MATH 300: CHAPTER 6- EQUIVALENCE RELATIONS

TOM BENHAMOU
RUTGERS UNIVERSITY

As we have seen previously, sets are equal if and only if they have the same elements. This is a quite rigid equality. There are mathematical theories where it is convenient to identify between two objects although they are not equal as sets, we say that they are *equivalent*. For example, to define a rational numbers $\frac{n}{m}$ from the integers, it is natural to identify it with the pair $\langle n, m\rangle$. However, note that while $\frac{1}{2} = \frac{2}{4}$, the pairs $\langle 1, 2\rangle, \langle 2, 4\rangle$ are distinct. What we usually do, is to set some criterion to determine when two objects are equivalent. Formally, this would mean that we have some relation R on a set A, and two members $a, b \in A$ will be equivalent if aRb. In our example of rationals, we would need to find a criterion which makes $\langle 1, 2\rangle, \langle 2, 4\rangle$ equivalent for examples, and not only them, but also $\langle 4, 2\rangle, \langle 8, 2\rangle$ and $\langle -1, 9\rangle, \langle 2, -18\rangle$ and so on.

Example 0.1. To find the right criteria for the rations, we need to express the equality $\frac{a}{b} = \frac{c}{d}$ in terms of integers, so let simply cross-multiply the equation and get $ad = bc$. Going back to the beginning, we define a relation R on the **set of pairs** $\mathbb{Z} \times \mathbb{Z} \setminus \{0\}$. Note that this is not a relation on $\mathbb{Z}$, rather then on pairs, and we exclude 0 by only considering pairs of the form $\langle a, b\rangle$ where $b \neq 0$. Now we set the criterion that $\langle a, b\rangle R\langle c, d\rangle$ (namely, the pairs $\langle a, b\rangle$ and $\langle c, d\rangle$ are equivalent) if and only if $ad = bc$. Formally, we define the relation R as follows:

$$R = \Big\{\langle\langle a, b\rangle, \langle c, d\rangle\rangle \in (\mathbb{Z} \times \mathbb{Z} \setminus \{0\})^2 \mid ad = bc\Big\}$$

Since equivalence relations imitate equality, there are some necessary properties which must be posed on a general relation in order for it to be an equivalence relation:

Definition 0.2 (Properties of relations and equivalence relation)**.** Let R be a relation on a set A. We say that:

(1) R is *reflexive* (on A) if: $\forall a \in A.aRa$.
(2) R is *symmetric* if: $\forall a, b \in A.aRb \Rightarrow bRa$.
(3) R is *transitive* if: $\forall a, b, c \in A.(aRb) \wedge (bRc) \Rightarrow aRc$.
(4) R is an *equivalence relation* if it is reflexive, symmetric and transitive.

Example 0.3. (1) Let us give some non mathematical relations on the "set" of all humans to illustrate these properties:

Date: April 8, 2024.

(a) The *brotherhood relation*: two humans x, y are brothers if and only if they have the same biological parents.[1]
<u>The brotherhood relation is reflexive</u>: Indeed, **every** human x is a brother of himself, as by this definition x has the same two biological parents as himself.
<u>The brotherhood relation is symmetric</u>: If x is a brother of y then clearly y is a brother of x because they both have the same biological parents.
<u>The brotherhood relation is transitive:</u> Suppose that x is a brother of y and y is a brother of z. Then x as the same two biological parents as y and y has the same two biological parents as z. Then x has the same two biological parents as z, hence x and z are brothers
We conclude that the brotherhood relation is an equivalence relation.

(b) The *descendent relation*: for two humans (dead or alive) we say that x is a descendent of y (or that y is an ancestor of x) is x is the son of a son of a son ... of a son of y. It is a matter of definition if this relation is reflexive, namely, is x is a descendent of himself. It is clearly transitive.This is not symmetric, since for example, Jeffery Jordan is a descendent (the son of) Michael Jordan, but Michael Jordan is not the a descendent of Jeffery Jordan.[2]

(2) Let $A = \{1, 2, 3, 4, 5, 6\}$ then

$$E = \{\underbrace{\langle 1,1\rangle, \langle 2,2\rangle, \langle 3,3\rangle, \langle 4,4\rangle, \langle 5,5\rangle, \langle 6,6\rangle}_{id_A}, \langle 1,5\rangle, \langle 5,1\rangle, \langle 2,3\rangle, \langle 3,2\rangle, \langle 3,6\rangle, \langle 6,3\rangle, \langle 2,6\rangle, \langle 6,2\rangle\}$$

is an equivalence relation on A.

