Quotients and Factorizations

Behnam Khosravi

IASBS

1402 Spring

Operation of numbers

Addition $+$: Latin word "Et" meaning "And".
$\sum$: Euler.

Subtraction $-$: May be derived from a tilde written over *m*; or it may come from a shorthand version of the letter *m* itself.

Multiplication $\times$ or $\cdot$ or $\prod$: Napier, Oughtred and ?, Leibniz, Gauss.

Division of numbers

Islamic Age → Fibonacci:

$$\frac{A}{B}$$

De Morgan:

$$A/B$$

Johann Heinrich Rahn:

$$\frac{\bullet}{\bullet} \longrightarrow \div$$

Leibniz:

$$A : B$$

Euclid and factorization of numbers

Euclid's lemma. If a prime p divides the product ab of two integers a and b, then p must divide at least one of those integers a or b.

Fundamental theorem of arithmetic. Every integer greater than 1 can be represented uniquely as a product of prime numbers, up to the order of the factors.

Euclid's theorem. There are infinitely many prime numbers.

What are building blocks in other structures?

How we can find building blocks?

If a prime number p divides a number n, then there exists $m \in \mathbb{N}$ such that

$$p = \frac{n}{m}.$$

There is **NO** number $m < m' < n$ such that

$$\frac{n}{m} = \frac{n}{m'} \times \frac{m'}{m}.$$

Simplest Factors

Factor?!!!

How we can find building blocks?

If a prime number p divides a number n, then there exists $m \in \mathbb{N}$ such that

$$p = \frac{n}{m}.$$

There is **NO** number $m < m' < n$ such that

$$\frac{n}{m} = \frac{n}{m'} \times \frac{m'}{m}.$$

Simplest Factors

Factor?!!!

How we can find building blocks?

If a prime number p divides a number n, then there exists $m \in \mathbb{N}$ such that

$$p = \frac{n}{m}.$$

There is **NO** number $m < m' < n$ such that

$$\frac{n}{m} = \frac{n}{m'} \times \frac{m'}{m}.$$

Simplest Factors

Factor?!!!

Congruences modulo m

If two integer numbers a and b have the property that their difference $a-b$ is integrally divisible by a number m (i.e., $(a-b)/m$ is an integer), then a and b are said to be "congruent modulo m" and we write $a \equiv b(\mod m)$.

Equivalence relation $a \sim b$ if and only if $a \equiv b$.

The equivalence class of a:

$$\overline{a} = \{n \in \mathbb{Z} \mid n \equiv a\}$$

$$\mathbb{Z}_m = \{\overline{a} \mid a \in \mathbb{Z}\}$$

Congruences modulo m

Properties: If $a \equiv a'$ and $b \equiv b'$ mod m, then

(1) $a + b \equiv a' + b'$; $\rightarrow \overline{a} + \overline{b} = \overline{a+b}$ is well-defined;

(2) $-a \equiv -a'$; $\rightarrow -\overline{a} = \overline{-a}$ is well-defined;

(3) $a - b \equiv a' - b'$.

(4) $ab \equiv a'b' \rightarrow \overline{a} \cdot \overline{b} = \overline{ab}$ is well-defined.

$(\mathbb{Z}_m, +)$ is a group;
$(\mathbb{Z}_m, \cdot)$ is a monoid,
$(\mathbb{Z}_m, +, \cdot)$ is a ring with identity $\overline{1}$.

Congruences modulo m

Properties: If $a \equiv a'$ and $b \equiv b'$ mod m, then

(1) $a + b \equiv a' + b'$; $\rightarrow \overline{a} + \overline{b} = \overline{a+b}$ is well-defined;

(2) $-a \equiv -a'$; $\rightarrow -\overline{a} = \overline{-a}$ is well-defined;

(3) $a - b \equiv a' - b'$.

(4) $ab \equiv a'b' \rightarrow \overline{a} \cdot \overline{b} = \overline{ab}$ is well-defined.

$(\mathbb{Z}_m, +)$ is a group;
$(\mathbb{Z}_m, \cdot)$ is a monoid,
$(\mathbb{Z}_m, +, \cdot)$ is a ring with identity $\overline{1}$.

Congruences modulo m

Properties: If $a \equiv a'$ and $b \equiv b'$ mod m, then

(1) $a + b \equiv a' + b'$; $\rightarrow \overline{a} + \overline{b} = \overline{a+b}$ is well-defined;

(2) $-a \equiv -a'$; $\rightarrow -\overline{a} = \overline{-a}$ is well-defined;

(3) $a - b \equiv a' - b'$.

(4) $ab \equiv a'b'$ $\rightarrow \overline{a} \cdot \overline{b} = \overline{ab}$ is well-defined.

