbb{Z}$ (pornind de la cele de pe $\mathbb{N}$). Pentru aceasta, se definesc operații pe clasele de echivalență din $\mathbb{Z} = \mathbb{N} \times \mathbb{N} / \sim$, folosind reprezentanți oarecare, urmînd să se demonstreze că nu depind de reprezentanți și deci sînt corect definite. De exemplu, notînd cu $\overline{(a, b)} \in \mathbb{N} \times \mathbb{N} / \sim$ clasa lui $(a, b) \in \mathbb{N} \times \mathbb{N}$, definim

$$\overline{(a, b)} + \overline{(c, d)} := \overline{(a + c, b + d)}.$$

Bineînțeles, $a + c$ semnifică suma în $\mathbb{N}$ a numerelor naturale a și c . Operația este *corect definită*.²⁸ Aceasta înseamnă că, $\forall (a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$ cu $(a, b) \sim (a', b')$ și $(c, d) \sim (c', d')$, atunci $(a + c, b + d) \sim (a' + c', b' + d')$. Verificarea este ușoară și constă în aplicarea definițiilor relației de echivalență și a operației $+$.

Invităm cititorul să definească înmulțirea, să demonstreze corectitudinea definiției și proprietățile uzuale ale operațiilor, care conferă lui $\mathbb{Z}$ structură de *inel comutativ și unitar, fără divizori ai lui 0* (se mai spune că $\mathbb{Z}$ este *inel integru* sau *domeniu de integritate*).

Relația de ordine pe $\mathbb{Z}$: fie $(a, b), (c, d) \in \mathbb{N} \times \mathbb{N}$. Spunem că $\overline{(a, b)} \leq \overline{(c, d)}$ dacă și numai dacă $a + d \geq b + c$ în $\mathbb{N}$ (de ce am definit astfel?). Demonstrați corectitudinea definiției și faptul că se obține o *relație de ordine totală* pe $\mathbb{Z} = \mathbb{N}/\sim$.

Se mai pot defini operațiile pe $\mathbb{Z}$ (respectiv relația de ordine pe $\mathbb{Z}$) folosind sistemul de reprezentanți Z de mai sus și operațiile din $\mathbb{N}$ (cum?). Ce avantaje și dezavantaje au cele două abordări?

O funcție deosebit de importantă este funcția *valoare absolută* (sau *modul*) $|| : \mathbb{Z} \rightarrow \mathbb{Z}$,

$$|x| = \begin{cases} x & \text{dacă } x \geq 0 \\ -x & \text{dacă } x < 0 \end{cases}$$

Importanța acestei funcții apare în legătură cu faptul că $\mathbb{Z}$ este *inel euclidian*, adică are loc:

2.1 Teoremă. (Teorema împărțirii cu rest în $\mathbb{Z}$) *Pentru orice numere întregi a, b , cu $b \neq 0$, există $q, r \in \mathbb{N}$, astfel încât $a = bq + r$, cu $r = 0$ sau $|r| < |b|$ (q se numește cît, iar r rest al împărțirii lui a la b). Dacă se impune și $r > 0$, q și r sînt unic determinate cu aceste proprietăți.* $\square$

II.3. Corpul numerelor raționale. Inele și corpuri de fracții

În gimnaziu, se introduc mai întîi doar numerele raționale *pozitive*, din motive didactice. Această distincție oarecum artificială nu își are locul aici. Din punct de vedere algebric, construcția lui $\mathbb{Q}$ pornind de la $\mathbb{Z}$ este principial aceeași cu construcția *corpului de fracții al unui inel integru oarecare* R .

Introducerea lui $\mathbb{Q}$ este motivată, printre altele, de imposibilitatea efectuării unor împărțiri în $\mathbb{Z}$. De exemplu, nu este definit rezultatul (cîtul) împărțirii lui 3 la 2; altfel spus, ecuația $3x = 2$ nu are soluții în $\mathbb{Z}$. Mai general, dacă $b, a \in \mathbb{Z}$ și a nu divide b , ecuația $bx = a$ nu are

²⁸ Subliniem că necesitatea demonstrării corectitudinii definiției apare tot timpul cînd se dau definiții pe o mulțime factor, folosind reprezentanți oarecare ai claselor.

soluții în $\mathbb{Z}$. Apare ideea (similară cu aceea de la construcția precedentă a lui $\mathbb{Z}$) de a introduce o nouă mulțime de numere (numerele *raționale*) ca fiind „toate cîturile posibile de numere întregi”. De exemplu, cîtul împărțirii lui 3 la 2 va fi „numărul rațional” („fracția”) $3/2$. Deoarece același cît este dat și de împărțirea lui 6 la 4 (sau a lui 9 la 6 etc.), este necesar să precizăm *cînd două fracții a/b și c/d sînt egale*. Aceasta revine la a defini o relație de echivalență pe mulțimea perechilor de forma (a, b) , cu $a, b \in \mathbb{Z}$, $b \neq 0$ (o fracție va fi o clasă de echivalență de perechi). Relația de echivalență este definită de

$$\forall (a, b), (c, d) \in \mathbb{Z} \times \mathbb{Z}^*, (a, b) \sim (c, d) \Leftrightarrow ad = bc.$$

Cititorul poate demonstra ușor că este vorba într-adevăr de o relație de echivalență.

O clasă de echivalență (un element al mulțimii $\mathbb{Z} \times \mathbb{Z}^* / \sim$) este notată cu a/b sau $\frac{a}{b}$ și este numit(ă) *fracție*; a este *numărătorul*, iar b este *numitorul* fracției a/b . Mulțimea fracțiilor (mulțimea cît $\mathbb{Z} \times \mathbb{Z}^* / \sim$) se notează prin tradiție cu $\mathbb{Q}$ (de la inițiala cuvîntului *quotient*, care înseamnă *cît* în engleză și în franceză). Mulțimea $\mathbb{Z}$ se poate identifica cu o parte a lui $\mathbb{Q}$: numărul întreg a se identifică cu fracția $\frac{a}{1}$. Pe $\mathbb{Q}$ se introduc operațiile de adunare și înmulțire, inspirate de regulile cunoscute din gimnaziu (aducerea la același numitor etc.):

$$\forall a/b, c/d \in \mathbb{Q}, \frac{a}{b} + \frac{c}{d} := \frac{ad + bc}{bd}, \frac{a}{b} \cdot \frac{c}{d} := \frac{ac}{bd}$$

Ca și la construcția lui $\mathbb{Z}$, trebuie arătat că *definițiile sînt corecte* (nu depind de alegerea reprezentanților fracțiilor) și că $\mathbb{Q}$, înzestrat cu aceste operații, este *inel comutativ unitar* (elementul nul este fracția $0/1$, iar elementul unitate este fracția $1/1$). Mai mult, $\mathbb{Q}$ este *corp*: orice element nenul $\frac{a}{b}$ are invers față de înmulțire: $\left(\frac{a}{b}\right)^{-1} = \frac{b}{a}$.

Importanța construcției de mai sus depășește cadrul elementar al construcției lui $\mathbb{Q}$; aceeași idee, cu modificări minore, se aplică la *construcția inelului de fracții al unui inel comutativ relativ la un sistem multiplicativ închis* al său, construcție fundamentală în toată matematica.

3.1 Definiție. Fie R un inel comutativ unitar. O submulțime nevidă S a lui R se numește *sistem multiplicativ închis* dacă $1 \in S$ și, oricare ar fi $x, y \in S$, rezultă $xy \in S$.

3.2 Observație. Ideea care motivează introducerea noțiunii de mai sus este următoarea: se dorește o construcție a unei mulțimi de fracții *cu numitori din S* . Cum produsul a doi numitori trebuie să fie tot un numitor, este naturală impunerea condiției ca S să fie parte stabilă la înmulțire. De asemenea, este naturală considerarea fracțiilor cu numitorul 1 (adică $1 \in S$). Exemple de sisteme multiplicative închise: $\mathbb{Z}^* = \mathbb{Z} \setminus \{0\}$ în $\mathbb{Z}$; $\mathbb{Z} \setminus 2\mathbb{Z}$ în $\mathbb{Z}$; $K[X] \setminus \{0\}$ în $K[X]$ (cu K un corp fixat și $K[X]$ inelul polinoamelor cu coeficienți în K).

Fixăm un *inel comutativ unitar* R și un *sistem multiplicativ închis* S al său. Ghidându-ne după echivalența binecunoscută $\frac{a}{s} = \frac{b}{t} \Leftrightarrow at = bs$, enunțăm următoarea:

3.3 Definiție. Pe mulțimea $R \times S$ se definește următoarea *relație*:

$$\forall (a, s), (b, t) \in R \times S, \text{ scriem } (a, s) \sim (b, t) \text{ dacă și numai dacă } at = bs. \quad (D)$$

Dacă $0 \notin S$ și S nu conține divizori ai lui zero în R (un element nenul $x \in R$ se numește divizor al lui zero dacă $\exists y \in R, y \neq 0$, astfel încât $xy = 0$), atunci relația definită este *relație de echivalență* (Exercițiu!).

În cazul în care S poate conține divizori ai lui zero este necesară modificarea definiției (D) :

$$\forall (a, s), (b, t) \in R \times S, (a, s) \sim (b, t) \Leftrightarrow \exists u \in S \text{ astfel încât } u(at - bs) = 0. \quad (D')$$

Este clar că, dacă S nu conține divizori ai lui zero și $0 \notin S$, (D) și (D') coincid.

Arătăm că D' este *relație de echivalență*:

- *reflexivitatea*: $\forall (a, s) \in R \times S$, avem $(a, s) \sim (a, s)$ căci $\exists 1 \in S$ astfel încât $1(as - as) = 0$.

- *simetria*: dacă $(a, s) \sim (b, t)$, atunci $\exists u \in S$ astfel încât $u(at - bs) = 0$, deci $u(bs - at) = 0$, adică $(b, t) \sim (a, s)$.

- *tranzitivitatea*: fie $(a, s), (b, t), (c, u) \in R \times S$, astfel încât $(a, s) \sim (b, t)$ și $(b, t) \sim (c, u)$. Din definiție, rezultă că $\exists x \in S$ astfel încât $x(at - bs) = 0$ și $\exists y \in S$ astfel încât $y(bu - ct) = 0$. Vrem să obținem o relație de forma $z(au - cs) = 0$, pentru un $z \in S$. Înmulțind cu uy , respectiv sx , obținem:

$$uyxat - uyxbs = 0$$

$$sxybu - sxyct = 0$$

Adunând membru cu membru și observând că $uyxbs = sxybu$, rezultă $uyxat - sxyct = 0$, adică $xyt(au - cs) = 0$. Cum $xyt \in S$ (sistem multiplicativ închis), aceasta înseamnă că $(a, s) \sim (c, u)$.

3.4 Definiție. Fie $(a, s) \in R \times S$. Clasa de echivalență a lui (a, s) în raport cu relația $\sim$ se notează cu $\frac{a}{s}$ sau a/s și se numește *fracție* (de *numitor* s și *numărător* a). Mulțimea $R \times S / \sim$ (mulțimea claselor de echivalență în raport cu relația $\sim$) se notează cu $S^{-1}R$. Deci

$$S^{-1}R := \{ a/s \mid a \in R, s \in S \}.$$

Direct din definiție rezultă regula de „amplificare a fracțiilor” cu numitori din S :

$$\frac{a}{s} = \frac{ta}{ts}, \forall s, t \in S, \forall a \in R.$$

Înzestrăm $S^{-1}R$ cu o structură de inel, inspirându-ne din regulile uzuale de adunare și înmulțire a două fracții. Fie $(a, s), (b, t) \in R \times S$. Definim:

$$\frac{a}{s} + \frac{b}{t} := \frac{ta + sb}{st}$$

$$\frac{a}{s} \cdot \frac{b}{t} := \frac{ab}{st}$$

3.5 Propoziție. Operațiile $+$ și $\cdot$ pe $S^{-1}R$ sînt bine definite și înzestreză pe $S^{-1}R$ cu o structură de inel comutativ și unitar. Elementele 0 și 1 în $S^{-1}R$ sînt:

$$0 = \frac{0}{1} = \frac{0}{s}, \forall s \in S;$$

$$1 = \frac{1}{1} = \frac{s}{s}, \forall s \in S.$$

Aplicația $\varphi: R \rightarrow S^{-1}R$, $\varphi(a) = a/1$, $\forall a \in R$, este un morfism unitar de inele, numit morfismul canonic (deci $S^{-1}R$ este o R -algebră comutativă (vezi definiția III.1.1)).

Demonstrație. Adunarea este corect definită. Fie $(a, s), (b, t), (a', s'), (b', t') \in R \times S$, astfel încît $(a, s) \sim (a', s')$ și $(b, t) \sim (b', t')$. Avem de arătat că $(ta + sb, st) \sim (t'a' + s'b', s't')$. Fie $u, v \in S$ astfel încît $u(s'a - sa') = 0$ și $v(t'b - tb') = 0$. Înmulțim prima egalitate cu $tt'v$ și a doua cu $ss'u$ și le adunăm. Obținem

$$vu((ta + sb)s't' - (t'a' + s'b')st) = 0.$$

Restul verificărilor sînt lăsate cititorului. □

Observăm că orice $s \in S$ are imaginea prin φ inversabilă în $S^{-1}R$: $\varphi(s) = s/1$ are inversul $1/s$. Deci construcția efectuată rezolvă problema pusă la început: chiar dacă ecuația $sx = b$ nu are soluții în R (unde $s \in S$), în $S^{-1}R$ există soluția $x = \frac{b}{s}$. Această proprietate a inelului de fracții este foarte importantă (vezi 3.9 mai jos).

3.6 Observație. a) Avem: $x/1 = 0$ în $S^{-1}R \Leftrightarrow \exists s \in S$ astfel încît $sx = 0$. Acest fapt este imediat din definiție.

b) Morfismul φ este injectiv $\Leftrightarrow S$ nu conține divizori ai lui 0.

Într-adevăr, fie φ injectiv. Dacă, prin absurd, $s \in S$ este divizor al lui 0, atunci $\exists x \in R$, $x \neq 0$, astfel încît $xs = 0$. Atunci $\varphi(x) = x/1 = 0$ (căci $sx = 0$), contradicție cu injectivitatea lui φ . Reciproca e propusă ca exercițiu.

c) Dacă $0 \in S$, atunci $S^{-1}R$ este inelul nul (căci $a/s = 0/1$, $\forall a \in R$, $\forall s \in S$: $\exists 0 \in S$ astfel încît $0 \cdot a = 0$). De aceea, în definiția sistemului multiplicativ închis se pune adesea condiția $0 \notin S$.

3.7 Cazuri particulare importante. Dacă R este inel integru și $S = R \setminus \{0\}$, atunci $S^{-1}R$ este corp, numit corpul total de fracții al lui R și notat uneori cu $Q(R)$. Într-adevăr, orice fracție nenulă a/b ($a, b \in R$, $b \neq 0$) are inversul b/a . În particular, $Q(\mathbb{Z}) = \mathbb{Q}$ (corpul de fracții al lui $\mathbb{Z}$ este $\mathbb{Q}$). Corpul de fracții al unui inel de polinoame $K[X]$ (unde K este corp) se notează cu $K(X)$ și se numește corpul fracțiilor raționale cu coeficienți în K .

3.8 Teoremă. (Proprietatea de universalitate a inelului de fracții) Fie R un inel unitar, comutativ și S un sistem multiplicativ închis în R . Atunci $S^{-1}R$ este un inel comutativ unitar și $\varphi: R \rightarrow S^{-1}R$ este un morfism unitar astfel încît $\varphi(s)$ este inversabil în S , $\forall s \in S$. Mai mult:

Pentru orice inel comutativ unitar T și orice morfism unitar $\gamma: R \rightarrow T$ astfel încât $\gamma(s)$ este inversabil în T , $\forall s \in S$, există un unic morfism de inele $g: S^{-1}R \rightarrow T$ astfel încât $\gamma = g\varphi$.

Demonstrație. Definim $g(a/s) = \gamma(a)(\gamma(s))^{-1}$, $\forall a \in R$, $\forall s \in S$. Lăsăm cititorului verificarea faptelor că g este corect definit, că este morfism și că este unic astfel încât $\gamma = g\varphi$. $\square$

În termeni de R -algebre, partea a doua a teoremei se formulează echivalent: pentru orice R -algebră comutativă T de morfism structural $\gamma: R \rightarrow T$, astfel încât $\gamma(s)$ este inversabil în T , $\forall s \in S$, există un unic morfism de R -algebre $g: S^{-1}R \rightarrow T$.

Teorema următoare exprimă faptul că proprietatea de universalitate a inelului de fracții determină inelul de fracții până la un (unic) izomorfism:

3.9 Teoremă. Fie R un inel unitar, comutativ și S un sistem multiplicativ închis în R . Presupunem că B este un inel comutativ unitar și $\beta: R \rightarrow B$ este un morfism astfel încât:

Pentru orice inel comutativ unitar T și orice morfism unitar $\gamma: R \rightarrow T$ astfel încât $\gamma(s)$ este inversabil în T , $\forall s \in S$, există un unic morfism de inele $g: B \rightarrow T$ astfel încât $\gamma = g\beta$.

Atunci există un unic izomorfism unitar de inele $h: S^{-1}R \rightarrow B$ astfel încât $h\varphi = \beta$.

Demonstrație. Definim $g(a/s) = \gamma(a)(\gamma(s))^{-1}$, $\forall a \in R$, $\forall s \in S$. Lăsăm cititorului verificarea faptului că definiția lui g este corectă, că g este morfism și că este unicul astfel încât $\gamma = g\varphi$. $\square$

Un exemplu important, destul de general, de sistem multiplicativ închis și de inel de fracții corespunzător este următorul:

3.10 Propoziție. Fie P un ideal prim în inelul R . Atunci $S := R \setminus P$ este un sistem multiplicativ închis în R și inelul de fracții $S^{-1}R$ are un unic ideal maximal (este inel local).

Demonstrație. Condiția de ideal prim este: dacă $a, b \notin P$, atunci $ab \notin P$, ceea ce arată că S este sistem multiplicativ închis. Dacă $I \leq R$, $I \cap S \neq \emptyset$, atunci $S^{-1}I = S^{-1}R$. Într-adevăr, dacă $s \in I \cap S$, atunci $s/1 \in S^{-1}I$ și este inversabil, deci $S^{-1}I = R$. Așadar, idealele proprii în $S^{-1}R$ sînt de forma $J = S^{-1}I$, cu $I \cap S = \emptyset$ ($\Leftrightarrow I \subseteq P$), adică $J \subseteq S^{-1}P$. Dar $S^{-1}P$ este ideal propriu: dacă $1/1 = p/s$, cu $p \in P$, $s \in S$, atunci $\exists u \in S$ astfel încât $u(s - p) = 0 \Rightarrow us \in P \Rightarrow u \in P$ sau $s \in P$, contradicție cu $S = R \setminus P$. Astfel, $S^{-1}P$ este unicul ideal maximal în $S^{-1}R$. $\square$

Dacă $S = R \setminus P$, cu P ideal prim, inelul de fracții $S^{-1}R$ se notează de obicei prin R_P și se numește *localizatul* în P al lui R . Avantajul acestei treceri este că se reduc multe probleme referitoare la idealul prim P din R la idealul maximal $S^{-1}P$ din localizatul $S^{-1}R$. De exemplu, dacă R este integru, atunci (0) este ideal prim și $R_{(0)}$ este corpul de fracții al lui R .

Menționăm că se pot construi inele de fracții - în anumite condiții - și în cazul inelelor necomutative (vezi de ex. NĂSTĂSESCU [1976]).

Revenim la corpul numerelor raționale $\mathbb{Q}$, care, în terminologia de mai sus, este *corpul total de fracții* al lui $\mathbb{Z}$. Rămîne să definim ordinea uzuală pe $\mathbb{Q}$.

3.11 Definiție. Fie a/b și $c/d \in \mathbb{Q}$, unde $a, b, c, d \in \mathbb{Z}$, cu $b, d > 0$. Definim:

$$a/b \leq c/d \Leftrightarrow ad \leq bc.$$

Corectitudinea definiției este propusă ca exercițiu.

3.12 Definiție. Un corp comutativ $(K, +, \cdot)$ se numește *corp ordonat* dacă este înzestrat cu o relație de ordine totală " $\leq$ " pe K astfel încât, $\forall a, b, c \in K$, au loc:

- i) $a \leq b \Rightarrow a + c \leq b + c$;
- ii) $a \leq b$ și $c \geq 0 \Rightarrow ac \leq bc$.

$\mathbb{Q}$ este un corp ordonat față de relația de ordine uzuală; mai mult, orice relație de ordine pe $\mathbb{Q}$ în raport cu care acesta devine un corp ordonat coincide cu ordinea uzuală (vezi Exerciții). O funcție deosebit de importantă pentru un corp ordonat K este *valoarea absolută (modulul)* $|| : K \rightarrow K$, definit la fel ca valoarea absolută pe $\mathbb{Z}$:

$$|x| = \begin{cases} x & \text{dacă } x \geq 0 \\ -x & \text{dacă } x < 0 \end{cases}$$

Exerciții

1. Fie $\mathbb{Z}[X]$ inelul polinoamelor cu coeficienți în $\mathbb{Z}$. Atunci $Q(\mathbb{Z}[X])$ (corpul de fracții al lui $\mathbb{Z}[X]$) este izomorf cu *corpul fracțiilor raționale* $\mathbb{Q}(X) := Q(\mathbb{Q}[X])$.
2. Este adevărat că, dacă inelele integrale R și S au proprietatea $Q(R) \cong Q(S)$, rezultă că $R \cong S$?
3. Demonstrați că orice element din $\mathbb{Q}$ se poate scrie ca o fracție a/b , cu $a, b \in \mathbb{Z}$ și $b > 0$.
4. Fie I un ideal în inelul R . Atunci $S^{-1}I := \{a/s \mid a \in I, s \in S\}$ este ideal în $S^{-1}R$. Mai mult, orice ideal din $S^{-1}R$ este de forma $S^{-1}I$, cu I ideal în R .
5. Demonstrați că relația de ordine uzuală pe $\mathbb{Q}$ (vezi def. II.3.11) este corect definită și $\mathbb{Q}$ devine corp ordonat.
6. Fie $(K, +, \cdot, \leq)$ un corp ordonat, cu element nul 0 și element unitate 1. Atunci, $\forall a, b, c \in K$, au loc: a) $a \leq b \Rightarrow -a \geq -b$; b) $0 < 1$; c) $0 < n \cdot 1, \forall n \in \mathbb{N}$; d) $0 < a$ și $0 < b \Rightarrow 0 < ab$ și $0 < a^{-1}$; e) $0 < a < b \Rightarrow 0 < b^{-1} < a^{-1}$.
În particular, car $K = 0$ (adică $n \cdot 1 \neq 0, \forall n \in \mathbb{N}^*$) și există un unic morfism de corpuri $\varphi : \mathbb{Q} \rightarrow K$ (cf. proprietatea de universalitate II.3.8 aplicată funcției $n \mapsto n \cdot 1$ de la $\mathbb{Z}$ la K). Morfismul φ este cu necesitate injectiv; arătați că este și morfism de ordine.
7. Demonstrați că relația de ordine uzuală este singura relație de ordine pe $\mathbb{Q}$ în raport cu care acesta devine corp ordonat.
8. Fie K un corp ordonat. Demonstrați că funcția valoare absolută $|| : K \rightarrow K$ are proprietățile uzuale ale modulului: a) $\forall x \in K \Rightarrow |x| \geq 0$; b) $\forall x \in K$, are loc: $|x| = 0 \Leftrightarrow x = 0$; c) $\forall x, y \in K \Rightarrow |x + y| \leq |x| + |y|$ (inegalitatea triunghiulară); d) $\forall x, y \in K \Rightarrow |x \cdot y| = |x| \cdot |y|$.

9. Arătați că nu orice submulțime nevidă majorată a lui $\mathbb{Q}$ are margine superioară.

II.4. Inele de clase de resturi $\mathbb{Z}_n$, inele factor

În mod tradițional, structurile „numerice” $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ sînt considerate de bază în matematică; cînd se face referire la noțiunea de „număr”, este de obicei vorba de un element al uneia din aceste mulțimi. Acest loc privilegiat este asigurat, în mare măsură, de rolul important pe care îl au aceste structuri în modelarea lumii reale (deși numerele complexe au fost mult timp privite ca niște creații pur abstracte ²⁹), lucru reflectat în importanța ce li se acordă în manualele de liceu și gimnaziu.

Considerăm că și structurile $\mathbb{Z}_n$ (inelele de clase de resturi modulo n) merită să ocupe un loc alături de aceste structuri, măcar din următoarele motive:

- construcția lor riguroasă este intuitivă și simplă (în comparație cu cea a lui $\mathbb{R}$, de exemplu), iar cunoașterea lor de către elevi prezintă evidente avantaje didactice.
- generalizarea directă la inele factor deschide calea către metodele algebrei moderne.
- au aplicații semnificative în matematică (mai ales în probleme de divizibilitate).
- calculatoarele, tehnologia informației și a comunicațiilor digitale (reprezentarea numerelor în calculator, implementarea operațiilor cu ele, codurile corectoare de erori, criptografia, securitatea datelor, ...), omniprezente în viața de astăzi, folosesc în mod intens inelele și corpurile *finite*, între care inelele de tip $\mathbb{Z}_n$ sînt cele mai la îndemînă.

Prezentăm mai întîi, pe scurt, etapele *construcției inelului de clase de resturi modulo n , $\mathbb{Z}_n$* . Apoi vom da construcția generală a inelului factor al unui inel R în raport cu un ideal I al său. Inelele factor intervin în multe alte construcții importante în matematică: corpurile $\mathbb{R}$ și $\mathbb{C}$, corpurile finite; o construcție asemănătoare celei a lui $\mathbb{R}$ (construit pornind de la $\mathbb{Q}$ și valoarea absolută uzuală pe $\mathbb{Q}$) permite obținerea corpurilor de numere *p-adice* (pornind de la $\mathbb{Q}$, un număr prim p și valoarea absolută *p-adică* pe $\mathbb{Q}$).

Fie n un număr întreg, fixat (numit *modul*).

4.1 Definiție. Spunem că numerele întregi a și b sînt *congruente modulo n* dacă n divide $a - b$. Scriem aceasta sub forma $a \equiv b \pmod{n}$.

4.2 Propoziție. Relația „ $\equiv \pmod{n}$ ” de congruență modulo n este o relație de echivalență pe $\mathbb{Z}$. □

²⁹ Vezi, de exemplu, sintagma „număr pur imaginar”...

Pentru orice $a \in \mathbb{Z}$, se notează cu $\hat{a}$ clasa lui a în raport cu relația de congruență modulo n . Avem deci $\hat{a} = \{b \in \mathbb{Z} \mid a \equiv b \pmod{n}\}$. Observăm că notația este ambiguă, în sensul că nu precizează modulul (numărul n); este deci necesară atenție și notații adecvate pentru evitarea confuziilor ce pot apărea în cazul folosirii mai multor relații de congruență. Mulțimea factor $\mathbb{Z}/\equiv \pmod{n}$ (adică $\{\hat{a} \mid a \in \mathbb{Z}\}$) se notează cu $\mathbb{Z}_n$ și se numește *mulțimea claselor de resturi modulo n* .

4.3 Exercițiu. a) Ce devine relația de congruență modulo n și mulțimea $\mathbb{Z}_n$ dacă $n = 0$ sau $n = 1$?

b) Două numere întregi a și b sînt congruente modulo n dacă și numai dacă „dau același rest la împărțirea cu n ”.

Pe $\mathbb{Z}_n$ se pot defini două operații (numite *adunarea*, respectiv *înmulțirea modulo n*), în raport cu care $\mathbb{Z}_n$ devine *inel comutativ și unitar*. Pentru orice $a, b \in \mathbb{Z}$, definim:

$$\begin{aligned}\hat{a} + \hat{b} &:= \widehat{a + b} \\ \hat{a} \cdot \hat{b} &:= \widehat{a \cdot b}\end{aligned}$$

Demonstrarea corectitudinii definițiilor de mai sus (adică independența de alegerea reprezentanților) și a axiomelor inelului este propusă cititorului.

Vom aplica ideea construcției de mai sus într-o situație mai generală. În acest scop, observăm că putem defini relația de congruență modulo n pe $\mathbb{Z}$ și în felul următor:

Notăm $n\mathbb{Z} := \{nk \mid k \in \mathbb{Z}\}$. Avem atunci, $\forall a, b \in \mathbb{Z}$:

$$a \equiv b \pmod{n} \Leftrightarrow a - b \in n\mathbb{Z}.$$

Mai mult, se vede imediat că $\hat{a} = \{a + nk \mid k \in \mathbb{Z}\}$, motiv pentru care $\hat{a}$ se mai notează cu $a + n\mathbb{Z}$. Deci, $\hat{0} = n\mathbb{Z}$, $\hat{1} = 1 + n\mathbb{Z}$ etc.

Mulțimea $n\mathbb{Z}$ este *ideal în $\mathbb{Z}$* , în sensul că este parte stabilă la adunare și, $\forall x \in \mathbb{Z}$, $\forall a \in n\mathbb{Z}$, rezultă că $xa \in n\mathbb{Z}$ ($n\mathbb{Z}$ este parte stabilă la înmulțirea cu *orice* element din $\mathbb{Z}$).

Mai general, dacă R este *inel* (presupus pentru simplitate *comutativ și unitar*), o submulțime nevidă I a sa se numește *ideal în R* (fapt notat $I \leq R$) dacă satisface condițiile:

- $\forall a, b \in I$, rezultă $a + b \in I$;
- $\forall a \in I, \forall r \in R$, rezultă $ra \in I$.

Se observă imediat că orice ideal I al lui R este subgrup al grupului aditiv $(R, +)$ (demonstrați!) și deci $0 \in I$. Idealul I se numește *propriu* dacă $I \neq R$.

Propoziția următoare arată că ideea de construcție a lui $\mathbb{Z}_n$ pornind de la $\mathbb{Z}$ și un ideal al său (de forma $n\mathbb{Z}$) se generalizează cuvînt cu cuvînt la cazul unui inel R și al unui ideal I al său.³⁰

³⁰ Afirmațiile rămîn valabile pentru un inel nu neapărat comutativ R și un ideal *bilateral* I al lui R .

Demonstrația constă în verificarea directă a proprietăților enunțate și o lășăm cititorului (și poate fi găsită în orice carte introductivă de algebră „modernă”).

4.4 Propoziție. Fie R un inel comutativ unitar și I un ideal al său.

a) Relația (de congruență modulo I), definită de:

$$a \equiv b \pmod{I} \Leftrightarrow a - b \in I$$

este o relație de echivalență pe I . Notînd cu $\hat{a} = \{b \in R \mid a \equiv b \pmod{I}\}$ (numită clasa lui a modulo I), are loc $\hat{a} = \{a + x \mid x \in I\}$ ($\hat{a}$ se mai notează $a + I$ din acest motiv).

b) Relația de congruență modulo I este compatibilă cu adunarea și înmulțirea din R , în sensul că, $\forall a, a', b, b' \in R$, au loc implicațiile:

$$a \equiv a' \pmod{I} \text{ și } b \equiv b' \pmod{I} \Rightarrow a + b \equiv a' + b' \pmod{I} \text{ și } a \cdot b \equiv a' \cdot b' \pmod{I}.$$

c) Operațiile pe mulțimea factor $R/I := \{\hat{a} \mid a \in R\}$, date de:

$$\hat{a} + \hat{b} := \widehat{a + b} \text{ și } \hat{a} \cdot \hat{b} := \widehat{a \cdot b}, \forall a, b \in R,$$

sînt corect definite și înzestrează pe R/I cu o structură de inel comutativ unitar (numit inelul factor al lui R în raport cu I).

d) Aplicația $\pi: R \rightarrow R/I$, $\pi(r) = \hat{r} = r + I$, $\forall r \in R$, este un morfism surjectiv de inele (numit surjecția canonică a inelului factor R/I). $\square$

În termeni mai puțin riguroși, trecerea de la inelul R la inelul factor R/I „duce toate elementele din I în zero” sau „anulează elementele lui I ”. Multe afirmații referitoare la idealul I în R se traduc prin afirmații referitoare la idealul 0 în R/I (un exemplu este 4.8), idee aplicată adesea în raționamente.

4.5 Observație. Are loc o afirmație reciprocă celei de la b): dacă ρ este o relație de echivalență pe inelul R care este compatibilă cu operațiile de pe R ($\forall a, a', b, b' \in R$ cu $a \rho a'$ și $b \rho b' \Rightarrow (a + b) \rho (a' + b')$ și $(a \cdot b) \rho (a' \cdot b')$), atunci clasa de echivalență a lui 0 în raport cu ρ (adică $I_\rho := \{a \in R \mid a \rho 0\}$) este ideal în R și ρ coincide cu relația de congruență modulo I_ρ . Pe de altă parte, o relație de echivalență pe R , cu proprietatea că mulțimea factor poate fi înzestrată cu două operații după regula de la c) din propoziția de mai sus, trebuie să fie o relație compatibilă cu structura de inel (pentru a asigura corectitudinea definițiilor!). Apare în acest fel legătura strînsă dintre noțiunea de *ideal* într-un inel și cea de inel factor.

Este de așteptat ca un rol esențial în ce privește proprietățile inelului factor R/I să îl aibă idealul I . În acest sens, sînt importante următoarele noțiuni:

4.6 Definiție. Fie R un inel comutativ. Un ideal P al lui R se numește *ideal prim* dacă $P \neq R$ și oricare ar fi $x, y \in R$, din $xy \in P$ rezultă $x \in P$ sau $y \in P$. Un ideal M al lui R se numește *ideal maximal* dacă $M \neq R$ și nu există ideale proprii ale lui R care includ strict pe M : pentru orice $J \leq R$, din $M \leq J$ rezultă $M = J$ sau $J = R$.

4.7 Exemple. a) Dacă p este un număr întreg prim ($\forall a, b \in \mathbb{Z}$, dacă p divide produsul ab , atunci $p|a$ sau $p|b$), atunci idealul generat de p în $\mathbb{Z}$, notat $p\mathbb{Z}$, este ideal prim în $\mathbb{Z}$. Reciproc, dacă $p\mathbb{Z}$ este ideal prim, atunci p este număr prim.

b) Un ideal I este maximal în inelul R dacă este element maximal al mulțimii ordonate (cu incluziunea) a idealelor proprii ale lui R . În inelul $\mathbb{Z}$, orice ideal este de forma $n\mathbb{Z}$, cu $n \in \mathbb{Z}$. De aici rezultă că idealul $n\mathbb{Z}$ este maximal dacă și numai dacă n este număr prim. Într-adevăr, fie $n\mathbb{Z}$ ideal maximal. Atunci, $\forall m \in \mathbb{Z}$, din $n\mathbb{Z} \subseteq m\mathbb{Z}$ rezultă $n\mathbb{Z} = m\mathbb{Z}$ sau $m\mathbb{Z} = \mathbb{Z}$; cu alte cuvinte, din $m|n$ rezultă $m = \pm n$ sau $m = \pm 1$. Aceasta înseamnă că n este ireductibil (nu are alți divizori decât cei triviali, $\pm n$ și ± 1), deci prim. Reciproca se obține în același mod.

c) Inelul R este integru dacă și numai dacă (0) este ideal prim.

d) Dacă K este corp, (0) este singurul său ideal propriu, deci (0) este și ideal maximal și ideal prim.

4.8 Teoremă. Fie R un inel comutativ și I un ideal propriu în R .

a) I este ideal prim dacă și numai dacă inelul factor R/I este integru (adică 0 este ideal prim în R/I).

b) I este ideal maximal dacă și numai dacă inelul factor R/I este corp (adică 0 este ideal maximal în R/I).

Demonstrație. a) Fie I un ideal prim. Fie $\alpha = a + I$, $\beta = b + I$ (cu $a, b \in R$) elemente din R/I . Dacă $\alpha\beta = 0$, atunci $(a + I)(b + I) = 0 + I$, adică $ab \in I$. Cum I este prim, obținem $a \in I$ sau $b \in I$, adică $a + I = \alpha = 0 + I$ sau $b + I = \beta = 0 + I$. Așadar, R/I este integru. Reciproc, presupunem că R/I este integru și fie $a, b \in R$ cu $ab \in I$. Aceasta înseamnă că $(a + I)(b + I) = 0 + I$, deci $a + I = 0 + I$ sau $b + I = 0 + I$. Astfel, $a \in I$ sau $b \in I$.

b) Presupunem că I este ideal maximal în R . Vrem să arătăm că orice element nenul al inelului R/I este inversabil. Fie deci $\alpha = a + I$, cu $\alpha \neq 0 + I$, deci $a \notin I$. Atunci idealul generat de I și a , adică $I + Ra$, include strict pe I ; din maximalitatea lui I obținem $I + Ra = R$. În particular, $1 \in R$ se scrie sub forma $i + ra$, cu $i \in I$ și $r \in R$. Avem deci $1 + I = (ra + i) + I = ra + I = (r + I)(a + I)$, ceea ce arată că $a + I$ este inversabil. Fie acum R/I corp și J un ideal care include strict pe I . Există așadar $x \in J$, $x \notin I$. Aceasta înseamnă că $x + I \neq 0 + I$, deci $x + I$ este inversabil în R/I . Putem scrie atunci $1 + I = (r + I)(x + I)$, cu $r \in R$, adică există $i \in I$ astfel încât $1 = rx + i$. De aici rezultă că $1 \in J$, adică $J = R$. $\square$

Propoziția de mai sus dă un procedeu simplu și valoros, des utilizat, de a *construi corpuri ca inele factor în raport cu ideale maximale*. Această metodă apare, între altele, la construcțiile corpurilor finite, a lui $\mathbb{R}$ și $\mathbb{C}$. De exemplu, $\mathbb{Z}_p = \mathbb{Z}/p\mathbb{Z}$, inelul claselor de resturi modulo p (unde p este un număr prim) este un corp finit.

4.9 Observație. a) Idealul I este maximal în R dacă și numai dacă $\forall x \in R$ cu $x \notin I$, rezultă că $\exists i \in I$ și $r \in R$ astfel încât $i + rx = 1$ (vezi demonstrația precedentă).

b) Dacă $\varphi: R \rightarrow S$ este un morfism surjectiv de inele, atunci există o corespondență bijectivă, care păstrează incluziunile, între idealele lui R care includ $\text{Ker } \varphi$ și idealele lui S . Corespondența asociază idealului J în R idealul $\varphi(J)$ (imaginea lui J prin φ), care este ideal în S . Aplicând această afirmație situației în care I este ideal maximal în R și surjecției canonice $\pi: R \rightarrow R/I$ (cu $\text{Ker } \pi = I$), rezultă că R/I nu are ideale proprii în afară de 0 și R/I (căci singurele ideale în R care să includă pe I sînt I și R). Dar un inel comutativ care nu are alte ideale în afară de 0 și inelul însuși este corp (demonstrați!).

4.10 Corolar. *Orice ideal maximal este prim.* □

Reciproca este falsă: idealul (X) al inelului $\mathbb{Z}[X]$ este prim și nu este maximal, după cum se vede considerînd inelul factor: $\mathbb{Z}[X]/(X) \cong \mathbb{Z}$, care e integru dar nu e corp. Propunem cititorului să demonstreze aceste fapte cu ajutorul definițiilor.

Tot în legătură cu idealele maximale, are loc următorul rezultat, care folosește în mod esențial Lema lui Zorn:

4.11 Teoremă. (Lema lui Krull³¹) *Fie R un inel unitar comutativ. Atunci orice ideal propriu al lui R este inclus într-un ideal maximal. În particular, R are ideale maximale.*

Demonstrație. Fie $I \leq_R R$, $I \neq R$. Notăm cu $\mathbf{P}$ mulțimea idealelor proprii ale lui R , care includ pe I . $\mathbf{P}$ este o mulțime ordonată cu incluziunea; elementele ei maximale (dacă există!) sînt exact idealele maximale ale lui R , care includ pe I . Vom folosi lema lui Zorn pentru a demonstra existența elementelor maximale în $\mathbf{P}$. Fie deci un lanț $(E_j)_{j \in J}$, cu $E_j \in \mathbf{P}$, $\forall i \in J$. Acest lanț de ideale are un majorant în $\mathbf{P}$, anume $\bigcup_{j \in J} E_j =: E$. Într-adevăr, E este ideal³²: dacă $x, y \in E$, atunci există $i, j \in J$ cu $x \in E_i$, $y \in E_j$; cum $(E_j)_{j \in J}$ este lanț, rezultă că $E_i \subseteq E_j$ sau $E_j \subseteq E_i$. Deci $x - y \in E_j$ (căci $E_j \leq_R R$) sau $x - y \in E_i$. În orice caz, $x - y \in E$. La fel se demonstrează că $\forall r \in R, \forall x \in E$, rezultă $rx \in E$. Deci E este ideal, care include evident pe I .

Trebuie să demonstrăm și că $E \neq R$. Dacă, prin absurd, $E = R$, atunci $1 \in E = \bigcup_{j \in J} E_j$, deci există $j \in J$ cu $1 \in E_j$. Însă atunci $E_j = R$, contradicție cu $E_j \in \mathbf{P}$ (E_j este ideal propriu!).

Din lema lui Zorn, există un element maximal al lui $\mathbf{P}$.

Luînd $I = 0$, rezultă existența unui ideal maximal în R . □

Aplicații la criterii de divizibilitate. Utilizarea congruențelor (a inelelor de resturi) modulo n) conduce la demonstrarea rapidă (și chiar fabricarea) de criterii de divizibilitate pentru numere scrise într-o anumită bază (de obicei baza 10). Iată un exemplu binecunoscut:

³¹ Wolfgang Adolf Ludwig Helmuth Krull (1899-1971), matematician german cu importante contribuții în algebră.

³² În general, reuniunea unei familii oarecare de ideale *nu* este ideal.

4.12 Propoziție. (Criteriul de divizibilitate cu 3) Un număr scris în baza 10 este divizibil cu 3 dacă și numai dacă suma cifrelor sale este divizibilă cu 3.

Demonstrație. Fie $a = \overline{c_{n-1} \dots c_1 c_0}$ un număr în baza 10, cu $c_i \in \{0, \dots, 9\}$. Vom demonstra, mai general, că $a \equiv \sum c_i \pmod{3}$. Dar (toate congruențele sînt modulo 3):

$$a = \sum c_i 10^i \equiv \sum c_i 1^i \equiv \sum c_i,$$

căci $10 \equiv 1 \pmod{3}$. □

Ideea care stă la baza tuturor criteriilor de divizibilitate cu d pentru numere scrise în baza b este aceeași cu cea de mai sus: fiind dat $a = \overline{c_{n-1} \dots c_1 c_0}$ în baza b , se calculează $a \equiv \sum_{i \geq 0} c_i b^i \pmod{d}$. Pentru aceasta, se calculează b^i modulo d , pentru $i = 0, 1, \dots$. Se poate demonstra că acest șir este periodic (cu posibila excepție a unui număr finit de termeni), adică există $k, t \in \mathbb{N}$, $t > 0$, astfel încît $b^i \equiv b^{i+t} \pmod{d}$, $\forall i \geq k$.

4.13 Exerciții. a) (Criteriul de divizibilitate cu 9) Un număr scris în baza 10 este divizibil cu 9 dacă și numai dacă suma cifrelor sale este divizibilă cu 9.

b) (Criteriul de divizibilitate cu 2, respectiv 5, respectiv 10) Un număr scris în baza 10 este divizibil cu 2 (respectiv 5, respectiv 10) dacă și numai dacă ultima sa cifră (c_0) este divizibilă cu 2 (respectiv 5, respectiv 10).

c) Generalizați a) și b) pentru o bază oarecare b .

d) (Criteriul de divizibilitate cu 7)³³ Restul împărțirii la 7 a unui număr $\overline{c_{n-1} \dots c_1 c_0}$ scris în baza 10 este același cu restul împărțirii la 7 a lui $c_0 + 3c_1 + 2c_2 - c_3 + 4c_4 + 5c_5 + c_6 + 3c_7 + \dots$

4.14 Teoremă. (Lema chineză a resturilor) Fie R inel comutativ, $n \geq 2$ și $I_1, \dots, I_n$ ideale ale lui R .

a) Dacă $I_i + I_j = R$ pentru $i \neq j$,³⁴ atunci produsul³⁵ $I_1 \cdot \dots \cdot I_n$ este egal cu intersecția $I_1 \cap \dots \cap I_n$ și există un izomorfism natural de inele (și de R -module):

$$\frac{R}{I_1 \cdot \dots \cdot I_n} = \frac{R}{I_1 \cap \dots \cap I_n} \cong \frac{R}{I_1} \times \dots \times \frac{R}{I_n}, \quad r + I_1 \cap \dots \cap I_n \mapsto (r + I_1, \dots, r + I_n), \quad \forall r \in R.$$

b) Reciproc, dacă morfismul $\varphi: R \rightarrow \frac{R}{I_1} \times \dots \times \frac{R}{I_n}$, $\varphi(r) = (r + I_1, \dots, r + I_n)$, $\forall r \in R$ este surjectiv (inducînd un izomorfism $\frac{R}{I_1 \cap \dots \cap I_n} \cong \frac{R}{I_1} \times \dots \times \frac{R}{I_n}$, ca mai sus), atunci idealele I_i și I_j sînt comaximale pentru $i \neq j$.

Demonstrație. a) Aplicăm o inducție după n pentru a demonstra că $I_1 \cdot \dots \cdot I_n = I_1 \cap \dots \cap I_n$ și că are loc izomorfismul cerut. Pentru $n = 2$, din $I_1 + I_2 = R$ deducem că există $x \in I_1$, $y \in I_2$

³³ Utilitatea practică acestui criteriu este discutabilă...

³⁴ Idealele I_i și I_j se numesc în acest caz *comaximale*. De exemplu, idealele $\mathbb{Z}a$ și $\mathbb{Z}b$ ale lui $\mathbb{Z}$ sînt comaximale dacă și numai dacă a și b sînt prime între ele.

³⁵ Reamintim că produsul IJ a două ideale I și J este idealul generat de mulțimea produselor ij , cu $i \in I$, $j \in J$. Se arată ușor că produsul de ideale este asociativ și că întotdeauna $IJ \subseteq I \cap J$.

astfel încât $x + y = 1$. Fie $z \in I_1 \cap I_2$. Atunci $z = z \cdot 1 = zx + zy$, cu $zx, zy \in I_1 \cdot I_2$, adică $I_1 \cap I_2 \subseteq I_1 I_2$. Astfel, $I_1 \cap I_2 = I_1 I_2$.

Fie $\varphi: R \rightarrow \frac{R}{I_1} \times \frac{R}{I_2}$, $\varphi(r) = (r + I_1, r + I_2)$, $\forall r \in R$. E ușor de văzut că φ este morfism de inele și de R -module (este produsul direct al surjecțiilor canonice $R \rightarrow R/I_j$). Avem $\text{Ker } \varphi = \{r \in R \mid (r + I_1, r + I_2) = (0 + I_1, 0 + I_2)\} = I_1 \cap I_2$; teorema de izomorfism asigură că $R/I_1 \cap I_2 \cong \text{Im } \varphi$. E suficient așadar să demonstrăm surjectivitatea lui φ . Fie $(r_1 + I_1, r_2 + I_2) \in \frac{R}{I_1} \times \frac{R}{I_2}$. Trebuie să găsim $r \in R$ cu $r - r_1 \in I_1$, $r - r_2 \in I_2$. Un astfel de element este

$r = r_1 y + r_2 x$. Într-adevăr,

$$r - r_1 = r_1 y + r_2 x - r_1 x - r_1 y = (r_2 - r_1)x \in I_1.$$

Analog se arată că $r - r_2 \in I_2$.