(3) Among the most important equivalence relations is the congruence relation. Recall that for a natural number $n > 0$ and two integers z_1, z_2 we say that $z_1 \equiv z_2 \mod n$ if $z_1 \mod n = z_2 \mod n$. In order to avoid the use modulo in the definition congruency, we can formulate it as follows:

$$E_n = \{\langle z_1, z_2\rangle \in \mathbb{Z}^2 \mid z_1 - z_2 \text{ is divisible by } n\}$$

Let us prove that E_n is an equivalence relation.
<u>Reflexive:</u> we want to prove that for every $z \in \mathbb{Z}$, zE_nz. Let $z \in \mathbb{Z}$, we want to prove that $z - z = 0$ is divisible by n, but this is true sine every number divides 0(recall the formal definition of divisibility and prom this easy fact!).

[1]This is simply a convenient choice of definition, one can consider other definitions for brotherhood.

[2]Note that in order to prove that a relation is not reflexive/symmetric/transitive we should always give a **specific** counter example, since these properties are universal properties and therefore their negation is an existential property.

Symmetric: We want to prove that for every $z_1, z_2 \in \mathbb{Z}$, if $z_1 E_n z_2$ then $z_2 E_n z_1$. Let $z_1, z_2 \in \mathbb{Z}$ and suppose (this is an implication!) that $z_1 E_n z_2$, we want to prove that $z_2 E_n z_1$. [3] By definition of E_n, we conclude that n divides $z_1 - z_2$ and therefore there is $k \in \mathbb{Z}$ such that $z_1 - z_2 = k \cdot n$. Hence $z_2 - z_1 = (-k) \cdot n$ and also $-k \in \mathbb{Z}$. It follows again by the definition of E_n that $z_2 E_n z_1$.
Transitive: Suppose that $z_1 E_n z_2$ and $z_2 E_n z_3$, we want to prove that $z_1 E_n z_3$. By definition of E_n, this means that n divides $z_1 - z_2$ and also $z_2 - z_3$. By definition f divisibility, there are $k_1, k_2 \in \mathbb{Z}$ such that $z_1 - z_2 = k_1 n$ and $z_2 - z_3 = k_2 n$. Summing the two equations, we get:

$$z_1 - z_3 = (z_1 - z_2) + (z_2 - z_3) = k_1 n + k_2 n = (k_1 + k_2)n)$$

Since $k_1 + k_2 \in \mathbb{Z}$, it follows that $z_1 - z_3$ is divisible by n. By the definition of E_n, it follow that $z_1 E_n z_3$.

We conclude that E_n is an equivalence relation.

(4) $S = \{\langle n, m\rangle \in \mathbb{Z}^2 \mid \exists k \in \mathbb{Z} n + k^2 = m\}$ is reflexive, not symmetric, since for example $0S1$ (as $0 + 1^2 = 1$) but $1 \not S 0$ (prove that!). It is not transitive since for example $1 + 1^2 = 2$ and $2 + 1^2 = 3$ however $3 - 1 = 2$ is not a square of a natural (or even rational) number.

(5) The following relation will serve to construct the integers from the natural numbers. On $\mathbb{N}^2$ we define the following relation

$$\sim_Z = \Big\{\langle\langle n, m\rangle, \langle k, l\rangle\rangle \in (\mathbb{N} \times \mathbb{N})^2 \mid n + l = m + k\Big\}$$

Problem 1. *Prove that $\sim_Z$ is an equivalence relation on $\mathbb{N} \times \mathbb{N}$.*