$(\mathbb{Z}_m, +)$ is a group;
$(\mathbb{Z}_m, \cdot)$ is a monoid,
$(\mathbb{Z}_m, +, \cdot)$ is a ring with identity $\overline{1}$.

Congruences modulo m

Properties: If $a \equiv a'$ and $b \equiv b'$ mod m, then

(1) $a + b \equiv a' + b'$; $\rightarrow \overline{a} + \overline{b} = \overline{a+b}$ is well-defined;

(2) $-a \equiv -a'$; $\rightarrow -\overline{a} = \overline{-a}$ is well-defined;

(3) $a - b \equiv a' - b'$.

(4) $ab \equiv a'b'$ $\rightarrow \overline{a} \cdot \overline{b} = \overline{ab}$ is well-defined.

$(\mathbb{Z}_m, +)$ is a group;
$(\mathbb{Z}_m, \cdot)$ is a monoid,
$(\mathbb{Z}_m, +, \cdot)$ is a ring with identity $\overline{1}$.

Congruences modulo m

Properties: If $a \equiv a'$ and $b \equiv b'$ mod m, then

(1) $a + b \equiv a' + b'$;$\to$ $\overline{a} + \overline{b} = \overline{a+b}$ is well-defined;

(2) $-a \equiv -a'$;$\to$ $-\overline{a} = \overline{-a}$ is well-defined;

(3) $a - b \equiv a' - b'$.

(4) $ab \equiv a'b'$$\to$ $\overline{a} \cdot \overline{b} = \overline{ab}$ is well-defined.

$(\mathbb{Z}_m, +)$ is a group;
$(\mathbb{Z}_m, \cdot)$ is a monoid,
$(\mathbb{Z}_m, +, \cdot)$ is a ring with identity $\overline{1}$.

Congruences modulo m

Properties: If $a \equiv a'$ and $b \equiv b'$ mod m, then

(1) $a + b \equiv a' + b'; \to \overline{a} + \overline{b} = \overline{a + b}$ is well-defined;

(2) $-a \equiv -a'; \to -\overline{a} = \overline{-a}$ is well-defined;

(3) $a - b \equiv a' - b'$.

(4) $ab \equiv a'b' \to \overline{a} \cdot \overline{b} = \overline{ab}$ is well-defined.

$(\mathbb{Z}_m, +)$ is a group;
$(\mathbb{Z}_m, \cdot)$ is a monoid,
$(\mathbb{Z}_m, +, \cdot)$ is a ring with identity $\overline{1}$.

Congruences modulo m

Properties: If $a \equiv a'$ and $b \equiv b'$ mod m, then

(1) $a + b \equiv a' + b'; \to \overline{a} + \overline{b} = \overline{a+b}$ is well-defined;

(2) $-a \equiv -a'; \to -\overline{a} = \overline{-a}$ is well-defined;

(3) $a - b \equiv a' - b'$.

(4) $ab \equiv a'b' \to \overline{a} \cdot \overline{b} = \overline{ab}$ is well-defined.

$(\mathbb{Z}_m, +)$ is a group;
$(\mathbb{Z}_m, \cdot)$ is a monoid,
$(\mathbb{Z}_m, +, \cdot)$ is a ring with identity $\overline{1}$.

Congruences modulo m

Properties: If $a \equiv a'$ and $b \equiv b'$ mod m, then

(1) $a + b \equiv a' + b'$;$\rightarrow \overline{a} + \overline{b} = \overline{a+b}$ is well-defined;

(2) $-a \equiv -a'$;$\rightarrow -\overline{a} = \overline{-a}$ is well-defined;

(3) $a - b \equiv a' - b'$.

(4) $ab \equiv a'b' \rightarrow \overline{a} \cdot \overline{b} = \overline{ab}$ is well-defined.

$(\mathbb{Z}_m, +)$ is a group;

$(\mathbb{Z}_m, \cdot)$ is a monoid,

$(\mathbb{Z}_m, +, \cdot)$ is a ring with identity $\overline{1}$.

Congruences modulo m

Properties: If $a \equiv a'$ and $b \equiv b'$ mod m, then

(1) $a + b \equiv a' + b'$;$\rightarrow \overline{a} + \overline{b} = \overline{a + b}$ is well-defined;

(2) $-a \equiv -a'$;$\rightarrow -\overline{a} = \overline{-a}$ is well-defined;

(3) $a - b \equiv a' - b'$.

(4) $ab \equiv a'b' \rightarrow \overline{a} \cdot \overline{b} = \overline{ab}$ is well-defined.

$(\mathbb{Z}_m, +)$ is a group;
$(\mathbb{Z}_m, \cdot)$ is a monoid,
$(\mathbb{Z}_m, +, \cdot)$ is a ring with identity $\overline{1}$.

