A linear analogue of Kneser's theorem

Speaker: Qing Xiang

February 26, 2016

The speaker gave an elegant lecture on an interesting result in additive combinatorics.

Suppose that A and B are subsets of an additive group G, and let $A + B$ be the sumset

$$A + B := \{a + b : a \in A,\ b \in B\}.$$

Here is perhaps the easiest theorem in additive combinatorics: if $G = \mathbb{Z}$, then

$$|A + B| \geq |A| + |B| - 1. \tag{1}$$

Proof: add the minimal element of A to everything in B, and the maximal element of B to everything in A; these sets can only have the one obvious common element.

If $G = \mathbb{Z}/p$, then we have

$$|A + B| \geq \min\{p, |A| + |B| - 1\}.$$

This turns out to be much more difficult! Indeed, it has a name: the Cauchy-Davenport theorem. (It seems that Davenport came up with a proof, and then realized that he had been scooped some 120 years ago.) The speaker presented a complete proof. Since he was using slides I was unable to follow all the details, but the idea was clear enough. For any $e \in G$, define the *Dyson e-transform* to be a certain tweaking of the sets A and B which leaves certain properties intact; then prove that with enough e-transforms you can reduce to a case for which the result is trivial, allowing for a proof by induction.

Kneser's theorem says that for a general additive group G we have

$$|A + B| \geq |A| + |B| - |H(A + B)|,$$

where $H(S)$, the stabilizer of S, is defined by

$$H(S) := \{g \in G \ : \ g + S = S\}.$$

This immediately implies Cauchy-Davenport: $H(S)$ must be a subgroup of G, and if $G = \mathbb{Z}/p\mathbb{Z}$ then $H(S)$ must be trivial or all of $\mathbb{Z}/p\mathbb{Z}$, and in the latter case $A + B$ must be trivial or all of $\mathbb{Z}/p\mathbb{Z}$. (Presumably the latter: a pedant would gripe that (1) is false if both A and B are empty.)

The speaker discussed a variety of generalizations where K/k is a field extension, and A and B are k-subspaces. Here one replaces $A + B$ with the k-span of all products ab. Strikingly, the proof is easier, but this version implies the original version of Kneser's theorem, as one can show by cooking a field extension specialized for the proof.