Euclids Theorem

Tim Lichtnau

2021

Abstract

We present a formalization of Euclid's Theorem from an algebraic and order-theoretic approach. The `PDF`-document contains some feature which allow us to unhide suppressed information visible via a mouseover event. At this time, this extra works not for all `PDF`-viewers, but surely for `Adobe Reader` or `Foxit Reader`.

Contents

1 Sets and classes

[synonym subset/-s]
Let X denote a set.

Definition. A subset of X is a set Y such that every element of Y is an element of X.

Axiom 1. Let Y be a class. Assume every element of Y is an element of

X. Then Y is a set.

Axiom 2. Every element of every set is setsized.

2 Order relations

Let $Y \subseteq X$ stand for Y is a subset of X.

Definition. X is nonempty iff there exists an element of X.

Signature 3. An order is a notion.

Let O denote a order.

Signature 4. $|O|$ is a set.

Let O stand for $|O|$.

Signature 5. Let $x, y \in O$. xOy is an atom.

Let $x \leq y$ stand for xOy.

Definition. An order on X is a order O such that $|O| = X$.

Definition. Let $N \subseteq O$. O restricted to N is an order T on N such that (xTy iff xOy) for all $x, y \in N$.

Let $O|_N$ stand for O restricted to N.

Definition. A suborder of O is an order T such that $|T| \subseteq |O|$ and $T = O|_{|T|}$.

Definition. Let $N \subseteq O$. An upper bound of N by O is an element x of O such that $n \leq x$ for all $n \in N$.

2.1 Partial orders

Definition. O is reflexive iff $x \leq x$ for any $x \in O$.

Definition. O is antisymmetric iff
$x \leq y \leq x => x = y$ for any $x, y \in O$.

Definition. O is transitive iff
$x \leq y \leq z => x \leq z$ for any $x, y, z \in O$.

Definition. O is partial iff O is reflexive and antisymmetric and transitive.

Lemma 1. Let O be a partial order. Let $X \subseteq |O|$. $O|_X$ is a partial order.

3 Monoids

Signature 6. A magma is a notion.

Let M,G denote magma.

Signature 7. $|M|$ is a set.

Signature 8. Let $x, y \in |M|$. $x \cdot_M y$ is an element of $|M|$.

Let M stand for $|M|$. Let $x \cdot y$ stand for $x \cdot_M y$.
[synonym element/-s] [synonym inverse/-s]

Definition. Let X be a set. M is based on X iff $|M| = X$.

Definition. G is associative iff $(x \cdot y) \cdot z = x \cdot (y \cdot z)$ for all $x, y, z \in G$.

Definition. G is abelian iff $x \cdot y = y \cdot x$ for all $x, y \in G$.

Definition. A neutral element of G is an element e of G such that $(e \cdot x = x$ and $x = x \cdot e)$ for all $x \in G$.

Lemma 2. **(uniqNeut)** Let e and e' be neutral elements of G. Then $e = e'$.

Proof. $e' = e \cdot e' = e$. ☐

Definition. A Monoid is an associative Magma with a neutral element.

Let M denote a Monoid.

Definition. Let $x, y \in M$. x divides y in M iff there exists $k \in M$ such that $k \cdot x = y$.

Lemma 3. **(transitiveDiv)** Let $k, m, n \in M$. Suppose n divides m in M and m divides k in M. Then n divides k in M.

Proof. Take an $l \in M$ such that $l \cdot n = m$.
Take an $p \in M$ such that $p \cdot m = k$.
Then $k = p \cdot m = p \cdot (l \cdot n) = (p \cdot l) \cdot n$. Thus n divides k in M. ☐

3.1 Divisibility theory

Let M denote a monoid.

Definition. $|$ is an order on M such that for any $x, y \in M$ we have $x|y$ iff x divides y in M .

Lemma 4. $|$ is reflexive and transitive.

Proof. $|$ is reflexive. Indeed x divides x in M for all $x \in M$.
$|$ is transitive (by transitiveDiv). ☐

3.2 Finiteness

Let X denote a set.

Signature 9. X is finite is an atom.

Axiom 10. (FiniteMultiplication) Let M be an abelian Monoid. Let X be a finite subset of M. Then X has an upper bound by $|$.

3.3 Groups

Signature 11. $\mathbf{e}_M$ is a neutral element of M.

