Seminar 1 - Inele și idempotenți
gr. 134 & 135 Info, sem. 2 2014-2015

Vom cîteva elemente privitoare la teoria elementară a inelelor și vom introduce cîteva rezultate noi pe care le vom folosi mai departe. Principalele inele care ne interesează sînt inelele de polinoame și inelele de matrice. Așadar, majoritatea exemplelor aplicative se vor adresa acestor cazuri.

1 Aspecte teoretice

Definiţie 1.1: Fie $(R, +, \cdot)$ un inel și $x \in R$ un element arbitrar. x se numește:

(1) *inversabil* (notat $x \in \mathcal{U}(R)$) dacă $x \neq 0$ și $\exists y \neq 0$ în R astfel încît $xy = 1$.

(2) *divizor al lui zero* (sau *zero-divizor*) dacă $x \neq 0$ și $\exists 0 \neq y \in R$ a.î. $xy = 0$. Notăm $x \in \mathcal{ZD}(R)$.

(3) *idempotent* dacă $x^2 = x$. (Notație ad-hoc: $x \in \mathcal{I}d(R)$)

(4) *nilpotent* dacă există $n \in \mathbb{N}$ cu $x^n = 0$. Cel mai mic n cu această proprietate se numește *indicele de nilpotență* al lui x. (Notație ad-hoc: $x \in \mathcal{N}(R)$)

Cu aceste noțiuni, avem următoarea proprietate:

Propoziţie 1.1: *Într-un inel finit R, orice element este inversabil sau zero-divizor.*

Dem.: Fie $a \in R$ un element arbitrar. Presupunem că a nu este zero-divizor. Atunci aplicația $f : R \to R$ dată de $f(x) = ax$ este injectivă. Cum R este mulțime finită, rezultă că este și surjectivă, deci bijectivă sau, mai exact, automorfism. Deci $1 \in Imf$, adică $\exists b \in R$ a.î. $f(b) = ab = 1 \Rightarrow b = a^{-1} \Rightarrow a \in \mathcal{U}(R)$. □

În inele care nu sînt finite, are loc următoarea proprietate:

Propoziţie 1.2: *Un element $x \in R$ care este unitate nu poate fi divizor al lui zero. Altfel spus, pentru orice inel R, $\mathcal{U}(R) \cap \mathcal{ZD}(R) = \emptyset$.*

Dem.: Dacă $x \in \mathcal{U}(R)$, atunci să presupunem prin absurd că există $0 \neq y \in R$, cu $xy = 0$. Dar atunci $0 = x^{-1} \cdot x \cdot y = 1 \cdot y$, contradicție. □

Amintim și următoarea proprietate:

Propoziţie 1.3: *Un element $x \in \mathbb{Z}_n$ este inversabil dacă și numai dacă $cmmdc(x, n) = 1$.*

Să vedem cîteva exemple concrete.

Exemplu 1.1: În inelul $R = \mathbb{Z}_{10}$, $\widehat{3}$ este inversabil, dar $\widehat{2}$, $\widehat{4}$ sînt divizori ai lui zero. De asemenea, $\mathbb{Z}_{10}$ nu conține elemente nilpotente, deoarece ecuația $x^n = 0$ nu are decît soluția trivială în $\mathbb{Z}_{10}$. Fie x un element idempotent. Adică $x^2 = x$, deci $x(x - \widehat{1}) = \widehat{0}$ în $\mathbb{Z}_{10}$. Obținem că elementele idempotente sînt doar $\widehat{0}$ și $\widehat{1}$.

Exemplu 1.2: Exemple de matrice idempotente (după cum se poate vedea din calcule directe) sînt:

$$\begin{pmatrix} 1 & 1 \\ 0 & 0 \end{pmatrix} \text{ și } \begin{pmatrix} 2 & -2 & -4 \\ -1 & 3 & 4 \\ 1 & -2 & -3 \end{pmatrix}$$

Observaţie 1.1: Se poate vedea ușor că, excepție făcînd matricea identitate, toate matricele idempotente sînt singulare, adică au determinantul nul (deci sînt neinversabile).

