Russ Johnson
Problem Set #5
March 26, 2013

Activity 24.12 Write a formal proof of Lagrange's Theorem (Theorem 24.4).

Proof. Let G be a finite group and let H be a subgroup of G. From Theorem 24.3 we know that the left cosets of H form a partition of G. Let n be the number of distinct cosets of H in G. Each left coset of H contains $|H|$ elements. (Activity 24.7). And so, $|G| = n|H|$. In conclusion, $|H|$ divides $|G|$. □

Activity 24.13. Let G be a group with identity e and assume that $\sim$ is a congruence relation on G.
(a) Let $H = \{x \in G : x \sim e\}$. Show that H is a subgroup of G.

First of all, we know that $e \sim e$ from the reflexive property of the congruence relation $\sim$. And so, the identity element of G is also in H.

Next, let $a \in H$. From the definition of the set H, we know that $a \sim e$. Because $\sim$ is a congruence relation, $a^{-1} \sim e^{-1}$. And so, $a^{-1} \sim e$ which means that $a^{-1} \in H$. In conclusion, every element in H has an inverse that is also in H. (Which is the same as the inverse of this element in G).

Finally, let $a, b \in H$. From the definition of the set H, we know that $a \sim e$ and $b \sim e$. Because $\sim$ is a congruence relation, $ab \sim e^2$. And so $ab \sim e$ which means that $ab \in H$. In conclusion, the operation of G is closed in H. The identity of G is in H, every element in H has an inverse, and the operator of G is closed in the set H. And so, the set H is a subgroup of G.

(b) Let $a, b \in G$. Prove that $a \sim b$ if and only if $a^{-1}b \in H$.

Proof. First, let $a, b \in G$ such that

$$a \sim b. \tag{1}$$

From the reflexive property of the congruence relation $\sim$ we know that

$$a^{-1} \sim a^{-1}. \tag{2}$$

From part 1 of the definition of a congruence relation we can take (1) and (2) to obtain

$$aa^{-1} \sim ab^{-1}. \tag{3}$$

From (3) we know that $e \sim ab^{-1}$ and from the symmetric property we know that $ab^{-1} \sim e$. From this we see that $ab^{-1} \in H$.

Next, let $a, b \in G$ such that $a^{-1}b \in H$ or in other words

$$a^{-1}b \sim e. \tag{4}$$

From the reflexive property of the congruence relation we know that

$$a \sim a. \tag{5}$$

From part 2 of the definition of a congruence relation we know from (4) and (5) that

$$aa^{-1}b \sim ae. \tag{6}$$

Simplifying (6) we arrive at

$$(6)b \sim a. \tag{7}$$

Applying the symmetric property of the congruence relation $\sim$ to (6) we obtain $a \sim a$. From this we have show that if $a \sim b$, then $ab^{-1} \in H$ and if $ab^{-1} \in H$, then $a \sim b$. In other words, $a \sim b$ if and only if $ab^{-1} \in H$. □

(c) Explain why $\sim_H$ is the only possible congruence relation on a group G.

At the beginning of this activity the only assumption that we made was the $\sim$ is a congruence relation on G. In parts (a) and (b), we proved that the congruence relation $\sim$ is equivalent to $\sim_H$. This means that if G has a congruence relation, then this congruence relation is $\sim_H$. In other words, $\sim_H$ is the only possible congruence relation on G. Activity 24.14.
(a) State the converse of Lagrange's Theorem. What do we need to do to show that the converse of Lagrange's Theorem is not true?

Converse. If m is a divisor of a finite group G, then there exists some subgroup of G with order m.

To prove that the converse of Lagrange's Theorem is false we need to give an example of group that has a divisor with no possible subgroup of that order.

(b) Consider the group $G = A_4$. List the elements of A_4 in cycle notation and determine the order of A_4.

The order of A_4 is 12 and

$\{I, (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243)\}$.

(c) Assume that H is a subgroup of A_4 of order 6.

(i) Explain why the nonidentity elements of H must have order 2 or 3.