(6) Let us prove that the relation

$$\sim_Q = \Big\{\langle\langle a, b\rangle, \langle c, d\rangle\rangle \in (\mathbb{Z} \times (\mathbb{Z} \setminus \{0\}))^2 \mid ad = bc\Big\}$$

we use to construct the rational numbers is indeed an equivalence relation on $\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$:
Reflexive: Let $\langle a, b\rangle \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$, [4] we want to prove that $\langle a, b\rangle \sim_Q \langle a, b\rangle$. This follows, since $ab = ab$ and by the definition of $\sim_Q$.
Symmetric: Suppose that $\langle a, b\rangle \sim_Q \langle c, d\rangle$, we want to prove that $\langle c, d\rangle \sim_Q \langle a, b\rangle$. By our assumption we see that $ad = bc$, and since we can switch the order of number multiplication we get that $da = cb$ and therefore $\langle c, d\rangle \sim_Q \langle a, b\rangle$.
Transitive: Suppose that $\langle a, b\rangle \sim_Q \langle c, d\rangle$, $\langle c, d\rangle \sim_Q \langle e, f\rangle$. We want to prove that $\langle a, c\rangle \sim_Q \langle e, f\rangle$. By the assumption we have that $ad = bc$ and $cf = de$. Note that $adf = bcf = bde$ and since[5] $d \neq 0$,

---

[3] Usually, we will start directly with "suppose that $z_1 E_n z_2$, we want to prove that $z_2 E_n z_1$".

[4] We want to prove that $\forall a \in A. a \sim_Q a$. In our case $A = \mathbb{Z} \times (\mathbb{Z} \setminus \{0\})$ is a set of pairs (!) hence we want to prove that $\forall \langle a, b\rangle \in \mathbb{Z} \times (\mathbb{Z} \setminus \{0\}). \langle a, b\rangle \sim_Q \langle a, b\rangle$.

[5] Indeed $\langle c, d\rangle \in \mathbb{Z} \times \mathbb{Z} \setminus \{0\}$, $c \in \mathbb{Z}$ and $d \in \mathbb{Z} \setminus \{0\}$. Therefore $d \neq 0$.

we can eliminate it from the equation to see that $af = be$. By definition of $\sim_Q$, it follows that $\langle a,b\rangle \sim_Q \langle e,f\rangle$.

It follows that $\sim_Q$ is an equivalence relation.

(7) For any set A, the identity relation id_A and $A\times A$ are always equivalence relations on the set A.

(8) Here are two examples of equivalence relations on $\mathbb{R}^3$:

$$H_1 = \{\langle\langle a,b,c\rangle,\langle a',b',c'\rangle\rangle \in \mathbb{R}^3 \mid a = a'\}$$

$$H_2 = \{\langle\langle a,b,c\rangle,\langle a',b',c'\rangle\rangle \in \mathbb{R}^3 \mid a+b+c = a'+b'+c'\}.$$

The equivalence criterion that the relation H_1 sets is to identify between triples with the same first coordinate. The equivalence that H_2 sets is to identify triples with the same sum.

(9) Here is an equivalence relations on the set $P(\mathbb{N}) \setminus \{\emptyset\}$:

$$T_1 = \{\langle X,Y\rangle \in (P(\mathbb{N})\setminus\{\emptyset\})^2 \mid \min(X) = \min(Y)\}$$

T_1 identifies sets with the same minimal elements. Here is an equivalence relation on the set $P(\mathbb{N})$:

$$T_2 = \{\langle X,Y\rangle \in (P(\mathbb{N})\setminus\{\emptyset\})^2 \mid X\cap\mathbb{N}_{even} = X\cap\mathbb{N}_{odd}\}$$

T_2 identifies sets which includes exactly the same even numbers.

Back to our example of the rational numbers, what is the object $\frac{1}{2}$? is it $\langle 1,2\rangle$ or is it $\langle 2,4\rangle$? the definition of $\frac{1}{2}$ is just the set of those pairs $\{\langle 1,2\rangle,\langle 2,4\rangle,\rangle 3,6\rangle,\langle -1,-2\rangle....\}$. The point is that we "glue" together all the conditions which are equivalent to $\langle 1,2\rangle$. Formally, we call this an *equivalence class*:

Definition 0.4. Let E be an equivalence relation on a set A. The *equivalence class* of an element $a\in A$ is the set of all conditions $b\in A$ such that a is E-equivalent to b. Formally, we denote the equivalence class of a by

$$[a]_E = \{b\in A \mid aEb\}$$

An E-equivalent class is just $[a]_E$ for some $a\in A$.

Example 0.5. We use the same notations from the previous example.

