Quelques questions de théories combinatoire et élémentaire des nombres

Thèse de l'Université de Lyon

École Doctorale Sciences, Ingéniérie, Santé ED SIS 488

présentée par

Salvatore Tringali

sous la direction de François Hennecart et Alain Plagne

pour obtenir le grade de : Docteur en Mathématiques Pures

Université Jean Monnet - Saint-Étienne, 26 novembre 2013

Plan de la présentation

La thèse est un recueil de contributions variées à :

(i) la théorie additive des groupes, des anneaux et de leurs généralisations (partie I)

1. Une généralisation de la transformée de Davenport.
2. Une extension du théorème de Cauchy-Davenport impliquant :
   (a) les théorèmes de Kemperman et de Hamidoune-Károlyi (cas commutatif) ;
   (b) une extension du théorème de Chowla ;
   (c) une version plus forte du théorème de Pillai (groupes cycliques).
3. Une preuve combinatoire d'une version plus forte du théorème de Hamidoune-Károlyi (pour *tous* les groupes) par la transformée de Kemperman.
4. Une généralisation des résultats par G. A. Freiman et ses coauteurs sur la théorie structurelle des groupes ordonnés au cas des semi-groupes ordonnés.

(ii) la théorie élémentaire des nombres (partie II)

1. Autour d'une conjecture par K. Győry et C. Smyth ;
2. Une contribution à l'étude des systèmes de congruences cycliques (problème de Znám).

Sur la divisibilité de $a^n \pm b^n$ par n^k

K. Győry et C. Smyth ont conjecturé que les ensembles $R_k^+(a,b)$ et $R_k^-(a,b)$ des entiers n t.q., respectivement, $n^k \mid a^n + b^n$ et $n^k \mid a^n - b^n$, où $a, b, k \in \mathbb{Z}$ avec $k \geq 3$, $|ab| \geq 2$ et $\gcd(a,b) = 1$, sont finis.

On démontre que $R_k^{\pm}(a,b)$ sont finis si $k \geq \max(|a|,|b|)$.

Théorème 1. Soient a, b, n être des entiers t.q. $n \geq 2$, $a \geq \max(1,|b|)$ et $b \geq 0$ quand n est pair, et soient $\delta := \gcd(a,b)$, $\alpha := \delta^{-1}a$ et $\beta := \delta^{-1}b$.

(i) Supposons que $\beta \neq -\alpha$ quand n est impair. Alors, $n^a \mid a^n + b^n$ et $n^\alpha \mid \alpha^n + \beta^n$ si et seulement si $(a,b,n) = (2,1,3)$ ou $(2^c, 2^c, 2)$ pour $c \in \{0,1,2\}$.

(ii) Supposons que $\beta \neq \alpha$. Alors, $n^a \mid a^n - b^n$ et $n^\alpha \mid \alpha^n - \beta^n$ si et seulement si $(a,b,n) = (3,1,2)$ ou $(2,-1,3)$.

La preuve se base sur le lemme suivant :

Lemme (Lucas, 1878 & Carmichael, 1909). Pour tous $x, y \in \mathbb{Z}$, $\ell \in \mathbb{N}^+$ et $p \in \mathbb{P}$ t.q. $p \nmid xy$ et $p \mid x - y$, on a (e_p est la valuation p-adique standard) :

(i) Si $p \geq 3$, ℓ est impair, ou $4 \mid x - y$, alors $e_p(x^\ell - y^\ell) = e_p(x-y) + e_p(\ell)$.

(ii) Si $p = 2$, ℓ est pair, et $e_2(x-y) = 1$, alors $e_2(x^\ell - y^\ell) = e_2(x+y) + e_2(\ell)$.

Un système d'equations cycliques dans les entiers (1/2)

Le problème de Znám : Quels sont les multi-ensembles $\mathcal{Z}_k$ d'entiers $x_1, \ldots, x_k \geq 2$ ($k \geq 2$) t.q. x_i est un diviseur *propre* de $1 + \prod_{i \neq j=1}^{k} x_j$ pour tout i ? Sont-ils finis ?