Presupunem că pentru orice $k < n$ și orice ideale $I_1, \dots, I_k$, comaximale două câte două, are loc $I_1 \dots I_k = I_1 \cap \dots \cap I_k$ și are loc izomorfismul cerut. Fie n ideale $I_1, \dots, I_n$ ca în enunț. Din $I_j + I_n = R$, $1 \leq j \leq n - 1$, rezultă că există $a_j \in I_j$, $b_j \in I_n$ astfel încât $a_j + b_j = 1$. Înmulțind aceste $n - 1$ egalități membru cu membru obținem

$$\prod_{j=1}^{n-1} (a_j + b_j) = a_1 \dots a_{n-1} + b = 1, \text{ unde } b \in I_n, a_1 \dots a_{n-1} \in I_1 \dots I_{n-1}.$$

Deci $I_1 \dots I_{n-1} + I_n = R$. Aplicînd cazul $n = 2$ idealelor comaximale $I_1 \dots I_{n-1}$ și I_n , rezultă că $I_1 \dots I_{n-1} \cdot I_n = (I_1 \dots I_{n-1}) \cap I_n = (I_1 \cap \dots \cap I_{n-1}) \cap I_n$ (am folosit și ipoteza de inducție $I_1 \dots I_{n-1} = I_1 \cap \dots \cap I_{n-1}$). Mai rezultă că:

$$\frac{R}{(I_1 \dots I_{n-1}) \cdot I_n} \cong \frac{R}{I_1 \dots I_{n-1}} \times \frac{R}{I_n} \text{ prin } r + I_1 \dots I_n \mapsto (r + I_1 \dots I_{n-1}, r + I_n), \forall r \in R.$$

Folosind ipoteza de inducție, avem izomorfismul:

$$\frac{R}{I_1 \dots I_{n-1}} \cong \frac{R}{I_1} \times \dots \times \frac{R}{I_{n-1}} \text{ prin } r + I_1 \dots I_{n-1} \mapsto (r + I_1, \dots, r + I_{n-1}), \forall r \in R.$$

Combinînd aceste izomorfisme, obținem rezultatul din enunț.

b) Vom demonstra că I_1 și I_2 sînt comaximale. Fie $(1 + I_1, 0 + I_2, \dots, 0 + I_n) \in \frac{R}{I_1} \times \dots \times \frac{R}{I_n}$.

Există $y \in R$ astfel încît $(y + I_1, y + I_2, \dots, y + I_n) = (1 + I_1, 0 + I_2, \dots, 0 + I_n)$, adică $y \in I_2$ și $y - 1 \in I_1$. Deci $1 = -x + y \in I_1 + I_2$, adică $I_1 + I_2 = R$. $\square$

4.15 Exemplu. În $\mathbb{Z}$, idealele $a\mathbb{Z}$ și $b\mathbb{Z}$ sînt comaximale $\Leftrightarrow (a, b) = 1$. Avem în acest caz, conform lemei chineze a resturilor, $\mathbb{Z}/ab\mathbb{Z} \cong \mathbb{Z}/a\mathbb{Z} \times \mathbb{Z}/b\mathbb{Z}$ (cu notațiile clasice pentru inelele de clase de resturi $\mathbb{Z}_{ab} \cong \mathbb{Z}_a \times \mathbb{Z}_b$, izomorfismul fiind dat de $x + ab\mathbb{Z} \mapsto (x + a\mathbb{Z}, x + b\mathbb{Z})$). În particular, pentru orice pereche de numere naturale (c, d) cu $0 \leq c < a$, $0 \leq d < b$, există un unic x , $0 \leq x < ab$, astfel încît $x \equiv c \pmod{a}$ și $x \equiv d \pmod{b}$.

II.5. Corpul numerelor reale

Necesitatea introducerii numerelor întregi și a celor raționale este aproape evidentă din experiența imediată. Nu acesta este cazul numerelor reale, care au apărut din rațiuni mai profunde. Descoperirea de către matematicienii Greciei antice că diagonală pătratului de lungime 1 nu poate fi exprimată ca un raport de numere întregi (în termeni moderni, $\sqrt{2} \notin \mathbb{Q}$) a condus la o adevărată criză a științei și filozofiei în acea vreme.

Imagina intuitivă cea mai simplă despre $\mathbb{R}$, care reflectă cel mai bine structura de ordine, este cea a punctelor de pe o *dreaptă* (alt concept abstract, dar mai accesibil gândirii), unde s-a fixat un punct O (*originea*, corespunzând lui 0) și un alt punct U , diferit de primul (corespunzător lui 1 și avînd rolul de a fixa unitatea de măsură pe acea dreaptă). Orice număr real corespunde în mod unic unui punct de pe dreaptă: numărul real corespunzător punctului P este *distanța* de la O la P (dacă P este de aceeași parte ca și U față de O), respectiv distanța de la O la P luată cu semnul minus dacă O este între U și P . Se conturează astfel ideea intuitivă că numerele reale „pot măsura orice distanță”. Este semnificativ acest punct de vedere dacă se observă rolul esențial pe care îl are $\mathbb{R}$ în definiția generală a *spațiilor metrice* (spații în care este definită o noțiune de *distanță*).

În multe cărți (între care și manualele de Analiză de liceu) structura numerelor reale este dată „axiomatic”: se numește *corp al numerelor reale* un *corp comutativ* $(\mathbb{R}, +, \cdot)$ înzestrat cu o relație de *ordine totală* $\leq$, satisfăcînd proprietățile:

R1. $\mathbb{R}$ este *corp ordonat*, adică $\forall a, b, c \in \mathbb{R}$ au loc:

$$a \leq b \Rightarrow a + c \leq b + c;$$

$$a \leq b \text{ și } c \geq 0 \Rightarrow ac \leq bc.$$

R2. Orice submulțime nevidă majorată a lui $\mathbb{R}$ are margine superioară.

Evident, această definiție ridică două probleme: *existența* unei structuri cu proprietățile de mai sus și *unicitatea* sa. Unicitatea este tranșată de următorul rezultat:

5.1 Teoremă. Pentru orice două corpuri comutativeordonate $(K, +, \cdot, \leq)$ și $(L, +, \cdot, \leq)$ care satisfac proprietatea R2 există un unic izomorfism de corpuri $\varphi: K \rightarrow L$, care este și izomorfism de ordine: $\forall x, y \in K, x \leq y \Rightarrow \varphi(x) \leq \varphi(y)$. $\square$

Problema existenței se rezolvă printr-o *construcție efectivă* a lui $\mathbb{R}$, presupunînd dat $\mathbb{Q}$. Cele mai cunoscute procedee sînt *construcția zecimală*, *construcția prin tăieturi în $\mathbb{Q}$* și *construcția cu ajutorul șirurilor Cauchy* (șiruri fundamentale). Construcția folosind șirurile Cauchy prezintă avantajele eleganței și rapidității și se folosește și la alte construcții importante: *completatul unui corp normat oarecare*, *completatul unui spațiu metric*, *completatul unui spațiu vectorial normat*.

Pentru edificarea cititorului, vom schița construcția zecimală și apoi prezentăm construcția cu șirurile Cauchy. Construcția prin tăieturi, aparținînd lui Dedekind, este descrisă la exerciții.

Construcția zecimală a lui $\mathbb{R}$ (datorată lui Weierstrass³⁶) identifică un număr real cu o „fracție zecimală infinită”. De exemplu,

1,4142135623730950488016887242097..., 3,1415926535897932384626433832795...
sînt numerele reale $\sqrt{2}$, respectiv π (de fapt, e vorba de „trunchieri” ale lor; nu am scris *toate* zecimalele, din motive evidente de spațiu...). Formal, se consideră mulțimea :

$$\mathfrak{R} = \{b_0, b_1 b_2 \dots b_n \dots \mid b_0 \in \mathbb{Z}, b_i \in \{0, 1, \dots, 9\}, \forall i \in \mathbb{N}^*\}$$

Interpretarea intuitivă este: „ $b_0, b_1 b_2 \dots b_n \dots$ este suma seriei $b_0 + \sum_{n \geq 1} b_n \cdot 10^{-n}$ ” (dar, evident, nu putem *defini* astfel un număr real. De ce?).

Alegerea lui 10 ca bază este mai degrabă legată de tradiție, în locul său putînd fi ales orice număr natural $b \geq 2$ (evident, avem atunci $b_i \in \{0, 1, \dots, b-1\}$, adică b_i sînt cifre în baza b).

Apar însă probleme : 0,9999... , scris și ca 0,(9) („cu perioada 9”) este de fapt 1 (formal 1,000...), după cum se vede făcînd suma seriei corespunzătoare; cum nu dorim ca un același număr real să aibă două reprezentări zecimale distincte, trebuie făcută următoarea „identificare”: orice șir de forma $b = b_0, b_1 b_2 \dots b_n \dots$, cu proprietatea că $\exists k \geq 0$ astfel încît $b_i = 9, \forall i > k$ și $b_k < 9$, este identificat cu șirul $b_0, b_1 b_2 \dots (b_k + 1) 000 \dots$ (dacă $k \geq 1$), respectiv cu $(b_0 + 1) 000 \dots$ (dacă $k = 0$). Pentru rigurozitate, se definește o relație de echivalență $\sim$ pe $\mathfrak{R}$, ca mai sus, iar mulțimea factor $\mathfrak{R}/\sim$ va fi prin definiție $\mathbb{R}$. Alte dificultăți apar la definirea adunării și înmulțirii a două fracții zecimale infinite (de fapt a unor clase de echivalență din $\mathfrak{R}/\sim$), fiind necesară apelarea la operațiile pe „trunchierile raționale” ale șirurilor respective și la definirea unei noțiuni de limită în $\mathfrak{R}/\sim$. Invităm cititorul să încerce să dea singur aceste definiții și să demonstreze pe baza lor proprietățile uzuale ale operațiilor cu numere reale, pentru a măsura dificultățile construcției. Avantajele acestei abordări (în măsura detalierii efective de către cititor!) constau în apropierea de imaginea intuitivă a conceptului de număr real și la definirea *relației de ordine*, care coincide cu cea *lexicografică*³⁷: se definește $b_0, b_1 b_2 \dots b_n \dots < c_0, c_1 c_2 \dots c_n \dots \Leftrightarrow \exists k \in \mathbb{N}$ astfel încît $b_k < c_k$ și, $\forall i < k$, are loc $b_i = c_i$.

Construcția lui $\mathbb{R}$ cu ajutorul șirurilor Cauchy (G. Cantor)

$\mathbb{Q}$ este un *corp normat*. Mai precis, aplicația *valoare absolută* (sau *modul*) $|\cdot| : \mathbb{Q} \rightarrow \mathbb{Q}$,

$$|x| = \begin{cases} x & \text{dacă } x \geq 0 \\ -x & \text{dacă } x < 0 \end{cases}$$

are proprietățile (binecunoscute) următoare:

- N1. $\forall x \in \mathbb{Q}$ are loc $|x| \geq 0$.
- N2. $\forall x \in \mathbb{Q}$ are loc $|x| = 0 \Leftrightarrow x = 0$.
- N3. $\forall x, y \in \mathbb{Q}$ are loc $|x + y| \leq |x| + |y|$ (inegalitatea triunghiulară).
- N4. $\forall x, y \in \mathbb{Q}$ are loc $|x \cdot y| = |x| \cdot |y|$.

³⁶ Karl Theodor Wilhelm Weierstrass (1815-1897), matematician german, considerat "părintele analizei moderne".

³⁷ Lexicon = dicționar. Puteți spune de ce se numește așa ordinea definită?

Altfel spus, valoarea absolută este o *normă*³⁸. Cu ajutorul normei definim o *distanță* (o *metrică*)³⁹, adică o aplicație $d : \mathbb{Q} \times \mathbb{Q} \rightarrow \mathbb{Q}$, $d(x, y) := |x - y|$, $\forall (x, y) \in \mathbb{Q}$, cu proprietățile:

D1. $\forall x, y \in \mathbb{Q}$ are loc $d(x, y) = d(y, x) \geq 0$.

D2. $\forall x, y \in \mathbb{Q}$ are loc $d(x, y) = 0 \Leftrightarrow x = y$.

D3. $\forall x, y, z \in \mathbb{Q}$ are loc $d(x, y) \leq d(x, z) + d(z, y)$ (inegalitatea triunghiulară).

Ca o consecință, se obține $|x - y| \geq ||x| - |y||$, $\forall x, y \in \mathbb{Q}$.

Metrica determină o *topologie*⁴⁰ pe $\mathbb{Q}$. Proprietățile metrice și topologice ale lui $\mathbb{Q}$ nu sînt prea bune, tocmai din cauzele amintite la început: nu orice șir de numere raționale „care ar trebui să fie convergent la ceva” este convergent la un număr rațional (de exemplu, șirul aproximărilor zecimale ale lui $\sqrt{2}$).

Construcția lui $\mathbb{R}$ cu șiruri Cauchy pornește de la ideea că un număr real este o „limită a unui șir de numere raționale”. În loc să ne îndreptăm atenția asupra unui tip particular de șiruri de numere raționale, ca la construcția zecimală (șirurile cu termen general de forma $b_0 + \sum_{i=1}^n b_i \cdot 10^{-i}$), se consideră *toate* șirurile de numere raționale $(x_n)_{n \geq 1}$ „care au o limită, nu neapărat în $\mathbb{Q}$ ”.

Bineînțeles, nu orice șir de numere raționale „are o limită” în sens intuitiv (de exemplu șirul $((-1)^n)_{n \geq 1}$). Pe de altă parte, nu putem defini „existența limitei” șirului (x_n) direct ($\exists l$ astfel încît $x_n \rightarrow l$), căci l este în general un număr real, concept pe care tocmai îl construim! Din fericire, știm de la Analiză că *șirurile care au limită în $\mathbb{R}$ sînt exact șirurile Cauchy* (noțiune în care *nu apare explicit* limita șirului).

5.1 Definiție. Șirul de numere raționale $(x_n)_{n \geq 1}$ se numește *șir Cauchy* (sau *șir fundamental*) dacă satisface condiția:

$$\forall \varepsilon \in \mathbb{Q}, \varepsilon > 0 \Rightarrow \exists N \in \mathbb{N} \text{ astfel încît } \forall m, n \geq N \text{ să aibă loc } |x_m - x_n| < \varepsilon.$$

Fie $\mathcal{C} := \{(x_n)_{n \geq 1} \mid x_n \in \mathbb{Q}, \forall n \geq 1, (x_n)_{n \geq 1} \text{ șir Cauchy}\}$.

Putem aplica acum ideea intuitivă expusă la început și să definim două șiruri $(x_n), (y_n) \in \mathcal{C}$ ca fiind *echivalente*⁴¹ dacă „au aceeași limită”. Și această idee se poate exprima fără a invoca explicit valoarea limitei:

$$(x_n)_n \sim (y_n)_n \Leftrightarrow \forall \varepsilon \in \mathbb{Q}, \varepsilon > 0 \Rightarrow \exists N \in \mathbb{N} \text{ astfel încît } \forall n \geq N \text{ să aibă loc } |x_n - y_n| < \varepsilon. \quad (R)$$

În sfîrșit, definim un *număr real* ca o *clasă de echivalență de șiruri din $\mathcal{C}$* ; mai precis, mulțimea factor $\mathcal{C}/\sim$ o notăm cu $\mathbb{R}$ și o numim *mulțimea numerelor reale*. Se observă că orice

³⁸ În general, o *normă* ia valori în $\mathbb{R}$, pe care nu l-am construit încă... , deci titulatura este puțin forțată.

³⁹ Aceeași observație ca mai sus: o *distanță* ia în general valori reale.

⁴⁰ Nu mai definim topologia, vezi orice manual de Analiză elementară.

⁴¹ Adică "definesc" același număr real.

număr rațional a poate fi identificat cu clasa în $\mathcal{C}/\sim$ a șirului constant $(a, a, \dots) \in \mathcal{C}$ (adică am obținut într-adevăr o extindere a lui $\mathbb{Q}$).

Rămân sarcinile: de a defini operațiile, de a demonstra corectitudinea definițiilor și de a verifica axiomele de corp comutativ pentru $\mathbb{R}$. Apoi trebuie definită relația de ordine și arătat că: $\mathbb{R}$ este total ordonat, relația de ordine este compatibilă cu structura de corp și orice submulțime nevidă majorată are margine superioară.

Aceste sarcini se pot ușura considerabil dacă folosim instrumente algebrice elementare: ideale și inele factor. Observăm că $\mathcal{C}$ este inel comutativ unitar și că $(x_n)_n \sim (y_n)_n \Leftrightarrow (x_n - y_n) \rightarrow 0$ (unde scriem $(z_n) \rightarrow 0$ dacă $\forall \varepsilon \in \mathbb{Q}, \varepsilon > 0 \Rightarrow \exists N \in \mathbb{N}$ astfel încât $\forall n \geq N$ să aibă loc $|z_n| < \varepsilon$). Dacă notăm

$$\mathcal{Z} := \{(z_n)_{n \geq 1} \in \mathcal{C} \mid (z_n) \rightarrow 0\},$$

se demonstrează că $\mathcal{Z}$ este ideal maximal în $\mathcal{C}$ (și relația " $\sim$ " coincide cu relația de congruență modulo $\mathcal{Z}$). Rezultă imediat atunci că $\mathbb{R} = \mathcal{C}/\mathcal{Z}$ este corp comutativ și cu aceasta se încheie partea „algebrică” a construcției lui $\mathbb{R}$. Notăm cu $[(x_n)]$ imaginea în $\mathcal{C}/\mathcal{Z}$ a șirului $(x_n) \in \mathcal{C}$. Sumarizăm construcția în următoarea:

5.2 Teoremă. a) Mulțimea $\mathcal{C}$ a șirurilor Cauchy de numere raționale este un inel comutativ unitar⁴² în raport cu operațiile de adunare și înmulțire definite „punctual”:

$$(x_n)_n + (y_n)_n := (x_n + y_n)_n,$$

$$(x_n)_n \cdot (y_n)_n := (x_n \cdot y_n)_n,$$

$\forall (x_n), (y_n) \in \mathcal{C}$.

b) Mulțimea $\mathcal{Z} = \{(z_n)_{n \geq 1} \in \mathcal{C} \mid (z_n) \rightarrow 0\}$ a șirurilor din $\mathcal{C}$ care au limita 0 este un ideal maximal în $\mathcal{C}$, deci inelul factor $\mathcal{C}/\mathcal{Z} =: \mathbb{R}$ este corp comutativ.

c) Pentru orice $a \in \mathbb{Q}$, considerăm „șirul constant” $(a_n)_n \in \mathcal{C}$, $a_n = a$, $\forall n \in \mathbb{N}^*$. Aplicația care asociază lui $a \in \mathbb{Q}$ clasa în $\mathcal{C}/\mathcal{Z} = \mathbb{R}$ a șirului constant $(a_n)_n$ este un morfism de corpuri. Clasa $[(a_n)] \in \mathbb{R}$ a șirului constant (a_n) va fi numită prin abuz „numărul rațional a ”.

d) Definim pe $\mathcal{C}/\mathcal{Z}$ relația binară " $<$ " :

$$[(x_n)] < [(y_n)] \Leftrightarrow \exists \varepsilon \in \mathbb{Q}, \varepsilon > 0 \text{ și } \exists N \in \mathbb{N} \text{ astfel încât } x_n + \varepsilon \leq y_n, \forall n \geq N.$$

Atunci " $<$ " este bine definită (nu depinde de reprezentanți) și este o relație de ordine strictă pe $\mathcal{C}/\mathcal{Z}$ (ireflexivă și tranzitivă). Relația de ordine nestrictă asociată, notată " $\leq$ ", este o relație de ordine totală pe $\mathbb{R}$; mai mult, $\mathbb{R}$ devine corp ordonat în raport cu această ordine.

e) (Valoarea absolută pe $\mathbb{R}$) Fie $|\cdot| : \mathbb{R} \rightarrow \mathbb{R}, [(x_n)] \mapsto [|x_n|]$, $\forall (x_n) \in \mathcal{C}$. Definiția este corectă și au loc proprietățile normei N1-N4 de mai sus (bineînțelese, $\mathbb{Q}$ este înlocuit cu $\mathbb{R}$).

f) Orice șir Cauchy $(r_n)_{n \geq 1}$ de numere reale este convergent la un număr real.⁴³

g) Orice submulțime nevidă majorată a lui $\mathbb{R}$ are margine superioară.

⁴² Este și integru?

⁴³ Lăsăm cititorului sarcina de a defini noțiunile de șir Cauchy și de limită în $\mathbb{R}$.

h) $\mathbb{Q}$ este dens în $\mathbb{R}$ (orice număr real este limita unui șir de numere raționale).

Demonstrație. *a) Demonstrarea faptului că suma și produsul a două șiruri Cauchy este tot șir Cauchy este un exercițiu elementar de Analiză (cf. demonstrația la „suma, resp. produsul, a două șiruri convergente este un șir convergent”). Este utilă demonstrarea în prealabil a faptului că orice șir Cauchy (x_n) este mărginit ($\exists M \in \mathbb{Q}$ astfel încît $|x_n| \leq M$, $\forall n \in \mathbb{N}^*$). Care este elementul nul, respectiv unitate, în $\mathbb{C}$?*

b) $\mathbb{Z}$ este ideal: argument standard de Analiză, ca la punctul precedent (se adaptează demonstrația proprietăților $\lim(x_n + y_n) = \lim x_n + \lim y_n$, $\lim(x_n \cdot y_n) = \lim x_n \cdot \lim y_n$).

$\mathbb{Z}$ este maximal: dacă $(x_n) \in \mathbb{C} \setminus \mathbb{Z}$, atunci există $N \in \mathbb{N}$ și $\delta > 0$ astfel încît $|x_n| > \delta$, $\forall n \geq N$. Într-adevăr, cum (x_n) nu tinde la 0, $\exists \varepsilon > 0$ astfel încît $\forall n \in \mathbb{N}$, $\exists k_n > n$ astfel încît $|x_{k_n}| > \varepsilon$. Însă (x_n) este Cauchy, deci, pentru $\varepsilon/2$, există $N \in \mathbb{N}$ astfel încît $\forall m, n \geq N$, $|x_n - x_m| < \varepsilon/2$. Fie $m = k_N$ dat de proprietatea precedentă. Atunci, $\forall n \geq N$,

$$|x_n| = |x_m + x_n - x_m| \geq |x_m| - |x_n - x_m| > \varepsilon - \varepsilon/2 = \varepsilon/2.$$

Raționamentul, ca și multe altele de același gen, se vede mai bine (și poate fi intuit!) reprezentînd numerele pe axă.

Revenind la (x_n) , rezultă că $\exists N \in \mathbb{N}$ astfel încît $x_n \neq 0$ dacă $n \geq N$. Definim atunci șirul (y_n) prin: $y_n = 0$ dacă $n < N$ și $y_n = 1/x_n$ dacă $n \geq N$. Șirul (y_n) este Cauchy (demonstrați!) și $x_n y_n = 1 + z_n$, unde z_n este 0 pentru $n \geq N$, deci $(z_n) \in \mathbb{Z}$.

e) Trebuie arătat mai întîi că $(|x_n|)$ este șir Cauchy și că definiția nu depinde de reprezentanți. Demonstratia proprietăților normei se face apelînd la proprietățile corespunzătoare pentru norma în $\mathbb{Q}$.

f) Argumentul este tipic de Analiză, dar îl includem, fiind mai delicat. Fie $(r_n)_{n \geq 1}$ un șir Cauchy de numere reale. Fie $r_n = [(r_{nk})_{k \geq 1}]$, unde $(r_{nk})_{k \geq 1}$ este un șir Cauchy de numere raționale (pentru orice n fixat). Notăm $r_{nk} =: r(n, k)$, $\forall n, k \geq 1$. Vom arăta că $(r_n)_{n \geq 1}$ are limită în $\mathbb{R}$, anume $[(r(i_n, j_n))_{n \geq 1}]$, unde i_n, j_n sînt niște șiruri strict crescătoare de numere naturale pe care le definim inductiv, astfel:

Cum $(r_n)_{n \geq 1}$ este șir Cauchy în $\mathbb{R}$, pentru $\varepsilon = 1/4$, $\exists i_1 \in \mathbb{N}$ astfel încît $\forall s, t \geq i_1$ avem $|r_s - r_t| < 1/4$.

Cum $(r_{i_1 k})_{k \geq 1}$ e șir Cauchy în $\mathbb{Q}$, $\exists j_1 \in \mathbb{N}$ astfel încît $|r(i_1, u) - r(i_1, v)| < 1/4$, $\forall u, v \geq j_1$.

Fie $n \in \mathbb{N}$, $n \geq 2$ și presupunem că am definit $i_1 < i_2 < \dots < i_{n-1}$ și $j_1 < j_2 < \dots < j_{n-1}$, numere naturale astfel încît, $\forall k \in \{1, \dots, n-1\}$:

$$|r_s - r_t| < 1/2^{k+1}, \forall s, t \geq i_k \text{ (inegalitate în } \mathbb{R}) \quad (1)$$

$$|r(i_k, u) - r(i_k, v)| < 1/2^{k+1}, \forall u, v \geq j_k \quad (2)$$

$$|r(i_k, u) - r(i_{k-1}, u)| < 1/2^k, \forall u \geq j_k \quad (3)$$

Condiția (3) este vidă pentru $k = 1$.

Să găsim i_n și j_n încît (1), (2) și (3) să fie satisfăcute pentru $k = n$.

Șirul $(r_n)_{n \geq 1}$ este Cauchy în $\mathbb{R}$; luînd $\varepsilon = 1/2^{n+1}$, există $i_n \in \mathbb{N}$ astfel încît $i_n > i_{n-1}$ și

$$|r_s - r_t| < 1/2^{n+1}, \forall s, t \geq i_n \text{ (inegalitate în } \mathbb{R}).$$

Cum $(r(i_n, k))_{k \geq 1}$ e șir Cauchy în $\mathbb{Q}$, $\exists p_n \in \mathbb{N}$ astfel încît

$$|r(i_n, u) - r(i_n, v)| < 1/2^{n+1}, \forall u, v \geq p_n$$

Pe de altă parte, din (1) aplicat pentru $k = n - 1$ și $s = i_n$, $t = i_{n-1}$, avem $|r_{i_n} - r_{i_{n-1}}| < 1/2^n$ (inegalitate în $\mathbb{R}$), deci (din definiția relației de ordine în $\mathbb{R}$) $\exists q_n$ astfel încît

$$|r(i_n, u) - r(i_{n-1}, u)| < 1/2^n, \forall u \geq q_n.$$

Luînd $j_n = \max(j_{n-1} + 1, p_n, q_n)$, rezultă că (2) și (3) sînt satisfăcute, cu $k = n$ și că $j_n > j_{n-1}$. Am construit inductiv șirurile strict crescătoare i_n, j_n , satisfăcînd (1), (2), (3), pentru orice $k \geq 1$.

Notăm $x_n := r(i_n, j_n)$, $\forall n \geq 1$. Să arătăm că $(x_n)_{n \geq 1}$ e șir Cauchy în $\mathbb{Q}$. Pentru orice $n, m \in \mathbb{N}$ cu $n < m$, avem:

$$|x_m - x_n| = |r(i_m, j_m) - r(i_n, j_n)| \leq |r(i_m, j_m) - r(i_n, j_m)| + |r(i_n, j_m) - r(i_n, j_n)| \quad (4)$$

Dar, folosind (3), avem

$$|r(i_m, j_m) - r(i_n, j_m)| = \sum_{k=n+1}^m |r(i_k, j_m) - r(i_{k-1}, j_m)| < \sum_{k=n+1}^m \frac{1}{2^k} < \frac{1}{2^n}. \quad (4')$$

Pe de altă parte, $|r(i_n, j_m) - r(i_n, j_n)| < 1/2^n$ pentru că $j_m > j_n$ și se aplică (2).

Înlocuind în (4), avem:

$$|x_m - x_n| < |r(i_m, j_m) - r(i_n, j_n)| < 1/2^n + 1/2^n = 1/2^{n-1},$$

ceea ce arată că (x_n) este șir Cauchy.

Să arătăm că r_n are limita $x := [(r(i_n, j_n))_{n \geq 1}]$. Fie $\varepsilon > 0$ și $k \in \mathbb{N}$ astfel încît $1/2^k < \varepsilon/3$. Din (1) avem:

$$|r_s - r_t| < 1/2^{k+1}, \forall s, t \geq i_k \quad (5)$$

Dacă $n \geq i_k$, arătăm că $|r_n - x| < \varepsilon$ (ceea ce va termina demonstrația). Aceasta revine la a proba existența unui N (depinzînd posibil de n) astfel încît $\forall t \geq N$ să avem

$$|r_{nt} - x_t| = |r(n, t) - r(i_t, j_t)| < \varepsilon.$$

Fixăm $q \in \mathbb{N}$ cu $i_q \geq n$. Din (5), $|r_n - r_{i_q}| < 1/2^{k+1}$, deci există un N_0 astfel încît, $\forall t \geq N_0$:

$$|r(n, t) - r(i_q, t)| < \varepsilon/3 \quad (6)$$

Cum r_n e Cauchy, există N_1 astfel încît, $\forall s, t \geq N_1$,

$$|r(n, t) - r(n, s)| < \varepsilon/3 \quad (7)$$

Fie $N := \max(N_0, N_1, i_q)$. Dacă $t \geq N$, avem:

$$|r(n, t) - r(i_t, j_t)| \leq |r(n, t) - r(n, j_t)| + |r(n, j_t) - r(i_q, j_t)| + |r(i_q, j_t) - r(i_t, j_t)| \quad (8)$$

Primul termen din dreapta inegalității (8) e mai mic decît $\varepsilon/3$ din (7). Al doilea termen e mai mic decît $\varepsilon/3$ din (6) (clar, $j_t > t \geq N$). Al treilea termen e mai mic decît $1/2^q$ din (4').

g) Cititorii care au parcurs teoria elementară a convergenței în $\mathbb{R}$ se vor fi întrebat de ce am dat o demonstrație separată pentru f), deși rezultă din g) (vezi Exerciții). Pentru răspuns, vezi construcția de mai jos a *completatului unui corp normat*.

h) Exercițiu. □

Metoda completării prin șiruri Cauchy este folosită și la *completatul unui spațiu metric* oarecare, construcție fundamentală în Analiză și topologie:

5.3 Definiție. Fie X o mulțime nevidă. O funcție $d : X \times X \rightarrow \mathbb{R}$ se numește *distanță* (metrică) pe X dacă satisface axiomele: i) $\forall x, y \in X$ are loc $d(x, y) = d(y, x) \geq 0$; ii) $\forall x, y \in X$ are loc: $d(x, y) = 0 \Leftrightarrow x = y$; iii) $\forall x, y, z \in X$ are loc $d(x, y) \leq d(x, z) + d(z, y)$ (inegalitatea triunghiulară). Un cuplu (X, d) , unde d este o distanță pe X , se numește *spațiu metric*; elementele lui X se mai numesc și *puncte* ale lui X .

Pentru orice $x \in X$, *sfera (bila) deschisă de rază r cu centrul în x* este mulțimea

$$S(x, r) := \{y \in X \mid d(x, y) < r\}.$$

Distanța d definește o *topologie* pe X , în care un sistem fundamental de vecinătăți al unui punct $x \in X$ este $\{S(x, r) \mid r \in \mathbb{R}, r > 0\}$ (mulțimea sferelor deschise centrate în x). Altfel spus, o submulțime D a lui X este declarată *deschisă* dacă $\forall x \in D, \exists r > 0$ astfel încât $S(x, r) \subseteq D$. Un șir $(x_n)_{n \geq 1}$ este *convergent* la $x \in X$ dacă și numai dacă $\forall \varepsilon > 0, \exists N \in \mathbb{N}$ astfel încât $\forall n > N$ are loc $d(x_n, x) < \varepsilon$. Spațiul metric (X, d) se numește *complet* dacă orice șir Cauchy de elemente din X este convergent la un element din X .

Am văzut că $\mathbb{Q}$ este spațiu metric, cu distanța $d(x, y) = |x - y|$, dar nu este complet. Din punct de vedere topologic, construcția lui $\mathbb{R}$ prezentată mai sus este un caz particular al *completării unui spațiu metric*, care, plecând de la un spațiu metric (X, d) , construiește un spațiu metric *complet* $(\hat{X}, \hat{d})$ și o aplicație injectivă $\varphi : X \rightarrow \hat{X}$, astfel încât $\varphi(X)$ este densă în $\hat{X}$ și φ păstrează distanțele. Construcția este asemănătoare cu cea de mai sus, cu deosebirea că nu putem face apel la ideale, nefiind definită nici o structură algebrică pe X . Se folosește direct o relație de echivalență " $\sim$ " definită pe mulțimea $\mathcal{C}$ a șirurilor Cauchy de elemente din X ; mulțimea $\mathcal{C}/\sim$ se înzestrează cu o metrică (cum?) și este spațiul metric complet căutat.

Mai importantă pentru Algebră și Teoria numerelor este ***completarea unui corp normat***.

5.4 Definiție. Fie K un corp comutativ. O funcție $N : K \rightarrow \mathbb{R}$ se numește *normă* dacă satisface condițiile:

$$N1. \forall x \in K \text{ are loc } N(x) \geq 0.$$

$$N2. \forall x \in K \text{ are loc } N(x) = 0 \Leftrightarrow x = 0.$$

$$N3. \forall x, y \in K \text{ are loc } N(x + y) \leq N(x) + N(y) \text{ (inegalitatea triunghiulară)}.$$

$$N4. \forall x, y \in K \text{ are loc } N(x \cdot y) = N(x) \cdot N(y).$$

Un cuplu (K, N) , unde K este corp și N o normă pe K se numește *corp normat*. Exemple uzuale sînt $(\mathbb{Q}, |\cdot|)$, $(\mathbb{R}, |\cdot|)$.

Norma pe K definește o metrică $d : K \times K \rightarrow \mathbb{R}$ prin relația $d(x, y) := N(x - y)$ (verificați!). Dacă spațiul metric (K, d) nu este complet, se poate construi ca mai sus *completatul său* $\hat{K}$, care e spațiu metric; în plus, se pot defini operații pe $\hat{K}$ față de care acesta devine corp normat. O abordare mai rapidă reia ideea de a folosi idealul $\mathcal{Z}$ al șirurilor cu limita 0 în inelul $\mathcal{C}$ al șirurilor Cauchy de elemente din K și construiește $\hat{K} := \mathcal{C}/\mathcal{Z}$.

5.5 Exemplu. (Corpul numerelor p -adice) Fie $p \in \mathbb{Z}$ un număr prim. Dacă $n \in \mathbb{Z}$ și $\alpha \in \mathbb{N}$, scriem $p^\alpha || n$ dacă $p^\alpha | n$ și $p^{\alpha+1} \nmid n$. Pentru orice $n \in \mathbb{Z}$, $\exists! \alpha \in \mathbb{N}$ astfel încât $p^\alpha || n$. Definim $v_p(n)$, *valuarea p -adică* a lui n , ca fiind unicul numărul natural α astfel încât $p^\alpha || n$. Dacă $r = m/n \in \mathbb{Q}$, cu $m, n \in \mathbb{Z}$, definim⁴⁴ $v_p(m/n) := v_p(m) - v_p(n)$. Norma p -adică a lui r este

$$|r|_p := p^{-v_p(r)}.$$

Se demonstrează că norma p -adică este o normă pe $\mathbb{Q}$ și îndeplinește o proprietate mai tare decât axioma N3 (inegalitatea triunghiulară), anume:

NA: $\forall x, y \in \mathbb{Q}$ are loc $|x + y|_p \leq \max(|x|_p, |y|_p)$.

Un corp normat $(K, |\cdot|)$ care satisface proprietatea NA se numește *non-arhimedean* (sau *ultrametric*), deoarece nu satisface *proprietatea lui Arhimede*⁴⁵: $\forall x, y \in K$ cu $x \neq 0$, $\exists n \in \mathbb{N}^*$ astfel încât $|nx| \geq |y|$.

Completatul lui $\mathbb{Q}$ în raport cu norma p -adică se notează cu $\mathbb{Q}_p$ și se numește *corpul numerelor p -adice*. Aceste corpuri joacă un rol important în teoria numerelor.

Aceeași idee, a șirurilor Cauchy, apare și la construcția *completatului unui spațiu liniar normat*. Nu mai intrăm în detalii (vezi de ex. MARINESCU [1983]).

Exerciții

1. a) Fie $a, b \in \mathbb{N}$, $(a, b) = 1$. Folosind algoritmul extins al lui Euclid (vezi Index), arătați că există $\alpha \in a\mathbb{Z}$, $\beta \in b\mathbb{Z}$ astfel încât $1 = \alpha + \beta$. Descrieți un procedeu efectiv de determinare a lui α și β .

b) Scrieți efectiv izomorfismul canonic $\varphi: \mathbb{Z}_a \times \mathbb{Z}_b \rightarrow \mathbb{Z}_{ab}$ dat de lema chineză a resturilor (Ind. Aplicați metoda din demonstrația lemei.)

c) Determinați $n \in \mathbb{N}$ astfel încât $n \equiv 7 \pmod{13}$ și $n \equiv 10 \pmod{18}$.

2. a) Fie p număr natural prim. Arătați că, în inelul de polinoame $\mathbb{Z}_p[X, Y]$, $(X + Y)^p = X^p + Y^p$ (Ind. Are loc binomul lui Newton, cu coeficienții binomiali calculați mod p .)

3. (Mica teoremă a lui Fermat) Fie p număr natural prim și $a \in \mathbb{N}$. Arătați că $a^p \equiv a \pmod{p}$. (Ind. Se poate folosi exercițiul precedent și o inducție după a . Sau, folosiți teorema lui Lagrange în grupul $(\mathbb{Z}_p^*, \cdot)$)

4. a) Demonstrați că $\mathbb{Z}_{11} \times \mathbb{Z}_{31} \cong \mathbb{Z}_{341}$ și scrieți efectiv acest izomorfism.

⁴⁴ Verificați corectitudinea definiției!

⁴⁵ $\mathbb{Q}$ și $\mathbb{R}$ sînt corpuri arhimedene, căci satisfac această proprietate.

b) Calculați $2^{341} \pmod{11}$ și $2^{341} \pmod{31}$.

c) Demonstrați că $2^{341} \equiv 2 \pmod{341}$.

d) Este adevărat că, dacă $2^n \equiv 2 \pmod{n}$, atunci n este prim?

5. Demonstrați că în $\mathbb{R}$ (construit cu șiruri Cauchy) orice submulțime nevidă majorată are margine superioară.

6. Fie K un corp comutativ total ordonat în care orice submulțime nevidă majorată are margine superioară. Demonstrați că orice șir Cauchy în K este convergent.

7. (Construcția lui Dedekind a lui $\mathbb{R}$ prin tăieturi în $\mathbb{Q}$) Se numește *tăietură* în $\mathbb{Q}$ o pereche (A, B) de submulțimi ale lui $\mathbb{Q}$ cu proprietățile: i) $A \neq \emptyset$, $B \neq \emptyset$; ii) $A \cup B = \mathbb{Q}$; iii) $\forall a \in A$, $\forall b \in B$ are loc $a < b$; iv) A nu are cel mai mare element.

Fie $T(\mathbb{Q}) := \{(A, B) \mid (A, B) \text{ tăietură în } \mathbb{Q}\}$. Demonstrați că:

a) Dacă (A, B) este tăietură în $\mathbb{Q}$, atunci $A \cap B = \emptyset$ și $B = \mathbb{Q} \setminus A$.

b) Definind relația " $\leq$ " pe $T(\mathbb{Q})$ prin $(A, B) \leq (C, D) \Leftrightarrow A \subseteq C \Leftrightarrow D \subseteq B$, se obține o relație de ordine totală pe $T(\mathbb{Q})$.

c) Aplicația $\varphi: \mathbb{Q} \rightarrow T(\mathbb{Q})$, $\varphi(x) = (L_x, R_x)$, cu $L_x = \{y \in \mathbb{Q} \mid y < x\}$ și $R_x = \{y \in \mathbb{Q} \mid y \geq x\}$, este injectivă și crescătoare (deci x poate fi identificat cu $\varphi(x) \in T(\mathbb{Q})$, iar $\mathbb{Q}$ cu $\varphi(\mathbb{Q})$).

d) Orice submulțime $(A_i, B_i)_{i \in I}$ a lui $T(\mathbb{Q})$ care este majorată în $T(\mathbb{Q})$ are margine superioară, anume $(\bigcup_{i \in I} A_i, \bigcap_{i \in I} B_i) \in T(\mathbb{Q})$.

e) Definind: $(A, B) + (C, D) := (A + C, B + D)$, $\forall (A, B), (C, D) \in T(\mathbb{Q})$, (unde $A + C = \{a + c \mid a \in A, c \in C\}$), se obține o lege de compoziție pe $T(\mathbb{Q})$; $(T(\mathbb{Q}), +)$ este grup abelian, iar $\varphi: \mathbb{Q} \rightarrow T(\mathbb{Q})$ definit mai sus este morfism de grupuri.

f) Fie $\alpha = (A, B)$, $\beta = (C, D) \in T(\mathbb{Q})$. Definim " $\cdot$ ": $T(\mathbb{Q}) \times T(\mathbb{Q}) \rightarrow T(\mathbb{Q})$ prin:

$$\alpha \cdot \beta = \begin{cases} (AC, BD) & \text{dacă } \alpha, \beta \geq 0 \\ |\alpha| \cdot |\beta| & \text{dacă } \alpha, \beta < 0 \\ -|\alpha| \cdot |\beta| & \text{în celelalte cazuri} \end{cases}$$

(unde $A \cdot C = \{a \cdot c \mid a \in A, c \in C\}$ și $||$ este funcția modul pe K). Atunci $(T(\mathbb{Q}), +, \cdot, \leq)$ este corp ordonat și $\varphi: \mathbb{Q} \rightarrow T(\mathbb{Q})$ este morfism de corpuri.

8. Verificați afirmațiile nedemonstrate de la exemplul II.5.5.

III. Polinoame, corpul complex și extinderi de corpuri

Conceptul de *polinom* (cu coeficienți într-un inel dat, adesea $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) joacă un rol central în matematică și este legat de noțiunea de *funcție polinomială*, cu care este de altfel confundat adesea. Această confuzie este inofensivă în cazul inelelor întregre infinite, dar nu și în cazul inelelor care nu sînt întregre sau infinite; mai mult, conceperea polinoamelor într-o manieră structurală (ca elemente ale unui nou inel construit plecînd de la un inel dat) are avantajul de a conduce la construcții importante și nebanale. În plus, se poate generaliza construcția riguroasă a inelului clasic de polinoame la inele monoidale, grupale...

Intuitiv, un *polinom* (cu coeficienți într-un inel dat, să zicem *corpul numerelor reale* $\mathbb{R}$) este o „expresie” de forma

$$f = a_0 + a_1 X + \dots + a_n X^n \quad (1)$$

în care apare o „variabilă” sau „nedeterminată” X , iar $a_0, a_1, \dots, a_n$ sînt „coeficienții polinomului”: niște elemente fixate ale inelului dat (în cazul nostru numere reale fixate).

Cea mai la îndemînă interpretare riguroasă a acestui obiect matematic este cea a *funcției* $\tilde{f}: \mathbb{R} \rightarrow \mathbb{R}$, $\tilde{f}(x) = a_0 + a_1 x + \dots + a_n x^n$, $\forall x \in \mathbb{R}$. Să considerăm însă inelul $\mathbb{Z}_3$ al claselor de resturi modulo 3 și polinoamele $f = X^3$ și $g = X$ cu coeficienți în $\mathbb{Z}_3$. Se observă că funcțiile $\tilde{f}: \mathbb{Z}_3 \rightarrow \mathbb{Z}_3$ și $\tilde{g}: \mathbb{Z}_3 \rightarrow \mathbb{Z}_3$ date de $\tilde{f}(x) = x^3$ și $\tilde{g}(x) = x$ sînt egale! Polinoamele f și g *nu* sînt totuși identice.

O soluție ar fi să definim un polinom cu coeficienți într-un inel dat R ca o „sumă formală” de tipul (1), în care $a_0, a_1, \dots, a_n \in R$ sînt „coeficienții polinomului”, iar X are un rol special, de „nedeterminată”, putînd fi înlocuită cu *orice element al lui* R . Aceste „sume formale” se adună și înmulțesc după regulile binecunoscute. Mulțimea acestor „sume formale de tipul (1)” cu coeficienți în R devine atunci un *inel*, notat $R[X]$.

Dar, în aplicații, nedeterminata X este adesea înlocuită cu un element dintr-un inel S *diferit* de inelul inițial R . De exemplu, în cazul polinoamelor cu coeficienți în $\mathbb{R}$, X poate fi înlocuită cu un *număr complex* sau cu o *matrice pătratică* cu elemente numere reale. Mai general, se pot da nedeterminatei valori alese într-o *R-algebră* (noțiune detaliată mai jos). Procedeu de „înlocuire a nedeterminatei” sau de „evaluare a unui polinom într-un punct”, asociază la fiecare polinom f și fiecărui $a \in A$ (unde A este o *R-algebră*) un element $f(a) \in A$ și trebuie să satisfacă regulile:

$$(f + g)(a) = f(a) + g(a); (fg)(a) = f(a) \cdot g(a), \text{ pentru orice polinoame } f \text{ și } g \in R[X]$$

Este util să fixăm $a \in A$ și să considerăm „evaluarea în a ” ca o funcție $v_a : R[X] \rightarrow A$, $v_a(f) = f(a)$. Proprietățile de mai sus revin atunci la a spune că v_a este *morfism de inele*.

Aceste idei intuitive despre polinoame se exprimă riguros și formal în secțiunea următoare, unde, pornind de la un inel R și un monoid G , se construiește *R -algebra monoidală* $R[G]$. În cazurile particulare $G = (\mathbb{N}, +)$ și $G = (\mathbb{N}^n, +)$ se regăsesc algebrele clasice de polinoame $R[X]$, respectiv $R[X_1, \dots, X_n]$.

Cititorii care sînt familiarizați cu noțiunea de R -algebră și inelele clasice de polinoame și nu sînt interesați de algebre monoidale pot trece direct la **III.2**, construcția lui $\mathbb{C}$.

III.1 Algebre. Algebre monoidale și algebre polinomiale

Fie $(R, +, \cdot)$ un inel *comutativ unitar*, cu elementul unitate notat cu 1, fixat pe tot cuprinsul acestui paragraf. Începem cu unele definiții referitoare la R -algebre.

1.1 Definiție. Se numește *R -algebră* un inel $(A, +, \cdot)$ (nu neapărat asociativ sau unitar), înzestrat cu o *operație externă* $"\cdot" : R \times A \rightarrow A$, $(r, a) \mapsto ra$, care îi conferă o structură de R -modul⁴⁶, astfel încît să aibă loc condițiile:

$$r(ab) = (ra)b = a(rb), \forall r \in R, \forall a, b \in A.$$

R -algebra A se numește *asociativă* (respectiv *unitară*, *comutativă*) dacă inelul A are proprietatea corespunzătoare. Notăm cu $\text{Cen}(A) := \{a \in A \mid ab = ba, \forall b \in A\}$ *centrul* lui A , adică subinelul format din elementele care comută cu orice element al lui A .

Pentru R -algebrele *asociative și unitare* există următoarea caracterizare (care poate fi luată drept *definiție* a noțiunii de R -algebră):

1.2 Propoziție. *a) Fie A o R -algebră asociativă și unitară și e elementul său unitate. Atunci aplicația $\alpha : R \rightarrow A$ definită de $\alpha(r) := re$, $\forall r \in R$, este un morfism unitar de inele cu proprietatea că $\alpha(r)a = a\alpha(r)$, $\forall r \in R, \forall a \in A$ (adică $\alpha(R) \subseteq \text{Cen}(A)$).*

b) Reciproc, dacă A este un inel asociativ și unitar, iar $\alpha : R \rightarrow A$ este un morfism unitar de inele cu $\alpha(R) \subseteq \text{Cen}(A)$, atunci A devine o R -algebră definind operația de R -modul prin

$$ra := \alpha(r)a, \forall r \in R, \forall a \in A.$$

Demonstrație. *a) Dacă $r, s \in R$, atunci, folosind definiția R -algebrei, avem:*

$$\alpha(r + s) = (r + s)e = re + se = \alpha(r) + \alpha(s)$$

$$\alpha(r)\alpha(s) = (re)(se) = r(e(se)) = r(se) = (rs)e = \alpha(rs).$$

⁴⁶ Reamintim că axiomele din definiția unui R -modul M sînt exact cele ale unui K -spațiu liniar M (înlocuind peste tot corpul K cu inelul R).