Definition. A submonoid of M is a monoid N such that $N \subseteq M$ and $\mathbf{e}_N = \mathbf{e}_M$ and $(x \cdot_N y = x \cdot_M y)$ for any $x, y \in N$.

Let $\mathbf{e}$ stand for $\mathbf{e}_M$.

Definition. Let $x \in M$. An inverse of x in M is an element y of M such that $x \cdot y = \mathbf{e}_M$ and $y \cdot x = \mathbf{e}_M$.

Lemma 5. (uniqInv) Let M be a Monoid. Let $x, y, y' \in M$. Assume y and y' are inverses of x in M. Then $y = y'$.

Proof. $y = \mathbf{e} \cdot y = (y' \cdot x) \cdot y = y' \cdot (x \cdot y) = y' \cdot \mathbf{e} = y'$. □

Definition. A Group is a Monoid G such that every element of G has an inverse in G.

Let G denote a Group.

Signature 12. Let $x \in G$. x_G^{-1} is an inverse of x in G.

4 Rings

[synonym ring/-s]
[synonym divisor/-s] [synonym unit/-s]

Signature 13. A Ring is a notion.

Let R denote a ring.

Signature 14. $|R|$ is a set.

Let R stand for $|R|$.

Signature 15. $\mathrm{Ab}(R)$ is an abelian group based on R.

Signature 16. $\mathrm{Mu}(R)$ is a Monoid based on R.

Let $x+y$ stand for $x \cdot_{\mathrm{Ab}(R)} y$. Let $x \cdot y$ stand for $x \cdot_{\mathrm{Mu}(R)} y$. Let R is commutative stand for $\mathrm{Mu}(R)$ is abelian.

Definition. $0 = \mathbf{e}_{\mathrm{Ab}(R)}$.

Definition. $1 = \mathbf{e}_{\mathrm{Mu}(R)}$.

Axiom 17. **(DistribI)** Let $x, y, z \in R$. $x \cdot (y + z) = (x \cdot y) + (x \cdot z)$.

Axiom 18. **(DistribII)** Let $x, y, z \in R$. $(x + y) \cdot z = (x \cdot z) + (y \cdot z)$.

Definition. Let $x \in R$. $\text{-}x = x^{-1}_{\mathrm{Ab}(R)}$.

Let $x\text{-}y$ stand for $x + (\text{-}y)$.

Lemma 6. Let $x \in R$. $0 \cdot x = 0$.

Proof. $0 = (0 \cdot x)\text{-}(0 \cdot x)$
$= ((0 + 0) \cdot x)\text{-}(0 \cdot x)$
$= ((0 \cdot x) + (0 \cdot x))\text{-}(0 \cdot x)$
$= (0 \cdot x) + ((0 \cdot x)\text{-}(0 \cdot x))$
$= (0 \cdot x) + 0$. □

Lemma 7. **(Minus)** Let $k, q \in R$. Then $\text{-}(k \cdot q) = (\text{-}k) \cdot q$.

Proof. $(k \cdot q) + ((\text{-}k) \cdot q) = (k\text{-}k) \cdot q = 0 \cdot q = 0$.
$(k \cdot q)$ is an inverse of $((\text{-}k) \cdot q)$ in $\mathrm{Ab}(R)$. □

Lemma 8. **(MDistrib)** Let $x, y, z \in R$. $(x\text{-}y) \cdot z = (x \cdot z)\text{-}(y \cdot z)$.

Proof. We have $(x + (\text{-}y)) \cdot z = (x \cdot z) + ((\text{-}y) \cdot z)$ (by DistribII).
$(x \cdot z) + ((\text{-}y) \cdot z) = (x \cdot z)\text{-}(y \cdot z)$ (by Minus). □

Let R denote a commutative ring. Let R stand for $\mathrm{Mu}(R)$.

Lemma 9. **(divDif)** Let $k, m, n \in R$. Assume k divides m in R and k divides n in R. Then k divides $m\text{-}n$ in R.

Proof. Take $x \in R$ such that $x \cdot k = m$.
Take $y \in R$ such that $y \cdot k = n$. $(x\text{-}y) \cdot k = m\text{-}n$ (by MDistrib). □

5 Wellfounded orders

Definition. Let $N \subseteq |O|$. A minimum of N with O is an element x of N such that $y \leq x \Rightarrow x = y$ for all $y \in N$.

Definition. O is wellfounded iff O is a partial order and for all nonempty subsets S of $|O|$ there exists a minimum of S with O.

