

Kneser's Theorem and the Cauchy–Davenport Theorem

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

March 17, 2025

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

1 Preliminaries	3
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
2 Kneser’s Theorem and the Cauchy–Davenport Theorem: main proofs	14
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-Argyraiki 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-Argyraiki 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
Plunnecke-Ruzsa-Inequality.Plunnecke-Ruzsa-Inequality
HOL-Number-Theory.Prime-Powers
```

```
begin
```

```
context subgroup-of-group
```

```
begin
```

```
interpretation left: left-translations-of-group ⟨proof⟩
```

```
interpretation right: right-translations-of-group ⟨proof⟩
```

```
interpretation transformation-group left.translation ` H G ⟨proof⟩
```

```
lemma Right-Coset-eq-iff:
```

```
assumes x ∈ G and y ∈ G
```

```
shows H |· x = (H |· y) ←→ H |· x ∩ (H |· y) ≠ {}  
⟨proof⟩
```

```
end
```

```
context additive-abelian-group
```

```
begin
```

1.1 Elementary lemmas on sumsets

```
lemma sumset-translate-eq-right:
```

```
assumes A ⊆ G and B ⊆ G and x ∈ G
```

```
shows (sumset A {x} = sumset B {x}) ←→ A = B ⟨proof⟩
```

```
lemma sumset-translate-eq-left:
```

```
assumes A ⊆ G and B ⊆ G and x ∈ G
```

```
shows (sumset {x} A = sumset {x} B) ←→ A = B ⟨proof⟩
```

```
lemma differenceset-translate-eq-right:
```

```
assumes A ⊆ G and B ⊆ G and x ∈ G
```

```
shows (differenceset A {x} = differenceset B {x}) ←→ A = B ⟨proof⟩
```

```
lemma differenceset-translate-eq-left:
```

```
assumes A ⊆ G and B ⊆ G and x ∈ G
```

```
shows (differenceset {x} A = differenceset {x} B) ←→ A = B ⟨proof⟩
```

```

lemma sumset-inter-union-subset:
  sumset (A ∩ B) (A ∪ B) ⊆ sumset A B
  ⟨proof⟩

lemma differenceset-group-eq:
  G = differenceset G G
  ⟨proof⟩

lemma card-sumset-singleton-subset-eq:
  assumes a ∈ G and A ⊆ G
  shows card (sumset {a} A) = card A
  ⟨proof⟩

lemma card-differenceset-singleton-mem-eq:
  assumes a ∈ G and A ⊆ G
  shows card A = card (differenceset A {a})
  ⟨proof⟩

lemma card-singleton-differenceset-eq:
  assumes a ∈ G and A ⊆ G
  shows card A = card (differenceset {a} A)
  ⟨proof⟩

lemma sumset-eq-Union-left:
  assumes A ⊆ G
  shows sumset A B = (⋃ a ∈ A. sumset {a} B)
  ⟨proof⟩

lemma sumset-eq-Union-right:
  assumes B ⊆ G
  shows sumset A B = (⋃ b ∈ B. sumset A {b})
  ⟨proof⟩

lemma sumset-singletons-eq:
  assumes a ∈ G and b ∈ G
  shows sumset {a} {b} = {a ⊕ b}
  ⟨proof⟩

lemma sumset-eq-subset-differenceset:
  assumes K ⊆ G and K ≠ {} and A ⊆ G and sumset A K = sumset B K
  shows A ⊆ differenceset (sumset B K) K
  ⟨proof⟩

end

locale subgroup-of-additive-abelian-group =
  subgroup-of-abelian-group H G (⊕) 0 + additive-abelian-group G (⊕) 0
  for H G and addition (infixl ⊕ 65) and zero (0)

```

```

begin

notation Left-Coset (infixl  $\cdot| \cdot$ ) 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  $\text{sumset } \{a\} H = \text{sumset } \{b\} H \longleftrightarrow$ 
     $(\text{sumset } \{a\} H) \cap (\text{sumset } \{b\} H) \neq \{\}$ 
  ⟨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  $S :: \text{'a set}$ 
  shows subgroup (stabilizer  $S$ )  $G$  ( $\oplus$ ) ( $\mathbf{0}$ )
   $\langle proof \rangle$ 

interpretation subgroup-of-additive-abelian-group stabilizer  $A$   $G$  ( $\oplus$ )  $\mathbf{0}$ 
   $\langle proof \rangle$ 

lemma zero-mem-stabilizer:  $\mathbf{0} \in \text{stabilizer } A$   $\langle proof \rangle$ 

lemma stabilizer-is-nonempty:
  shows stabilizer  $S \neq \{\}$ 
   $\langle proof \rangle$ 

