

# Kneser's Theorem and the Cauchy–Davenport Theorem

Mantas Bakšys and Angeliki Koutsoukou-Argyraiki  
University of Cambridge  
{mb2412, ak2110}@cam.ac.uk

June 6, 2026

## Abstract

We formalise Kneser's Theorem in combinatorics [2, 3] following the proof from the 2014 paper "A short proof of Kneser's addition theorem for abelian groups" by Matt DeVos [1]. We also show a strict version of Kneser's Theorem as well as the Cauchy–Davenport Theorem as a corollary of Kneser's Theorem.

## Contents

<b>1 Preliminaries</b>	<b>3</b>
1.1 Elementary lemmas on sumsets . . . . .	3
1.2 Stabilizer and basic properties . . . . .	5
1.3 Convergent . . . . .	10
1.4 Technical lemmas from DeVos’s proof of Kneser’s Theorem .	10
1.5 A function that picks coset representatives randomly . . . . .	11
1.6 Useful group-theoretic results . . . . .	14
<b>2 Kneser’s Theorem and the Cauchy–Davenport Theorem: main proofs</b>	<b>14</b>
2.1 Proof of Kneser’s Theorem . . . . .	14
2.2 Strict version of Kneser’s Theorem . . . . .	14
2.3 The Cauchy–Davenport Theorem . . . . .	15

## Acknowledgements

Angeliki Koutsoukou-Argyraki is funded by the ERC Advanced Grant ALEXANDRIA (Project GA 742178) funded by the European Research Council and led by Lawrence C. Paulson (University of Cambridge, Department of Computer Science and Technology). Mantas Bakšys received funding for his internship supervised by Koutsoukou-Argyraki by the Cambridge Mathematics Placements (CMP) Programme and by the ALEXANDRIA Project. We wish to thank Manuel Eberl for his useful suggestion for treating induction when there is a type discrepancy between the induction hypothesis and the induction step.

