COLLEGE OF NATURAL SCIENCE

DEPARTMENT OF MATHEMATICS

GRADUATE PROJECT REPORT ON PERPENDICULARITY IN ABELIAN GROUP

Submited in partial fulfilment of requirements for the Degree of Master of Science in Mathematics

Prepared by: HABTU BAYAFERS

Advisor: BERHANU BEKELE(Ph.D)

August, 2014

Addis Ababa, Ethiopia

Contents

Addis Ababa University
Department of Mathematics

The undersigned hereby certify that they have read and recommend to the college of natural science for acceptance of a project entitled **perpendicularity in Abelian Group** by Habtu Bayafers in partial fulfillment of the requirements for the degree of master of Science.

Date:August,2014

Advisor: _____

Dr.Berhanu Bekele

Examining committee:_____

_____

August,2014

Acknowledgement

First and foremost I would like to give my thanks to the God who gave me the chance to live and have all such experiences in learning up to this level of which I did not think of. Secondly, I deeply thank my advisor, Dr.Berhanu Bekele, whose help, advice and material support was invaluable. Finally, I would also like to express my deepest thanks to Dr.K.Venkatswarlu, my wife Ehite Getachew and my family, for their helps directly or indirectly and to all my instructors for the long lasting they gave me during my course work.

Abstract

The main objective of the present Project is to address how to set axioms to establish a perpendicularity relation in Abelian Group and then study the existence of perpendicularity in$(Z_n, +)$ and $(Q_+, .)$ in certain other groups. This approach provides a justification for the use of the symbol $\perp$ denoting relative primeness in number theory and extends the domain of this convention to some degree.Related to that we also consider parallelism from an axiomatic perspective.

Introduction

Graham et al.made the following suggestions: When $\gcd(m, n) = 1$, the integers m and n have no prime factors in common and we say that they are relatively prime . This concept is so important in practice ,we have special notation for it. Let us agree to write $m \perp n$ and to say m is relatively prime to n if m and n are positive integers.Like perpendicular lines do not have a common direction, perpendicular numbers do not have common factors.

Namely ,in studying l-group (i.e,group with lattice structure),Birkhoff defines that two positive elements a and b of an l-group are disjoint if $a \bigwedge b = 0$ and uses the notation $a \perp b$ for disjoint element .He also remarks that disjointness specializes to relative primeness in the l-group of positive integer.The motivation of this paper is to study how justified ultimately it is to use the symbol of perpendicularity to denote relative primeness .Does this practice rely only on analogy between having no common direction and no having common factor or is a deeper linkage to entitle this convention?This equation leads us to ask properties essentially establish the notion of perpendicularity in the algebraic context and what the most suitable context for the axiomatization of perpendicularity actually is we have recently studied the axioms of perpendiculariy from the elementary geometric point of view. In an inner product space ,perpendicularity obviously trace back to their product being zero.

However ,certain feature of the perpendicularity can be shifted down to simpler algebraic structures .We will see axioms and properties of perpendicularity in abelian group and examine it in section(2.1). We will focus on

perpendicularity in $(Z_n, +)$ in section(2.2).

As Davis defined perpendicularity in abelian group differently, we will introduce another definition of perpendicularity in in section(2.3). We will consider divisibility in Q_+ in section (2.4) and finaly we will see parallelism in abelian group in section(2.5).

Chapter 1

PRELIMINARIES

1.1 *DIVISION ALGORITHM*

Theorem 1.1.1. *If a and b are integers and $a \neq 0$, then there exist unique integers q and r such that b=aq+r and $0 \leq r < |a|$, the element q is the quotient and r is the remainder.*

Proof. First we prove the existence of q and r.
Case1:let a is a positive integer.
Now consider the set $S = \{b - am : m \in Z, b - am \geq 0\} \subseteq N \bigcup \{0\}$.
S is not empty.Therefore S has a smallest element r and r=b-aq, for some integer q.
Further more, r is smaller than a, since the relation $r \geq$ a implies that $0 \leq r - a = b - a(q + 1) < r$ which contradict minimality of r.
Thus for the positive integer a and the integer b, there exist q and r such that b=aq+r and $0 \leq r < a$.
Case2:if $a < 0$, then $-a > 0$ so that by the above argument there are integers $q^{'}$ and r such that $b = (-a)q^{'} + r$ and $0 \leq r < (-a)$.
Therefore for any two integers a and b, a$\neq$, there are integers q and r such that b=aq+r and $0 \leq r < |a|$.
(Uniqueness)
Suppose $q^{'}$ *and* $r^{'}$ are integer with the same properties as q and r, then

$b = aq^{'} + r^{'}$ and $0 \leq r^{'} < |a| \Rightarrow aq^{'} + r^{'} = aq + r$
$\Rightarrow aq' - aq = r - r^{'}$
$\Rightarrow \mid a(q^{'} - q) \mid = \mid r - r^{'} \mid$.
By the definition of absolute value of an integer we know that $|r - r^{'}| = r - r^{'}$ or $r^{'} - r$ both of which are smaller than $|a|$, so that we have $|a|.|q^{'} - q| = |r - r^{'}| < |a|$.
Now if $q^{'} \neq q$ we see that $|q^{'} - q| \geq 1$ and thus $|a|.|q' - q| \geq |a|$ which is acontradiction.
Since the integer $|a|.|q^{'} - q|$ cannot both smaller than $|a|$ and greater than or equal to $|a|$, we concluded that $q^{'} = q$ which implies that $r = r^{'}$. Thus the quotient and remainder are unique. □

Definition 1.1.1. *If a and b are integers, $n > 0$, then a is congruent with b modulo n, written as $a \equiv b(modn)$ if and only if a-b divisible by n.*

Example.$8 \equiv 1(mod7)$.

Definition 1.1.2. *If $d \mid a, d \mid b$ and $c \mid a \bigwedge c \mid b \Rightarrow c \mid d$, then d is greatest common divisor of a and b denoted by* $\gcd(a, b)$

Definition 1.1.3. *An integer $a \neq 0$is factor of An integer b if and only if there is an integer c such that $b = ac$.In other words, a is a factor of b if and only if a divides b,write $(a \mid b)$*

Definition 1.1.4. *Two integers a and b not both zero , are relatively prime if and only if gcd (a,b)=1.*

Theorem 1.1.2. *If a , b and c are positive integers such that gcd(a,b)=1 and a is factor of bc, then a is factor of c.*

Proof. From $\gcd(a , b)=1$ we know there are integers x and y such that $1 = ax + by$.
Now WTS a is a factor of c.

Since $a \mid bc$ we know that $bc = ak$, for some $k \in Z$.

$$\begin{aligned} c &= c.1 \\ &= c(ax + by) \\ &= (ac)x + (bc)y \\ &= a(cx) + a(ky) \\ &= a(cx + ky) \end{aligned}$$

$\therefore a$ is a factor of c. □

Lemma 1.1.1. *If p is a prime factor of a positive integer m which is expressible as $m = p_1 p_2 \cdots p_n$, where the p_i 's are primes, then p equals one of p_i.*

Proof. Since $p \mid m$ and $m = p_1 p_2 \cdots p_n$
WTS:- p equals one of p_i 's.
By induction on n, the number of prime factors of p_i. if $n = 1$, then $m = p_1$ is a prime and, $p \mid m \Rightarrow p = p_1$.
Suppose the result holds for k prime factors.
So suppose that $p|(p_1 p_2 \cdots p_k p_{k+1})$ and p equals one of the p_i 's.
Now compare p and p_{k+1}, if $p = p_{k+1}$ we are done.If $p \neq p_{k+1}$ then by theorem1.2 $gcd(p, p_{k+1}) = 1$ .Since $p|(p_1 p_2 ... p_k)p_{k+1}$ and $gcd(p, p_{k+1}) = 1$ we have $p|(p_1 p_2 \cdots p_k)$, then by induction hypothesis p=p_i □

Theorem 1.1.3. *Given two integers a and b, at least one different from zero, then there exists unique natural number satisfying the definition of gcd.*

Proof. Let a, $b \in Z$, where at least a or b is non-zero.
WTS:- Existence and Uniqueness of gcd(a,b).
First we show existence.
Define $S = \{ma + nb : m, n \in Z \ \ and \ \ ma + nb > 0\}$, then $S \subseteq N$,and S is non-empty.
By well-ordering principle for N, S has smallest element say g.

