SUPPLEMENTARY LECTURE NOTES : WEEK 48

MONDAY, NOVEMBER 29

**Definition 1.1.** Let $(G, +)$ be any abelian semigroup, $A$ and $B$ two subsets of $G$. The *sumset* $A + B$ is defined as

$$A + B = \{a + b : a \in A,\ b \in B\}. \tag{1.1}$$

**Proposition 1.2.** *If $G = \mathbb{Z}$ or, more generally, a sub-semigroup of any totally ordered group, and $A, B$ are two finite subsets of $G$, then*

$$|A + B| \geq |A| + |B| - 1. \tag{1.2}$$

*Proof.* Let $|A| = m$, $|B| = n$ and write the elements of each set in increasing order, say

$$A = \{a_1 < a_2 < \cdots < a_m\}, \quad B = \{b_1 < b_2 < \cdots < b_n\}. \tag{1.3}$$

Then we can explicitly write down a strictly increasing sequence of $m+n-1$ elements in $A + B$, for example

$$a_1 + b_1 < a_1 + b_2 < \cdots < a_1 + b_n < a_2 + b_n < \cdots < a_m + b_n. \tag{1.4}$$

□

This proposition does not hold in general. For example, if $H$ is a finite subgroup of $G$ and $A = B = H$, then $A+B = H$ also. However, there is an appropriate generalisation of the proposition to arbitrary abelian groups, known as *Kemperman's theorem*. Here we will only discuss the special (and most important) case where $G = \mathbb{Z}_p$, for some prime $p$.

**Theorem 1.3. (Cauchy-Davenport-Chowla)** *Let $p$ be a prime and let $A, B$ be subsets of $\mathbb{Z}_p$. Then*

$$|A + B| \geq \min\{p, |A| + |B| - 1\}. \tag{1.5}$$

*Proof.* Let $|A| = r$, $|B| = s$. First note that it suffices to prove that

$$r + s - 1 \leq p \Rightarrow |A + B| \geq r + s - 1. \tag{1.6}$$

For if $r + s - 1 > p$, then we can just remove some elements from $A$ and/or $B$ and thus obtain subsets $A' \subseteq A$, $B' \subseteq B$ such that $|A'| + |B'| - 1 = p$. Once we know that $|A' + B'| = p$, then one must also have $|A + B| = p$, since $A' + B' \subseteq A + B$.

So let's assume (1.6). We then proceed by induction on $s = |B|$. If $s = 1$, then $B = \{b\}$ is a singelton set and $A + B = A + \{b\}$ is just a translation of the set $A$. Hence, in this case, $|A + B| = |A| = r = r + s - 1$.

So now suppose $s > 1$ and that (1.6) holds for all smaller values of $s$. Note that the theorem is also trivial if $r = p$, so we may assume that $r < p$. Now choose any non-zero element $b \in B$ (since $s > 1$ such an element exists) and consider

$$X = \{a + b : a \in A\}. \tag{1.7}$$

I claim that $X$ cannot coincide with $A$. For, if it did, then we would have

$$\sum_{a \in A} a = \sum_{x \in X} x = \sum_{a \in A} (a + b) = \sum_{a \in A} a + rb, \tag{1.8}$$

which would imply that $rb = 0$ in $\mathbb{Z}_p$. But this is not possible since $p$ is prime, $r < p$ and $b \neq 0$. Thus $X \neq A$ and so there exists $c \in A$ such that $c + b \notin A$. Fix a choice of such a $c$, and let

$$C := \{b \in B : c + b \notin A\}. \tag{1.9}$$

Now let $A_1, B_1$ be the following two sets :

$$A_1 := A \sqcup (\{c\} + C), \quad B_1 := B \backslash C. \tag{1.10}$$

Note that the definition of the set $C$ implies that the disjoint union above really is a *disjoint* union. Hence it follows that $|A_1| + |B_1| = |A| + |B|$. Moreover, $|B_1| < |B|$ since, by assumption, the set $C$ is non-empty. Moreover, since WLOG $0 \in B$, we may assume that $B_1$ is non-empty. Hence we can apply the induction hypothesis to conclude that

$$|A_1 + B_1| \geq |A_1| + |B_1| - 1 = r + s - 1. \tag{1.11}$$

To complete the proof, it thus suffices to show that

$$A_1 + B_1 \subseteq A + B. \tag{1.12}$$

So let $a_1 \in A_1$ and $b_1 \in B_1$. There are two cases to consider :

*Case 1* : $a_1 \in A$.

Then $b_1 \in B_1 \subseteq B$, so $a_1 + b_1 \in A + B$ as desired.

*Case 2* : $a_1 \notin A$.

Then there exists $x \in C$ such that $a_1 = c + x$. Thus $a_1 + b_1 = (c + x) + b_1 = (c + b_1) + x$. Now $x \in C \subseteq B$, so $x \in B$. Also $b_1 \in B_1 = B \backslash C$ so, by definition of the set $C$, this means that $c + b_1 \in A$. Hence $(c + b_1) + x = a_1 + b_1 \in A + B$, and the proof is complete. $\square$