PROBLEM SET 6

HAMID SAGBAN

Exercise 1. *Let $(M, *)$ be a group and $(H, *)$ be a subgroup of M such that $H \neq M$.*

(a) *Define $=_R$ on M such that for every $a, b \in M$ (a, b not necessarily distinct), $a =_R b$ if $b^{-1} * a \in H$. Show that $=_R$ is an equivalent relation on $(M, *)$.*

(b) *Assume that M is an abelian group (and hence H is abelian). Let S be the set of all distinct equivalence classes of $(M, *, =_R)$. Define a binary opeartion $\wedge$ on S as following: Let $d, k \in S$. Then $d = [a]$ and $k = [b]$ for some $a, b \in M$. Now $[a] \wedge [b]$ means: choose $u \in [a]$ and $j \in [b]$, and let $[a] \wedge [b] = [u * j]$. Show that $\wedge$ is a well-defined relation on S, and then show that $(S, \wedge)$ is an abelian group.*

Proof. For (a), we have $a =_R a \iff a^{-1} * a \in H$, so that $e \in H$, which is true since H is a subgroup of M. Now $a =_R b \iff b^{-1} * a \in H$, and since $(b^{-1} * a)^{-1} = a^{-1} * b \in H$, we have $b =_R a$. Finally, we have $a =_R b$ and $b =_R c \iff b^{-1} * a \in H$ and $c^{-1} * b \in H$. Now $c^{-1} * b * b^{-1} * a = c^{-1} * a \in H$ and thus $a =_R c$, as desired.

To show well-definition of $\wedge$, it suffices to show that $(u' * j')^{-1} * (u * j) \in H$, since this implies $u' * j' =_R u * j$ and thus $[u' * j'] = [u * j]$. We know that $u'^{-1} * u = h_1$ for some $h_1 \in H$, and this is clear since $u', u \in [a]$ $\iff u' =_R a$ and $u =_R a \iff u' =_R u$. Similarly, we have $j'^{-1} * j = h_2$ for some $h_2 \in H$. Thus, we have $(u' * j')^{-1} * (u * j) = j'^{-1} * u'^{-1} * u * j = j'^{-1} * h_1 * j = h_1 * (j'^{-1} * j) = h_1 * h_2 \in H$. Thus $[u * j] = [u' * j']$, and the operation is well-defined.

We now show that S is an abelian group. Take $[a], [b] \in S$, and pick a, b as representatives for $[a], [b]$ respectively. Then $[a] \wedge [b] = [a * b]$. Since $a * b \in M$, and there exists $[c] \in S$ such that $a * b \in [c]$, we have $[a * b] = [c] \in S$, and thus S is closed under $\wedge$. Now to show associativity, take $[a], [b], [c] \in S$. Then $([a] \wedge [b]) \wedge [c] = [a * b] \wedge [c] = [(a * b) * c] = [a * (b * c)] = [a] \wedge [b * c] = [a] \wedge ([b] \wedge [c])$. Now take $e \in M$, then there exists $[x] \in S$ such that $e \in [x]$. Thus $[e] = [x] \in S$, and for any $[a] \in S$, we have $[e] \wedge [a] = [e * a] = [a]$ and $[a] \wedge [e] = [a * e] = [a]$. Now for inverses, take any $a \in M$. There exists $a^{-1} \in M$ such that $a * a^{-1} = a^{-1} * a = e$. There also exist $[x], [y] \in S$ such that $a \in [x]$ and $a^{-1} \in [y]$. Thus $[a] = [x] \in S$ and $[a^{-1}] = [y] \in S$. Now we have $[a] \wedge [a^{-1}] = [a * a^{-1}] = [e]$, and $[a^{-1}] \wedge [a] = [a^{-1} * a] = [e]$, and thus S is a group. It remains to show that its an abelian group, but this is clear by first picking $a, b \in M$. Then there exist $[x], [y] \in S$ such that $a \in [x]$ and $b \in [y]$. Thus $[a] = [x] \in S$ and $[b] = [y] \in S$. Now $[a] \wedge [b] = [a * b] = [b * a] = [b] \wedge [a]$, as desired.

□

Exercise 2. *Let* $(M, *)$ *be a group.*

(a) *Let* $a, b \in M$ *such that* $a * b = b * a$, $|a| = m$, $|b| = n$, *and* $\gcd(n, m) = 1$. *Show that* $|a * b| = nm$.

(b) *Let* $a, b \in M$ *such that* $a * b = b * a$, $|a| = m$, $|b| = n$. *Show there is an element* $c \in M$ *such that* $|c| = \text{lcm}(n, m)$.

Lemma 1. *Let* $a, b \in N^*$. *Suppose* $a \mid b$ *and* $b \mid a$. *Then* $a = b$.

Proof. If $a \mid b$, then $b = ma$ for some $m \in N^*$. If $b \mid a$, then $a = nb$ for some $n \in N^*$. Thus we have $b = ma = mnb$, and thus $mn = 1$. The only combination of positive integers that satisfies $mn = 1$ is $m = n = 1$. Thus we have $a = b$. □

Proof of Exercise 2. For (a), we have $(a*b)^{nm} = a^{nm} * b^{nm} = (a^m)^n * (b^n)^m = (e)^n * (e)^m = e$. It remains to show that nm is the least positive integer such that $(a * b)^{nm} = e$. Suppose $|a * b| = k$. Then k is a factor of nm. Also, since $e^m = ((a * b)^k)^m = (a * b)^{km} = (a^{km} * b^{km}) = b^{km}$, we have $n \mid km$, and thus $n \mid k$ since $\gcd(n, m) = 1$. Similarly, $e^n = ((a * b)^k)^n = (a * b)^{kn} = (a^{kn} * b^{kn}) = a^{kn}$ gives us $m \mid k$. Now since $m \mid k$ and $n \mid k$, and $\gcd(m, n) = 1$, we have $mn \mid k$. Since $mn \mid k$ and $k \mid mn$, we have $k = mn$ by Lemma 1.

For (b), we have two cases. Suppose $\gcd(n, m) = 1$, and let $c = a * b$. Then by part (a), $|c| = |a * b| = nm = \frac{nm}{\gcd(n,m)} = \text{lcm}(n, m)$. Now suppose $gcd(n, m) = k > 1$. Then there exist two positive integers x, y such that $xy = k$ and $\gcd(\frac{m}{x}, \frac{n}{y}) = 1$. Thus $x \mid m$ and $y \mid n$. Let $c = a^x * b^y$. We know that $|a^x| = \frac{m}{\gcd(m,x)} = \frac{m}{x}$ and $|b^y| = \frac{n}{\gcd(n,y)} = \frac{n}{y}$. Since $\gcd(\frac{m}{x}, \frac{n}{y}) = 1$, we can apply part (a) to get $|c| = \frac{m}{x} \times \frac{n}{y} = \frac{nm}{\gcd(n,m)} = \text{lcm}(n, m)$, as desired. □

Exercise 3. *Construct the additive table for* $(Z_7, +_7)$ *and the multiplicative table for* $(Z_7^*, \times_7)$.

Solution. The additive table is shown first, followed by the multiplicative table. We emphasize that the entries in the tables are *equivalence classes*.

	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

	1	2	3	4	5	6
1	1	2	3	4	5	6
2	2	4	6	1	3	5
3	3	6	2	5	1	4
4	4	1	5	2	6	3
5	5	3	1	6	4	2
6	6	5	4	3	2	1

□