(1) In the brotherhood relation we have for example the following equivalence classes:

$$[\text{Orville Wright}]_{brotherhood} = \{\text{Orville Wright, Wilbur Wright}\}$$

$$[\text{Steph Curry}]_{brotherhood} = \{\text{Steph Curry, Seth Curry, Sydel Curry}\}$$

$$[\text{Kim Kardashian}]_{brotherhood} = \{\text{Kim Kard., Kourtney Kard., Khloé Kard., Rob Kard.}\}$$

(2) For $A = \{1,2,3,4,5,6\}$ and E from example (2), We have that:

$$[1]_E = \{1,5\}$$

$$[2]_E = \{2,3,6\}$$

$$[3]_E = \{2,3,6\}$$

$$[4]_E = \{4\}$$

$$[5]_E = \{1, 5\}$$
$$[6]_E = \{2, 3, 6\}$$

This is not a coincidence that $[1]_E = [5]_E$ and that $[2]_E = [3]_E = [6]_E$, can you guess way?

(3) The equivalence classes of E_n are

$$[0]_{E_n} = \{0, n, -n, 2n, -2n, 3n, ...\} = \{zn \mid z \in \mathbb{Z}\}$$
$$[1]_{E_n} = \{1, n-1, -n+1, 2n-1, -2n+1, ...\} = \{zn + 1 \mid z \in \mathbb{Z}\}$$

A general equivalence class is just:

$$[i]_{E_n} = \{zn + i \mid z \in \mathbb{Z}\}$$

and $i \equiv j \mod n$ if and only if $[i]_{E_n} = [j]_{E_n}$.

(4) Using equivalence classes and the equivalence relation $\sim_Q$ we can now formally define the rational number $\frac{n}{m} = [\langle n, m\rangle]_{\sim_Q}$. For example, the number $\frac{1}{2}$ is just $[\langle 1, 2\rangle]_{\sim_Q}$. We will see later that $[\langle 1, 2\rangle]_{\sim_Q} = [\langle 2, 4\rangle]_{\sim_Q}$ for example, where the last equality is an actual set equality!

(5) As for $\sim_Z$, we think of a pair $\langle n, m\rangle \in \mathbb{N}^2$ and representing $n-m$. So we identify between $n \in \mathbb{N}$ with $[\langle n, 0\rangle]_{\sim_Z}$ and define $-n = [\langle 0, n\rangle]_{\sim_Z}$.

(6) The equivalence class of a general triple $\langle a, b, c\rangle \in \mathbb{R}^3$ has the form:

$$[\langle a, b, c\rangle]_{H_1} = \{\langle a, x, y\rangle \mid x, y \in \mathbb{R}\}$$

and

$$[\langle a, b, c\rangle]_{H_2} = \{\langle x, y, (a + b + c - x - y)\rangle \mid x, y \in \mathbb{R}\}$$

(7) We have fore example

$$[\{4, 7, 3, 22\}]_{T_1} = \{X \in P(\mathbb{N}) \mid 3 = \min(X)\}$$

and

$$[\{4, 7, 3, 22\}]_{T_2} = \{X \in P(\mathbb{N}) \mid X \cap \mathbb{N} = \{2, 22\}\}$$

Proposition 0.6. *Let E be an equivalence relation on A. Then for every $a, b \in A$:*

(1) Either $[a]_E = [b]_E$.
(2) Or $[a]_E \cap [b]_E = \emptyset$

Moreover, $[a]_E = [b]_E$ if and only if aEb.

Proof. Let $a, b \in A$. We formally need to prove a $\vee$-statement. Let us split into cases:

(1) Suppose $[a]_E \cap [b]_E = \emptyset$, the (2) holds and we are done.
(2) Suppose $[a]_E \cap [b]_E \neq \emptyset$. We want to prove that $[a]_E = [b]_E$, which is sets equality. Let us prove a double inclusion:
   (a) $\underline{[a]_E \subseteq [b]_E}$: Let $x \in [a]_E$. We want to prove that $x \in [b]_E$. Let $c \in [a]_E \cap [b]_E$, which exists by the assumption in this case. By definition of equivalence relation, xEa, cEa and cEb.
      - By symmetry, since cEa, then aEc.

- By transitivity, since xEa and aEc, then xEc.
- Again by trasitivity since xEc and cEb, xEb.

By the definition of equivalence class it follows that $x \in [b]_E$.

(b) $[b]_E \subseteq [a]_E$: Follows from the symmetry between a and b.