# 1 Preliminaries

**theory** *Kneser-Cauchy-Davenport-preliminaries*

**imports**

*Complex-Main*

*Pluenecke-Ruzsa-Inequality.Pluenecke-Ruzsa-Inequality*

*HOL-Number-Theory.Prime-Powers*

**begin**

**context** *subgroup-of-group*

**begin**

**interpretation** *left: left-translations-of-group*  $\langle$ *proof* $\rangle$

**interpretation** *right: right-translations-of-group*  $\langle$ *proof* $\rangle$

**interpretation** *transformation-group left.translation* ‘  $H G$   $\langle$ *proof* $\rangle$

**lemma** *Right-Coset-eq-iff:*

**assumes**  $x \in G$  **and**  $y \in G$

**shows**  $H \cdot x = (H \cdot y) \iff H \cdot x \cap (H \cdot y) \neq \{\}$

$\langle$ *proof* $\rangle$

**end**

**context** *additive-abelian-group*

**begin**

## 1.1 Elementary lemmas on sumsets

**lemma** *sumset-translate-eq-right:*

**assumes**  $A \subseteq G$  **and**  $B \subseteq G$  **and**  $x \in G$

**shows**  $(\text{sumset } A \{x\} = \text{sumset } B \{x\}) \iff A = B$   $\langle$ *proof* $\rangle$

**lemma** *sumset-translate-eq-left:*

**assumes**  $A \subseteq G$  **and**  $B \subseteq G$  **and**  $x \in G$

**shows**  $(\text{sumset } \{x\} A = \text{sumset } \{x\} B) \iff A = B$   $\langle$ *proof* $\rangle$

**lemma** *differenceset-translate-eq-right:*

**assumes**  $A \subseteq G$  **and**  $B \subseteq G$  **and**  $x \in G$

**shows**  $(\text{differenceset } A \{x\} = \text{differenceset } B \{x\}) \iff A = B$   $\langle$ *proof* $\rangle$

**lemma** *differenceset-translate-eq-left:*

**assumes**  $A \subseteq G$  **and**  $B \subseteq G$  **and**  $x \in G$

**shows**  $(\text{differenceset } \{x\} A = \text{differenceset } \{x\} B) \iff A = B$   $\langle$ *proof* $\rangle$

**lemma** *sumset-inter-union-subset*:

*sumset*  $(A \cap B) (A \cup B) \subseteq \text{sumset } A B$

*<proof>*

**lemma** *differenceset-group-eq*:

$G = \text{differenceset } G G$

*<proof>*

**lemma** *card-sumset-singleton-subset-eq*:

**assumes**  $a \in G$  **and**  $A \subseteq G$

**shows**  $\text{card } (\text{sumset } \{a\} A) = \text{card } A$

*<proof>*

**lemma** *card-differenceset-singleton-mem-eq*:

**assumes**  $a \in G$  **and**  $A \subseteq G$

**shows**  $\text{card } A = \text{card } (\text{differenceset } A \{a\})$

*<proof>*

**lemma** *card-singleton-differenceset-eq*:

**assumes**  $a \in G$  **and**  $A \subseteq G$

**shows**  $\text{card } A = \text{card } (\text{differenceset } \{a\} A)$

*<proof>*

**lemma** *sumset-eq-Union-left*:

**assumes**  $A \subseteq G$

**shows**  $\text{sumset } A B = (\bigcup a \in A. \text{sumset } \{a\} B)$

*<proof>*

**lemma** *sumset-eq-Union-right*:

**assumes**  $B \subseteq G$

**shows**  $\text{sumset } A B = (\bigcup b \in B. \text{sumset } A \{b\})$

*<proof>*

**lemma** *sumset-singletons-eq*:

**assumes**  $a \in G$  **and**  $b \in G$

**shows**  $\text{sumset } \{a\} \{b\} = \{a \oplus b\}$

*<proof>*

**lemma** *sumset-eq-subset-differenceset*:

**assumes**  $K \subseteq G$  **and**  $K \neq \{\}$  **and**  $A \subseteq G$  **and**  $\text{sumset } A K = \text{sumset } B K$

**shows**  $A \subseteq \text{differenceset } (\text{sumset } B K) K$

*<proof>*

**end**

**locale** *subgroup-of-additive-abelian-group* =

*subgroup-of-abelian-group*  $H G (\oplus) \mathbf{0}$  + *additive-abelian-group*  $G (\oplus) \mathbf{0}$

**for**  $H G$  **and** *addition* (*infixl*  $\langle \oplus \rangle$  65) **and** *zero* ( $\langle \mathbf{0} \rangle$ )

**begin**

**notation** *Left-Coset* (**infixl**  $\langle \cdot | \rangle$  70)

**lemma** *Left-Coset-eq-sumset*:

**assumes**  $x \in G$

**shows**  $\text{sumset } \{x\} H = x \cdot | H$

*<proof>*

**lemma** *sumset-subgroup-eq-iff*:

**assumes**  $a \in G$  **and**  $b \in G$

**shows**  $\text{sumset } \{a\} H = \text{sumset } \{b\} H \iff$

$(\text{sumset } \{a\} H) \cap (\text{sumset } \{b\} H) \neq \{\}$

*<proof>*

**lemma** *card-divide-sumset*:

**assumes**  $A \subseteq G$

**shows**  $\text{card } H \text{ dvd } \text{card } (\text{sumset } A H)$

*<proof>*

**lemma** *sumset-subgroup-eq-Class-Union*:

**assumes**  $A \subseteq G$

**shows**  $\text{sumset } A H = (\bigcup (\text{Class } 'A))$

*<proof>*

**lemma** *Class-image-sumset-subgroup-eq*:

**assumes**  $A \subseteq G$

**shows**  $\text{Class } ' (\text{sumset } A H) = \text{Class } ' A$

*<proof>*

**lemma** *Class-cover-imp-subset-or-disj*:

**assumes**  $A = (\bigcup (\text{Class } ' C))$  **and**  $x \in G$  **and**  $C \subseteq G$

**shows**  $\text{Class } x \subseteq A \vee \text{Class } x \cap A = \{\}$

*<proof>*

**end**

**context** *additive-abelian-group*

**begin**

## 1.2 Stabilizer and basic properties

We define the stabilizer or group of periods of a nonempty subset of an abelian group.

**definition** *stabilizer*::'a set  $\Rightarrow$  'a set **where**

*stabilizer*  $S \equiv \{x \in G. \text{sumset } \{x\} (S \cap G) = S \cap G\}$

**lemma** *stabilizer-is-subgroup*: **fixes**  $S :: 'a$  set  
**shows** *subgroup (stabilizer S) G (⊕) 0*  
 ⟨proof⟩

**interpretation** *subgroup-of-additive-abelian-group stabilizer A G (⊕) 0*  
 ⟨proof⟩

**lemma** *zero-mem-stabilizer*:  $0 \in \text{stabilizer } A$  ⟨proof⟩

**lemma** *stabilizer-is-nonempty*:  
**shows** *stabilizer S ≠ {}*  
 ⟨proof⟩

**lemma** *Left-Coset-eq-sumset-stabilizer*:  
**assumes**  $x \in G$   
**shows** *sumset {x} (stabilizer B) = x · | (stabilizer B)*  
 ⟨proof⟩

