Analele ştiinţifice ale Universităţii „Al. I. Cuza" din Iaşi
Tomul XXXI, s. I a, 1985 (supliment)

UNE GÉNÉRALISATION DES CODES CYCLIQUES

BY

MIHAELA RĂDUICA

Nous nous proposons d'introduire dans cette note la notion de transformation cyclique généralisée, les sous-espaces invariants de ces transformations représentant une extension des codes cycliques. Le cadre nécessaire à cette démarche peut intéresser aussi dans le sens qu'il offre un langage adéquat permettant une analyse d'ensemble du cas particulier de la famille des codes cycliques, ce qui fait le principal objet du travail, une place importante revenant à la description de la structure booléene de cette classe spéciale de codes correcteurs d'erreurs.

Nous rappelons qu'il s'agit de plusieurs degrés de généralisation et que nous n'insisterons que sur ceux qui prouvent leur capacité d'éventuelle applicabilité pratique.

Pour le cas le plus général, soit A — un ensemble, S_A — le groupe symétrique sur A, K — un champ et V — un espace vectoriel sur K. Nous dotons l'ensemble $V^A = \{v : A \to V\}$ d'une structure de K-espace vectoriel face aux lois de composition définies ponctuellement. Le résultat suivant est immédiat.

Proposition 1. *L'application*

i) $s : S_A \times V^A \to V^A, \quad (\sigma, v) \to \sigma v := v \circ \sigma^{-1}$

est une action du groupe symétrique S_A sur l'ensemble V^A ;

ii) $t : S_A \to GL(V^A), \ \sigma \to T_\sigma$

est une représentation du groupe symétrique, où nous avons pour $\sigma \in S_A$ fixé

$$T_\sigma : V^A \to V^A, \quad v \to \sigma v. \tag{1}$$

Grâce à la propriété d'universalité de la K-algèbre $K[X]$ des polynômes dans l'indéterminée X sur K, l'application $\tau : K \to \mathrm{End}\,(V^A)$, $\alpha \to \alpha 1_{V^A}$ s'étend par $X \to T_\sigma$ à un morphisme de K-algèbres

$ev_{T_\sigma} : K[X] \to \mathrm{End}(V^A)$, $f = \sum_{i=0}^{m} \alpha_i X \to f[T_\sigma] := \sum_{i=0}^{m} \alpha_i T_\sigma^i$, où les puissances de l'opérateur sont considérées dans le sens de la composition et $T_\sigma^0 = 1_{V^A}$.

Soit $K[T_\sigma] := \mathrm{Im}\, ev_{T_\sigma}$.

Définition 1. *Tout élément $\omega \in K[T_\sigma]$ s'appelle transformation cyclique généralisée et nous appelons code cyclique généralisé un sous-espace ω-invariant.*

Remarque. Le choix de cette terminologie est justifié par le fait que les transformations, soit les codes cycliques usuels, se retrouvent par une particularisation adéquate, [3].

Nous parcourons ensuite une première étape dans ce processus de particularisation. Puisque les principaux problèmes propres à la théorie algébrique des codes [1] ont à la base des considérations d'ordre finital relativement à T_σ de (1), soit $|A| = n$, par exemple $A = \{1, 2, \ldots, n\}$, $V = K^n$ et pour $\sigma \in S_n$, soit $\sigma = \sigma_1 \circ \sigma_2 \circ \ldots \circ \sigma_k$ la décomposition en cycles disjoints, évidemment avec $1 \leqslant k \leqslant n$.

Si nous notons par $(\mathcal{F})_1$ le plus grand diviseur commun unitaire de la famille des polynômes $\mathcal{F}$, nous pouvons énoncer :

Proposition 2. *Le polynôme minimal $M_\sigma \in K[X]$ de la transformation T_σ est*

$$M_\sigma = \prod_{i=1}^{k} (X^{\mathrm{ord}(\sigma_i)} - 1) / (\{ \prod_{i=1, i \neq l}^{k} (X^{\mathrm{ord}(\sigma_i)} - 1) \mid l = \overline{1, k} \})_1.$$

Corollaire. *Si les ordes des cycles qui apparaissent dans la décomposition de la permutation σ sont relativement primes par paires, alors*

$$M_\sigma = \prod_{i=1}^{k} (X^{\mathrm{ord}(\sigma_i)} - 1) / (X - 1)^{k-1}. \tag{2}$$

Nous avons par conséquent les affirmations suivantes de la

Proposition 3. i) *$K[T_\sigma]$ est une sous-algèbre commutative de l'algèbre $End\,(V^A)$ sur K.*

ii) $\mathrm{Ker}\ ev_{T_\sigma} = (M_\sigma)$.

iii) *Il existe un isomorphisme e de K-algèbres qui rend commutatif le diagramme*

$$\begin{tikzcd} K(X) \arrow[rr, "ev_{T_\sigma}"] \arrow[dr, "p"'] & & K[T_\sigma] \\ & K[X]/(M_\sigma) \arrow[ur, "e"'] & \end{tikzcd} \tag{3}$$

où p est la projection canonique sur l'algèbre quotient correspondante.