1. $\mathcal{Z}_k = \emptyset$ pour $2 \leq k \leq 4$ (Jának et Skula, 1978) ;
2. Une borne inférieure sur $|\mathcal{Z}_k|$ qui implique $\mathcal{Z}_k \neq \emptyset$ si $k \geq 5$ (Sun Qi, 1983).

Un problème lié : Étant donné un entier $n \geq 3$, soient

(i) $u_1, \ldots, u_n$ des entiers ≥ 2 et premiers entre eux deux à deux;

(ii) $\mathcal{D}$ une famille de sous-ensembles propres et non vides de $\{1, \ldots, n\}$ qui contient un nombre "suffisant" d'éléments (e.g., $|\mathcal{D}| \geq n^{\kappa}$ pour quelque $\kappa > 0$);

(iii) ε une fonction $\mathcal{D} \to \{\pm 1\}$ (on écrit ε_I au lieu de $\varepsilon(I)$).

On pose la question suivante :

Question 1. Existe-t-il au moins un nombre premier q t.q. q divise $\prod_{i \in I} u_i - \varepsilon_I$ pour un certain $I \in \mathcal{D}$, mais ne divise pas $u_1 \cdots u_n$?

• • • Nous donnons une réponse positive dans un cas particulier.

Un système d'equations cycliques dans les entiers (2/2)

Soient n un entier positif et $S_n := \{1, \ldots, n\}$. Pour tout $k \in \mathbb{N}$ on dénote par $\mathcal{P}_k(S_n)$ la collection de tous les sous-ensembles I de S_n t.q. $|I| = k$.

Théorème 2. Étant donné un entier $n \geq 3$, soient $p_1, \ldots, p_n$ des nombres premiers, $v_1, \ldots, v_n$ des entiers positifs et $\mathcal{D}$ une collection de sous-ensembles *propres et non-vides* de S_n t.q. $\mathcal{D}_0 \subseteq \mathcal{D}$, où $\mathcal{D}_0 := \mathcal{P}_1(S_n) \cup \mathcal{P}_{n-2}(S_n) \cup \mathcal{P}_{n-1}(S_n)$. Alors, pour toute fonction $\varepsilon : \mathcal{D} \to \{\pm 1\}$ t.q. la restriction de ε à $\mathcal{D}_0$ est constante, il existe un nombre premier $q \notin \{p_1, \ldots, p_n\}$ t.q. q divise $\prod_{i \in I} p_i^{v_i} - \varepsilon_I$ pour un certain $I \in \mathcal{D}$.

Cela implique :

Théorème 3. Si $\varepsilon_0 \in \{\pm 1\}$ et si A est un ensemble de trois ou plus nombres premiers qui contient les diviseurs premiers des tous les produits $\prod_{p \in B} p - \varepsilon_0$ pour lesquels B est un sous-ensemble propre, fini et non vide de A, alors A contient $\mathbb{P}$.

Les preuves sont basées sur le théorème suivant :

Théorème (Zsigmondy, 1892). Soient $a, b \in \mathbb{N}^+$ et $n \geq 2$ un entier t.q. (i) $a > b$, (ii) $(a, b, n) \neq (2, 1, 6)$, et (iii) si $n = 2$, alors $a + b$ n'est pas une puissance de 2. Alors, il existe $p \in \mathbb{P}$ t.q. $p \mid a^n - b^n$ et $p \nmid a^k - b^k$ pour chaque entier positif $k < n$.

Quelques définitions générales

Semi-groupe : une paire $\mathbb{A} = (A, +)$ constituée par un ensemble et une loi associative.