**lemma** *stabilizer-subset-difference-singleton*:  
**assumes**  $S \subseteq G$  **and**  $s \in S$   
**shows** *stabilizer S ⊆ differenceset S {s}*  
 ⟨proof⟩

**lemma** *stabilizer-subset-singleton-difference*:  
**assumes**  $S \subseteq G$  **and**  $s \in S$   
**shows** *stabilizer S ⊆ differenceset {s} S*  
 ⟨proof⟩

**lemma** *stabilizer-subset-nempty*:  
**assumes**  $S \neq \{\}$  **and**  $S \subseteq G$   
**shows** *stabilizer S ⊆ differenceset S S*  
 ⟨proof⟩

**lemma** *stabilizer-coset-subset*:  
**assumes**  $A \subseteq G$  **and**  $x \in A$   
**shows** *sumset {x} (stabilizer A) ⊆ A*  
 ⟨proof⟩

**lemma** *stabilizer-subset-stabilizer-dvd*:  
**assumes** *stabilizer A ⊆ stabilizer B*  
**shows** *card (stabilizer A) dvd card (stabilizer B)*  
 ⟨proof⟩

**lemma** *stabilizer-coset-Un*:  
**assumes**  $A \subseteq G$   
**shows**  $(\bigcup x \in A. \text{sumset } \{x\} (\text{stabilizer } A)) = A$   
 ⟨proof⟩

**lemma** *stabilizer-empty*: *stabilizer {} = G*

*<proof>*

**lemma** *stabilizer-finite:*

**assumes**  $S \subseteq G$  **and**  $S \neq \{\}$  **and** *finite*  $S$

**shows** *finite* (*stabilizer*  $S$ )

*<proof>*

**lemma** *stabilizer-subset-group:*

**shows** *stabilizer*  $S \subseteq G$  *<proof>*

**lemma** *sumset-stabilizer-eq-iff:*

**assumes**  $a \in G$  **and**  $b \in G$

**shows**  $\text{sumset } \{a\} (\text{stabilizer } A) = \text{sumset } \{b\} (\text{stabilizer } A) \iff$   
 $(\text{sumset } \{a\} (\text{stabilizer } A)) \cap (\text{sumset } \{b\} (\text{stabilizer } A)) \neq \{\}$

*<proof>*

**lemma** *sumset-stabilizer-eq-Class-Union:*

**assumes**  $A \subseteq G$

**shows**  $\text{sumset } A (\text{stabilizer } B) = (\bigcup (\text{Class } B \text{ ' } A))$

*<proof>*

**lemma** *card-stabilizer-divide-sumset:*

**assumes**  $A \subseteq G$

**shows**  $\text{card} (\text{stabilizer } B) \text{ dvd } \text{card} (\text{sumset } A (\text{stabilizer } B))$

*<proof>*

**lemma** *Class-image-sumset-stabilizer-eq:*

**assumes**  $A \subseteq G$

**shows**  $\text{Class } B \text{ ' } (\text{sumset } A (\text{stabilizer } B)) = \text{Class } B \text{ ' } A$

*<proof>*

**lemma** *Class-cover-imp-subset-or-disj:*

**assumes**  $A = (\bigcup (\text{Class } B \text{ ' } C))$  **and**  $x \in G$  **and**  $C \subseteq G$

**shows**  $\text{Class } B \ x \subseteq A \vee \text{Class } B \ x \cap A = \{\}$

*<proof>*

**lemma** *stabilizer-sumset-disjoint:*

**fixes**  $S1 \ S2 :: 'a \text{ set}$

**assumes**  $\text{stabilizer } S1 \cap \text{stabilizer } S2 = \{0\}$  **and**  $S1 \subseteq G$  **and**  $S2 \subseteq G$

**and** *finite*  $S1$  **and** *finite*  $S2$  **and**  $S1 \neq \{\}$  **and**  $S2 \neq \{\}$

**shows**  $\text{card} (\text{sumset} (\text{stabilizer } S1) (\text{stabilizer } S2)) =$

$\text{card} (\text{stabilizer } S1) * \text{card} (\text{stabilizer } S2)$

*<proof>*

**lemma** *stabilizer-sub-sumset-left:*

$\text{stabilizer } A \subseteq \text{stabilizer} (\text{sumset } A \ B)$

*<proof>*

**lemma** *stabilizer-sub-sumset-right:*

*stabilizer*  $B \subseteq \text{stabilizer} (\text{sumset } A B)$   
*<proof>*

**lemma** *not-mem-stabilizer-obtain:*

**assumes**  $A \neq \{\}$  **and**  $x \notin \text{stabilizer } A$  **and**  $x \in G$  **and**  $A \subseteq G$  **and** *finite*  $A$   
**obtains**  $a$  **where**  $a \in A$  **and**  $x \oplus a \notin A$