lemma Left-Coset-eq-sumset-stabilizer:
  assumes  $x \in G$ 
  shows sumset  $\{x\}$  (stabilizer  $B$ ) =  $x \cdot |$  (stabilizer  $B$ )
   $\langle proof \rangle$ 

lemma stabilizer-subset-difference-singleton:
  assumes  $S \subseteq G$  and  $s \in S$ 
  shows stabilizer  $S \subseteq \text{differenceset } S \{s\}$ 
   $\langle proof \rangle$ 

lemma stabilizer-subset-singleton-difference:
  assumes  $S \subseteq G$  and  $s \in S$ 
  shows stabilizer  $S \subseteq \text{differenceset } \{s\} S$ 
   $\langle proof \rangle$ 

lemma stabilizer-subset-nempty:
  assumes  $S \neq \{\}$  and  $S \subseteq G$ 
  shows stabilizer  $S \subseteq \text{differenceset } S S$ 
   $\langle proof \rangle$ 

lemma stabilizer-coset-subset:
  assumes  $A \subseteq G$  and  $x \in A$ 
  shows sumset  $\{x\}$  (stabilizer  $A$ )  $\subseteq A$ 
   $\langle proof \rangle$ 

lemma stabilizer-subset-stabilizer-dvd:
  assumes stabilizer  $A \subseteq \text{stabilizer } B$ 
  shows card (stabilizer  $A$ ) dvd card (stabilizer  $B$ )
   $\langle proof \rangle$ 

lemma stabilizer-coset-Un:
  assumes  $A \subseteq G$ 
  shows  $(\bigcup_{x \in A} \text{sumset } \{x\} (\text{stabilizer } A)) = A$ 
   $\langle proof \rangle$ 

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 sumset  $\{a\}$  (stabilizer  $A$ ) = sumset  $\{b\}$  (stabilizer  $A$ )  $\longleftrightarrow$ 
    (sumset  $\{a\}$  (stabilizer  $A$ ))  $\cap$  (sumset  $\{b\}$  (stabilizer  $A$ ))  $\neq \{\}$ 
  ⟨proof⟩

lemma sumset-stabilizer-eq-Class-Union:
  assumes  $A \subseteq G$ 
  shows sumset  $A$  (stabilizer  $B$ ) = ( $\bigcup$  (Class  $B$  ‘  $A$ ))
  ⟨proof⟩

lemma card-stabilizer-divide-sumset:
  assumes  $A \subseteq G$ 
  shows card (stabilizer  $B$ ) dvd card (sumset  $A$  (stabilizer  $B$ ))
  ⟨proof⟩

lemma Class-image-sumset-stabilizer-eq:
  assumes  $A \subseteq G$ 
  shows Class  $B$  ‘ (sumset  $A$  (stabilizer  $B$ )) = Class  $B$  ‘  $A$ 
  ⟨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 Class  $B$   $x \subseteq A \vee$  Class  $B$   $x \cap A = \{\}$ 
  ⟨proof⟩

lemma stabilizer-sumset-disjoint:
  fixes  $S1 S2 :: \text{'a set}$ 
  assumes stabilizer  $S1 \cap$  stabilizer  $S2 = \{\mathbf{0}\}$  and  $S1 \subseteq G$  and  $S2 \subseteq G$ 
    and finite  $S1$  and finite  $S2$  and  $S1 \neq \{\}$  and  $S2 \neq \{\}$ 
  shows card (sumset (stabilizer  $S1$ ) (stabilizer  $S2$ )) =
    card (stabilizer  $S1$ ) * card (stabilizer  $S2$ )
  ⟨proof⟩

lemma stabilizer-sub-sumset-left:
  stabilizer  $A \subseteq$  stabilizer (sumset  $A$   $B$ )
  ⟨proof⟩