Note: by construction $g = m_o a + n_o b$ for some $m_o, n_0 \in Z$ we will show g is the greatest divisor of a and b.
Suppose first that $g \nmid a$, then by theorem 1.1.1 for Z there exist unique integers $q, r \in Z$, where $o \leq r < g$ such that a=qg+r, by assumption $g \nmid a$, so we have $0 < r = a - gq = a - q(m_o a + n_o b) = a - qm_o a - qn_o b$
$= (1 - qm_o)a - qn_o b < g$, but r is an element of S strictly less than g.
This contradicts the fact that g is the smallest.
Thus it must be that $g \mid a$.
Similarly we have $g \mid b$.
Now suppose $h \in N$ is a divisor of both a and b.Then there exist $k, l \in Z$,such that a=kh and $b = lh$,but then $g = m_o a + n_o b = m_o kh + n_o lh = (m_o k + n_o l)h$.
$\Rightarrow \gcd(a, b) = g$
uniqueness Suppose $g^{'} \in N$ is also gcd (a, b), then we have $g^{'} | g$ and $g | g^{'}$ and hence $g = g^{'}$. □

1.2 *ABELIAN GROUP*

Definition 1.2.1. *If (G,*) is group such that $a*b = b*a$ for all $a, b \in G$,then (G,*) is a belian group (commutative group).*

Example1.(Z,+),(Q,+) etc are abelian groups.
Example2.Let $a \in R$ be a fixed real number .
Let $G = \{a^n : n \in Z\}$, then G is an a belian group under multiplication.
CONGRUENCE CLASSES MODULO n
Let a be an integer,then $\overline{a}$ denote the set of all integers congruent to a (mod n).
$\overline{a} = \{x : x \in Z, x \equiv a(mod n)\} = \{x : x \in Z, x = a + kn, for some k \in Z\}$.
$\overline{a}$ is known as the equivalent class mod n represented by a
$Z_n = \{\overline{0}, \overline{1}, ..., \overline{n-1}\}$
Example.$Z_5 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}\}$
FINITE ABELIAN GROUP

Definition 1.2.2. *An abelian group with finite number of element is called finite abelian group.*

Definition 1.2.3. *The order of an element a in a group G is the smallest positive integer n such that na=e.If no such number exists then it is infinite order.*

Lemma 1.2.1. *Let a and b two elements of finite orders of a group G Such that o(a)and o(b)are co-prime and if ab=ba.Then o(ab)=o(a)o(b).*

Proof. Let o(a)=m and o(b)=n.Let $H =< ab >$ be the subgroup of G generated by ab.
WTS:-o(ab)=o(a)o(b)
$(ab)^{mn} = a^{mn}b^{mn}$ =e, we get o(H)=$o(ab) \mid mn$.
Now $(ab)^m = a^m b^m = b^m \in H$ (since a^m=e).
As gcd(m,n)=1 and o(b)=n,we have $o(b^m)$=o(b)=n.
$\Rightarrow b^m \in H \Rightarrow o(b^m) \mid o(H) \Rightarrow n \mid o(H)$.
Similarly $m \mid o(H)$.
Thus we have $mn \mid o(H)$.Hence o(H)=mn=o(ab)=o(a)o(b). □

Theorem 1.2.1. *(LAGRANGES THEOREM) If G is finite group and H is a subgroup of G,then the order of H divides the order of G.*

Proof. since G is finite and $H \leq G$,H is also finite .Let o(G)=n and o(H)=m. Now G is partitioned in to finite number of distinct right coset namely H,$Ha_1, Ha_2, ..., Ha_{k-1}$. Also order of each coset is the order of H. $o(Ha_1) = o(Ha_2) =, ..., = o(Ha_{k-1}) = o(H) = m$ Also $o(G) = o(H) + o(Ha_1) + ... + o(Ha_{k-1})$ n=n+n+...+n(k times) =nk
Therefore the order of H divides the order of G. □

Definition 1.2.4. *An abelian group (G,+) is called finitely generate if there exists finitly many elements $x_1, x_2, ..., x_s$ in G such that every x in G can be written in the form $x = n_1x_1 + n_2x_2 + ... + n_sx_s$ with integers $n_1, n_2, ..., n_s$. In this case ,we say that the set$\{x_1, x_2, x_3, .., x_s\}$ is a generating set of G. Every finite abelian group is finitely generated abelian group.*

Example.(Zn,+) is finitely generated abelian group

Definition 1.2.5. *An abelian group which is not finite is called infinite abelian group.*

Example.The set of all non-zero rational number with respect to the usual multiplication(i.e,$(Q/\{0\},.)$) is infinite abelian group.

1.3 *CYCLIC GROUP*

Definition 1.3.1. *G is said to be cyclic if there exists an element a in G,such that every element of G is a power of a.*

Definition 1.3.2. *Let G be a group .Let $a \in G$ then subgroup H of G given by $H = \{a^n : n \in Z\}$ is called the cyclic subgroups of G generated by a and denoted by (a) ,a is called generator of G.*

Example. (nZ,+) is cyclic group with generators n and-n.

Theorem 1.3.1. *Any cyclic group is abelian group .*

Proof. Let G=(a) be cyclic group and let x , $y \in G$,then $x = a^n$, $y = a^m$ for some $m, n \in Z$.Now $xy = a^n a^m = a^{n+m} = a^{m+n} = yx$ .So G is abelian group. □

Example.Consider $Z_2 \times Z_3$ which has the element such that
$(\overline{0}, \overline{0}), (\overline{0}, \overline{1}), (\overline{0}, \overline{2}), (\overline{1}, \overline{0}), (\overline{1}, \overline{1}), (\overline{1}, \overline{2})$.
We claim that $Z_2 \times Z_3$ is cyclic,since$Z_2 \times Z_3 =< (\overline{1}, \overline{1} >$

Theorem 1.3.2. *Any infinite cyclic group is isomorphic to the additive group of integers.*

Proof. :-Let G=(a) be an infinite cyclic group generated by a and (Z ,+) be the additive group of integers.
Define $f : Z \mapsto G$ by $f(x) = a^x$ for all $x \in Z$.
Given $x, y \in Z, then x + y \in Z$ and we have $f(x + y) = a^{x+y} = a^x.a^y = f(x).f(y)$, then f is homomorphism.
For $x, y \in Z$,$x \neq y \Rightarrow a^x \neq a^y$(since G is infinite) and hence $f(x) \neq f(y)$, therefore f is one to one.
Also for each$a^x \in G$, take $x \in Z$ and $f(x) = a^x$
$\Rightarrow f$ is onto.
Therefore $G \cong Z$ □

1.4 *DIRECT SUM*

Definition 1.4.1. *Let S and T are subgroups of an abelian group G,then G is the direct sum of S and T denoted by* $G = S \bigoplus T$, *if G=S+T (i.e for each* $a \in G, s \in S$ *and* $t \in T$ *with a=s+t) and* $S \bigcap T = \{0\}$.

Definition 1.4.2. *The abelian group (A,+) is the direct product(sum) of the n non-trivial subgroups* $H_1, H_2, \cdots, H_n$ *if and only if for each* $x \in A$ *there is exactly one element* $x_i \in H_i$, *i=1,2,...,n such that* $x = x_1 + x_2 + ... + x_n$,*in this case we write* $A = H_1 \times H_2 \times H_3 \times \cdots \times H_n$

Example .write the group $A = Z/(10)$ as a direct sum of subgroups.
The non-trivial subgroups.
$H = \{\overline{0}, \overline{5}\}$
$K = \{\overline{0}, \overline{2}, \overline{4}, \overline{6}, \overline{8}\}$
$o(H) = 2$, $o(K) = 5$
$o(A) = o(H).o(k) = 2 \times 5 = 10$
Since $\overline{0} = \overline{0} + \overline{0}$
$\overline{1} = \overline{5} + \overline{6}$
$\overline{2} = \overline{0} + \overline{2}$
$\overline{3} = \overline{5} + \overline{8}$
$\overline{4} = \overline{0} + \overline{4}$

$\overline{5} = \overline{0} + \overline{5}$
$\overline{6} = \overline{0} + \overline{6}$
$\overline{7} = \overline{5} + \overline{2}$
$\overline{8} = \overline{0} + \overline{8}$
and $\overline{9} = \overline{5} + \overline{4}$.
Hence $A = Z/(10) = \{\overline{0}, \overline{1}, ..., \overline{9}\}$.
$(A) = 10$, A=H× K, $H \bigcap K = \{\overline{0}\}$

Proposition 1.4.1. *For abelian group G and subgroup S and T of G, then the following statments are equivalent.*
i)$G = S \bigoplus T$
ii)Every $g \in G$ has a unique expression of the form g=s+t, where $s \in S$ and $t \in T$
iii)There are homomorphisms $p : G \mapsto S$ and $q : G \mapsto T$ called projections and $i : S \mapsto G$, $j : T \mapsto G$ called injection such that $pi = I_s$, $qj = I_r$, $pj = o$, $qi = 0$ and $ip + jq = I_G$, where i is identity map.