This concludes the proof that $[a]_E = [b]_E$ or $[a]_R \cap [b]_E = \emptyset$. For the moreover part, we nee to prove a double implication:

(1) $\implies$: Suppose that $[a]_E = [b]_E$, we need to prove that aEb. Since E is reflexive, aEa and therefore $a \in [a]_E$. By the equality of the set $[a]_E = [b]_E$ we conclude that $a \in [b]_E$ and by the definition of equivalence class we conclude that aEb.

(2) $\impliedby$: Suppose that aEb, we need to prove that $[a]_E = [b]_E$. Again since E is reflexive we have that $a \in [a]_E$ and by the definition of equivalence class we have that $a \in [b]_E$. Thus $a \in [a]_E \cap [b]_E$, which means that $[a]_E \cap [b]_E \neq \emptyset$. By the first part, this must means that $[a]_E = [b]_E$.

□

Corollary 0.7. *The following are equivalent:*

(1) $a \not{E} b$.
(2) $[a]_E \neq [b]_E$.
(3) $[a]_E \cap [b]_E = \emptyset$.

Proof. exercise. □

Definition 0.8. Let E be an equivalence relation on A. The *quotient set* of A by E (a.k.a "A modulo E") is the set of **all** equivalence classes.[6]. We denote it by[7]

$$A/E = \{[a]_E \mid a \in A\}$$

Example 0.9. (1) The "set" Humans/brotherhood consist of all possible equivalence classes, each equivalence class is the set of siblings from a given family. We can label each equivalence class according to the family name and think of the quotient

Humans/brotherhood = {"The Kardeshians", "The Curry's", "The Wright's", ...}

(2) $A/E = \{\{1,5\},\{2,3,6\},\{4\}\}$.

(3) We have that

$$\mathbb{Z}/E_n = \{\{zn+i \mid z \in \mathbb{Z}\} \mid i = 0,1,2,...,n-1\}$$

Since each equivalence class in E_n is associated with a residue modulo n, we think of $\mathbb{Z}/E_n$ as the sets of residues modulo n.

(4) The integers are defined by $\mathbb{Z} = \mathbb{N}^2/\sim_Z$

(5) The rational numbers are defined as

$$\mathbb{Q} = (\mathbb{Z} \times (\mathbb{Z} \setminus \{0\})/\sim_Z$$

[6] Needless to say, without repetitions.

[7] Do not confused A/E with set difference $A \setminus E$.

(6)
$$\mathbb{R}^3/H_1 = \{\{\langle a,x,y\rangle \mid x,y\in\mathbb{R}\} \mid a\in\mathbb{R}\}$$
Here every equivalence class can be identified with a single real number a.
$$\mathbb{R}^3/H_2 = \{\{\langle x,y,(s-x-y)\rangle \mid x,y\in\mathbb{R}\} \mid s\in\mathbb{R}\}$$
Also here the equivalence classes can be identifies with a single real number s which represents the sum $a+b+c$.

(7)
$$(P(\mathbb{N})\setminus\{\emptyset\})/T_1 = \{\{X\in P(\mathbb{N})\setminus\{\emptyset\} \mid \min(X)=n\} \mid n\in\mathbb{N}\}$$
And each equivalence class can be identified with a natural number.
$$P(\mathbb{N})/T_2 = \{\{X\in P(\mathbb{N}) \mid X\cap\mathbb{N}_{even}=Y\} \mid Y\in P(\mathbb{N}_{even})\}$$
And each equivalence class can be identified with a set of even numbers.

Definition 0.10 (Partition)**.** Let A be any set. A partition of the set A is any set $\Pi\subseteq P(A)$ such that:

(1) $\emptyset\notin\Pi$.
(2) $\cup\Pi = A$.
(3) If $X,Y\in\Pi$, $X\neq Y$, then $X\cap Y=\emptyset$.

Example 0.11. (1) $\{\{1,5\},\{2,3,6\},\{4\}\}$ is a partition of $\{1,2,3,4,5,6\}$.
(2) $\{\mathbb{N}_{even},\mathbb{N}_{odd}\}$ is a partition of $\mathbb{N}$.

Corollary 0.12. *If E is an equivalent relation on A then A/E is a partition of A.*

Proof. Follows directly from Proposition 0.6. □

Theorem 0.13. *Let Π be a partition on A. Let R_Π be the relation on A defined by*
$$xR_\Pi y \iff \exists B\in\Pi,\ x,y\in B$$
Then:

(1) R_Π is an equivalence relation on A.
(2) $A/R_\Pi = \Pi$.