CONGRUENCES MODULO m

Properties: If $a \equiv a'$ and $b \equiv b'$ mod m, then

(1) $a + b \equiv a' + b'$;$\rightarrow$ $\overline{a} + \overline{b} = \overline{a + b}$ is well-defined;

(2) $-a \equiv -a'$;$\rightarrow$ $-\overline{a} = \overline{-a}$ is well-defined;

(3) $a - b \equiv a' - b'$.

(4) $ab \equiv a'b'$$\rightarrow$ $\overline{a} \cdot \overline{b} = \overline{ab}$ is well-defined.

$(\mathbb{Z}_m, +)$ is a group;
$(\mathbb{Z}_m, \cdot)$ is a monoid,
$(\mathbb{Z}_m, +, \cdot)$ is a ring with identity $\overline{1}$.

Is it true for every equivalence relation on $\mathbb{Z}$?

Let the relation ρ be defined by

$\rho = \{(a, b) \in \mathbb{Z}\times\mathbb{Z} \mid \text{both } a \text{ and } b \text{ are odd}\}\cup\{(a, a) \mid a \in \mathbb{Z}\}$.

$$[1]_\rho + [1]_\rho = \{2, 4, 6, \cdots\};$$

$$[1 + 1]_\rho = [2]_\rho = \{2\}.$$

No!

Is it true for every equivalence relation on $\mathbb{Z}$?

Let the relation ρ be defined by

$\rho = \{(a, b) \in \mathbb{Z}\times\mathbb{Z} \mid \text{both } a \text{ and } b \text{ are odd}\}\cup\{(a, a) \mid a \in \mathbb{Z}\}$.

$$[1]_\rho + [1]_\rho = \{2, 4, 6, \cdots\};$$

$$[1 + 1]_\rho = [2]_\rho = \{2\}.$$

No!

Is it true for every equivalence relation on $\mathbb{Z}$?

Let the relation ρ be defined by

$\rho = \{(a, b) \in \mathbb{Z}\times\mathbb{Z} \mid \text{both } a \text{ and } b \text{ are odd}\}\cup\{(a, a) \mid a \in \mathbb{Z}\}.$

$$[1]_\rho + [1]_\rho = \{2, 4, 6, \cdots\};$$

$$[1 + 1]_\rho = [2]_\rho = \{2\}.$$

No!

For which equivalence relation on $\mathbb{Z}$ we have this property?

For the equivalence relation ρ,

1. if the operation $[a]_\rho + [b]_\rho = [a+b]_\rho$ is well-defined, then $[0]_\rho$ is a subsemigroup of $(\mathbb{Z}, +)$ because $[a+b]_\rho = [0+0]_\rho = [0]_\rho$ for every $a, b \in [0]_\rho$;
2. if the operation $-[a]_\rho = [-a]_\rho$ is well-defined too, then $[0]_\rho$ is a subgroup of $(\mathbb{Z}, +)$;

$$a\rho b \Leftrightarrow \quad 0 = (a-a)\rho(b-a) \Leftrightarrow \quad b-a \in [0]_\rho$$

For which equivalence relation on $\mathbb{Z}$ we have this property?

For the equivalence relation ρ,

1. if the operation $[a]_\rho + [b]_\rho = [a+b]_\rho$ is well-defined, then $[0]_\rho$ is a subsemigroup of $(\mathbb{Z}, +)$ because $[a+b]_\rho = [0+0]_\rho = [0]_\rho$ for every $a, b \in [0]_\rho$;
2. if the operation $-[a]_\rho = [-a]_\rho$ is well-defined too, then $[0]_\rho$ is a subgroup of $(\mathbb{Z}, +)$;

$$a\rho b \Leftrightarrow \quad 0 = (a-a)\rho(b-a) \Leftrightarrow \quad b-a \in [0]_\rho$$

For which equivalence relation on $\mathbb{Z}$ we have this property?

For the equivalence relation ρ,

1. if the operation $[a]_\rho + [b]_\rho = [a+b]_\rho$ is well-defined, then $[0]_\rho$ is a subsemigroup of $(\mathbb{Z}, +)$ because $[a+b]_\rho = [0+0]_\rho = [0]_\rho$ for every $a, b \in [0]_\rho$;
2. if the operation $-[a]_\rho = [-a]_\rho$ is well-defined too, then $[0]_\rho$ is a subgroup of $(\mathbb{Z}, +)$;

$$a\rho b \Leftrightarrow \quad 0 = (a-a)\rho(b-a) \Leftrightarrow \quad b-a \in [0]_\rho$$

Subgroups and well-behaviour equivalence relations

For the equivalence relation ρ on $\mathbb{Z}$, $\mathbb{Z}/\rho = \{[n]_\rho \mid n \in \mathbb{Z}\}$ with the addition defined by $[a]_\rho + [b]_\rho = [a+b]_\rho$ is a group if and only if $[0]_\rho$ is a subgroup of $\mathbb{Z}$.

