Involutions2Squares

Maksym Bortin

February 6, 2026

Abstract

This theory contains the involution-based proof of the 'two squares' theorem from THE BOOK.

Contents

theory *Involutions2Squares*
imports *Main*
begin

1 A few basic properties

lemma *nat-sqr* :
shows $nat(n^2) = (nat(abs\ n))^2$
⟨*proof*⟩

lemma *nat-mod-int* :
assumes $n\ mod\ m = k$
shows $int\ n\ mod\ int\ m = int\ k$
⟨*proof*⟩

lemma *sqr-geq-nat* :
shows $(n::nat) \leq n^2$
⟨*proof*⟩

lemma *sqr-geq-abs* :
  shows $abs(n::int) \leq n^2$
⟨*proof*⟩

lemma *sqr-fix-nat* :
  assumes $(n::nat) = n^2$
  shows $n = 0 \lor n = 1$
  ⟨*proof*⟩

lemma *card1* :
  shows $(card\{a, b\} = Suc\ 0) = (a = b)$
  ⟨*proof*⟩

lemma *card2* :
  shows $card\{a, b\} \geq Suc\ 0 \land card\{a, b\} \leq 2$
  ⟨*proof*⟩

2 The relevant properties of involutions

definition *involution-on* $A\ \varphi = (\varphi\ \text{`}\ A \subseteq A \land (\forall x \in A.\ \varphi(\varphi\ x) = x))$

lemma *involution-bij* :
  assumes *involution-on* $A\ \varphi$
  shows *bij-betw* $\varphi\ A\ A$
  ⟨*proof*⟩

lemma *involution-sub-bij* :
  assumes *involution-on* $A\ \varphi$
    and $S \subseteq A$
    and $\forall x \in A.\ (x \in S) = (\varphi\ x \notin S)$
  shows *bij-betw* $\varphi\ S\ (A - S)$
⟨*proof*⟩

lemma *involution-sub-card* :
  assumes *involution-on* $A\ \varphi$
    and *finite* A
    and $S \subseteq A$
    and $\forall x \in A.\ (x \in S) = (\varphi\ x \notin S)$
  shows $2 * card\ S = card\ A$
⟨*proof*⟩

2.1 Unions of preimage/image sets, fixed points

definition *preimg-img-on* $A\ \varphi = (\bigcup x{\in}A.\ \{\{x,\ \varphi\ x\}\})$
definition *fixpoints-on* $A\ \varphi = \{x{\in}A.\ \varphi\ x = x\}$

lemma *preimg-img-on-Union* :
assumes φ ‘ $A \subseteq A$
shows $A = \bigcup(\textit{preimg-img-on}\ A\ \varphi)$
⟨*proof*⟩

lemma *preimg-img-on-finite* :
assumes *finite A*
shows *finite* (*preimg-img-on A* φ)
⟨*proof*⟩

lemma *fixpoints-on-finite* :
assumes *finite A*
shows *finite* (*fixpoints-on A* φ)
⟨*proof*⟩

lemma *preimg-img-on-card* :
assumes $x \in$ *preimg-img-on A* φ
shows $1 \leq \textit{card}\ x \wedge \textit{card}\ x \leq 2$
⟨*proof*⟩

corollary *preimg-img-on-eq* :
shows *preimg-img-on A* $\varphi = \{x \in \textit{preimg-img-on}\ A\ \varphi.\ \textit{card}\ x = 1\} \cup$
$\{x \in \textit{preimg-img-on}\ A\ \varphi.\ \textit{card}\ x = 2\}$
⟨*proof*⟩

lemma *fixpoints-on-card-eq* :
shows *card*(*fixpoints-on A* φ) = *card* $\{x \in \textit{preimg-img-on}\ A\ \varphi.\ \textit{card}\ x = 1\}$
⟨*proof*⟩

lemma *preimg-img-on-disjoint* :
assumes *involution-on A* φ
shows *pairwise disjnt* (*preimg-img-on A* φ)
⟨*proof*⟩

theorem *involution-dom-card-sum* :
assumes *involution-on A* φ
and *finite A*
shows *card A* = *card* (*fixpoints-on A* φ) +

$2 * card \{x \in preimg\text{-}img\text{-}on\ A\ \varphi.\ card\ x = 2\}$
⟨*proof*⟩

corollary *involution-dom-fixpoints-parity* :
assumes *involution-on A* φ
and *finite A*
shows $odd(card\ A) = odd(card(fixpoints\text{-}on\ A\ \varphi))$
⟨*proof*⟩

3 Primes and the two squares theorem

definition *is-prime* $(n :: nat) = (n > 1 \wedge (\forall d.\ d\ dvd\ n \longrightarrow d = 1 \vee d = n))$

lemma *prime-factors* :
assumes *is-prime p*
and $p = n * m$
shows $(n = 1 \wedge m = p) \vee (n = p \wedge m = 1)$
⟨*proof*⟩

lemma *prime-not-sqr* :
assumes *is-prime p*
shows $p \neq n^2$
⟨*proof*⟩

lemma *int-prime-not-sqr* :
assumes *is-prime p*
shows $int\ p \neq n^2$
⟨*proof*⟩

lemma *prime-gr4* :
assumes *is-prime p*
and $p\ mod\ 4 = 1$
shows $p > 4$
⟨*proof*⟩

theorem *two-squares* :
assumes *a*: *is-prime p*
and *b*: $p\ mod\ 4 = 1$
shows $\exists n\ m.\ p = n^2 + m^2$
⟨*proof*⟩

end