Avem $\alpha(1) = 1e = e$ (căci A este R -modul). Astfel, α este morfism unitar de inele. Dacă $r \in R$, $a \in A$, $\alpha(r)a = (re)a = r(ea) = ra = r(ae) = a(re) = a\alpha(r)$. $\square$

Morfismul $\alpha: R \rightarrow A$ dat de teorema de mai sus se numește *morfismul structural* al R -algebrei asociative și unitare A . Evident, un inel A poate avea mai multe structuri de R -algebră (depinzând de morfismul structural, respectiv de operația externă " $\cdot$ ": $R \times A \rightarrow A$).

1.3 Exemple. a) Inelul de matrice pătratice $M_n(R)$ este o R -algebră asociativă și unitară (necomutativă dacă $n \geq 2$). Morfismul structural asociază lui $r \in R$ matricea cu r pe diagonala principală și 0 în rest.

b) Inelul de polinoame $R[X]$ este o R -algebră comutativă. Dacă $K \subseteq L$ este o extindere de corpuri, L este o K -algebră. Care sînt morfismele structurale (echivalent, care este structura de modul) pentru aceste exemple?

1.4 Definiție. Fie A și B două R -algebre. Un morfism de inele $\varphi: A \rightarrow B$ care este și morfism de R -module se numește *morfism de R -algebre*. Mai precis, φ este morfism de R -algebre dacă și numai dacă, $\forall r \in R$, $\forall a, b \in A$, au loc:

$$\varphi(a + b) = \varphi(a) + \varphi(b); \quad \varphi(ab) = \varphi(a)\varphi(b) \quad (\varphi \text{ este morfism de inele});$$

$$\varphi(ra) = r\varphi(a) \quad (\varphi \text{ este și morfism de } R\text{-module}).$$

Dacă A și B sînt asociative și unitare, iar α , respectiv β sînt morfismele structurale, un morfism unitar de inele $\varphi: A \rightarrow B$ este morfism de R -algebre dacă și numai dacă $\varphi \circ \alpha = \beta$ (Verificați!).

În continuare, prin R -algebră vom înțelege o R -algebră unitară și asociativă.

1.5 Definiție. O submulțime C a R -algebrei A se numește *R -subalgebră* a lui A dacă C este subinel în A și $\forall r \in R$, $\forall a \in C$, rezultă $ra \in C$ (adică C este și R -submodul în A).

Intersecția unei familii de subalgebre ale lui A este tot o subalgebră a lui A (demonstrați!). Astfel, pentru o submulțime oarecare S a lui A , se poate defini *subalgebra generată de S* : este *intersecția tuturor subalgebrelor lui A care includ S* .

1.6 Exercițiu. a) Fie A o R -algebră unitară și $x \in A$. Atunci subalgebra generată de $\{x\}$ (notată cu $R[x]$) este mulțimea „expresiilor polinomiale în x cu coeficienți în R ”, adică:

$$R[x] = \{a_0 + a_1x + \dots + a_nx^n \mid n \in \mathbb{N}, a_0, a_1, \dots, a_n \in R\}.$$

b) Fie A o R -algebră unitară și $S \subseteq \text{Cen}(A)$. Atunci subalgebra generată de S (notată cu $R[S]$) este mulțimea „expresiilor polinomiale în elementele lui S , cu coeficienți în R ”, adică:

$$R[S] = \left\{ \sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} a_{i_1, \dots, i_n} s_1^{i_1} \dots s_n^{i_n} \mid a_{i_1, \dots, i_n} \in R, s_1, \dots, s_n \in S \right\},$$

unde sumele sînt finite (doar un număr finit dintre $a_{i_1, \dots, i_n}$ sînt nenuli). Acest rezultat dă forma subalgebrei generate de orice submulțime S a unei R -algebre comutative și unitare.

Pentru R -algebre și morfisme de R -algebre au loc proprietățile uzuale de la inele și morfisme de inele. Astfel, au loc următoarele proprietăți și construcții, întru totul analoage celor de la inele (demonstrați!):

a) Dacă $\varphi: A \rightarrow B$ este morfism de R -algebre, atunci $\varphi(A)$ este o subalgebră a lui B .

b) Un ideal bilateral I al inelului A se mai numește *ideal* al R -algebrei A . Dacă I este ideal bilateral al R -algebrei A de morfism structural α , atunci inelul factor A/I este o R -algebră, de morfism structural $\pi \circ \alpha$, unde $\pi: A \rightarrow A/I$ este proiecția canonică. Această algebră se numește *algebra factor* a lui A relativ la idealul I .

c) Dacă $\varphi: A \rightarrow B$ este un morfism de R -algebre, atunci $\text{Ker}\varphi = \{a \in A \mid \varphi(a) = 0\}$ este ideal al lui A și are loc teorema fundamentală de izomorfism:

$$\frac{A}{\text{Ker}\varphi} \cong \text{Im}\varphi \text{ (izomorfism de } R\text{-algebre).}$$

Construcția clasică a inelului de polinoame $R[X]$ cu coeficienți în inelul comutativ R (în care un *polinom* este definit ca un *șir de elemente din R , șir în care un număr finit de termeni sînt nenuli*) este predată în liceu și o presupunem cunoscută. Vom prezenta o generalizare a acestei construcții, care permite între altele obținerea directă a inelului de polinoame de mai multe nedeterminate și scoate în evidență rolul esențial al *morfismului de evaluare*.

Fiind dat un monoid $(G, \cdot)$ și un inel comutativ R , vom construi **algebra monoidală** $R[G]$ peste inelul R . Se obțin drept cazuri particulare inelele de polinoame de una, două, sau o mulțime oarecare de nedeterminate.

Ideea ce stă la baza construcției este următoarea: fiind date inelul comutativ R și monoidul $(G, \cdot)$, pe $R^{(G)}$ (R -modulul liber peste mulțimea G) se definește o operație de înmulțire asociativă și distributivă față de adunarea din $R^{(G)}$, care pentru elementele lui G să coincidă cu înmulțirea din G . Orice element din $R^{(G)}$ se scrie în mod unic ca o sumă finită de forma

$$\sum_{g \in G} a_g g, \text{ (cu } a_g \in R, \forall g \in G).$$

Altfel spus, elementele lui G sînt văzute ca elementele unei baze în R -modulul liber $R^{(G)}$. Produsul dintre $g, h \in G$ (văzute ca elemente în baza lui $R^{(G)}$) este gh (văzut tot ca element în baza lui $R^{(G)}$); acest produs se extinde la orice element al lui $R^{(G)}$ de forma de mai sus, astfel încît să fie respectată distributivitatea înmulțirii față de adunare. *Detalierea acestei idei este făcută în continuare.*

Fie deci $(G, \cdot)$ un monoid (adică G este o mulțime nevidă înzestrată cu o operație „ $\cdot$ ”, asociativă și cu element neutru e). Construim mai întîi *mulțimea suport* pe care o vom structura cu operații.

Definim *suportul* unei aplicații $\varphi: G \rightarrow R$ ca fiind mulțimea $\text{supp}(\varphi) := \{g \in G \mid \varphi(g) \neq 0\}$. Notăm $R[G] := \{\varphi: G \rightarrow R \mid \text{supp}(\varphi) \text{ este finit}\}$.

O funcție din $R[G]$ se numește *funcție de suport finit*.⁴⁷ Pe $R[G]$ definim *adunarea* și *înmulțirea*: $\forall \varphi, \psi \in R[G], \forall g \in G$, punem

$$\begin{aligned}(\varphi + \psi)(g) &:= \varphi(g) + \psi(g) \\ (\varphi \cdot \psi)(g) &:= \sum_{\substack{(u,v) \in G \times G \\ uv=g}} \varphi(u)\psi(v).\end{aligned}$$

Prima egalitate definește cu claritate $\varphi + \psi$ ca funcție de la G la R . Trebuie arătat că și $\varphi\psi$ este corect definită, adică suma din definiția lui $\varphi \cdot \psi$ are un număr finit de termeni nenuli. Într-adevăr, mulțimea perechilor $(u,v) \in G \times G$ cu proprietatea că $\varphi(u)\psi(v) \neq 0$ este inclusă în $\text{supp}(\varphi) \times \text{supp}(\psi)$, care este finită.

1.7 Observație. Definiția adunării $\varphi + \psi$ este naturală. Să explicăm de ce s-a definit ca mai sus *înmulțirea* $\varphi \cdot \psi$. În cazul clasic, în care $(G, \cdot)$ este $(\mathbb{N}, +)$, fie $\varphi = (a_0, a_1, \dots, a_n, \dots)$, $\psi = (b_0, b_1, \dots, b_n, \dots)$, adică $\varphi(i) = a_i \dots$ etc. Atunci $\varphi \cdot \psi$ este definit ca $(c_0, c_1, \dots, c_n, \dots)$, unde:

$$c_k = a_0 b_k + a_1 b_{k-1} + \dots + a_k b_0 = \sum_{\substack{(u,v) \in \mathbb{N} \times \mathbb{N} \\ u+v=k}} a_u b_v = \sum_{\substack{(u,v) \in \mathbb{N} \times \mathbb{N} \\ u+v=k}} \varphi(u)\psi(v)$$

Trebuie să arătăm că $\varphi + \psi$ și $\varphi\psi$ sînt funcții de suport finit. Se observă că $\text{supp}(\varphi + \psi) \subseteq \text{supp}(\varphi) \cup \text{supp}(\psi)$, care e finită. Pentru $\varphi\psi$, dacă $g \in G \setminus \{uv \mid u \in \text{supp}(\varphi) \text{ și } v \in \text{supp}(\psi)\}$, atunci $(\varphi\psi)(g)$ este 0, căci toți termenii din suma din definiție sînt nuli. Deci $\text{supp}(\varphi\psi)$ este inclus în $\{uv \mid u \in \text{supp}(\varphi) \text{ și } v \in \text{supp}(\psi)\}$, care este finită.

Așadar, „+” și „ $\cdot$ ” sînt corect definite și sînt legi de compoziție internă pe $R[G]$. Se poate defini și o operație externă „ $\cdot$ ” : $R \times R[G] \rightarrow R[G]$, prin

$$(r\varphi)(g) := r\varphi(g), \forall r \in R, \forall \varphi \in R[G], \forall g \in G.$$

În raport cu această operație, $R[G]$ devine R -modul, care este (izomorf cu) R -modulul liber de bază G (dacă se face abstracție de operația de înmulțire în $R[G]$).

1.8 Propoziție. $(R[G], +, \cdot)$ este inel asociativ unitar.

Demonstrație. Probăm asociativitatea înmulțirii. Fie $\varphi, \psi, \eta \in R[G]$ și $g \in G$.

$$((\varphi\psi)\eta)(g) = \sum_{\substack{(u,v) \in G^2 \\ uv=g}} (\varphi\psi)(u)\eta(v) = \sum_{\substack{(u,v) \in G^2 \\ uv=g}} \left(\sum_{\substack{(s,t) \in G^2 \\ st=u}} \varphi(s)\psi(t) \right) \eta(v) = \sum_{\substack{(s,t,v) \in G^3 \\ stv=g}} \varphi(s)\psi(t)\eta(v).$$

Calculînd $(\varphi(\psi\eta))(g)$, se obține același lucru, deci $(\varphi\psi)\eta = \varphi(\psi\eta)$.

Existența elementelor neutre pentru adunare și înmulțire este demonstrată mai jos. Verificarea celorlalte axiome este propusă ca exercițiu. $\square$

⁴⁷ A se observa analogia cu cazul clasic, în care $(G, \cdot)$ este $(\mathbb{N}, +)$. Un „șir de elemente din R cu un număr finit de termeni nenuli” este de fapt o funcție $\varphi : \mathbb{N} \rightarrow R$, de suport finit.

1.9 Observație. Din construcție, rezultă că $R[G]$ este izomorf cu R -modulul liber de bază G . Putem scrie elementele lui $R[G]$ ca sume „formale” finite de forma $\sum_{g \in G} a_g g$, cu $(a_g)_{g \in G}$ o familie de suport finit de elemente din R , indexată după elementele lui G . Se „identifică” $a \in R$ cu „suma” cu un termen $a \cdot e$; la fel, identificăm $g \in G$ cu $1 \cdot g$. Aceste identificări revin de fapt la a defini două morfisme injective $i : R \rightarrow R[G]$ și $j : G \rightarrow R[G]$ (vezi propoziția de mai jos). Adunarea se face după regula $\sum_{g \in G} a_g g + \sum_{g \in G} b_g g = \sum_{g \in G} (a_g + b_g)g$, iar înmulțirea satisface distributivitatea la stînga și la dreapta față de adunare și regula $(1 \cdot g) \cdot (1 \cdot h) = 1 \cdot (gh)$. Avem :

$$\left(\sum_{g \in G} a_g g \right) \cdot \left(\sum_{g \in G} b_g g \right) = \sum_{g \in G} \left(\sum_{uv=g} (a_u b_v) \right) g.$$

Astfel, $R[G]$ satisface condițiile de la începutul acestui paragraf. Orice element al lui $R[G]$ se scrie în mod unic sub forma $\sum_{g \in G} a_g g$, subînțelegîndu-se că este vorba de sume finite. În particular, $\sum_{g \in G} a_g g = 0 \Leftrightarrow a_g = 0, \forall g \in G$.

Să facem legătura cu inelele de polinoame clasice și să arătăm că această construcție satisface cerințele de la începutul paragrafului. Considerăm următoarele elemente din $R[G]$:

$$\forall g \in G, \text{ definim } \eta_g : G \rightarrow R \text{ prin } \eta_g(h) = \begin{cases} 0, & \text{dacă } h \neq g \\ 1, & \text{dacă } h = g \end{cases}, \forall h \in G;$$

$$\forall r \in R, \text{ definim } \psi_r : G \rightarrow R \text{ prin } \psi_r(h) = \begin{cases} 0, & \text{dacă } h \neq e \\ r, & \text{dacă } h = e \end{cases}, \forall h \in G.$$

Este evident că $\eta_g, \psi_r \in R[G], \forall g \in G, \forall r \in R$. Au loc următoarele proprietăți:

1.10 Propoziție. a) Aplicația $i : R \rightarrow R[G]$, dată prin $i(r) = \psi_r, \forall r \in R$, este un morfism injectiv de inele. În plus, $\text{Im } i \subseteq R[G]$ (adică $R[G]$ este o R -algebră de morfism structural i). De aceea, vom scrie r în loc de ψ_r (identificînd pe $r \in R$ cu imaginea sa $\psi_r \in R[G]$).

b) Aplicația $j : G \rightarrow (R[G], \cdot), j(g) = \eta_g, \forall g \in G$, este un morfism injectiv de monoizi. Vom scrie g în loc de η_g (identificînd pe $g \in G$ cu imaginea sa $\eta_g \in R[G]$).

$$c) \text{ Pentru orice } g, h \in G \text{ și } r \in R, \text{ avem } (\psi_r \cdot \eta_g)(h) = \begin{cases} 0, & \text{dacă } h \neq g \\ r, & \text{dacă } h = g \end{cases}.$$

d) Fie $\varphi \in R[G]$. Notăm $\varphi(g)$ cu $a_g, \forall g \in G$. Atunci φ se scrie sub forma unei sume finite:

$$\varphi = \sum_{g \in \text{supp}(\varphi)} a_g g,$$

unde am identificat pe η_g cu g și pe ψ_{a_g} cu $a_g = \varphi(g), \forall g \in G$.

Scrierea lui φ este unică: dacă $\sum_{g \in G} a_g g = \sum_{g \in G} b_g g$, pentru două aplicații de suport finit $g \mapsto a_g$ și $g \mapsto b_g$ de la G la R , atunci $a_g = b_g, \forall g \in G$.

e) Elementul neutru pentru adunare este ψ_0 (scris ca sumă de tipul $\sum_{g \in G} a_g g$ sub forma sumei cu un termen $0e$). Elementul neutru la înmulțire este $\eta_e = 1e$.

Demonstrație. a) Evident, $\psi_{r+s} = \psi_r + \psi_s$, $\forall r, s \in R$. Calculînd $\psi_r \cdot \psi_s$, obținem $\psi_r \cdot \psi_s(g) = \sum_{uv=g} \psi_r(u) \psi_s(v)$. Dacă $g \neq e$, atunci, pentru orice cuplu (u, v) cu proprietatea că $uv = g$, avem că $u \neq e$ sau $v \neq e$, deci $\psi_r(u) \psi_s(v) = 0$. Așadar, dacă $g \neq e$, atunci $\psi_r \cdot \psi_s(g) = 0$. La fel se observă că $(\psi_r \cdot \psi_s)(e) = \psi_r(e) \cdot \psi_s(e) = rs$. În concluzie, avem $\psi_r \cdot \psi_s = \psi_{rs}$. Injectivitatea este clară.

b) Arătăm că $\eta_g \eta_h = \eta_{gh}$, $\forall g, h \in G$. Pentru $\forall x \in G$, $x \neq gh$, avem $(\eta_g \eta_h)(x) = \sum_{uv=x} \eta_g(u) \eta_h(v) = 0$, căci din $uv = x \neq gh$ rezultă că $u \neq g$ sau $v \neq h$. Pe de altă parte, $(\eta_g \eta_h)(gh) = 1$ (verificare ușoară).

d) Avem, $\forall h \in G$,

$$\left(\sum_{g \in \text{supp}(\varphi)} a_g g \right)(h) = \sum_{g \in \text{supp}(\varphi)} (\psi_{\varphi(g)} \eta_g)(h) = \begin{cases} 0, & \text{dacă } h \notin \text{supp}(\varphi) \\ \varphi(h), & \text{dacă } h \in \text{supp}(\varphi) \end{cases} = \varphi(h).$$

Am folosit în ultima egalitate faptul că $(\psi_{\varphi(g)} \eta_g)(h) = \begin{cases} 0, & \text{dacă } h \neq g \\ \varphi(g), & \text{dacă } h = g \end{cases}$, după punctul c).

Unicitatea rezultă din $\left(\sum_{g \in G} a_g g \right)(h) = a_h$, $\forall h \in G$.

e) Demonstrăm că η_e este unitatea inelului $R[G]$. Pentru orice $g \in G$, avem $\eta_g \eta_e = \eta_{ge} = \eta_g = \eta_e \eta_g$ (am aplicat c). Cazul general rezultă folosind d) și distributivitatea. $\square$

Dacă G este monoid comutativ, atunci și $R[G]$ este inel comutativ. Dacă G nu este comutativ, atunci nici $R[G]$ nu este comutativ (vezi b) de mai sus).

Algebrele polinomiale clasice

1. Pentru $(G, \cdot) = (\mathbb{N}, +)$ se obține construcția uzuală a R -algebrei de polinoame într-o nedeterminată⁴⁸ cu coeficienți în R . Într-adevăr, $R[\mathbb{N}]$ este format din funcțiile $\varphi: \mathbb{N} \rightarrow R$ de suport finit (adică șiruri finite de elemente din R). Notînd $\varphi(i) =: a_i$, $\forall i \in \mathbb{N}$, forma generală a unui element f din $R[\mathbb{N}]$ este $f = \sum_{i \in \mathbb{N}} a_i \eta_i$. Ținînd cont că $\eta_i \eta_j = \eta_{i+j}$, pentru orice $i, j \in \mathbb{N}$, avem că $\eta_i = (\eta_1)^i$, $\forall i \in \mathbb{N}$. Notînd η_1 cu X , se obține scrierea uzuală $f = \sum_{i \in \mathbb{N}} a_i X^i$ (sumă finită). $R[\mathbb{N}]$ se notează de obicei cu $R[X]$.

2. Considerînd monoidul comutativ $(\mathbb{N}^n, +)$ (pentru $n \in \mathbb{N}^*$ fixat), unde adunarea este definită pe componente, se obține construcția R -algebrei $R[\mathbb{N}^n]$, numită R -algebra de polinoame în n nedeterminate. Un element din $R[\mathbb{N}^n]$ se numește *polinom* (în n nedeterminate). Pentru a face legătura cu scrierea clasică a polinoamelor, fie $e_i := (0, \dots, 1, \dots, 0) \in \mathbb{N}^n$ (1 pe locul i , 0 în rest), pentru fiecare $i \in \{1, \dots, n\}$. Se vede ușor că orice element din $\mathbb{N}^n$ se scrie în mod unic – pînă la o ordine a termenilor – ca o sumă de e_i (cu alte

⁴⁸ Se mai folosește terminologia „necunoscută” sau „variabilă” în loc de „nedeterminată”.

cuvinte, e_i generează monoidul $\mathbb{N}^n$). Notăm elementul η_{e_i} cu X_i și îl numim *nedeterminată*. Un produs de nedeterminate (de forma $X_1^{i_1} \dots X_n^{i_n}$) se numește *term*. Orice polinom g din $R[\mathbb{N}^n]$ se scrie în mod unic sub forma unei sume finite:

$$g = \sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} a_{i_1 \dots i_n} X_1^{i_1} \dots X_n^{i_n},$$

unde $(a_{i_1 \dots i_n})_{(i_1, \dots, i_n) \in \mathbb{N}^n}$ este o familie *de suport finit* de elemente din R . Deci g este o combinație liniară cu coeficienți în R de termi. Orice termen al sumei din membrul drept (de forma $a_{i_1 \dots i_n} X_1^{i_1} \dots X_n^{i_n}$, cu $a_{i_1 \dots i_n} \in R$, nenul) se numește *monom* al lui g .

Invităm cititorul să verifice afirmațiile nedemonstrate de mai sus. $R[\mathbb{N}^n]$ se notează de obicei cu $R[X_1, \dots, X_n]$.

3. Inelul de polinoame de S nedeterminate, unde S este o mulțime nevidă oarecare. Se consideră mulțimea $\mathbb{N}^{(S)}$ a funcțiilor de suport finit definite pe S cu valori în $\mathbb{N}$. Interpretăm elementele lui $\mathbb{N}^{(S)}$ ca „multiindici” și le notăm cu $\mathbf{i}, \mathbf{j}, \dots$. Înzestram $\mathbb{N}^{(S)}$ cu o operație notată aditiv: dacă $\mathbf{i}, \mathbf{j} \in \mathbb{N}^{(S)}$, punem $(\mathbf{i} + \mathbf{j})(s) = \mathbf{i}(s) + \mathbf{j}(s)$, $\forall s \in S$. Se vede imediat că se obține o structură de monoid comutativ. Inelul $R[\mathbb{N}^{(S)}]$ se numește *inelul de polinoame de S nedeterminate cu coeficienți în R* . Pentru orice $s \in S$, considerăm funcția $\mathbf{e}_s \in \mathbb{N}^{(S)}$, dată prin $\mathbf{e}_s(t) = \begin{cases} 0, & \text{dacă } s \neq t \\ 1, & \text{dacă } s = t \end{cases}$, $\forall t \in S$ și notăm cu X_s elementul $\eta_{\mathbf{e}_s} \in R[\mathbb{N}^{(S)}]$. Orice element $\mathbf{i}$ din $\mathbb{N}^{(S)}$ se scrie în mod unic sub forma $\mathbf{i} = \sum_{s \in S} m_s \mathbf{e}_s$, unde $(m_s)_{s \in S}$ este o familie de suport finit de numere naturale⁴⁹ indexată după S . Așadar, $\eta_{\mathbf{i}} = \prod_{s \in \text{supp}(\mathbf{i})} X_s^{m_s}$. În consecință, un polinom oarecare f din $R[\mathbb{N}^{(S)}]$ se scrie sub forma $f = \sum_{\mathbf{i} \in F} a_{\mathbf{i}} \eta_{\mathbf{i}}$, cu F o submulțime finită a lui $\mathbb{N}^{(S)}$; dacă notăm $\bigcup_{\mathbf{i} \in F} \text{supp}(\mathbf{i})$ cu $\{s_1, \dots, s_n\}$ (este o submulțime finită a lui S), atunci avem o scriere

$$f = \sum_{(m_1, \dots, m_n) \in \mathbb{N}^n} a_{m_1 \dots m_n} X_{s_1}^{m_1} \dots X_{s_n}^{m_n},$$

unde suma este finită, adică familia $(a_{m_1 \dots m_n})_{(m_1, \dots, m_n) \in \mathbb{N}^n}$ este de suport finit.

Se observă că *orice polinom de S nedeterminate este polinom de un număr finit de nedeterminate din S* . Inelul $R[\mathbb{N}^{(S)}]$ se notează cu $R[(X_s)_{s \in S}]$ sau $R[X_s]_{s \in S}$ sau $R[X; S]$.

Teorema care urmează este de primă importanță și generalizează într-un cadru abstract procedura de „înlocuire a nedeterminatei (nedeterminatelor) cu o valoare (valori) dintr-o R -algebră”.

⁴⁹ Evident, înmulțirea dintre $m \in \mathbb{N}$ și $\mathbf{i} \in R[\mathbb{N}^{(S)}]$ este dată de $(m\mathbf{i})(s) := m \cdot \mathbf{i}(s)$, $\forall s \in S$.

1.11 Teoremă. (Proprietatea de universalitate a algebrei monoidale) Fie R un inel comutativ, $(G, \cdot)$ un monoid și $i : R \rightarrow R[G], j : G \rightarrow R[G]$ aplicațiile canonice definite la 1.10. Tripletul format din algebra monoidală $R[G]$ împreună cu aplicațiile i și j are următoarea proprietate de universalitate: pentru orice R -algebră T de morfism structural $\alpha : R \rightarrow T$ și orice morfism de monoizi $\beta : G \rightarrow (T, \cdot)$, există un unic morfism de R -algebre $\varphi : R[G] \rightarrow T$ astfel încât $\varphi \circ i = \alpha$ și $\varphi \circ j = \beta$:

$$\begin{array}{ccc} G & \xrightarrow{j} & R[G] \\ & \searrow \beta & \downarrow \varphi \\ & & T \end{array}$$

Demonstrație. Presupunem că φ este un morfism cu proprietățile din enunț. Așadar, $\varphi(r) = \alpha(r)$, $\forall r \in R$ și $\varphi(g) = \beta(g)$, $\forall g \in G$. Dacă $\sum_{g \in G} a_g g$ este un element oarecare din $R[G]$, atunci $\varphi\left(\sum_{g \in G} a_g g\right) = \sum_{g \in G} \varphi(a_g) \varphi(g) = \sum_{g \in G} \alpha(a_g) \beta(g)$, ceea ce arată că φ este unic determinat de α și β . Un calcul direct arată că φ dat de egalitatea de mai sus este morfism de inele și satisface condițiile cerute. $\square$

1.12 Observație. Proprietatea de universalitate a algebrei monoidale *determină această algebră pînă la un (unic) izomorfism*: dacă tripletul (A, γ, δ) (cu A o R -algebră de morfism structural $\gamma : R \rightarrow A$ și cu $\delta : G \rightarrow (A, \cdot)$ un morfism de monoizi) satisface aceeași proprietate de universalitate ca tripletul $(R[G], i, j)$, atunci există un unic izomorfism de R -algebre $\varphi : R[G] \rightarrow A$ astfel încât $\varphi i = \gamma$ și $\varphi j = \delta$. Demonstrați!

În cazul algebrelor polinomiale clasice se obține următoarea teoremă importantă, care formalizează și dă un sens precis expresiei „se dau valorile $a_1, \dots, a_n$ nedeterminatelor $X_1, \dots, X_n$ ”:

1.13 Teoremă. Fie R un inel comutativ și A o R -algebră.

a) (Proprietatea de universalitate a algebrei de polinoame $R[X]$) Pentru orice $a \in A$ există un unic morfism de R -algebre $v_a : R[X] \rightarrow A$ cu proprietatea că $v_a(X) = a$.

b) (Proprietatea de universalitate a algebrei de polinoame $R[X_1, \dots, X_n]$) Fie $n \in \mathbb{N}^*$ fixat. Pentru orice n -uplu $\mathbf{a} = (a_1, \dots, a_n) \in A^n$ există un unic morfism de R -algebre $v_{\mathbf{a}} : R[X_1, \dots, X_n] \rightarrow A$ astfel încât $v_{\mathbf{a}}(X_i) = a_i$, $\forall i \in \{1, \dots, n\}$.

c) (Proprietatea de universalitate a inelului de polinoame $R[X; S]$) Fie S o mulțime nevidă. Pentru orice aplicație $\gamma : S \rightarrow A$ există un unic morfism de R -algebre $v_{\gamma} : R[X; S] \rightarrow A$ astfel încât $v_{\gamma}(X_s) = \gamma(s)$, $\forall s \in S$.

Demonstrație. Propunem cititorului să demonstreze direct a) și b). Punctul a) este un caz particular al lui b), care se obține la rîndul său din c) punînd $S = \{1, \dots, n\}$. Pentru a demonstra c), observăm că γ induce un morfism de monoizi

$$\beta: \mathbb{N}^{(S)} \rightarrow (A, \cdot), \beta(\mathbf{i}) = \prod_{s \in \text{supp}(\mathbf{i})} \gamma(s)^{i(s)}, \forall \mathbf{i} \in \mathbb{N}^{(S)}$$

Aplicînd proprietatea de universalitate a algebrei monoidale $R[\mathbb{N}^{(S)}] = R[X; S]$, rezultă existența unui morfism de R -algebre $v_\gamma: R[X; S] \rightarrow A$ astfel încît $v_\gamma \circ j = \beta$, unde $j: \mathbb{N}^{(S)} \rightarrow R[X; S]$ este aplicația canonică; în cazul nostru $j(\mathbf{e}_s) = X_s$, $\forall s \in S$. Deci $v_\gamma(X_s) = \beta(\mathbf{e}_s) = \gamma(s)$.

Unicitatea lui v_α rezultă astfel: dacă $v: R[\mathbb{N}^{(S)}] \rightarrow A$ este un morfism de R -algebre cu $v(X_s) = \gamma(s)$, atunci $v \circ j = \beta$, unde β este morfismul definit mai sus. Din partea de unicitate a proprietății de universalitate a algebrei monoidale rezultă că $v = v_\alpha$. $\square$

Morfismul v_a (respectiv v_a) care apare la punctele *a*) și *b*) se numește *morfismul de evaluare*; dacă $\mathbf{a} = (a_1, \dots, a_n) \in A^n$ și $f \in R[X_1, \dots, X_n]$, atunci $v_a(f)$ se notează prin tradiție $f(a_1, \dots, a_n)$ și se numește *valoarea polinomului f în $(a_1, \dots, a_n)$* . Așadar:

$$\begin{aligned} \forall f = \sum_{i=0}^n b_i X^i \in R[X], \forall a \in A, \text{avem } v_a(f) &= f(a) = \sum_{i=0}^n b_i a^i; \\ \forall f = \sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} b_{i_1 \dots i_n} X_1^{i_1} \dots X_n^{i_n} \in R[X_1, \dots, X_n], \forall \mathbf{a} = (a_1, \dots, a_n) \in A^n, \text{avem} \\ v_{\mathbf{a}}(f) &= f(a_1, \dots, a_n) = \sum_{(i_1, \dots, i_n) \in \mathbb{N}^n} b_{i_1 \dots i_n} a_1^{i_1} \dots a_n^{i_n}. \end{aligned}$$

Este important de observat că procedura de „a da valori nedeterminatei”, formalizată în teorema de mai sus, determină algebra polinomială pînă la un izomorfism (cf. Obs. 1.12). Cum formulați această proprietate pentru $R[X]$, respectiv $R[X_1, \dots, X_n]$?

O proprietate utilă a R -algebrelor $R[X_1, \dots, X_n]$ (uneori folosită pentru a le *defini* recursiv după n) este:

1.14 Teoremă. Fie $n \geq 1$. Atunci există un izomorfism canonic de R -algebre:

$$R[X_1, \dots, X_n] \cong R[X_1, \dots, X_{n-1}][X_n].$$

Demonstrație. Folosim 1.13.b): $\exists!$ $\varphi: R[X_1, \dots, X_n] \rightarrow R[X_1, \dots, X_{n-1}][X_n]$, φ morfism de R -algebre, cu $\varphi(X_i) = X_i$, $1 \leq i \leq n$. Fie $A := R[X_1, \dots, X_{n-1}]$.

Invers, din 1.13.b) aplicat lui $R[X_1, \dots, X_{n-1}]$, $\exists!$ $\alpha: R[X_1, \dots, X_{n-1}] \rightarrow R[X_1, \dots, X_n]$, α morfism de R -algebre, cu $\alpha(X_i) = X_i$, $1 \leq i \leq n-1$. Astfel, $R[X_1, \dots, X_n]$ devine o A -algebră de morfism structural α . Proprietatea de universalitate a A -algebrei de polinoame $A[X_n]$ arată că există un unic $\beta: A[X_n] \rightarrow R[X_1, \dots, X_n]$, β morfism de A -algebre și $\beta(X_n) = X_n$. Evident, β este și morfism de R -algebre.

Arătăm că $\beta\varphi = \text{id}$. $\beta\varphi: R[X_1, \dots, X_n] \rightarrow R[X_1, \dots, X_n]$ este morfism de R -algebre cu $\beta\varphi(X_i) = X_i$, $1 \leq i \leq n$, iar $\text{id}: R[X_1, \dots, X_n] \rightarrow R[X_1, \dots, X_n]$ are aceleași proprietăți. Partea de unicitate de la 1.13.b) arată că $\beta\varphi = \text{id}$. La fel, $\varphi\beta = \text{id}$, deci φ este izomorfism. $\square$

În continuare, facem cîteva considerații asupra noțiunii de *grad* al unui polinom.

Dacă aX^n este un monom în $R[X]$ (cu $a \neq 0$), n se numește *gradul* lui aX^n . Punem $\text{grad } 0 = -\infty$.

Dacă $g \in R[X]$, $g = a_0 + a_1X + \dots + a_nX^n$, cu $a_n \neq 0$, numărul natural n se numește *gradul* lui g , notat $\text{grad } g$ (sau $\deg g$)⁵⁰. Deci gradul lui g este cel mai mare grad al monoamelor lui g . Elementele $a_0, \dots, a_n \in R$ se numesc *coeficienții* polinomului g , iar a_n se numește *coeficientul dominant* al lui g .

Dacă $aX_1^{i_1} \dots X_n^{i_n}$ este un monom în $R[X_1, \dots, X_n]$ (cu $a \neq 0$), și $1 \leq k \leq n$, definim *gradul în X_k* : $\text{grad}(aX_1^{i_1} \dots X_n^{i_n}, X_k) := i_k$ (exponentul lui X_k în monom). Pentru un polinom $g \in R[X_1, \dots, X_n]$, $\text{grad}(g, X_k)$ este cel mai mare grad în X_k al monoamelor lui g . Dacă R este inel integru, atunci gradul este *aditiv*: $\forall g, h \in R[X_1, \dots, X_n]$,

$$\text{grad}(gh, X_k) = \text{grad}(g, X_k) + \text{grad}(h, X_k).$$

Avem și:

$$\text{grad}(g + h, X_k) \leq \max(\text{grad}(g, X_k), \text{grad}(h, X_k)).$$

Este utilă și noțiunea de *grad total*: gradul total al monomului $aX_1^{i_1} \dots X_n^{i_n}$ este $i_1 + \dots + i_n$; gradul total al unui polinom g este cel mai mare grad total al monoamelor sale. În general, când se vorbește fără alte precizări de „gradul” unui polinom în mai multe nedeterminate, este vorba de gradul său total. Un polinom care are toate monoamele de același grad se numește *polinom omogen* sau *formă*. Și gradul total este aditiv, dacă R este integru.

III.2 Corpul numerelor complexe construit ca inel factor

Unul din motoarele dezvoltării matematicii, a algebrei în special, a fost, pînă la mijlocul secolului XIX, *rezolvarea ecuațiilor polinomiale* cu coeficienți reali (remarcăm totuși că o teorie riguroasă a corpului numerelor reale apare abia în a doua jumătate a sec. XIX). Însă ecuații polinomiale foarte simple, de exemplu $X^2 + 1 = 0$, *nu au soluții reale*: formal, „soluția” acestei ecuații este „rădăcina pătrată din -1 ” care, evident, *nu* este un număr real. Încă din sec. XVI s-au folosit „cantități” de tipul $i = \sqrt{-1}$ în exprimarea soluțiilor ecuațiilor și s-a observat că se poate opera în mod coerent cu „numere” de forma $a + bi$, cu a și b numere reale: ele se adună și se înmulțesc conform regulilor „uzuale” (adică se respectă proprietățile de comutativitate, distributivitate, ..., care se regăsesc în axiomele corpului), cu mențiunea (oarecum șocantă) că $i^2 = -1$. Numerele de forma bi au fost numite *numere pur imaginare*, pentru a sublinia că *nu* este vorba de numere reale. Cum se poate face însă pe baze riguroase construcția „numerelor complexe”?

⁵⁰ De la englezescul *degree* (sau francezul *degré*).

În general, construcția care se dă corpului $\mathbb{C}$ al numerelor complexe este următoarea: se definește $\mathbb{C} = \mathbb{R} \times \mathbb{R} = \{(a, b) \mid a, b \in \mathbb{R}\}$ și se înzestreaază $\mathbb{C}$ cu două operații, adunarea și înmulțirea, astfel:

$$(a, b) + (c, d) := (a + c, b + d); \quad (a, b) \cdot (c, d) := (ac - bd, ad + bc), \quad \forall (a, b), (c, d) \in \mathbb{C}$$

Dacă definiția adunării este naturală și este clar că $(\mathbb{C}, +)$ este grup abelian, nu este clar de ce se definește astfel *înmulțirea*; în plus, nu este deloc evident că avem de a face cu o operație asociativă, distributivă față de adunare, care are element neutru și că orice element nenul (diferit de $(0, 0)$) are invers. Aceste fapte sînt consecința unor verificări directe care aduc prea puțină lumină în *motivarea* definiției înmulțirii.

Există o abordare naturală a construcției lui $\mathbb{C}$, folosind noțiuni elementare de algebră: *inele factor, teorema de izomorfism și teorema împărțirii cu rest în inele de polinoame*.

Începem cu această ultimă teoremă, de o importanță ce nu poate fi îndeajuns subliniată.

2.1 Teoremă (teorema împărțirii cu rest în inele de polinoame) *Fie K un corp comutativ și $f, g \in K[X]$, cu $g \neq 0$. Atunci există două polinoame $q, r \in K[X]$ astfel încît $f = gq + r$, unde $r = 0$ sau $\text{grad } r < \text{grad } g$.*

În plus, q, r sînt unic determinate cu proprietățile de mai sus.

Demonstrație. Demonstrația este inspirată din algoritmul de împărțire a polinoamelor predat în școală. Fie $f = a_0 + \dots + a_n X^n$ și $g = b_0 + \dots + b_m X^m$ polinoame din $K[X]$, cu $g \neq 0$ (adică $b_m \neq 0$). Facem o inducție după $n = \text{grad } f$. Dacă $n < m$, punem $q = 0, r = f$. Dacă $n \geq m$, polinomul $h := f - b_m^{-1} a_n X^{n-m} g$ are gradul strict mai mic decît n (termenii de grad n se reduc, de aceea am și ales coeficienții astfel) și, din ipoteza de inducție, putem scrie $h = gq + r$, cu $\text{grad } r < m$. Astfel, $f = g(q + b_m^{-1} a_n X^{n-m}) + r$. Unicitatea e propusă ca exercițiu. $\square$

Problema construcției lui $\mathbb{C}$ poate fi reformulată în termeni mai preciși astfel:

Considerăm în $\mathbb{R}[X]$ polinomul $f = X^2 + 1$, care este ireductibil în $\mathbb{R}[X]$ (căci nu are rădăcini în $\mathbb{R}$ și este de grad 2). Căutăm o *extindere a lui $\mathbb{R}$* (adică un corp $\mathbb{C}$, în care $\mathbb{R}$ să fie subcorp) în care polinomul f să aibă o rădăcină. Acesta este un caz particular al unei probleme fundamentale în teoria ecuațiilor polinomiale:

2.1 Problemă. *Fie K un corp și $f \in K[X]$ un polinom ireductibil, $\text{grad } f \geq 2$ (deci f nu are rădăcini în K). Există un corp L , extindere a lui K , în care f să aibă o rădăcină? Se poate construi efectiv?*

Presupunem problema rezolvată. Fie L un corp care include K , astfel încît f are o rădăcină α în L . Afirmația „polinomul $f \in K[X]$ are rădăcina α în L ” se interpretează riguros astfel: morfismul de evaluare în α , $v_\alpha: K[X] \rightarrow L, f \mapsto f(\alpha)$, are proprietatea că $v_\alpha(f) = 0$. (L fiind o K -algebră, v_α este bine definit, vezi **III.1.13**)

Considerăm morfismul de evaluare în α ,

$$v_\alpha : K[X] \rightarrow L, v_\alpha(g) = g(\alpha), \forall g \in K[X].$$

Atunci $v_\alpha(f) = 0$. În consecință, $\text{Ker } v_\alpha (= \{g \in K[X] \mid v_\alpha(g) = 0\})$ este nenul, căci $f \in \text{Ker } v_\alpha$. Teorema fundamentală de izomorfism spune că

$$\begin{aligned} K[X]/\text{Ker } v_\alpha &\cong \text{Im } v_\alpha \\ g + \text{Ker } v_\alpha &\mapsto v_\alpha(g) \end{aligned} \quad (1)$$

$\text{Im } v_\alpha$ este un subinel al lui L , care conține α (de ce?), deci $\text{Im } v_\alpha$ (sau mai degrabă $K[X]/\text{Ker } v_\alpha$, cu care e izomorf!) ar fi un bun candidat la soluția problemei (dacă ar fi corp!). Să vedem cine e $\text{Ker } v_\alpha$. Cum f este ireductibil, idealul generat de f , notat (f) , este *maximal*. Cum $(f) \subseteq \text{Ker } v_\alpha$ și (f) este maximal, $(f) = \text{Ker } v_\alpha$ ($\text{Ker } v_\alpha \neq K[X]$, căci polinomul constant $1 \notin \text{Ker } v_\alpha$).⁵¹ Astfel, $K[X]/\text{Ker } v_\alpha = K[X]/(f)$ este chiar corp, conform teoremei II.4.8.

Am găsit soluția problemei: punem $L = K[X]/(f)$. Putem însă să considerăm corpul K drept un subcorp al lui $K[X]/(f)$? Există aplicația canonică $\varphi : K \rightarrow K[X]/(f)$, $\varphi(a) = \hat{a}$ (clasa lui a modulo (f) , notată și $a + (f)$), $\forall a \in K$, care este morfism de corpuri (de ce?). Cum φ este injectivă⁵², se poate identifica $a \in K$ cu imaginea sa $\varphi(a) \in L$, deci K este izomorf cu subcorpul $\varphi(K)$ al lui L . Această situație apare des în teoria corpurilor:

2.2 Definiție. Fie K un corp. Dacă $\sigma : K \rightarrow L$ este un morfism de corpuri, atunci tripletul (K, L, σ) se numește o *extindere a lui K* . În acest caz, pentru orice element $a \in K$, obișnuim să identificăm $\sigma(a) \in L$ cu $a \in K$. Astfel, dacă $a \in K$ și $x \in L$, vom scrie $a \cdot x$ în loc de $\sigma(a) \cdot x$ etc. Prin această identificare, K este *subcorp* al lui L și scriem, prin abuz, „extinderea $K \subseteq L$ ” în loc de „extinderea (K, L, σ) ”. Observăm că L este o extindere a lui K dacă și numai dacă L este un corp care are o structură de K -algebră.

Putem acum formula soluția la problema 2.1 de mai sus:

2.3 Teoremă. Fie K un corp și $f \in K[X]$ un polinom ireductibil. Atunci există un corp L , extindere a lui K , în care f are o rădăcină. Mai precis, inelul factor $L := K[X]/(f)$ este corp și K -algebră prin intermediul aplicației naturale $a \mapsto a + (f) = \hat{a}$ (clasa lui a modulo idealul (f)), iar elementul $\alpha = X + (f) = \hat{X}$ este rădăcină a lui f în L .

Demonstrație. Faptul că $L = K[X]/(f)$ este corp a fost justificat mai sus; dăm și o demonstrație „elementară”, care furnizează și un mijloc efectiv de a găsi inverse în $K[X]/(f)$. Fie $\hat{g} \neq \hat{0}$ un element nenul din L , unde $g \in K[X]$. Cum $g \notin (f)$, rezultă $f \nmid g$; ireductibilitatea lui f arată că $(f, g) = 1$. Deci există $u, v \in K[X]$ astfel încât $1 = uf + vg$ ⁵³. Trecând la clase modulo f , obținem $\hat{1} = \widehat{uf + vg} = \widehat{vg}$. Deci $\hat{g}$ are invers, anume $\hat{v} \in L$.

Rădăcina lui f în L este $\hat{X}$ (lucru care poate fi intuit dacă privim la izomorfismul (1) și căutăm contraimaginea lui α). Într-adevăr, fie $f = a_0 + a_1X + \dots + a_nX^n$; atunci:

⁵¹ Cititorul "pierdut" de aceasta demonstrație poate găsi una elementară citind toată pagina.

⁵² Orice morfism de corpuri este injectiv!

⁵³ Polinoamele u și v se pot găsi efectiv cu *algoritmul extins al lui Euclid*.

$$f(\hat{X}) = a_0\hat{1} + a_1\hat{X} + \dots + a_n\hat{X}^n = \overline{a_0 + a_1X + \dots + a_nX^n} = \hat{f} = \hat{0}. \quad \square$$

Construcția lui $\mathbb{C}$. Revenind la $K = \mathbb{R}$ și $f = X^2 + 1$, rezultă că $\mathbb{R}[X]/(X^2 + 1)$ este un corp în care $i := \hat{X}$ (clasa lui X modulo idealul $(X^2 + 1)$) este rădăcină a polinomului $X^2 + 1$:

$$i^2 + \hat{1} = \hat{X}^2 + \hat{1} = \widehat{X^2 + 1} = \hat{0}$$

Să arătăm că putem scrie elementele din $\mathbb{R}[X]/(X^2 + 1)$ sub forma familiară $a + bi$, cu $a, b \in \mathbb{R}$. Un element oarecare din $\mathbb{R}[X]/(X^2 + 1)$ este de forma $\hat{g} = g + (X^2 + 1)$, cu $g \in \mathbb{R}[X]$. Aplicînd teorema împărțirii cu rest polinoamelor g și $X^2 + 1$, există $q, r \in \mathbb{R}[X]$ astfel încît:

$$g = (X^2 + 1)q + r, \text{ cu grad } r < 2.$$

Deci $r = a + bX$, cu $a, b \in \mathbb{R}$. Trecem la clase modulo $(X^2 + 1)$ în egalitatea de mai sus:

$$\hat{g} = \widehat{(X^2 + 1)q + r} = \widehat{r} = \widehat{a + bX} = \hat{a} + \hat{b}\hat{X}$$

Dacă ținem cont că identificăm elementele a din $\mathbb{R}$ cu imaginile lor $\hat{a} = a + (X^2 + 1)$ din $\mathbb{R}[X]/(X^2 + 1)$, iar $\hat{X} = i$, egalitatea de mai sus se scrie

$$\hat{g} = a + bi$$

Scrierea aceasta este unică: dacă $a + bi = c + di$, cu $a, b, c, d \in \mathbb{R}$, atunci $(X^2 + 1)$ divide $a + bX - (c + dX)$ și rezultă imediat că $a = c$ și $b = d$.

Ceea ce am făcut nu este altceva decît determinarea unui *sistem de reprezentanți* pentru clasele din $\mathbb{R}[X]/(X^2 + 1)$; acesta este $\{\widehat{a + bX} \mid a, b \in \mathbb{R}\} = \{a + bi \mid a, b \in \mathbb{R}\}$, clasele tuturor resturilor posibile la împărțirea cu $X^2 + 1$.

Să verificăm și regula uzuală de înmulțire a două elemente scrise sub forma $a + bi$. Pentru aceasta, ținînd cont de distributivitate și că $i^2 = -1$, avem

$$(a + bi) \cdot (c + di) = ac + bdi^2 + adi + bci = ac - bd + (ad + bc)i.$$

Avantajele introducerii lui $\mathbb{C}$ ca $\mathbb{R}[X]/(X^2 + 1)$ sînt următoarele:

- se folosește o construcție (inelul claselor de resturi modulo $(X^2 + 1)$) care are aceeași idee de bază ca și construcția inelului de clase de resturi modulo n , $\mathbb{Z}_n$;
- construcția este naturală, are legătură directă cu polinomul $X^2 + 1$ și ilustrează importanța teoremei împărțirii cu rest în $\mathbb{R}[X]$ și a noțiunii de ireductibilitate;
- nu mai este necesar calculul de verificare a îndeplinirii axiomelor corpului (asociativitate, existența elementului neutru la adunare și înmulțire etc.);
- posibilitatea generalizării imediate la construcții de extinderi de corpuri oarecare, pornind de la polinoame ireductibile.