Exemplu 1.3: Exemple de matrice nilpotente sînt:

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \text{ și } \begin{pmatrix} 0 & 2 & 1 & 6 \\ 0 & 0 & 1 & 2 \\ 0 & 0 & 0 & 3 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Prima are indicele de nilpotență 2, iar cea de-a doua, 4.

Deși din cele de mai sus pare că o matrice nilpotentă trebuie să aibă cît mai multe intrări nule, în general nu este adevărat. Matricea $\begin{pmatrix} 5 & -3 & 2 \\ 15 & -9 & 6 \\ 10 & -6 & 4 \end{pmatrix}$ este nilpotentă, cu indicele de nilpotență 2!

Avem o caracterizare interesantă pentru elementele nipotente dintr-un inel.

Propoziţie 1.4: *Elementul $x \in R$ este nilpotent dacă și numai dacă elementul $1+x$ este inversabil.*

Dem.: Să presupunem că x este nilpotent, cu indicele n, deci $x^n = 0$. Atunci, considerînd expresia:

$$(1+x)(1-x+x^2-x^3+\cdots+(-1)^{n-1}x^{n-1}) = 1+x^n = 1,$$

deducem că $1+x$ este inversabil, inversul fiind elementul din a doua paranteză. □

Ne îndreptăm acum atenția asupra divizorilor lui zero, elementelor inversabile și nilpotente din inele de polinoame.

Teoremă 1.1 (McCoy)**:** *Fie $f \in R[X]$ un polinom, cu R inel comutativ. Dacă f este zero-divizor, atunci $rf = 0$, pentru un element $r \in R$.*

Dem.: Să presupunem că f este anulat de un polinom de grad $\geqslant 0$. Deci există $g \in R[X]$, cu $fg = 0$. Îl alegem cu grad minim. Să scriem cele două polinoame: $f = \sum_{i=0}^{m} f_i$, iar $g = \sum_{j=0}^{n} g_j$.

Dacă $g_n = 0$, am terminat, deoarece avem o contradicție cu minimalitatea lui g.

Dacă $g_n \neq 0$, înseamnă că există un i astfel încît $f_i g_n = 0$. Alegem cel mai mare i cu proprietatea că $f_i g \neq 0$. Dar atunci avem:

$$0 = fg = (f_0+\cdots+f_i)g = (f_0+\cdots+f_i)(g_0+\cdots+g_n),$$

de unde $f_i g_n = 0$. Dar atunci $f_i g$ are grad mai mic decît g și anulează pe f, contradicție. □

Așadar, polinoamele care sînt zero-divizori sînt, de fapt, anulate de constante.

Polinoamele nilpotente au o formă foarte simplă:

Propoziţie 1.5: *Un polinom $p = a_0 + a_1X + \cdots + a_nX^n$ este nilpotent dacă și numai dacă toți coeficienții săi sînt nilpotenți.*

Dem.: Implicația " $\Leftarrow$ " este clară, deoarece putem ridica p la cmmmc al indicilor de nilpotență pentru coeficienții săi și atunci obținem p nilpotent.

Pentru implicația directă, fie p nilpotent. Scădem din p toți termenii care au coeficienți nilpotenți și obținem un nou polinom, tot nilpotent. Dacă este zero, am terminat. Dacă nu, are un cel mai mare termen aX^h pentru care coeficientul a nu este nilpotent. Dar atunci, pentru orice $\alpha \in \mathbb{N}$, f^α are termenul dominant $a^\alpha x^{\alpha h}$, care este nenul, contradicție. □

Polinoamele inversabile sînt caracterizate de următorul rezultat.

Propoziţie 1.6: *Fie R un inel comutativ. Atunci polinomul $p = a_0 + a_1X + a_2X^2 + \cdots + a_nX^n$ este inversabil dacă și numai dacă a_0 este inversabil și a_i este zero-divizor, pentru toți $i = 1, \ldots, n$.*

Dem.: " $\Leftarrow$ " : Dacă are coeficienții ca în enunț, atunci, conform propoziției de mai sus, va fi o sumă între un element inversabil și nu polinom nilpotent. Să presupunem că $a_0 b = 1$ și $p - a_0$ îl notăm cu g, cu $g^N = 0$. Este suficient să arătăm că $b(a_0+g) = 1+bg = 1-h$ este inversabil, unde cu h am notat $-bg$, avînd proprietatea $h^N = 0$. Dar, cum am văzut mai sus, $(1-h)(1+h+h^2+\cdots+h^{N-1}) = 1-h^N = 1$, ceea ce trebuia demonstrat.