*<proof>*

**lemma** *sumset-eq-sub-stabilizer:*

**assumes**  $A \subseteq G$  **and**  $B \subseteq G$  **and** *finite*  $B$   
**shows**  $\text{sumset } A B = B \implies A \subseteq \text{stabilizer } B$

*<proof>*

**lemma** *sumset-stabilizer-eq:*

**shows**  $\text{sumset} (\text{stabilizer } A) (\text{stabilizer } A) = \text{stabilizer } A$

*<proof>*

**lemma** *differenceset-stabilizer-eq:*

**shows**  $\text{differenceset} (\text{stabilizer } A) (\text{stabilizer } A) = \text{stabilizer } A$

*<proof>*

**lemma** *stabilizer2-sub-stabilizer:*

**shows**  $\text{stabilizer}(\text{stabilizer } A) \subseteq \text{stabilizer } A$

*<proof>*

**lemma** *stabilizer-left-sumset-invariant:*

**assumes**  $a \in G$  **and**  $A \subseteq G$   
**shows**  $\text{stabilizer} (\text{sumset } \{a\} A) = \text{stabilizer } A$

*<proof>*

**lemma** *stabilizer-right-sumset-invariant:*

**assumes**  $a \in G$  **and**  $A \subseteq G$   
**shows**  $\text{stabilizer} (\text{sumset } A \{a\}) = \text{stabilizer } A$

*<proof>*

**lemma** *stabilizer-right-differenceset-invariant:*

**assumes**  $b \in G$  **and**  $A \subseteq G$   
**shows**  $\text{stabilizer} (\text{differenceset } A \{b\}) = \text{stabilizer } A$

*<proof>*

**lemma** *stabilizer-unchanged:*

**assumes**  $a \in G$  **and**  $b \in G$   
**shows**  $\text{stabilizer} (\text{sumset } A B) = \text{stabilizer} (\text{sumset } A (\text{sumset} (\text{differenceset } B \{b\}) \{a\}))$

*<proof>*

**lemma** *subset-stabilizer-of-subset-sumset:*

**assumes**  $A \subseteq \text{sumset } \{x\}$  (*stabilizer B*) **and**  $x \in G$  **and**  $A \neq \{\}$  **and**  $A \subseteq G$   
**shows**  $\text{stabilizer } A \subseteq \text{stabilizer } B$

*<proof>*

**lemma** *sumset-stabilizer-eq-self:*

**assumes**  $A \subseteq G$

**shows**  $\text{sumset } (\text{stabilizer } A) = A$

*<proof>*

**lemma** *stabilizer-neq-subset-sumset:*

**assumes**  $A \subseteq \text{sumset } \{x\}$  (*stabilizer B*) **and**  $x \in A$  **and**  $\neg \text{sumset } \{x\}$  (*stabilizer B*)  $\subseteq C$  **and**

$A \subseteq C$  **and**  $C \subseteq G$

**shows**  $\text{stabilizer } A \neq \text{stabilizer } B$

*<proof>*

**lemma** *subset-stabilizer-Un:*

**shows**  $\text{stabilizer } A \cap \text{stabilizer } B \subseteq \text{stabilizer } (A \cup B)$

*<proof>*

**lemma** *mem-stabilizer-Un-and-left-imp-right:*

**assumes** *finite B* **and**  $x \in \text{stabilizer } (A \cup B)$  **and**  $x \in \text{stabilizer } A$  **and** *disjnt A B*

**shows**  $x \in \text{stabilizer } B$

*<proof>*

**lemma** *mem-stabilizer-Un-and-right-imp-left:*

**assumes** *finite A* **and**  $x \in \text{stabilizer } (A \cup B)$  **and**  $x \in \text{stabilizer } B$  **and** *disjnt A B*

**shows**  $x \in \text{stabilizer } A$

*<proof>*

**lemma** *Union-stabilizer-Class-eq:*

**assumes**  $A \subseteq G$

**shows**  $A = \bigcup (\text{Class } A \text{ ' } A)$  *<proof>*

**lemma** *card-stabilizer-sumset-divide-sumset:*

$\text{card } (\text{stabilizer } (\text{sumset } A \ B)) \ \text{dvd} \ \text{card } (\text{sumset } A \ B)$  *<proof>*