Vom trece în revistă cîteva dezvoltări ale acestor idei la extinderi oarecare de corpuri. Teorema 2.3 are drept consecință:

2.4 Teoremă. Fie K un corp și $f \in K[X]$, $\text{grad } f \geq 1$. Atunci există o extindere L a lui K , astfel încît f se descompune în factori de gradul 1 în $L[X]$ (f „are toate rădăcinile în L ”).

Demonstrație. Inducție după grad f . Mai precis, considerăm afirmația $P(n)$: „pentru orice corp K și pentru orice polinom $f \in K[X]$, $\text{grad } f = n$, există o extindere L a lui K astfel încât f se descompune în factori de grad 1 în $L[X]$ ”. Dacă $n = 1$, atunci extinderea căutată este chiar K . Presupunem afirmația adevărată pentru orice $t < n$ și o demonstrăm pentru n . Fie deci $f \in K[X]$, $\text{grad } f = n$ și $g \in K[X]$ un factor ireductibil al lui f (f se scrie ca un produs de polinoame ireductibile, vezi IV.2.5). Teorema 2.3 asigură că există o extindere E a lui K în care g are o rădăcină α . În $E[X]$, $f = (X - \alpha)h$, cu $h \in E[X]$. Cum $\text{grad } h = n - 1$, îi putem aplica ipoteza de inducție și deci există o extindere L a lui E în care h (deci și f) se descompune în produs de factori de grad 1. $\square$

2.5 Definiție. Fie $K \subseteq L$ o extindere de corpuri. Atunci L are o structură canonică de K -spațiu vectorial⁵⁴: înmulțirea unui „scalar” din K cu un „vector” din L este înmulțirea din L . Dimensiunea lui L văzut ca spațiu vectorial peste K se numește *gradul extinderii* $K \subseteq L$ și se notează $[L : K]$.

2.6 Definiție. Fie $K \subseteq L$ o extindere și $x \in L$. Spunem că x este *algebric peste* K dacă există un polinom nenul $f \in K[X]$ astfel încât $f(x) = 0$. Spunem că x este *transcendent peste* K dacă nu este algebric peste K .

În extinderea $\mathbb{R} \subseteq \mathbb{C}$, elementul $i \in \mathbb{C}$ este algebric peste $\mathbb{R}$, deoarece este rădăcina polinomului $X^2 + 1 \in \mathbb{R}[X]$. Gradul extinderii este $[\mathbb{C} : \mathbb{R}] = 2$, deoarece $\{1, i\}$ este o bază a $\mathbb{R}$ -spațiului liniar $\mathbb{C}$.

Dacă $K \subseteq L$ este o extindere și $x \in L$ este algebric peste K , atunci există un polinom nenul de grad minim în $K[X]$ care are rădăcina x . Acest polinom este unic determinat dacă cerem să fie unitar (cu coeficientul dominant egal cu 1) și se numește *polinomul minimal al lui x peste K* , notat $\text{Irr}(x, K)$. Are loc următoarea caracterizare a polinomului minimal:

2.7 Teoremă. Fie $K \subseteq L$ o extindere de corpuri și $x \in L$, algebric peste K și $v_x : K[X] \rightarrow L$, $v_x(g) = g(x)$, $\forall g \in K[X]$ (morfismul de evaluare în x). Fie f un polinom unitar cu coeficienți în K . Următoarele afirmații sînt echivalente:

a) $f(x) = 0$ și $\text{grad } f = \min \{\text{grad } g \mid g \in K[X], g(x) = 0, g \neq 0\}$.

b) $f(x) = 0$ și f este ireductibil.

c) f este un generator al idealului $\text{Ker } v_x = \{g \in K[X] \mid g(x) = 0\}$.

d) $f(x) = 0$ și, oricare ar fi $g \in K[X]$ cu $g(x) = 0$, rezultă că $f \mid g$. $\square$

2.8 Exemple. a) $\text{Irr}(\sqrt{2}, \mathbb{Q}) = X^2 - 2$ căci $X^2 - 2 \in \mathbb{Q}[X]$, este unitar, se anulează în $\sqrt{2}$ și este ireductibil în $\mathbb{Q}[X]$.

b) $\text{Irr}(\sqrt{2}, \mathbb{R}) = X - \sqrt{2}$. În general, pentru orice corp K și $a \in K$, $\text{Irr}(a, K) = X - a$.

⁵⁴ Această interpretare este fundamentală în toată teoria extinderilor de corpuri.

Fie extinderea $K \subseteq L$ și $x \in L$. Sînt de primă importanță următoarele noțiuni:

- *subinelul* lui L generat⁵⁵ de K și $\{x\}$, notat $K[x]$. Are loc (demonstrați!):

$$K[x] = \{a_0 + a_1x + \dots + a_nx^n \mid n \in \mathbb{N}, a_i \in K, 0 \leq i \leq n\} = \text{Im } v_x. \quad (\text{S})$$

- *subcorpul* lui L generat de K și $\{x\}$, notat $K(x)$. Are loc:

$$K(x) = \{\alpha\beta^{-1} \mid \alpha, \beta \in K[x], \beta \neq 0\}.$$

De exemplu, subcorpul lui $\mathbb{C}$ generat de $\mathbb{Q}$ și $\sqrt{2}$ este $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$ (demonstrați!). Se observă că nu este nevoie să luăm *toate* expresiile polinomiale (de orice grad) în $\sqrt{2}$, cu coeficienți în $\mathbb{Q}$, ca în caracterizarea (S), ci doar cele de grad mai mic decît 2 = grad Irr($\sqrt{2}$, $\mathbb{Q}$). De asemenea, are loc și $\mathbb{Q}(\sqrt{2}) = \mathbb{Q}[\sqrt{2}]$. Lucrul acesta nu este întîmplător și este caracteristic elementelor *algebrice*:

2.9 Teoremă (de caracterizare a elementelor algebrice). *Fie $K \subseteq L$ o extindere de corpuri și $x \in L$. Următoarele afirmații sînt echivalente:*

- a) x este algebric peste K .
- b) $K[x]$ este corp.
- c) $K[x] = K(x)$.
- d) Extinderea $K \subseteq K(x)$ este finită.

Dacă x este algebric peste K și $f = \text{Irr}(x, K)$, grad $f = n$, atunci $K[X]/(f) \cong K(x)$. În particular, $[K(x) : K] = n$ și o bază a K -spațiului liniar $K(x)$ este $\{1, x, \dots, x^{n-1}\}$.

Demonstrație. $a) \Rightarrow b)$ Fie $f = \text{Irr}(x, K) \in K[X]$ și $v_x : K[X] \rightarrow L$ morfismul de evaluare în x . Avem $\text{Ker } v_x = (f)$. Din teorema de izomorfism pentru inele, $K[X]/(f) \cong \text{Im } v_x = K[x]$. Cum f este ireductibil în $K[X]$, idealul (f) este maximal și $K[X]/(f)$ este corp. Atunci $K[x]$, izomorf cu $K[X]/(f)$, este și el corp.

$b) \Leftrightarrow c)$ Evident.

$c) \Rightarrow a)$ Presupunem că $x \neq 0$ și fie $x^{-1} = a_0 + a_1x + \dots + a_nx^n \in K[x]$ inversul lui x . Înmulțind cu x , obținem $a_0x + a_1x^2 + \dots + a_nx^{n+1} - 1 = 0$, adică x este rădăcina unui polinom nenul cu coeficienți în K .

$d) \Rightarrow a)$ Familia infinită $\{x^i \mid i \in \mathbb{N}\}$ de elemente ale K -spațiului vectorial finit dimensional $K(x)$ este liniar dependentă. Deci, există o relație de dependență liniară de forma $a_0 \cdot 1 + a_1x + \dots + a_nx^n = 0$, cu $n \in \mathbb{N}$ și $a_0, a_1, \dots, a_n \in K$, nu toți nuli, adică x este algebric peste K .

$a) \Rightarrow d)$ Avem K -izomorfismul de corpuri $K[X]/(f) \cong K(x)$. Acesta este și un izomorfism de K -spații vectoriale. Fie $n = \text{grad } f$. Demonstrăm că în K -spațiul vectorial $K[X]/(f)$, clasele elementelor $1, X, \dots, X^{n-1}$ sînt elementele unei baze. Dacă $a_0\hat{1} + a_1\hat{X} + \dots + a_{n-1}\widehat{X^{n-1}} = \hat{0}$, cu $a_0, a_1, \dots, a_{n-1} \in K$, atunci $g = a_0 + a_1X + \dots + a_{n-1}X^{n-1} \in (f)$, adică $f \mid g$. Cum grad $f = n$, rezultă că $g = 0$, adică $a_0, a_1, \dots, a_{n-1}$ sînt nule. Pe de altă parte, folosind teorema împărțirii

⁵⁵ Subinelul lui L generat de o submulțime S a lui L este definit ca intersecția tuturor subinelor lui L care includ S . La fel se definește subcorpul generat de S .

cu rest, orice clasă modulo f a unui polinom $h \in K[X]$ are un reprezentant de grad mai mic decât n . Aceasta înseamnă că $\hat{h}$ este combinație liniară cu coeficienți în K de $\hat{1}, \hat{X}, \dots, \hat{X}^{n-1}$.

Izomorfismul $K[X]/(f) \cong K(x)$ duce $X + (f)$ în x , deci baza $\{1, X, \dots, X^{n-1}\}$ este dusă în baza $\{1, x, \dots, x^{n-1}\}$ în $K[x]$. $\square$

2.10 Definiție. Fie K un corp și x un element algebric peste K . Gradul extinderii $K \subseteq K[x]$ (egal cu grad $\text{Irr}(x, K)$) se numește *gradul elementului x peste K* .

Fie K un corp. Teorema III.2.4 arată că, pentru $f \in K[X]$ dat, există o extindere $K \subseteq L$ în care f are toate rădăcinile. Ar fi de dorit să putem găsi un corp Ω , extindere a lui K , încât orice polinom $f \in K[X]$ de grad ≥ 1 are toate rădăcinile în Ω . În acest sens, este esențial conceptul următor:

2.11 Definiție. Un corp Ω se numește corp *algebric închis* dacă orice polinom de grad ≥ 1 din $\Omega[X]$ are cel puțin o rădăcină în Ω .

2.12 Teoremă (Caracterizarea corpurilor algebric închise). Fie Ω un corp. Următoarele afirmații sînt echivalente:

- a) Ω este corp algebric închis.
- b) Orice polinom cu coeficienți în Ω , de grad $n \geq 1$ se descompune în factori liniari în $\Omega[X]$ (are n rădăcini în Ω).
- c) Nu există extinderi finite proprii ale lui Ω .
- d) Singurele polinoame ireductibile din $\Omega[X]$ sînt cele de grad 1.

Demonstrație. $a) \Rightarrow b)$ Presupunem prin reducere la absurd că există $f \in \Omega[X]$, grad $f \geq 1$, astfel încît f nu se scrie ca un produs de factori liniari în $\Omega[X]$. Alegem f de grad minim cu această proprietate. Din ipoteză, f are o rădăcină $a \in \Omega$, deci $f = (X - a)g$, cu $g \in \Omega[X]$. Dar grad $g < \text{grad } f$, deci g se descompune în factori liniari. Egalitatea $f = (X - a)g$ arată că și f se descompune în factori liniari, contradicție.

$b) \Rightarrow c)$ Dacă $\Omega \subseteq L$ este o extindere finită, iar $\alpha \in L \setminus \Omega$, atunci α este algebric peste Ω ; fie $g = \text{Irr}(\alpha, \Omega)$. Cum $g \in \Omega[X]$, g are o rădăcină în Ω , deci grad $g = 1$ (g este ireductibil!). Deci $\alpha \in \Omega$, contradicție.

Restul implicațiilor sînt lăsate cititorului. $\square$

Are loc următorul rezultat fundamental:

2.13 Teoremă. Orice corp K are o extindere care este corp algebric închis. $\square$

Demonstrația este neconstructivă și folosește Axioma Alegerii (mai precis Lema lui Zorn). Vezi, de exemplu, ION și RADU [1981] sau TOFAN și VOLF [2001].

Un exemplu clasic important de corp algebric închis este $\mathbb{C}$. Nu includem o demonstrație, fiind mai mult tehnică. Așadar, are loc:

2.14 Teoremă.⁵⁶ Corpul $\mathbb{C}$ al numerelor complexe este algebric închis.

□

III.3 Corpuri finite și criptografie

Corpurile finite au depășit de mult stadiul de curiozitate matematică. Corpurile finite sînt esențiale în tehnologiile legate de transmisia, stocarea, secretizarea și prelucrarea informației digitale. Codurile liniare corectoare de erori se bazează pe corpuri finite, iar unele din cele mai puternice scheme criptografice moderne au la bază logaritmul discret într-un corp finit.

Clasificarea corpurilor finite este simplă: *pentru orice număr q , putere a unui prim, există un unic (pînă la izomorfism) corp finit cu q elemente, notat $\mathbb{F}_q$* . Acestea sînt toate corpurile finite (pînă la izomorfism). În plus, grupul $(\mathbb{F}_q^*, \cdot)$ este ciclic. Vom demonstra în continuare aceste fapte.

În acest paragraf, „corp” înseamnă „corp comutativ”.

3.1 Teoremă. Fie F un corp finit cu q elemente. Au loc următoarele afirmații:

- a) Există un număr prim p și $n \in \mathbb{N}^*$ astfel încît $|F| = p^n$.
- b) Pentru orice număr prim p și $n \in \mathbb{N}^*$, există un corp finit cu p^n elemente.

Demonstrație. a) Fie e elementul unitate al lui F . Atunci mulțimea multiplilor lui e , $P := \{n \cdot e \mid n \in \mathbb{N}^*\}$, este o submulțime a lui F și este finită. Deci există $p \in \mathbb{N}^*$ astfel încît $p \cdot e = 0$. Alegem p să fie minim cu această proprietate ($p = \text{car } F$, vezi exercițiul III.3.1). Dacă p nu ar fi prim, atunci $p = ab$, cu $1 < a, b < p$. Cum $p \cdot e = (ab) \cdot e = (a \cdot e) \cdot (b \cdot e) = 0$, rezultă că $a \cdot e = 0$ sau $b \cdot e = 0$, contradicție cu minimalitatea lui p .

Rămîne că există un unic p prim astfel încît $p \cdot e = 0$. Deci $P = \{0, e, 2e, \dots, (p-1)e\}$. Observăm că există o bijecție între P și $\mathbb{Z}_p = \{\hat{0}, \hat{1}, \dots, \widehat{p-1}\}$ (inelul claselor de resturi modulo p), dată de $i \cdot e \mapsto \hat{i}$. Este chiar un izomorfism, după cum se verifică imediat. Deci P este corp (fiind izomorf cu corpul $\mathbb{Z}_p$), iar F este o extindere a sa.

Interpretăm F ca un spațiu liniar peste P . Atunci dimensiunea lui F peste P este finită, fie $\dim_P F = n$. Deci $F \cong P^n$ (izomorfism de spații liniare), adică $|F| = p^n$.

⁵⁶ Această teoremă e cunoscută sub numele de *teorema fundamentală a algebrei* sau *teorema d'Alembert-Gauss*. Jean le Rond d'Alembert propune o demonstrație (incompletă) în 1746. C.F. Gauss dă patru demonstrații corecte acestei teoreme, prima oară în 1797. Alte demonstrații au mai fost date de Jean Argand (1814), Augustin Louis Cauchy (1820). Teorema lui Liouville (datorată de fapt lui Cauchy, 1844) — „orice funcție olomorfa mărginită pe $\mathbb{C}$ este constantă” — demonstrează teorema într-un rînd. Remarcăm că toate demonstrațiile fac apel și la rezultate de analiză matematică, datorită faptului că proprietăți fundamentale (topologice) ale corpului $\mathbb{R}$ nu admit descrieri pur algebrice. Rolul esențial îl joacă mai degrabă proprietățile de ordine ale lui $\mathbb{R}$.

b) Presupunem problema rezolvată: dacă F este corp finit cu $q := p^n$ elemente, grupul $(F^*, \cdot)$ are $q - 1$ elemente. Aplicînd teorema lui Lagrange, obținem că $x^{q-1} = 1$, deci $x^q = x$, $\forall x \in F$. Pe de altă parte, din punctul a), F conține un subcorp izomorf cu $\mathbb{Z}_p$. Deci F este o extindere a lui $\mathbb{Z}_p$, iar $X^q - X \in \mathbb{Z}_p[X]$ se descompune în factori liniari în $F[X]$ (ca în teorema 2.4). Argumentăm acum astfel existența unui corp cu $q = p^n$ elemente: fie corpul $\mathbb{Z}_p$ și $f = X^q - X \in \mathbb{Z}_p[X]$. Din 2.4, există o extindere E a lui $\mathbb{Z}_p$ încît f se descompune în factori liniari în $E[X]$. Considerăm mulțimea $F := \{x \in E \mid x^q = x\}$. Să demonstrăm că F este subcorp al lui E (va fi corpul cu q elemente căutat). Fie $x, y \in F$. Atunci $(xy)^q = x^q y^q = xy$, deci $xy \in F$. Avem și $(x + y)^q = x^q + y^q$ (vezi lema următoare), deci $x + y \in F$. Dacă $x \neq 0$, atunci $(x^{-1})^q = (x^q)^{-1} = x^{-1}$, deci $x^{-1} \in F$. Elementele lui F sînt exact rădăcinile polinomului f , iar acestea sînt în număr de exact q . Într-adevăr, un polinom de grad q are cel mult q rădăcini (IV.3.13); pe de altă parte, f nu are rădăcini multiple, după cum se vede folosind criteriul cu derivata formală IV.3.16: $f' = qX^{q-1} - 1 = -1$, deci $(f, f') = 1$. $\square$

3.2 Lemă. Fie F un corp de caracteristică $p > 0$. Atunci aplicația $\varphi: F \rightarrow F$, $\varphi(x) = x^p$, $\forall x \in F$, este un morfism de corpuri (numit endomorfismul lui Frobenius⁵⁷ al lui F). Dacă F este finit, atunci φ este bijectiv (este un automorfism al lui F). Notînd $q = p^n$, atunci $\varphi^n = \varphi \circ \dots \circ \varphi$ (de n ori) este morfism, iar $\varphi^n(x) = x^q$, $\forall x \in F$.

Demonstrație. Fie $x, y \in F$. Este clar că $\varphi(xy) = \varphi(x)\varphi(y)$. Corpul F fiind comutativ, are loc formula binomului lui Newton:

$$\varphi(x + y) = (x + y)^p = \sum_{0 \leq i \leq p} C_p^i x^{p-i} y^i = x^p + y^p,$$

ultima egalitate avînd loc pentru că p divide coeficienții binomiali C_p^i dacă $1 \leq i < p$ (de ce?).

Morfismul de corpuri $\varphi: F \rightarrow F$ este injectiv, deci bijectiv dacă F este finit.

Avem $(\varphi \circ \varphi)(x) = \varphi(x^p) = (\varphi(x))^p = x^{p^2}$ și, prin inducție, $\varphi^n(x) = x^{p^n}$, $\forall x \in F$, $\forall n \in \mathbb{N}$. $\square$

Grupul multiplicativ al unui corp finit este *ciclic*, proprietate care are multe aplicații:

3.3 Teoremă. Fie F un corp finit cu q elemente. Atunci grupul $(F^*, \cdot)$ este ciclic: există $\alpha \in F^*$ astfel încît $F^* = \{\alpha^i \mid 1 \leq i \leq q - 1\}$. Un astfel de element se numește element primitiv⁵⁸ al lui F .

Demonstrație. Fie m exponentul lui $(F^*, \cdot)$ (vezi exercițiul III.3.2). Tot din exercițiu rezultă că există $\alpha \in F^*$ cu $\text{ord } \alpha = m$. Rămîne să arătăm că $m = q - 1$. Dacă $m < q - 1$, atunci polinomul $X^m - 1$ ar avea $q - 1$ rădăcini (toate elementele lui F^*), contradicție. $\square$

⁵⁷ Ferdinand Georg Frobenius (1849-1917), matematician german.

⁵⁸ În cazul extinderilor oarecare, dacă pentru extinderea $K \subseteq L$ există $a \in L$ astfel încît $L = K(a)$, atunci a se numește *element primitiv* al extinderii. Un element primitiv al unui corp finit F este și un element primitiv al oricărei extinderi $K \subseteq F$.

3.4 Teoremă. *Orice două corpuri finite care au același cardinal sînt izomorfe.*

Demonstrație. Fie F, E corpuri finite cu $q = p^n$ elemente (cu p prim) și $\alpha \in F$ un element primitiv. Atunci $f = X^q - X \in \mathbb{Z}_p[X]$ are rădăcina α în F . Pe de altă parte, f este produs de polinoame ireductibile în $\mathbb{Z}_p[X]$; deci există un (unic) factor ireductibil g al lui f astfel încît $g(\alpha) = 0$. Din III.2.9, $\text{grad } g = [\mathbb{Z}_p(\alpha) : \mathbb{Z}_p] = [F : \mathbb{Z}_p] = n$. Fie β o rădăcină a lui g în E (g are toate rădăcinile în E), atunci $[\mathbb{Z}_p[\beta] : \mathbb{Z}_p] = \text{grad } g = n = [E : \mathbb{Z}_p]$, deci $\mathbb{Z}_p[\beta] = E$. Avem acum izomorfismele (cf. III.2.9): $F = \mathbb{Z}_p[\alpha] \cong \mathbb{Z}_p[X]/(g) \cong \mathbb{Z}_p[\beta] = E$. $\square$

Corpul finit cu p^n elemente (unic pînă la izomorfism) se notează cu $\text{GF}(p^n)$ (Galois Field = corp Galois)⁵⁹ sau $\mathbb{F}_{p^n}$.

Din existența unui corp finit F cu p^n elemente rezultă că există polinoame ireductibile de grad n cu coeficienți în $\mathbb{Z}_p$: de exemplu, polinomul minimal al unui element primitiv al lui F .

3.5 Propoziție. *Pentru orice $n \in \mathbb{N}^*$, există măcar un polinom ireductibil de grad n în $\mathbb{F}_p[X]$; pentru orice astfel de polinom f , $\mathbb{F}_p[X]/(f)$ este un corp cu p^n elemente.* $\square$

Problema construcției efective a unui corp cu p^n elemente se reduce la căutarea unui polinom ireductibil g de grad n în $\mathbb{Z}_p[X]$. Corpul căutat va fi inelul factor $\mathbb{Z}_p[X]/(g)$.

Am determinat corpurile finite în ipoteza că sînt comutative. Este remarcabil faptul că ipoteza aceasta este superfluă: *orice corp finit este comutativ* (Teorema lui Wedderburn⁶⁰). Nu includem o demonstrație.

Aplicație. Logarithmul discret într-un corp finit. Criptografie. Semnături digitale

Fie p un număr prim fixat și $q = p^t$, cu $t \geq 1$. Fie $F = \mathbb{F}_q$, corpul cu q elemente. Fie b un element primitiv al lui F , adică b generează grupul multiplicativ F^* . Atunci orice $a \in F^*$ poate fi scris în mod unic sub forma

$$a = b^r,$$

unde $r \in \mathbb{N}$ și $0 \leq r \leq q - 2$. Numărul r se numește *logarithmul discret al lui a în baza b* și se notează $\log_b(a)$ sau $\text{ind}_b a$.

Date b și a ca mai sus, determinarea algoritmică a lui $\log_b(a)$ este cunoscută ca *problema logarithmului discret* (Discrete Logarithm Problem, DLP). Pe baza unui mare număr de fapte teoretice și practice, DLP este *presupusă ca fiind dificilă* (pentru q mare, ales judicios), mai precis spus *intratabilă computațional*, în sensul că un calcul efectiv al lui $\log_b(a)$ ar lua sute de ani cu algoritmii și mijloacele cunoscute de calcul, pentru valori curent folosite ale lui q și b .

⁵⁹ Structura corpurilor finite a fost determinată de Galois în 1830.

⁶⁰ Joseph Henry MacLagen Wedderburn (1882-1948), matematician scoțian.

Fie $w = \lceil \log_2 r \rceil + 1$ (numărul de biți din reprezentarea lui r în baza 2). Algoritmul de ridicare la putere dat de exercițiul III.3.8 calculează b^r (b și r fiind date) și cere cel mult $2w$ înmulțiri, adică are un timp de rulare de ordinul $O(w)$. Astfel, verificarea faptului că $r = \log_b(a)$ poate fi făcută foarte rapid.

Algoritmul evident (și total ineficient) de găsire a lui $\log_b(a)$ prin căutare exhaustivă (se calculează toate puterile lui b până se găsește a) cere în cel mai rău caz $q - 1$ ridicări la putere (sau înmulțiri) și teste de egalitate, fiind prohibitiv din acest punct de vedere. De exemplu, dacă q are 512 cifre binare (se folosesc astfel de q în scheme criptografice actuale), iar o ridicare la putere în $\mathbb{F}_q$ durează 10^{-12} s, 1000 de calculatoare calculând în paralel au nevoie cam de $2^{512} \cdot 10^{-15}$ secunde de găsire a lui $\log_b(a)$ prin această metodă, adică aproximativ 10^{140} secunde. Vîrsta Universului este estimată la 14 miliarde de ani, aproximativ $5 \cdot 10^{17}$ secunde.

Întrebare. Vi se par plauzibile aceste estimări? De ce? Dar dacă q are 128 de cifre binare?

Criptosistemul ElGamal

Se fixează următorii parametri: q (o putere a unui număr prim) și un element primitiv g al lui $\mathbb{F}_q$ și se fac publice către toți utilizatorii. Utilizatorul A are o *cheie privată* a , $2 \leq a \leq q - 2$ (a este cunoscută doar de A) și publică $y = g^a \in \mathbb{F}_q^*$. Dacă un utilizator B vrea să trimită un mesaj secret m (presupunem că $m \in \mathbb{F}_q^*$) lui A, atunci B alege la întâmplare k , $2 \leq k \leq q - 2$ și calculează în $\mathbb{F}_q^*$

$$y_1 = g^k \text{ și } y_2 = my_1^k.$$

Cuplul (y_1, y_2) („mesajul cifrat”) este trimis de B lui A. Deoarece

$$m = (mg^{ak})g^{-ak} = y_2(g^{-k})^a = y_2(y_1^{-1})^a,$$

A poate descifra mesajul m calculând $m = y_2(y_1^{-1})^a$.

Dacă o persoană neautorizată C interceptează (y_1, y_2) (și, evident, cunoaște y , cheia publică a lui A), C nu poate descoperi mesajul m decât calculând k sau a (ambele implicînd calcularea logaritmului discret în baza g : $k = \log_g y_1$, $a = \log_g y$). Un ipotetic algoritm rapid de găsire a DLP ar permite deci descifrarea rapidă a mesajului secret m . Nu s-a găsit un mijloc de a sparge această metodă de cifrare fără calculul logaritmului discret.

Algoritmul de semnătură digitală ElGamal

Semnarea digitală a unui mesaj m este o modalitate de a asigura un utilizator B că un anumit mesaj m (despre care B crede că provine de la un utilizator A) este într-adevăr trimis de A și nu de cineva care dorește să se dea drept A.⁶¹ Pentru aceasta, se anexează mesajului m o „semnătură digitală” (un șir de simboluri⁶²). Iată un mod de a face aceasta:

Utilizatorul A, care vrea să semneze electronic mesaje, face publice: q (o putere a unui număr prim), g (un element primitiv g al lui $\mathbb{F}_q$) și y , $1 \leq y \leq q - 2$, unde $y = g^a$ ($1 < a < q - 2$,

⁶¹ Puteți da exemplu de o astfel de situație în practică?

⁶² Semnătura electronică trebuie să depindă de A (evident), dar și de m ! De ce?

a este ținut secret de către A). În general, q și g sînt aceleași pentru toți utilizatorii sistemului, doar y fiind specific lui A (nici un alt utilizator nu publică acest y). Pentru a semna mesajul $m \in \mathbb{F}_q^*$, A anexează mesajului m o pereche de numere întregi (r, s) , $1 \leq r, s \leq q - 2$, astfel încît

$$g^m = y^r r^s$$

Întregii r și s sînt generați astfel: A alege aleator un k cu $1 \leq k \leq q - 2$ și $(k, q - 1) = 1$ și calculează $r = g^k$. Cum $y = g^a$, s trebuie să satisfacă ecuația

$$g^m = g^{ar + ks},$$

echivalentă cu $m \equiv ar + ks \pmod{q - 1}$. Deoarece $(k, q - 1) = 1$, ecuația are o unică soluție s modulo $q - 1$, anume $s \equiv (m - ar) \cdot k^{-1} \pmod{q - 1}$, ușor de găsit de către A.

Un utilizator B care primește mesajul m , semnat digital de către A (adică tripletul (m, r, s)) testează autenticitatea prin verificarea egalității $g^m = y^r r^s$.

Se observă că acest algoritm de semnare triplează lungimea mesajelor.

Institutul Național de Standarde și Tehnologii al S.U.A. (National Institute of Standards and Technology, NIST) a stabilit *Standardul de Semnătură Digitală (Digital Signature Standard, DSS)*, care este bazat pe o variantă a algoritmului de semnătură ElGamal de mai sus. DSS este standardul de autentificare digitală al guvernului Statelor Unite. Descriem pe scurt principiile DSS. Algoritmul are următorii parametri:

- un număr prim p a cărui scriere în baza 2 are 512 biți, încît determinarea logaritmului discret în $\mathbb{F}_p^*$ este intratabilă și $p - 1$ are un divizor prim q care are 160 biți;
- un element g de ordin q în $\mathbb{F}_p^*$.

Utilizatorul A își alege o cheie secretă $a \in \mathbb{F}_p^*$ și publică $g^a = b \in \mathbb{F}_p^*$. Pentru a semna un mesaj $m \in \mathbb{F}_p^*$, A alege aleator $k \in \mathbb{Z}_q$ și calculează $(\gamma, \delta) \in \mathbb{Z}_q \times \mathbb{Z}_q$, unde:

$$\gamma = g^k \pmod{q}, \quad \delta = (m + a\gamma) k^{-1} \pmod{q}$$

Cum g are ordin q în $\mathbb{F}_p^*$ și $q|(p - 1)$, g^k este bine definit și în $\mathbb{F}_p^*$ (nu depinde decît de clasa lui k modulo q). Perechea (γ, δ) este anexată mesajului m . Receptorul mesajului certifică autenticitatea lui m prin verificarea egalității:

$$\gamma = (g^m \cdot b^\gamma)^{\delta^{-1}} \pmod{q}$$

Propunem cititorului demonstrarea faptului că algoritmul funcționează așa cum e descris. Se observă că acest algoritm transformă un mesaj m de 512 biți în mesajul (m, γ, δ) de $512 + 2 \cdot 160 = 842$ biți, fiind mai eficient din acest punct de vedere decît algoritmul original ElGamal.

Exerciții

- (Caracteristica unui inel) Fie K un inel și e elementul său unitate. Dacă există $k \in \mathbb{N}^*$ astfel încât $ke = 0$, atunci definim $\text{car } K = \min\{k \in \mathbb{N}^* \mid ke = 0\}$. În caz contrar, punem $\text{car } K = 0$.
 - Demonstrați că, dacă K este integru, atunci $\text{car } K = 0$ sau un număr prim.
 - Dacă K este corp de caracteristică $p > 0$, atunci K are un unic subcorp izomorf cu $\mathbb{Z}_p$.
 - Dacă K este corp de caracteristică 0, atunci K are un unic subcorp izomorf cu $\mathbb{Q}$.
- Fie $(G, \cdot)$ un grup finit. Definim *exponentul* lui G , $\exp(G) := \text{cmmmc}\{\text{ord } a \mid a \in G\} = \min\{n \mid x^n = 1, \forall x \in G\}$.⁶³ Să se arate că:
 - Dacă $a, b \in G$, $ab = ba$ și $(\text{ord } a, \text{ord } b) = 1$, atunci $\text{ord } ab = (\text{ord } a) \cdot (\text{ord } b)$.
 - Pentru orice $a, b \in G$ cu $ab = ba$, există $c \in G$ cu $\text{ord } c = [\text{ord } a, \text{ord } b]$.
 - Dacă G este abelian, există un element al lui G care are ordinul egal cu $\exp(G)$.
- Dacă R este inel comutativ integru, iar G este un subgrup finit al lui $(U(R), \cdot)$, atunci G este ciclic.
- Dacă F este un corp cu p^n elemente, iar K este un subcorp al său, atunci există $m \mid n$ astfel încât $|K| = p^m$. Reciproc, pentru orice divizor m al lui n există un unic subcorp al lui F cu $p^m =: r$ elemente, anume $K = \{x \in F \mid x^r = x\}$.
- Fie F un corp finit și $m \in \mathbb{N}^*$. Demonstrați că există un polinom ireductibil de grad m în $F[X]$.
- Construiți corpuri finite cu 4, 8, 16, 25, 9 și 27 elemente. Pentru fiecare din ele găsiți câte un element primitiv.
- (Numărul polinoamelor ireductibile de grad m cu coeficienți într-un corp finit) Fie $F \subseteq L$ o extindere de grad m de corpuri finite, unde F are q elemente. Pentru orice $d \in \mathbb{N}^*$, notăm $P_{q,d} = \{f \in F[X] \mid \text{grad } f = d, f \text{ ireductibil și unitar}\}$.
 - Demonstrați că $X^{q^m} - X = \prod_{\alpha \in L} (X - \alpha) = \prod_{d \mid m} \prod_{f \in P_{q,d}} f$.
 - Notăm cu $R_f = \{\alpha \in L \mid f(\alpha) = 0\}$, $\forall f \in F[X]$. Arătați că $\bigcup \{R_f \mid f \in P_{q,d}, d \mid m\} = L$ (reuniune disjunctă).
 - Demonstrați că $q^m = \sum_{d \mid m} |P_{q,d}| \cdot d$.
 - Calculați $P_{2,m}$ și $P_{3,m}$, $1 \leq m \leq 6$.
- Scrieți un algoritm eficient de calcul al lui b^r , unde b este un element dintr-un inel sau monoid pentru care se cunoaște un algoritm de înmulțire a două elemente oarecare, iar r este un număr natural. (Ind. Folosiți ridicări la pătrat repetate și pe înmulțiri cu b , când e cazul. Exemplu: pentru a calcula $a = b^{22}$, scriem mai întâi 22_{10} în baza 2, $22 = 10110_2$ și calculăm succesiv $a = b$, $b^2 = a * a$, $b^5 = (a * a) * b$, $b^{10} = a * a$, $b^{21} = (a * a) * b$. Vezi tabel:

⁶³ Din teorema lui Lagrange, $\exp(G)$ divide cardinalul lui G .

Pasul	0	1	2	3	4
Cifra binară a lui r	1	0	1	1	0
Valoarea lui a	b	$b^2 = a*a$	$b^5 = (a*a)*b$	$b^{11} = (a*a)*b$	$b^{22} = a*a$

III.4 Polinoame simetrice

Fie R un inel comutativ unitar, fixat. Fie $n \in \mathbb{N}^*$ și $\sigma \in S_n$ (grupul permutărilor de n obiecte). Există un unic morfism de R -algebre $\varphi_\sigma: R[X_1, \dots, X_n] \rightarrow R[X_1, \dots, X_n]$ astfel încât $\varphi_\sigma(X_i) = X_{\sigma(i)}$, $\forall i = 1, \dots, n$ (am folosit **1.13** – proprietatea de universalitate a R -algebrei de polinoame $R[X_1, \dots, X_n]$). Dacă $g \in R[X_1, \dots, X_n]$, atunci

$$\varphi_\sigma(g) = g(X_{\sigma(1)}, \dots, X_{\sigma(n)}).$$

4.1 Definiție. Fie R un inel comutativ unitar și $g \in R[X_1, \dots, X_n]$. Spunem că g este *polinom simetric* în $R[X_1, \dots, X_n]$ dacă, $\forall \sigma \in S_n$, are loc $\varphi_\sigma(g) = g$.

Dacă R este integru, de corp de fracții K , considerăm $K(X_1, \dots, X_n)$ (corpul de fracții al inelului integru $R[X_1, \dots, X_n]$, numit *corpul fracțiilor raționale* în nedeterminatele $X_1, \dots, X_n$ cu coeficienți în K). Se definește noțiunea de fracție rațională simetrică, astfel: φ_σ se prelungește la un unic morfism de corpuri (notat tot cu φ_σ) $\varphi_\sigma: K(X_1, \dots, X_n) \rightarrow K(X_1, \dots, X_n)$; are loc, $\forall g, h \in R[X_1, \dots, X_n]$, $h \neq 0$: $\varphi_\sigma(g/h) = \varphi_\sigma(g)/\varphi_\sigma(h)$. Frația rațională $g/h \in K(X_1, \dots, X_n)$ se numește *simetrică* dacă, $\forall \sigma \in S_n$, are loc $\varphi_\sigma(g/h) = g/h$.

4.2 Exemple. În $R[X_1, X_2, X_3]$, polinoamele următoare sînt simetrice: $X_1 + X_2 + X_3$, $X_1 X_2 X_3$, $X_1^2 X_2 + X_1^2 X_3 + X_2^2 X_1 + X_2^2 X_3 + X_3^2 X_1 + X_3^2 X_2$. Polinomul $X_1 + X_2$ nu este simetric în $R[X_1, X_2, X_3]$ (dar este simetric în $R[X_1, X_2]$).

4.3 Observații. a) Mulțimea polinoamelor simetrice este o subalgebră a lui $R[X_1, \dots, X_n]$: dacă $g, h \in S$, atunci $\varphi_\sigma(g+h) = \varphi_\sigma(g) + \varphi_\sigma(h) = g+h$, $\forall \sigma \in S_n$. Analog se verifică celelalte condiții.

Arătați că, dacă K este corp, atunci fracțiile raționale simetrice din $K(X_1, \dots, X_n)$ formează un subcorp.

b) Dacă $aX_1^{i_1} \dots X_n^{i_n}$ apare ca monom în polinomul simetric $g \in R[X_1, \dots, X_n]$, atunci, $\forall \sigma \in S_n$, $aX_{\sigma(1)}^{i_1} \dots X_{\sigma(n)}^{i_n}$ apare ca monom în g .

4.4 Definiție. Fie $n \in \mathbb{N}^*$ și $0 \leq k \leq n$. Se numește *polinom simetric fundamental* (sau *elementar*) de grad k în $R[X_1, \dots, X_n]$ polinomul

$$s_k := \sum \{ \prod_{i \in I} X_i \mid I \subseteq \{1, \dots, n\}, |I| = k \}.$$

s_k este așadar suma tuturor produselor de k nedeterminate distincte alese din $\{X_1, \dots, X_n\}$; s_k are așadar C_n^k monoame. Prin convenție, se pune $s_k = 0$ pentru $k > n$ și $s_0 = 1$. Polinomul s_k este *omogen* de grad k (toate monoamele sale au gradul k). Întrucât s_k depinde de numărul nedeterminatelor, uneori vom nota $s_k(X_1, \dots, X_n)$ pentru a evita confuziile. De exemplu, pentru $n = 4$:

$$s_0 = 1$$

$$s_1 = X_1 + X_2 + X_3 + X_4$$

$$s_2 = X_1 X_2 + X_1 X_3 + X_1 X_4 + X_2 X_3 + X_2 X_4 + X_3 X_4$$

$$s_3 = X_1 X_2 X_3 + X_1 X_2 X_4 + X_1 X_3 X_4 + X_2 X_3 X_4$$

$$s_4 = X_1 X_2 X_3 X_4$$

Polinoamele simetrice fundamentale apar în relațiile dintre coeficienții și rădăcinile unui polinom.

4.5 Teoremă. a) Fie $n \in \mathbb{N}^*$ și $s_k = s_k(X_1, \dots, X_n)$. În $R[X_1, \dots, X_n][X]$ are loc relația:

$$(X - X_1) \dots (X - X_n) = X^n - s_1 X^{n-1} + s_2 X^{n-2} - \dots + (-1)^n s_n.$$

b) Dacă R este subinel al inelului integru S și $g = a_0 + a_1 X + \dots + a_n X^n \in R[X]$ are rădăcinile $x_1, \dots, x_n \in S$, atunci $a_n s_k(x_1, \dots, x_n) = (-1)^k a_{n-k}$.

Demonstrație. a) Inducție după n (exercițiu).

b) Există un unic morfism de R -algebre $\varphi: R[X_1, \dots, X_n][X] \rightarrow S[X]$ astfel încât $\varphi(X_i) = x_i$ și $\varphi(X) = X$. Avem, din a):

$$\varphi(a_n(X - X_1) \dots (X - X_n)) = a_n(X - x_1) \dots (X - x_n) = a_n(X^n - s_1 X^{n-1} + s_2 X^{n-2} - \dots + (-1)^n s_n).$$

Pe de altă parte, $a_n(X - x_1) \dots (X - x_n) = g$ (în corpul de fracții K al lui S , au aceleași rădăcini și același coeficient dominant). Se identifică acum coeficienții. $\square$

4.6 Lemă. a) Fie $(A, \leq)$ și $(B, \leq)$ două mulțimi bine ordonate. Atunci $A \times B$ este o mulțime bine ordonată de ordinea lexicografică dată de:

$$(a, b) \leq (a', b') \text{ dacă și numai dacă } a < a' \text{ sau } (a = a' \text{ și } b \leq b').$$

b) Într-o mulțime bine ordonată $(A, \leq)$ nu există șiruri infinite strict descrescătoare.

c) $\forall n \in \mathbb{N}$, mulțimea T_n a termenilor din $R[X_1, \dots, X_n]$ este bine ordonată de ordinea lexicografică (deci nu există un șir infinit strict descrescător de termi).

Demonstrație. a) Reamintim că mulțimea ordonată $(A, \leq)$ se numește *bine ordonată* dacă orice submulțime nevidă a lui A are un prim element. Fie $S \subseteq A \times B$, nevidă. Cum $S_1 := \{a \in A \mid \exists b \in B \text{ cu } (a, b) \in S\} \neq \emptyset$, iar A este bine ordonată, există primul său element $\alpha \in S_1$ (deci $\forall (a, b) \in S, \alpha \leq a$). Fie $S_2 := \{b \in B \mid (\alpha, b) \in S\}$. Există primul element β al lui S_2 . Atunci (α, β) este primul element al lui S : $\forall (a, b) \in S$, avem sau $\alpha < a$ (deci $(\alpha, \beta) < (a, b)$) sau $\alpha = a$, caz în care $b \in S_2$, deci $\beta \leq b$.

b) Fie $(a_n)_{n \geq 1}$ un șir descrescător de elemente din A . Atunci mulțimea $\{a_n \mid n \geq 1\}$ are un prim element, fie acesta a_k . Pentru $n \geq k$, avem deci $a_k \leq a_n$; cum $a_n \leq a_k$ (șirul este descrescător), rezultă $a_n = a_k$ și șirul nu este strict descrescător.

c) Inducție după n . Dacă $n = 1$, $T_1 = \{X^n \mid n \in \mathbb{N}\}$ este izomorfă ca mulțime ordonată cu $(\mathbb{N}, \leq)$, care este bine ordonată. Dacă $n > 1$, T_n cu ordinea lexicografică este izomorfă cu $T_{n-1} \times T_1$ cu ordinea definită ca la punctul a). Din ipoteza de inducție, T_{n-1} este bine ordonată și din a) rezultă $T_{n-1} \times T_1$ bine ordonată.

4.7 Teoremă. (Teorema fundamentală a polinoamelor simetrice) Fie R un inel comutativ unitar și g un polinom simetric din $R[X_1, \dots, X_n]$. Atunci există un unic polinom $h \in R[X_1, \dots, X_n]$ astfel încât $g = h(s_1, \dots, s_n)$.

Cu alte cuvinte, notînd cu S subalgebra polinoamelor simetrice din $R[X_1, \dots, X_n]$, unicul morfism de R -algebre $\psi: R[X_1, \dots, X_n] \rightarrow S$ cu proprietatea că $\psi(X_i) = s_i$ (pentru $1 \leq i \leq n$) este un izomorfism.

Demonstrație. Notăm cu $T := \{X_1^{i_1} \dots X_n^{i_n} \mid (i_1, \dots, i_n) \in \mathbb{N}^n\}$ mulțimea termenilor din $R[X_1, \dots, X_n]$. Definim o relație de ordine pe T (ordinea lexicografică): ordonăm total $\{X_1, \dots, X_n\}$ (de exemplu $X_1 > X_2 > \dots > X_n$) și definim $X_1^{i_1} \dots X_n^{i_n} < X_1^{k_1} \dots X_n^{k_n} \Leftrightarrow \exists r, 1 \leq r \leq n$, astfel încît $i_r = k_r, \forall t < r$ și $i_r < k_r$. Se obține o relație de ordine strictă (ireflexivă și tranzitivă) pe T . De exemplu, avem $1 < X_3^7 < X_2 X_3^2 < X_1 < X_1 X_2^2$. Ca de obicei, notăm cu $\leq$ relația de ordine (nestrictă) asociată. Această relație de ordine este totală⁶⁴ și compatibilă cu înmulțirea, adică, $\forall \lambda, \mu, \nu \in T$, din $\mu \leq \nu$ rezultă $\lambda \mu \leq \lambda \nu$. Relația astfel definită este chiar singura ordine pe T , compatibilă cu înmulțirea, care satisface $X_1 > X_2 > \dots > X_n$.

Ordinea lexicografică induce o relație de preordine⁶⁵, notată tot „ $\leq$ ”, pe mulțimea $\{a\lambda \mid \lambda \in T, a \in R, a \neq 0\}$ a monoamelor din $R[X_1, \dots, X_n]$, prin $a\lambda \leq b\mu \Leftrightarrow \lambda \leq \mu$. Demonstrarea afirmațiilor precedente este un exercițiu de rutină. Dacă $p \in R[X_1, \dots, X_n]$, există un unic monom care este cel mai mare monom al lui p (față de preordinea lexicografică), numit *monom dominant* al lui p . Îl notăm cu $hm(p)$. Are loc următoarea proprietate:

Dacă $p, q \in R[X_1, \dots, X_n]$, astfel încît $hm(p) = a\lambda, hm(q) = b\mu$, unde $\lambda, \mu \in T, a, b \in R$ și $ab \neq 0$, atunci $hm(pq) = hm(p)hm(q) = ab\lambda\mu$.

Într-adevăr, orice monom al lui pq este o sumă de monoame de forma $r\alpha \cdot s\beta$, unde $r\alpha$ este monom al lui p , $s\beta$ este monom al lui q . Dar $\alpha \leq \lambda$ și $\beta \leq \mu$, deci $\alpha\beta \leq \lambda\beta \leq \lambda\mu$. Astfel, $ab\lambda\mu = hm(pq)$.

Fie deci g un polinom simetric și fie $hm(g) = aX_1^{i_1} \dots X_n^{i_n}$. Atunci $i_1 \geq i_2 \geq \dots \geq i_n$ (dacă $\exists k$ astfel încît $i_k < i_{k+1}$, atunci $aX_1^{i_1} \dots X_k^{i_{k+1}} X_{k+1}^{i_k} \dots X_n^{i_n}$ este monom în g , strict mai mare decît

⁶⁴ Mai mult, T este o mulțime bine ordonată de ordinea lexicografică (orice submulțime nevidă a lui T are un prim element). Se pot face deci demonstrații prin inducție după această ordine (cum este demonstrația de față).

⁶⁵ Adică o relație reflexivă și tranzitivă, dar nu neapărat antisimetrică.

