Kneser's Theorem and the Cauchy–Davenport Theorem

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

December 1, 2022

Abstract

We formalise Kneser's Theorem in combinatorics [2, 3] following the proof from the 2014 paper "A short proof of Knesers 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

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
Pluennecke-Ruzsa-Inequality.Pluennecke-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 $x \in G$ **and** $y \in G$
shows $H \mid\cdot x = (H \mid\cdot y) \longleftrightarrow H \mid\cdot x \cap (H \mid\cdot y) \neq \{\}$
⟨*proof*⟩

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 (*sumset A* $\{x\}$ = *sumset B* $\{x\}$) $\longleftrightarrow$ $A = B$ ⟨*proof*⟩

lemma *sumset-translate-eq-left*:
assumes $A \subseteq G$ **and** $B \subseteq G$ **and** $x \in G$
shows (*sumset* $\{x\}$ *A* = *sumset* $\{x\}$ *B*) $\longleftrightarrow$ $A = B$ ⟨*proof*⟩

lemma *differenceset-translate-eq-right*:
assumes $A \subseteq G$ **and** $B \subseteq G$ **and** $x \in G$
shows (*differenceset A* $\{x\}$ = *differenceset B* $\{x\}$) $\longleftrightarrow$ $A = B$ ⟨*proof*⟩

lemma *differenceset-translate-eq-left*:
assumes $A \subseteq G$ **and** $B \subseteq G$ **and** $x \in G$
shows (*differenceset* $\{x\}$ *A* = *differenceset* $\{x\}$ *B*) $\longleftrightarrow$ $A = B$ ⟨*proof*⟩

lemma *sumset-inter-union-subset*:
sumset $(A \cap B)$ $(A \cup B) \subseteq$ *sumset* A B
⟨*proof*⟩

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

lemma *card-sumset-singleton-subset-eq*:
assumes $a \in G$ **and** $A \subseteq G$
shows *card* (*sumset* $\{a\}$ A) = *card* A
⟨*proof*⟩

lemma *card-differenceset-singleton-mem-eq*:
assumes $a \in G$ **and** $A \subseteq G$
shows *card* A = *card* (*differenceset* A $\{a\}$)
⟨*proof*⟩

lemma *card-singleton-differenceset-eq*:
assumes $a \in G$ **and** $A \subseteq G$
shows *card* A = *card* (*differenceset* $\{a\}$ A)
⟨*proof*⟩

lemma *sumset-eq-Union-left*:
assumes $A \subseteq G$
shows *sumset* A $B = (\bigcup\ a \in A.$ *sumset* $\{a\}$ $B)$
⟨*proof*⟩

lemma *sumset-eq-Union-right*:
assumes $B \subseteq G$
shows *sumset* A $B = (\bigcup\ b \in B.$ *sumset* A $\{b\})$
⟨*proof*⟩

lemma *sumset-singletons-eq*:
assumes $a \in G$ **and** $b \in G$
shows *sumset* $\{a\}$ $\{b\} = \{a \oplus b\}$
⟨*proof*⟩

lemma *sumset-eq-subset-differenceset*:
assumes $K \subseteq G$ **and** $K \neq \{\}$ **and** $A \subseteq G$ **and** *sumset* A K = *sumset* B K
shows $A \subseteq$ *differenceset* (*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** $\oplus$ *65*) **and** *zero* ($\mathbf{0}$)

begin

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

lemma *Left-Coset-eq-sumset*:
assumes $x \in G$
shows *sumset* $\{x\}$ $H = x \cdot| H$
⟨*proof*⟩

lemma *sumset-subgroup-eq-iff*:
assumes $a \in G$ **and** $b \in G$
shows *sumset* $\{a\}$ $H =$ *sumset* $\{b\}$ $H \longleftrightarrow$
(*sumset* $\{a\}$ H) $\cap$ (*sumset* $\{b\}$ H) $\neq \{\}$
⟨*proof*⟩

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

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

lemma *Class-image-sumset-subgroup-eq*:
assumes $A \subseteq G$
shows *Class* ‘ (*sumset A H*) = *Class* ‘ *A*
⟨*proof*⟩

lemma *Class-cover-imp-subset-or-disj*:
assumes $A = (\bigcup$ (*Class* ‘ *C*)) **and** $x \in G$ **and** $C \subseteq G$
shows *Class x* $\subseteq A \vee$ *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* ⇒ *'a set* **where**
stabilizer S ≡ {$x \in G$. *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** ∈ *stabilizer A* ⟨*proof*⟩