How about an arbitrary group?

Subgroups and well-behaviour equivalence relations

For the equivalence relation ρ on $\mathbb{Z}$, $\mathbb{Z}/\rho = \{[n]_\rho \mid n \in \mathbb{Z}\}$ with the addition defined by $[a]_\rho + [b]_\rho = [a+b]_\rho$ is a group if and only if $[0]_\rho$ is a subgroup of $\mathbb{Z}$.

How about an arbitrary group?

For which equivalence relation on $\mathbb{Z}$ we have this property?

1. if the operation $[a]_\rho \cdot [b]_\rho = [ab]_\rho$ is well-defined, then $[0]_\rho$ is a subsemigroup of $(\mathbb{Z}, \cdot)$ because $[a \cdot b] = [0 \cdot 0] = [0]$ for every $a, b \in [0]$.
2. if the operation $[a]_\rho \cdot [b]_\rho = [ab]_\rho$ is well-defined too, then $[0]_\rho$ is a subring of $(\mathbb{Z}, +, \cdot)$.

Remember quotients of rings!

For which equivalence relation on $\mathbb{Z}$ we have this property?

1. if the operation $[a]_\rho \cdot [b]_\rho = [ab]_\rho$ is well-defined, then $[0]_\rho$ is a subsemigroup of $(\mathbb{Z}, \cdot)$ because $[a \cdot b] = [0 \cdot 0] = [0]$ for every $a, b \in [0]$.
2. if the operation $[a]_\rho \cdot [b]_\rho = [ab]_\rho$ is well-defined too, then $[0]_\rho$ is a subring of $(\mathbb{Z}, +, \cdot)$.

Remember quotients of rings!

For which equivalence relation on $\mathbb{Z}$ we have this property?

1. if the operation $[a]_\rho \cdot [b]_\rho = [ab]_\rho$ is well-defined, then $[0]_\rho$ is a subsemigroup of $(\mathbb{Z}, \cdot)$ because $[a \cdot b] = [0 \cdot 0] = [0]$ for every $a, b \in [0]$.
2. if the operation $[a]_\rho \cdot [b]_\rho = [ab]_\rho$ is well-defined too, then $[0]_\rho$ is a subring of $(\mathbb{Z}, +, \cdot)$.

Remember quotients of rings!

Arbitrary group

For a group G and an equivalence relation ρ on it such that G/ρ is a group we have $H = [1]_\rho \leq G$ and $a\rho b$ if and only if $aH = bH$.

Furthermore, for every $g \in G$ we have

$$H^g = gHg^{-1} = g\{x \in G \mid x\rho 1\}g^{-1} = \{gxg^{-1} \mid x\rho 1\}.$$

Since $[gxg^{-1}]_\rho = [g]_\rho[x]_\rho[g^{-1}]_\rho = [g]_\rho[1]_\rho[g^{-1}]_\rho = [1]_\rho$,
H is a normal subgroup of G!

Arbitrary ring

For a ring R and an equivalence relation ρ on it such that R/ρ is a ring we have $I = [0]_\rho \leq R$ and $a\rho b$ if and only if $a + I = b + I$.

Furthermore, for every $r \in R$ we have

$$rI = r[0]_\rho = \{rx \mid x\rho 0\} \text{ and } Ir = \{xr \mid x\rho 0\}.$$

Since $[rx]_\rho = [r]_\rho [x]_\rho = [r]_\rho [0]_\rho = [0]_\rho$,
I is an ideal of R!

How about other algebraic structures?

Modules or vector spaces. For an R-module M and an equivalence relation ρ on it such that M/ρ is an R-module with the following operations

$$[a]_\rho + [b]_\rho = [a+b]_\rho \text{ and } r[a]_\rho = [ra]_\rho.$$

Since $[ra]_\rho = r[a]_\rho = r[0]_\rho = [0]_\rho$,
the class $[0]_\rho$ is a submodule of M!

Congruences

Roughly speaking, for every algebraic structure A, an equivalence relation ρ on A is called a congruence if natural operations on the set of equivalence classes of A are well-behaviour (e.g. if A is a group (ring), then A/ρ is a group (ring) with natural operations).

Groups	$\rightarrow$	Normal subgroups
Rings	$\rightarrow$	Ideals
R-modules	$\rightarrow$	Submodules
Vector Spaces	$\rightarrow$	Subspaces
	?	

Is there always a bijection between congruences and a collection of subalgebras?

Semigroups. For $(\mathbb{N}, +)$, the equivalence relation $\Delta = \{(n, n) \mid n \in \mathbb{N}\}$ is a congruence and every equivalence class of Δ is not a subsemigroup.

