Combinatorial and Additive Number Theory 2016

Additive combinatorics methods in associative algebras

Vincent Beck

Université d'Orléans

7 janvier 2016

Credits

Thanks to the organizers

Credits

Thanks to the organizers

Joint work with Cédric Lecouvey of Université de Tours

Preprint : arXiv:1504.02287

Supported by ANR-12-JS01-0003-01 ACORT grant

Kneser's and Diderrich's Theorems

Theorem Let G be a group and A, B finite non empty subsets of G. Assume A is a commutative subset of G (that is to say $aa' = a'a$ for every a, a' in A) and let $H := \{g \in G, gAB = AB\}$. We have

$$|AB| \geqslant |A| + |B| - |H|.$$

Main idea of the proof
Dyson e-transform : fix $e \in B$ and let $A' = A \cap Be^{-1}$ and $B' = Ae \cup B$. We have $A'B' \subset AB$ and $|A'| + |B'| = |A| + |B|$.

Motivations

Is it possible to replace groups by more complex algebraic structures (fields, associative algebras over a field) ?

Motivations

Is it possible to replace groups by more complex algebraic structures (fields, associative algebras over a field) ?

$$\text{Group} \longrightarrow \text{field, algebra}$$

Motivations

Is it possible to replace groups by more complex algebraic structures (fields, associative algebras over a field) ?

$$\begin{aligned} \text{Group} &\longrightarrow \text{ field, algebra} \\ \text{Combinatorics} &\longrightarrow \text{ linear algebra} \end{aligned}$$

Motivations

Is it possible to replace groups by more complex algebraic structures (fields, associative algebras over a field) ?

$$\text{Group} \longrightarrow \text{ field, algebra}$$
$$\text{Combinatorics} \longrightarrow \text{ linear algebra}$$

In the rest of the talk, k will be an infinite field

Field extensions

Theorem – X.D.Hou, K.H.Leung, Q.Xiang (2002)-Kainrath (2005). Let K be a field extension of k. Assume every algebraic element in K is separable over k. Let A and B be two nonempty finite subsets of K^*. Then

$$\dim_k(AB) \geqslant \dim_k(A) + \dim_k(B) - \dim_k(H) \qquad (1)$$

where $H := \{h \in K \mid h\langle AB\rangle_{k-vs} \subseteq \langle AB\rangle_{k-vs}\}$ and $\dim_k(C)$ stands for $\dim_k(\langle C\rangle_{k-vs})$ for every finite subset C of K.

Field extensions

Theorem – X.D.Hou, K.H.Leung, Q.Xiang (2002)-Kainrath (2005). Let K be a field extension of k. Assume every algebraic element in K is separable over k. Let A and B be two nonempty finite subsets of K^*. Then

$$\dim_k(AB) \geqslant \dim_k(A) + \dim_k(B) - \dim_k(H) \tag{1}$$

where $H := \{h \in K \mid h\langle AB\rangle_{k-vs} \subseteq \langle AB\rangle_{k-vs}\}$ and $\dim_k(C)$ stands for $\dim_k(\langle C\rangle_{k-vs})$ for every finite subset C of K.

Main ideas of the proof

Dyson e-transform,

Field extensions

Theorem – X.D.Hou, K.H.Leung, Q.Xiang (2002)-Kainrath (2005). Let K be a field extension of k. Assume every algebraic element in K is separable over k. Let A and B be two nonempty finite subsets of K^*. Then

$$\dim_k(AB) \geqslant \dim_k(A) + \dim_k(B) - \dim_k(H) \qquad (1)$$

where $H := \{h \in K \mid h\langle AB\rangle_{k-vs} \subseteq \langle AB\rangle_{k-vs}\}$ and $\dim_k(C)$ stands for $\dim_k(\langle C\rangle_{k-vs})$ for every finite subset C of K.

Main ideas of the proof

Dyson e-transform, Vandermonde determinant,

Field extensions

Theorem – X.D.Hou, K.H.Leung, Q.Xiang (2002)-Kainrath (2005). Let K be a field extension of k. Assume every algebraic element in K is separable over k. Let A and B be two nonempty finite subsets of K^*. Then

$$\dim_k(AB) \geqslant \dim_k(A) + \dim_k(B) - \dim_k(H) \qquad (1)$$

where $H := \{h \in K \mid h\langle AB\rangle_{k-vs} \subseteq \langle AB\rangle_{k-vs}\}$ and $\dim_k(C)$ stands for $\dim_k(\langle C\rangle_{k-vs})$ for every finite subset C of K.