On dit que $\mathbb{A}$ est (un semi-groupe) simplifiable si

$$\forall x, y, z \in A : x + z = y + z \quad \text{ou} \quad z + x = z + y \implies x = y.$$

Si $X, Y \subseteq A$, on définit $X + Y := \{x + y : x \in X, y \in Y\}$, et

$$X - Y := \{z \in A : (z + Y) \cap X \neq \emptyset\}, \quad -X + Y := \{z \in A : (X + z) \cap Y \neq \emptyset\}.$$

On définit l'*unitarisation* de $\mathbb{A}$, qu'on dénote par $\mathbb{A}^{(0)}$, de la manière suivante :

(i) si $\mathbb{A}$ est un monoïde, alors $\mathbb{A}^{(0)} := \mathbb{A}$;

(ii) sinon, $\mathbb{A}^{(0)}$ est la paire $(A \cup \{0\}, +)$, où $0 \notin A$ et $+$ est la seule extension de $+$ à une opération binaire sur $A \cup \{0\}$ t.q. 0 sert comme un elément neutre.

Si $Z \subseteq A$, on écrit $\langle Z \rangle_{\mathbb{A}}$ pour le plus petit *sous-semi-groupe* de $\mathbb{A}$ qui contient Z.

On écrit $\mathfrak{p}_{\mathbb{A}}(Z)$ pour l'infimum des ordres d'un sous-semi-groupe non trivial de $\langle Z \rangle_{\mathbb{A}^{(0)}}$, i.e.

$$\mathfrak{p}_{\mathbb{A}}(Z) := \inf_{z \in Z \setminus \{0\}} \operatorname{ord}_{\mathbb{A}^{(0)}}(z).$$

Quelques considérations avant de procéder

Deux motivations "naturelles" :

(i) le monoïde des éléments non nuls d'un anneau à unité intégre est, en général, un monoïde simplifiable, mais pas un groupe ;

(ii) même si $\mathbb{A}$ est un groupe commutatif, les sous-ensembles non vides de A, munis de l'opération qui envoie (X, Y) sur la somme $X + Y$, sont un monoïde *non* simplifiable.

On rappelle que :

(i) chaque semi-groupe commutatif et simplifiable s'injecte dans un groupe ;

(ii) rien de semblable n'est vrai dans le cas *non-commutatif*, pas même si le semi-groupe ambient est *de type fini*.

C'est lié à une question bien connue en théorie des semi-groupes (A. I. Malcev, 1937).

• • • L'étude des sommes d'ensembles dans les semi-groupes, même simplifiables et de type fini, ne se réduit pas au cas des groupes (au moins, pas d'une manière triviale).

Cauchy-Davenport et quelques généralisations connues (1/2)

Théorème (Cauchy, 1813 & Davenport, 1935). Si $\mathbb{A}$ est un groupe d'ordre premier p et $X, Y \subseteq A$ sont non-vides, alors $|X + Y| \geq \min(p, |X| + |Y| - 1)$.

Ce résultat a été généralisé de plusieurs façons :

Théorème (Chowla, 1935). Si $\mathbb{A} = (\mathbb{Z}/m\mathbb{Z}, +)$ et $\emptyset \subsetneq X, Y \subseteq A$ sont t.q. $0 \in Y$ et $\gcd(m, y) = 1$ pour tout $y \in Y \setminus \{0\}$, alors $|X + Y| \geq \min(m, |X| + |Y| - 1)$.

Une autre généralisation aux groupes cycliques :

Théorème (Pillai, 1937). Supposons que $\mathbb{A} = (\mathbb{Z}/m\mathbb{Z}, +)$ et soient X et Y des sous-ensembles non-vides de A. Si $|Y| = 1$, on pose $\delta := 1$; sinon on définit δ comme le maximum de $\gcd(m, y - y_0)$ sur toutes les paires (y, y_0) d'éléments distincts de Y. Alors, $|X + Y| \geq \min(\delta^{-1}m, |X| + |Y| - 1)$.

On a établi :

1. une preuve alternative d'une généralisation *commune* des deux ;
2. une version plus forte du théorème de Pillai.

Cauchy-Davenport et quelques généralisations connues (2/2)

Plus précisément : étant donné un sous-ensemble non-vide X de $\mathbb{Z}/m\mathbb{Z}$, posons $\delta_X := 1$ si $|X| = 1$, sinon $\delta_X := \min_{x_0 \in X} \max_{x_0 \neq x \in X} \gcd(m, x - x_0)$.