Therefore the answer is **NO!**

Rees Congruence on semigroups

Let I be a subset of a semigroup S such that $SI, IS \subseteq I$. Then the relation ρ_I defined by $\{(s,s) \mid s \in S\} \cup \{(a,a') \mid a, a' \in I\}$ is a congruence.

Example. For $(\mathbb{N} \cup \{0\}, \cdot)$ we have $\{(n,n) \mid n \in \mathbb{N} \cup \{0\}\} = \rho_{\{0\}}$.

Quotients and factorizations

Recall that in the group $\mathbb{Z}_6$ the subgroups $2\mathbb{Z}_6$ and $3\mathbb{Z}_6$ have trivial intersection and $\mathbb{Z}_6 = 2\mathbb{Z}_6 + 3\mathbb{Z}_6$ and in fact

$$\mathbb{Z}_6 \cong \frac{\mathbb{Z}_6}{2\mathbb{Z}_6} \times \frac{\mathbb{Z}_6}{3\mathbb{Z}_6}.$$

For an arbitrary group G, let $N_1, N_2 \lhd G$ such that the following conditions hold.

(I) $N_1 \cap N_2 = \{1\}$;

(II) $G = N_1 N_2 (= N_2 N_1)$ (**uniqueness:** $n = n_1 n_2$).

Then

$$G \cong \frac{G}{N_1} \times \frac{G}{N_2}.$$

Quotients and factorizations

Recall that in the group $\mathbb{Z}_6$ the subgroups $2\mathbb{Z}_6$ and $3\mathbb{Z}_6$ have trivial intersection and $\mathbb{Z}_6 = 2\mathbb{Z}_6 + 3\mathbb{Z}_6$ and in fact

$$\mathbb{Z}_6 \cong \frac{\mathbb{Z}_6}{2\mathbb{Z}_6} \times \frac{\mathbb{Z}_6}{3\mathbb{Z}_6}.$$

For an arbitrary group G, let $N_1, N_2 \lhd G$ such that the following conditions hold.

(I) $N_1 \cap N_2 = \{1\}$;

(II) $G = N_1 N_2 (= N_2 N_1)$ (**uniqueness:** $n = n_1 n_2$).

Then

$$G \cong \frac{G}{N_1} \times \frac{G}{N_2}.$$

Quotients and factorizations

Indecomposable groups Groups without any pair of non-trivial normal subgroups which satisfies the conditions at the above.

Example. $\mathbb{Z}_8$ (in general, every abelian group of order p^n for some prime number p)

Krull-Schmidt theorem. Every finite group can be uniquely written as a finite direct product of indecomposable subgroups.

The fundamental theorem of finite abelian groups. Every finite abelian group can be expressed as the direct sum of cyclic subgroups of prime-power order.

Quotients and factorizations

Indecomposable groups Groups without any pair of non-trivial normal subgroups which satisfies the conditions at the above.

Example. $\mathbb{Z}_8$ (in general, every abelian group of order p^n for some prime number p)

Krull-Schmidt theorem. Every finite group can be uniquely written as a finite direct product of indecomposable subgroups.

The fundamental theorem of finite abelian groups. Every finite abelian group can be expressed as the direct sum of cyclic subgroups of prime-power order.

Quotients and factorizations

Indecomposable groups Groups without any pair of non-trivial normal subgroups which satisfies the conditions at the above.

Example. $\mathbb{Z}_8$ (in general, every abelian group of order p^n for some prime number p)

Krull-Schmidt theorem. Every finite group can be uniquely written as a finite direct product of indecomposable subgroups.

The fundamental theorem of finite abelian groups. Every finite abelian group can be expressed as the direct sum of cyclic subgroups of prime-power order.

How they are useful?

$$\begin{aligned}\text{Natural numbers} &\rightarrow \text{prime numbers}\\ \text{Finite groups} &\rightarrow \text{indecomposable finite groups}\end{aligned}$$

What are abelian groups of order less than 100 which have an element of order 5 and an element of order 7?

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_m^{n_m}}$$

Just $\mathbb{Z}_5 \times \mathbb{Z}_7 \cong \mathbb{Z}_{35}$ and $\mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \cong \mathbb{Z}_{70}$

How they are useful?

$$\text{Natural numbers} \rightarrow \text{prime numbers}$$
$$\text{Finite groups} \rightarrow \text{indecomposable finite groups}$$

What are abelian groups of order less than 100 which have an element of order 5 and an element of order 7?

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_m^{n_m}}$$

Just $\mathbb{Z}_5 \times \mathbb{Z}_7 \cong \mathbb{Z}_{35}$ and $\mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \cong \mathbb{Z}_{70}$

How they are useful?

$$\begin{aligned} \text{Natural numbers} &\rightarrow \text{prime numbers} \\ \text{Finite groups} &\rightarrow \text{indecomposable finite groups} \end{aligned}$$

What are abelian groups of order less than 100 which have an element of order 5 and an element of order 7?