**lemma** *card-stabilizer-le:*

**assumes**  $A \subseteq G$  **and** *finite A* **and**  $A \neq \{\}$

**shows**  $\text{card } (\text{stabilizer } A) \leq \text{card } A$  *<proof>*

**lemma** *sumset-Inter-subset-sumset:*

**assumes**  $a \in G$  **and**  $b \in G$

**shows**  $\text{sumset } (A \cap \text{sumset } \{a\})$  (*stabilizer C*)  $(B \cap \text{sumset } \{b\})$  (*stabilizer C*)

$\subseteq$   
*sumset*  $\{a \oplus b\}$  (*stabilizer*  $C$ ) (**is** *sumset*  $?A ?B \subseteq -$ )  
 ⟨*proof*⟩

### 1.3 Convergent

**definition** *convergent* :: 'a set  $\Rightarrow$  'a set  $\Rightarrow$  'a set  $\Rightarrow$  bool **where**  
*convergent*  $C A B \equiv C \subseteq \text{sumset } A B \wedge C \neq \{\}$   $\wedge$   
 $\text{card } C + \text{card } (\text{stabilizer } C) \geq \text{card } (A \cap B) + \text{card } (\text{sumset } (A \cup B) (\text{stabilizer } C))$

**definition** *convergent-set* :: 'a set  $\Rightarrow$  'a set  $\Rightarrow$  'a set set **where**  
*convergent-set*  $A B = \text{Collect } (\lambda C. \text{convergent } C A B)$

**lemma** *convergent-set-sub-powerset*:  
*convergent-set*  $A B \subseteq \text{Pow } (\text{sumset } A B)$  ⟨*proof*⟩

**lemma** *finite-convergent-set*:  
**assumes** *finite*  $A$  **and** *finite*  $B$   
**shows** *finite* (*convergent-set*  $A B$ )  
 ⟨*proof*⟩

### 1.4 Technical lemmas from DeVos's proof of Kneser's Theorem

The following lemmas correspond to intermediate arguments in the proof of Kneser's Theorem by DeVos that we will be following [1].

**lemma** *stabilizer-sumset-psubset-stabilizer*:  
**assumes**  $a \in G$  **and**  $b \in G$  **and**  $A \cap \text{sumset } \{a\} (\text{stabilizer } C) \neq \{\}$  **and**  
 $B \cap \text{sumset } \{b\} (\text{stabilizer } C) \neq \{\}$  **and** *hnotsub*:  $\neg \text{sumset } \{a \oplus b\} (\text{stabilizer } C) \subseteq \text{sumset } A B$   
**shows** *stabilizer* (*sumset* ( $A \cap \text{sumset } \{a\} (\text{stabilizer } C)$ ) ( $B \cap \text{sumset } \{b\} (\text{stabilizer } C)$ ))  $\subset$   
*stabilizer*  $C$  (**is**  $?H \subset -$ )  
 ⟨*proof*⟩

**lemma** *stabilizer-eq-stabilizer-union*:  
**assumes**  $a \in G$  **and**  $b \in G$  **and**  $A \cap \text{sumset } \{a\} (\text{stabilizer } C) \neq \{\}$  **and**  
 $B \cap \text{sumset } \{b\} (\text{stabilizer } C) \neq \{\}$  **and** *hnotsub*:  $\neg \text{sumset } \{a \oplus b\} (\text{stabilizer } C) \subseteq \text{sumset } A B$  **and**  
 $C \subseteq \text{sumset } A B$  **and** *finite*  $C$  **and**  
 $C \cap \text{sumset } (A \cap \text{sumset } \{a\} (\text{stabilizer } C)) (B \cap \text{sumset } \{b\} (\text{stabilizer } C)) = \{\}$  **and**  $C \neq \{\}$  **and**  
*finite*  $A$  **and** *finite*  $B$   
**shows** *stabilizer* (*sumset* ( $A \cap \text{sumset } \{a\} (\text{stabilizer } C)$ ) ( $B \cap \text{sumset } \{b\} (\text{stabilizer } C)$ )) =  
*stabilizer* ( $C \cup \text{sumset } (A \cap \text{sumset } \{a\} (\text{stabilizer } C)) (B \cap \text{sumset } \{b\} (\text{stabilizer } C))$ ) (**is** *stabilizer*  $?H = \text{stabilizer } ?K$ )  
 ⟨*proof*⟩