$hm(g)$). Căutăm un polinom p de forma $as_1^{j_1} \dots s_n^{j_n}$ astfel încât $hm(p)$ să fie $hm(g)$. Din proprietatea de mai sus, $hm(as_1^{j_1} \dots s_n^{j_n}) = aX_1^{j_1}(X_1X_2)^{j_2} \dots (X_1 \dots X_n)^{j_n}$. Acest monom este egal cu $hm(g)$ dacă și numai dacă $j_1 + \dots + j_n = i_1, j_2 + \dots + j_n = i_2, \dots, j_n = i_n$. Rezultă $j_n = i_n, j_k = i_k - i_{k+1}$ pentru $1 \leq k < n$. Polinomul

$$g_1 := g - as_1^{j_1} \dots s_n^{j_n}$$

este simetric și are $hm(g_1) < hm(g)$. Dacă $hm(g_1) = 0$, avem $g_1 = 0$ și am terminat. Dacă $hm(g_1) \neq 0$, aplicăm același procedeu pentru g_1 . Algoritmul se termină după un număr finit de pași deoarece nu poate exista un șir infinit strict descrescător de termi, conform lemei 4.6. Aceasta încheie demonstrația părții de existență.

Arătăm unicitatea (cu alte cuvinte, $\text{Ker} \psi = 0$). Presupunem că există un polinom nenul $p \in R[X_1, \dots, X_n]$ astfel încât $\psi(p) = p(s_1, \dots, s_n) = 0$. Afirmăm că există un unic monom nenul λ al lui p astfel încât $hm(\psi(p)) = hm(\lambda(s_1, \dots, s_n))$. Dacă $\alpha = X_1^{i_1} \dots X_n^{i_n}, \beta = X_1^{j_1} \dots X_n^{j_n} \in T$, cu $\alpha \neq \beta$, atunci:

$$hm(\alpha(s_1, \dots, s_n)) = X_1^{i_1+\dots+i_n} \dots X_n^{i_n} \neq X_1^{j_1+\dots+j_n} \dots X_n^{j_n} = hm(\beta(s_1, \dots, s_n)).$$

Deci $\exists! \lambda \neq 0$ monom al lui p astfel încât $hm(\lambda(s_1, \dots, s_n)) = \max \{hm(\alpha(s_1, \dots, s_n)) \mid \alpha \text{ monom al lui } p\}$. Cum $p(s_1, \dots, s_n) = \sum \{\alpha(s_1, \dots, s_n) \mid \alpha \text{ monom al lui } p\}$, rezultă că

$$hm(p(s_1, \dots, s_n)) = hm(\lambda(s_1, \dots, s_n)) \neq 0, \text{ contradicție cu } p(s_1, \dots, s_n) = 0. \quad \square$$

Teorema 4.7 se extinde ușor și la fracții raționale simetrice:

4.8 Corolar. (Teorema fundamentală a fracțiilor raționale simetrice) *Fie R un inel integr și K corpul său de fracții. Dacă $p, q \in R[X_1, \dots, X_n], q \neq 0$, astfel încât p/q este o fracție rațională simetrică, atunci există polinoamele $f, g \in R[X_1, \dots, X_n]$ astfel încât $\frac{p}{q} = \frac{f(s_1, \dots, s_n)}{g(s_1, \dots, s_n)}$. Cu alte cuvinte, subcorpul fracțiilor raționale simetrice din corpul $K(X_1, \dots, X_n)$ este $K(s_1, \dots, s_n)$.*

Demonstrație. Dacă q este polinom simetric, atunci p este simetric (ca produs în subcorpul fracțiilor raționale simetrice dintre q și p/q). Din 4.7 rezultă că $p, q \in R[s_1, \dots, s_n]$. Dacă q nu este simetric, fie $s = \prod_{\sigma \in S_n} \varphi_\sigma(q)$. Atunci s este simetric și

$$\frac{p}{q} = \frac{p \prod_{\sigma \neq \text{id}} \varphi_\sigma(q)}{s},$$

și am revenit la primul caz. $\square$

Să exprimăm polinomul simetric $t_m := X_1^m + \dots + X_n^m \in R[X_1, \dots, X_n]$ ($m \in \mathbb{N}$) în funcție de polinoamele simetrice $s_1, \dots, s_n$. Identitățile următoare permit un calcul recursiv al lui t_m ca polinom de $s_1, \dots, s_n$.

4.9 Propoziție. (Identitățile lui Newton) *În $R[X_1, \dots, X_n]$ are loc relația:*

$$t_m = s_1 t_{m-1} - s_2 t_{m-2} + \dots + (-1)^{m-2} s_{m-1} t_1 + (-1)^{m-1} m s_m.$$

Demonstrație. Dacă $m > n$, atunci convenția $s_k = 0$ pentru $k > n$ trunchiază formula de mai sus (sînt numai n termeni).

Fie $r \leq n$ și $(a_1, \dots, a_r)$ un r -uplu de numere naturale cu $a_1 \geq a_2 \geq \dots \geq a_r$. Notăm cu $s(a_1, \dots, a_r)$ unicul polinom simetric din $R[X_1, \dots, X_n]$ cu monomul dominant $X_1^{a_1} X_2^{a_2} \dots X_r^{a_r}$.

De exemplu, $s(m, 0, \dots, 0) = X_1^m + \dots + X_n^m = t_m$, $s(1, 1, 0, \dots, 0) = X_1 X_2 + X_1 X_3 + \dots = s_2$. Pentru a simplifica notația, punem $1_i := (1, \dots, 1)$ (1 apare de i ori) și $(a, 1_i) := (a, 1, \dots, 1)$ (1 apare de i ori); de asemenea, vom omite să scriem un șir de 0: $s(m, 0, \dots, 0) = s(m)$, $s(1, 1, 0, \dots, 0) = s(1, 1) = s_2$, $s(1_i, 0, \dots, 0) = s(1_i) = s_i$. Relațiile următoare se verifică ușor:

$$s_1 t_{m-1} = t_m + s(m-1, 1)$$

$$s_2 t_{m-2} = s(m-1, 1) + s(m-2, 1, 1)$$

$$s_3 t_{m-3} = s(m-2, 1, 1) + s(m-3, 1, 1, 1)$$

...

Mai general, pentru orice $i \leq \min\{m-1, n\}$,

$$s_i t_{m-i} = s(m-i+1, 1_i) + s(m-i, 1_i).$$

Dacă $m \leq n$ și $i = m-1$, atunci

$$s_{m-1} t_1 = s(2, 1_{m-2}) + m s_m.$$

Dacă $m > n = i$, atunci

$$s_n t_{m-n} = s(m-n+1, 1_{n-1}).$$

Identitățile lui Newton rezultă folosind relațiile de mai sus în suma $\sum_{1 \leq i < m} (-1)^{i-1} s_i t_{m-i}$. $\square$

IV. Aritmetică în inele și aplicații

Considerăm indispensabilă o bună cunoaștere de către profesorii de matematică a teoriei divizibilității („aritmetica”) în $\mathbb{Z}$ și în inele de forma $K[X]$, cu K corp, această teorie apărând sub diverse forme pe tot parcursul algebrei studiate în gimnaziu și liceu. Conceptele și rezultatele privind divizibilitatea în $\mathbb{Z}$ prezintă multe analogii cu cele din $K[X]$, fenomen care nu este întâmplător, ci este consecința faptului că ambele sînt inele *euclidiene*.

O clasă largă de inele în care se poate dezvolta o teorie a divizibilității care să o urmeze pe cea din $\mathbb{Z}$ este clasa *inelelor integrale*. O astfel de generalizare, pe lângă un interes intrinsec, aduce de multe ori clarificări și rezultate noi privind chiar divizibilitatea în $\mathbb{Z}$.

Se vor trece în revistă proprietățile generale mai importante ale relației de divizibilitate într-un inel integru. Clase importante de inele (*euclidiene, principale, factoriale*) apar prin abstractizarea unor proprietăți aritmetice ale lui $\mathbb{Z}$. Noțiunile și rezultatele expuse sînt fundamentale pentru toată algebra, în special pentru teoria algebrică a numerelor și teoria extinderilor de corpuri.

IV.1 Divizibilitate

Definiția divizibilității în $\mathbb{Z}$ se transpune cuvînt cu cuvînt pentru un inel oarecare R .

1.1 Definiție. Dacă $a, b \in R$, spunem că a divide b în R (notație: $a|b$ sau $b : a$) dacă există $c \in R$ astfel încît $b = ac$. Exprimări echivalente: a este *divizor* (uneori se spune și *factor*) al lui b ; b este *multiplu* al lui a ; b este *divizibil* cu a .

Faptul că $a|b$ în R *depinde în mod esențial de inelul R* . De exemplu, $2|3$ în $\mathbb{Q}$, dar nu și în $\mathbb{Z}$! Notăm $a \nmid b$ dacă a nu îl divide pe b .

O teorie relevantă a divizibilității se poate dezvolta în inele cu proprietăți care le apropie cumva de $\mathbb{Z}$. Un set minimal de astfel de proprietăți este: inelul să fie *unitar, comutativ și fără divizori ai lui zero* (adică $\forall a, b \in R$, din $ab = 0$ rezultă $a = 0$ sau $b = 0$). Un astfel de inel (notat în continuare cu R) se numește *inel integru* sau *domeniu de integritate*, denumire care provine chiar din faptul că proprietățile sale sînt oarecum apropiate de cele din inelul $\mathbb{Z}$ al

întregilor. În această secțiune, toate inelele vor fi integrale, toate corpurile ce intervin vor fi presupuse comutative, iar subinelele care apar vor conține elementul unitate al inelului (subinele unitare). Vom nota cu R^* mulțimea $R \setminus \{0\}$.

1.2 Exemple. Orice corp este inel integru. Teoria divizibilității într-un corp K este trivială: $\forall a, b \in K$, are loc $a|b$ (cu excepția cazului cînd $a = 0$ și $b \neq 0$). Orice subinel al unui inel integru este la rîndul său integru. În particular, orice subinel al unui corp este integru. Dacă R este inel integru, atunci inelul de polinoame cu coeficienți în R , $R[X]$, este integru.

În inele integrale se pot simplifica factorii nenuli:

1.3 Propoziție. Fie R un inel integru și $a, b, c \in R$, cu $c \neq 0$. Dacă $ac = bc$, atunci $a = b$.

Demonstrație. Avem $ac = bc \Leftrightarrow ac - bc = 0 \Leftrightarrow (a - b)c = 0$. Nu putem avea $a - b \neq 0$, căci atunci $(a - b)c \neq 0$ din integritatea lui R . Deci $a - b = 0$. $\square$

Proprietățile generale ale relației de divizibilitate sînt binecunoscute (demonstrați-le!):

1.4 Propoziție. Fie R un inel integru. Atunci:

- a) Pentru orice $a \in R$ are loc $a|a$.
- b) Pentru orice $a, b, c \in R$ astfel încît $a|b$ și $b|c$, rezultă $a|c$.
- c) Pentru orice $a \in R$, are loc $a|0$ și $1|a$.
- d) Oricare ar fi $x, y \in R$ și $a, b, c \in R$ astfel încît $a|b$ și $a|c$, rezultă $a|(bx + cy)$. $\square$

Relația de divizibilitate este așadar o relație *reflexivă* și *tranzitivă*, adică o relație de *preordine* pe R . Relația de echivalență asociată acestei preordini se numește relația de *asociere în divizibilitate*:

1.5 Definiție. Spunem că elementele a și b din R sînt *asociate în divizibilitate* (pe scurt, *asociate*) dacă $a|b$ și $b|a$. Notăție: $a \sim b$. Dacă $d, a \in R$, spunem că d este *divizor propriu al lui* a (sau *divide propriu pe* a) dacă $d|a$ și d nu este nici inversabil, nici asociat cu a .

Relația " $\sim$ " definită mai sus este o relație de echivalență pe inelul R și este deosebit de importantă în studiul aritmeticii lui R : *două elemente asociate în divizibilitate au aceleași proprietăți din punct de vedere al divizibilității* (au aceiași divizori și aceiași multipli). Mulțimea elementelor asociate cu 1, adică

$$U(R) = \{x \in R \mid \exists y \in R \text{ astfel încît } xy = yx = 1\},$$

are un statut special: se numește *grupul unităților* lui R , deoarece este grup față de înmulțirea inelului (chiar dacă R nu este comutativ).

1.6 Propoziție. Fie R un inel integru. Atunci:

- a) Pentru orice $u \in R$, avem: $u \in U(R) \Leftrightarrow u \sim 1 \Leftrightarrow u|a, \forall a \in R \Leftrightarrow uR = R$.
- b) Pentru orice $a, b \in R$, avem: $a \sim b \Leftrightarrow$ există $u \in R$ astfel încît $a = bu$. $\square$

Se justifică denumirea de „unități” dată elementelor inversabile: *unitățile se comportă ca și 1 (unitatea inelului) față de divizibilitate*. De aceea, determinarea grupului unităților este importantă în studiul divizibilității în R .

1.7 Exemple. a) $U(\mathbb{Z}) = \{-1, 1\}$.

b) Dacă K este un corp, $U(K[X]) = \{f \in K[X] \mid \text{grad } f = 0\} = K^*$.

Pe mulțimea claselor de echivalență în raport cu relația „ $\sim$ ” de asociere în divizibilitate, relația de divizibilitate „ $\mid$ ” definește în mod natural o *relație de ordine*. Traducând noțiunile de margine inferioară (respectiv superioară) a unei submulțimi într-o mulțime ordonată, se ajunge la noțiunile clasice de *cel mai mare divizor comun* și *cel mai mic multiplu comun*:

1.8 Definiție. Fie R un inel integru, $n \in \mathbb{N}^*$ și $a_1, \dots, a_n \in R$. Spunem că elementul d din R este un *cel mai mare divizor comun* (pe scurt, *cmmdc*) al elementelor $a_1, \dots, a_n$ dacă:

i) $d \mid a_1, \dots, d \mid a_n$.

ii) Pentru orice $e \in R$ astfel încât $e \mid a_1, \dots, e \mid a_n$, rezultă $e \mid d$.

Spunem că elementul m din R este un *cel mai mic multiplu comun* (pe scurt, *cmmmc*) al elementelor $a_1, \dots, a_n$ dacă satisface condițiile:

i') $a_1 \mid m, \dots, a_n \mid m$.

ii') Pentru orice $e \in R$ astfel încât $a_1 \mid e, \dots, a_n \mid e$, rezultă $m \mid e$.

1.9 Observație. Pentru $a_1, \dots, a_n \in R$, dacă există un *cmmdc* al lor $d \in R$, atunci d este unic determinat pînă la o asociere în divizibilitate: dacă și e este un *cmmdc* al $a_1, \dots, a_n$, atunci $e \sim d$. Aceeași observație se aplică *cmmmc*.

În continuare vom nota cu $(a_1, \dots, a_n)$ sau cu $\text{cmmdc}\{a_1, \dots, a_n\}$ un *cmmdc* al $a_1, \dots, a_n$, în cazul cînd acesta există. Scrierea $d = (a_1, \dots, a_n)$ semnifică faptul că d este **asociat** cu un *cmmdc* al $a_1, \dots, a_n$. De exemplu, în $\mathbb{Z}$, putem scrie $1 = (1, 2)$ și $(1, 2) = -1$, dar aceasta nu înseamnă că $1 = -1$ (ci $1 \sim -1$). Spunem că $a_1, \dots, a_n$ sînt *relativ prime* (*prime între ele*) dacă și numai dacă $(a_1, \dots, a_n) = 1 \Leftrightarrow$ orice divizor comun al lor este o unitate în R .

Notăm cu $[a_1, \dots, a_n]$ sau cu $\text{cmmmc}\{a_1, \dots, a_n\}$ un *cmmmc* al $a_1, \dots, a_n$, dacă există.

1.10 Observație. $\forall a \in R, \exists (a, 0) = a$ și $\exists [a, 0] = 0$.

Pentru un inel integru oarecare R și $x, y \in R$, nu este garantată existența unui *cmmdc* al lor. Un inel integru R cu proprietatea că, pentru orice două elemente $x, y \in R$, există un *cmmdc* al lor, se numește *GCD-inel* (*Greatest Common Divisor* înseamnă *cel mai mare divizor comun*).

Iată cîteva proprietăți elementare generale ale *cmmdc* și *cmmmc*:

1.11 Propoziție. Fie R un domeniu de integritate și $a_1, \dots, a_n, r \in R \setminus \{0\}$.

a) Dacă există $d = (a_1, \dots, a_n)$, atunci $a_1/d, \dots, a_n/d$ au cmmdc, egal cu 1.⁶⁶

b) Dacă există $(a_1, \dots, a_n) =: d$ și există $(ra_1, \dots, ra_n) =: e$, atunci $e = rd$, adică:

$$(ra_1, \dots, ra_n) = r(a_1, \dots, a_n).$$

c) Dacă există $[a_1, \dots, a_n] = m$ și există $[ra_1, \dots, ra_n] =: \mu$, atunci $\mu = rm$, adică:

$$[ra_1, \dots, ra_n] = r[a_1, \dots, a_n].$$

Demonstrație. a) Fie $x_i \in R$ astfel încât $a_i = dx_i$, pentru $1 \leq i \leq n$. Evident, 1 este un divizor comun al elementelor $x_1, \dots, x_n$. Dacă $e \in R$ este un alt divizor comun al lor, atunci de este un divizor comun al $a_1, \dots, a_n$, deci $de|d$. De aici rezultă că $e|1$.

b) Din $rd|ra_i$, pentru $\forall i$, rezultă că $rd|e$. Fie $u \in R$ cu $e = rdu$. Arătăm că $u|1$. Fie $x_i, y_i \in R$ astfel încât $a_i = dx_i$ și $ra_i = ey_i$, pentru $1 \leq i \leq n$. Avem, pentru orice i : $ra_i = rdx_i = rduy_i$. De aici rezultă că u este divizor comun al elementelor x_i , care au cmmdc 1, conform punctului a). $\square$

Rezultatul următor este fundamental în argumentele legate de divizibilitate.

1.12 Corolar. Fie R un inel integru în care orice două elemente au cmmdc (GCD-inel) și $a, b, c \in R$ cu proprietatea că $a|bc$ și a este prim cu b . Atunci $a|c$.

Demonstrație. Din $(a, b) = 1$ și din propoziția precedentă, punctul b), rezultă că $(ac, bc) = c$. Cum $a|ac$ și $a|bc$, din definiția cmmdc obținem $a|(ac, bc) = c$. $\square$

1.13 Propoziție. Fie R un inel integru astfel încât orice două elemente din R au un cmmdc. Atunci, $\forall a, b \in R$, există și cmmmc al lor $[a, b]$ și avem $ab = (a, b) \cdot [a, b]$. Mai mult, pentru orice $n \in \mathbb{N}^*$, orice n elemente $a_1, \dots, a_n$ din R au cmmdc și cmmmc.

Demonstrație. Fie $a, b \in R$ cu $a, b \neq 0$ și fie $d = (a, b)$. Există $x, y \in R$ cu $a = dx$, $b = dy$. Elementul $m = dxy$ este un multiplu comun al elementelor a și b . Fie μ un alt multiplu comun al elementelor a și b . Există $z, t \in R$ astfel încât $\mu = az = dxz$ și $\mu = bt = dyt$. Deci m divide elementele $\mu y = dxyz$ și $\mu x = dxyt$. Știm că există $(\mu x, \mu y)$, deci m divide și pe $(\mu x, \mu y) = \mu(x, y) = \mu$. Aceasta arată că m este un cmmmc al elementelor a și b și că $ab = dm$.

Partea a doua se demonstrează prin inducție după n . (Exercițiu!). $\square$

Pentru scurtarea exprimării, dacă R este inel integru, notăm

$$R^\circ := \{x \in R \mid x \text{ este nenul și nu este inversabil}\} = R^* \setminus U(R).$$

Un rol important în divizibilitatea în $\mathbb{Z}$ îl au numerele *prime*. Definiția elementară uzuală care se dă noțiunii de număr natural prim este „numărul $p > 1$ este prim dacă singurii săi divizori naturali sînt 1 și p ”. Aceasta este de fapt noțiunea de element *irreductibil* (se va vedea legătura cu noțiunea de element *prim* definită mai jos).

⁶⁶ Dacă $d \neq 0$ și $d|a$, am notat cu a/d unicul element x din R cu proprietatea că $a = dx$.

1.14 Definiție. Fie R un inel integru și $p \in R$.

a) Spunem că p este *ireductibil* (în R) dacă $p \in R^\circ$ și p nu are divizori proprii: $\forall d \in R$, $d \mid p \Rightarrow d \sim 1$ sau $d \sim p$.

b) Spunem că p este *prim* (în R) dacă $p \in R^\circ$ și oricare ar fi $a, b \in R$ astfel încât $p \mid ab$, rezultă $p \mid a$ sau $p \mid b$.

Subliniem că *un element prim sau ireductibil este prin definiție nenul și neinvertibil*. Se demonstrează imediat că *dacă p este prim și p divide un produs de m elemente din R , atunci p divide unul din factori*.

1.15 Propoziție. Fie R un inel integru. Atunci orice element prim este ireductibil. □

Noțiunile de element prim și element ireductibil (care sînt echivalente pentru $\mathbb{Z}$, după cum se va vedea) nu coincid în general, dar coincid pentru GCD-inele:

1.16 Propoziție. Fie R un GCD-inel. Atunci orice element ireductibil în R este prim în R .

Demonstrație. Fie $p \in R$, ireductibil și $x, y \in R$ astfel încât $p \mid xy$. Dacă $p \nmid x$, atunci $\exists (p, x) = 1$. Într-adevăr, dacă $d \mid x$ și $d \mid p$, atunci este imposibil ca $d \sim p$ (ar rezulta $p \mid x$), deci $d \sim 1$. Astfel, $p \mid xy$ și p este prim cu x . Corolarul 1.12 asigură că $p \mid y$. □

Noțiunea de divizibilitate poate fi exprimată în termeni de *ideale*:

1.17 Propoziție. Fie R un inel integru, $n \in \mathbb{N}^*$ și $a, b, x_1, \dots, x_n \in R$. Atunci:

- a) $a \mid b$ dacă și numai dacă $Ra \supseteq Rb$.⁶⁷
- b) $a \sim b$ dacă și numai dacă $Ra = Rb$.
- c) a este invertibil dacă și numai dacă $Ra = R$.
- d) a este prim în R dacă și numai dacă Ra este ideal prim.
- e) a este ireductibil în R dacă și numai dacă Ra este ideal maximal printre idealele principale proprii ale lui R (mai precis: $\forall x \in R$ astfel încât $Ra \subseteq Rx$, rezultă $Ra = Rx$ sau $Rx = R$).

f) a este divizor comun al $x_1, \dots, x_n$ dacă și numai dacă $Rx_1 + \dots + Rx_n \subseteq Ra$.

g) Dacă $Rx_1 + \dots + Rx_n = Ra$, atunci $a = (x_1, \dots, x_n)$.⁶⁸

h) a este multiplu comun al $x_1, \dots, x_n$ dacă și numai dacă $Rx_1 \cap \dots \cap Rx_n \supseteq Ra$.

i) $a = [x_1, \dots, x_n]$ dacă și numai dacă $Rx_1 \cap \dots \cap Rx_n = Ra$.

Demonstrație. a) $a \mid b \Leftrightarrow$ există $c \in R$ cu $b = ca \Leftrightarrow b \in Ra \Leftrightarrow Rb \subseteq Ra$.

e) Presupunem că a este ireductibil. Dacă Rx este un ideal principal propriu al lui R astfel încât $Ra \subseteq Rx$, rezultă că $x \mid a$. Cum a nu are divizori proprii, x este asociat cu a sau x este o unitate. Dar x nu poate fi o unitate, căci Rx nu coincide cu inelul R . Astfel $x \sim a$, adică $Rx =$

⁶⁷ Am notat cu Ra idealul generat de a : $Ra = \{ra \mid r \in R\} = aR$. O altă notație pentru Ra este (a) .

⁶⁸ Reciproca este falsă în general. Pentru un contraexemplu, a se vedea secțiunea „Inele principale”.

Ra. Reciproc, dacă Rx e maximal printre idealele principale proprii, iar $d \in R$ este un divizor al lui a , atunci $Ra \subseteq Rd$, deci $Rd = Ra$ sau $Rd = R$. Aceasta înseamnă că $d \sim a$ sau $d \sim 1$.

g) Din f) rezultă că a este divizor comun al $x_1, \dots, x_n$. Fie $d \in R$ un alt divizor comun al lor. Cum $a \in Rx_1 + \dots + Rx_n$, $\exists c_1, \dots, c_n \in R$ cu $a = c_1x_1 + \dots + c_nx_n$. Din $d|x_1, \dots, d|x_n$ rezultă că $d|a$. $\square$

IV.2 Algoritmul lui Euclid, teorema fundamentală a aritmeticii

Un rol esențial în aritmetica lui $\mathbb{Z}$ îl are *teorema împărțirii cu rest*:

- Pentru orice $a, b \in \mathbb{Z}$, cu $b \neq 0$, există $q, r \in \mathbb{Z}$, astfel încât $a = bq + r$ și $|r| < |b|$ sau $r = 0$.

Această teoremă are drept consecință încă două teoreme fundamentale în $\mathbb{Z}$:

- Orice ideal al lui $\mathbb{Z}$ este principal (adică de forma $n\mathbb{Z}$, cu $n \in \mathbb{Z}$).

- Orice număr întreg nenul și neinvertibil se poate scrie în mod unic ca un produs finit de numere întregi prime (unicitatea fiind înțeleasă pînă la ordinea factorilor și la o asociere a lor în divizibilitate). („Teorema fundamentală a aritmeticii” sau „Teorema de descompunere unică în factori primi”)

Prin abstractizare, se obțin noțiunile generale de *inel euclidian* (inel în care are loc o teoremă de împărțire cu rest), *inel principal* (în care orice ideal e principal) și, respectiv, de *inel factorial* (în care este valabilă o teoremă de descompunere unică în factori primi).

2.1 Definiție. Un inel integru R se numește *inel euclidian* dacă există o funcție $\varphi: R^* \rightarrow \mathbb{N}$ astfel încât: pentru orice $a, b \in R$ cu $b \neq 0$, există $q, r \in R$ cu proprietățile:

$$a = bq + r \text{ și } (r = 0 \text{ sau } \varphi(r) < \varphi(b)).$$

Vom spune în acest caz că R este inel euclidian față de funcția φ .

Proprietatea din definiție este cunoscută sub numele de „teorema împărțirii cu rest în R ”; q este numit *cît*, iar r *rest* al împărțirii lui a prin b . Definiția de mai sus e inspirată din teoremele corespunzătoare din inelul $\mathbb{Z}$ (unde rolul funcției φ este jucat de valoarea absolută pe $\mathbb{Z}$), respectiv din inelele $K[X]$ cu K corp, unde φ este funcția grad. Aceste inele constituie și cele mai importante exemple de inele euclidiene.

2.2 Teoremă (Algoritmul lui Euclid). Fie R un inel euclidian și $a, b \in R$, cu $b \neq 0$. Atunci există un cmmdc d al elementelor a și b . În plus, există (și se pot determina algoritmic) $u, v \in R$ astfel încât $d = au + bv$.

Demonstrație. Fie următorul șir de împărțiri cu rest în R ("Algoritmul lui Euclid"):

$$(1) \quad a = bq_1 + r_1 \quad \text{cu } r_1 = 0 \text{ sau } \varphi(r_1) < \varphi(b);$$

$$(2) \quad b = r_1q_2 + r_2 \quad \text{cu } r_2 = 0 \text{ sau } \varphi(r_2) < \varphi(r_1);$$

$$\begin{aligned}
(3) \quad & r_1 = r_2 q_3 + r_3 && \text{cu } r_3 = 0 \text{ sau } \varphi(r_3) < \varphi(r_2); \\
& \dots \\
(n-2) \quad & r_{n-4} = r_{n-3} q_{n-2} + r_{n-2} && \text{cu } r_{n-2} = 0 \text{ sau } \varphi(r_{n-2}) < \varphi(r_{n-3}); \\
(n-1) \quad & r_{n-3} = r_{n-2} q_{n-1} + r_{n-1} && \text{cu } r_{n-1} = 0 \text{ sau } \varphi(r_{n-1}) < \varphi(r_{n-2}); \\
(n) \quad & r_{n-2} = r_{n-1} q_n + r_n && \text{cu } r_n = 0.
\end{aligned}$$

Existența elementelor $q_i, r_i \in R$ cu proprietățile specificate este asigurată la fiecare pas de definiția inelului euclidian. Întrucît șirul de numere naturale $\varphi(b), \varphi(r_1), \varphi(r_2), \dots$ este strict descrescător, există $n \in \mathbb{N}^*$ cu $r_n = 0$ (algoritmul se termină după un număr finit de pași). Afirmăm că r_{n-1} („ultimul rest nenul”) este cmmdc al lui a și b .

Din relația (n) avem $r_{n-1} | r_{n-2}$. Relația (n-1) arată că $r_{n-1} | r_{n-3}$. Folosind în continuare egalitățile (n-2), ..., (3), (2), (1), obținem (prin inducție⁶⁹) că $r_{n-1} | b$ și $r_{n-1} | a$. Fie acum $e \in R$ un divizor comun al elementelor a și b ; atunci e va divide și pe $r_1 = a - bq_1$. Din relația (2), obținem că $e | r_2 = b - r_1 q_2$. Procedînd inductiv, rezultă că $e | r_i$ pentru orice $i < n$, deci $e | r_{n-1}$.

Pentru a obține scrierea lui $d = r_{n-1}$ sub forma $au + bv$, observăm că $r_1 = a - bq_1$; înlocuind r_1 în (2), obținem scrierea lui r_2 sub forma $au' + bv'$ ș.a.m.d. Următorul algoritm (numit *algoritmul extins al lui Euclid*) realizează acest lucru (la fiecare pas variabilele u și v sînt astfel încît ultimul rest găsit este $au + bv$):

Se dau : $a, b \in R$. **Se obțin** : $d = (a, b) \in R$ și $u, v \in R$ astfel încît $d = au + bv$.

Începe

Dacă $b = 0$, atunci $d := a$; $u := 1, v := 0$; **Stop**.

Altfel $u1 := 1; v1 := 0; u := 0; v := 1$;

Pas 1. Găsește $q, r \in R$ cu $a = bq + r$ și $r = 0$ sau $\varphi(r) < \varphi(b)$;

Dacă $r = 0$, atunci pune $d := b$; **Stop**.

Altfel $a := b; b := r; u1 := u1 - q \cdot u; v1 := v1 - q \cdot v$;

$t := u; u := u1; u1 := t;$ „aici se schimbă între ele cuplurile (u, v) și

$t := v; v := v1; v1 := t;$ ($u1, v1$)”

Mergi la *Pas 1*.

Sfîrșit

□

2.3 Exemple. a) $\mathbb{Z}$ este inel euclidian față de funcția „valoarea absolută”. Cîtuș și restul unei împărțiri cu rest nu sînt unic determinate: de exemplu, $3 = 2 \cdot 1 + 1 = 2 \cdot 2 + (-1)$.

b) Fie K un corp. Inelul $K[X]$ este euclidian față de funcția $\text{grad} : K[X] \setminus \{0\} \rightarrow \mathbb{N}$, conform teoremei **III.2.1**. $\mathbb{Z}$ și $K[X]$ sînt cele mai importante exemple de inele euclidiene.

2.4 Definiție. Un inel integru R se numește *inel principal* dacă orice ideal al inelului R este principal. Cu alte cuvinte, oricare ar fi idealul I al lui R , există $a \in R$ astfel încît $I = Ra$.

⁶⁹ Detaliați raționamentul prin inducție!

Orice corp K este inel principal (singurele sale ideale sînt 0 și K). Exemple importante de inele principale sînt furnizate de următoarea propoziție.

2.5 Teoremă. *Orice inel euclidian este inel principal.*

Demonstrație. Fie R un inel euclidian față de funcția φ și I un ideal nenul al lui R . Fie $\{\varphi(x) \mid x \in I, x \neq 0\}$, submulțime nevidă a lui $\mathbb{N}$. Această submulțime are cel mai mic element, fie acesta $\varphi(a)$, cu $a \in I$, $a \neq 0$ (a poate să nu fie unic determinat). Demonstrăm că $I = Ra$. Evident, $Ra \subseteq I$. Pentru incluziunea inversă, presupunem că există un element $b \in I \setminus Ra$. Din teorema împărțirii cu rest, există $q, r \in R$ cu proprietatea că $b = aq + r$, $r \neq 0$ (căci $b \notin Ra$) și $\varphi(r) < \varphi(a)$. Cum $a, b \in I$, rezultă că $r \in I$. Însă $\varphi(r) < \varphi(a)$ contrazice alegerea lui a . $\square$

Astfel, dacă K este corp, inelul $K[X]$ este principal; dat un ideal $I \neq 0$ în $K[X]$, un generator al lui I este un polinom $g \in I$ de grad minim printre gradele polinoamelor nenule din I .

Există inele principale care nu sînt euclidiene, dar nu sînt ușor de construit. Un astfel de inel este $\mathbb{Z}\left[\frac{1+i\sqrt{19}}{2}\right]$ (vezi ALBU și ION [1984]).

Inelele principale sînt GCD-inele; oricare ar fi $a, b \in R$, există un cmmdc al lor, anume orice generator al idealului $aR + bR$:

2.6 Propoziție. *Fie R un inel principal și $a, b \in R$. Atunci:*

a) *Elementul $d \in R$ este un cmmdc al a și b dacă și numai dacă $dR = aR + bR$. În particular, există un cmmdc d al lui a și b și există $u, v \in R$ astfel încît $d = au + bv$.*

b) *Elementul $d \in R$ este un cmmmc al a și b dacă și numai dacă $dR = aR \cap bR$.*

Demonstrație. a) R fiind inel principal, există un generator d al idealului $aR + bR = \{ax + by \mid x, y \in R\}$. Atunci $a, b \in dR$, deci $d|a$, $d|b$. Dacă $e \in R$ astfel încît $e|a$, $e|b$, atunci $e|ax + by$, $\forall x, y \in R$. În particular, $e|d$. Astfel, d este un cmmdc al a și b . Reciproc, dacă d este un cmmdc al a și b , rezultă că $d|a$ și $d|b$, deci $dR \supseteq aR$ și $dR \supseteq bR$, adică $dR \supseteq aR + bR$. Fie e un generator al idealului $aR + bR$. Cum $e|a$, $e|b$, rezultă că $e|d$, adică $d \in eR = aR + bR$. $\square$

Propoziția de mai sus justifică notația (a, b) , folosită atît pentru cmmdc al elementelor a și b , cît și pentru idealul generat de a și b , $aR + bR$.

2.7 Exemplu. Fie R un inel integru care nu e corp și $r \in R$, nenul, neinvertibil. Atunci idealul (r, X) al inelului $R[X]$ nu este principal, deci *inelul $R[X]$ nu este principal*. Într-adevăr, presupunem că există $f \in R[X]$ cu $(^{\circ}f) = (r, X)$. Atunci rezultă că $f|r$. Trecînd la grade, obținem că $\text{grad } f = 0$, adică $f \in R$. Din $f|X$, adică $\exists g \in R[X]$ cu $X = fg$, avem că f este invertibil în R . Deci cmmdc al lui r și X este 1. Dar idealul generat de r și X nu conține pe 1, căci altfel ar exista $h, q \in R[X]$ astfel încît $1 = hr + qX$. Punînd $X = 0$ în această egalitate de polinoame, rezultă $1 = h(0) \cdot r$, adică r este invertibil, contradicție.

În particular, inelele $\mathbb{Z}[X]$, $K[X, Y]$ cu K corp *nu sînt principale*. Deci, proprietatea „dacă $a, b \in R$ și există $d = (a, b)$, atunci $\exists u, v \in R$ astfel încît $d = au + bv$ ” este falsă în inele care nu

sînt principale. De exemplu, în $K[X, Y]$, avem $(X, Y) = 1$, dar 1 nu se poate scrie ca $X \cdot u + Y \cdot v$, cu $u, v \in K[X, Y]$.

Din Propoziția 1.16 și din faptul că inelele principale sînt GCD-inele, rezultă:

2.8 Propoziție. *Într-un inel principal, noțiunile de element ireductibil și element prim coincid.* $\square$

2.9 Corolar. *Într-un inel principal R , idealele prime nenule sînt ideale maximale. Orice ideal maximal este de forma pR , unde p este ireductibil în R . Un element $p \in R$ este ireductibil dacă și numai dacă pR este ideal maximal.*

Demonstrație. Este suficient să observăm că orice ideal prim nenul este principal, generat cu necesitate de un element prim p (Propoziția 1.17.d)). Elementul p este ireductibil, deci (Propoziția 1.17.e)) idealul pR este maximal. Celelalte afirmații sînt evidente, ținînd cont de propoziția citată și de faptul că R este principal. $\square$

Cazul particular $R = \mathbb{Z}$ al Propoziției următoare este cunoscut sub numele de „Teorema fundamentală a aritmeticii”. Reamintim că $R^\circ = \{x \in R \mid x \text{ este nenul și nu este inversabil}\}$.

2.10 Teoremă. *Fie R un inel principal. Atunci orice element nenul și neinvertibil din R se poate scrie ca un produs finit de elemente prime.*

Demonstrație. Presupunem că există $r_0 \in R^\circ$ astfel încît r nu se poate scrie ca un produs finit de elemente prime (sau, echivalent, ireductibile, căci R este principal). În particular, r_0 nu este ireductibil, deci $r_0 = r_1 s_1$, cu $r_1, s_1 \in R^\circ$, neasociate cu r_0 . Dacă r_1 și s_1 sînt produse finite de ireductibile, atunci r_0 este produs de ireductibile, fals. Deci măcar unul dintre ele (fie acesta r_1) nu se scrie ca produs de elemente ireductibile. Înlocuind în raționamentul de mai sus pe r_0 cu r_1 , rezultă că există $r_2 \in R^\circ$, $r_2 \mid r_1$, $r_2 \sim r_1$. Procedînd recursiv, rezultă existența unui șir $(r_n)_{n \geq 0}$ de elemente din R , astfel încît pentru orice $n \in \mathbb{N}$, r_{n+1} este un divizor propriu al lui r_n . Altfel spus, am obținut un șir infinit strict crescător de ideale $r_0 R \subset r_1 R \subset \dots \subset r_n R \subset \dots$. Dar acest lucru este imposibil într-un inel principal, după cum arată lema următoare.

2.11 Lemă. *Fie R un inel principal și $(r_n)_{n \geq 0}$ un șir de elemente din R astfel încît $r_n R \subseteq r_{n+1} R$, pentru orice $n \in \mathbb{N}$. Atunci există $m \in \mathbb{N}$ astfel încît $r_m R = r_{m+i} R$, pentru orice $i \in \mathbb{N}$. (Orice șir ascendent de ideale este staționar).*

Demonstrație. Fie I reuniunea idealelor $r_n R$, $n \in \mathbb{N}$. Se arată imediat că I este ideal în R . Cum R este principal, există $a \in R$ astfel încît $I = aR$. Întrucît $a \in I$, există $m \in \mathbb{N}$ astfel încît $a \in r_m R$, adică $aR = r_m R$. Deci $r_m R = aR = I = r_{m+i} R$, $\forall i \in \mathbb{N}$. $\square$

2.12 Definiție. Un inel integrăru R cu proprietatea că orice element nenul și neinvertibil se scrie ca un produs finit⁷⁰ de elemente prime se numește *inel factorial* sau *inel cu descompunere unică în factori (primi)*. În literatura anglo-saxonă, astfel de inele sînt numite *Unique Factorization Domains (UFD)*.

Din teorema 2.10 rezultă că inelele principale (deci și cele euclidiene) sînt factoriale. Orice corp este inel factorial, căci nu are elemente nenule și neinvertibile.

2.13 Propoziție. Într-un inel factorial R orice element ireductibil este prim.

Demonstrație. Fie p ireductibil. Cum $p \in R^\circ$, p este un produs de elemente prime. Acest produs nu poate avea decît un factor, altfel elementul p ar admite divizori proprii. Cu alte cuvinte, p este el însuși prim. $\square$

Propoziția următoare justifică și precizează denumirea de *inele cu descompunere unică în factori* primi, care se mai dă inelelor factoriale.

2.14 Propoziție. Fie R un inel integrăru și $r \in R^\circ$. Dacă r admite o descompunere în factori primi, atunci această descompunere este unic determinată pînă la o ordine a factorilor și pînă la o asociere a acestora în divizibilitate. Mai precis, dacă $r = p_1 \dots p_n = q_1 \dots q_m$ sînt două scrieri ale lui r ca produse de elemente prime, atunci $m = n$ și există o permutare σ a mulțimii $\{1, \dots, n\}$ astfel încît p_i să fie asociat în divizibilitate cu $q_{\sigma(i)}$, $\forall i \in \{1, \dots, n\}$.

Demonstrație. Demonstrăm afirmația propoziției prin inducție după n .

Dacă $n = 1$, atunci $r = p_1 = q_1 \dots q_m$, cu $p_1, q_1, \dots, q_m$ prime. Deci r este prim și divide $q_1 \dots q_m$; rezultă că r divide unul din factori, fie acesta (după o eventuală renumerotare) q_1 . Întrucît q_1 este ireductibil, rezultă că $r \sim q_1$, adică $r = q_1 u$, cu u invertibil. Dacă $m \geq 2$, din egalitatea $q_1 u = q_1 q_2 \dots q_m$, obținem $q_2 \dots q_m = u$, adică $q_2, \dots, q_m$ sînt invertibile, contradicție. Deci $m = 1$.

Fie $n > 1$ și presupunem că afirmația este adevărată pentru orice $x \in R^\circ$ care admite o descompunere în factori primi cu mai puțin de n factori. Fie $r \in R$ cu $r = p_1 \dots p_n = q_1 \dots q_m$, cu $p_1, \dots, p_n, q_1, \dots, q_m$ prime. Din faptul că p_n este prim, rezultă că există $i \in \{1, \dots, n\}$ astfel încît $p_n | q_i$. Cum q_i este ireductibil, rezultă că $p_n \sim q_i$, adică $\nu p_n = q_i$, cu ν invertibil. Simplificînd prin p_n , obținem $p_1 \dots p_{n-1} = \nu q_1 \dots q_{i-1} q_{i+1} \dots q_m$. Putem acum aplica ipoteza de inducție pentru produsul $p_1 \dots p_{n-1}$ și se obține că $n - 1 = m - 1$ și $p_1, \dots, p_{n-1}$ sînt asociate cu $q_1, \dots, q_{i-1}, q_{i+1}, \dots, q_m$, eventual în altă ordine. $\square$

2.15 Teoremă. Fie R un inel integrăru. Următoarele afirmații sînt echivalente:

a) R este inel factorial.

⁷⁰ Un astfel de produs se mai numește *descompunere în factori* a elementului respectiv. Produsele pot avea și un singur factor (adică elementul însuși este prim).

b) Orice element din R° este un produs de elemente ireductibile și orice element ireductibil este prim.

c) Orice element din R° are o descompunere în factori ireductibili, unică până la ordinea factorilor și până la o asociere în divizibilitate a acestora.

d) Orice element din R° are o descompunere în factori ireductibili și orice două elemente au un cmmdc.

Demonstrație. $a) \Rightarrow b)$ Evident, din Propoziția 2.13.

$b) \Rightarrow c)$ Rezultă din Propoziția 2.14.

$c) \Rightarrow d)$ Fie $a, b \in R^\circ$ (dacă a, b sînt nule sau inversabile, există evident un cmmdc al lor). Pentru a găsi un cmmdc al elementelor a și b , se folosește procedeul de determinare a cmmdc învățat în gimnaziu : „se iau factorii primi comuni la puterea cea mai mică”. Trebuie însă puțină atenție la asocierea în divizibilitate. Fie P un sistem de reprezentanți ai claselor de echivalență ale elementelor ireductibile din R (în raport cu relația de asociere în divizibilitate). Aceasta înseamnă că orice element ireductibil din R este asociat cu exact un element din P . Atunci există și sînt unic determinate $p_1, \dots, p_n \in P$, distincte, $s_1, \dots, s_n, t_1, \dots, t_n \in \mathbb{N}$, $u, v \in U(R)$ astfel încît $a = p_1^{s_1} \dots p_n^{s_n} u$ și $b = p_1^{t_1} \dots p_n^{t_n} v$. Faptul că aceste elemente sînt unic determinate rezultă imediat din unicitatea descompunerilor în R . Fie $r_i = \min(s_i, t_i)$ și definim $d = p_1^{r_1} \dots p_n^{r_n}$. Se observă că $d|a$, $d|b$. Dacă $e|a$, $e|b$, atunci orice factor ireductibil $c \in P$ care îl divide pe e divide pe a și pe b . Aceasta implică $c \in \{p_1, \dots, p_n\}$, căci altfel a (sau b) ar avea două descompuneri în factori ireductibili, dintre care una îl conține pe c , iar cealaltă nu, ceea ce contrazice unicitatea descompunerilor. Deci e este de forma $p_1^{w_1} \dots p_n^{w_n} q$, cu $w_1, \dots, w_n \in \mathbb{N}$, $q \in U(R)$. Din $e|a$ rezultă că $w_i \leq s_i$, iar din $e|b$ rezultă că $w_i \leq t_i$, $i = \overline{1, n}$. Deci $w_i \leq r_i$ și $e|d$.

$d) \Rightarrow a)$ Prop. 1.16 asigură că orice element ireductibil este prim, căci R este GCD-inel. Implicația e acum evidentă. $\square$

Într-un inel factorial R orice două elemente a și b au un cmmmc, produsul „factorilor primi comuni și necomuni la puterea cea mai mare”. Cu notațiile din demonstrație, se definește $q_i = \max(s_i, t_i)$, iar elementul $m = p_1^{q_1} \dots p_n^{q_n}$ este un cmmmc al lui a și b . Demonstrați!

Proprietatea următoare apare adesea în raționamentele privind divizibilitatea:

2.16 Propoziție. Fie R un inel factorial, $n \in \mathbb{N}^*$ și $a, b_1, \dots, b_n \in R$. Dacă a este prim cu orice b_i , $1 \leq i \leq n$, atunci a este prim cu produsul $b_1 \dots b_n$.

Demonstrație. Vom arăta că nu există nici un element prim p care să dividă atît pe a cît și produsul $b_1 \dots b_n$. Dacă p este un astfel de element, atunci există j , $1 \leq j \leq n$ astfel încît $p|b_j$. Cum $p|a$, rezultă că $p|(a, b_j) = 1$. Deci p este inversabil, contradicție. $\square$

Vom demonstra următorul rezultat important privitor la inelele de polinoame:

2.17 Teoremă. Dacă R este inel factorial, atunci inelul de polinoame $R[X]$ este inel factorial.

Pentru demonstrație sînt necesare cîteva noțiuni și rezultate, care au și un interes de sine stătător.

2.18 Definiție. Fie R un inel factorial și $f = a_0 + a_1X + \dots + a_nX^n \in R[X]$. Cmmdc al coeficienților $a_0, a_1, \dots, a_n$ este numit *conținutul* polinomului f , notat $c(f)$. Un polinom cu conținutul asociat cu 1 se numește polinom *primitiv*.

Polinomul f este primitiv dacă și numai dacă nu există p prim în R astfel încît p să dividă toți coeficienții lui f . Orice polinom $f \in R[X]$ se poate scrie sub forma $f = c(f) \cdot f'$, unde f' este polinom primitiv. Reciproc, dacă $f = a \cdot f'$, cu $a \in R$ și f' primitiv, atunci $a = c(f)$.

2.19 Propoziție. a) Fie R un inel integru. Dacă p este un element prim în R , atunci p este prim și în $R[X]$.

b) (Lema lui Gauss) Fie R un inel factorial și $f, g \in R[X]$ două polinoame primitive. Atunci și produsul fg este polinom primitiv.

c) Fie R un inel factorial și $f, g \in R[X]$. Atunci $c(fg) = c(f) \cdot c(g)$.