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_m^{n_m}}$$

Just $\mathbb{Z}_5 \times \mathbb{Z}_7 \cong \mathbb{Z}_{35}$ and $\mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \cong \mathbb{Z}_{70}$

How they are useful?

$$\begin{aligned} \text{Natural numbers} &\to \text{prime numbers} \\ \text{Finite groups} &\to \text{indecomposable finite groups} \end{aligned}$$

What are abelian groups of order less than 100 which have an element of order 5 and an element of order 7?

$$\mathbb{Z}_n \cong \mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_m^{n_m}}$$

Just $\mathbb{Z}_5 \times \mathbb{Z}_7 \cong \mathbb{Z}_{35}$ and $\mathbb{Z}_2 \times \mathbb{Z}_5 \times \mathbb{Z}_7 \cong \mathbb{Z}_{70}$

Other algebraic structures?

If $G \cong \frac{G}{N_1} \times \frac{G}{N_2}$ under the map $\phi(g) = (g_{N_1}, g_{N_2})$, then for every $x, y \in G$, there exists $z \in G$ such that $\phi(z) = (xN_1, yN_2)$ and specially,

$$xN_1 \cap yN_2 \neq \emptyset.$$

For every algebraic structure A let ρ_1 and ρ_2 be two congruences on A such that

(I) $\rho_1 \cap \rho_2 = \Delta = \{(a, a) \mid a \in A\}$;

(II) for every $x, y \in A$ there exist $z, z' \in A$ such that

$(x, z) \in \rho_1$ and $(z, y) \in \rho_2$; and
$(x, z') \in \rho_2$ and $(z', y) \in \rho_1$.

a pair of factor congruences

Other algebraic structures?

If $G \cong \frac{G}{N_1} \times \frac{G}{N_2}$ under the map $\phi(g) = (g_{N_1}, g_{N_2})$, then for every $x, y \in G$, there exists $z \in G$ such that $\phi(z) = (xN_1, yN_2)$ and specially,

$$xN_1 \cap yN_2 \neq \emptyset.$$

For every algebraic structure A let ρ_1 and ρ_2 be two congruences on A such that

(I) $\rho_1 \cap \rho_2 = \Delta = \{(a, a) \mid a \in A\}$;

(II) for every $x, y \in A$ there exist $z, z' \in A$ such that

$(x, z) \in \rho_1$ and $(z, y) \in \rho_2$; and
$(x, z') \in \rho_2$ and $(z', y) \in \rho_1$.

a pair of factor congruences

Other algebraic structures?

If $G \cong \frac{G}{N_1} \times \frac{G}{N_2}$ under the map $\phi(g) = (g_{N_1}, g_{N_2})$, then for every $x, y \in G$, there exists $z \in G$ such that $\phi(z) = (xN_1, yN_2)$ and specially,

$$xN_1 \cap yN_2 \neq \emptyset.$$

For every algebraic structure A let ρ_1 and ρ_2 be two congruences on A such that

(I) $\rho_1 \cap \rho_2 = \Delta = \{(a, a) \mid a \in A\}$;

(II) for every $x, y \in A$ there exist $z, z' \in A$ such that
$(x, z) \in \rho_1$ and $(z, y) \in \rho_2$; and
$(x, z') \in \rho_2$ and $(z', y) \in \rho_1$.

a pair of factor congruences

Other algebraic structures?

If $G \cong \frac{G}{N_1} \times \frac{G}{N_2}$ under the map $\phi(g) = (g_{N_1}, g_{N_2})$, then for every $x, y \in G$, there exists $z \in G$ such that $\phi(z) = (xN_1, yN_2)$ and specially,

$$xN_1 \cap yN_2 \neq \emptyset.$$

For every algebraic structure A let ρ_1 and ρ_2 be two congruences on A such that

(I) $\rho_1 \cap \rho_2 = \Delta = \{(a, a) \mid a \in A\}$;

(II) for every $x, y \in A$ there exist $z, z' \in A$ such that
$(x, z) \in \rho_1$ and $(z, y) \in \rho_2$; and
$(x, z') \in \rho_2$ and $(z', y) \in \rho_1$.

a pair of factor congruences

Quotients and factorizations of finite algebras

An algebra A is (directly) indecomposable if A is not isomorphic to a direct product of two nontrivial algebras (equivalently, A has no pair of factor congruences $\rho_1, \rho_2 \neq \Delta$).

Theorem. Every finite algebra is isomorphic to a direct product of directly indecomposable algebras.

S. Burris, and H. P. Sankappanavar, A Course in Universal Algebra, Springer New York, 2011.

Other structures?