**lemma** *sumset-inter-ineq*:

**assumes**  $B \cap \text{sumset } \{a\} (\text{stabilizer } C) = \{\}$  **and**  $\text{stabilizer } (\text{sumset } (A \cap \text{sumset } \{a\} (\text{stabilizer } C)) (B \cap \text{sumset } \{b\} (\text{stabilizer } C))) \subset \text{stabilizer } C$  **and**  
 $a \in A$  **and**  $a \in G$  **and** *finite*  $A$  **and** *finite*  $B$  **and**  $A \neq \{\}$  **and**  $B \neq \{\}$  **and** *finite*  $(\text{stabilizer } C)$

**shows**  $\text{int } (\text{card } (\text{sumset } (A \cup B) (\text{stabilizer } C))) - \text{card } (\text{sumset } (A \cup B) (\text{stabilizer } (\text{sumset } (A \cap \text{sumset } \{a\} (\text{stabilizer } C)) (B \cap \text{sumset } \{b\} (\text{stabilizer } C)))))) \geq$

$\text{int } (\text{card } (\text{stabilizer } C)) - \text{card } (\text{sumset } (A \cap \text{sumset } \{a\} (\text{stabilizer } C)) (\text{stabilizer } (\text{sumset } (A \cap \text{sumset } \{a\} (\text{stabilizer } C)) (B \cap \text{sumset } \{b\} (\text{stabilizer } C))))))$

(**is**  $\text{int } (\text{card } (\text{sumset } (A \cup B) (\text{stabilizer } C))) - \text{card } (\text{sumset } (A \cup B) ?H1) \geq$   
 $\text{int } (\text{card } (\text{stabilizer } C)) - \text{card } (\text{sumset } ?A1 ?H1)$ )

*<proof>*

**lemma** *exists-convergent-min-stabilizer*:

**assumes** *hind*:  $\forall m < n. \forall C D. C \subseteq G \longrightarrow D \subseteq G \longrightarrow \text{finite } C \longrightarrow \text{finite } D \longrightarrow C \neq \{\} \longrightarrow$

$D \neq \{\} \longrightarrow \text{card } (\text{sumset } C D) + \text{card } C = m \longrightarrow$

$\text{card } (\text{sumset } C (\text{stabilizer } (\text{sumset } C D))) + \text{card } (\text{sumset } D (\text{stabilizer } (\text{sumset } C D))) -$

$\text{card } ((\text{stabilizer } (\text{sumset } C D)))$

$\leq \text{card } (\text{sumset } C D)$  **and** *hAG*:  $A \subseteq G$  **and** *hBG*:  $B \subseteq G$  **and** *hA*: *finite*  $A$

**and**

*hB*: *finite*  $B$  **and** *hAne*:  $A \neq \{\}$  **and**  $A \cap B \neq \{\}$  **and**

*hcardsum*:  $\text{card } (\text{sumset } A B) + \text{card } A = n$  **and** *hintercardA*:  $\text{card } (A \cap B) < \text{card } A$

**obtains**  $X$  **where** *convergent*  $X A B$  **and**  $\bigwedge Y. Y \in \text{convergent-set } A B \implies$

$\text{card } (\text{stabilizer } Y) \geq \text{card } (\text{stabilizer } X)$

*<proof>*

**end**

**context** *normal-subgroup*

**begin**

## 1.5 A function that picks coset representatives randomly

**definition**  $\varphi :: 'a \text{ set} \Rightarrow 'a$  **where**

$\varphi = (\lambda x. \text{if } x \in G // K \text{ then } (\text{SOME } a. a \in G \wedge x = a \cdot | K) \text{ else undefined})$

**definition** *quot-comp-alt* ::  $'a \Rightarrow 'a \Rightarrow 'a$  **where** *quot-comp-alt*  $a b = \varphi ((a \cdot b) \cdot | K)$