Nous continuons la particularisation jusqu'au cas des transformations cycliques, une pareille transformation T_σ correspondant à une permutation σ d'ordre n, par exemple, $\sigma = (12 \ldots n)$. Grâce au fait que dans la théorie des codes cycliques la finitude cu champ K est essentielle, dans le contexte des données de l'étape antérieure nous choisissons en plus, $K = GF(q)$, où q est une puissance naturelle non nulle d'un nombre prime. En gardant la notation pour K, nous convenons d'utiliser dans ce cas spécial la symbolique:

$$T = T_\sigma \text{ et } M = M_\sigma.$$

L'importance attachée à cette nouvelle étape du processus de particularisation réside dans le fait que, conformément à [3], les codes cycliques seront les idéaux de la structure de K-algèbre construite sur K^n (relativement à l'opérateur T).

Dans ce sens, nous observons que de (2), il résulte $M = X^n - 1$, c'est-à-dire $T^n = 1_{K^n}$ et $\dim K[T] = n$, $(T^i)_{i=\overline{1,n}}$ etant un système linéaire indépendant. Nous considérons les isomorphismes de K-espaces vectoriels,

$$\varepsilon : K^n \rightarrowtail\!\!\!\!\twoheadrightarrow K[X]/(X^n - 1), \ (\alpha_i)_{i=\overline{0,n-1}} \to \sum_{i=0}^{n-1} \alpha_i X^i + (X^n - 1), \text{ respectivement}$$

$$\varphi = e \circ \varepsilon : K^n \rightarrowtail\!\!\!\!\twoheadrightarrow K[T], \ a = (\alpha_i)_{i=\overline{0,n-1}} \to a[T] = \sum_{i=0}^{n-1} \alpha_i T^i, \text{ où } e \text{ paraît dans (3).}$$

Tant ε, que ρ permettent le transfert de la structure de K-algèbre des co-domaines sur le domaine K^n. Ainsi, la multiplication en K^n, $*: K^n \times K^n \to K^n$, peut être définie par n'importe laquelle des égalités suivantes valables pour a, $b \in K^n$ arbitraires :

$$a * b = \varepsilon^{-1}(\varepsilon(a)\varepsilon(b)), \quad a * b = \varphi^{-1}(\varphi(a) \circ \varphi(b)).$$

Nous rappelons que la première acception pour $*$ illustre la technique usuelle de calcul, alors que la deuxième description, c'est-à-dire

$$(\forall a)_{a,b \in K^n} (\forall b) ((a * b)[T] = a[T](b)[T] = a[T] \circ b[T]),$$

„internalise" l'opération $*$. De cette manière, K-espace vectoriel K^n doté de $*$ devient une K-algèbre comutative et, en plus, nous avons $(\forall a)_{a,b \in K^n} (\forall b)$ $(a[T](b) = b[T](a))$.

Ensuite, cette deuxième acception de l'opération $*$ facilite la mise en évidence de la structure booléene de l'ensemble des codes cycliques. Dans ce but, il est utile de considérer l'application

$$\delta : (K^n)^c \to \{0, 1, \ldots, n-1\}, a = (\alpha_i)_{i=\overline{0,n-1}} \to \max \{e \in \mathbf{N} \mid (0 \leqslant e \leqslant n-1) \wedge (\alpha_e \neq 0)\}.$$

Définition 2. i) *L'application* δ *s'appelle degré sur* $(K^n)^*$,

ii) *Si* $a = (\alpha_i)_{i=\overline{0,n-1}} \in (K^n)^c$, $\delta(a) = m$ *et* $\alpha_m = 1$, *alors* a *s'appelle unitaire.*

La famille des éléments unitaires de la $(K^n)^*$ étant notée par $\mathcal{U}$, soit

$$\mathcal{C}(K^n) = \{a \in \mathcal{U} \mid (\exists a^c)(a^c \in \mathcal{U})[(a * a^c = 0) \wedge (\delta(a) + \delta(a^c) = n)]\}$$

Remarque. Avec les notations de (4), évidemment l'application $a \to a^c$ est une bijection involutive.

En vue d'atteindre l'un des buts fondamentaux que nous nous proposons dans cet ouvrage, nous notons le résultat intermédiaire suivant.

Proposition 4. *Si* I *est un idéal de la* K-*algèbre* K^n *et* $a \in I$ *est un élément unitaire de degré minime, alors :* (i) a *est uniquement déterminé ;* ii) $a \in \mathcal{C}(K^n)$; iii) $I = a * K^n = (a)$.

Remarque. I est un idéal en K^n si et seulement si I est un sous-espace T-invariant.

Enfin, en illustrant dans K^n la structure de divisibilité de $X^n - 1 \in K[X]$ par l'intermédiaire de la famille $\mathcal{C}(K^n)$, nous démontrons la proposition suivante, qui met en évidence la structure d'algèbre Boole de la famille Id (K^n) des idéaux de K^n.