Demonstrație. a) Remarcăm mai întîi că p divide un polinom în $R[X]$ dacă și numai dacă p divide toți coeficienții polinomului. Fie $f = a_0 + a_1X + \dots + a_nX^n$, $g = b_0 + b_1X + \dots + b_mX^m \in R[X]$ astfel încît $p \nmid f$ și $p \nmid g$. Să demonstrăm că $p \nmid fg$. Din $p \nmid f$ rezultă că există i , $0 \leq i \leq n$, astfel încît $p \nmid a_i$. Alegem i minim cu această proprietate. La fel, fie j minim astfel încît $p \nmid b_j$. Atunci coeficientul lui X^{i+j} în produsul fg este

$$\sum_{k+l=i+j} a_k b_l$$

În această sumă, $a_i b_j$ nu este divizibil cu p , iar ceilalți termeni sînt divizibili cu p , fiind produse de doi factori dintre care măcar unul este divizibil cu p . Deci coeficientul lui X^{i+j} nu este divizibil cu p și nici polinomul fg nu este.

b) Dacă fg nu ar fi polinom primitiv, atunci ar exista $p \in R$, prim, astfel încît $p \mid fg$. Din punctul precedent obținem că $p \mid f$ sau $p \mid g$, contradicție.

c) Fie $f = c(f) \cdot f'$, $g = c(g) \cdot g'$, unde f' și g' sînt polinoame primitive. Atunci

$$fg = c(f)c(g) \cdot f'g',$$

cu $f'g'$ polinom primitiv din b). Este clar acum că $c(fg) = c(f)c(g)$. □

2.20 Propoziție. Fie R un inel factorial, K corpul său de fracții și $f \in R[X]$, $\text{grad } f \geq 1$. Atunci f este ireductibil în $R[X]$ dacă și numai dacă f este primitiv și este ireductibil în $K[X]$.

Demonstrație. Fie f ireductibil în $R[X]$. Atunci e clar că f este primitiv. Să arătăm că f este ireductibil în $K[X]$. Dacă $f = gh$, cu $g, h \in K[X]$, atunci, înmulțind cu cmmmc al numitorilor coeficienților polinoamelor g și h , obținem o relație de forma $af = g_1h_1$, cu $g_1, h_1 \in R[X]$, $a \in R$. Trecînd la conținutul polinoamelor, avem $a = c(g_1)c(h_1)$, căci $c(f) = 1$. Fie $g_1 = c(g_1) \cdot g_2$, $h_1 = c(h_1) \cdot h_2$, unde g_2, h_2 sînt polinoame primitive. Deci, $af = c(g_1) \cdot c(h_1) \cdot g_2 \cdot h_2$; simplificînd prin a , obținem $f = g_2h_2$. Ireductibilitatea lui f implică $\text{grad } g_2 = 0$ (de exemplu). Cum $\text{grad } g = \text{grad } g_1 = \text{grad } g_2$, rezultă $\text{grad } g = 0$.

Reciproc, dacă $f \in R[X]$ este ireductibil în $K[X]$, nu are divizori proprii (de grad ≥ 1) în $K[X]$; cu atât mai mult nu are divizori de grad ≥ 1 în $R[X]$. Dacă f este și primitiv, nu are nici factori de grad 0 neinvertibili, deci este ireductibil în $R[X]$. $\square$

Propoziția are o importanță practică: studiul ireductibilității unui polinom în $K[X]$ se reduce la ireductibilitatea în $R[X]$, în principiu mai abordabilă.

Demonstrația teoremei 2.17. Arătăm mai întâi că în $R[X]$ orice ireductibil este prim: fie $f \in R[X]$, ireductibil. Dacă $f|gh$, cu $g, h \in R[X]$, din faptul că f este ireductibil în $K[X]$ (deci și prim în $K[X]$) rezultă că $f|g$ sau $f|h$ în $K[X]$. Presupunem că $f|g$ în $K[X]$; există deci $a \in R$, $q \in R[X]$ astfel încât $ag = fq$. Trecând la conținutul polinoamelor, avem $a \cdot c(g) = c(q)$. Scriind că $q = c(q) \cdot q'$, $g = c(g) \cdot g'$, cu q', g' primitive în $R[X]$, obținem $ac(g) \cdot g' = f \cdot c(q) \cdot q'$; simplificând prin $c(q) = ac(g)$, rezultă $g' = fq'$, adică $f|g$ în $R[X]$.

Rămîne de arătat că orice f nenul și neinvertibil din $R[X]$ este un produs de ireductibile. Vom demonstra aceasta prin inducție după grad f . Dacă $\text{grad } f = 0$, atunci $f \in R^\circ$ și deci are o descompunere în factori ireductibili în R , care rămîn ireductibili în $R[X]$. Dacă $\text{grad } f > 0$, fie $f = c(f)f'$, cu f' primitiv; este suficient să găsim o descompunere pentru f' . Dacă f' este ireductibil, am terminat; dacă nu, f' are un divizor propriu în $R[X]$, care este un polinom de grad strict mai mic decât $\text{grad } f$ (f' nu are divizori proprii în R , căci este primitiv). În concluzie, $f' = gh$, cu $g, h \in R[X]$, de grade strict mai mici decât $\text{grad } f$. Aplicînd ipoteza de inducție pentru g și h , rezultă că f' este un produs de factori ireductibili în $R[X]$. $\square$

Deci inelele $\mathbb{Z}[X]$, $\mathbb{Z}[X_1, \dots, X_n]$, $K[X_1, \dots, X_n]$ cu K corp sînt inele factoriale.

IV.3 Ireductibilitate în inele polinomiale

Fiind dat un inel integru (sau un corp) R , problema deciderii ireductibilității unui polinom în inelul de polinoame $R[X]$ nebanală și adesea deosebit de importantă. De aici rezultă utilitatea cunoașterii unui arsenal cît mai bogat de criterii de ireductibilitate. Mai întîi determinăm toate polinoamele *invertibile* în $R[X]$.

3.1 Propoziție. Fie R un inel integru. Atunci $U(R[X]) = U(R)$. În particular, pentru K corp, $U(K[X]) = K^*$. $\square$

3.2 Observație. Dacă R este inel integru și $f \in R[X]$ este un polinom *unitar reductibil*, atunci există o descompunere a lui f de forma $f = gh$, cu $g, h \in R[X]$ *unitare*, de grade > 1 . (demonstrați!). Această observație simplă este utilă în investigarea ireductibilității polinoamelor.

Dacă R este inel care nu e corp, inelul $R[X]$ nu este principal, deci cu atât mai mult nu este euclidian (nu are loc teorema împărțirii cu rest în $R[X]$). Totuși, dacă $f, g \in R[X]$, iar g are coeficientul dominant *inversabil* în R , se poate face „împărțirea cu rest” a lui f la g :

3.3 Propoziție. (teorema împărțirii întregi) *Fie R un inel și $f, g \in R[X]$. Dacă coeficientul dominant al lui g este inversabil în R , atunci există $q, r \in R[X]$ astfel încât $f = gq + r$, cu $r = 0$ sau $\text{grad } r < \text{grad } f$.*

Demonstrație. Se aplică exact aceeași idee ca la demonstrația teoremei împărțirii cu rest în $K[X]$, cu K corp. $\square$

3.4 Corolar (teorema lui Bézout). *Fie R un inel integru, $f \in R[X]$ și $a \in R$. Atunci a este rădăcină a lui f dacă și numai dacă polinomul $X - a$ îl divide pe f în $R[X]$.*

Demonstrație. Există $q, r \in R[X]$ astfel încât $f = (X - a)q + r$, unde $\text{grad } r = 0$ sau $r = 0$. Observăm că $(X - a) \mid f$ dacă și numai dacă $r = 0$. Din egalitatea $f(a) = (a - a)q(a) + r(a) = r$, deducem că $f(a) = 0$ echivalează cu $r = 0$. $\square$

Deci, dacă $\text{grad } f \geq 2$ și f are o rădăcină $a \in R$, atunci f este reductibil în $R[X]$ (fiind divizibil cu $X - a$). Reciproca este falsă: polinomul $(X^2 + 1)^2$ nu are rădăcini în $\mathbb{Q}$, dar este evident reductibil în $\mathbb{Q}[X]$. Are loc o reciprocă „parțială”:

3.5 Propoziție. *Fie K un corp. Atunci un polinom f de grad 2 sau 3 din $K[X]$ este ireductibil dacă și numai dacă nu are rădăcini în K . În particular, dacă R este inel factorial, un polinom primitiv de grad 2 sau 3 din $R[X]$ este ireductibil în $R[X]$ dacă și numai dacă nu are rădăcini în K .*

Demonstrație. Fie $f \in K[X]$, reductibil și de grad 2 sau 3. Din examinarea gradelor într-o descompunere a lui f , rezultă că are un factor de grad 1, care are o rădăcină în K . Restul rezultă din echivalența „ f este ireductibil în $R[X]$ dacă și numai dacă f este primitiv și ireductibil în $K[X]$ ”. $\square$

Criteriul de mai sus trebuie aplicat cu precauție pentru stabilirea ireductibilității polinoamelor cu coeficienți într-un inel integru (mai ales dacă nu e factorial):

3.6 Exemple. a) Polinomul $f = (2X + 1)^2$ este evident reductibil în $\mathbb{Z}[X]$, dar nu are rădăcini în $\mathbb{Z}$. Însă f are rădăcini în corpul de fracții al lui $\mathbb{Z}$, $\mathbb{Q}$.

b) Fie $R = \{a + 2bi \mid a, b \in \mathbb{Z}\}$. Se verifică imediat că R este subinel integru al lui $\mathbb{Z}[i]$. Polinomul $X^2 + 1$ este ireductibil în $R[X]$ (demonstrați!), dar are rădăcinile $i, -i$ în corpul de fracții al lui R , $\mathbb{Q}[i]$. Aceasta arată că existența rădăcinilor unui polinom de grad 2 sau 3 din $R[X]$ în corpul de fracții al lui R nu implică în general reductibilitatea polinomului în $R[X]$.

În cazul corpurilor $\mathbb{C}$ și $\mathbb{R}$, ideile simple de mai sus, cuplate cu Teorema fundamentală a algebrei, furnizează lista *tuturor* polinoamelor ireductibile peste aceste corpuri:

3.7 Propoziție. a) Polinomul $f \in \mathbb{C}[X]$ este ireductibil dacă și numai dacă este polinom de grad I.

b) Polinomul $f \in \mathbb{R}[X]$ este ireductibil dacă și numai dacă: sau este polinom de grad I, sau este de grad II (de forma $aX^2 + bX + c$, cu $a \neq 0$) și discriminantul său $b^2 - 4ac$ este negativ.

Demonstrație. a) Evident, orice polinom de grad I este ireductibil. Reciproc, dacă $f \in \mathbb{C}[X]$ și $\text{grad } f > 1$, atunci f are o rădăcină $z \in \mathbb{C}$ (conform teoremei fundamentale a algebrei), deci f nu poate fi ireductibil.

b) Exercițiu. □

Pentru găsirea rădăcinilor unui polinom este util următorul criteriu (vezi și Exerc. 13).

3.8 Propoziție. Fie R un inel factorial, K corpul său de fracții și $f = a_0 + \dots + a_n X^n \in R[X]$. Dacă $p/q \in K$ este o rădăcină a lui f , cu $p, q \in R$, $(p, q) = 1$, atunci $p|a_0$ și $q|a_n$.

Demonstrație. Scriind că p/q este rădăcină a lui f și înmulțind cu q^n , avem

$$-a_0 q^n = a_1 p q^{n-1} + \dots + a_n p^n,$$

deci $p|a_0 q^n$. Cum $(p, q) = 1$, avem și $(p, q^n) = 1$ (R este factorial) și deci $p|a_0$. Analog se demonstrează că $q|a_n$. □

3.9 Exemplu. Fie $f = X^3 - X + 2 \in \mathbb{Z}[X]$. Dacă $p/q \in \mathbb{Q}$ este rădăcină a lui f , $(p, q) = 1$, atunci $p|2$ și $q|1$. Rădăcinile raționale ale lui f (dacă există) se găsesc așadar printre elementele mulțimii $\{1, -1, 2, -2\}$. Prin testare directă, obținem că nici unul din aceste elemente nu este rădăcină. Deci f nu are rădăcini raționale. Cum f este de grad 3, rezultă că este ireductibil în $\mathbb{Q}[X]$ (și în $\mathbb{Z}[X]$, fiind primitiv).

Fie R un inel. Teorema lui Bézout afirmă că polinomul $f \in R[X]$ are rădăcina $a \in R$ dacă și numai dacă $X - a$ divide f în $R[X]$. Este așadar naturală considerarea următoarei definiții:

3.10 Definiție. Fie R un inel integru, $f \in R[X]$ un polinom nenul, $a \in R$ o rădăcină a lui f și $n \in \mathbb{N}$. Spunem că a este rădăcină multiplă de ordin n a lui f dacă $(X - a)^n | f$ și $(X - a)^{n+1} \nmid f$. Numărul natural n se numește *ordinul de multiplicitate al rădăcinii* a . Dacă $n = 1$, a se numește rădăcină simplă, dacă $n = 2, 3, \dots$, a se numește rădăcină dublă, triplă... . Atunci când se numără rădăcinile unui polinom, se numără fiecare rădăcină de atâtea ori cât este ordinul său de multiplicitate.

3.11 Propoziție. Fie R un inel factorial și $f \in R[X]$ un polinom nenul. Dacă $a_1, \dots, a_n \in R$ sînt rădăcini distincte ale lui f , de ordine de multiplicitate $m_1, \dots, m_n$, atunci f se divide cu $(X - a_1)^{m_1} \dots (X - a_n)^{m_n}$ în $R[X]$.

Demonstrație. Prin inducție după n . Dacă $n = 1$, afirmația rezultă din definiție. Presupunem afirmația adevărată pentru $n - 1$ și fie f ca în enunț. Din ipoteza de inducție, $f = (X - a_1)^{m_1} \dots (X - a_{n-1})^{m_{n-1}} g$, cu $g \in R[X]$. Polinoamele $X - a_i$, cu $1 \leq i \leq n$, sînt

ireductibile și neasociate două câte două; deci $(X - a_1)^{m_1}, \dots, (X - a_n)^{m_n}$ sînt două câte două relativ prime. Din Prop. IV.2.16 rezultă că $(X - a_n)^{m_n}$ este prim cu produsul $(X - a_1)^{m_1} \dots (X - a_{n-1})^{m_{n-1}}$. Dar $(X - a_n)^{m_n}$ divide pe $(X - a_1)^{m_1} \dots (X - a_{n-1})^{m_{n-1}} g$, deci $(X - a_n)^{m_n} \mid g$. $\square$

3.12 Observație. În $\mathbb{C}[X]$, orice polinom se scrie în mod unic sub forma $b(X_1 - a_1)^{m_1} \dots (X_n - a_n)^{m_n}$, unde $a_1, \dots, a_n \in \mathbb{C}$ sînt distincte două câte două (sînt rădăcinile polinomului), iar b este coeficientul său dominant. Acest lucru rezultă din faptul că $\mathbb{C}[X]$ este inel factorial (orice polinom se scrie ca un produs de polinoame ireductibile), ținînd cont de lista polinoamelor ireductibile din $\mathbb{Z}[X]$. Care este forma generală a unei descompunerii în factori ireductibili a unui polinom din $\mathbb{R}[X]$?

3.13 Corolar. Fie R un inel integră și $f \in R[X]$, $\text{grad } f = n$. Atunci f are cel mult n rădăcini în R .

Demonstrație. Fie K corpul de fracții al lui R . Interpretînd f ca polinom în $K[X]$, afirmația decurge din propoziția precedentă. $\square$

Vom da un criteriu pentru a decide dacă un polinom are rădăcini multiple, folosind noțiunea de *derivată formală* a unui polinom.

3.14 Definiție. Fie R un inel comutativ unitar și $f = a_0 + a_1X + \dots + a_nX^n \in R[X]$. Numim *derivată (formală)* a polinomului f polinomul

$$df := a_1 + 2a_2X + \dots + na_nX^{n-1}.$$

Se mai folosește notația $df = f'$ sau $df = f^{(1)}$.

Un calcul direct arată că derivata formală are proprietățile uzuale ale derivatei cunoscute din Analiză:

$$(f + g)' = f' + g', \quad (af)' = af', \quad (fg)' = f'g + fg', \quad \forall a \in R, \forall f, g \in R[X].$$

Compunerea morfismului d cu el însuși de n ori ($n \in \mathbb{N}^*$) se notează d^n ; $d^n : R[X] \rightarrow R[X]$. Avem deci $d^n = d \circ d^{n-1}$, $\forall n \in \mathbb{N}^*$, cu convenția că $d^0 = \text{id}$. Mai notăm $d^n f = f^{(n)}$, $\forall f \in R[X]$.

3.15 Propoziție. Fie R un inel integră, $f \in R[X]$ un polinom de grad $n > 0$ și $\alpha \in R$.

a) Există și sînt unice elementele $b_0, \dots, b_n \in R$ astfel încît $f = \sum_{0 \leq i \leq n} b_i (X - \alpha)^i$.

b) Dacă α este rădăcină multiplă de ordin m ($m \in \mathbb{N}^*$) a polinomului f , atunci $f^{(i)}(\alpha) = 0$, pentru orice $i \in \{0, \dots, m-1\}$.

c) Dacă $f(\alpha) = f'(\alpha) = 0$, atunci α este rădăcină multiplă a lui f (de multiplicitate cel puțin 2).

Demonstrație. a) Prin inducție după grad f . Dacă $f = a_0 + a_1X$, atunci $f = a_0 + a_1(X - \alpha) + a_1(X - \alpha)^2$. Dacă $\text{grad } f = n > 1$, aplicînd teorema împărțirii întregi (IV.3.3), obținem

$f = (X - \alpha)g + b_0$, cu $b_0 \in R$ și $g \in R[X]$, grad $g = n - 1$. Scriind pe g sub forma dată de ipoteza de inducție și înlocuind în relația precedentă, se obține rezultatul.

Unicitatea scrierii este echivalentă cu R -liniara independență a mulțimii de polinoame $\{(X - \alpha)^i \mid i \in \mathbb{N}\}$ în $R[X]$, ușor de demonstrat.

b) Din relația dedusă la punctul a), rezultă că $(X - \alpha)^m \mid f$ dacă și numai dacă $b_0, b_1, \dots, b_{m-1}$ sînt nuli. Pe de altă parte, se demonstrează ușor că $f^{(i)}(\alpha) = i!b_i$, $\forall i \in \{0, \dots, n\}$. De aici rezultă că $f^{(i)}(\alpha) = 0$, $\forall i \in \{0, \dots, m-1\}$.

c) Din cele demonstrate pînă acum, obținem că $f(\alpha) = b_0 = 0$ și $f'(\alpha) = b_1 = 0$. Deci $(X - \alpha)^2 \mid f$. $\square$

În cazul polinoamelor cu coeficienți într-un corp K , un element α dintr-o extindere E a lui K este rădăcină multiplă a polinomului f dacă și numai dacă este simultan rădăcină a polinomului și a derivatei sale, adică $(X - \alpha) \mid f$ și $(X - \alpha) \mid f'$. Aceasta implică faptul că cmmdc al lui f și f' în $E[X]$ este de grad ≥ 1 . Însă cmmdc a două polinoame se obține cu algoritmul lui Euclid și nu depinde de corpul considerat: dacă $K \subseteq L$ este o extindere de corpuri, iar $f, g \in K[X]$, atunci $(f, g)_{K[X]} = (f, g)_{L[X]}$. În concluzie:

3.16 Propoziție. Fie K un corp și $f \in K[X]$. Atunci f are rădăcini multiple dacă și numai dacă f și f' nu sînt prime între ele. $\square$

Astfel, se poate decide dacă un polinom are rădăcini multiple fără a cunoaște rădăcinile.

Iată o aplicație importantă a teoremei împărțirii cu rest în inele de polinoame: teorema de descompunere a unei funcții raționale în sumă de funcții raționale simple, instrument esențial pentru găsirea primitivei unei funcții raționale.

3.17 Teoremă (Descompunerea unei funcții raționale în sumă de funcții raționale simple). Fie $P, Q \in \mathbb{R}[X]$, cu $Q \neq 0$. Fie descompunerea lui Q în factori ireductibili în $\mathbb{R}[X]$:

$$Q = (X - a_1)^{\alpha_1} \dots (X - a_k)^{\alpha_k} (X^2 + b_1X + c_1)^{\beta_1} \dots (X^2 + b_rX + c_r)^{\beta_r}$$

unde: $k \in \mathbb{N}$, $a_1, \dots, a_k$ sînt reale, distincte două cîte două și $\alpha_1, \dots, \alpha_k \in \mathbb{N}$; $r \in \mathbb{N}$, $X^2 + b_iX + c_i$, $1 \leq i \leq r$, sînt polinoame ireductibile ($b_i^2 - 4a_ic_i < 0$) și distincte două cîte două, iar $\beta_1, \dots, \beta_r \in \mathbb{N}$.

Atunci funcția rațională P/Q se scrie în mod unic sub forma:

$$\frac{P}{Q} = L + \sum_{i=1}^k \left(\frac{d_{i,1}}{(X - a_i)} + \dots + \frac{d_{i,\alpha_i}}{(X - a_i)^{\alpha_i}} \right) + \sum_{j=1}^r \left(\frac{e_{j,1}X + f_{j,1}}{(X^2 + b_jX + c_j)} + \dots + \frac{e_{j,\beta_j}X + f_{j,\beta_j}}{(X^2 + b_jX + c_j)^{\beta_j}} \right)$$

unde: $L \in \mathbb{R}[X]$, $d_{i,t} \in \mathbb{R}$, ($1 \leq i \leq k$, $1 \leq t \leq \alpha_i$), $e_{j,s}, f_{j,s} \in \mathbb{R}$, ($1 \leq j \leq r$, $1 \leq s \leq \beta_j$).

Demonstrație. Vezi exercițiile. $\square$

Propoziția următoare dă cîteva criterii generale de ireductibilitate.

3.18 Propoziție. Fie R un inel integru, K corpul său de fracții și $f = a_0 + a_1X + \dots + a_nX^n$ un polinom nenul cu coeficienți în R ($n \geq 2$).

a) Fie $c, d \in R$, cu c inversabil în R . Atunci f este ireductibil dacă și numai dacă $f(cX + d)$ este ireductibil.

b) Presupunem că $a_0 \neq 0$. Atunci f este ireductibil dacă și numai dacă polinomul

$$r(f) = a_n + a_{n-1}X + \dots + a_0X^n,$$

numit „polinomul reciproc al lui f ” este ireductibil.

c) Presupunem că f nu are divizori neinversabili de grad 0. Dacă S este un inel comutativ și $\varphi: R \rightarrow S$ este un morfism de inele astfel încât $\varphi(a_n) \neq 0$ și polinomul $\varphi(a_0) + \varphi(a_1)X + \dots + \varphi(a_n)X^n$ este ireductibil în $S[X]$, atunci f este ireductibil în $R[X]$.

d) (Criteriul lui Eisenstein) Fie R un inel factorial. Dacă există un element prim $p \in R$ astfel încât $p|a_i, \forall i < n, p \nmid a_n, p^2 \nmid a_0$, atunci f este ireductibil în $K[X]$ (deci f ireductibil și în $R[X]$ dacă este primitiv).

Demonstrație. a) Fie $\varphi: R[X] \rightarrow R[X]$ unicul morfism de R -algebre cu proprietatea că $\varphi(X) = cX + d$. Altfel spus, $\varphi(f)$ se obține înlocuind nedeterminata X în polinomul f cu $cX + d$. Elementul c este inversabil dacă și numai dacă φ este izomorfism de R -algebre (morfismul de R -algebre $\psi: R[X] \rightarrow R[X]$ care duce X în $c^{-1}X - c^{-1}d$ este inversul lui φ). Avem așadar $f = gh \Leftrightarrow \varphi(f) = \varphi(g)\varphi(h), \forall g, h \in R[X]$. Observînd că φ păstrează gradele și că $\varphi|_R = \text{id}_R$, se obține imediat că f este ireductibil dacă și numai dacă $\varphi(f)$ este ireductibil.

b) Dacă g și h sînt polinoame din $R[X]$, cu termenul liber nenul, atunci $r(gh) = r(g)r(h)$. Într-adevăr, observăm că $r(f) = X^n f\left(\frac{1}{X}\right)$ (pentru rigurozitatea argumentului se consideră egalitățile în $K(X)$, corpul de fracții al lui $K[X]$). Deci, dacă $\text{grad } g = m, \text{grad } h = p$, avem

$$r(gh) = X^{m+p}(gh)\left(\frac{1}{X}\right) = X^m g\left(\frac{1}{X}\right) X^p h\left(\frac{1}{X}\right) = r(g)r(h).$$

Concluzia rezultă observînd că r păstrează gradele și că, pentru orice $d \in R$, avem $d|f \Leftrightarrow d|r(f)$.

c) Fie $\psi: R[X] \rightarrow S[X]$ unicul morfism de R -algebre (adică ψ este morfism de inele și $\psi|_R = \varphi$) astfel încât $\psi(X) = X$. Avem de demonstrat că $\psi(f)$ ireductibil implică f ireductibil. Presupunem că $f = gh$, cu $g, h \in R[X]$. Atunci $\psi(f) = \psi(g)\psi(h)$; condiția $\varphi(a_n) \neq 0$ asigură că $\text{grad } \psi(g) + \text{grad } \psi(h) = \text{grad } \psi(f) = n$. Cum $\text{grad } \psi(q) \leq \text{grad } q, \forall q \in R[X]$, obținem că $\text{grad } \psi(g) = \text{grad } g$ și $\text{grad } \psi(h) = \text{grad } h$. Din ireductibilitatea lui $\psi(f)$ deducem că $\psi(g)$ (pentru a face o alegere) este inversabil, deci are grad 0. Astfel, $0 = \text{grad } \psi(g) = \text{grad } g$. Cum f nu are divizori neinversabili de grad 0, $g \in U(R)$.

d) Scriind $f = c(f) \cdot f'$, cu f' primitiv, avem că f și f' sînt asociate în $K[X]$. Înlocuind polinomul f cu f' , putem presupune că f este primitiv. Este suficient acum să demonstrăm că f este ireductibil în $R[X]$. Dacă f ar fi reductibil, atunci:

$$f = a_0 + a_1X + \dots + a_nX^n = (b_0 + b_1X + \dots + b_mX^m)(c_0 + c_1X + \dots + c_pX^p),$$

unde $m > 0$, $p > 0$, $b_0, b_1, \dots, b_m, c_0, c_1, \dots, c_p \in R$, $b_m \neq 0$, $c_p \neq 0$. Avem $b_0 c_0 = a_0$, deci $p \mid b_0 c_0$ și $p^2 \nmid b_0 c_0$; de aici rezultă că p divide exact unul din elementele b_0 și c_0 . Presupunem că $p \mid b_0$ și $p \nmid c_0$. Întrucât $p \nmid a_n$, p nu divide toți coeficienții b_i ; există așadar un i minim, $1 \leq i \leq m$, astfel încât $p \nmid b_i$ (și deci $p \mid b_j$, $\forall j < i$). Atunci $p \nmid b_i c_0$ și deci elementul

$$a_i = b_i c_0 + \sum_{j=1}^{i-1} b_j c_{i-j}$$

nu se divide cu p , contradicție cu ipoteza. $\square$

Există *algoritmi* de decizie a ireductibilității pentru polinoame din $\mathbb{Z}[X]$ (deci și pentru cele din $\mathbb{Q}[X]$), un asemenea algoritm (datorat lui Kronecker) fiind descris în exercițiul 19. O aplicare repetată a unui astfel de algoritm conduce la un *algoritm de factorizare* (de descompunere în factori ireductibili) a oricărui polinom din $\mathbb{Q}[X]$. Programele moderne de calcul simbolic (*Maple*, *Mathematica*, *Macaulay*, *Axiom*, etc.) au implementate rutine puternice de decizie a ireductibilității, inclusiv pentru polinoame de mai multe variabile și pentru polinoame cu coeficienți în extinderi algebrice ale lui $\mathbb{Q}$ sau într-un corp finit. Se poate demonstra că, dacă există un algoritm de factorizare pentru $K[X]$, cu K un corp, atunci există unul și pentru $L[X]$, oricare ar fi L o extindere finit generată a lui K . În particular, există algoritm de factorizare pentru $K[X_1, \dots, X_n]$. Pentru detalii și dezvoltări recente, vezi de ex. ALBU și ION [1997], SPINDLER [1994], GEDDES, CZAPOR, LABAHN [1992], WINKLER [1996].

3.19 Exemple. a) Polinomul $6X^9 + 13X^2 + 26$ este ireductibil în $\mathbb{Q}[X]$ (și în $\mathbb{Z}[X]$, căci este primitiv), conform criteriului lui Eisenstein aplicat cu $p = 13$.

b) Pentru orice număr prim p și orice $n \in \mathbb{N}^*$, $X^n - p$ este ireductibil în $\mathbb{Q}[X]$ și în $\mathbb{Z}[X]$ (tot cu criteriul lui Eisenstein).

c) Fie p un număr prim și $f = X^{p-1} + X^{p-2} + \dots + X + 1 \in \mathbb{Z}[X]$. Criteriul lui Eisenstein nu este aplicabil direct lui f . Considerînd însă polinomul

$$g = f(X+1) = \frac{(X+1)^p - 1}{X+1-1} = \sum_{i=1}^p C_p^i X^{i-1},$$

observăm că lui g i se poate aplica criteriul lui Eisenstein, căci p divide toți coeficienții binomiali C_p^i cu $1 \leq i < p$. Deci g este ireductibil și astfel, conform punctului a) al propoziției de mai sus, f este ireductibil.

d) Polinomul $f = Y^9 + X^9 Y^7 - 3X^2 Y + 2X$ este ireductibil în $\mathbb{Z}[X, Y]$. Pentru demonstrație, considerăm f ca polinom în Y cu coeficienți în inelul factorial $\mathbb{Z}[X]$. Aplicăm acum criteriul lui Eisenstein cu $p = X$ (X este element ireductibil în $\mathbb{Z}[X]$). Remarcăm că inelul $\mathbb{Z}$ putea fi înlocuit cu orice inel factorial de caracteristică diferită de 2.

e) Considerăm polinomul $f = X^5 + X^2 + 1 \in \mathbb{Z}_2[X]$. Polinomul f nu are rădăcini în $\mathbb{Z}_2$, deci divizorii proprii ai lui f nu pot fi de grad 1 (sînt de grad 2 sau 3). O descompunere a lui f poate fi doar de forma:

$$X^5 + X^2 + 1 = (X^3 + aX^2 + bX + 1)(X^2 + cX + 1),$$

cu $a, b, c \in \mathbb{Z}_2$. Identificând coeficienții, se obține un sistem de ecuații în a, b, c , despre care se vede imediat că nu are soluții în $\mathbb{Z}_2$. Așadar, f este ireductibil în $\mathbb{Z}_2[X]$.

f) O aplicare tipică a criteriului 3.18.c) la un polinom f cu coeficienți întregi constă în a „reducere coeficienților modulo n ”. Mai precis, pentru un $n \in \mathbb{N}$ convenabil ales, se consideră unicul morfism de inele $\varphi: \mathbb{Z} \rightarrow \mathbb{Z}_n$ și se cercetează ireductibilitatea polinomului „ f redus modulo n ” (notat cu $\psi(f)$ în demonstrație). Fie, de exemplu, polinomul $f = 7X^5 + 4X^3 - X^2 + 6X + 9 \in \mathbb{Z}[X]$. Redusul modulo 2 al lui f este $X^5 + X^2 + 1 \in \mathbb{Z}_2[X]$, despre care am văzut că este ireductibil. Condițiile de la 3.18.c) sînt îndeplinite, deci f este ireductibil în $\mathbb{Z}[X]$ (deci și în $\mathbb{Q}[X]$, fiind primitiv).

g) Polinomul $10X^7 + 5X^2 + 2$ este ireductibil în $\mathbb{Z}[X]$, căci reciprocul său este $2X^7 + 5X^5 + 10$, căruia i se poate aplica criteriul lui Eisenstein cu $p = 5$.

Exerciții

În exerciții, R este un inel integru și K este corpul său de fracții (dacă nu se specifică altfel).

1. Orice inel integru finit este corp.
2. Fie R un inel unitar infinit. Demonstrați că mulțimea R° a elementelor nenule și neinvertabile este infinită. (Ind. Dacă R° este finită, atunci $U(R)$ este infinită. Fie $S(R^\circ)$ mulțimea bijecțiilor de la R° la R° . Aplicația $\varphi: U(R) \rightarrow S(R^\circ)$ $x \mapsto \varphi_x$, $\varphi_x(a) = xa$, $\forall a \in R^\circ$, este injectivă, contradicție.)
3. Fie R un inel integru în care orice două elemente au cmmdc. Atunci orice element din K se poate scrie sub forma a/b , ($b \neq 0$), cu $a, b \in R$, prime între ele („fracția a/b este ireductibilă”). Ce se poate spune despre unicitatea unei astfel de scrieri?
4. Arătați că un inel comutativ R este integru dacă și numai dacă $R[X]$ este integru.
5. Fie $p \in R^\circ$. Demonstrați că idealul generat de p în $R[X]$, $pR[X]$, este prim dacă și numai dacă p este element prim în R . (Ind.: Arătați că $R[X]/(pR[X]) \cong (R/pR)[X]$). Deduceți o nouă demonstrație pentru 2.19.a).
6. Fie $d \in \mathbb{Z}$, liber de pătrate (adică d nu se divide cu pătratul nici unui întreg > 1), și $\mathbb{Z}[\sqrt{d}] := \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}\}$. Definim „norma” $N: \mathbb{Z}[\sqrt{d}] \rightarrow \mathbb{Z}$, $N(a + b\sqrt{d}) = a^2 - db^2$, $\forall a, b \in \mathbb{Z}$. Atunci:
 - a) $N(\alpha)N(\beta) = N(\alpha\beta)$, $\forall \alpha, \beta \in \mathbb{Z}[\sqrt{d}]$.
 - b) $U(\mathbb{Z}[\sqrt{d}]) = \{\alpha \in \mathbb{Z}[\sqrt{d}] \mid N(\alpha) = \pm 1\} = \{a + b\sqrt{d} \mid a, b \in \mathbb{Z}, a^2 - db^2 = \pm 1\}$.
 Determinați efectiv $U(\mathbb{Z}[\sqrt{d}])$ dacă $d < 0$.
7. Elementele 6 și $2 + \sqrt{-5}$ nu au cmmdc (și deci nici cmmmc) în inelul $\mathbb{Z}[\sqrt{-5}]$.
8. Un număr prim $p \in \mathbb{Z}$ este prim și în inelul $\mathbb{Z}[i]$ dacă și numai dacă $4 \mid p - 1$.

9. Fie R un inel euclidian față de funcția φ . Atunci există $u \in R$ nenul și neinvertibil cu proprietatea: $\forall x \in R, \exists q \in R$ astfel încât $x - qu$ este invertibil sau 0. Cît poate fi ales u pentru $R = \mathbb{Z}, K[X]$? (Ind. $\min \{\varphi(v) \mid v \in R^\circ\} = \varphi(u)$ pentru un $u \in R^\circ$.)

10. Fie d un întreg liber de pătrate, $d \equiv 1 \pmod{4}$. Atunci inelul $\mathbb{Z}[\sqrt{d}]$ nu este GCD-inel. (Ind. 2 este ireductibil și nu este prim.)

11. Să se arate că în $\mathbb{Z}$ există o infinitate de elemente prime neasociate în divizibilitate.

12. Fie R un inel principal, $n \in \mathbb{N}^*$, $a_1, \dots, a_n \in R$ și d un cmmdc al lor. Demonstrați că există $u_1, \dots, u_n \in R$ astfel încât $d = a_1u_1 + \dots + a_nu_n$.

13. Fie R un inel factorial și $f = a_0 + a_1X + \dots + a_nX^n \in R[X]$.

a) Dacă $p/q \in K$ este o rădăcină a lui f , unde $p, q \in R$ și $(p, q) = 1$, atunci $p|a_0$, $q|a_n$ și $(p - qr)|f(r)$, $\forall r \in R$. Ce devin relațiile pentru $a_n = 1$?

b) Fie $g = a_n^{n-1}a_0 + a_n^{n-2}a_1X + \dots + a_{n-1}X^{n-1} + X^n$. Atunci $a_n^{n-1}f(X) = g(a_nX)$. Descrieți legătura dintre rădăcinile lui g și cele ale lui f .

c) Găsiți rădăcinile din $\mathbb{Q}$ ale polinoamelor $2X^3 + 5X^2 + 9X - 15$ și $4X^3 - 7X^2 - 7X + 15$.

14. Fie K un corp. Demonstrați că orice polinom nenul $f \in K[X]$ are cel mult $\deg f$ rădăcini în K (fiecare fiind numărată cu multiplicitatea sa).

15. Fie R un inel. Demonstrați echivalența următoarelor afirmații:

a) Orice polinom nenul $f \in R[X]$ are cel mult $\deg f$ rădăcini în R (fiecare fiind numărată cu multiplicitatea sa).

b) Orice polinom de grad 1 are cel mult o rădăcină în R .

c) R este inel integru.

(Ind. Considerați corpul de fracții al lui R și folosiți problema precedentă).

16. Fie K un corp. Vrem să demonstrăm, într-un caz mai general, teorema de descompunere a unei funcții raționale în sumă de funcții raționale simple.

a) Fie $Q \in K[X]$, ireductibil. Atunci, pentru orice $k \in \mathbb{N}$ și $P \in K[X]$, există o scriere de forma:

$$\frac{P}{Q} = L + \frac{f_1}{Q} + \dots + \frac{f_k}{Q^k},$$

unde $L, f_1, \dots, f_k \in K[X]$ și $\deg f_i < \deg Q$. (Ind. Cazul $k = 1$ se reduce la teorema împărțirii cu rest a lui P la Q . În continuare se aplică o inducție după k .)

b) Fie $Q \in K[X]$, $Q = q_1^{\alpha_1} \dots q_k^{\alpha_k}$, cu q_i ireductibile în $K[X]$, prime între ele două câte două. Atunci, pentru orice $P \in K[X]$, există o scriere de forma:

$$\frac{P}{Q} = L + \sum_{i=1}^k \left(\frac{f_{i,1}}{q_i} + \dots + \frac{f_{i,\alpha_i}}{q_i^{\alpha_i}} \right),$$

unde $L, f_{i,t} \in K[X]$ și $\deg f_{i,t} < \deg q_i$, pentru orice i și t .

(Ind. Fie $u_i = \frac{Q}{q_i^{\alpha_i}} \in K[X]$. Avem $(u_1, \dots, u_n) = 1$, deci există $v_1, \dots, v_n \in K[X]$ astfel încît

$$u_1 v_1 + \dots + u_n v_n = 1 \Rightarrow P = P u_1 v_1 + \dots + P u_n v_n \Rightarrow \frac{P}{Q} = \frac{P v_1}{q_1^{\alpha_1}} + \dots + \frac{P v_k}{q_k^{\alpha_k}}. \text{ Se aplică acum a)}$$

pentru fiecare termen.)

c) (unicitatea scrierii) Dacă $L + \sum_{i=1}^k \left(\frac{f_{i,1}}{q_i} + \dots + \frac{f_{i,\alpha_i}}{q_i^{\alpha_i}} \right) = M + \sum_{i=1}^k \left(\frac{g_{i,1}}{q_i} + \dots + \frac{g_{i,\alpha_i}}{q_i^{\alpha_i}} \right)$, unde $L, M,$

$f_{i,t}, g_{i,t} \in K[X]$ și $\text{grad } f_{i,t}, \text{grad } g_{i,t} < \text{grad } q_i$, pentru orice i și t , atunci $L = M$ și $f_{i,t} = g_{i,t}, \forall i, t$.

(Ind. Înmulțind cu Q , se obține o relație de forma $LQ + R_1 = MQ + R_2$, unde $\text{grad } R_1$ și $\text{grad } R_2$

sînt $< \text{grad } Q$. Din unicitatea împărțirii cu rest la Q rezultă că $L = M$ și $R_1 = R_2$. Rămîne de

demonstrat că, dacă $\sum_{i=1}^k \left(\frac{f_{i,1}Q}{q_i} + \dots + \frac{f_{i,\alpha_i}Q}{q_i^{\alpha_i}} \right) = 0$ și $\text{grad } f_{i,t} < \text{grad } q_i$, atunci $f_{ij} = 0, \forall i, j$. Pentru

i fixat, se observă că q_i apare ca factor pentru toți termenii din membrul stîng, cu excepția lui

$\frac{f_{i,\alpha_i}Q}{q_i^{\alpha_i}}$. Cum q_i este prim cu $\frac{Q}{q_i^{\alpha_i}}$, rezultă că $q_i \mid f_{i,\alpha_i}$, deci $f_{i,\alpha_i} = 0$ din motive de grade. Se

împarte acum relația la q_i și se repetă raționamentul, obținîndu-se $f_{i,\alpha_i-1} = 0$ etc.)

d) Demonstrați teorema IV.3.17, punînd $K = \mathbb{R}$.

17. Fie R un inel. Dacă $f \in R[X]$, i se asociază funcția polinomială $\tilde{f} : R \rightarrow R$ unde, $\forall x \in R$, $\tilde{f}(x) = f(x)$ (valoarea polinomului f în x). Demonstrați că, dacă R este integru infinit, atunci funcția $\varphi : R[X] \rightarrow R^R$, $\varphi(f) = \tilde{f}$, $\forall f \in R[X]$, este injectivă. Rămîne valabilă concluzia dacă se renunță la ipoteza R infinit?

18. (Polinomul de interpolare Lagrange) Fie K un corp, $n \geq 1$, $x_0, \dots, x_n \in K$, ($n+1$ elemente distincte) și $y_0, \dots, y_n \in K$. Demonstrați că există un unic polinom $L \in K[X]$ de grad cel mult n astfel încît $L(x_i) = y_i, 0 \leq i \leq n$.

19. (Algoritmul de factorizare al lui Kronecker în $\mathbb{Z}[X]$) Fie $p \in \mathbb{Z}[X]$, primitiv, $\text{grad } p = n$. Notăm cu m cel mai mare întreg $\leq n/2$.

a) Arătați că p reductibil în $\mathbb{Z}[X] \Leftrightarrow p$ are un factor neconstant de grad $\leq m$.

b) Fie $(x_0, \dots, x_m) \in \mathbb{Z}^{m+1}$, cu x_i distincte două cîte două. Arătați că următorul algoritm se termină într-un număr finit de pași și furnizează un factor neconstant al lui p de grad $\leq m$ sau demonstrează iredutibilitatea lui p :

1. Dacă $\exists i$ cu $p(x_i) = 0$, atunci $X - x_i$ este un factor al lui p și am terminat. Dacă nu, treci la 2.

2. Fie $D = \{d = (d_0, \dots, d_m) \in \mathbb{Z}^{m+1} \mid d_i \mid p(x_i), \forall i\}$. D este o mulțime finită.

Pentru orice $d \in D$, fie $L_d \in \mathbb{Q}[X]$ polinomul (de interpolare Lagrange) cu proprietățile $L_d(x_i) = d_i, \forall i$, și $\text{grad } L_d \leq m$. Dacă există $d \in D$ cu $L_d \in \mathbb{Z}[X]$ și $L_d \mid p$, atunci L_d este un factor al lui p și am terminat. Dacă nu, atunci p este iredutibil.

c) Deduceți un algoritm de decizie a iredutibilității pentru polinoame din $\mathbb{Q}[X]$.

d) Presupunem că $m = 2$. Ce alegere pentru $(x_0, \dots, x_m)$ propuneți?

e) Presupunem că în inelul factorial R există un algoritm de factorizare (de descompunere a oricărui element din R° în factori primi). Ce proprietăți trebuie să aibă R pentru a putea generaliza la $R[X]$ algoritmul de mai sus?

f) Presupunem că R este factorial și că în $R[X]$ există un algoritm de factorizare. Atunci există un algoritm de factorizare în $K[X]$.

20. Decideți ireductibilitatea polinomului $X^4 + X^2 + 2X - 1$ din $\mathbb{Z}[X]$ cu algoritmul Kronecker.

21. Fie R un inel integru.

a) Fie $f \in R[X]$, $\text{grad } f = m$. Dacă f are cel puțin $m + 1$ rădăcini în R , atunci $f = 0$.

b) Fie $g \in R[X_1, \dots, X_n]$, cu R infinit. Dacă $g(a_1, \dots, a_n) = 0$, $\forall (a_1, \dots, a_n) \in R^n$, atunci g este polinomul nul. (Ind. Inducție după n .) Deduceți că două polinoame din $R[X_1, \dots, X_n]$ sînt egale dacă și numai dacă funcțiile polinomiale asociate sînt egale.

c) Dați exemplul de corp finit K și de polinoame distincte din $K[X]$ care au aceeași funcție polinomială asociată.

22. Fie K un corp de caracteristică diferită de 2 (adică $1 + 1 \neq 0$ în K) și p un polinom omogen de grad 2 în $K[X, Y]$, adică $p = aX^2 + bXY + cY^2$, cu $a, b, c \in K$. Demonstrați că p este reductibil în $K[X, Y] \Leftrightarrow b^2 - 4ac$ este un pătrat în $K \Leftrightarrow b^2 - 4ac = 0$ sau există $\alpha, \beta \in K$, $(\alpha, \beta) \neq (0, 0)$, cu $p(\alpha, \beta) = 0$.

23. Să se descompună în factori ireductibili polinomul $X_1^3 + X_2^3 \in K[X_1, X_2]$. Discuție după caracteristica lui K .

24. Fie K un corp de caracteristică diferită de 3 și $f = X_1^3 + \dots + X_n^3 \in K[X_1, \dots, X_n]$. Arătați că f este ireductibil dacă și numai dacă $n \geq 3$. Generalizare. (Ind. Pentru $n = 3$, folosiți criteriul Eisenstein pentru $f \in K[X_1, X_2][X_3]$. Se face apoi o inducție după n .)

25. Fie n^2 nedeterminate X_{ij} , $1 \leq i, j \leq n$ și matricea $A = (X_{ij})_{1 \leq i, j \leq n} \in M_n(\mathbb{Z}[X_{ij}; 1 \leq i, j \leq n])$. Atunci polinomul $\det A = \sum \{X_{1\sigma(1)} \dots X_{n\sigma(n)} \mid \sigma \in S_n\}$ este ireductibil în $\mathbb{Z}[X_{ij}; 1 \leq i, j \leq n]$.

26. Fie $x, y \in R$. Dacă există un cmmmc al lor $[x, y] \in R$, atunci există și un cmmdc al lor (x, y) și avem $xy \sim x, y$.

27. Fie R un subinel unitar al unui inel comutativ S . Un element al lui S se numește *întreg* peste R dacă este rădăcină a unui polinom unitar nenul din $R[X]$. Demonstrați că, dacă R este GCD-inel și $x \in K$ este întreg peste R , atunci $x \in R$.

28. Fie R un inel principal și S un sistem multiplicativ închis în R . Atunci inelul de fracții $S^{-1}R$ este principal.

29. Fie R un inel factorial și S un sistem multiplicativ închis în R . Atunci inelul de fracții $S^{-1}R$ este factorial.

30. Proprietatea unui inel R de a fi euclidian (respectiv principal, factorial) se transmite și la subinelele unitare ale lui R ?

31. Fie R un inel factorial care nu este corp, astfel încât grupul unităților $U(R)$ este finit. Atunci în R există o infinitate de elemente prime neasociate în divizibilitate. (Ind. Dacă $p_1, \dots, p_n$ sînt toate elementele prime pînă la asociere, atunci există $m \geq 1$ astfel încît $1 + (p_1 \dots p_n)^m \in R^\circ$.)

32. Fie R un inel factorial și $p \in R$ un element prim. Folosind morfismul canonic $\pi: R \rightarrow R/pR$ și prelungirea sa la un morfism $\psi: R[X] \rightarrow (R/pR)[X]$, dați o nouă demonstrație criteriului lui Eisenstein. (Ind. Dacă $f = a_0 + a_1 X + \dots + a_n X^n$ satisface ipotezele criteriului și $f = gh$, atunci $\psi(f) = \pi(a_n)X^n = \psi(g)\psi(h)$. Dacă $\text{grad } g, \text{grad } h \geq 1$, atunci termenii liberi ai lui g și h sînt multipli de p .)

V. Spații liniare, matrice și aplicații

V.1 Algebre de matrice

Scopul acestei secțiuni este de a da demonstrații scurte și relativ elementare teoremelor Cayley-Hamilton și Frobenius folosind polinoamele matriciale.