Proof. (i)⇒(ii) by hypothesis $G = S + T$ so that for each $g \in G$ has an expression of the form g=s+t with $s \in S$ and $t \in T$.
To see that this expression is unique ,suppose also that g= s'+t' where $s' \in S$,$t' \in T$,s+t=s'+t' gives $s - s' = t' - t \in S \bigcap T = \{0\}$.
Hence $s = s^{'}$ *and* $t = t^{'}$.
(ii)⇒(iii)For $g \in G$ then there are unique $s \in S$ and $t \in T$ with g=s+t.
Define $p : G \mapsto S and q : G \mapsto T$ by p(g)=s and q(g)=t are wel defined because of the uniqueness hypothesis .It is routine to check p and q are homomorphism and that are the equation in the statement hold, S+T=G and then $G = S \bigoplus T$.
(iii)⇒ (i).If $g \in G$, the equation $1_G = ip + jq\ gives\ g = ip(g) + jq(g) \in S + T$.
If $g \in S, g = ig\ and\ pg = pig = g; if\ g \in T, then\ g = jg\ and\ pg = pjg = 0$.
$Therefore\ if\ g \in S \bigcap T, then\ S \bigcap T, G = S + T\ and\ hence\ G = S \bigoplus T$. □

Corollary 1.4.1. *Let S and T be subgroup of abelian group G,if $G = S \bigoplus T$, then $S \bigoplus T \cong S \times T$,*

conversely, given Abelian Groups S *and* T *,define subgroups* $S' \cong S$ *and* $T' \cong T$ *of* $S \times T$ *by* $S' = \{(s, o) : s \in S\}$ *and* $T' = \{(0, t) : t \in T\}$, *then* $S \times T = S' \bigoplus T'$.

Proof. Define f:$S \bigoplus T \mapsto S \times T$ as follows .If $g \in S \bigoplus T$ the proposition says that there is unique expression of the form g=s+t and so $f : g \mapsto (s, t)$ is well-defined function.It is routine to check that f is an isomorphism.
Conversely if g=(s,t) $\in S \times T$, then $g = (s, o)+(0, t) \in S+T$, $S \bigcap T = \{(0, 0)\}$
Hence, $S \times T = S \bigoplus T$. □

Chapter 2

PERPENDICULARITY IN ABELIAN GROUP

2.1 AXIOMS AND PROPERTIES OF PERPENDICULARITY

Definition 2.1.1. *Let(G,+) be an abelian group so that the binary relation $\perp$is a perpendicularity in G satisfying the following axioms.*
(A_1) $\forall a \in G\ \exists b \in G$ such that $a \perp b$
(A_2) $\forall a \in G \backslash \{0\}$ such that $a \not\perp a$
(A_3) $\forall a, b \in G$ such that , if $a \perp b$, then $b \perp a$
(A_4) $\forall a, b, c \in G$ such that $a \perp b \wedge a \perp c$, 'then $a \perp (b + c)$
(A_5) $\forall a, b \in G$ such that if $a \perp b$,' then $a \perp -b$.

Example. Let $G = (Z_6, +)$ be an abelian group.
Define the perpendicularity $\perp$ *in* Z_6 such that $\forall \overline{a}, \overline{b} \in Z_6$ *such that* $\overline{a} \perp \overline{b}$ *if and only if* $ab \equiv 0(mod 6)$.
Let us verify the axioms as follows.
Since $Z_6 = \{\overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\}$
A_1.$\forall \overline{a} \in Z_6\ \exists \overline{0} \in Z_6$ *such that* $\overline{a} \perp \overline{0}$ (since $0 \times a \equiv 0(mod 6)$).
Therefore A_1 holds.

A_2.$\forall \overline{a} \in Z_6 \backslash \{\overline{0}\}$ *such that* $\overline{a} \not\perp \overline{a}$.
Note that: $1 \times 1 \not\equiv o(mod6)$, $2 \times 2 \not\equiv o(mod6)$, $3 \times 3 \not\equiv o(mod6)$, $4 \times 4 \not\equiv o(mod6)$ *and* $5 \times 5 \not\equiv o(mod6)$
Therefore A_2 holds.
A_3.$\forall \overline{a}, \ \overline{b} \in Z_6$ *such that if* $\overline{a} \perp \overline{b}$, *then* $\overline{b} \perp \overline{a}$.
Since $\overline{a} \perp \overline{b}$ *if and only if* $ab \equiv 0(mod6)$
this implies $ba \equiv 0(mod6)$
which impleis $\overline{b} \perp \overline{a}$
Therefore A_3 holds.
A_4. Let $\overline{a}, \ \overline{b}, \ \overline{c} \in Z_6$ *such that if* $\overline{a} \perp \overline{b} \bigwedge \overline{a} \perp \overline{c}$
since $\overline{a} \perp \overline{b} \Rightarrow ab \equiv 0(mod6)$.
this implies $6 \mid ab$
which is $ab = 6t, for\ some\ t \in Z$
similarly, $\overline{a} \perp \overline{c}$
this implies $ac \equiv 0(mod6)$
which is $6 \mid ac$
so that $ac = 6k, \ for\ some\ k \in Z$.
Now, ab+ac=6t+6k for some $t, k, \in Z$ *this implies* $a(b+c) = 6w, w = t+k \in Z$.
which implies $6 \mid a(b+c)$.
implies that $a(b+c) \equiv 0(mod6)$
so that $\overline{a} \perp (\overline{b} + \overline{c})$
Therefore A_4 holds.
A_5. Let $\overline{a}, \ \overline{b} \in Z_6$ *such that* $\overline{a} \perp \overline{b}$
this implies $ab = 0(mod6)$.
which implies $-ab = 0(mod6)$ *which is* $a(-b) \equiv 0(mod6)$
$\Rightarrow \overline{a} \perp \overline{-b}$.
Therefore A_5 *holds*.
Remark1: This concept can be defined also in weaker structures by changing these axioms appropriately.
For example, if G is an abelian monoid, then we simply omit (A_5).

Remark2: For any abelian group G, the binary relation $\perp$ is trivial perpendicularity :

$$x \perp y \Leftrightarrow x = 0 \bigvee y = 0 \tag{2.1}$$

is always exists, we are mainly interested in non trivial perpendicularity.

Proposition 2.1.1. *.Let (G,+) be an abelian group and $\perp$ aperpendicularity in G, then*

a. $\forall a \in G$ *such that* $a \perp 0$

b . $\forall a \in G \backslash \{0\}$ *such that* $a \not\perp -a$

c . $\forall a, b_1, b_2, \cdots, b_k \in G, \gamma_1, \cdots, \gamma_k \in Z$ *such that if* $a \perp b_1, b_2 \cdots b_k$, *then* $a \perp (\gamma_1 b1 + \cdots + a \perp \gamma_k b_k)$

d. $\forall a, b \in G$ *,*$\mu, \nu \in Z$ *such that if* $a \perp b$, *then* $\mu a \perp \nu b$

Proof. a) $\forall a \in G \; \exists \; b \in G$ *such that* $a \perp b$ *by* (A_1)

$\Rightarrow a \perp -b$ *by* (A_5)

$\Rightarrow a \perp (b - b)$ *by* (A_4)

$\Rightarrow a \perp 0$ therefore $\forall a \in G : a \perp 0$. □

b): $\forall a \in G \backslash \{0\} : a \not\perp -a$

Proof. suppose not ,i.e $a \perp -a$

$\Rightarrow a \perp -(-a)$ by (A_5)

$\Rightarrow a \perp a$ *which is contradict to* (A_2)

Therefore $a \not\perp -a$.

c .$a \perp b_1 \Rightarrow a \perp (b_1 + b_1) \Rightarrow a \perp (2b_1), \cdots, a \perp (\gamma_1 b_1,$

$a \perp b_2 \Rightarrow a \perp (b_2 + b_2) \Rightarrow a \perp (2b_2), \cdots, a \perp (\gamma_2 b_2)$

$, ..., a \perp (\gamma_k b_k)$

$\therefore a \perp (\gamma_1 b_1 + \gamma_2 b_2 + \cdots + \gamma_k b_k)$

d.$\forall a, b, c \in G, \mu, \nu \in Z : a \perp b \Rightarrow \mu a \perp \nu b$

suppose $a \perp b \Rightarrow a \perp (b + b) \Rightarrow a \perp (2b), \cdots, a \perp (\nu b)$

and let $a \perp \nu b \Rightarrow (a + a) \perp \nu b \Rightarrow 2a \perp \nu b, \cdots, \mu a \perp \nu b$ for $\mu, \nu \in Z$

Therefore $\mu a \perp \nu b$. □

Proposition 2.1.2. *A binary relation $\perp$ in G is a perpendicularity if and only if it satisfies (A_1) ,(A_2), (A_6) $\forall a, b, c \in G : a \perp b \bigwedge a \perp c \Rightarrow (b - c) \perp a$.*

Proof. $(\Rightarrow)$*Since* $\perp$ *is perpendicularity in* G, *then* A_1, A_2 *follows from definition.*
To show A_6 *let* $a \perp b \bigwedge a \perp c$.
$\Rightarrow a \perp b \bigwedge a \perp -c$ *by* A_5
$\Rightarrow a \perp (b - c)$ *by* A_4
$(b - c) \perp a$
$(\Leftarrow)$*suppose* $A_1, A_2,$ A_6*are holds.*
Claim : $-$ $\perp$ *is perpendicularity in* G.
Let $a \in G$ *by* $(A_1) \exists b$ *such that* $a \perp b$. *putting* $c := b$ *in* $(A_6) \Rightarrow 0 \perp a$.
Further apply (A_6) *with* $a := 0, b := a$ *and* $c := 0$ *gives* $(a-0) \perp 0$ *that is* $a \perp 0$.
Now we can verity that the remaining axioms.
Assume $a \perp b$, *apply* (A_6) *with* $c = 0$, *then* $b \perp a$ *and* (A_3) *is satisfied.*
Assume $a \perp b$ *and apply*(A_6) $b := 0$*and* $c := b$ *it gives* $b \perp a$ *by* $(A_3) a \perp -b$,
then A_5 is satisfied.
Now again apply (A_6) with $c := -c \Rightarrow (b - (-c)) \perp a$ *that is* $(b + c) \perp a$
Hence by (A_3) $a \perp (b + c)$ *and hence* (A_4) is satisfied.
Therefore $\perp$ is a perpendicularity in G. □

Proposition 2.1.3. *If every element of G have finite order and if* $\perp$ *satisfies* $(A_1) - (A_4)$, *then it satisfies* (A_5) .
If G has at least one element of G infinite order then there exists a relation $\perp$ *which satisfies* $(A_1) - (A_4)$ *but not* (A_5).