Proposition 5. (i) $(\forall b)$ $(\exists! a)$ $b \in K^n$, $a \in \mathcal{C}(K^n)$ $(b * K^n = a * K^n)$; (ii) *L'application* $u : \mathcal{C}(K^n) \to \mathrm{Id}\,(K^n)$, $a \to a * K^n$ *est une bijection* ; (iii) *Si* char $(K) \nmid n$, *alors* $(\forall a) a \in \mathcal{C}(K^n)$, $a * K^n = \mathrm{Im}\, a[T] = \mathrm{Ker}\, a^c[T]$, *et nous avons la décomposition directe* $(\forall a) a \in \mathcal{C}(K^n)[K^n = (a * K^n) \oplus (a^c * K^n)]$.

BIBLIOGRAPHIE

1. van Lint, J. H.—*Introduction to Coding Theory*, Springer Verlag, New York Inc., 1982.
2. Wedderburn J. H. M.—*Lectures on Matrices*, Amer. Math. Soc. Colloquim Publ., New York, 1934.
3. Creangă, I., Simovici, D.—*Teoria codurilor*, E.D.P., București, 1975.

Université de Brașov

Analele științifice ale Universității „Al. I. Cuza" din Iași
Tomul XXXI, s. I a, 1985 (supliment)

UNE GÉNÉRALISATION DES GROUPES RÉSOLUBLES

PAR

GH. IVAN

Dans cette Note on définit les notions de groupe quasi-résoluble et de suite quasi-résoluble en généralisant d'une manière naturelle les notions bien connues de groupe résoluble et de suite résoluble.

Soient G un groupe et $D^*(G) = (D^n(G))_{n \in \mathbf{N}}$ la suite dérivée de G.

Définition 1. *On dit qu'un groupe* G *est quasi-résoluble s'il existe un entier* $s \geqslant 0$ *tel que* $D^s(G)$ *soit un groupe simple. Un groupe* G *s'appelle quasi-résoluble de classe* s *si* s *est le plus petit entier tel que* $D^s(G)$ *soit un groupe simple.*

Exemples 1. a) Tout groupe simple non commutatif est quasi-résoluble de classe 0 car $D^k(G) = G$ pour tout $k \geqslant 0$.

b) Tout groupe résoluble de classe s est un groupe quasi-résoluble de classe $s-1$ ou s selon le cas où $D^{s-1}(G)$ est un groupe simple ou non simple.

c) Pour tout $n \geqslant 5$, le groupe symétrique S_n est un groupe quasi résoluble de classe 1 puisque le groupe dérivé de S_n est le groupe alterné A_n qui est simple pour tout $n \geqslant 5$.

Remarque 1. Il y a des groupes non quasi-résolubles. Tout groupe G non commutatif et non simple qui a la propriété que $D(G) = G$ est un groupe qui n'est pas quasi-résoluble (par exemple, le groupe $A_n \times A_n$ pour tout $n \geqslant 5$ est non commutatif, non simple et $D(A_n \times A_n) = D(A_n) \times D(A_n) = A_n \times A_n$).

Une *suite normale* de G, $G = H_0 \trianglerighteq H_1 \trianglerighteq H_2 \trianglerighteq \ldots \trianglerighteq H_i \trianglerighteq \ldots$ telle que H_i soit distingué dans G pour tout i s'appellera *suite invariante* de G.

La suite dérivée de G, $D^*(G)$ este une suite invariante qui a la propriété que les quotients $D^i(G)/D^{i+1}(G)$ sont des groupes commutatifs.

Définition 2. *Une suite normale de* G *de la forme :* $\mathfrak{N}_q = (G = H_0 \trianglerighteq H_1 \trianglerighteq H_2 \trianglerighteq \ldots \trianglerighteq H_{q-1} \trianglerighteq H_q = \{e\})$ *s'appelle quasi-résoluble à longueur* q *si les quotients* H_i/H_{i+1} *sont commutatifs pour tout* $0 \leqslant n \leqslant q-2$.

Remarque 2. Si un groupe G satisfait à la condition que toutes ses suites normales décroissantes de sous-groupes sont finies, alors la suite dérivée $D^*(G)$ est finie, c'est-à-dire il existe $n \in \mathbf{N}$ tel que $D^{n+k}(G) = D^n(G)$ pour tout $k \geqslant 1$. Dans ce cas, la suite dérivée $D^*(G)$ est une suite quasi-résoluble à longueur $n+1$, à savoir : $D^*(G) = (G = D^0(G) \trianglerighteq D^1(G) \trianglerighteq D^2(G) \trianglerighteq \ldots \trianglerighteq D^n(G) \trianglerighteq \{e\})$

Théorème 1. a) *Tout sous-groupe distingué d'un groupe quasi-résoluble est aussi un groupe quasi-résoluble.*

b) b) *Si* $f : G \to G'$ *est un homomorphisme du groupe quasi-résoluble* G *dans le groupe* G' *alors* $f(G)$ *est quasi-résoluble.*