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

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

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

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

lemma *stabilizer-subset-nempty*:
assumes *S* ≠ {} **and** *S* ⊆ *G*
shows *stabilizer S* ⊆ *differenceset S S*
⟨*proof*⟩

lemma *stabilizer-coset-subset*:
assumes *A* ⊆ *G* **and** *x* ∈ *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* ⊆ *G*
shows (⋃ *x* ∈ *A*. *sumset* {*x*} (*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 *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* = ($\bigcup$ (*Class B* ‘ *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* :: *'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 $B \subseteq$ *stabilizer* (*sumset* A B)
⟨*proof*⟩

lemma *not-mem-stabilizer-obtain*:
assumes $A \neq \{\}$ **and** $x \notin$ *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 *sumset* A $B = B \Longrightarrow A \subseteq$ *stabilizer* B
⟨*proof*⟩

lemma *sumset-stabilizer-eq*:
shows *sumset* (*stabilizer* A) (*stabilizer* A) = *stabilizer* A
⟨*proof*⟩

lemma *differenceset-stabilizer-eq*:
shows *differenceset* (*stabilizer* A) (*stabilizer* A) = *stabilizer* A
⟨*proof*⟩

lemma *stabilizer2-sub-stabilizer*:
shows *stabilizer*(*stabilizer* A) $\subseteq$ *stabilizer* A
⟨*proof*⟩

lemma *stabilizer-left-sumset-invariant*:
assumes $a \in G$ **and** $A \subseteq G$
shows *stabilizer* (*sumset* $\{a\}$ A) = *stabilizer* A

⟨*proof*⟩

lemma *stabilizer-right-sumset-invariant*:
assumes $a \in G$ **and** $A \subseteq G$
shows *stabilizer* (*sumset* A $\{a\}$) = *stabilizer* A
⟨*proof*⟩

lemma *stabilizer-right-differenceset-invariant*:
assumes $b \in G$ **and** $A \subseteq G$
shows *stabilizer* (*differenceset* A $\{b\}$) = *stabilizer* A
⟨*proof*⟩

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

⟨*proof*⟩

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

lemma *sumset-stabilizer-eq-self*:
assumes $A \subseteq G$
shows *sumset* (*stabilizer* A) $A = A$
⟨*proof*⟩

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

lemma *subset-stabilizer-Un*:
shows *stabilizer* $A \cap$ *stabilizer* $B \subseteq$ *stabilizer* $(A \cup B)$
⟨*proof*⟩

lemma *mem-stabilizer-Un-and-left-imp-right*:
assumes *finite* B **and** $x \in$ *stabilizer* $(A \cup B)$ **and** $x \in$ *stabilizer* A **and** *disjnt* A B
shows $x \in$ *stabilizer* B
⟨*proof*⟩

lemma *mem-stabilizer-Un-and-right-imp-left*:
assumes *finite* A **and** $x \in$ *stabilizer* $(A \cup B)$ **and** $x \in$ *stabilizer* B **and** *disjnt* A B
shows $x \in$ *stabilizer* A
⟨*proof*⟩

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

lemma *card-stabilizer-sumset-divide-sumset*:
card (*stabilizer* (*sumset* A B)) *dvd card* (*sumset* A B) ⟨*proof*⟩

lemma *card-stabilizer-le*:
assumes $A \subseteq G$ **and** *finite* A **and** $A \neq \{\}$
shows *card* (*stabilizer* A) $\leq$ *card* A ⟨*proof*⟩

lemma *sumset-Inter-subset-sumset*:
assumes $a \in G$ **and** $b \in G$
shows *sumset* $(A \cap$ *sumset* $\{a\}$ (*stabilizer* C)) $(B \cap$ *sumset* $\{b\}$ (*stabilizer* C))