**lemma** *phi-eq-coset*:

**assumes**  $\varphi x = a$  **and**  $a \in G$  **and**  $x \in G // K$

**shows**  $x = a \cdot | K$

*<proof>*

**lemma** *phi-coset-mem*:

**assumes**  $a \in G$

**shows**  $\varphi (a \cdot | K) \in a \cdot | K$

*<proof>*

**lemma** *phi-coset-eq*:

**assumes**  $a \in G$  **and**  $\varphi x = a$  **and**  $x \in G // K$

**shows**  $\varphi (a \cdot | K) = a$  *<proof>*

**lemma** *phi-inverse-right*:

**assumes**  $g \in G$

**shows**  $\text{quot-comp-alt } g (\varphi (\text{inverse } g \cdot | K)) = \varphi K$

*<proof>*

**lemma** *phi-inverse-left*:

**assumes**  $g \in G$

**shows**  $\text{quot-comp-alt } (\varphi (\text{inverse } g \cdot | K)) g = \varphi K$

*<proof>*

**lemma** *phi-mem-coset-eq*:

**assumes**  $a \in G // K$  **and**  $b \in G$

**shows**  $\varphi a \in b \cdot | K \implies a = (b \cdot | K)$

*<proof>*

**lemma** *forall-unique-repr*:

$\forall x \in G // K. \exists! k \in \varphi (G // K). x = k \cdot | K$

*<proof>*

**lemma** *phi-inj-on*:

**shows** *inj-on*  $\varphi (G // K)$

*<proof>*

**lemma** *phi-coset-eq-self*:

**assumes**  $a \in G // K$

**shows**  $\varphi a \cdot | K = a$

*<proof>*

**lemma** *phi-coset-comp-eq*:

**assumes**  $a \in G // K$  **and**  $b \in G // K$

**shows**  $\varphi a \cdot \varphi b \cdot | K = a [.] b$  *<proof>*

**lemma** *phi-comp-eq*:

**assumes**  $a \in G // K$  **and**  $b \in G // K$

**shows**  $\varphi (a [.] b) = \text{quot-comp-alt } (\varphi a) (\varphi b)$

*<proof>*

**lemma** *phi-image-subset*:

$\varphi '(G // K) \subseteq G$   
*<proof>*

**lemma** *phi-image-group:*

*Group-Theory.group* ( $\varphi '(G // K)$ ) *quot-comp-alt* ( $\varphi K$ )  
*<proof>*

**lemma** *phi-map: Set-Theory.map*  $\varphi$  *Partition* ( $\varphi ' Partition$ )  
*<proof>*

**lemma** *phi-image-isomorphic:*

*group-isomorphism*  $\varphi (G // K)$  ( $[.]$ ) (*Class 1*) ( $\varphi '(G // K)$ ) *quot-comp-alt* ( $\varphi K$ )  
*<proof>*

**end**

**context** *subgroup-of-additive-abelian-group*

**begin**

**lemma** *Union-Coset-card-eq:*

**assumes** *hSG: S*  $\subseteq G$  **and** *hSU: (* $\bigcup$  *(**Class ' S**)) = S*  
**shows** *card S = card H \* card (**Class ' S**)*  
*<proof>*

**end**

**context** *subgroup-of-abelian-group*

**begin**

**interpretation** *GH: additive-abelian-group*  $G // H$  ( $[.]$ ) *Class 1*  
*<proof>*

**interpretation** *GH-repr: additive-abelian-group*  $\varphi '(G // H)$  *quot-comp-alt*  $\varphi H$   
*<proof>*

**lemma** *phi-image-sumset-eq:*

**assumes**  $A \subseteq G // H$  **and**  $B \subseteq G // H$   
**shows**  $\varphi '(GH.sumset A B) = GH-repr.sumset (\varphi ' A) (\varphi ' B)$   
*<proof>*

**lemma** *phi-image-stabilizer-eq:*

**assumes**  $A \subseteq G // H$   
**shows**  $\varphi '(GH.stabilizer A) = GH-repr.stabilizer (\varphi ' A)$   
*<proof>*

**end**

## 1.6 Useful group-theoretic results

**lemma** *residue-group: abelian-group*  $\{0..(m :: nat)-1\}$   $(\lambda x y. ((x + y) \text{ mod } m))$   
 $(0 :: int)$   
 $\langle \text{proof} \rangle$

**lemma** *(in subgroup-of-group) prime-order-simple:*  
**assumes** *prime*  $(\text{card } G)$   
**shows**  $H = \{1\} \vee H = G$   
 $\langle \text{proof} \rangle$

**lemma** *residue-group-simple:*  
**assumes** *prime*  $p$  **and** *subgroup*  $H$   $\{0..(p :: nat)-1\}$   $(\lambda x y. ((x + y) \text{ mod } p))$   
 $(0 :: int)$   
**shows**  $H = \{0\} \vee H = \{0..int(p-1)\}$   
 $\langle \text{proof} \rangle$

**end**

## 2 Kneser's Theorem and the Cauchy–Davenport Theorem: main proofs

**theory** *Kneser-Cauchy-Davenport-main-proofs*  
**imports**  
*Kneser-Cauchy-Davenport-preliminaries*

**begin**

**context** *additive-abelian-group*

**begin**

### 2.1 Proof of Kneser's Theorem

The proof we formalise follows the paper [1]. This version of Kneser's Theorem corresponds to Theorem 3.2 in [3], or to Theorem 4.3 in [2].