Proof. Assume that $a, b, \in G$ *satisfies* $a \perp b$ *and let the order of* b *be* n, *then we have* $a \perp (n - 1)b$ *by* $(A4) \Rightarrow a \perp (nb - b)$
Since n is order of b then nb =0
$\Rightarrow a \perp (o - b) \Rightarrow a \perp -b$ and hence (A_5) holds.
For the second part , let$a \in G$ have an infinite orde.Then the subgroup $\{0, \pm a, \pm 2a, ...\}$ is isomorphic to Z.
Consider relation $\perp$ defined by

$$x \perp y \Leftrightarrow (\exists \mu, \nu \in Z : x = \mu a \bigwedge y = \nu a \bigwedge \nu\mu < 0) \bigvee x = 0 \bigvee y = 0 \quad (2.2)$$

Definition 2.1.2. *Let G be an abelian group, $A, B \leq G, x \in G, \perp be perpendicularity on G$:*
1.By $x \perp A$, we mean $x \perp y$ for all $y \in A$.
2.By $B \perp A$, we mean $x \perp y$ for all $x \in A$ and for all $y \in B$.

If A is a non - empty subset of G, we define the perpendicular complement ($\perp-$ complement) of A as follows.

Definition 2.1.3. *Let G be a group, $A, B \subseteq G, x \in G$ and $\perp$ be perpendicularity in G*
1.By $x \perp A$, we mean $x \perp y$ for all y in A.
2.By $B \perp A$, we mean $x \perp y$ for all $x \in B$ and $y \in A$.

$$A^{\perp} = \{y \in G : y \perp A\} = \bigcup B, where G \supseteq B \perp A \quad (2.3)$$

Then $A^{\perp}$ *is the maximal set.*
In particular, $G^{\perp} = \{0\} and \{0\}^{\perp} = G$. □

Proposition 2.1.4. *If $A \subseteq G$, then $A^{\perp}$ is a subgroup of G. If G is cyclic, then $A^{\perp}$ is cyclic.*

Proof 2.1.1. *Let A be the subgroup of G.*
Claim $A^{\perp}$ is subgroup of G.
$A^{\perp} = \{y \in G : y \perp A\} \Rightarrow y \perp x, \forall x \in A$
Since $0 \perp x$ for all $x \in A$, we have $0 \in A^{\perp}$, so $A^{\perp} \neq \emptyset$
Let $x, y \in A^{\perp}$.
Then $x \perp a$ and $y \perp a$ for $a \in A \Rightarrow x - y \perp a$ by (A_4)
$\Rightarrow x - y \in A^{\perp}$. *Thus $A^{\perp}$ subgroup of G.*
Second part of the proof follows from the fact that any subgroup of acyclic group is cyclic.
Hence $A^{\perp}$ is cyclic.

Theorem 2.1.1. *The following condition are equivalent*
a). G has a non- trivial perpendicularity $\perp$
b). G has non- trivial cyclic subgroups H and K satisfying $H \bigcap K = \{0\}$

Proof. (a) $\Rightarrow$ $(b).Since \perp is\ non-trivial\ thereexists x, y \in G.$
$Claim : Ghas\ non\ trivial\ cyclic\ subgroups\ HandKsatisfying\ H \bigcap K = \{0\}$
$Since \perp is\ non\ trivial\ \exists x, y \in G\ such\ that\ x \perp y.$
$LetH =< x >\ and\ K =< y >, thenH =< x >\ and\ K =< y >$ *are non trivial cyclic subgroups.*
$Moreover, letz \in H \bigcap K = \{0\} \Rightarrow z = nx\ and\ z = myforsomem, n \in Z.$
$Sincex \perp y \Rightarrow nx \perp my \Rightarrow z \perp z \Leftrightarrow z = 0$
$\therefore H \bigcap K = \{0\}.$
(b) $\Rightarrow$ (a) since G has non-trivial cyclic subgroups H and K satisfying $H \bigcap K = \{0\}$, therefore G has non-trivial perpendicularity$\perp$ defined by

$$x \perp y \Leftrightarrow (x \in H \bigwedge y \in K) \bigvee (x \in K \bigwedge y \in H) \bigvee x = 0 \bigvee y = 0 \qquad (2.4)$$

□

Example 2.1.1. $Let\ G = Z_6.By\ lagrange's theorem,\ the\ smallest\ n\ such\ that\ Z_n\ has\ anon-trivial\ Perpendicularity\ is\ 6 = 2.3\ because\ n\ must\ have\ at\ least\ two\ different\ prime\ factors.$
$ConsiderH =< 3 >= \{\overline{0}, \overline{3}\}\ and\ K =< 2 >= \{\overline{0}, \overline{2}, \overline{4}\}.$
$Then\ H\ and\ Kare\ the\ only\ non\ tirivial\ subgroups\ ofZ_6.$
$Thus\ Z_6\ has\ exactly\ one\ non-trivial\ perpendicularity,\ defined\ by\overline{0} \perp \overline{0}, \overline{1}, \overline{2}, \overline{3}, \overline{4}, \overline{5}\ and\ \overline{3} \perp \overline{2}, \overline{4}\ a$

Example 2.1.2. *letG=R has infinitely many pairs of nontrivial subgroups with intersection* $\{0\}$*,it has infinitely many nontrivial perpendicularities.*
For example ,let H= Q and K=$\{x\sqrt{2} : x \in Q\}$ *and define* $\perp$ *by (4).To see that this perpendicularity is not maximal ,let* $H_1 = \{x\sqrt{3} : x \in Q\}$ *and* $K_1 = \{x\sqrt{5} : x \in Q\}$ *and define* $\perp'$ *by*

$$x \perp' y \Leftrightarrow (x \in H \bigwedge y \in K) \bigvee (y \in K \bigwedge x \in H)$$

$$\bigvee(x \in H_1 \bigwedge y \in K_1) \bigvee(x \in K_1 \bigwedge y \in H_1) \bigvee x = 0 \bigvee y = 0 \qquad (2.5)$$

Example 2.1.3. *let G=(Q_+,.),where Q_+ denote the set of positive rational numbers.*
Every $c \in Q_+$ can be expressed as

$$c = \prod P^{v_p(c)} \qquad (2.6)$$

where
$v_p(c) \in Z$ *and* $p \in \rho$.
Assign now

$$a \perp b \Leftrightarrow \forall p \in \rho, v_p(a) = 0 \bigvee v_p(b) = 0 \qquad (2.7)$$

where ρ is the set of primes.
In other words

$$a = \frac{m}{u} \text{ and } b = \frac{n}{v}, where\ m, n, u, v \in Z_+,\ gcd(m, u) = \gcd(n, v) = 1 \qquad (2.8)$$

then

$$a \perp b \Leftrightarrow \gcd(mu, nv) = 1 \qquad (2.9)$$

for

$$m, n \in Z_+, m \backslash 1 \text{ and } n \backslash 1\ m \perp n \Leftrightarrow \gcd(m, n) = 1 \qquad (2.10)$$

2.2 *PERPENDICULARITY IN* Z_n

Studying perpendicularties requires that we know the structure of G. Next we take a more through look at perpendicularity in Z_n.