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

1.3 Convergent

definition *convergent* :: *'a set* ⇒ *'a set* ⇒ *'a set* ⇒ *bool* **where**
convergent C A B ≡ *C* $\subseteq$ *sumset A B* ∧ *C* ≠ {} ∧
 card C + *card* (*stabilizer C*) ≥ *card* (*A* ∩ *B*) + *card* (*sumset* (*A* ∪ *B*) (*stabilizer C*))

definition *convergent-set* :: *'a set* ⇒ *'a set* ⇒ *'a set set* **where**
convergent-set A B = *Collect* (λ *C*. *convergent C A B*)

lemma *convergent-set-sub-powerset*:
 convergent-set A B $\subseteq$ *Pow* (*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* ∈ *G* **and** *b* ∈ *G* **and** *A* ∩ *sumset* {*a*} (*stabilizer C*) ≠ {} **and**
 B ∩ *sumset* {*b*} (*stabilizer C*) ≠ {} **and** *hnotsub*: ¬ *sumset* {*a* ⊕ *b*} (*stabilizer C*) $\subseteq$ *sumset A B*
  shows *stabilizer* (*sumset* (*A* ∩ *sumset* {*a*} (*stabilizer C*)) (*B* ∩ *sumset* {*b*} (*stabilizer C*))) ⊂
   stabilizer C (**is** *?H* ⊂ -)
⟨*proof*⟩

lemma *stabilizer-eq-stabilizer-union*:
 assumes *a* ∈ *G* **and** *b* ∈ *G* **and***A* ∩ *sumset* {*a*} (*stabilizer C*) ≠ {} **and**
 B ∩ *sumset* {*b*} (*stabilizer C*) ≠ {} **and** *hnotsub*: ¬ *sumset* {*a* ⊕ *b*} (*stabilizer C*) $\subseteq$ *sumset A B* **and**
 C $\subseteq$ *sumset A B* **and** *finite C* **and**
 C ∩ *sumset* (*A* ∩ *sumset* {*a*} (*stabilizer C*)) (*B* ∩ *sumset* {*b*} (*stabilizer C*)) = {} **and** *C* ≠ {} **and**
 finite A **and** *finite B*
  shows *stabilizer* (*sumset* (*A* ∩ *sumset* {*a*} (*stabilizer C*)) (*B* ∩ *sumset* {*b*} (*stabilizer C*))) =
    stabilizer (*C* ∪ *sumset* (*A* ∩ *sumset* {*a*} (*stabilizer C*)) (*B* ∩ *sumset* {*b*} (*stabilizer C*))) (**is** *stabilizer ?H* = *stabilizer ?K*)
⟨*proof*⟩

lemma *sumset-inter-ineq*:
assumes $B \cap$ *sumset* $\{a\}$ (*stabilizer* C) $= \{\}$ **and** *stabilizer* (*sumset* ($A \cap$ *sumset* $\{a\}$ (*stabilizer* C)) ($B \cap$ *sumset* $\{b\}$ (*stabilizer* C))) $\subset$ *stabilizer* C **and**
$a \in A$ **and** $a \in G$ **and** *finite* A **and** *finite* B **and** $A \neq \{\}$ **and** $B \neq \{\}$ **and** *finite* (*stabilizer* C)
shows *int* (*card* (*sumset* ($A \cup B$) (*stabilizer* C))) $-$ *card* (*sumset* ($A \cup B$) (*stabilizer* (*sumset* ($A \cap$ *sumset* $\{a\}$ (*stabilizer* C)) ($B \cap$ *sumset* $\{b\}$ (*stabilizer* C))))) $\geq$
int (*card* (*stabilizer* C)) $-$ *card* (*sumset* ($A \cap$ *sumset* $\{a\}$ (*stabilizer* C)) (*stabilizer* (*sumset* ($A \cap$ *sumset* $\{a\}$ (*stabilizer* C)) ($B \cap$ *sumset* $\{b\}$ (*stabilizer* C)))))
(**is** *int* (*card* (*sumset* ($A \cup B$) (*stabilizer* C))) $-$ *card* (*sumset* ($A \cup B$) *?H1*) $\geq$
int (*card* (*stabilizer* C)) $-$ *card* (*sumset ?A1 ?H1*))
⟨*proof*⟩