Proof. (1) Let us prove that R_Π is an equivalence relation:

R_Π is reflexive: Let $a\in A$, since $\cup\Pi=A$, there is $X\in\Pi$ such that $a\in X$ and therefore by definition of R_Π, $\langle a,a\rangle\in R_\Pi$.

R_Π is symmetric: Suppose that $\langle a,b\rangle\in R_\Pi$, then there is $X\in\Pi$ such that $a,b\in X$. Hence $b,a\in X$, and therefore $\langle b,a\rangle\in R_\Pi$.

R_Π is transitive: Suppose that $\langle a,b\rangle\in R_\Pi$ and $\langle b,c\rangle\in R_\Pi$, then there are $X,Y\in\Pi$ such that $a,b\in X$ and $b,c\in Y$. Since $b\in X\cap Y$, we conclude that $X\cap Y\neq\emptyset$ and since Π is a partition, $X=Y$. hence $a,c\in X$ and therefore $\langle a,c\rangle\in R_\Pi$.

(2) To see that $A/R_\Pi=\Pi$ we prove a double inclusion:

$\subseteq$: Let $[a]_{R_\Pi} \in A/R_\Pi$. Then there is $X \in \Pi$ such that $a \in X$. We claim that $[a]_{R_\Pi} = X$ and from this it follows that $[a]_{R_\Pi} \in \Pi$. Again we prove it by double inclusion:

- $\subseteq$: Let $b \in [a]_{R_\Pi}$, then $aR_\Pi b$ and therefore there is $Y \in \Pi$ such that $a, b \in Y$. Since $a \in X \cap Y$ we conclude that $X = Y$ and therefore $b \in X$.
- $\supseteq$: If $b \in X$ then $a, b \in X \in \Pi$ and therefore $aR_\Pi b$ which implies that $b \in [a]_{R_\Pi}$.

$\subseteq$: Let $X \in \Pi$, we want to prove that $X \in A/R_\Pi$. Since $X \neq \emptyset$, pick any $a \in X$, we claim that $X = [a]_{R_\Pi} \in A/R_\Pi$. The prof is similar to the previous part.

□

Problem 2. *If R is an equivalence relation on A, then $R = R_{A/R}$.*

Definition 0.14. A relation R does not depend on the choice of representatives of E if whenever aEa' and bEb' then $aRb \Rightarrow a'Rb'$.

Example 0.15.

(1) $[\langle n, m\rangle]_{\sim Z} + [\langle n', m'\rangle]_{\sim Z} = [\langle n+n', m+m'\rangle]_{\sim Z}$ Does not depend on the choice of representatives.

Proof. If $\langle n_1, m_1\rangle \sim_Z \langle n_2, m_2\rangle$ and $\langle n_1', m_1'\rangle \sim_Z \langle n_2', m_2'\rangle$, then $n_1 + m_2 = n_2 + m_1$ and $n_1' + m_2' = n_2' + m_1'$. We would like to prove that

$$\langle n_1 + n_1', m_1 + m_1'\rangle \sim_Z \langle n_2 + n_2', m_2 + m_2'\rangle$$

. To see this,

$$n_1 + n_1' + m_2 + m_2' = n_1 + m_2 + n_1' + m_2' = n_2 + m_1 + n'2 + m_1' = m_1 + m_1' + n_2 + n_2'$$

as wanted. □

(2) $[n]_{E_m} \cdot [n']_{E_m} = [n \cdot n']_{E_m}$ does not depend on the choice of representative.

Proof. Suppose that $nE_m n_0$ and $n'E_m n_0'$ we want to prove that $nn'E_m n_0 n_0'$. Note that $m|n - n_0$ and $m|n' - n_0'$. Hence

$$nn' - n_0 n_0' = nn' - n'n_0 + n'n_0 - n_0 n_0' = n'(n - n_0) + n_0(n' - n_0').$$

This is a sum of two numbers which are divisible by m and therefore $nn' - n_0 n_0'$ is divisible by m. □

(3) $F([\langle a, b, c\rangle]_{H_1}) = a$ Does not depend on the choice of representatives. Clearly if $\langle a, b, c\rangle H_1 \langle a', b', c'\rangle$, then $a = a'$ and therefore $F([\langle a, b, c\rangle]_{H_1}) = F([\langle a', b', c'\rangle]_{H_1})$.