Pentru implicația cealaltă, din $pq = 1$ rezultă $p(0)q(0) = 1$, deci obținem că termenul liber trebuie să fie inversabil. Pentru nilpotența celorlalți coeficienți, obținem din aproape în aproape, astfel: dacă $p = \sum_{i=0}^{n} a_i X^i$ și $q = \sum_{j=0}^{m} b_j X^j$, făcînd produsul, obținem succesiv:

$$\begin{gathered} a_0b_1 + a_1b_0 = 0 \\ a_0b_2 + a_1b_1 + a_2b_0 = 0 \\ \cdots\cdots\cdots \\ a_{n-1}b_m + a_nb_{m-1} = 0 \\ a_nb_m = 0. \end{gathered}$$

Înmulțim penultima relație cu a_n și obținem $a_n^2 b_{m-1} = 0$. Dacă înmulțim antepenultima ecuație cu a_n^2, obținem $a_n^3 b_{m-2} = 0$ ș.a.m.d., pînă la $a_n^{m+1} b_0 = 0 \Rightarrow a_n$ este nilpotent. Similar procedăm pentru a obține nilpotența și pentru ceilalți coeficienți. □

O generalizare a polinoamelor o constituie *seriile formale*. Acestea se pot defini, ca și polinoamele, cu ajutorul șirurilor.

Definiţie 1.2: Fie R un inel. Pe mulțimea R^N, a șirurilor cu N termeni, definim operațiile:

$$(a_0, a_1, \dots, a_n) + (b_0, b_1, \dots, b_N) = (a_0 + b_0, a_1 + b_1, \dots, a_N + b_N),$$

iar produsul celor două șiruri să fie $(c_0, \dots, c_N)$, unde $c_i = \sum_{j=1}^{i} a_j b_{N_j}$.

Atunci definim $X = (0, 1, 0, \dots)$ și, cu ajutorul operațiilor de mai sus, obținem $X^i = (0, \dots, 1, \dots)$, unde 1 este pe poziția $i + 1$. Se observă că elementul neutru la înmulțire este $(1, 0, 0, \dots)$ și acesta se asociază elementului $1 \in R$. Similar $0 = (0, 0, \dots)$.

Astfel definit, obținem $R_N[X]$, inelul de polinoame cu nedeterminata X, coeficienți în R și grad cel mult N.

Admițînd acum că $N = \mathbb{N}$, obținem inelul de serii formale în nedeterminata X, scrise, în general, sub forma $f = \sum_{i=0}^{\infty} a_i X^i$. Inelul se notează cu $R[[X]]$.

Inversabilitatea seriilor formale este dată de propoziția următoare:

Propoziţie 1.7: *O serie formală* f *este inversabilă dacă și numai dacă are termenul liber inversabil.*

Dem.: Implicația directă este simplă. Luînd $f = \sum_{i=0}^{\infty} a_i X^i$ și inversul său $g = \sum_{j=0}^{\infty} b_j X^j$, din condiția $fg = 1$ rezultă imediat $a_0 b_0 = 1$.

Pentru implicația reciprocă, vrem să definim g ca mai sus. Luăm, pentru început, $b_0 = a_0^{-1}$, iar ceilalți coeficienți se definesc în general recurent prin:

$$b_i = -(a_0^{-1})(a_1 b_{i-1} + a_2 b_{i-2} + \cdots + a_i b_0).$$

□

O construcție care ne interesează acum este produsul direct de inele.

Definiţie 1.3: Fie R, S inele. Pe mulțimea $R \times S = \{(x, y) \mid x \in R,\ y \in S\}$ putem da o structură de inel pe componente. Adică $(x, y) + (z, t) = (x + z, y + t)$, respectiv $(x, y) \cdot (z, t) = (x \cdot z, y \cdot t)$.