lemma stabilizer-sub-sumset-right:

```

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

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** $x \oplus a \notin A$
 $\langle \text{proof} \rangle$

lemma *sumset-eq-sub-stabilizer*:

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

lemma *sumset-stabilizer-eq*:

shows $\text{sumset}(\text{stabilizer } A) (\text{stabilizer } A) = \text{stabilizer } A$
 $\langle \text{proof} \rangle$

lemma *differenceset-stabilizer-eq*:

shows $\text{differenceset}(\text{stabilizer } A) (\text{stabilizer } A) = \text{stabilizer } A$
 $\langle \text{proof} \rangle$

lemma *stabilizer2-sub-stabilizer*:

shows $\text{stabilizer}(\text{stabilizer } A) \subseteq \text{stabilizer } A$
 $\langle \text{proof} \rangle$

lemma *stabilizer-left-sumset-invariant*:

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

$\langle \text{proof} \rangle$

lemma *stabilizer-right-sumset-invariant*:

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

lemma *stabilizer-right-differenceset-invariant*:

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

lemma *stabilizer-unchanged*:

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

$\langle \text{proof} \rangle$

lemma *subset-stabilizer-of-subset-sumset*:
assumes $A \subseteq \text{sumset } \{x\} (\text{stabilizer } B)$ **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 $\text{sumset} (\text{stabilizer } A) A = A$
(proof)

lemma *stabilizer-neq-subset-sumset*:
assumes $A \subseteq \text{sumset } \{x\} (\text{stabilizer } B)$ **and** $x \in A$ **and** $\neg \text{sumset } \{x\} (\text{stabilizer } B) \subseteq C$ **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 $A = (\bigcup (\text{Class } A \cdot A))$ *(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 $\text{sumset} (A \cap \text{sumset } \{a\} (\text{stabilizer } C)) (B \cap \text{sumset } \{b\} (\text{stabilizer } C))$

\subseteq
 $\text{sumset } \{a \oplus b\} (\text{stabilizer } C) (\text{is sumset } ?A ?B \subseteq -)$
 $\langle \text{proof} \rangle$

1.3 Convergent

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

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

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

lemma finite-convergent-set:
assumes finite A **and** finite B
shows finite ($\text{convergent-set } A B$)
 $\langle \text{proof} \rangle$

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 ($\text{sumset } (A \cap \text{sumset } \{a\} (\text{stabilizer } C)) (B \cap \text{sumset } \{b\} (\text{stabilizer } C))$) \subset
 $\text{stabilizer } C$ (**is** $?H \subset -$)
 $\langle \text{proof} \rangle$

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 ($\text{sumset } (A \cap \text{sumset } \{a\} (\text{stabilizer } C)) (B \cap \text{sumset } \{b\} (\text{stabilizer } C))$) =
 $\text{stabilizer } (C \cup \text{sumset } (A \cap \text{sumset } \{a\} (\text{stabilizer } C)) (B \cap \text{sumset } \{b\} (\text{stabilizer } C)))$ (**is** stabilizer $?H = \text{stabilizer } ?K$)
 $\langle \text{proof} \rangle$

```

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  $\text{finite } A$  and  $\text{finite } B$  and  $A \neq \{\}$  and  $B \neq \{\}$  and  $\text{finite } (\text{stabilizer } C)$ 
  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:  $\forall m < n. \forall C D. C \subseteq G \rightarrow D \subseteq G \rightarrow \text{finite } C \rightarrow \text{finite } D \rightarrow$ 
     $C \neq \{\} \rightarrow$ 
     $D \neq \{\} \rightarrow \text{card } (\text{sumset } C D) + \text{card } C = m \rightarrow$ 
     $\text{card } (\text{sumset } C (\text{stabilizer } (\text{sumset } C D))) + \text{card } (\text{sumset } D (\text{stabilizer } (\text{sumset } C D))) -$ 
     $\text{card } ((\text{stabilizer } (\text{sumset } C D)))$ 
     $\leq \text{card } (\text{sumset } C D)$  and hAG:  $A \subseteq G$  and hBG:  $B \subseteq G$  and hA:  $\text{finite } A$ 
    and
    hB:  $\text{finite } B$  and hAn:  $A \neq \{\} \text{ and } A \cap B \neq \{\}$  and
    heardsum:  $\text{card } (\text{sumset } A B) + \text{card } A = n$  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  $\varphi :: 'a \text{ set} \Rightarrow 'a \text{ where}$ 
 $\varphi = (\lambda x. \text{if } x \in G // K \text{ then } (\text{SOME } a. a \in G \wedge x = a \cdot| K) \text{ else undefined})$ 

```

```

definition quot-comp-alt ::  $'a \Rightarrow 'a \Rightarrow 'a \text{ where}$  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  $\varphi(a \cdot| K) \in a \cdot| K$ 
   $\langle proof \rangle$ 

lemma phi-coset-eq:
  assumes  $a \in G$  and  $\varphi x = a$  and  $x \in G // K$ 
  shows  $\varphi(a \cdot| K) = a$   $\langle proof \rangle$ 

lemma phi-inverse-right:
  assumes  $g \in G$ 
  shows quot-comp-alt  $g (\varphi(\text{inverse } g \cdot| K)) = \varphi K$ 
   $\langle proof \rangle$ 

lemma phi-inverse-left:
  assumes  $g \in G$ 
  shows quot-comp-alt  $(\varphi(\text{inverse } g \cdot| K)) g = \varphi K$ 
   $\langle proof \rangle$ 