Main ideas of the proof

Dyson e-transform, Vandermonde determinant, pigeonhole principle

Applications

Theorem – Kneser's theorem. Let G be an abelian group and A, B finite non empty subsets of G, and $H := \{g \in G,\ gAB = AB\}$. We have

$$|AB| \geqslant |A| + |B| - |H|.$$

Applications

Theorem – Kneser's theorem. Let G be an abelian group and A, B finite non empty subsets of G, and $H := \{g \in G,\ gAB = AB\}$. We have

$$|AB| \geqslant |A| + |B| - |H|.$$

Main ideas of the proof

Realize $G = \langle A, B \rangle_{gr}$ as the Galois group of a field extension (of field of fractions) $k \hookrightarrow K$, define a map from G to K and use Galois correspondence theorem.

The algebra case

Question : Can we replace K by an associative algebra $\mathcal{A}$ in Hou, Leung and Xiang's or Kainrath's theorem ?

The algebra case

Question : Can we replace K by an associative algebra $\mathcal{A}$ in Hou, Leung and Xiang's or Kainrath's theorem ?

Answer : Of course, not ! Because of zero divisors : we can have $AB = 0$ for a big subspaces A and B of $\mathcal{A}$.

The algebra case

Question : Can we replace K by an associative algebra $\mathcal{A}$ in Hou, Leung and Xiang's or Kainrath's theorem ?

Answer : Of course, not ! Because of zero divisors : we can have $AB = 0$ for a big subspaces A and B of $\mathcal{A}$.

$\longrightarrow$ Hypothesis on A and B : $\langle A \rangle_{k-vs}$ and $\langle B \rangle_{k-vs}$ contain an invertible element.

The algebra case

Question : Can we replace K by an associative algebra $\mathcal{A}$ in Hou, Leung and Xiang's or Kainrath's theorem ?

Answer : Of course, not ! Because of zero divisors : we can have $AB = 0$ for a big subspaces A and B of $\mathcal{A}$.

$\longrightarrow$ Hypothesis on A and B : $\langle A\rangle_{k-vs}$ and $\langle B\rangle_{k-vs}$ contain an invertible element.

$\longrightarrow$ unformal Hypothesis on $\mathcal{A}$: "it is easy to construct invertibles elements in $\mathcal{A}$".

The algebra case

Question : Can we replace K by an associative algebra $\mathcal{A}$ in Hou, Leung and Xiang's or Kainrath's theorem ?

Answer : Of course, not ! Because of zero divisors : we can have $AB = 0$ for a big subspaces A and B of $\mathcal{A}$.

$\longrightarrow$ Hypothesis on A and B : $\langle A \rangle_{k-vs}$ and $\langle B \rangle_{k-vs}$ contain an invertible element.

$\longrightarrow$ unformal Hypothesis on $\mathcal{A}$: "it is easy to construct invertibles elements in $\mathcal{A}$".

More precisely, we assume that $\mathcal{A}$ is of either one of the following type finite dimensional algebras, Banach algebras or finite products of field extensions of k.

In particular, for all $a \in \mathcal{A}$ there exists $\lambda \in k$ such that $a - \lambda 1$ is invertible in $\mathcal{A}$.

Diderrich's theorem for algebras

Theorem – B., Lecouvey (2015). Assume $\mathcal{A}$ is isomorphic to a subalgebra of an algebra of the three preceeding types.

Assume A and B to be two finite nonempty subsets of $\mathcal{A}$ such that $\langle A\rangle_{k-vs.} \cap U(\mathcal{A}) \neq \varnothing$ and $\langle B\rangle_{k-vs.} \cap U(\mathcal{A}) \neq \varnothing$.

Assume that A is commutative and $\mathbb{A}(A)$ admits a finite number of finite-dimensional subalgebras.

Let $\mathcal{H} := \{x \in \mathcal{A}, x\langle AB\rangle_{k-vs} \subset \langle AB\rangle_{k-vs}\}$.

We have

$$\dim_k(AB) \geqslant \dim_k(A) + \dim_k(B) - \dim(\mathcal{H})$$

Sketch of proof of the theorem

Lemma Assume $\mathcal{A}$ is of one of the three preceeding types.

Let A and B be two finite subsets of $\mathcal{A}$ such that A is commutative, $\langle A\rangle_{k-vs.} \cap U(\mathcal{A}) \neq \varnothing$ and $\langle B\rangle_{k-vs.} \cap U(\mathcal{A}) \neq \varnothing$.