Inelul astfel obținut se numește *produsul direct* al inelelor R și S, notat $R \times S$ sau $R \oplus S$.

Să mai amintim o structură importantă.

Definiţie 1.4: Fie R un inel și I o submulțime a lui R. Spunem că I este *ideal* al inelului R, notat $I \trianglelefteq R$, dacă $(I, +)$ este subgrup al grupului aditiv $(R, +)$ și $\forall x \in R,\ a \in I$ are loc $ax \in I$.

Există o proprietate interesantă care leagă inelele obținute ca produs direct și elementele idempotente.

Teoremă 1.2: *Inelul comutativ* R *se poate scrie ca un produs de două inele dacă și numai dacă* R *conține un idempotent diferit de* 0 *și de* 1.

Dem.: Să presupunem că $R = R_1 \times R_2$. Atunci, cu operațiile de mai sus, $(1, 0)$ este un idempotent al inelului $R_1 \times R_2$.

Reciproc, dacă există $e^2 = e$ un element idempotent din inelul R, construim inelele R_1 și R_2 de mai sus. Definim $R_1 = Re$ și $R_2 = R(1 - e)$. Mai trebuie arătat că $R \simeq R_1 \times R_2$. Definim $f : R \to R_1 \times R_2$ prin $f(x) = (ex, (1 - e)x)$. Arătați că f este izomorfism de inele. □

Un caz particular de elemente idempotente, pe care l-am întîlnit deja mai sus, este următorul:

Definiţie 1.5: Idempotenții e, f ai inelului R se numesc *ortogonali* dacă $ef = 0$.

În exemplul de mai sus, e și $(1 - e)$ sînt idempotenți ortogonali.

Mai avem și următoarea:

Definiţie 1.6: Idempotentul e se numește *central* dacă $ex = xe,\ \forall x \in R$.

Polinoamele idempotente sînt foarte ușor de caracterizat:

Propoziţie 1.8: *Polinomul* f *este idempotent dacă și numai dacă termenul său liber este idempotent și toți ceilalți coeficienți sînt zero.*

2 Exerciții

1. Arătați că, dacă $n = a^k \cdot b$, pentru niște numere naturale a, b, atunci elementul $\widehat{a \cdot b}$ este nilpotent în inelul $\mathbb{Z}_n$.

2. Fie $a \in \mathbb{Z}$ un număr întreg. Arătați că $\widehat{a}$ este nilpotent în $\mathbb{Z}_n$ dacă și numai dacă orice divizor prim al lui n este divizor și al lui a.

3. Fie x un element nilpotent în inelul comutativ A. Arătați că: (rezolvat!)

(a) x este zero sau divizor al lui zero;

(b) $1 + x$ este inversabil în A.

4. Un inel B se numește *boolean* dacă orice element al său este idempotent. Arătați că orice inel boolean este comutativ și că $2x = 0$, $\forall x \in B$.

5. O matrice $A \in \mathcal{M}_n(\mathbb{C})$ se numeşte *involutivă* dacă $A^2 = I_n$. O matrice $A \in \mathcal{M}_n(\mathbb{C})$ se numeşte *idempotentă* dacă $B^2 = B$. Arătaţi că:

(a) Dacă B este idempotentă, atunci $2B - I_n$ este involutivă;

(b) Dacă A este involutivă, atunci $\frac{1}{2}(A + I_n)$ este idempotentă.

6. Să se determine matricele idempotente din $M_2(\mathbb{Z}_p)$.

7. Să se arate că, dacă I este un ideal al inelului R și I conține un element inversabil din R, atunci $I = R$.

8. Să se arate că un corp nu are ideale diferite de 0 și el însuși.

9. Fie $A \in M_n(\mathbb{k})$, unde $\mathbb{k}$ este un corp comutativ. Să se arate că A este inversabilă sau divizor al lui zero.

10. Să se determine elementele nilpotente și idempotente din inelul $\mathbb{Z}_n$. (Puteți considera cazuri particulare și încercați să generalizați.)

(*) Verificați că polinomul $f = \widehat{7} + \widehat{5}X + \widehat{15}X^2$ este inversabil în inelul $\mathbb{Z}_{75}[X]$.