1.1 Definiție. O matrice $m \times n$ cu elemente polinoame din $K[X]$ se numește *polinom matricial* peste corpul K . Putem scrie un polinom matricial $P \in M(m, n, K[X])$ sub forma:

$$P = \begin{bmatrix} p_{11} & \cdots & p_{1n} \\ \vdots & & \\ p_{n1} & \cdots & p_{nn} \end{bmatrix}, \text{ cu } p_{ij} \in K[X], \quad (1)$$

sau (grupînd după puterile lui X) sub forma:

$$P = P_0 + X P_1 + \dots + X^r P_r, \quad (2)$$

unde $P_0, P_1, \dots, P_r \in M(m, n, K)$.

De exemplu, avem:

$$\begin{bmatrix} 5+2X & 3X^3 \\ 1 & 2-2X+X^2 \end{bmatrix} = \begin{bmatrix} 5 & 0 \\ 1 & 2 \end{bmatrix} + X \begin{bmatrix} 2 & 0 \\ 0 & -2 \end{bmatrix} + X^2 \begin{bmatrix} 0 & 0 \\ 0 & 1 \end{bmatrix} + X^3 \begin{bmatrix} 0 & 3 \\ 0 & 0 \end{bmatrix}$$

1.2 Definiție. Fie $P \in M(n, K[X])$ un polinom matricial de forma (2), cu P_i matrice pătratică ($\in M(n, K)$), iar $A \in M(n, K)$. Definim $P(A)$, *valoarea lui P în A* :

$$P(A) := P_0 + A P_1 + \dots + A^r P_r \in M(n, K).$$

1.3 Observație. Dacă $P, Q \in M(n, K[X])$ sînt polinoame matriciale, atunci avem definite $P + Q, PQ$ (operațiile uzuale în $M(n, K[X])$). Pentru $\forall A \in M(n, K)$, au sens $(P + Q)(A)$ și $(PQ)(A)$, definite ca mai sus. Are loc $(P + Q)(A) = P(A) + Q(A)$ (demonstrație ușoară), *însă în general* $(PQ)(A) \neq P(A)Q(A)$. De exemplu, dacă P și Q sînt "de grad 1", $P = X P_1$ și $Q = X Q_1$, cu $P_1, Q_1 \in M(n, K)$, atunci $PQ = X^2 P_1 Q_1$. Avem $P(A)Q(A) = A P_1 A Q_1$, $(PQ)(A) = A^2 P_1 Q_1$ și $A P_1 A Q_1 \neq A^2 P_1 Q_1$ în general. Totuși, are loc:

1.4 Propoziție. Dacă $P = P_0 + X P_1 + \dots + X^r P_r$ și $AP_i = P_i A$, $1 \leq i \leq r$ (A comută cu P_i , $\forall i$), atunci $(PQ)(A) = P(A)Q(A)$, $\forall Q = Q_0 + X Q_1 + \dots + X^d Q_d \in M(n, K[X])$.

Demonstrație. PQ se obține prin regula uzuală (atenție la ordinea factorilor!):

$$PQ = P_0 Q_0 + X(P_0 Q_1 + P_1 Q_0) + \dots + X^{r+d} P_r Q_d,$$

$$\text{iar } P(A)Q(A) = (P_0 + AP_1 + \dots + A^r P_r)(Q_0 + AQ_1 + \dots + A^d Q_d).$$

Un termen oarecare al produsului $P(A)Q(A)$ este de forma $A^i P_i A^j Q_j = A^i A^j P_i Q_j = A^{i+j} P_i Q_j$ (căci P_i comută cu A^j). Grupînd termenii ce conțin A^k ($0 \leq k \leq r+d$), rezultă că

$$P(A)Q(A) = P_0 Q_0 + A(P_0 Q_1 + P_1 Q_0) + \dots + A^{r+d} P_r Q_d = (PQ)(A).$$

1.5 Teoremă. (Teorema Cayley-Hamilton⁷¹) Fie K un corp, $A \in M(n, K)$ și $f_A = \det(XI - A)$ polinomul său caracteristic. Atunci $f_A(A) = 0$.

Demonstrație. Se știe că, dacă $B = (b_{ij}) \in M(n, R)$ este o matrice cu coeficienți într-un inel comutativ R , are loc: $B \cdot \text{ad}(B) = \det(B) \cdot I$, unde este $\text{ad}(B)$ matricea reciprocă (adjunctă) a lui B (pe locul (i, j) al lui $\text{ad}(B)$ este complementul algebric al lui b_{ij} în B). Aplicînd această observație matricei $XI - A \in M(n, K[X])$, are loc

$$(XI - A) \cdot \text{ad}(XI - A) = \begin{bmatrix} \det(XI - A) & & 0 \\ & \ddots & \\ 0 & & \det(XI - A) \end{bmatrix} =: P,$$

Din lema următoare rezultă $P(A) = 0$, iar $P(A) = f_A(A)$, deci $f_A(A) = 0$. □

1.6 Lemă. Fie $P \in M(n, K[X])$ un polinom matricial și $A \in M(n, K)$. Atunci $P(A) = 0 \Leftrightarrow$ există $Q \in M(n, K[X])$ astfel încît $P = (XI - A) \cdot Q$.

Demonstrație. Fie $P = P_0 + X P_1 + \dots + X^r P_r$. Avem:

$$P - P(A) = P_0 + X P_1 + \dots + X^r P_r - (P_0 + A P_1 + \dots + A^r P_r) =$$

$$(XI - A)P_1 + (X^2 I - A^2)P_2 + \dots + (X^r I - A^r)P_r.$$

Însă $X^k I - A^k = (XI - A)(X^{k-1} I + X^{k-2} A + \dots + A^{k-1})$, $\forall k$. Înlocuind în relația de mai sus, avem $P - P(A) = (XI - A)Q$, cu $Q \in M(n, K[X])$. Dacă $P(A) = 0$, rezultă $P = (XI - A)Q$.

Reciproc, fie $P = (XI - A)Q$. Cum coeficienții lui $XI - A$ sînt I și $A \in M(n, K)$ (care comută cu A), din observația 1.4 rezultă că $P(A) = (AI - A)Q(A) = 0$. □

Pentru o matrice dată $A \in M(n, K)$, polinomul caracteristic f_A nu este neapărat de grad minim printre polinoamele $p \in K[X]$ cu $p(A) = 0$.

1.7 Propoziție. Fie $A \in M(n, K)$. Există un unic polinom unitar $\mu_A \in K[X]$ cu proprietățile:

a) $\mu_A(A) = 0$;

b) $\forall p \in K[X]$ cu $p(A) = 0$ rezultă că $\mu_A \mid p$.

În plus, μ_A este polinomul unitar de grad minim printre polinoamele $p \in K[X]$ cu $p(A) = 0$.

⁷¹ Arthur Cayley (1821-1895) și Sir William Rowan Hamilton (1805-1865), matematicieni britanici. Cazul general al teoremei a fost demonstrat însă de Frobenius.

Demonstrație. Fie $M = \{p \in K[X] \mid p \neq 0, p(A) = 0\}$. M este nevidă ($f_A \in M$). Mulțimea de numere naturale $\{\text{grad } p \mid p \in M\}$ are un cel mai mic element, deci există $\mu_A \in M$ (îl putem alege unitar) astfel încât $\text{grad } \mu_A \leq \text{grad } p, \forall p \in M$. Fie $p \in M$. Atunci există $q, r \in K[X]$ astfel încât $p = \mu_A q + r$, cu $\text{grad } r < \text{grad } \mu_A$. Avem $0 = p(A) = \mu_A(A)q(A) + r(A) = r(A)$, deci $r = 0$ (dacă $r \neq 0$, ar rezulta $r \in M$ și $\text{grad } r < \text{grad } \mu_A$, contradicție cu alegerea lui μ_A). Astfel, $\mu_A \mid p$. Dacă $q \in K[X]$ este unitar și satisface condițiile a) și b), atunci $\mu_A \mid q$ și $q \mid \mu_A$. Cum μ_A este unitar, rezultă $\mu_A = q$. $\square$

1.8 Definiție. Fie $A \in M(n, K)$. Polinomul unitar $\mu_A \in K[X]$ din propoziția precedentă se numește *polinomul minimal* al lui A .

1.9 Teoremă. Fie $A \in M(n, K)$. Atunci:

- a) Polinomul minimal μ_A divide polinomul caracteristic f_A .
- b) (Frobenius⁷²) Polinomul minimal μ_A și polinomul caracteristic f_A au aceleași rădăcini⁷³ (posibil cu multiplicități diferite).

Demonstrație. a) Clar, din definiția lui μ_A .

b) Dacă $f_A(\lambda) = 0$, atunci λ este valoare proprie a lui A , deci $Ax = \lambda x$ pentru un $x \in E$, nenul. Rezultă că $A^r x = \lambda^r x, \forall r \in \mathbb{N}$ și, mai general, $p(A) \cdot x = p(\lambda)x, \forall p \in K[X]$. Deci $0 = \mu_A(A) \cdot x = \mu_A(\lambda) \cdot x$, de unde $\mu_A(\lambda) = 0$. Invers, orice rădăcină a lui μ_A este rădăcină a lui f_A , căci $\mu_A \mid f_A$. $\square$

V.2 Coduri liniare corectoare de erori

Algebra liniară își găsește un domeniu fertil și neașteptat de aplicabilitate în teoria *codurilor corectoare de erori*, teorie născută în anii 1940, odată cu era calculatoarelor și a comunicațiilor digitale. Vom prezenta ideile de bază din această teorie și câteva aplicații ale algebrei liniare, relativ elementare, dar cu utilitate practică deosebită.

Prin "informație digitală" înțelegem un șir de simboluri (elemente) dintr-un alfabet finit. De exemplu, 011110101100 este un șir de simboluri din alfabetul $\{0,1\}$ (în acest caz, simbolurile se numesc *biți*). Transmiterea unei *informații digitale*⁷⁴ între două puncte diferite *în spațiu* (de exemplu o transmisie de date pe o linie telefonică) sau *în timp* (stocarea pe un

⁷² Ferdinand Georg Frobenius (1849-1917), matematician german.

⁷³ Este vorba de rădăcinile din K . Enunțul rămîne valabil și pentru rădăcinile dintr-o *extindere* L a lui K (un corp L astfel încât K este subcorp în L).

⁷⁴ Transmiterea de sunete, imagini, texte etc. ca un șir de 0 și 1 pare azi evidentă, dar în anii 1940 a fost o idee revoluționară și îi aparține lui *Claude Shannon* (1916-2001), matematician american, unul din fondatorii teoriei informației (articolul *A mathematical theory of communication*, 1948).

suport material cum ar fi un compact disc, pentru o citire ulterioară), este supusă *erorilor* cauzate de o varietate de factori: zgomot pe linia telefonică, deteriorarea suportului fizic al informației etc. Presupunem că o *eroare* cauzează receptarea altui simbol decât cel transmis (dar nu „pierderea” simbolului prin transmisie). Se impune găsirea unui procedeu prin care mesajul să poată ajunge în formă corectă la receptor (sau receptorul să poată detecta eventualele erori și să ceară retransmisia mesajului).

Ideea care stă la baza teoriei *codurilor bloc corectoare de erori* este următoarea: se fixează $k, n \in \mathbb{N}^*$, cu $k < n$. Se împarte mesajul original (un șir finit de simboluri din A) în „blocuri” (numite „cuvinte”) de k simboluri. Fiecărui cuvânt⁷⁵ de lungime k i se asociază un cuvânt mai lung, de lungime n , după o lege prestabilită; cele $n - k$ simboluri „în plus” sînt puse pentru detectarea și eventual corectarea erorilor ce pot apărea în transmisie. Pe canal se transmite cuvîntul de n simboluri, la recepție urmînd ca, prin analizarea cuvîntului recepționat, să se decidă dacă au apărut erori (sau să se reconstituie cuvîntul transmis).

2.1 Exemplu. Fie $A = \{0, 1\}$ (alfabet *binar*). O idee simplă și nu prea eficientă de codare pentru corectarea erorilor este de a transmite fiecare bit de 3 ori, urmînd ca decodarea să se facă după „regula majorității”. Mai precis, luăm $k = 1, n = 3$ și stabilim următorul procedeu de codare: 0 este codat ca 000, iar 1 ca 111. Astfel, dacă mesajul original este 0101, el va fi codat ca 000111000111. Să presupunem că acest mesaj este afectat de erori pe canal, încît la recepție se primește 001111000011. La decodare, fiecare grup de 3 biți este tratat individual: de exemplu grupul 001 este decodat în 0 (se presupune că 001 provine din 000 în care unul din 0 a devenit 1), 011 este decodat în 1 etc. Acest procedeu de corecție a erorilor funcționează atît timp cît nu apare mai mult de o eroare la fiecare grup de trei simboluri transmise.

Modelăm o situație de tipul descris, astfel: *transmițătorul* trimite un *mesaj* către *receptor* pe un *canal de transmisie*. *Mesajul* este un șir finit de *simboluri*, care sînt elemente ale unei mulțimi finite A , numită *alfabet*. Orice șir de simboluri poate fi mesaj⁷⁶. Posibilitatea de apariție de erori pe canal este modelată de o *funcție de tranziție* $P: A \times A \rightarrow [0, 1]$, cu semnificația că $\forall x, y \in A, P(y, x)$ reprezintă probabilitatea ca la transmiterea simbolului x , la recepție să fie primit simbolul y .

Unul din cele mai răspîndite modele pentru un canal de transmisie este *canalul q -ar simetric de probabilitate p* : A are q elemente (este un „alfabet q -ar”); funcția de tranziție P are proprietatea că $P(y, x) = p, \forall y, x \in A$ cu $y \neq x$. Altfel spus, probabilitatea de apariție a unei

⁷⁵ Prin *cuvînt de lungime k* se înțelege un k -uplu de simboluri din A (un element din A^k).

⁷⁶ Desigur, acest lucru e fals dacă se transmit numai mesaje din limba română, de exemplu. Însă această presupunere e valabilă dacă se efectuează în prealabil o *compresie fără pierderi* a mesajului, lucru curent în practica transmisiei de date (de exemplu compresiile zip, rar, lha etc). Acest procedeu, formalizat de Huffman, se bazează pe o analiză statistică a mesajului și codarea simbolurilor cele mai probabile în șiruri scurte și a celor mai puțin probabile în șiruri mai lungi.

erori (simbolul primit diferă de cel trimis⁷⁷) este $(q-1)p$, indiferent de simbolul transmis (de unde și denumirea de canal *simetric*) și *indiferent de locul simbolului în mesaj* (canal „fără memorie”). Deci, probabilitatea ca un simbol transmis x să fie recepționat corect este $P(x, x) = 1 - (q-1)p$. Se presupune că $0 \leq p < 1/2(q-1)$ (altfel este mai probabil să se recepționeze un simbol eronat decât cel corect!). Dacă $q = 2$, se vorbește de un canal *binar*.

Formalizăm ideea de codare bloc de mai sus: se fixează $k, n \in \mathbb{N}$, cu $k \leq n$; se dă o funcție injectivă $E: A^k \rightarrow A^n$ care *codează* fiecare $a = a_1 \dots a_k \in A^k$ într-un *cuvânt cod* $c = c_1 \dots c_n \in A^n$. (Un element oarecare din A^n , $(x_1, \dots, x_n)$, (unde $x_i \in A, \forall i$) îl scriem mai simplu $x_1 \dots x_n$.)

Mulțimea $C := E(A^k) = \{E(a_1 \dots a_k) \mid a_1 \dots a_k \in A^k\}$ a tuturor cuvintelor cod se numește *cod* (în cazul nostru, *cod bloc de tip $[n, k]$*). Pentru funcționarea codului trebuie dată și o *funcție de decodare* $D: A^n \rightarrow C$, care asociază oricărui cuvânt x din A^n cuvântul cel mai probabil transmis $D(x) \in C$. Evident, $D(c) = c, \forall c \in C$.

În acest caz, $|C| = q^k$. Este utilă și o accepție *mai largă* a noțiunii de cod:

2.2 Definiție. Un *cod de lungime n* peste alfabetul A este o submulțime C a lui A^n . Elementele lui C se numesc *cuvinte cod*. Dacă $|A| = q$, C se numește *cod q -ar*.

Un cod bloc de tip $[n, k]$ transformă orice bloc de k simboluri într-un cuvânt cod de lungime mai mare n , ceea ce va permite (se speră) detecția sau corecția erorilor. Însă acest procedeu *mărește lungimea mesajelor transmise* (ceea ce nu este de dorit). Pentru a măsura eficiența unui cod din acest punct de vedere, se definește *rata de transmisie* a unui cod C de tip $[n, k]$ ca fiind $R(C) := k/n$. Rata măsoară proporția de simboluri care poartă informație (restul sînt simboluri *redundante*, care folosesc la detecție sau corectare de erori). Dacă C este ca în def. 2.2, *rata* e definită ca $R(C) := \log_q |C|/n$ (de ce?).

Posibilitatea unui cod C de a corecta erori se bazează în întregime pe ideea că, dacă un cuvânt cod $c \in C$ este afectat pe canalul de transmisie de (un număr mic de) erori, cuvântul receptat $c_t \neq c$ nu este cuvânt cod (nu aparține lui C), dar este „suficient de apropiat” de c încît să putem reconstitui c din c_t . Acest lucru este posibil doar dacă c_t nu este el însuși un alt cuvânt cod sau nu e „mai apropiat” de alt cuvânt cod c' !

Aceste idei se pot formula riguros. Avem nevoie de cîteva pregătiri.

2.3 Definiție. Fie A o mulțime nevidă. *Distanța Hamming*⁷⁸ pe A^n se definește astfel:

$$\forall x = (x_1, \dots, x_n), y = (y_1, \dots, y_n), d(x, y) := |\{i \mid 1 \leq i \leq n, x_i \neq y_i\}|.$$

Deci, distanța între două cuvinte este *numărul de locuri în care cuvintele diferă*.

⁷⁷ Se presupune că nu "se pierd" simboluri la transmisie: numărul de simboluri transmise este egal cu numărul celor recepționate.

⁷⁸ În onoarea lui Richard Hamming (1915-1998), matematician american, fondator, alături de Shannon, al teoriei informației (articolul *Error detecting and error correcting codes*, 1950).

2.4 Propoziție. Distanța Hamming $d : A^n \times A^n \rightarrow \mathbb{R}$ este o distanță (o metrică) pe A^n , adică:

- a) $\forall x, y \in A^n$, avem $d(x, y) \geq 0$;
- b) $\forall x, y \in A^n$, avem: $d(x, y) = 0 \Leftrightarrow x = y$;
- c) $\forall x, y, z \in A^n$, avem: $d(x, y) \leq d(x, z) + d(z, y)$.

Demonstrație. c) Pentru orice $x = (x_1, \dots, x_n), y = (y_1, \dots, y_n) \in A^n$, fie $C(x, y) := \{i \mid x_i = y_i\}$. Arătăm că $d(x, y) \leq d(x, z) + d(z, y)$, $\forall x, y, z \in A^n$. Cum $d(x, y) = n - |C(x, y)|$, inegalitatea devine: $n \geq |C(x, z)| + |C(z, y)| - |C(x, y)|$. Evident, avem $C(x, z) \cup C(z, y) \subseteq \{1, \dots, n\}$, deci $|C(x, z) \cup C(z, y)| \leq n$, adică $|C(x, z)| + |C(z, y)| - |C(x, z) \cap C(z, y)| \leq n$. Însă $C(x, z) \cap C(z, y) \subseteq C(x, y)$, deci $n \geq |C(x, z)| + |C(z, y)| - |C(x, z) \cap C(z, y)| \geq |C(x, z)| + |C(z, y)| - |C(x, y)|$. $\square$

Pentru $x \in A^n$ și $r > 0$, sfera (bila) de rază r centrată în x este mulțimea cuvintelor care sînt la distanță cel mult r față de x :

$$S(x, r) := \{y \in A^n \mid d(x, y) \leq r\}.$$

Pentru $x \in A^n$, unde $|A| = q$, există $C_n^i(q-1)^i$ cuvinte aflate la distanță exact i de x . Deci:

2.5 Propoziție. Fie $|A| = q$. Numărul de elemente al unei sfere de rază r din A^n este

$$|S(x, r)| = \sum_{i=0}^r C_n^i (q-1)^i. \quad \square$$

2.6 Definiție. Distanța minimă a unui cod $C \subseteq A^n$ este:

$$d(C) := \min \{d(x, y) \mid x, y \in C, x \neq y\}.$$

Capacitatea de corecție a codului C este:

$$e(C) := [(d(C) - 1)/2].$$

Fie C un cod cu $d(C) = d$ și $e(C) = e = [(d-1)/2]$. Atunci orice două sfere centrate în cuvinte cod distincte și de rază e sînt disjuncte (demonstrați!). Drept consecință, dacă la transmiterea unui cuvînt cod $c \in C$ au apărut cel mult e erori, iar cuvîntul receptat este c_t , atunci $d(c, c_t) \leq e$, deci c_t este mai aproape de c decît de orice alt cuvînt cod.

Pentru a găsi c , plecînd de la c_t , se poate folosi un *algoritm de distanță minimă*, adică un algoritm care, dat un cuvînt $x \in A^n$, găsește un cuvînt cod $w_x \in C$ care este cel mai aproape de x , adică $d(x, w_x) = \min \{d(x, y) \mid y \in C\}$.

2.7 Observație. Utilizarea unui cod C de lungime n , distanță minimă d și capacitate de corecție e se poate face în două moduri distincte:

- modul „corectare de erori”: se presupune că orice bloc de n simboluri c este afectat de cel mult e erori. Dacă cuvîntul recepționat este c_t , c_t poate fi decodat în mod univoc în c .⁷⁹

⁷⁹ De aici și denumirea de *capacitate de corecție a lui C* ce se dă lui e .

- modul „detectare de erori”: se presupune că la transmiterea oricărui bloc de n simboluri apar cel mult $d - 1$ erori. Atunci nici un cuvânt cod c nu poate fi transformat pe parcursul transmiterii în alt cuvânt cod c' . Astfel, dacă receptorul primește un cuvânt c_t care nu este cuvânt cod, semnalează „eroare” (și cere eventual retransmiterea cuvântului).

2.8 Exercițiu. a) Demonstrați afirmațiile din observația de mai sus.

b) Arătați că există două sfere centrate în cuvinte cod distincte și de rază $e + 1$ care nu sînt disjuncte. În consecință, există o situație în care un cuvânt afectat de $e + 1$ erori nu este decodat corect prin algoritmul de distanță minimă.

În general, teoria codurilor bloc corectoare de erori se poate dezvolta pentru acele coduri C care au o anumită *structură*. O astfel de situație este cea în care *alfabetul este un corp finit* F (cu q elemente⁸⁰, unde q este o putere a unui număr prim), iar codul $C \subseteq F^n$ este *subspațiu liniar* în F^n . Deși aceste condiții limitează drastic clasa codurilor pe care le studiem, această clasă este suficient de largă pentru a furniza coduri importante și eficiente, folosite pe scară largă în practică. În continuare presupunem că cititorul este familiarizat cu noțiuni și rezultate elementare de Algebră Liniară: spațiu liniar, dependență liniară, sistem de generatori, baze, dimensiune, produsul scalar standard în F -spațiul liniar F^n .

2.9 Definiție. Fie F un corp finit cu q elemente. Se numește *cod liniar* de lungime n peste F orice subspațiu liniar C al lui F^n . Cu alte cuvinte, C este o mulțime de cuvinte de lungime n în care simbolurile sînt elemente din F , închisă la adunarea (pe componente) din F^n și la înmulțirea cu scalari din F .⁸¹

Dimensiunea codului liniar C este dimensiunea lui C ca spațiu liniar peste F . Dacă $\dim C = k$ și distanța minimă a lui C este d , spunem că C este cod liniar *de tip* $[n, k, d]_q$ (sau *cod liniar q -ar de tip* $[n, k, d]$); n, k, d se numesc *parametrii* codului C .

Corpul finit cu q elemente este notat cu $\mathbb{F}_q$.

2.10 Exemplu. Codul „de repetiție de 3 ori” din exemplul 2.1 este $C = \{000, 111\}$, care este subspațiu în $\mathbb{F}_2^3$. Distanța minimă a lui C este 3, deci C este un cod liniar binar de tip $[3, 1, 3]_2$. Astfel, $e(C) = 1$, ceea ce a fost deja remarcat.

Pentru un cod C dat, determinarea distanței minime este foarte importantă. A priori, pentru aceasta ar trebui să considerăm toate distanțele $d(x, y)$ cu $x, y \in C$ distincte, adică $|C| \cdot (|C| - 1)/2$ distanțe, ceea ce este practic inabordabil (la codurile Reed-Solomon folosite în CD-uri, $|C|$ este în mod curent de ordinul 2^{240} sau mai mult). La coduri *liniare*, avem deja o sarcină ușurată:

⁸⁰ Foarte adesea, F este $\mathbb{F}_2$, corpul cu două elemente.

⁸¹ Condiția ca C să fie parte stabilă la înmulțirea cu scalari este redundantă pentru cazul corpului cu două elemente. De ce? Mai puteți da exemple de corpuri pentru care se întîmplă același fenomen?

2.11 Propoziție. Fie F un corp finit. Atunci distanța Hamming pe F^n este invariantă la translații: $d(x, y) = d(x + z, y + z)$, $\forall x, y, z \in F^n$. În particular, $d(x, y) = d(x - y, 0)$ și deci distanța minimă a unui cod liniar $C \leq F^n$ este:

$$d(C) = \min\{d(x, 0) \mid x \in C, x \neq 0\}.$$

□

Ponderea (Hamming) $\text{wt}(x)$ a unui cuvânt (vector) $x = x_1 \dots x_n \in F^n$ se definește ca numărul coordonatelor sale nenule (echivalent, $\text{wt}(x) = d(x, 0)$)⁸². Deci, distanța minimă a unui cod liniar este ponderea minimă nenulă a cuvintelor cod.

Cum putem preciza în mod concret un cod liniar? Există două moduri naturale de a da un subspațiu liniar C (un cod liniar) de dimensiune k în F^n : se dă o bază a lui C (adică se dau k vectori liniar independenți în C) sau se descrie C ca mulțimea soluțiilor unui sistem omogen de $n - k$ ecuații liniar independente:

2.12 Definiție. Fie $C \leq F^n$ un cod liniar de dimensiune $k \leq n$ peste corpul F . O matrice generatoare a lui C este o matrice $G \in M(k, n, F)$ ale cărei linii (văzute ca vectori în F^n) formează o bază în C (deci liniile lui G sînt liniar independente, adică $\text{rang } G = k$).

O matrice de paritate⁸³ a lui C este o matrice $H = (h_{ij}) \in M(n - k, n, F)$ astfel încît, $\forall x = (x_1, \dots, x_n) \in F^n$:

$$x \in C \Leftrightarrow h_{i1}x_1 + \dots + h_{in}x_n = 0, 1 \leq i \leq n - k.$$

Deci, pentru ca H să fie o matrice de paritate pentru codul C de dimensiune k , trebuie ca $\text{rang } H = n - k$ și să aibă loc: $x \in C \Leftrightarrow Hx^T = 0 \in M(n - k, 1, F)$.

2.13 Observație. Denumirea de matrice de paritate (parity-check matrix) provine din cazul particular al codului binar următor: se fixează $k \in \mathbb{N}^*$ și orice vector $x_1 \dots x_k \in \mathbb{F}_2^k$ este codat ca $x_1 \dots x_k x_{k+1}$, unde x_{k+1} este astfel încît $x_1 + \dots + x_k + x_{k+1} = 0$ (în $\mathbb{F}_2$). Codul este așadar $C = \{x_1 \dots x_k x_{k+1} \in \mathbb{F}_2^{k+1} \mid x_1 + \dots + x_k + x_{k+1} = 0\}$. Orice cuvînt cod are un număr par de biți egali cu 1 și de aceea bitul x_{k+1} este numit *bit de paritate*. Verificarea faptului că un cuvînt x este cuvînt cod revine la a verifica „paritatea” cuvîntului, adică un tip particular de sistem liniar omogen pe care îl satisfac coordonatele lui x . Determinați parametrii acestui cod!

Fie $\langle x, y \rangle = x_1 y_1 + \dots + x_n y_n$, $\forall x = (x_1, \dots, x_n), y = (y_1, \dots, y_n) \in F^n$ produsul scalar standard pe F^n ; dacă $S \subseteq F^n$, fie $S^\perp := \{y \in F^n \mid \langle x, y \rangle = 0, \forall x \in S\}$ ortogonalul lui S (doi vectori $x, y \in F^n$ se numesc *ortogonali* sau *perpendiculari* dacă $\langle x, y \rangle = 0$). Lăsăm ca exercițiu demonstrarea proprietăților următoare:

2.14 Teoremă. Fie C un cod liniar de tip $[n, k, d]$ peste corpul F . Atunci:

⁸² Notăția wt vine de la *weight* (greutate, pondere).

⁸³ Se mai folosește terminologia "matrice de control".

a) $C^\perp$ este un cod liniar de dimensiune $n - k$ (numit codul dual lui C).

b) $(C^\perp)^\perp = C$.

c) Dacă G este o matrice generatoare a lui C , atunci G este o matrice de paritate pentru $C^\perp$. Dacă H este matrice de paritate pentru C , atunci H este matrice generatoare pentru $C^\perp$. $\square$

Folosind noțiunea de ortogonalitate putem spune: $H \in M(n - k, n, F)$ este matrice de paritate pentru codul $C \leq F^n \Leftrightarrow$ liniile lui H sînt liniar independente și C este mulțimea vectorilor ortogonali pe liniile lui H (văzute ca vectori în F^n).

Observăm că un vector nenul în F^n poate fi ortogonal pe el însuși (de ex. $(1, 1)$ în $\mathbb{F}_2^2$), deci este posibil ca C și $C^\perp$ să aibă intersecție nenulă⁸⁴. Dacă $C = C^\perp$, C se numește *autodual*. Distanța minimă a unui cod liniar poate fi citită de pe matricea sa de paritate:

2.15 Teoremă. Fie C un cod liniar peste F și $H \in M(n - k, n, F)$ o matrice de paritate pentru C . Atunci distanța minimă d a lui C este

$$d = \min\{\delta \mid \text{există } \delta \text{ coloane în } H \text{ care sînt liniar dependente}\}.$$

Demonstrație. Fie $H_i \in F^{n-k}$ coloana i a lui H , $1 \leq i \leq n$. Avem $(x_1, \dots, x_n) \in C$ dacă și numai dacă $x_1 H_1 + \dots + x_n H_n = 0$. Fie $d' = \min\{\delta \mid \text{există } \delta \text{ coloane în } H, \text{ liniar dependente}\}$.

Fie $(x_1, \dots, x_n) \in C$, de pondere minimă d . Atunci coloanele H_i pentru care $x_i \neq 0$ (în număr de d) sînt liniar dependente, deci $d' \leq d$. Reciproc, fie o mulțime de d' coloane $\{H_i\}_{i \in J}$, liniar dependentă. Atunci există $(x_1, \dots, x_n) \in F^n$ cu $x_1 H_1 + \dots + x_n H_n = 0$ și $x_i \neq 0 \Rightarrow i \in J$. Deci $x = (x_1, \dots, x_n) \in C$ și $d \leq \text{wt}(x) \leq d'$. $\square$

Observăm că avem și

$$d = 1 + \max\{m \in \mathbb{N} \mid \text{orice } m \text{ coloane în } H \text{ sînt liniar independente}\}.$$

O clasă importantă de coduri corectoare de erori a fost descoperită de Hamming.

2.16 Definiție. (Coduri Hamming) Fie $F = \mathbb{F}_q$ și $r \in \mathbb{N}^*$ fixat. Definim *codul Hamming q -ar de redundanță r* , $H_{q,r}$, astfel:

Construim o matrice de paritate H care să aibă orice 2 coloane liniar independente, dar există 3 liniar dependente (deci distanța minimă a codului va fi 3). Alegem cîte un vector nenul din fiecare subspațiu de dimensiune 1 din F^r ; construim matricea H ce are drept coloane acești vectori (într-o ordine arbitrară). Matricea H este prin definiție matricea de paritate H a codului $H_{q,r}$.

Un alt mod de a exprima ideea de mai sus este: pe $F^r \setminus \{0\}$ definim o relație de echivalență: $x \sim y \Leftrightarrow \exists \alpha \in F^*$ astfel încît $y = \alpha x$. Din fiecare clasă de echivalență alegem cîte un vector⁸⁵. Acești vectori sînt coloanele matricei de paritate H .

⁸⁴ Adică, deși $\dim C + \dim C^\perp = n$, nu are loc în general $C \oplus C^\perp = F^n$. Ce puteți spune dacă F este de caracteristică 0?

Cîte coloane are H ? Se observă că clasele de echivalență de mai sus au fiecare cîte $q - 1$ elemente (clasa de echivalență a lui $x \in F^r \setminus \{0\}$ este $\{\alpha x \mid \alpha \in F^*\}$). Cum reuniunea lor (disjunctă) este $F^r \setminus \{0\}$, avem $q^r - 1 = n(q - 1)$, unde n este numărul claselor de echivalență.

Deci H are $n = (q^r - 1)/(q - 1)$ coloane și r linii.

Pentru ca $H \in M(r, n, K)$ să fie matrice de paritate, trebuie ca rang $H = r$. Există într-adevăr r coloane liniar independente în H , de exemplu (multipli scalari de) $(1, 0, \dots, 0)^T, (0, 1, \dots, 0)^T, \dots, (0, 0, \dots, 1)^T$.

2.17 Observație. Construcția de mai sus nu determină în mod unic matricea de paritate H . De exemplu, pentru două ordonări diferite ale coloanelor se obțin două matrice de paritate H, H' distincte și deci coduri Hamming corespunzătoare *distincte* C, C' . Însă aceste coduri sînt *echivalente pînă la o permutare*, în sensul că $\exists \sigma \in S_n$ (grupul permutărilor mulțimii $\{1, 2, \dots, n\}$) astfel încît $\forall x_1 \dots x_n \in F^n$, avem $x_1 \dots x_n \in C \Leftrightarrow x_{\sigma(1)} \dots x_{\sigma(n)} \in C'$.

Dacă în matricea de paritate H a codului Hamming C se înlocuiește coloana i (fie aceasta P_i) cu coloana αP_i , unde $\alpha \in F^*$, atunci se obține o matrice H' , de paritate pentru un cod C' astfel încît avem $x_1 \dots x_i \dots x_n \in C \Leftrightarrow x_1 \dots (\alpha^{-1} x_i) \dots x_n \in C$.

Această situație sugerează definirea unui alt tip de echivalență: două coduri C, C' de lungime n peste corpul F se numesc *diagonal echivalente* dacă $\exists (\alpha_1, \dots, \alpha_n) \in (F^*)^n$ astfel încît $\forall (x_1, \dots, x_n) \in F^n$, avem $(x_1, \dots, x_n) \in C \Leftrightarrow (\alpha_1 x_1, \dots, \alpha_n x_n) \in C'$. Două coduri C, C' care sînt echivalente (diagonal sau pînă la o permutare) au în esență „aceleași”⁸⁶ proprietăți: de exemplu, C este liniar $\Leftrightarrow C'$ este liniar.

Reuniunea celor două relații de echivalență pentru coduri de lungime n peste F se numește *echivalență monomială*. Deci, *codul Hamming $H_{q,r}$ este unic determinat pînă la o echivalență monomială*.

2.18 Exemplu. (codul binar Hamming $[7, 4, 3]$) Pentru $q = 2$ și $r = 3$, avem $n = 7$ și H este:

$$H = \begin{bmatrix} 1 & 0 & 1 & 0 & 1 & 0 & 1 \\ 0 & 1 & 1 & 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 & 1 & 1 & 1 \end{bmatrix}$$

În cazul $F = \mathbb{F}_2$, coloanele lui H sînt unic determinate pînă la o ordine a lor (fiecare subspațiu de dimensiune 1 din F^r are exact un vector nenul). Ordinea coloanelor adoptată aici este cea lexicografică (altfel spus, am scris „pe verticală” toate numerele nenule de 3 cifre în baza 2, în ordinea lor naturală). Acest cod are o importanță istorică deosebită:

Studiile superioare ale lui Hamming erau de matematică pură, iar teza sa de doctorat era despre ecuații diferențiale. A făcut parte din "Manhattan Project", proiectul ultrasecret de fabricare a bombei atomice de la Los Alamos din timpul celui de al doilea război mondial. În 1946 a plecat de la Los Alamos la Bell Laboratories :

⁸⁵ Se vede o legătură strînsă cu *spațiile proiective*.

⁸⁶ Enunțați cît mai multe proprietăți ale unui cod care se conservă prin echivalențele definite aici. Puteți defini și alte tipuri de echivalențe?

I was a pure mathematician – I felt somewhat lost at the place. Every once in a while I got terribly discouraged at the department being mostly electrical engineering.

La Bell Labs aveau un computer Model V, care ocupa 90 metri pătrați, cântărea 10 tone și putea rezolva sisteme liniare de 13 ecuații în mai puțin de 4 ore. Hamming avea acces doar în weekend la computer; cum nu exista personal de supraveghere în weekenduri, dacă computerul descoperea o eroare, abandona pur și simplu sarcina și trecea la următoarea.

Two weekends in a row I came in and found that all my stuff had been dumped and nothing was done. I was really aroused and annoyed because I wanted those answers and two weekends had been lost. And so I said “Damn it, if the machine can detect an error, why can’t it locate the position of the error and correct it?”

Codul pe care l-a descoperit Hamming este chiar codul binar tip $[7, 4, 3]$ de mai sus, care poate corecta o eroare la 7 simboluri. Nu este totdeauna de dorit să obținem coduri care să corecteze cât mai multe erori, deoarece rata de transmisie ar putea fi prea mică sau decodarea ar putea consuma prea mult timp. Este necesară obținerea de coduri suficient de bune pentru o anumită sarcină. Hamming spunea în legătură cu aceasta:

The Relay Computer, operating with a self-checking code, stops whenever an error is detected. Under normal operating conditions this amounts to two or three stops per day. However, if we imagine a comparable electronic computing machine operating 10^5 times the speed and with elements 10^5 times more reliable than relays, we find two to three hundred stops per day.

Putem spune că Hamming a prevăzut apariția atât a computerelor rapide de astăzi, cât și a sistemelor de operare Windows.

Să descriem o modalitate practică de codare și de decodare pentru acest cod $H_{2,3}$. Întrucât este un cod tip $[7, 4]$, fiecare mesaj de 4 biți este codat pe un cuvânt cod de 7 biți. Coordonatele unui cuvânt cod $d = d_1 \dots d_7 \in H_{2,3}$ satisfac ecuația $Pd^T = 0$, adică

$$\begin{aligned} d_1 + d_3 + d_5 + d_7 &= 0 \\ d_2 + d_3 + d_6 + d_7 &= 0 \\ d_4 + d_5 + d_6 + d_7 &= 0 \end{aligned} \quad (*)$$

Alegem biții d_1, d_2, d_4 să fie „de control”, iar biții mesajului original sînt plasați în pozițiile 3, 5, 6, 7. Biții d_1, d_2, d_4 se obțin din ecuațiile de mai sus, adică $d_1 = d_3 + d_5 + d_7$ etc.⁸⁷

La recepția unui cuvânt de 7 biți $r = r_1 \dots r_7$, se verifică dacă r este cuvânt cod (adică dacă $r_1, \dots, r_7$ satisfac ecuațiile (*)). Altfel spus, se calculează $(c_1, c_2, c_3) = H(r_1, \dots, r_7)^T$. Dacă $(c_1, c_2, c_3) = (0, 0, 0)$, atunci nu au avut loc erori. Dacă $(c_1, c_2, c_3) \neq (0, 0, 0)$, atunci eroarea (presupusă a fi singura) e plasată în bitul a cărui poziție este dată de numărul binar $c_3c_2c_1$ (și deci poate fi corectată!).⁸⁸

2.19 Propoziție. Fie $F = \mathbb{F}_q$ și $r \in \mathbb{N}^*$. Atunci codul Hamming $H_{q,r}$ este un cod liniar de lungime $n = (q^r - 1)/(q - 1)$, dimensiune $n - r$ și distanță minimă 3.

Demonstrație. Rămîne să vedem că distanța minimă este 3. Este clar că putem alege 3 coloane liniar dependente în H , de exemplu $(1, 0, \dots, 0)^T$, $(0, 1, \dots, 0)^T$, $(1, 1, \dots, 0)^T$, (ultima este suma primelor două). Orice două coloane sînt liniar independente din construcție. $\square$

2.20 Teoremă (inegalitatea Hamming). Fie C un cod q -ar de lungime n cu capacitate de corecție e . Atunci

⁸⁷ De ce s-a ales astfel poziția biților de control?

⁸⁸ Justificați această procedură de decodare!

$$|C| \sum_{i=0}^e C_n^i (q-1)^i \leq q^n.$$

Demonstrație. Sînt q^n elemente în A^n și $|C|$ cuvinte cod în C . Sferele de rază e centrate în cuvintele cod sînt disjuncte două cîte două, deci $|C| \cdot |S(x, e)| \leq q^n$. Se aplică propoziția 2.5. $\square$

Pentru orice cod C (nu neapărat liniar) de capacitate de corecție e , sferele centrate în cuvintele cod de rază e sînt disjuncte; dacă reuniunea lor este întreg F^n , atunci codul se numește *(e)-perfect*. Echivalent, *un cod este perfect dacă are loc egalitate în inegalitatea Hamming*.

2.21 Exercițiu. Orice cod e -perfect are distanță minimă $2e + 1$.

Codurile Hamming sînt *1-perfecte* (verificați!). Altfel spus, orice cuvînt din F^n se găsește la distanță ≤ 1 de exact un cuvînt cod. Acest fenomen are aplicații oarecum surprinzătoare.

2.22 Aplicație. *Jocul Pronosport* constă în ghicirea rezultatelor a 13 partide de fotbal. Rezultatul unei partide este un element al mulțimii $\{x, 1, 2\}$ (x = egalitate; 1 = cîștigă gazdele; 2 = cîștigă oaspeții). Jucătorii completează *variante*; numim variantă orice 13-uplu $(s_1, \dots, s_{13})$, cu $s_i \in \{x, 1, 2\}$. Pentru a cîștiga cu siguranță premiul I (13 rezultate exacte), este necesară a priori completarea a 3^{13} variante. Se pune întrebarea: *care este numărul minim de variante ce trebuie completate pentru a cîștiga cu siguranță premiul II (12 rezultate exacte)?*

Reformulăm problema în termenii teoriei codurilor: Fie $F = \mathbb{F}_3$, corpul cu 3 elemente. Să se găsească o submulțime (un cod) $S \subseteq F^{13}$ (cît mai „mică”), astfel încît orice cuvînt din F^{13} să se găsească la distanță cel mult 1 de un cuvînt din S . Altfel spus, să se găsească un cod *1-perfect* de lungime 13 peste $\mathbb{F}_3$.

Răspunsul este dat de codul Hamming cu $q = 3$ și $r = 3$: avem $n = (3^3 - 1)/2 = 13$, deci este un cod tip $[13, 10, 3]_3$. Numărul de cuvinte cod (de „variante”) este $3^{10} = 59049$.

2.23 Exercițiu. Scrieți o matrice de paritate pentru codul Hamming de mai sus.

2.24 Aplicație. *Problema pălăriilor*. Se dă o echipă de 3 persoane care joacă următorul joc: în mod aleator, pe capul fiecărei persoane se pune o pălărie roșie sau albastră, fără ca persoana să știe culoarea pălăriei. În schimb, fiecare poate vedea pălăriile tuturor celorlalți. Fiecare persoană ghicește culoarea pălăriei proprii sau se abține (spune „pas”). Echipa cîștigă dacă măcar o persoană a ghicit corect. Dacă toată lumea a greșit, echipa pierde; dacă toată lumea s-a abținut, echipa pierde.

Membrii echipei nu au voie să comunice între ei după ce au primit pălăriile; în schimb, pot stabili o strategie înaintea jocului.

Se pune problema de a determina o strategie optimă și probabilitatea de cîștig a echipei cu această strategie. O strategie evidentă, cu 50% șanse de cîștig, este de a desemna un membru al echipei care să ghicească la întîmplare, iar restul să se abțină. Se poate mai bine?

Pentru aceasta, să definim câteva noțiuni relativ la acest joc. Considerăm cazul mai general a n persoane, iar mulțimea culorilor o considerăm $C = \{0, 1\}$ ($0 = \text{roșu}$, $1 = \text{albastru}$).

Să numerotăm persoanele de la 1 la n . Fiecare persoană i ghicește în funcție de configurația de pălării pe care o vede la ceilalți. Vom defini deci :

- o *configurație* este un n -uplu de culori, adică un element $(x_1, \dots, x_n) \in C^n$.
- o *strategie* este o familie de funcții $\varphi = (\varphi_i)_{1 \leq i \leq n}$, cu $\varphi_i : C^{n-1} \rightarrow \{0, 1, \text{pas}\}$, cu sensul că: persoana i declară $\varphi_i(x_1, \dots, \widehat{x_i}, \dots, x_n)$, pentru o configurație dată $(x_1, \dots, x_n)$ (am notat cu $(x_1, \dots, \widehat{x_i}, \dots, x_n)$ faptul că x_i este omis din n -uplul $(x_1, \dots, x_n)$).
- configurația $(x_1, \dots, x_n) \in C^n$ este *configurație câștigătoare pentru strategia* $(\varphi_i)_{1 \leq i \leq n}$ dacă există i astfel încât $\varphi_i(x_1, \dots, \widehat{x_i}, \dots, x_n) = x_i$.
- *mulțimea câștigătoare pentru strategia* $\varphi = (\varphi_i)_{1 \leq i \leq n}$ este $W_\varphi = \{(x_1, \dots, x_n) \in C^n \mid (x_1, \dots, x_n) \text{ este configurație câștigătoare pentru } \varphi\}$.

Pentru $n = 3$, să considerăm următoarea strategie: dacă persoana i ($i \in \{1, 2, 3\}$) vede două pălării identice, ghicește culoarea opusă; dacă nu, spune *pas*⁸⁹. Configurațiile posibile sînt toate tripletele de forma 000, 001, ..., 111 (în număr de 8). Configurațiile în care se *pierde* sînt 000 și 111 (de ce?). Orice altă configurație este câștigătoare pentru această strategie (de ce?). Astfel, probabilitatea de câștig este: (numărul cazurilor favorabile)/(numărul total de cazuri) = $1 - 2/8 = 0,75$.

Observăm că mulțimea configurațiilor pierzătoare este chiar codul Hamming binar $H_{2,2}$, de tip $[3, 1, 3]$. Acest lucru nu este întâmplător.

În cazul general, este esențial următorul rezultat: Fie $W \subseteq C^n$. Atunci există o strategie φ astfel încât W este mulțime câștigătoare pentru φ dacă și numai dacă $P := C^n \setminus W$ are proprietatea:

$$\forall x \notin P, \exists x' \in P \text{ astfel încât } d(x, x') = 1. \quad (P)$$

Cu d s-a notat distanța Hamming. Proprietatea (P) înseamnă că: $\forall x = (x_1, \dots, x_n) \notin P$, există un i astfel încât, modificînd x_i (în $1 - x_i$), se obține cuvîntul $(x_1, \dots, 1 - x_i, \dots, x_n) \in P$.

Demonstrație. Presupunem W câștigătoare pentru φ . Fie $x = (x_1, \dots, x_n) \notin P$. Deci $x \in W$, adică $\exists i$ astfel încât $\varphi_i(x_1, \dots, \widehat{x_i}, \dots, x_n) = x_i$. Atunci $\varphi_i(x_1, \dots, \widehat{1 - x_i}, \dots, x_n) = \varphi_i(x_1, \dots, \widehat{x_i}, \dots, x_n) = x_i \neq 1 - x_i$, deci $x' := (x_1, \dots, 1 - x_i, \dots, x_n) \in P$, iar $d(x, x') = 1$.

Fie acum P cu proprietatea enunțată. Definim strategia $\varphi = (\varphi_i)_{1 \leq i \leq n}$ astfel:

Pentru $(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) \in C^{n-1}$, $\varphi_i(x_1, \dots, x_{i-1}, x_{i+1}, \dots, x_n) = \varepsilon$, unde ε este definit astfel:

- dacă $\exists x_i \in \{0, 1\}$ astfel încât $(x_1, \dots, x_{i-1}, x_i, x_{i+1}, \dots, x_n) \in P$, atunci $\varepsilon = 1 - x_i$.
- *pas*, în caz contrar.