Then, for each $a \in \langle A\rangle_{k-vs} \cap U(\mathcal{A})$, there exists a (commutative) finite-dimensional subalgebra $\mathcal{A}_a$ of $\mathcal{A}$ such that $\mathcal{A}_a \subseteq \mathbb{A}(A)$ and a vector space V_a contained in $\langle AB\rangle_{k-vs}$ such that $V_a \cap U(\mathcal{A}) \neq \varnothing$, $\mathcal{A}_a V_a = V_a$, $\langle aB\rangle_{k-vs} \subseteq V_a$ and

$$\dim_k(V_a) + \dim_k(\mathcal{A}_a) \geqslant \dim_k(A) + \dim_k(B).$$

Sketch of proof of the theorem

Lemma Assume $\mathcal{A}$ is of one of the three preceeding types.

Let A and B be two finite subsets of $\mathcal{A}$ such that A is commutative, $\langle A\rangle_{k-vs.} \cap U(\mathcal{A}) \neq \varnothing$ and $\langle B\rangle_{k-vs.} \cap U(\mathcal{A}) \neq \varnothing$.

Then, for each $a \in \langle A\rangle_{k-vs} \cap U(\mathcal{A})$, there exists a (commutative) finite-dimensional subalgebra $\mathcal{A}_a$ of $\mathcal{A}$ such that $\mathcal{A}_a \subseteq \mathbb{A}(A)$ and a vector space V_a contained in $\langle AB\rangle_{k-vs}$ such that $V_a \cap U(\mathcal{A}) \neq \varnothing$, $\mathcal{A}_a V_a = V_a$, $\langle aB\rangle_{k-vs} \subseteq V_a$ and

$$\dim_k(V_a) + \dim_k(\mathcal{A}_a) \geqslant \dim_k(A) + \dim_k(B).$$

Proof of Lemma e-Dyson transform, recursion on dimension of $\langle A\rangle_{k-vs}$; the type of $\mathcal{A}$ ensures us that at each step there are enough invertible elements in $\langle A\rangle_{k-vs}$.

Sketch of proof of the theorem

Let $(x_1, \ldots, x_n)$ be a basis of $\langle A \rangle_{k-vs}$ with x_1 invertible.

For any $\alpha \in k$, set $x_\alpha = x_1 + \alpha x_2 + \cdots + \alpha^{n-1} x_n$.

For each α such that x_α is invertible (there exists an infinity of such α), there exists a finite-dimensional subalgebra $\mathcal{A}_\alpha$ and a subspace V_α such in the preceeding lemma.

Since $\mathbb{A}(A)$ has only a finite number of subalgebras, there exists n distincts elements of k, $\alpha_1, \ldots, \alpha_n$ such that $\mathcal{B} := \mathcal{A}_{\alpha_1} = \cdots = \mathcal{A}_{\alpha_n}$. Moreover $(x_{\alpha_1}, \ldots, x_{\alpha_n})$ is a basis of $\langle A \rangle_{k-vs}$.

We have $\mathcal{B} \subset \mathcal{H}$.

A first example

Example Let $\mathscr{C}$ the Banach algebra of continuous functions from $[0,1]$ into $\mathbb{R}$. Let V and W be finite dimensional subspaces containing a positive function. We have
$\dim_{\mathbb{R}}(VW) \geqslant \dim_{\mathbb{R}}(V) + \dim_{\mathbb{R}}(W) - 1$.

Back to Kneser-Diderrich's theorem for groups

Let G be a group and A, B finite non empty subsets of G. Assume A is a commutative subset of G and let $H := \{g \in G, gAB = AB\}$.

$$|AB| \geqslant |A| + |B| - |H|.$$

Back to Kneser-Diderrich's theorem for groups

Let G be a group and A, B finite non empty subsets of G. Assume A is a commutative subset of G and let $H := \{g \in G, gAB = AB\}$.

$$|AB| \geqslant |A| + |B| - |H|.$$

Going to algebras. We consider $\mathcal{A} = \mathbb{C}[G]$. This is a subalgebra of a Banach algebra.

The algebra $\mathbb{A}(A) \overset{\mathbb{C}\text{-alg.}}{\simeq} \mathbb{C}[X_1^{\pm 1}, \ldots, X_n{}^{\pm 1}]^r$ has only a finite number of finite dimensional subalgebras.

The stabilizer of $\langle AB \rangle_{\mathbb{C}-vs}$ in $\mathbb{C}[G]$ is $\mathbb{C}[H]$.

Diderrich's theorem in $\mathbb{C}[G]$ gives Didderich's theorem for G.