Théorème 4. Supposons que $\mathbb{A} = (\mathbb{Z}/m\mathbb{Z}, +)$ et soient X, Y des sous-ensembles non-vides de A. Si $\delta := \min(\delta_X, \delta_Y)$, alors $|X + Y| \geq \min(\delta^{-1}m, |X| + |Y| - 1)$.

Une généralisation d'un type différent :

Théorème (Hamidoune & Károlyi, 2005). Si $\mathbb{A}$ est un groupe et X, Y sont des sous-ensembles non-vides de A, alors $|X + Y| \geq \min(\mathfrak{p}(A), |X| + |Y| - 1)$.

On retrouve le théorème suivant :

Théorème (Kemperman, 1956). Si $\mathbb{A}$ est un groupe t.q. l'ordre de chaque élément $z \neq 0$ est $\geq |X| + |Y| - 1$ et si X, Y sont des sous-ensembles non-vides de A, alors on a $|X + Y| \geq |X| + |Y| - 1$.

• • • Cas commutatif : folklore (par le théorème de Kneser). Cas fini : Károlyi (par Feit-Thompson). Cas général : Hamidoune (par la méthode isopérimétrique).

Deux théorèmes et une conjecture (1/3)

Si X est un sous-ensemble de A, on définit la *constante de Cauchy-Davenport* de X par

$$\gamma(X) := \sup_{x_0 \in X^\times} \inf_{x_0 \neq x \in X} \mathrm{ord}(x - x_0).$$

De plus, si $X_1, \ldots, X_n \subseteq A$ on définit

$$\gamma(X_1, \ldots, X_n) := \max_{1 \leq i \leq n} \gamma(X_i).$$

Théorème 5. Si $\mathbb{A}$ est un semi-groupe simplifiable (éventuellement non-commutatif) et X, Y sont des sous-ensembles non vides de A t.q. $\langle Y \rangle_{\mathbb{A}}$ est commutatif, alors $|X + Y| \geq \min(\gamma(Y), |X| + |Y| - 1)$.

On a le corollaire suivant (qui s'applique, en particulier, aux groupes commutatifs) :

Corollaire 1. Si $\mathbb{A}$ est un semi-groupe simplifiable et commutatif et X, Y sont des sous-ensembles non vides de A, alors $|X + Y| \geq \min(\gamma(X, Y), |X| + |Y| - 1)$.

On obtient le théorème 1 : si $\mathbb{A} = (\mathbb{Z}/m\mathbb{Z}, +)$, alors $\mathrm{ord}(z - z_0) = m/\gcd(m, z - z_0)$ pour tout $z_0, z \in A$, de façon que $\gamma(X, Y) = \delta^{-1} m$ si $\emptyset \subsetneq X, Y \subseteq A$.

Deux théorèmes et une conjecture (2/3)

De plus, on prouve le suivant :

Théorème 6. Si $\mathbb{A}$ est (un semi-groupe) simplifiable, commutatif ou non, et $X, Y \subseteq A$ sont non-vides, alors $|X+Y| \geq \min(\gamma(X+Y), |X|+|Y|-1)$.

Ce résultat est une généralisation, une abstraction, et une version plus forte du théoréme de Hamidoune-Károlyi :

Lemme 1. Si X, Y sont sous-ensembles de A, si $\mathbb{A}$ est simplifiable, et si $X^\times, Y^\times \neq \emptyset$, alors $\gamma(X,Y) \geq \min(\gamma(X), \gamma(Y)) \geq \gamma(X+Y) \geq \mathfrak{p}(A)$.