Theorem 2.2.1. *If*

$$n = p_1^{\alpha_1}.p_2^{\alpha_2}...p_r^{\alpha_r} \qquad (2.11)$$

where $p_1, ..., p_r \in \rho$ which are distinct primes and $\alpha_1, ..., \alpha_r > 0$, then

$$Z_n = H_1 \bigoplus H_2 \bigoplus ... \bigoplus H_r \tag{2.12}$$

where

$$H_i =< e_i >, e_i = \frac{n}{p_i^{\alpha_i}} \tag{2.13}$$

i= 1,2,3,...,r and the decomposition of $Z_n = H_1 \bigoplus H_2 \bigoplus \cdots \bigoplus H_r$ *is unique (up to the order of sub groups).*

Proof. Define H_i to be the set of all elements of Z_n order of a power of p_i.
To show H_i is subgroup of Z_n we take $x, y \in H_i$ of order p^a and p^b respectively where $p = p_i$.
Taking c to denote larger of a and b we see that $p^c(x + y) = p^c x + p^c y = 0$.
So that the order of x+y is a divisor of p^c .
Hence $x + y \in H_i$ *and if* $x \in H_i$ *then*$(p^a - 1)x = p^a x - x = -x$
Thus $-x \in H_i$
Therefore H_i is subgroup of Z_n.This implies $H_1, H_2, \cdots, H_r$ are subgroups of Z_n, and then $H1 \bigoplus H_2 \bigoplus \cdots \bigoplus H_r \leq Z_n$.
($\Leftarrow$).Select $w \in Z_n$ with order m=$p_1^{\theta_1}.p_2^{\theta_2}...p_r^{\theta_r}$, where $\alpha_i \geq \theta_i$.Since m divides n then $p_i^{\theta_i}$ is factor of $p_i^{\alpha_i}$.
Denote q_i be positive integer $q_i = \frac{m}{p_i^{\theta_i}}$, where i=1,2,...,r.
$q_1 = \frac{m}{p_1^{\theta_1}} = p_2^{\theta_2}...p_r^{\theta_r}$.
$q_2 = \frac{m}{p_2^{\theta_2}} = p_1^{\theta_1}.p_3^{\theta_3}...p_r^{\theta_r}$
$\vdots$
$q_r = \frac{m}{p_r^{\theta_r}} = p_1^{\theta_1}.p_2^{\theta_2}...p_{r-1}^{\theta_{r-1}}$.
gcd$(q_1, q_2, ..., q_r)$=1.
Then the set of r integers $\{q_1, q_2, ..., q_r\}$ is relatively prime sets
and we know from gcd, the integer t_i exists such that $1 = q_1t_1 + ... + q_rt_r$.Since w=1.w
$=(q_1t_1 + ... + q_rt_r)w = (q_1t_1)w + ... + (q_rt_r)w$, decomposition of w as a sum of certain elements $w_i = q_it_iw \in Z_n$.
We know that $q_ip_i^{\theta_i} = m$ *so that* $p_i^{\theta_i}wi = ti(mw) = 0 \in H_i$.Which implies $w_i \in H_i$.

$\Rightarrow Z_n \leq H_1 \bigoplus H_2 \bigoplus \cdots \bigoplus H_r.$
$\therefore Z_n = H_1 \bigoplus H2 \bigoplus \bigoplus Hr.$ □

Lemma 2.2.1. *For all i, j= 1, ..., r, $i \neq j$, $e_i^2 \neq 0$, $e_i e_j = 0$.*

Proof. It is enough to consider that i=1,j=2. Regarding e_1 and e_2 as integers, we have i)$e_1^2 = \frac{n^2}{p_1^{2\alpha_1}}$
$\Rightarrow \frac{(p_1^{\alpha_1}....p_r^{\alpha_r})^2}{p_1^{2\alpha_1}} = \frac{p_1^{2\alpha_1}...p_r^{2\alpha_r}}{p_1^{2\alpha_1}} = p_2^{2\alpha_2}...p_r^{2\alpha_r} \not\equiv 0(modn).$
Hence $e_i^2 \neq 0$
ii)

$$e_1 e_2 = \frac{n}{p_1^{\alpha_1}}.\frac{n}{p_2^{\alpha_2}} \tag{2.14}$$

since $e_1 = \frac{n}{p_1^{\alpha_1}}$ and $e_2 = \frac{n}{p_2^{\alpha_2}}$ then $e_1 e_2 = \frac{n}{p_1^{\alpha_1}}.\frac{n}{p_2^{\alpha_2}} = \frac{n^2}{p_1^{\alpha_1} p_2^{\alpha_2}} = p_2^{\alpha_2}...p_r^{\alpha_r}.p_1^{\alpha_1}...p_r^{\alpha_r}$ and $p_1^{\alpha_1}....p_r^{\alpha_r}$. $p_3^{\alpha_3}....p_r^{\alpha_r}$ by
re-arrange the order, then we have$p_3^{\alpha_3}...p_r^{\alpha_r}.n \equiv 0(modn)$, Where from the product$e_i e_j = 0$ follows. □

Lemma 2.2.2. *Let $\perp$ be perpendicularity in Z_n, then $\forall \overline{a}, \overline{b}, \overline{c}, \overline{d} \in Z_n$ such that*

$$\overline{a} \perp \overline{b} \Rightarrow \overline{ca} \perp \overline{db} \tag{2.15}$$

Proof. Let $\overline{c} = \gamma\overline{1}$,$\overline{d} = \delta\overline{1}$ where γ and δ are integers with $0 \leq r, \delta < n$. Since $\overline{ca} = (\gamma\overline{1})\overline{a} = \gamma(\overline{1a}) = \gamma\overline{a}$ similarly $\overline{db} = (\delta\overline{1})\overline{b} = \delta(\overline{1b}) = \gamma\overline{b}$ by proposition1(d) $\gamma\overline{a} \perp \delta\overline{b} \Rightarrow \overline{ca} \perp \overline{db}$
$\therefore \overline{ca} \perp \overline{db}.$

□

Now we are ready to introduce perpendicularity which turns out to be maximal in Z_n.
Let

$$x = x_1 + ... + x_r, y = y_1 + ... + y_r \in Z_n \tag{2.16}$$

where $x_i, y_i \in H_i$, i=1, ..., r. The relation$\perp_0$, defined in Z_n by

$$x\perp_0 y \Rightarrow \forall i \in \{1,...,r\} : x_i = 0 \bigvee y_i = 0 \tag{2.17}$$

is aperpendicularity.

Definition 2.2.1. *The perpendicularity $\perp$ is maximal if there is no another perpendicularity contains it.*

Theorem 2.2.2. *The perpendicularity $\perp_0$ is maximal and every other perpendicularity in Z_n is contained in it.*

Proof. Let$\perp$ be another perpendicularity in Z_n. Our claim is that $x\perp y \Rightarrow x\perp_0 y$ by (**12**) we can express

$$x = \xi_1 e_1 + \cdots + \xi_r e_r, y = \eta_1 e_1 + ... + \eta_r e_r \tag{2.18}$$

where the integers $\xi_i, \eta_i \in \{0, ..., p_i^{\alpha i} - 1\}$ and the residue class $e_i = \frac{n}{p_i^{\alpha_i}}$ i = 1,2,...,r

Suppose against the claim of theorem that there exist $x, y \in Z_n$ such that $x\perp y, but\ x \not\perp_0 y$. Then $\xi_i, \eta i \neq 0$ for some i. Reordering the indices so that i=1 and apply lemma 2 We have

$$xe_1\perp ye_1 \Rightarrow \xi_1 e_1^2 \perp \eta_1 e_1^2 \tag{2.19}$$

by prop 1 d

$$\frac{\eta_1}{gcd(\xi_1, \eta 1)}\xi_1 e_1^2 \perp \frac{\xi_1}{\gcd(\xi_1, \eta_1)}\eta_1 e_1^2 \tag{2.20}$$

that is $lcm(\xi_1, \eta_1)e_1^2 \perp lcm(\xi_1, \eta_1)e_1^2$ *consequently* $lcm(\xi_1, \eta_1)e_1^2 = 0$ by (A_2).

In other words regarding e_1 as an integer and

$$lcm(\xi_1, \eta_1)e_1^2 = lcm(\xi_1, \eta_1).\frac{n^2}{p_1^{2\alpha_1}} \tag{2.21}$$

$$= lcm(\xi_1, \eta_1).p_2^{2\alpha_2}...p_r^{2\alpha_r} \tag{2.22}$$

and $p_1^{\alpha_1}$ divides $lcm(\xi_1, \eta_1)$. However, since it divides neither ξ_1 nor η_1, this is a contradiction. Hence $x \perp_0 y$.