The order of an element in H is the number of elements in the cycle group generated by that element. From Lagrange's Theorem it must therefore have order 1, 2, 3, or 6. Since the element is not the identity, we know that the order cannot be 1 and because the element cannot be a generator of G we know that the order cannot be 6. Therefore, the order must be 2 or 3.

(ii) Explain why there must be an element α of A_4 of order 3 that is not in H.

The elements (123), (142), and (134) all have order 3. Because H is a subgroup of A_4, it must be closed and in order to have all three of (123), (142), and (134) H would need to have an order of at least 9.

(iii) Explain why the left cosets H, αH and $\alpha^2 H$ cannot all be distinct.

From Theorem 24.3 part 2 we know that the group G can be written as a disjoint union of left If we assume that they are all distinct, from Theorem 24.3 part 1 we know that they cannot share any elements. The total number of elements for each of these sets is six and so A_4 must contain at least 18 elements in order for all of the left cosets to be distinct. Because this is not the case, at least two of these left cosets must be equal.

(iv) Show that it is not possible for any two of H, αH and $\alpha^2 H$ to be equal.

We know that α has order 3 and so e, α and α^2 are all unique elements. Because the H is a subgroup of G we know that G's identity, e, is in H. And so, we can also see that $e \in H$, $\alpha \in \alpha H$, and $\alpha^2 \in \alpha^2 H$. Because α is not in H, $\alpha \notin H$, $\alpha^2 \notin \alpha H$, and $\alpha^3 = e \notin \alpha^2 H$. From this we see that $H \neq \alpha H$, $\alpha H \neq \alpha^2 H$, and $\alpha^2 H \neq H$. (d) Explain why the converse of Lagrange's Theorem is not true.

The group A_4 does not have a subgroup of order 6 and so the converse is not true. When we tried to construct a subgroup of A_4 with order six we arrived at a contradiction. We had the three left cosets H, αH and $\alpha^2 H$ that could not all be distinct, but none could be equal.

(4) A group G contains elements of every order from 1 to 10. What is the smallest order G could have? Find a group G of that order that contains elements of every order from 1 through 10.

By Lagrange's Theorem the order of a subgroup must divide the order of the group. The order of an element is equal to the number of elements

in the subgroup generated by that element. Therefore, a group with elements of every order from 1 through 10 must be divisible by the numbers 1 through 10. The least common multiple of the numbers 1 through 10 is the lowest of these numbers. Therefore, the smallest order that G could be is $lcm(1,2,3,4,5,6,7,8,9,10) = 2^3 \cdot 3^2 \cdot 5 \cdot 7 = 2520$. An example of a group with this order is $\mathbb{Z}_{2520}$ under addition. The identity, $[2520/1] = [0]$, has order 1, $[2520/2] = [1260]$ has order 2, $[2520/3] = [840]$ has order 3, and so on. Because 2520 is divisible by each of the numbers 1 through 10, we are able to follow this pattern to obtain elements with the orders 1 through 10.

(6) Let $H = \{I, r\}$ in D_4.

(a) Determine all of the distinct left cosets of H in D_4.

First of all, $D_4 = \{I, R, R^2, R^3, r, Rr, R^2r, R^3r\}$ and so $|D_4| = 8$. The number of distinct left cosets of H in D_4 is referred to as the index and is $\frac{|D_4|}{|H|} = 4$. These four distinct left cosets are

$$IH = rH = \{I, r\},$$

$$RH = RrH = \{R, Rr\},$$

$$R^2H = R^2rH = \{R^2, R^2r\},$$

and

$$R^3H = R^3rH = \{R^3, R^3r\}.$$

(b) Determine all of the distinct right cosets of H in D_4.

Like in part (a), there are four distinct right cosets. These right cosets are

$$HI = Hr = \{I, r\},$$

$$HR = HR^3r = \{R, R^3\},$$

$$HR^2 = HR^2r = \{R^2, R^2r\},$$

and

$$HR^3 = HRr = \{R^3, Rr\}.$$