[synonym predecessor/-s]

Definition. A minimum of O is a minimum of $|O|$ with O.

Definition. $\mathcal{M}(O) = \{m \in O \mid m \text{ is a minimum of } O\ \}$.

Definition. Let $x \in O$. A predecessor of x by O is an element y of O

such that $y \leq x$.

Lemma 10. Let O be a wellfounded order. Let $x \in O$. Then there exists a predecessor y of x by O such that y is a minimum of O.

Proof. Define $X = \{z \in O \mid z \leq x\}$. $X \subseteq O$. Take a minimum z of X with O. z is a minimum of O. □

Definition. Let $x \in O$. A stranger of x in O is an element y of O such that x and y have no common predecessors by O.

Theorem. **(StrangerTheorem)** Let O be a wellfounded order. Assume every element of O has a stranger in O. Then $\mathcal{M}(O)$ has no upper bound by O.

6 The ring of integers

[synonym number/-s]

Signature 19. $\mathbb{Z}$ is a commutative ring.

Definition. $\mathbb{N}_{>0}$ is a submonoid of $\mathrm{Mu}(\mathbb{Z})$.

Definition. A positive number is an element of $\mathbb{N}_{>0}$.

Let n, m denote positive numbers.

Lemma 11. 1 is a positive number.

Axiom 20. **(MultEquiv)** Assume n divides m in $\mathbb{Z}$ and m divides n in $\mathbb{Z}$. Then $n = m$.

Lemma 12. $|$ is a partial order.

Proof. $|$ is antisymmetric (by MultEquiv). Indeed (if $x|y$ then x divides y in $\mathbb{Z}$) for all $x, y \in \mathbb{N}_{>0}$.

□

Let n is nontrivial stand for $n \neq 1$.

Definition. $\mathbb{N}_{>1} = \{x \in \mathbb{N}_{>0} \mid x \text{ is nontrivial }\}$.

Axiom 21. $n+m$ is a nontrivial positive number.

Axiom 22. Let S be a nonempty subset of $\mathbb{N}_{>1}$. Then there exists a minimum of S with $|$.

Definition. $|_{>1}$ is $|$ restricted to $\mathbb{N}_{>1}$.

Lemma 13. **(Wellfounding)** $|_{>1}$ is a wellfounded order.

Proof. $|_{>1}$ is a partial order. Every nonempty subset of $\mathbb{N}_{>1}$ has a minimum with $|$. □

7 Euclids Theorem

Lemma 14. **(ExistenceOfStrangers)** Every element of $\mathbb{N}_{>1}$ has a stranger in $|_{>1}$.

Proof. Let $x \in \mathbb{N}_{>1}$. Consider $y = 1{+}x$. $y \in \mathbb{N}_{>1}$. Let us show that x and y have no common predecessor by $|_{>1}$.
Proof by contradiction. Assume the contrary. Take a common predecessor k of x and y by $|_{>1}$. k divides $(1{+}x)$ in $\mathbb{Z}$ and k divides x in $\mathbb{Z}$. $(1{+}x)$-$x = 1$. Then k divides 1 in $\mathbb{Z}$(by divDif). 1 divides k in $\mathbb{Z}$. 1 and k are positive numbers. Thus $k = 1$(by MultEquiv) . contradiction. qed. $\square$

Definition. Let $p \in \mathbb{N}_{>1}$. p is prime iff for all $d \in \mathbb{N}_{>1}$ we have $(d|p) => d = p$.

Definition. $\mathbb{P} = \{\ p \in \mathbb{N}_{>1} \mid p \text{ is prime }\}$.

Theorem. **(Euclid)** $\mathbb{P}$ is not finite.

Proof. Proof by contradiction. Assume $\mathbb{P}$ is finite.
$\mathbb{P} = \mathcal{M}(|_{>1})$.
$\mathcal{M}(|_{>1})$ has no upper bound by $|_{>1}$ (by Wellfounding , ExistenceOfStrangers , StrangerTheorem).
$\mathcal{M}(|_{>1})$ is a finite subset of $\mathbb{N}_{>0}$.
$\mathbb{N}_{>0}$ is an abelian monoid.
Take an upper bound b of $\mathcal{M}(|_{>1})$ by $|$ (by FiniteMultiplication).
b $= 1$. $\mathcal{M}(|_{>1})$ is nonempty.
contradiction. $\square$