**theorem** *Kneser:*  
**assumes**  $A \subseteq G$  **and**  $B \subseteq G$  **and** *finite*  $A$  **and** *finite*  $B$  **and**  $hAne: A \neq \{\}$  **and**  
 $hBne: B \neq \{\}$   
**shows**  $\text{card } (\text{sumset } A B) \geq \text{card } (\text{sumset } A (\text{stabilizer } (\text{sumset } A B))) +$   
 $\text{card } (\text{sumset } B (\text{stabilizer } (\text{sumset } A B))) - \text{card } (\text{stabilizer } (\text{sumset } A B))$   
 $\langle \text{proof} \rangle$

### 2.2 Strict version of Kneser's Theorem

We show a strict version of Kneser's Theorem as presented in Theorem 3.2 of [3].

**theorem** *Kneser-strict-aux*: **fixes**  $A$  **and**  $B$  **assumes**  $hAG: A \subseteq G$  **and**  $hBG: B \subseteq G$  **and**  $hA$ : *finite*  $A$   
**and**  $hB$ : *finite*  $B$  **and**  $hAne: A \neq \{\}$  **and**  $hBne: B \neq \{\}$  **and**  
 $hineq: \text{card} (\text{sumset } A \ B) > \text{card} (\text{sumset } A \ (\text{stabilizer} (\text{sumset } A \ B))) +$   
 $\text{card} (\text{sumset } B \ (\text{stabilizer} (\text{sumset } A \ B))) - \text{card} (\text{stabilizer} (\text{sumset } A \ B))$   
**shows**  $\text{card} (\text{sumset } A \ B) \geq \text{card } A + \text{card } B$

*<proof>*

**theorem** *Kneser-strict*: **fixes**  $A$  **and**  $B$  **assumes**  $A \subseteq G$  **and**  $B \subseteq G$  **and** *finite*  $A$  **and** *finite*  $B$   
**and**  $\text{stabilizer} (\text{sumset } A \ B) = H$  **and**  $A \neq \{\}$  **and**  $B \neq \{\}$  **and**  $\text{card} (\text{sumset } A \ B) < \text{card } A + \text{card } B$   
**shows**  $\text{card} (\text{sumset } A \ B) = \text{card} (\text{sumset } A \ (\text{stabilizer} (\text{sumset } A \ B))) +$   
 $\text{card} (\text{sumset } B \ (\text{stabilizer} (\text{sumset } A \ B))) - \text{card} (\text{stabilizer} (\text{sumset } A \ B))$   
*<proof>*

### 2.3 The Cauchy–Davenport Theorem

We show the Cauchy–Davenport Theorem as a corollary of Kneser’s Theorem, following a comment on Theorem 3.2 in [3].

**interpretation** *Z-p: additive-abelian-group*  $\{0..int ((p :: nat)-1)\}$   $(\lambda x y. ((x + y) \text{ mod } int p))$   $0::int$   
*<proof>*

**theorem** *Cauchy-Davenport*:  
**fixes**  $p :: nat$   
**assumes** *prime*  $p$  **and**  $A \neq \{\}$  **and**  $B \neq \{\}$  **and** *finite*  $A$  **and** *finite*  $B$  **and**  
 $A \subseteq \{0..p-1\}$  **and**  $B \subseteq \{0..p-1\}$   
**shows**  $\text{card} (Z\text{-}p.\text{sumset } p \ A \ B) \geq \text{Min } \{p, \text{card } A + \text{card } B - 1\}$

*<proof>*

**end**  
**end**

## References

- [1] M. DeVos. A short proof of kneser’s addition theorem for abelian groups. In M. B. Nathanson, editor, *Combinatorial and Additive Number Theory*, pages 39–41, New York, NY, 2014. Springer New York.
- [2] M. B. Nathanson. *Additive Number Theory: Inverse Problems and the Geometry of Sumsets*, volume 165 of *Graduate Texts in Mathematics*. Springer-Verlag, 1996.

- [3] I. Z. Ruzsa. Sunsets and structure, 2008. Course notes, available on <https://www.math.cmu.edu/users/af1p/Teaching/AdditiveCombinatorics/Additive-Combinatorics.pdf>.