Let x $= x_1 + x_2 + ... + x_r$, y$= y_1 + y_2 + ... + y_r$ *with vectors* $(x_1, x_2, ..., x_r)$ and $(y_1, y_2, ..., y_r)$ respectively, so it is natural to define their " inner product"

$$< x, y >= x_1y_1 + x_2y_2 + ... + x_ry_r \tag{2.23}$$

□

Proposition 2.2.1. *Give*

$$x, y \in Z_n, < x, y >= xy \tag{2.24}$$

Proof. We have

$$xy = (\sum_{i=1}^{r} x_i)(\sum_{i=1}^{r} y_i) = \sum_{i=1}^{r} x_iy_i + \sum_{i,j=1}^{r} x_iy_j(j \neq i) \tag{2.25}$$

$= (x_1 + x_2 + x_3 + ... + x_r)(y_1 + y_2 + y_3 + y_r)$

$= (x_1y_1 + x_1y_2 + ... + x_1y_r) + (x_2y_1 + x_2y_2 + ... + x_2y_r) + ... + x_ry_1 + ...x_ry_r)$

$= (x_1y_1 + x_2y_2 + ... + x_ry_r) + [(x_1y_2 + ... + x_1y_r) + (x_2y_1 + x_2y_3 + ... + x_2y_r) + ... + (x_{r-1}y_1 + ...$

$= \sum_{i=1}^{r} x_iy_i + \sum_{i,j=1}^{r} x_iy_j$

where $i \neq j$

Now let show $< x, y >= xy$ since xy$=\sum_{i=1}^{r} x_iy_i + \sum_{i,j=1}^{r} x_iy_j$ where $i \neq j$

We have $x_i = \xi_i e_i$ *and* $y_i = \eta_j e_j$ *and* $e_ie_j = 0$.Then

$$\sum_{i,j}^{r}{}_{,i\neq j} x_iy_j = \sum_{i,j}^{r}{}_{,i\neq j} \xi_i e_i \eta_j ej = 0 \tag{2.26}$$

Thus $\sum_i^r x_iy_i = x_1y_1 + x_2y_2 + ... + x_ry_r$ and then $< x, y >= x_1y_1 + ... + x_ry_r$ $\therefore < x, y >= xy$ □

Theorem 2.2.3. *Let* $\perp$ *be a perpendicularity in* Z_n*. Then*

$$\forall x, y \in Z_n : x \perp y \Rightarrow xy = 0 \tag{2.27}$$

Proof 2.2.1. *If $x\perp y$, then $x\perp_0 y$ by theorem3.so xy=0 because of $x\perp_0 y$ iff $\forall i \in \{\{1,...,r\}; x_i = 0 or\ y_i = 0$ and proposition 5 $< x, y >= xy$*

Theorem 2.2.4. *Let(G,+) be an abelian group and $n = p_1^{\alpha_1}.p_2^{\alpha_2}...p_r^{\alpha_r}$,then the following condition are equivalent*
a.$\alpha_1 = ... = \alpha_r = 1$
b.$\forall x, y \in Z_n : xy = 0 \Rightarrow x\perp_0 y$
c.$\forall x \in Z_n : x^2 = 0 \Rightarrow x = 0$

Proof. (a)$\Rightarrow$ (*b*). Assume that $x\perp_0 y$,now express x and y as x= $\xi_1 e_1 + ... + \xi_r e_r$ *and* $y = \eta_1 e_1 + ... + \eta_r e_r$ we can rearrange the indices so that, for some $s \in \{1, ...r\}$ such that $\xi_i, \eta_i \neq 0$, i=1,...,s

$$\xi_i = 0 \bigvee \eta_i = 0, i = s+1, ..., r \tag{2.28}$$

From (prop5) we have

$$xy = \xi_1\eta_1 e_1^2 + ... + \xi_s\eta_s e_s^2 \tag{2.29}$$

If $\xi_1\eta_1 e_1^2 + ... + \xi_s\eta_s e_s^2 = 0$ then the integer$\xi_1\eta_1 e_1^2 + ... + \xi_s\eta_s e_s^2 \equiv 0$ (mod n) that is

$$\xi_1\eta_1\frac{n^2}{p_1^2} + ... + \xi_s\eta_s\frac{n^2}{p_s^2} \equiv 0(modn) = p_1p_2...p_r) \tag{2.30}$$

However this is impossible because none of $p_1, p_2, ..., p_s$ divides the left hand side (namely,pi divides every other summands except the i^{th} one). There fore $xy \neq 0$ and our claim follows by contradition
(b)$\Rightarrow$ (*c*). If $x^2 = 0$, then $x\perp_0 x$ by (b) and x=0 by (A_2)
(c)$\Rightarrow$(a). Suppose (a) does not hold,then, say $\alpha 1 > 1$.
Let x=$\frac{n}{p_1}$ since the integer $x^2 = \frac{n^2}{p_1^2} = \frac{p_1^{2\alpha 1}.p_2^{2\alpha 2}...p_r^{2\alpha r}}{p_1^2}$=

$$p_1^{2\alpha_1 - 2}...p_r^{2\alpha r} \equiv 0(modn) \tag{2.31}$$

The residue class $x^2 = 0$, But $x \neq 0$. And hence (c) does not hold. Again the claim follows now by contradiction. □

Corollary 2.2.1. *If and only if the conditions of theorem5 are satisfied then*

$$\forall x, y \in Z_n : x \perp_0 y \Rightarrow n|(xy) \tag{2.32}$$

where(xy is the product of integers x and y)

Proof. Suppose the conditions of theoremm5 are satisfied.
WTS $\forall x, y \in Z_n$ *such* $x \perp_0 y$, *then* $n|(xy)$.
If $\forall x, y \in Z_n$ *implies* $x \perp_0 y$ by(Theorem3b) *that is* $xy = 0$ *by definition of* $\perp_0$
which is $xy \equiv 0(modn)$ *so that* $n|(xy - 0) \Rightarrow n|(xy)$
$\therefore n|(xy)$ □

Example 2.2.1. *Let* $G = Z_{30}$, *since 30 =*$2\times3\times5$ *by theorem2 (i.e* $Z_n = H_1 \bigoplus H_2 \bigoplus ... \bigoplus H_r$*)*
we have

$$Z_{30} =< \frac{30}{2} > \bigoplus < \frac{30}{3} > \bigoplus < \frac{30}{5} > \tag{2.33}$$

$= \{\overline{0}, \overline{15}\} \bigoplus \{\overline{0}, \overline{10}, \overline{20}\} \bigoplus \{\overline{0}, \overline{6}, \overline{12}, \overline{18}, \overline{24}\}$
Since $\overline{2} = 0.\overline{15} + 2.\overline{6} + 2.\overline{10}$ *and* $\overline{15} = 1.\overline{15} + 0.\overline{10} + 0.\overline{6}$
$\Rightarrow \overline{2} \perp_0 \overline{15}$ *iff* $30 \mid (2 \times 15)$
Therefore $30 \mid (xy)$

Example 2.2.2. *Let* $G = Z_{360}$ *,since 360=*$2^3 \times 3^2 \times$ *5*
we have $Z_{360} =< \frac{360}{8} > \bigoplus < \frac{360}{9} > \bigoplus < \frac{360}{5} >$

$$= \{\overline{45}, \overline{90}, \overline{135}, \overline{200}, \overline{270}, \overline{315}\} \bigoplus \{\overline{40}, \overline{80}, \overline{120}, \overline{160}, \overline{200}, \overline{280}, \overline{320}\} \bigoplus \{\overline{72}, \overline{144}, \overline{216}, \overline{288}\} \tag{2.34}$$

$\overline{5} \perp_0 \overline{72}$ *because* $\overline{5} = 1.\overline{45} + 8.\overline{40} + 0.\overline{72} and \overline{72} = 0.\overline{45} + 0.\overline{40} + 1.\overline{72}$
Now (33) is the only necessary for $\perp_0$ *but not sufficient.*
Let see $\overline{10} \not\perp_0 \overline{36}$ *due to the fact that* $\overline{10} = 2.\overline{45} + 7.\overline{40} + 0.\overline{72}$ *and* $\overline{36} = 4.\overline{45} + 0.\overline{40} + 3.\overline{72}. However 360|(10 \times 36)$

2.3 ANOTHER DEFINITION OF PERPENDICULARITY

Davis defined perpendicularity as binary relation $\perp$ in G if it is satisfying the following conditions.
(D_1) $\forall a, b \in G$ such that, if $a \perp b$, *then* $b \perp a$.
(D_2) $\forall a \in G$ *such that* $0 \perp a$
(D_3) $\forall a \in G$ such that, if $a \perp a$, *then* $a = 0$
(D_4) $\forall a, b, c \in G$ *such that if* $b \perp a \bigwedge c \perp a$, *then* $(b + c) \perp a$ $(D_5) \forall a, b \in G$ *such* if $a \perp b \Leftrightarrow \{a\}^{\perp\perp} \bigcap \{b\}^{\perp\perp} = \{0\}$. He assumes that G is an abelian group but the definition applies more generally to an abelian monoid too. It is easy to see that$(D_1) - (D_4)$ are equivalent to $(A_1) - (A_4)$. Axiom (D_5) arises from introducing the concept of " disjointness " on a vector lattice.

Proposition 2.3.1. *Assume that*$\perp$ *satisfies* $(D_1) - (D_3)$ *equivalently* $(A_1) - (A_3)$.

$$\forall a, b \in \ G such\ that\ a \perp b, then \{a\}^{\perp\perp} \bigcap \{b\}^{\perp\perp} = \{0\} \tag{2.35}$$

Proof. We show that 1^{st} that if $\emptyset \neq A \subseteq G$, then

$$A \bigcap A^{\perp} = \{0\} \tag{2.36}$$

If x $\in A \bigcap A^{\perp}$, *then* $x \perp y \ \ \forall y \in A. In\ particular, x \perp x$ *and hence* $x = 0$ *by* (D_3)
$\therefore A \bigcap A^{\perp} = \{0\}$.
Assume next that $a \perp b$ *and let* $x \in \{a\}^{\perp\perp} \bigcap \{b\}^{\perp\perp}$
Note that, $\{a\}^{\perp} = \{y \in G : y \perp \{a\}\}$
$\{a\}^{\perp\perp} = \{a \in G | a \perp \{a\}^{\perp}\}$
Then now, since $x \perp \{b\}^{\perp}$ *and* $a \in \{b\}^{\perp}$, we have $x \perp a \Rightarrow$ x$\in \{a\}^{\perp}$. Thus x$\in \{a\}^{\perp} \bigcap \{a\}^{\perp\perp}$
But $A \bigcap A^{\perp} = \{0\}$. Then applied this to $A = \{a\}^{\perp} \Rightarrow \{a\}^{\perp} \bigcap \{a\}^{\perp\perp} = \{0\}$

and x=0

How are these two perpendicularities related? there is partial answer.Let denote by A and D the axioms $(A_1)-(A_5)$ *and* $(D_1)-(D_5)$ respectively. □

Proposition 2.3.2. *If all elements of G have finite orders ,then* $D \Rightarrow A$ *.If G has at least one element of infinite order, then* $\exists$ *a relation* $\perp$ *satisfying D but not A.*

PART 1

Proof. Let every elements of G has finite order.