Ces inégalités peuvent bien être larges :

Exemple 1. Soient $m \in \mathbb{Z}$ et $p, q \in \mathbb{P}$ t.q. $2 \leq m < p < q$. On pose

$$X := \{mk \bmod n : k = 0, \ldots, p-1\} \quad \text{et} \quad Y := \{mk \bmod n : k = 1, \ldots, p\},$$

où $n := m \cdot p \cdot q$. On trouve $|X+Y| = 2p$, $\gamma(X) = \gamma(Y) = p \cdot q$ et $\gamma(X+Y) = q$, et d'autre partie, $\mathfrak{p}(\mathbb{Z}/n\mathbb{Z})$ est le plus petit diviseur premier de m. Donc,

$$\mathfrak{p}(\mathbb{Z}/n\mathbb{Z}) < \gamma(X+Y) < \min(\gamma(X), \gamma(Y)) = \gamma(X,Y),$$

et en fait $\mathfrak{p}(\mathbb{Z}/n\mathbb{Z}) \ll \gamma(X+Y)$ si $q \gg m$, et $\gamma(X+Y) \ll \gamma(X,Y)$ si $p \gg 2$.

Deux théorèmes et une conjecture (3/3)

Une comparaison :

(i) le théorème 2 est, en quelques sortes, bien plus fort que le théorème 3, parce qu'on peut avoir $\gamma(X, Y) \gg \gamma(X + Y)$ (exemple 1) ;

(ii) le théorème 3 est, en quelques sortes, bien plus général que le théorème 2, parce qu'il ne requiert aucune hypothèse de commutativité.

Cela nous amène à la conjecture suivante :

Conjecture 1. Si X, Y sont des sous-ensembles de A et $\mathbb{A}$ est simplifiable, alors on a : $|X + Y| \geq \min(\gamma(X, Y), |X| + |Y| - 1)$.

On pose aussi la question suivante :

Question 2. Si $X_1, \ldots, X_n$ sont sous-ensembles de A et $\mathbb{A}$ est simplifiable, c'est vrai que $|X_1 + \cdots + X_n| \geq \min(\gamma(X_1, \ldots, X_n), |X|_1 + \cdots + |X_n| + 1 - n)$?

On a trouvé que :

(i) la conjecture 1 est vraie pour $n = 2$ si $\langle X \rangle_{\mathbb{A}}$ et $\langle Y \rangle_{\mathbb{A}}$ sont commutatifs (théorème 2).

(ii) la question 2 a une réponse positive si $\mathbb{A}$ est simplifiable et sans torsion (lemme 1).

À propos des preuves des théorèmes 1 et 2

Les preuves (toutes les deux par l'absurde) sont combinatoires en reposant sur :

(i) les propriétés de la soustraction d'ensembles qu'on a introduit ;

(ii) une généralisation de la transformée classique de Davenport (pour le théorème 1) et une variante de la transformée de Kemperman (pour le théorème 2) ;

(iii) des propriétés d'invariance de la constante de Cauchy-Davenport par rapport à certaines transformations (en fait, des translations).

(iv) une induction qui part de l'existence d'un contre-exemple $(\bar{X}, \bar{Y})$ au théorème 1 t.q. $|\bar{Y}|$ est minimal (après les cas triviaux) ;

(v) une induction qui part d'un contre-exemple $(\bar{X}, \bar{Y})$ au théorème 2 t.q. la paire est "mini-maximal" dans le sens suivant : Si (X, Y) est un autre contre-exemple, alors (1) $|X + Y| < |\bar{X} + \bar{Y}|$ où (2) $|\bar{X} + \bar{Y}| = |X + Y|$ et

$$\text{(2a) } |X| + |Y| < |\bar{X}| + |\bar{Y}| \quad \text{où} \quad \text{(2b) } |\bar{X}| + |\bar{Y}| = |X| + |Y| \text{ et } |X| \leq |\bar{X}|.$$

• • • On remarque que les preuves des théorèmes 1 et 2 n'utilisent ni le théorème de Feit-Thompson ni la méthode isopérimétrique.

Théorie de Freiman et semi-groupes ordonnables

Soit $\mathbb{A} = (A, \cdot)$ un semi-groupe (en notation multiplicative), et soit $S \subseteq A$.

Une question typique de la théorie de Freiman : prouver que S est "bien structuré" dans l'hypothèse que $|S^2|$ est "petit" par rapport à $|S|$.