For every structure A let ρ_1 and ρ_2 be two compatible equivalence relation on A such that

(I) $\rho_1 \cap \rho_2 = \Delta = \{(a, a) \mid a \in A\}$;

(II) for every $x, y \in A$ there exist $z, z' \in A$ such that
$(x, z) \in \rho_1$ and $(z, y) \in \rho_2$; and
$(x, z') \in \rho_2$ and $(z', y) \in \rho_1$.

Quotients and factorizations of ordered structures

Order on Quotients Given a poset $(P, \leq)$ and an equivalence relation ρ, let $[p] \leq [q]$ if and only if there exists $p' \in [p]$ and $q' \in [q]$ such that $p' \leq q'$.
An equivalence ρ on P is called compatible if P/ρ is a poset.
$(\mathbb{Z}, \leq)$?

Nicholas J. Williams, A survey of congruences and quotients of partially ordered sets, arXiv:2303.03765.

Quotients and factorizations of ordered structures

Order on Quotients Given a poset $(P, \leq)$ and an equivalence relation ρ, let $[p] \leq [q]$ if and only if there exists $p' \in [p]$ and $q' \in [q]$ such that $p' \leq q'$.
An equivalence ρ on P is called compatible if P/ρ is a poset.
$(\mathbb{Z}, \leq)$?

Nicholas J. Williams, A survey of congruences and quotients of partially ordered sets, arXiv:2303.03765.

Quotients and factorizations of ordered structures

Order on Quotients Given a poset $(P, \leq)$ and an equivalence relation ρ, let $[p] \leq [q]$ if and only if there exists $p' \in [p]$ and $q' \in [q]$ such that $p' \leq q'$.
An equivalence ρ on P is called compatible if P/ρ is a poset.
$(\mathbb{Z}, \leq)$?

Nicholas J. Williams, A survey of congruences and quotients of partially ordered sets, arXiv:2303.03765.

Quotients and factorizations of ordered group or ordered semigroup

Let S be a set endowed with a law of composition that is written multiplicatively. By a compatible order on S we mean an order $\leq$ with respect to which all translations $y \to xy$ and $y \to yx$ are isotone.

Example. By an ordered group we shall mean a group on which there is defined a compatible order. $(\mathbb{Z}, +, \leq)$?

T.S. Blyth, Lattices and Ordered Algebraic Structures, Springer-Verlag London Limited 2005.

Quotients and factorizations of ordered group or ordered semigroup

Let S be a set endowed with a law of composition that is written multiplicatively. By a compatible order on S we mean an order $\leq$ with respect to which all translations $y \to xy$ and $y \to yx$ are isotone.

Example. By an ordered group we shall mean a group on which there is defined a compatible order. $(\mathbb{Z}, +, \leq)$?

T.S. Blyth, Lattices and Ordered Algebraic Structures, Springer-Verlag London Limited 2005.

Quotients and factorizations of ordered group or ordered semigroup

Let S be a set endowed with a law of composition that is written multiplicatively. By a compatible order on S we mean an order $\leq$ with respect to which all translations $y \to xy$ and $y \to yx$ are isotone.
Example. By an ordered group we shall mean a group on which there is defined a compatible order. $(\mathbb{Z}, +, \leq)$?

T.S. Blyth, Lattices and Ordered Algebraic Structures, Springer-Verlag London Limited 2005.

Quotients and factorizations of directed graphs

Remark. The definition of the quotient also applies to arbitrary relations and directed graphs.

Quotient of a directed graph Given a directed graph $\Gamma = (V, E)$ and an equivalence relation ρ, let $([p], [q]) \in \tilde{E}$ if and only if there exists $p' \in [p]$ and $q' \in [q]$ such that $(p', q') \in E$.

W. Imrich, and S. Klavzar, Product graphs:structure and recognition, Wiley, 2000.

Quotients and factorizations of directed graphs

Remark. The definition of the quotient also applies to arbitrary relations and directed graphs.

Quotient of a directed graph Given a directed graph $\Gamma = (V, E)$ and an equivalence relation ρ, let $([p], [q]) \in \tilde{E}$ if and only if there exists $p' \in [p]$ and $q' \in [q]$ such that $(p', q') \in E$.

W. Imrich, and S. Klavzar, Product graphs:structure and recognition, Wiley, 2000.

Quotients and factorizations of topological structures

A topological space X and an equivalence relation ρ

Quotient topology induced by the natural projection $\pi : X \to X/\rho$.

Quotient space

Hausdorff spaces???

Fatorization? $X = X_1 \times X_2$ and $\pi_i : X \to X_i$

$$\emptyset \subset \{(1,1)\} \subset \{(1,1),(1,2)\} \subset \{(1,1),(1,2),(2,1)\} \subset \{(1,1),(1,2),(2,1),(2,2)\}$$

Quotients and factorizations of topological structures

A topological space X and an equivalence relation ρ

Quotient topology induced by the natural projection $\pi : X \to X/\rho$.