WTS $D \Rightarrow A$

i).Let $a, b \in G$ $satisfying$ $a \perp b$, then A_1 is satisfied.

ii).$\forall a \in G$ *such that* $a \perp a$, *then* $a = 0$ *unless* $a \not\perp a$...$(A_2)$is satisfied)

iii)$\forall a, b \in G$ *suchthat* $a \perp b$, *then* $b \perp a$ *by* D_1, *then* (A_3) is satisfied.

iv). $\forall a, b, c \in G$ *such that* $b \perp a \bigwedge c \perp a$, *then* $(b + c) \perp a$ *by* (D_1)
implies that $a \perp (b + c)$ A_4 is satisfied.

v)Let order of b be n then ,if$a \perp b$, *then* $b \perp a$*implies that* $b(n-1) \perp a$
which is equivalent to $bn - b \perp a$

$\Rightarrow -b \perp a$

$\Rightarrow a \perp -b$ by (D1)

Then A_5 is satisfied .

Therefore $D \Rightarrow A$

PART 2.

If G has at least one element of infinite order then $\ni$ a relation $\perp$ satisfying D_5 but A.Because A_5 does not satisfied i.e let $a \in G$ has infinite order ,then the subgroup $\{0, \pm a_1, \pm a_2, ...\}$ is isomorphic to Z .The relation $\perp$ defined by $x \perp y \Leftrightarrow (\exists \alpha, \beta \in Z$ such that $x = \alpha a \bigwedge y = \beta a \bigwedge \alpha\beta \leq 0$ V $x = 0 \bigvee y = 0$
$(A_1 - A_4)$ $satisfied$ $but A_5$ is not satisfied by (pr2) □

Proposition 2.3.3. *Assume that G has elements* $a_1, a_2, a_3, a_4 \neq 0$ *such that* $< a_i > \bigcap < a_j >= \{0\}$ *whenever* $i \neq j$*.There exists a relation* $\perp$ *satisfying A but not D.*

Proof. The relation $\perp$ defined by (5) with H= $< a_1 >, K =< a_2 >, H_1 =< a_3 >$ and K=$< a_4 >$satisfies A. Since $\{a1\}^{\perp\perp} \bigcap \{a_3\}^{\perp\perp} =< a_1 > \bigcap < a_3 >= \{0\}$ and $a_1 \not\perp a_3$, then it does not satisfy (D_5) □

2.4 *DIVSIBILITY IN* Q_+

The binary relation" |" is said to be divisibility in G satisfying the following conditions

i). $\forall a \in Q_+$ *such* $a \mid a$

ii) $\forall a, b, c \in Q_+$ *such that* $c|a \bigwedge c \mid b \Rightarrow c \mid (ab)$

iii) $\forall a, b, c \in Q_+ :\ c \mid b \bigwedge b \mid a \Rightarrow c|a$

Divisibility is a reflexive and transitive relation satisfying (ii).

If $b \mid a$ then we say that b is divisor of a and that a is divisible by b.

If $d \mid a, d \mid b$ *and* $c \mid a \bigwedge c \mid b \Rightarrow c \mid d$, then d is greatest common divisor of a and‘ b denoted by gcd $\mid (a, b)$.

All these notions are meaningful also in any abelian monoid.

Let us recall that every

$$c \in Q_+ \text{ can be expressed as } c = \prod P^{V_p(c)} \tag{2.37}$$

$v_p(c) \in Z$,for each $p \in \rho$ and only finite number of them are non-zero.

$If v_p(c) \neq 0$ then p is prime factor of c.

Consider the set S of all sequence $(n_1, n_2, n_3, ..., n_p, ...)$,where the index runs through ρ,each $n_p \in Z$,and only a finite number of them are non-zero.

The mapping

$$f(c) = (v_2(c), v_3(c), ..., v_p(c), ...) \tag{2.38}$$

is an isomorphism from $(Q_+, .)$ onto (S,+) where addition is defined termwise Example. f(45) + $f(\frac{8}{25})$=$f(3^2 \times 5) + f(2^3 \times 5^{-2})$,for f(45), then we have the following $v_2(45) = 0, v_3(45) = 2, v_5(45) = 1, v_7(45) = 0, ..., = 0$ and similarly for $f(\frac{8}{25}), v_2(\frac{8}{25}) = 3, v_3(\frac{8}{25}) = 0, v_5(\frac{8}{25}) = -2, v_7(\frac{8}{25})$ =0 ,... =0 now we have

$$f(45) + f(\frac{8}{25}) = (0, 2, 1, 0, 0, ...) + (3, 0, -2, 0, 0, ...) = (3, 2, -1, 0, 0, ...) \tag{2.39}$$

Given $a, b \in Q_+$, we define their inner product being Euclidean inner product of vectors

$$f(a), f(b) :< a, b >=< f(a), f(b) >= \sum v_p(a)v_p(b), p \in \rho \tag{2.40}$$

Since finite number of summands are non-zero ,this sum is finite .
For example.

$$< 45, \frac{8}{25} >= 0.3 + 2.0 + 1(-2) + 0 + 0 + ...+ = -2 \tag{2.41}$$

Next we define $\mid c \mid$ by setting $v_p(\mid c \mid) =\mid v_p(c) \mid$ for all $p \in \rho$ or equivalently $\mid c \mid= f^{-1}(v_2(\mid c \mid), v_3(\mid c \mid), ...,)$.
For example if $c = \frac{40}{63} = 2^3 \times 3^{-2} \times 5^1 \times 7^{-1}$,then $\mid c \mid= 2^3 \times 3^2 \times 5^1 \times 7^1 =$ 2520.Letting $\perp_1$ be the same relation as the one defined by (7), now it can be characterized by

$$a \perp_1 b \Leftrightarrow < |a|, |b| >= 0 \tag{2.42}$$

and also the relation $\perp_2 in Q_+$, defined by

$$a \perp_2 b \Leftrightarrow < a, b >= 0 \tag{2.43}$$

is a perpendicularity.
We will introduce one more non-trivial perpendicularity using divisibility. For that purpose ,we first notice that the relation δ defined by

$$b \delta a \Leftrightarrow \forall p \in \rho : v_p(b) \leq v_p(a) \tag{2.44}$$

is a divisibility,

$$\underset{\delta}{\gcd}(a, b) = \prod p^{min(v_p(a), v_p(b))}, p \in \rho \tag{2.45}$$

Assume now that $m, n, u, v \in Z_+$ *so that* $\gcd(m,u) = \gcd(n,v)$=1.
An alternative expression for

$$a\delta b \Leftrightarrow \forall p \in \rho : v_p(b) \leq v_p(a) is \frac{n}{v}\delta\frac{m}{u} \Leftrightarrow n|m \bigwedge u|v \tag{2.46}$$

and that for

$$\gcd_{\delta}(a,b) = \prod p^{min(v_p(a),v_p(b))}, p \in \rho, gcd(\frac{m}{u},\frac{n}{v}) = \frac{\gcd(m,n)}{lcm(u,v)} \tag{2.47}$$

For example if $\frac{45}{14} = 2^{-1} \times 3^2 \times 5^2 \times 7^{-1}$ and $b = \frac{33}{100} = 2^{-2} \times 3^1 \times 5^{-2} \times 11^1$,then $\gcd_{\delta}(a,b) = 2^{-2} \times 3^1 \times 5^{-2} \times 7^{-1} = \frac{3}{700}$. Alternatively

$$\frac{\gcd(45,33)}{lcm(14,100)} = \frac{3}{700} \tag{2.48}$$

Since $\gcd_{\delta}(|\frac{m}{u}|, |\frac{n}{v}|) = \gcd(mu, nv)$ by(9) we have

$$a\perp_1 b \Leftrightarrow \gcd_{\delta}(|a|,|b|) = 1 \tag{2.49}$$

EUGENI AND RIZZI define divisibility in Q_+ by setting the relation γ so that

$$\frac{n}{v}\gamma\frac{m}{u} \Leftrightarrow n|m \bigwedge v|uT \tag{2.50}$$

hen $\gcd\gamma(a,b)$ always exists and unique and

$$\gcd\gamma(\frac{m}{u},\frac{n}{v}) = \frac{\gcd(m,n)}{\gcd(u,v)} \tag{2.51}$$

Example

$$gcd\gamma(\frac{45}{14},\frac{33}{100}) = \frac{\gcd(45,33)}{\gcd(14,100)} = \frac{3}{2} \tag{2.52}$$