⁸⁹ Definiți funcțiile φ_i pentru acest caz!

Demonstrăm că $W = C^n \setminus P$ este mulțime câștigătoare pentru φ . Fie $x = (x_1, \dots, x_n) \notin P$. Din proprietatea (P), există un i astfel încât $(x_1, \dots, 1 - x_i, \dots, x_n) \in P$. Atunci, conform strategiei de mai sus, $\varphi(x_1, \dots, \widehat{x_i}, \dots, x_n) = 1 - 1 + x_i = x_i$. $\square$

Astfel, a da o strategie φ revine la a da o mulțime P (o putem numi *pierzătoare* pentru φ) cu proprietatea (P). Pentru ca strategia să fie optimă, trebuie ca mulțimea câștigătoare $W = C^n \setminus P$ să fie cât mai mare, deci P să fie cât mai mică. Astfel, a găsi strategii optime revine la a găsi mulțimi P cu proprietatea (P), care să fie cât mai mici. Proprietatea (P) spune că reuniunea sferelor centrate în cuvintele din P , de rază 1, acoperă C^n . Altfel spus, să se găsească un cod 1-perfect de lungime n peste $C = \mathbb{F}_2$. Se vede analogia cu problema jocului Pronosport.

Pentru n de forma $2^r - 1$, o soluție este dată de codul Hamming H_{2^r-1} . Acest cod, de tip $[n, n-r, 3]$ are 2^{n-r} cuvinte, deci probabilitatea de câștig este $1 - 2^{n-r}/2^n = 1 - 2^{-r}$. De exemplu, pentru $n = 7$, probabilitatea este $1 - 2^{-3} = 7/8$.

O altă familie de coduri cu aplicații practice importante este următoarea.

2.25 Definiție (coduri Reed-Solomon). Fie q o putere a unui prim și $F = \mathbb{F}_q$. Fixăm un element primitiv $\alpha \in F^*$, (deci $F \setminus \{0\} = \{1, \alpha, \dots, \alpha^{q-2}\}$, α este de ordin $q-1$ în F^*) și k , $1 \leq k \leq q-1$. Codul Reed-Solomon $RS(k, q)$ este:

$$RS(k, q) := \{(f(1), \dots, f(\alpha^{q-2})) \in F^{q-1} \mid f \in F[X], \deg f \leq k-1\}$$

Se observă că $RS(k, q)$ este cod de lungime $n = q-1$ peste F . Notăm

$$L_{k-1} := \{f \mid f \in F[X], \deg f \leq k-1\}$$

L_{k-1} este un subspațiu liniar în $F[X]$, de dimensiune k . Atunci $RS(k, q)$ este imaginea aplicației de evaluare $ev : L_{k-1} \rightarrow F^{q-1}$, $ev(f) = (f(1), \dots, f(\alpha^{q-2}))$, care este evident liniară, deci $RS(k, q)$ este subspațiu liniar în F^{q-1} . Avem $\dim RS(k, q) = k$, căci ev este injectivă (orice $f \in L_{k-1}$ cu $ev(f) = (0, \dots, 0)$ are $q-1 > \deg f$ rădăcini și deci este 0). Ponderea (distanța) minimă a lui $RS(k, q)$ este $d = q - k = n - k + 1$ (exercițiu!), adică are loc egalitatea în inegalitatea de mai jos:

2.26 Teoremă. (inegalitatea Singleton) Fie C un cod de lungime n și distanță minimă d peste un alfabet A cu q simboluri. Atunci $|C| \leq q^{n-d+1}$. Dacă C este liniar, atunci $d \leq n - k + 1$.

Demonstrație. Rezultă din faptul că, pentru $(x_1, \dots, x_{n-d+1}) \in A^{n-d+1}$ fixat, există cel mult un cuvânt cod în C ale cărui coordonate de pe primele $n-d+1$ locuri sînt $(x_1, \dots, x_{n-d+1})$ (justificați!). $\square$

Codurile liniare pentru care $d = n - k + 1$ se numesc *coduri MDS* (Maximum Distance Separable) și sînt „cele mai bune” dintr-un anumit punct de vedere (distanța minimă a codului este maxim posibilă dacă dimensiunea și lungimea codului sînt fixate).

Codurile Reed-Solomon (RS) sînt deci MDS. Vom arăta că ele sînt adaptate la transmisia pe canale afectate de *pachete de erori* (în engleză *burst errors*): erorile apar mai probabil unele după altele (în „pachete”). Această situație apare adesea în practică, de pildă la stocarea datelor pe bandă sau CD (o zgîrietură pe CD afectează un șir de biți succesivi), comunicații radio etc.

Presupunem că mesajul inițial (necodat) este o succesiune de cuvinte de cîte k simboluri binare. Alegem un t astfel încît $q := 2^t > k$, punem F = corpul cu q elemente și folosim un cod $RS(k, q)$. Cum $|F| = 2^t$, există o bijecție între F și $\{0, 1\}^t$; putem atunci ca în fiecare cuvînt cod $c = (x_1, \dots, x_{q-1}) \in RS(k, q) \subseteq F^{q-1}$ să considerăm x_i ca un cuvînt de t cifre binare. Astfel, cuvîntul cod $c = (x_1, \dots, x_{q-1}) \in F^{q-1}$ este transmis ca un cuvînt binar w de lungime $t(q-1)$. Un pachet de b erori în cuvîntul binar w corespunde unui pachet de b/t erori în c , care poate fi corectat dacă $b/t \leq e$, unde $e = [(q-k-1)/2]$ este capacitatea de corecție a codului.

De exemplu, alegînd $k = 240$, $t = 8$, $q = 2^8 = 256$, $d = 16$, $e = 7$, se pot corecta pachete de 56 biți eronați. Prin tehnici de *concatenare* și *întreșesere*, se ajunge în practică la posibilitatea de corecție a circa 4000 erori binare (corespunzînd unei lungimi pe CD de 2,5 mm).

Teoria codurilor corectoare de erori este mult mai vastă decît am putut schița aici. Este un domeniu dinamic, în care se regăsesc în mod spectaculos și alte ramuri ale matematicii precum geometria algebrică, combinatorica, teoria grafurilor etc.

Exerciții

1. Fie F un corp cu q elemente, $n \in \mathbb{N}$ și $m < q^n$. Cîte coduri de lungime n peste F cu m cuvinte există? Cîte din acestea sînt liniare? (Ind. Dacă m nu este de forma q^k , nu există subspații liniare cu m elemente în F^n . Dacă $m = q^k$, trebuie găsit numărul subspațiilor liniare de dimensiune k din F^n .)

2. (Coduri de repetiție) Considerăm următorul procedeu de codare: pentru a coda cuvinte oarecare de lungime k (peste alfabetul binar $\{0, 1\} = F$) se repetă fiecare bit de r ori; astfel, orice cuvînt $x_1 \dots x_k$ este codat ca $x_1 \dots x_1 x_2 \dots x_2 \dots x_k \dots x_k$ (fiecare x_i apare de r ori). Se obține un cod de lungime kr .

a) Arătați că acest cod este liniar, de dimensiune r .

b) Arătați că distanța sa minimă este r .

c) Folosim codul de repetiție de tip $[3, 1]$. Dacă se primește mesajul 000101111100, unde au apărut erori? Corectați-le.

d) Care este rata de transmisie a codului de repetiție tip $[kr, r]$?

3. Scrieți toate cuvintele codului Hamming $H_{2,2}$. Care este rata sa de transmisie?

4. Scrieți toate cuvintele codului binar Hamming tip $[7, 4, 3]$. Care este rata sa de transmisie?
5. Calculați numărul de cuvinte și rata de transmisie ale codului Hamming $H_{q,r}$ (în general) și pentru $q = 2, r \leq 5$.
6. Fie C un cod liniar de tip $[n, k, d]$ peste F , corp cu q elemente.
- a) Arătați că: ori toate cuvintele din C încep cu 0, ori exact $1/q$ din cuvinte încep cu 0. (Ind. Fie $D := \{x_1 \dots x_n \in F^n \mid x_1 = 0\}$, subspațiu liniar în F^n . Aplicați formula pentru $\dim(C + D)$).
- b) Demonstrați că suma ponderilor tuturor cuvintelor lui C este cel mult $n(q-1)q^{k-1}$.
- c) Demonstrați că $d \leq \frac{n(q-1)q^{k-1}}{q^k - 1}$. (Ind. Distanța minimă este mai mică decât media ponderilor cuvintelor nenule.)
- d) (Inegalitatea Plotkin) Demonstrați că, dacă $\frac{d}{n} > \frac{q-1}{q}$, atunci $|C| \leq \frac{d}{d - \frac{q-1}{q}n}$.
7. Demonstrați că dualul unui cod liniar MDS este tot cod MDS.
8. Demonstrați că un cod binar MDS de lungime n este unul din următoarele: un cod de repetiție, codul de paritate sau tot spațiul $\mathbb{F}_2^n$.

VI. Acțiuni ale grupurilor

VI.1. Acțiuni ale grupurilor pe mulțimi

Conceptul de grup este strâns legat de noțiunea de *acțiune*. Cauchy are ideea de a privi substituțiile (permutările) unei mulțimi ca obiecte în sine și observă că aceste substituții se pot compune. Lagrange studiasse deja comportarea polinoamelor la permutarea nedeterminatelor; mai precis, „acțiunea” unei permutări a nedeterminatelor asupra unui polinom dat. Galois duce această idee mai departe și o utilizează în studiul rezolvabilității ecuațiilor polinomiale, studiind acțiunile permutărilor asupra rădăcinilor ecuației. Tot la Galois apare utilizarea termenului de *grup* de permutări și folosirea unui singur simbol pentru a nota o permutare.

1.1 Exemplu. Fie polinomul (în 4 nedeterminate) $p = X_1 + X_2 + X_3 + X_4$. Oricum am permuta cele 4 nedeterminate, polinomul p rămâne același. În schimb, pentru $q = X_1X_2 + X_3X_4$, putem obține prin permutarea nedeterminatelor polinoamele: $X_1X_3 + X_2X_4$, $X_1X_4 + X_2X_3$ și, bineînțeles, polinomul inițial $X_1X_2 + X_3X_4$.

Lagrange a demonstrat că, pentru orice polinom p de n nedeterminate, numărul polinoamelor ce se pot obține din p prin permutarea nedeterminatelor este un divizor al lui $n!$. Vom vedea că acest enunț este un caz particular al cunoscutei teoreme (numită chiar „Teorema lui Lagrange”): *ordinul oricărui subgrup al unui grup finit divide ordinul grupului*.

1.2 Definiție. Fie $(G, \cdot)$ un grup, e elementul său unitate și X o mulțime. Spunem că este dată o *acțiune la stînga a lui G pe X* (sau că grupul G *acționează la stînga pe X* , sau că X este o *G -mulțime*) dacă este definită o funcție $\varphi : G \times X \rightarrow X$, cu următoarele proprietăți (notăm cu gx elementul $\varphi(g, x) \in X$, $\forall g \in G$, $\forall x \in X$):

- a) $(gh)x = g(hx)$, $\forall g, h \in G$, $\forall x \in X$;
- b) $ex = x$, $\forall x \in X$.

Dacă se dă o funcție $\varphi : X \times G \rightarrow X$ (notăm cu xg elementul $\varphi(x, g) \in X$), astfel încît:

- a') $x(gh) = (xg)h$, $\forall g, h \in G$, $\forall x \in X$;
- b') $xe = x$, $\forall x \in X$,

spunem că grupul G acționează la dreapta pe X .

Dacă G acționează la stînga pe X , iar $g \in G$, fie $\varphi_g : X \rightarrow X$ aplicația dată de $\varphi_g(x) = gx$, $\forall x \in X$. Observăm că φ_g este o bijecție, deoarece avem, $\forall x \in X$, $x = (gg^{-1})x = g(g^{-1}x) = (\varphi_g \circ \varphi_{g^{-1}})(x)$, deci $\varphi_g \circ \varphi_{g^{-1}} = \text{id}$ (la fel, $\varphi_{g^{-1}} \circ \varphi_g = \text{id}$); astfel, $\varphi_{g^{-1}}$ este inversa lui φ_g . Acest fapt conduce la următoarea:

1.3 Observație. Notăm cu $S(X)$ grupul permutărilor mulțimii X (numit și *grupul simetric* pe X), adică :

$$S(X) = \{\sigma : X \rightarrow X \mid \sigma \text{ bijecție}\}.$$

Operația cu care este înzestrat $S(X)$ este compunerea uzuală a funcțiilor: $\forall \sigma, \tau \in S(X)$, $(\sigma \circ \tau)(x) = \sigma(\tau(x))$, $\forall x \in X$.

A da o acțiune la stînga a lui G pe X revine la a da un morfism de grupuri $\lambda : G \rightarrow S(X)$.

Într-adevăr, dacă G acționează la stînga pe X , definim $\lambda : G \rightarrow S(X)$ prin $\lambda(g) = \varphi_g$, $\forall g \in G$. Am văzut mai sus că $\varphi_g \in S(X)$. A spune că λ este morfism este o altă formulare a proprietății a) din definiție. Reciproc, dacă $\lambda : G \rightarrow S(X)$ este morfism de grupuri, definim $gx = \lambda(g)(x)$, $\forall g \in G, \forall x \in X$. Se verifică imediat că se obține o acțiune la stînga a lui G pe X .

1.4 Observație. *A da o acțiune la dreapta a lui G pe X revine la a da un morfism de grupuri $\rho : G \rightarrow S(X)^{\text{op}}$, unde $S(X)^{\text{op}} = (S(X), *)$ este grupul „opus” lui $S(X)$, adică mulțimea $S(X)$ înzestrată cu operația de compunere a funcțiilor „scrise la dreapta argumentului”:* $(\sigma * \tau)(x) = \tau(\sigma(x))$, $\forall x \in X$.⁹⁰

În continuare, vom considera acțiuni la stînga, cazul acțiunilor la dreapta fiind asemănător (cf. exercițiul 1). Introducem următoarea terminologie, inspirată din interpretarea „dinamică” a acțiunilor grupale:

1.5 Definiție. Fie $(G, \cdot)$ un grup, X o mulțime pe care G acționează și $x \in X$. Mulțimea:

$$\mathcal{O}_x = \{gx \mid g \in G\}$$

este numită *orbita* (sau *traietoria*) lui x (sub acțiunea lui G). Elementul x se numește *fixat* de $g \in G$ (sau *punct fix al lui g*) dacă $gx = x$. Dacă $gx = x$, $\forall g \in G$ (echivalent, $\mathcal{O}_x$ are un singur element), x este numit *punct fix al acțiunii lui G* . Notăm cu $\text{Fix}_G(X)$ mulțimea punctelor fixe ale acțiunii lui G pe X .

Pentru orice $x \in X$, definim *stabilizatorul lui x în G* (sau *grupul de izotropie al lui x în G*), $\text{Stab}_G(x) := \{g \in G \mid gx = x\}$ (notat uneori și G_x). Vom omite indicele G dacă nu este pericol de confuzie, scriind $\text{Stab}(x)$.

⁹⁰ Această compunere a funcțiilor este naturală dacă se scrie $(x)\sigma$ în loc de $\sigma(x)$: avem $(x)(\sigma * \tau) = ((x)\sigma)\tau$.

1.6 Exemple. a) Fie R un inel comutativ și n un număr natural, $n \geq 2$. Grupul S_n al permutărilor mulțimii $\{1, 2, \dots, n\}$ acționează asupra mulțimii $R[X_1, \dots, X_n]$ (inelul polinoamelor de n nedeterminate cu coeficienți în R), astfel :

$$\forall \sigma \in S_n, \forall p(X_1, \dots, X_n) \in R[X_1, \dots, X_n], (\sigma p)(X_1, \dots, X_n) := p(X_{\sigma(1)}, \dots, X_{\sigma(n)}).$$

Punctele fixe ale acțiunii lui S_n sunt polinoamele simetrice. La Exemplul 1, polinoamele listate reprezintă orbita lui $X_1X_2 + X_3X_4$ sub acțiunea lui S_4 .

b) Orice grup G acționează asupra mulțimii G prin *translații la stînga*: $\forall g \in G, \forall x \in X, gx := gx$ (înmulțirea lui g cu x în grupul G). O altă acțiune a lui G pe G este prin *conjugare*: $\forall g \in G, \forall x \in X, g * x := gxg^{-1}$. De obicei, acțiunea prin conjugare se consideră *la dreapta* definindu-se $x^g := g^{-1}xg, \forall g \in G, \forall x \in G$. Un element $x \in G$ are orbita formată dintr-un singur element $(x) \Leftrightarrow x \in C(G)$ (centrul lui G , elementele care comută cu toate elementele lui G).

c) Iată un exemplu din teoria ecuațiilor diferențiale. Fie $u: \mathbb{R}^n \rightarrow \mathbb{R}^n$ o funcție cu proprietatea că, $\forall p \in \mathbb{R}^n$, problema Cauchy

$$x'(t) = u(x(t)), \quad x(0) = p \quad (1)$$

are o unică soluție $x_p: \mathbb{R} \rightarrow \mathbb{R}^n$. De pildă, o condiție suficientă ca u să satisfacă proprietatea cerută este ca u să fie lipschitziană pe $\mathbb{R}^n$ ($\exists C > 0$ astfel încît $\|u(x) - u(y)\| \leq C\|x - y\|, \forall x, y \in \mathbb{R}^n$). Pentru detalii, vezi, de exemplu, BARBU [1985].

Definim atunci acțiunea "*" a grupului $(\mathbb{R}, +)$ pe $\mathbb{R}^n$ prin: $t * p = x_p(t), \forall t \in \mathbb{R}, \forall p \in \mathbb{R}^n$.

Să verificăm că am definit o acțiune. Avem de arătat că $(t + s) * p = t * (s * p), \forall s, t \in \mathbb{R}, \forall p \in \mathbb{R}^n$, adică $x_p(t + s) = x_{s * p}(t) = x_{x_p(s)}(t)$. Pentru s fixat, funcția $z(t) := x_p(t + s)$ este soluție a problemei

$$z'(t) = u(z(t)), \quad z(0) = x_p(s).$$

Dar soluția acestei probleme este unică și am notat-o $x_{x_p(s)}(t)$. Deci avem egalitatea de funcții $x_{x_p(s)}(t) = z(t) = x_p(t + s)$.

Avem și $0 * p = x_p(0) = p, \forall p \in \mathbb{R}^n$.

O interpretare a acestei acțiuni este următoarea: problema (1) definește, pentru orice $p \in \mathbb{R}^n$, o *traietorie* a unui punct material M în $\mathbb{R}^n$ care, la momentul $t = 0$, este în punctul p . Rezultatul acțiunii lui t asupra lui p este poziția punctului M la momentul t .

d) **Izometrii.** Acest exemplu este extrem de sugestiv în ilustrarea faptului că *grupurile sînt o măsură a simetriei*.

Fie (X, d) un spațiu metric. O funcție bijectivă $T: X \rightarrow X$ care „păstrează distanțele”, adică $\forall x, y \in X, d(T(x), T(y)) = d(x, y)$, se numește *izometrie*.

Condiția de bijectivitate este importantă pentru a putea defini *grupul izometriilor lui X* , $\text{Izom}(X) := \{T: X \rightarrow X \mid T \text{ izometrie}\}$. Mai general, pentru orice submulțime $Y \subseteq X$, se

definește *grupul de simetrie al lui Y* , $S(Y) := \{T: X \rightarrow X \mid T(Y) = Y\}$.⁹¹ Există spații metrice și aplicații care păstrează distanțele, dar nu sînt izometrii (vezi Exercițiile). Deci $\text{Izom}(X)$ este un subgrup al grupului tuturor permutărilor lui X (o permutare este o bijecție definită pe X cu valori în X).

Luînd $X = \mathbb{R}^2$, cu distanța euclidiană, $\text{Izom}(\mathbb{R}^2)$ este un grup care conține cu siguranță *translațiile de vector oarecare, simetriile față de o dreaptă dată și rotațiile în jurul unui punct dat*.

Fie $u \in \mathbb{R}^2$. Translația de vector u este funcția $T_u: \mathbb{R}^2 \rightarrow \mathbb{R}^2$, $T_u(v) = u + v$, $\forall v \in \mathbb{R}^2$.

Simetria față de dreapta d duce orice punct $P \in \mathbb{R}^2$ în „simetricul său față de dreapta d ” (unicul punct $S_d(P)$ cu proprietatea că d este mediatoarea segmentului $PS_d(P)$).

Rotația de unghi α în jurul punctului C duce un punct oarecare P în punctul $P' = R_{C, \alpha}(P)$ cu proprietatea că $d(C, P) = d(C, P')$ și unghiul orientat (în sens trigonometric) $\widehat{PCP'}$ are măsura α .

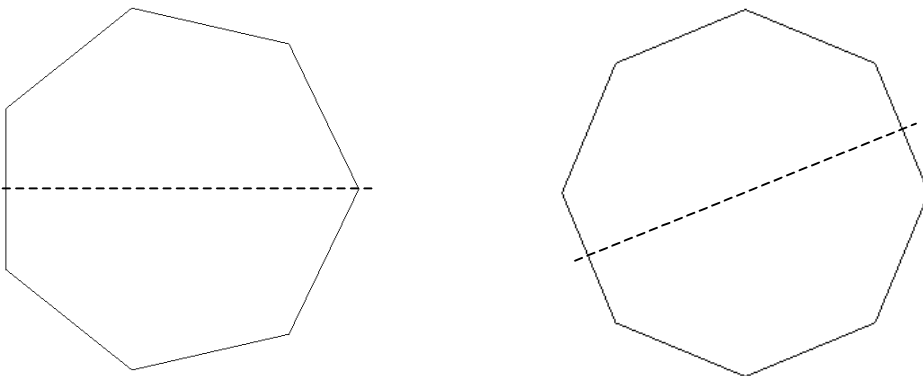
Observăm că izometria identitate este și rotație (de unghi 0) și translație (de vector 0). Are loc următoarea teoremă importantă:

O izometrie oarecare a planului este o translație urmată de o rotație și eventual de o simetrie față de o dreaptă. (pentru demonstrație, vezi Exerciții)

Pentru teoria grupurilor este important grupul de simetrie al unui *poligon regulat cu n laturi*, numit grupul diedral D_n .

1.7 Propoziție. *Fie O centrul cercului circumscris unui poligon regulat cu n laturi. Grupul diedral D_n are $2n$ elemente și este generat de rotația ρ de unghi $2\pi/n$ și de simetria σ față de o axă de simetrie a poligonului (o axă de simetrie a poligonului este o dreaptă ce unește centrul cercului circumscris cu un vîrf dacă n este impar și o mediatoare a unei laturi dacă n este par). Aceste izometrii satisfac relațiile $\rho^n = \sigma^2 = \text{id}$ și $\sigma\rho = \rho^{n-1}\sigma$. $\square$*

Pentru detalii, vezi Exercițiile. Iată heptagonul regulat și octogonul regulat, cu cîte o axă de simetrie:



⁹¹ Arătați că $\text{Izom}(X)$ este grup și $S(Y)$ este subgrup al său.

Proprietăți elementare ale acțiunilor grupurilor pe mulțimi sînt colectate în:

1.8 Propoziție. Fie G un grup care acționează pe o mulțime X . Atunci au loc afirmațiile:

a) Definind $x \sim y \Leftrightarrow \exists g \in G$ astfel încît $y = gx$, se obține o relație de echivalență pe X . Clasa de echivalență a unui element x este orbita lui x , O_x .

b) Pentru orice $x \in X$, $\text{Stab}(x)$ este un subgrup al lui G . Notînd cu $G/S \text{Stab}(x)$ mulțimea claselor la stînga ale lui G relativ la $\text{Stab}(x)$ (adică $\{g \cdot \text{Stab}(x) \mid g \in G\}$), aplicația $\alpha: G/S \text{Stab}(x) \rightarrow O_x$, $\alpha(g \cdot \text{Stab}(x)) = gx$ ($\forall g \in G$) este bine definită și este o bijecție. În particular, avem

$$|O_x| = [G : \text{Stab}(x)]$$

(cardinalul orbitei lui x este indicele stabilizatorului lui x în G).

c) Fie S un sistem de reprezentanți pentru orbitele lui G în X care au cel puțin 2 elemente. Altfel spus, orice element din X este sau în $\text{Fix}_G(X)$, sau în orbita unui unic element din S . Atunci

$$X = \text{Fix}_G(X) \cup \bigcup_{a \in S} O_a \text{ (reuniune disjunctă)}$$

Trecînd la cardinali, rezultă relația:

$$|X| = |\text{Fix}_G(X)| + \sum_{a \in S} [G : \text{Stab}(a)]$$

Demonstrație. Exercițiu. □

Se pune problema calculării numărului de orbite al unei acțiuni.

1.9 Definiție. Pentru orice $g \in G$, notăm cu $\text{Fix}(g) := \{x \in X \mid gx = x\}$ mulțimea acelor $x \in X$ fixați de g . Mai general, dacă $T \subseteq G$, punem $\text{Fix}(T) = \{x \in X \mid gx = x, \forall g \in T\}$. Observăm că $\text{Fix}(g) = \text{Fix}(\langle g \rangle)$, unde $\langle g \rangle$ este subgrupul generat de g .

1.10 Propoziție. (Lema lui Burnside) Fie G un grup finit care acționează pe o mulțime finită X . Atunci numărul k al orbitelor în X sub acțiunea lui G este „numărul mediu de puncte fixate” :

$$k = \frac{1}{|G|} \sum_{g \in G} |\text{Fix}(g)|.$$

Demonstrație. Considerăm mulțimea $M := \{(g, x) \in G \times X \mid gx = x\}$. Calculăm $|M|$.

Observăm că $(g, x) \in M \Leftrightarrow g \in \text{Stab}(x)$; deci $M = \bigcup_{x \in X} \text{Stab}(x) \times \{x\}$ (reuniune disjunctă). Astfel,

$$|M| = \sum_{x \in X} |\text{Stab}(x)| = \sum_{x \in X} \frac{|G|}{[G : \text{Stab}(x)]} = \sum_{x \in X} \frac{|G|}{|O_x|}.$$

Însă X este reuniunea disjunctă a celor k orbite în X sub acțiunea lui G (fie acestea $T_1, \dots, T_k$); putem scrie în continuare:

$$|M| = \sum_{i=1}^k \sum_{x \in T_i} \frac{|G|}{|O_x|} = \sum_{i=1}^k \sum_{x \in T_i} \frac{|G|}{|T_i|} = \sum_{i=1}^k |G| = k \cdot |G|.$$

Pe de altă parte, $\forall g \in G, (g, x) \in M \Leftrightarrow x \in \text{Fix}(g)$, deci $M = \bigcup_{g \in G} \{g\} \times \text{Fix}(g)$ (reuniune disjunctă), deci:

$$|M| = \sum_{g \in G} |\text{Fix}(g)|.$$

Comparînd cele două expresii pentru $|M|$, obținem formula. □

Aplicații

a) „Problema coroanei”. Fie $m, n \in \mathbb{N}$. Se consideră o coroană cu m vîrfuri (vîrfurile coroanei sînt vîrfurile unui poligon regulat cu m laturi). Se dau perle de n culori, în cantități suficiente. Cîte modele de coroană distincte se pot crea atașînd perle în fiecare vîrf al coroanei?

Soluție. În fiecare din cele m vîrfuri putem pune n culori, ceea ce dă n^m posibilități. Dar acesta nu e răspunsul corect: două astfel de configurații dau coroane identice dacă se obțin una din alta printr-o rotație a coroanei.

Traducem problema în termeni de *acțiuni ale grupurilor pe mulțimi*.

Se consideră X mulțimea colorărilor cu n culori a vîrfurilor unui poligon regulat cu m laturi, de centru O . Considerăm $X = \{(c_0, \dots, c_{m-1}) \mid c_i \in \{1, 2, \dots, n\}\}$; c_i este "culoarea vîrfului i ". Fie R_m grupul rotațiilor planului (în jurul lui O) de unghiuri multiplu de $2\pi/m$. R_m este un grup ciclic cu m elemente, $R_m = \{r_0, r_1, \dots, r_{m-1}\}$ unde r_k este rotația de unghi $2k\pi/m$.

G acționează asupra lui X . Cu notațiile de mai sus, avem $r_{-k}(c_0, \dots, c_{m-1}) = (c_k, \dots, c_{m-1+k})$ (indicii se consideră modulo m , adică $c_t = c_i, \forall t \in \mathbb{Z}$, unde i este restul împărțirii lui t la m).

Două colorări dau aceeași coroană dacă și numai dacă sînt în aceeași orbită a acestei acțiuni. Deci numărul orbitelor lui R_m în X este numărul cerut.

Pentru a găsi numărul de orbite, aplicăm lema lui Burnside. Fie $r_k \in R_m$; calculăm $|\text{Fix}(r_k)|$.

Fie $d = (k, m)$; atunci $\langle r_k \rangle = \langle r_d \rangle$ (demonstrați!). Cum $\text{Fix}(r_k) = \text{Fix}(\langle r_k \rangle) = \text{Fix}(\langle r_d \rangle) = \text{Fix}(r_d)$, calculăm $|\text{Fix}(r_d)|$. Dacă $(c_0, \dots, c_{m-1})$ este o colorare invariata de r_d , atunci $c_0 = c_d = c_{2d} = \dots = c_{id}, \forall i \in \mathbb{Z}$; în general, fixarea unei culori a unui vîrf determină culorile a m/d vîrfuri. Astfel, putem alege d vîrfuri distincte pe care să le colorăm arbitrar (de ex. $c_0, \dots, c_{d-1}$), culorile celelalte fiind determinate de faptul că $(c_0, \dots, c_{m-1})$ este o colorare invariata de r_d . Sînt $n^d = n^{(k, m)}$ posibilități de colorare, deci $|\text{Fix}(r_k)| = n^{(k, m)}$. Formula lui Burnside dă numărul de orbite:

$$\frac{1}{m} \sum_{k=1}^m n^{(k, m)}$$

Propunem cititorului să trateze direct (fără a folosi formula de mai sus) cazul $m = 5, n = 3$.

b) „Problema colierului”. Fie $m, n \in \mathbb{N}$. Cîte coliere distincte formate din m perle de n culori se pot fabrica? Se presupune că există suficiente perle de fiecare culoare.

Indicație. Aici acționează grupul diedral D_m (al simetriilor unui poligon regulat cu m laturi) asupra mulțimii X a colorărilor (colierul poate fi și „întors”, spre deosebire de coroană). D_m

are ca subgrup grupul R_m al rotațiilor, dar conține și reflecții față de drepte care trec prin centrul O . Se disting cazurile m par și m impar.

c) În câte moduri se poate scrie 1000 ca un produs de trei numere naturale (la un produs dat nu contează ordinea factorilor)?

Exerciții

1. Fie $(G, \cdot)$ un grup și $(G^{\text{op}}, *)$ grupul opus lui G , adică mulțimea G înzestrată cu operația $x*y := y \cdot x$, $\forall x, y \in G$. Arătați că $(G^{\text{op}}, *)$ este grup și că a da o acțiune la stînga a lui G pe o mulțime X este echivalent cu a da o acțiune la dreapta a lui G^{op} pe X .

2. Fie M mulțimea șirurilor reale mărginite. Arătați că M este un spațiu liniar normat în raport cu norma $\|(x_n)_{n \geq 1}\| = \sup\{|x_n| \mid n \geq 1\}$. Dați exemplu de funcție $\varphi: M \rightarrow M$ care păstrează norma (deci și distanțele), dar care nu este bijecție.

3. Fie T o izometrie a planului. Demonstrați că:

a) T duce dreapta AB în dreapta $T(A)T(B)$.

b) Dacă T are trei puncte necoliniare fixe, atunci T este identitatea. Deduceți că o izometrie este determinată de imaginile a trei puncte necoliniare.

c) Dacă T are două puncte fixe A și B și $T \neq \text{id}$, atunci T este simetria față de dreapta AB .

d) Dacă T are exact un punct fix O , atunci T este o rotație în jurul lui O .

4. Două figuri plane (submulțimi ale planului) X și Y se numesc *congruente* dacă există o izometrie T a planului astfel încît $Y = T(X)$. Arătați că, dacă X și Y sînt congruente, atunci grupurile lor de simetrie sînt izomorfe. Reciproca este adevărată?

5. Fie X un spațiu metric și $Y \subseteq X$, $|Y| = n$. Atunci grupul de simetrie $S(Y)$ este izomorf cu un subgrup al grupului simetric S_n (grupul permutărilor de n obiecte).

6. Fie O centrul cercului circumscris unui poligon regulat cu n laturi $A_0A_1 \dots A_{n-1}$ și φ o izometrie din grupul său de simetrie D_n . Demonstrați că:

a) $\forall i, 0 \leq i \leq n-1$, are loc $\varphi(O) = O$ și $\varphi(A_i) \in \{A_0, A_1, \dots, A_{n-1}\}$. Deduceți că D_n este un subgrup în S_n .

b) φ este determinat de imaginile a două vîrfuri consecutive. În plus, dacă $\varphi(A_0) = A_i$, atunci $\varphi(A_1)$ este unul din vîrfurile adiacente cu A_i .

c) Deduceți că D_n are cel mult $2n$ elemente.

d) Fie ρ rotația de unghi $2\pi/n$ în jurul lui O și σ simetria față de o axă de simetrie a poligonului. Atunci elementele: $\text{id}, \rho, \rho^2, \dots, \rho^{n-1}, \sigma, \rho\sigma, \rho^2\sigma, \dots, \rho^{n-1}\sigma$ sînt distincte.

e) Scrieți tabla operației grupului D_n .

Index

A

acțiune a unui grup, 136, 137
alfabet, 123
algebra
 factor, 71
algebră, 69
algebric (element), 82
algoritm de distanță minimă, 125
algoritm de factorizare, 114
algoritm extins al lui Euclid, 102
algoritmul lui Euclid, 101
Algoritmul lui Euclid, 101
apartenență, 11
aplicație, 21
 crescătoare, 36
argument, 21
asociere în divizibilitate, 97
axioma
 alegerii, 38
 extensionalității, 15
 fundării, 38
 inducției, 27
 infinității, 28
 mulțimii părților, 16
 reuniunii, 16
axioma-schemă a substituției, 16
axiome, 15
axiomele Dedekind-Peano, 27

B

bilă, 65
bine ordonată (mulțime), 92

C

canal de transmisie, 123
canal q -ar simetric de probabilitate p , 123
capacitatea de corecție a unui cod, 125
caracteristica unui inel, 90
cardinal, 39
cel mai mare divizor comun, 98
cel mai mic multiplu comun, 98
centrul unui inel, 69
cît, 101
clasa
 ordinalelor, 29
clasă, 19
 bine ordonată, 30
clasă de echivalență, 43
cmmdc, 98
cmmmc, 98
cod, 124
 Hamming, 128
 perfect, 131
cod liniar, 126
codomeniul unei funcții, 21
coduri
 diagonal echivalente, 129
 echivalente pînă la o permutare, 129
coeficient al unui polinom, 78

coeficientul dominant, 78
 comaximale, 57
 compunerea a două relații, 23
 conectori, 11
 conjugare, 138
 conjuncția, 11
 constantă, 11
 corp
 algebric închis, 84
 corpul fracțiilor raționale, 49, 51, 91
 corpul total de fracții, 49
 cuantificatori, 11
 cuantori, 11
 cuplu, 20
 cuvânt cod, 124

D

definiții prin recurență, 33
 derivată (formală), 111
 diferență, 18
 dimensiunea unui cod liniar, 126
 disjuncția, 11
 distanța Hamming, 124
 distanța minimă a unui cod, 125
 distanță, 65
 divizor al lui zero, 48
 domeniu de integritate, 96
 domeniul unei funcții, 21

E

egalitate, 11
 element
 întreg, 118
 enunț, 11
 exponentul unui grup, 90
 expresie, 11
 expresii echivalente, 13
 extensiune, 18

extindere de corpuri, 80

F

familie de mulțimi, 22
 figuri congruente, 142
 formă, 78
 fracție, 48
 fracție rațională
 simetrică, 91
 funcția identică, 21
 funcția polinomială, 117
 funcție, 21
 bijectivă, 23
 identitate, 24
 injectivă, 23
 inversabilă, 23
 surjectivă, 23

G

GCD-inel, 98
G-mulțime, 136
 grad, 77
 al unui element, 84
 total, 78
 graficul
 unei funcții, 22
 grup
 al izometriilor, 138
 de simetrie, 139
 grupul diedral, 139

I

ideal
 al unei *R*-algebre, 71
 maximal, 54
 prim, 54
 Identitățile lui Newton, 94
 imagine, 22

imagine printr-o relație funcțională, 17

inducție

transfinită, 33

inel

euclidian, 101

factorial, 105

integru, 96

principal, 102

infimum, 26

intersecție, 18

a unei familii, 23

inversa

unei relații, 23

inversa unei funcții, 23

irreductibil, 100

izometrie, 138

izomorfism

de ordine, 36

L

lanț, 25

latice, 26

completă, 26

lema chineză a resturilor, 57

Lema lui Zorn, 39

lexicografică (ordine), 93

liber de pătrate, 115

localizatul, 50

lungimea unui cod, 124

M

majorant, 25

majorată (submulțime), 25

maximal (element), 26

metrică, 65

minorant, 25

minorată (submulțime), 25

model, 37

modul (funcția), 51

monom, 75

dominant, 93

morfism

de algebre, 70

de ordine, 36

morfism structural (al unei algebre), 70

mulțime, 9

bine ordonată, 26

finită, 39

inductiv ordonată, 39

infinită, 39

numărabilă, 39

ordonată, 25

total ordonată, 25

mulțime cât, 43

mulțime factor, 43

mulțimea vidă, 17

mulțimi

cardinal echivalente, 39

echipotente, 39

N

negația, 11

normă, 65

noțiuni primare, 15

numărător, 48

nume constant, 11

nume variabil, 11

numitor, 48

O

orbită, 137

ordin de multiplicitate, 110

ordinal, 28, 36

finit, 31

infinit, 31

limită, 40

predecesor, 31
 succesor, 31
 ordine
 lexicografică, 60

P

parametrii (unui cod), 126
 partiție
 a unei mulțimi, 43
 pereche ordonată, 20
 polinom
 omogen, 78
 reciproc, 113
 simetric elementar, 91
 simetric fundamental, 91
 polinom matricial, 120
 polinom minimal, 82
 polinom simetric, 91
 polinom unitar, 82
 polinomul
 de interpolare Lagrange, 117
 polinomul minimal
 al unui endomorfism, 122
 pondere a unui cuvânt, 127
 predicat, 12
 prim, 100
 prime între ele (elemente), 98
 primul element, 26
 Principiul bunei ordonări, 39
 produs cartezian, 21
 propoziție, 12
 proprietatea de universalitate
 a algebrei monoidale, 76
 a inelului de fracții, 49
 a inelului de polinoame, 76
 punct fix, 137

R

rata unui cod, 124
 rădăcină
 multiplă, 110
 simplă, 110
 relativ prime (elemente), 98
 relație
 antisimetrică, 25
 de bună ordine, 26
 de echivalență, 25
 de ordine, 25
 de ordine strictă, 25
 de ordine totală, 25
 de preordine, 25
 ireflexivă, 25
 reflexivă, 24
 simetrică, 25
 tranzitivă, 25
 relație (clasă), 22
 relație binară, 21
 relație funcțională, 16
 reprezentarea unui număr într-o bază, 41
 rest, 101
 reuniune
 a unei familii, 23
 disjunctă, 23

S

schema de comprehensiune, 17
 segment inițial, 29
 sferă, 65
 simbol, 11
 sistem de reprezentanți, 43
 spațiu metric, 65
 complet, 65
 stabilizator, 137
 subalgebra generată, 70
 subalgebră, 70

submulțime, 16
 suport, 71
 supremum, 26

Ș

șir, 34
 șir Cauchy, 61
 șir fundamental, 61

T

tăietură, 67
 teorema împărțirii cu rest, 101
 teorema perechii, 19
 term, 75
 tip de ordine, 36
 transcendent, 82

U

UFD, 105
 ultimul element, 26

V

valoare de adevăr, 12
 valoarea absolută, 51
 valuarea p -adică, 66
 variabilă, 11
 variabilă legată, 12
 variabilă liberă, 12

Z

Zermelo, 9
 ZFS, 15

Bibliografie

1. ALBU, T., ION, I.D. [1984] *Capitole de teoria algebrică a numerelor*, Ed. Academiei R.S.R., București.
2. ALBU, T., ION, I.D. [1997] *Itinerar elementar în algebra superioară*, Ed. All, București.
3. ALBU, T., MANOLACHE, N. [1987] *19 Lecții de teoria grupurilor*, Ed. Universității București, București.
4. ALBU, T., RAIANU, Ș. [1984] *Lecții de algebră comutativă*, Ed. Universității București, București.
5. ANDERSON, F.W., FULLER, K.R. [1974] *Rings and categories of modules*, Springer-Verlag, New York.
6. AYAD, M. [1997] *Théorie de Galois. 122 exercices corrigés*, Ellipses, Paris.
7. BARBU, V. [1985] *Ecuații diferențiale*, Ed. Junimea, Iași.
8. BECHEANU, M. et al. [1983], *Algebră pentru perfecționarea profesorilor*, Ed. didactică și pedagogică, București.
9. BOREVICI, Z.I., ȘAFAREVICI, I.R. [1985], *Teoria numerelor*, Ed. Științifică și Enciclopedică, București.
10. BOURBAKI, N. [1958] *Eléments de mathématique*, Fasc. VII, Livre II: *Algèbre*, Chapitre 3, *Algèbre multilinéaire*, Hermann, Paris.
11. BOURBAKI, N. [1967] *Eléments de mathématique*, Fasc. VI, Livre II: *Algèbre*, Chapitre 2, *Algèbre linéaire*, Hermann, Paris.
12. BOURBAKI, N. [1981] *Algèbre*, Chapitres 4 à 7, Masson, Paris.
13. BOURBAKI, N. [1985] *Eléments de mathématique: Algèbre commutative*, Chapitres 1 à 4, Masson, Paris.
14. ESCOFIER, J.P. [1997] *Théorie de Galois*, Masson, Paris.
15. FRIED, M., JARDEN, M. [1986], *Field Arithmetic*, Springer Verlag, Berlin.
16. FREUDENTHAL, H. [1973], *Limbajul logicii matematice*, Ed. Tehnică, București.
17. GEDDES, K., CZAPOR, S., LABAHN, G. [1992], *Algorithms for Computer Algebra*, Kluwer Academic Publishers.
18. GOZARD, I. [1997] *Théorie de Galois*, Ellipses, Paris.
19. HALL, M. [1959] *The Theory of Groups*, Macmillan, New York.
20. HUNGERORD, T.W. [1974], *Algebra*, Springer-Verlag, New York.

21. ION, I.D., NĂSTĂSESCU, C., NIȚĂ, C. [1984] *Complemente de algebră*, Ed. Științifică și enciclopedică, București.
22. ION, I.D., RADU, N. [1981a] *Algebra*, Ed. Didactică și pedagogică, București.
23. ION, I.D., RADU, N., NIȚĂ, C., POPESCU, D. [1981b] *Probleme de algebră*, Ed. Didactică și pedagogică, București.
24. JACOBSON, N. [1964], *Lectures in Abstract Algebra III. Theory of Fields and Galois Theory*, Springer-Verlag, New York.
25. JACOBSON, N. [1974], *Basic Algebra I*, W.H. Freeman and Co., San Francisco.
26. KAPLANSKY, I. [1973], *Fields and Rings*, The University of Chicago Press, Chicago.
27. KOSTRIKIN, A.I., SHAFAREVICH, I.R. (Eds.) [1990] *Algebra I. Basic Notions of Algebra* (I.R. SHAFAREVICH), Encyclopaedia of Mathematical Sciences, vol. 11, Springer Verlag.
28. LAFON, J.P. [1977] *Algèbre commutative. Langages géométrique et algébrique*, Hermann, Paris.
29. LINT, J.H. VAN [1982], *Introduction to Coding Theory*, Springer-Verlag, New York.
30. MACCARTHY, P.J. [1966], *Algebraic Extensions of Fields*, Blaisdell Publishing, Waltham, Massachusetts.
31. MANIN, YU. I. [1977], *A Course in Mathematical Logic*, Springer Verlag, New York.
32. MARINESCU, GH. [1983], *Analiză matematică, vol. I*, Ed. Academiei R.S.R., București.
33. MORANDI, P. [1996] *Field and Galois Theory*, Springer-Verlag, New York.
34. NĂSTĂSESCU, C. [1974] *Introducere în teoria mulțimilor*, Ed. Didactică și pedagogică, București.
35. NĂSTĂSESCU, C. [1976] *Inele. Module. Categorii*, Ed. Academiei R.S.R., București.
36. NĂSTĂSESCU, C., NIȚĂ, C. [1979] *Teoria calitativă a ecuațiilor algebrice*, Ed. Tehnică, București.
37. NĂSTĂSESCU, C., NIȚĂ, C., VRACIU, C. [1986] *Bazele Algebrei, vol. I*, Ed. Academiei R.S.R., București.
38. NĂSTĂSESCU, C. [1983] *Teoria dimensiunii în algebra necomutativă*, Ed. Academiei R.S.R., București.
39. NEUKIRCH, J. [1986] *Class Field Theory*, Springer-Verlag, Berlin.
40. NIȚĂ, C., SPIRCU, T. [1974] *Probleme de structuri algebrice*, Ed. Tehnică, București.
41. PARENT, D.P. [1978] *Exercices en théorie des nombres*, Gauthier-Villars, Paris.
42. POPESCU, N. [1971] *Categorii abeliene*, Ed. Academiei R.S.R., București.
43. PURDEA, I. [1982] *Tratat de algebră modernă, vol II*, Ed. Academiei R.S.R., București.
44. RADU, GH. [1988] *Algebra categoriilor și functorilor*, Ed. Junimea, Iași.
45. RADU, N. [1968] *Inele locale, vol. I*, Ed. Academiei R.S.R., București.
46. REGHIȘ, M. [1981] *Elemente de teoria mulțimilor și logică matematică*, Ed. Facla, Timișoara.
47. SAMUEL, P. [1963] *Anneaux factoriels*, Sociedade de Matemática de São Paulo.

48. SAMUEL, P. [1968] *Théorie algébrique des nombres*, Hermann, Paris.
49. SCORPAN, A. [1996] *Introducere în teoria axiomatică a mulțimilor*, Ed. Universității București, București.
50. SIREȚCHI, GH. [1978] *Analiză matematică, vol. I*, ed IV., Tipografia Univ. București.
51. SHPARLINSKI, I., [2003] *Cryptographic applications of analytic number theory. Complexity lower bounds and pseudorandomness*, Progress in Computer Science and Applied Logic, 22. Birkhäuser Verlag, Basel.
52. SPINDLER, K. [1994] *Abstract Algebra with Applications, vol. I, II*, M. Dekker, New York.
53. ȘTEFĂNESCU, M., [1993] *Introducere în teoria grupurilor*, Ed. Universității „Al. I. Cuza”, Iași.
54. TEODEORESCU, P.P., NICOROVICI-PORUMBARU, N. [1985], *Aplicații ale teoriei grupurilor în mecanică și fizică*, Ed. Tehnică, București.
55. TIGNOL, J.-P. [1987] *Galois' Theory of Algebraic Equations*, Longman Scientific and Technical.
56. WINKLER, F. [1996], *Polynomial Algorithms in Computer Algebra*, Springer Verlag Wien-NewYork.
57. VAN DER WAERDEN, B.L. [1967], *Algebra II* (Fünfte auflage der Modernen Algebra) Springer-Verlag, Berlin.
58. VAN DER WAERDEN, B.L. [1971], *Algebra I* (Achte auflage der Modernen Algebra) Springer-Verlag, Berlin.
59. VAN DERWAERDEN, B.L. [1985], *A History of Algebra*, Springer-Verlag, Berlin.
60. WALKER, R.J. [1950] *Algebraic Curves*, Dover Publications, New York.