Lagrange's Theorem

Daniel Rostovtsev
Date: May 10, 2017

Equivalence Relations

Let B be the boolean set {true, false}. A relation, $\sim: S \times S \to B$ is an equivalence relation if each of the following axioms are true for all $a, b, c \in S$:

i. $a \sim a$

ii. $a \sim b \leftrightarrow b \sim a$

iii. $a \sim b; b \sim c \to a \sim c$

Equivalence Classes

A subset E of S is an equivalence class of S under an equivalence relation $\sim$ if, for any $a, b \in E$, $a \sim b$.

Partitions

Let $U = \{U_1, \cdots, U_n\}$ be a set of sets U_i. Given a set S, U partitions S if and only if the following is true:

i. $U_i \cap U_j = \emptyset$ for all $i \neq j$

ii. $\bigcup_{i=1}^{n} U_i = S$

Equivalence Partitioning Theorem

Let $E = \{E_1, \cdots E_n\}$ be the set of equivalence classes of S with $\sim$, then E must partition S.

Proof. Since $a \sim a$, each element in S must at least be in an equivalence class with itself. Therefore $\bigcup_{i=0}^{n} E_i = S$. To show E partitions S, it remains only to show that $E_i \cap E_j = \emptyset$ if $i \neq j$.

Suppose $E_i \cap E_j = K \neq \emptyset$. Since E_i is an equivalence class, all elements in E_i must be equivalent to each other. So, if a is an arbitrary element of E_i, $a \sim s$ for all $s \in E_i$. Likewise, let b be a an arbitrary element in E_j, such that $b \sim s$ for all $s \in E_j$. Note that $a \not\sim b$. If K is not the empty set, then it must contain some element k. Since $k \in E_i \cap E_j$, $a \sim k$, and $b \sim k$. It follows that $a \sim b$. But $a \not\sim b$, so, by contradiction, E must partition S. $\square$

Lemma

If $h \in H$, then $hH = H$.

Proof. Let $f_h : H \to H$ where $h \in H$, and $f_h(x) = hx$. f_h is bijective, since it is surjective and injective, so $hH = H$.

$$f_h(a) = f_h(b) \leftrightarrow ha = hb \leftrightarrow h^{-1}ha = h^{-1}hb \leftrightarrow a = b \therefore f_h(a) = f_h(b) \leftrightarrow a = b \text{ (injectivity)}$$

$$\forall a \in H : f_h(x) = a \leftrightarrow hx = a \leftrightarrow x = h^{-1}a \therefore \exists x \in H : f_h(x) = a \text{ (surjectivity)}$$

$\square$

Lemma

If $a \in bH$, then $aH = bH$.

Proof. If $a \in bH$, then $a = bh$ for some $h \in H$. Thus $aH = (bh)H = b(hH) = bH$, so $aH = bH$.

$\square$

Proposition 1

Let $H \leq G$, then the cosets of H partition G.

Proof. If there is an equivalence relation whose equivalence classes form the cosets of H in G, then the cosets of H must partition G by the equivalence partitioning theorem proved above. Consider the following relation:

$$a \sim b = \begin{cases} \text{true} & \text{if } b \in aH \\ \text{false} & \text{if } b \notin aH \end{cases}$$

By the above proposition, $\sim$ can also be stated in the following way:

$$a \sim b = \begin{cases} \text{true} & \text{if } aH = bH \\ \text{false} & \text{if } aH \neq bH \end{cases}$$

To show that $\sim$ is an equivalence relation:

i. $a \sim a \because aH = aH$

ii. $a \sim b \leftrightarrow b \sim a \because aH = bH \leftrightarrow bH = aH$

iii. $a \sim b$; $b \sim c \rightarrow a \sim c \because aH = bH$; $bH = cH \rightarrow aH = cH$

□

Proposition 2

Let $H \leq G$ and $a \in G$, then $|aH| = |H|$.

Proof. Let $f_a : H \rightarrow aH$ such that $f_a(h) = ah$.

f_a is surjective since it is defined for all h.

$f_a(h) = f_a(h') \leftrightarrow ah = ah' \leftrightarrow h = h'$ so f_a is injective

Therefore f_a is a bijection, and $|H| = |aH|$.

□

Lagrange's Theorem

Let $H \leq G$, then $|G| = (G : H)|H|$, where $(G : H)$ is the number of cosets of H in G.

Proof. The equivalence classes of the equivalence relation defined in the first proposition are precisely the cosets of H in G. Therefore, by the Equivalence Partitioning Theorem, the cosets of H partition G. By the second proposition, each coset has the same order, so each partition is of equal size. Since the number of cosets of H in G is defined to be $(G : H)$, it follows directly that $|G| = (G : H)|H|$.

□