We define now the corresponding perpendicularity by writing

$$a\perp_{ER} b \Leftrightarrow gcd\gamma(a,b) = 1 \Leftrightarrow \gcd(m,n) = \gcd(u,v) = 1 \tag{2.53}$$

Summing up ,we have at least three non-trivial perpendicularity inQ_+. Let us see how they relate to another .i). $\perp_1$ versus $\perp_2$ (i.e. $x\perp_1 y \Rightarrow x\perp_2 y$)

but the converse does not hold .
Example $6\perp_2 \frac{2}{3}$ but it is not true for $6\perp_1 \frac{2}{3}, < 6, \frac{2}{3} >= 0$,but $< |6|, |\frac{2}{3}| > \neq 0$
$\perp_1 versus \perp_{ER} \Rightarrow (i.e \perp_1 \Rightarrow \perp_{ER}) x \perp_1 y \Rightarrow x \perp_{ER} y$
Example. $< 7, \frac{2}{3} >= o$,the converse does not hold.
Example $\frac{2}{3} \perp_{ER} \frac{3}{2}$ but it does not imply that $\frac{2}{3} \perp_1 \frac{3}{2}$

2.5 *PARALLELISM*

Definition 2.5.1. *Let G has a perpendicularity $\perp$ and let $a, b \in G$.*
We say that a and b are parallel and write $a \parallel b$ if $\{a\}^\perp = \{b\}^\perp$.

The relation clearly equivalence.
Because
i.Since $\{a\}^\perp$=$\{a\}^\perp$,then $a \parallel a$.
ii.$a \parallel b \Rightarrow \{a\}^\perp = \{b\}^\perp$
$\Rightarrow \{b\}^\perp = \{a\}^\perp$
$\Rightarrow b \parallel a.$
Therefore $a \parallel b \Rightarrow b \parallel a$
iii.Let $a \parallel b$ *and* $b \parallel c \Rightarrow \{a\}^\perp = \{b\}^\perp$ and $\{b\}^\perp = \{c\}^\perp$
$\Rightarrow \{a\}^\perp$=$\{c\}^\perp$
$\Rightarrow a \parallel$ c
Therefore $a \parallel b$ *and* $b \parallel c \Rightarrow a \parallel$ c.
Let $G = Z_{30}$.
Since $\{\overline{2}\}^\perp = \{\overline{16}\}^\perp$
then$2 \parallel 16$

since $\{0\}^\perp = G$ by proposition1(a) but $\{a\}^\perp \neq G$ by (A2).
All non-zero elements are parallel if and only if $\perp$ is trivial. If $G = Z_n$ and $\perp = \perp_0$,then recalling (19).

$$x \parallel y \Leftrightarrow \forall i \in \{1, 2, 3, ...r\} : \xi_i = 0 \Leftrightarrow \eta_i = 0 \tag{2.54}$$

$\Leftrightarrow \{x\}^{\perp} = \{y\}^{\perp} = H_{i_1} \bigoplus H_{i_2} \bigoplus ... \bigoplus H_{i_t}$. Where $\xi_i = \eta_i = 0 \Leftrightarrow i \in \{i_1, i_2, i_3, ..., i_t\}$.

For example, consider Z_{30}. Since $\overline{2} = 0.\overline{1}+2.\overline{10}+2.\overline{6}$ *and* $\overline{16} = 0.\overline{15}+1.\overline{10}+1.\overline{6}$ we have $\{2\}^{\perp}$=$\{16\}^{\perp}$ =$\{\overline{0}, \overline{15}\} \Rightarrow 2 \parallel 16$.

Now,let $G = Q_+$ and let $\perp_1, \perp_2$ and $\perp_{ER}$ be as before denote the corresponding parallelism $\parallel_1$ *and* $\parallel_2$ and $\parallel_{ER}$ respectively .Then $a \parallel_1 b$ if and only if a and b have the same prime factors. Further$\frac{m}{u} \parallel_{ER} \frac{n}{v}$ if and only if m and n have the same prime factors ,similarly if u and v have the same prime factors.

Let study how these parallelisms related to one another $\parallel_1$ *versus* $\parallel_2$.

WTS $\parallel_2 \Rightarrow \parallel_1$

Proof. Assume first that is $a \parallel_2 b$ .If $a \nparallel_1 b$ then $\exists p_o \in \rho$ such that, say $v_{p_o}(a) = 0$ and $v_{p_o}(b) \neq 0$,but now $p_o \perp_2 a$ *and* $p_o \not\perp_2 b$ and so that $\{a\}^{\perp_2} \neq \{b\}^{\perp_2}$ that is contradicting our assumption (i.e $a \parallel_2 b \Rightarrow \{a\}^{\perp_2} = \{b\}^{\perp_2}$

Therefore $\parallel_2 \Rightarrow \parallel_1$

The converse is not true.Let see by using example.Let a=6 and b=12 then $a \parallel_1 b$.

If $x = \frac{2}{3}$ then $x \perp_2 a$ but x is not in b and hence$\{a\}^{\perp_2} \neq \{b\}^{\perp_2}$

In other words$a \nparallel_2 b(I.e < \frac{2}{3}, 6 >= 0$ *but* $< \frac{2}{3}, 12 > \neq 0$ □

ii). $\parallel_2$ *versus* $\parallel_{ER}$ (i.e. $\parallel_2 \Rightarrow \parallel_{ER}$).

Proof. Given $p_1, p_2, p_3, ..., p_t \in \rho$, denote by $N(p_1, p_2, p_3, ..., p_t)$ the set such positive integers that are not divisible by any p_i ,i=1,2,3,...t. Let $a = \frac{m}{u} \in Q_+, \gcd(m, u) = 1$. Now factorize

$$m = p_1^{\alpha_1}.p_2^{\alpha_2}...p_h^{\alpha_h}, u = q_1^{\beta_1}.q_2^{\beta_2}...q_k^{\beta_k} \tag{2.55}$$

where $p_1, p_2, p_3..., p_n, q_1, ..., q_k \in \rho$ are distinct and $\alpha_1, ..., \alpha_k, \beta_1, ..., \beta_n > 0$.(If m=1 or u=1 then the corresponding "empty product"is1).

Now

$$\{a\}^{\perp_2} = \{\frac{p_1^{\xi_1}.p_2^{\xi_2}...p_h^{\xi_h}}{q_1^{\eta_1}q_2^{\eta_2}...q_k^{\eta_k}}.\frac{x}{y} : \alpha_1\xi_1+...+\alpha_h\xi_h+\eta_1\beta_1+...+\beta_k\eta_k = 0x, y \in N(p_1,...,p_n,q_1,...,q_k)\} \tag{2.56}$$

("empty sum" is zero).Assume that $b = \frac{n}{v} \in Q_+$ and $\gcd(n, v) = 1$ satisfies $a \parallel_2 b$,that is $\{a\}^{\perp_2} = \{b\}^{\perp_2}$ .Then by (57), where

$$n = p_1^{\rho_1}p_2^{\rho_2}...p_h^{\rho_h}v = q_1^{\alpha_1}...q_k^{\alpha_k} \tag{2.57}$$

Where $\rho_1, ..., \rho_h, \alpha_1, ..., \alpha_k > 0$

Hence $a \parallel_{ER} b$ and the claim follows

But the converse is not hold . □

Example.$\frac{2}{3} \parallel_{ER} \frac{4}{3}$ but $\frac{2}{3} \nparallel_2 \frac{4}{3}$.

SUMMARY

This project shows the use of the symbol of perpendicularity in number theory.Indeed ,we have seen how this notion settle comfortably in this setting and gains new meanings at a more general level in the context of Abelian group.
And also we have seen the definition of perpendicularity using the five axioms,Divisibility in positive rational number with respect to perpendicularity.Finally we defined parallelism and we have seen the relation between perpendicularity and parallelism using examples.

Bibliography

[1] R.L.Graham D.E.knuth and O.Patashnik,Concrit Mathematics Afoudation for computer science (2nd edition), Addison -Wesley, USA(1994).

[2] W.K.Nicholson ,Introduction to Abstract Algebra, John Wiley and Sons,New York,USA,fourth edition 2012.

[3] G.Davis,Rings with orthogonalityrelations, Bulletin of Australian Mathematical Society.voi.pp.163-171, Australia, 1971

[4] F.Eugeni and B.Rizzi, An Incidence Algebra on Aational Number Rendiconti di Matematica ,vol.12,no.3-4,pp.557-576, 1979

[5] G.Birkhoff,Lattice Theory, American Mathematical society,Providence,RI,USA,3rd edition,1993

[6] Thomas W.Hungerford(Grauate text in Mathematics).

[7] Modern Algebra(Sujeet Singh)

[8] Abstract Algebra[Dover]