lemma *exists-convergent-min-stabilizer*:
assumes *hind*: $\forall\, m{<}n.\ \forall\, C\ D.\ C \subseteq G \longrightarrow D \subseteq G \longrightarrow$ *finite* $C \longrightarrow$ *finite* $D \longrightarrow C \neq \{\} \longrightarrow$
$D \neq \{\} \longrightarrow$ *card* (*sumset* C D) $+$ *card* $C = m \longrightarrow$
card (*sumset* C (*stabilizer* (*sumset* C D))) $+$ *card* (*sumset* D (*stabilizer* (*sumset* C D))) $-$
card ((*stabilizer* (*sumset* C D)))
$\leq$ *card* (*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: *card* (*sumset* A B) $+$ *card* $A = n$ **and** *hintercardA*: *card* ($A \cap B$) $<$ *card* A
obtains X **where** *convergent* X A B **and** $\bigwedge Y.\ Y \in$ *convergent-set* A $B \Longrightarrow$
card (*stabilizer* Y) $\geq$ *card* (*stabilizer* X)
⟨*proof*⟩

end

context *normal-subgroup*
begin

1.5 A function that picks coset representatives randomly

definition φ :: *'a set* $\Rightarrow$ *'a* **where**
$\varphi = (\lambda\, x.$ *if* $x \in G$ // K *then* (*SOME a.* $a \in G \wedge x = a \cdot|\ K$) *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 *quot-comp-alt* $g\ (\varphi\ (\mathit{inverse}\ g \cdot|\ K)) = \varphi\ K$
⟨*proof*⟩

lemma *phi-inverse-left*:
assumes $g \in G$
shows *quot-comp-alt* $(\varphi\ (\mathit{inverse}\ g \cdot|\ K))\ g = \varphi\ K$
⟨*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 $\varphi\ a \cdot \varphi\ b \cdot|\ K = a\ [\cdot]\ b$ ⟨*proof*⟩

lemma *phi-comp-eq*:
assumes $a \in G\ //\ K$ **and** $b \in G\ //\ K$
shows $\varphi\ (a\ [\cdot]\ b) =$ *quot-comp-alt* $(\varphi\ a)\ (\varphi\ b)$
⟨*proof*⟩

lemma *phi-image-subset*:

φ ` $(G$ // $K) \subseteq G$
⟨*proof*⟩

lemma *phi-image-group*:
Group-Theory.group $(\varphi$ ` $(G$ // $K))$ *quot-comp-alt* $(\varphi$ $K)$
⟨*proof*⟩

lemma *phi-map*: *Set-Theory.map* φ *Partition* $(\varphi$ ` *Partition*)
⟨*proof*⟩

lemma *phi-image-isomorphic*:
group-isomorphism φ $(G$ // $K)$ $([\cdot])$ $(Class$ **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*: $(\bigcup$ $(Class$ ` $S)) = S$
shows *card* S = *card* H $*$ *card* $(Class$ ` $S)$
⟨*proof*⟩

end

context *subgroup-of-abelian-group*
begin

interpretation *GH*: *additive-abelian-group* G // H $([\cdot])$ *Class* **1**
⟨*proof*⟩

interpretation *GH-repr*: *additive-abelian-group* φ ` $(G$ // $H)$ *quot-comp-alt* φ H
⟨*proof*⟩

lemma *phi-image-sumset-eq*:
assumes $A \subseteq G$ // H **and** $B \subseteq G$ // H
shows φ ` $(GH.sumset$ $A$ $B) = GH\text{-}repr.sumset$ $(\varphi$ ` $A)$ $(\varphi$ ` $B)$
⟨*proof*⟩

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

end

1.6 Useful group-theoretic results

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

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

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

end

2 Kneser's Theorem and the CauchyDavenport 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 *card* (*sumset A B*) $\geq$ *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*: *finite A*
and *hB*: *finite B* **and** *hAne*: $A \neq \{\}$ **and** *hBne*: $B \neq \{\}$ **and**
hineq: *card* (*sumset A B*) > *card* (*sumset A* (*stabilizer* (*sumset A B*))) +
card (*sumset B* (*stabilizer* (*sumset A B*))) − *card* (*stabilizer* (*sumset A B*))
shows *card* (*sumset A B*) ≥ *card A* + *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 *stabilizer* (*sumset A B*) = H **and** $A \neq \{\}$ **and** $B \neq \{\}$ **and** *card* (*sumset A B*) < *card A* + *card 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*⟩

2.3 The CauchyDavenport Theorem

We show the CauchyDavenport 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*)} (λ *x y*. ((*x* + *y*) *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 *card* (*Z-p.sumset p A B*) ≥ *Min* {*p*, *card A* + *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. Sumsets and structure, 2008. Course notes, available on https://www.math.cmu.edu/users/af1p/Teaching/AdditiveCombinatorics/Additive-Combinatorics.pdf.