Quotient space

Hausdorff spaces???

Fatorization? $X = X_1 \times X_2$ and $\pi_i : X \to X_i$

$$\emptyset \subset \{(1,1)\} \subset \{(1,1),(1,2)\} \subset \{(1,1),(1,2),(2,1)\} \subset \{(1,1),(1,2),(2,1),(2,2)\}$$

Quotients and factorizations of topological structures

A topological space X and an equivalence relation ρ

Quotient topology induced by the natural projection $\pi : X \to X/\rho$.

Quotient space

Hausdorff spaces???

Fatorization? $X = X_1 \times X_2$ and $\pi_i : X \to X_i$

$$\emptyset \subset \{(1,1)\} \subset \{(1,1),(1,2)\} \subset \{(1,1),(1,2),(2,1)\} \subset \{(1,1),(1,2),(2,1),(2,2)\}$$

Quotients and factorizations of topological structures

A topological space X and an equivalence relation ρ

Quotient topology induced by the natural projection $\pi : X \to X/\rho$.

Quotient space

Hausdorff spaces???

Fatorization? $X = X_1 \times X_2$ and $\pi_i : X \to X_i$

$$\emptyset \subset \{(1,1)\} \subset \{(1,1),(1,2)\} \subset \{(1,1),(1,2),(2,1)\} \subset \{(1,1),(1,2),(2,1),(2,2)\}$$

Quotients and factorizations of topological structures

A topological space X and an equivalence relation ρ

Quotient topology induced by the natural projection $\pi : X \to X/\rho$.

Quotient space

Hausdorff spaces???

Fatorization? $X = X_1 \times X_2$ and $\pi_i : X \to X_i$

$$\emptyset \subset \{(1,1)\} \subset \{(1,1),(1,2)\} \subset \{(1,1),(1,2),(2,1)\} \subset \{(1,1),(1,2),(2,1),(2,2)\}$$

Algebraic topological structures and topological congruences?

Topological semigroup: A semigroup S with a topology on it is called a topological semigroup if its multiplication is continuous.

Topological congruence

Wallace A. D., On the structure of topological semigroups, Bull. Amer. Math. Soc., 61 (1955),95-112.

Lawson, J. D. and Madison, B., On congruences and cones, Math. Z., 120 (1971), 18-24.

Quotients and factorizations of algebraic topological structures

Algebraic topological structures and topological congruences?

Topological semigroup: A semigroup S with a topology on it is called a topological semigroup if its multiplication is continuous.

Topological congruence

Wallace A. D., On the structure of topological semigroups, Bull. Amer. Math. Soc., 61 (1955),95-112.
Lawson, J. D. and Madison, B., On congruences and cones, Math. Z., 120 (1971), 18-24.

Quotients and factorizations of algebraic topological structures

Algebraic topological structures and topological congruences?

Topological semigroup: A semigroup S with a topology on it is called a topological semigroup if its multiplication is continuous.

Topological congruence

Wallace A. D., On the structure of topological semigroups, Bull. Amer. Math. Soc., 61 (1955),95-112.
Lawson, J. D. and Madison, B., On congruences and cones, Math. Z., 120 (1971), 18-24.

Quotients and factorizations of normal edge-transitive Cayley graphs

Praeger determined quotients of normal edge-transitive Cayley graphs which are again normal edge-transitive Cayley graphs.

C. E. Praeger, Finite Normal Edge-transitive Cayley graphs, Bull. Austral. Math. Soc. 60 (1999), 207-220.

Factorization?

B. Khosravi, B. Khosravi, and B. Khosravi, On reconstruction of normal edge-transitive Cayley graphs, Annals of Combinatorics, 24 (2020), 791–807.

B. Khosravi, and C. E. Praeger, Normal edge-transitive Cayley graphs and Frattini-like subgroups, Journal of Algebra, 607 (2022) 473-498.

Quotients and factorizations of normal edge-transitive Cayley graphs

Praeger determined quotients of normal edge-transitive Cayley graphs which are again normal edge-transitive Cayley graphs.

C. E. Praeger, Finite Normal Edge-transitive Cayley graphs, Bull. Austral. Math. Soc. 60 (1999), 207-220.

Factorization?

B. Khosravi, B. Khosravi, and B. Khosravi, On reconstruction of normal edge-transitive Cayley graphs, Annals of Combinatorics, 24 (2020), 791–807.

B. Khosravi, and C. E. Praeger, Normal edge-transitive Cayley graphs and Frattini-like subgroups, Journal of Algebra, 607 (2022) 473-498.

Thanks for your attention

https://www.karnaval.ir/blog/chichen-itza-pyramid-maya-civilization