lemma phi-mem-coset-eq:
  assumes  $a \in G // K$  and  $b \in G$ 
  shows  $\varphi a \in b \cdot| K \implies a = (b \cdot| K)$ 
   $\langle proof \rangle$ 

lemma forall-unique-repr:
   $\forall x \in G // K. \exists! k \in \varphi ` (G // K). x = k \cdot| K$ 
   $\langle proof \rangle$ 

lemma phi-inj-on:
  shows inj-on  $\varphi(G // K)$ 
   $\langle proof \rangle$ 

lemma phi-coset-eq-self:
  assumes  $a \in G // K$ 
  shows  $\varphi a \cdot| K = a$ 
   $\langle proof \rangle$ 

lemma phi-coset-comp-eq:
  assumes  $a \in G // K$  and  $b \in G // K$ 
  shows  $\varphi a \cdot \varphi b \cdot| K = a [\cdot] b$   $\langle proof \rangle$ 

lemma phi-comp-eq:
  assumes  $a \in G // K$  and  $b \in G // K$ 
  shows  $\varphi(a [\cdot] b) = \text{quot-comp-alt } (\varphi a) (\varphi b)$ 
   $\langle proof \rangle$ 

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  $\varphi (G // K) ([\cdot])$  (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:  $(\bigcup (\text{Class } ` S)) = S$ 
  shows card  $S = \text{card } H * \text{card } (\text{Class } ` S)$ 
⟨proof⟩

end

context subgroup-of-abelian-group
begin

interpretation GH: additive-abelian-group  $G // H ([\cdot])$  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 ⊆  $G // H$  and B ⊆  $G // H$ 
  shows  $\varphi` (GH.\text{sumset } A B) = GH.\text{repr.sumset} (\varphi` A) (\varphi` B)$ 
⟨proof⟩

lemma phi-image-stabilizer-eq:
  assumes A ⊆  $G // H$ 
  shows  $\varphi` (GH.\text{stabilizer } A) = GH.\text{repr.stabilizer} (\varphi` A)$ 
⟨proof⟩

end

```

1.6 Useful group-theoretic results

```

lemma residue-group: abelian-group {0..(m :: nat)-1} ( $\lambda x y. ((x + y) \bmod m)$ )
(0 :: int)
⟨proof⟩

lemma (in subgroup-of-group) prime-order-simple:
  assumes prime (card G)
  shows H = {1} ∨ H = G
⟨proof⟩

lemma residue-group-simple:
  assumes prime p and subgroup H {0..(p :: nat)-1} ( $\lambda x y. ((x + y) \bmod p)$ )
(0 :: int)
  shows H = {0} ∨ H = {0..int(p-1)}
⟨proof⟩

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 ⊆ G and B ⊆ G and finite A and finite B and hAne: A ≠ {} and
  hBne: B ≠ {}
  shows card (sumset A B) ≥ card (sumset A (stabilizer (sumset A B))) +
    card (sumset B (stabilizer (sumset A B))) - card (stabilizer (sumset A B))
⟨proof⟩

```

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** $hA: \text{finite } A$
and $hB: \text{finite } B$ **and** $hAne: A \neq \{\}$ **and** $hBne: B \neq \{\}$ **and**
 $\text{hineq: } \text{card}(\text{sumset } A B) > \text{card}(\text{sumset } A (\text{stabilizer}(\text{sumset } A B))) +$
 $\text{card}(\text{sumset } B (\text{stabilizer}(\text{sumset } A B))) - \text{card}(\text{stabilizer}(\text{sumset } A B))$
shows $\text{card}(\text{sumset } A B) \geq \text{card } A + \text{card } B$

$\langle\text{proof}\rangle$

theorem Kneser-strict: **fixes** A **and** B **assumes** $A \subseteq G$ **and** $B \subseteq G$ **and** $\text{finite } A$ **and** $\text{finite } B$
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 $\text{card}(\text{sumset } A B) = \text{card}(\text{sumset } A (\text{stabilizer}(\text{sumset } A B))) +$
 $\text{card}(\text{sumset } B (\text{stabilizer}(\text{sumset } A B))) - \text{card}(\text{stabilizer}(\text{sumset } A B))$
 $\langle\text{proof}\rangle$

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 $\{0.. \text{int}((p :: \text{nat}) - 1)\}$ $(\lambda x y. ((x + y) \bmod \text{int } p)) 0::\text{int}$
 $\langle\text{proof}\rangle$

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

$\langle\text{proof}\rangle$

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. Sumsets and structure, 2008. Course notes, available on <https://www.math.cmu.edu/users/af1p/Teaching/AdditiveCombinatorics/Additive-Combinatorics.pdf>.