Théorème (Freiman et alii, à paraître). Si $\mathbb{A}$ est un groupe linéairement ordonnable (l.o.) et $|S^2| \leq 3|S| - 3$, alors le sous-groupe de $\mathbb{A}$ engendré par S est abélien.

Ici, on dit que $\mathbb{A}$ est un (semi-)groupe l.o. s'il existe un ordre total $\preceq$ sur A t.q.

$$\forall a, b, c \in A : a \prec b \quad \Longrightarrow \quad a \cdot c \prec b \cdot c \ \text{ et } \ c \cdot a \prec c \cdot b.$$

On a généralisé le théorème aux semi-groupes l.o. :

Théorème 7. Si $\mathbb{A}$ est un semi-groupe linéairement ordonnable et $|S^2| \leq 3|S| - 3$, alors $\langle S \rangle_{\mathbb{A}}$ est un sous-semigroupe abélien de $\mathbb{A}$.

• • • C'est une généralisation parce que, si $\mathbb{A}$ est un groupe et $\langle S \rangle_{\mathbb{A}}$ est abélien, alors le sous-groupe de $\mathbb{A}$ engendré par S est lui même abélien.

Quelques résultats secondaires

La preuve : même schéma général de la preuve du théorème de Freiman, mais il y a beaucoup de difficultés.

Lemme 2. Si $\mathbb{A}$ est un semi-groupe linéairement ordonnable et $a, b \in A$ sont t.q. $a^n b = ba^n$ pour un certain entier $n \geq 2$, alors $ab = ba$.

Cela généralise le lemme suivant (et en simplifie la preuve) :

Lemme 3 (Neumann, 1949). Si $\mathbb{A}$ est un groupe linéairement ordonnable et $a, b \in A$ sont t.q. $[a^n, b] = 1$ pour un certain entier $n \geq 2$, alors $[a, b] = 1$.

De plus, le lemme 2 implique le suivant :

Lemme 4. Si $\mathbb{A}$ est un groupe linéairement ordonnable, S est un sous-ensemble fini et non-vide de A, et $y \in A \setminus \mathrm{C}_{\mathbb{A}}(S)$, alors $|yS \cup Sy| \geq |S| + 1$.

Et on utilise ce dernier résultat pour prouver le suivant :

Théorème 8. Si $\mathbb{A}$ est un semi-groupe linéairement ordonnable et S est un sous-ensemble fini de A, alors $\mathrm{C}_{\mathbb{A}}(S) = \mathrm{N}_{\mathbb{A}}(S)$.

Vers des semi-groupes l.o. intéressants (1/3)

Il y a une question fondamentale qui se pose :

- Peut-on trouver quelque semi-groupe l.o. qui ne s'injecte pas dans un groupe l.o. ?

Un probléme ouvert pendant de nombreuses années : il a reçu une réponse positive par C. G. Chehata and A. A. Vinogradov (1953), et plus tard par R. E. Johnson (1969).

- Peut-on trouver des exemples un peu plus "naturels" ?

Cela m'a conduit à l'étude des semi-anneaux : un 4-uplet $\mathbb{K} = (K, +, \cdot)$ t.q.

(i) $(K, +)$ est un monoïde et $(K, \cdot)$ est un semi-groupe ;
(ii) $0 \cdot a = a \cdot 0 = 0$ pour tous les $a \in K$, où 0 est l'elément neutre de $(K, +)$;
(iii) la multiplication est distributive par rapport à l'addition.

On dit que $\mathbb{A}$ est un semi-anneau l.o. s'il existe un ordre total $\preceq$ sur K t.q. :

(iv) $(K, +, \preceq)$ est un semi-groupe l.o. ;
(v) $ab \prec ac$ et $ba \prec ca$ pour tous $a, b, c \in K$ t.q. $0 \prec a$ et $b \prec c$.

Alors on dit que $(K, +, \cdot, \preceq)$ est un semi-anneau linéairement ordonné.

Vers des semi-groupes l.o. intéressants (2/3)

Supposons que $\mathbb{A}_\sharp = (A, +, \cdot, \preceq)$ est un semi-anneau l.o., et soient $\mathbb{A} := (A, +, \cdot)$ et $n \in \mathbb{N}^+$. On écrit $\mathcal{M}_n(\mathbb{A})$ pour le semi-anneau des matrices $n \times n$.

Théorème 9. Soit $\mathcal{U}_n(\mathbb{A}_\sharp^+)$ le sous-semi-groupe de $(\mathcal{M}_n(\mathbb{A}), \cdot)$ qui consiste en les matrices triangulaires supérieures dont les éléments sur ou au-dessus de la diagonale principale sont positifs par rapport à $\mathbb{A}_\sharp$. Alors $\mathcal{U}_n(\mathbb{A}_\sharp^+)$ est un semi-groupe l.o.

On pose la question suivante :

Question 3. $\mathcal{U}_n(\mathbb{A}_\sharp^+)$, s'injecte-t-il dans un groupe l.o. ?

Soit $\mathcal{L}_n(\mathbb{A}_\sharp^+)$ le semi-groupe des matrices transposées de $\mathcal{U}_n(\mathbb{A}_\sharp^+)$, et soit $\mathcal{T}_n(\mathbb{A}_\sharp^+)$ le plus petit sous-semi-groupe de $(\mathcal{M}_n(\mathbb{A}), \cdot)$ qui contient $\mathcal{U}_n(\mathbb{A}_\sharp^+) \cup \mathcal{L}_n(\mathbb{A}_\sharp^+)$.

Question 4. $\mathcal{T}_n(\mathbb{A}_\sharp^+)$, est-il l.o. ? Si oui, s'injecte-t-il dans un groupe l.o. ?

• • • Des réponses négatives donneraient des exemples plus "naturels" que ceux déjà connus.

Vers des semi-groupes l.o. intéressants (3/3)

Un autre exemple : Supposons que $\mathbb{K} = (K, +, \cdot)$ est un semi-anneau et $\mathbb{A} = (A, \diamond)$ est un semi-groupe. On écrit $K[A]$ pour l'ensemble de toutes les fonctions $f : A \to K$ t.q. $f^{-1}(0_K)$ est fini.

$K[A]$ devient un semi-anneau, ici noté $\mathbb{K}[\mathbb{A}]$, si on le dote des opérations d'addition ponctuelle et produit à la Cauchy induites par $\mathbb{A}$ et $\mathbb{K}$.

Théorème 10. Si $\mathbb{K}$ est un semi-anneau l.o. et $\mathbb{A}$ est un semi-groupe l.o., alors $\mathbb{K}[\mathbb{A}]$ est lui-même un semi-anneau l.o.

Cela implique la caractérisation suivante :

Théorème 11. $\mathbb{K}$ est un semi-anneau l.o. si et seulement si le semi-anneau des polynômes sur $\mathbb{K}$ à un nombre quelconque d'indéterminées commutatives (respectivement, non-commutatives) est lui-même l.o.

• • • Quand $\mathbb{K}$ est un semi-anneaux l.o. et $\mathbb{A}$ est un semi-groupe, on regarde le semi-groupe des eléments positifs de $\mathbb{K}[\mathbb{A}]$.

Références

- Chapitre I : S. Tringali, *A Cauchy-Davenport theorem for semigroups,* à paraître dans Uniform Distribution Theory, 16 pages (preprint : arXiv/1210.4203)
- Chapitre II : S. Tringali, *Cauchy-Davenport type theorems for semigroups*, soumis, 19 pages (preprint : arXiv/1307.8396)
- Chapitre III : S. Tringali, *Small doubling in ordered semigroups,* soumis, 15 pages (preprint : arXiv/1208.3233)
- Chapitre IV : S. Tringali, *On the divisibility of $a^n \pm b^n$ by powers of n,* Integers, vol. 13, no. A71 (nov 2013), pp. 1–6 (preprint : arXiv/1301.0131)
- Chapitre V : P. Leonetti and S. Tringali, *On a system of equations with primes,* à paraître dans Journal de Théorie des Nombres de Bordeaux, 15 pages (preprint : arXiv/1212.0802)

Merci pour votre attention !