Moshe Mason Rubin
MATH 330 Homework #7
19 October 2016

Exercise 6.7. Verify Euler's Theorem for $n = 15$ and $a = 4$.

Solution. Because $\gcd(15, 4) = 1$, we may apply Euler's Theorem that $a^{\phi(n)} \equiv 1 \pmod{n}$.

$$\begin{aligned}\phi(15) &= \#\{x \in ([1, 15) \cap \mathbb{Z}) \,|\gcd(x, 15) = 1\} \\ &= \#\{1, 2, 4, 7, 8, 11, 13, 14\} \\ &= 8\end{aligned}$$

and

$$\begin{aligned}4^8 &= 4^{2^3} \\ &\equiv 1 \quad \text{as } 4^{2^0} \equiv 4 \implies 4^{2^1} \equiv 1 \implies 4^{2^2} \equiv 4 \implies 4^{2^3} \equiv 1\end{aligned}$$

So Euler's Theorem holds for $n = 15$ and $a = 4$. ✓ □

Exercise 6.8. Use Fermat's Little Theorem to show that if $p = 4n + 3$ is prime, there is no solution to the equation $x^2 \equiv -1 \pmod{p}$.

Proof. Notice $x \in [(\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}]$ and $x^2 \equiv -1 \pmod{p} \implies x^4 \equiv 1 \pmod{p}$.
If $x \equiv 1$ then $x^2 \equiv 1$ and $x^2 \equiv -1$, so $1 \equiv -1 \implies 2 \equiv 0 \implies p = 2 = 4n + 3$, which is a contradiction. So $x \not\equiv 1$ and $x^2 \not\equiv 1$, so $|x|= 4$.
Since $|x|= 4$ and $x \in [(\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}]$, we have 4 divides $|G|$, where clearly $|G|= p-1$. So $4|p-1 \implies 4|(4n+3)-1 \implies 4|4n+2$ which is a contradiction. Therefore there is no $x \in [(\mathbb{Z}/p\mathbb{Z}) \setminus \{0\}]$ such that $x^2 \equiv -1 \pmod{p}$. □

Exercise 6.11. Let H be a sub-group of G and suppose that $g_1 \cdot g_2 \in G$. Prove that the following conditions are equivalent.

(a) $g_1 H = g_2 H$ (b) $H g_1^{-1} = H g_2^{-1}$ (c) $g_1 H \subseteq g_2 H$ (d) $g_2 \in g_1 H$ (e) $g_1^{-1} g_2 \in H$

Proof. **(a) $\iff$ (b):**

$$\begin{aligned}g_1 H \ = g_2 H &\iff g_1 \sim_{H,L} g_2, \quad \text{as } [x]_{\sim_{H,L}} = xH \\ &\iff g_1^{-1} g_2 \in H \quad \text{by definition of } \sim_{H,L} \\ &\iff g_1^{-1} \sim_{H,R} g_2^{-1} \quad \text{by definition of } \sim_{H,R} \\ &\iff H g_1^{-1} = H g_2^{-1}, \quad \text{as } [x]_{\sim_{H,R}} = Hx\end{aligned} \tag{1}$$

So $g_1 H = g_2 H \iff H g_1^{-1} = H g_2^{-1}$. □

(a) $\implies$ (d):

$$g_1 H = g_2 H \text{ and } g_2 \in g_2 H \implies g_2 \in g_1 H \quad \square$$

(c) $\iff$ (a):

$$\begin{aligned}g_1 H \ \subseteq g_2 H &\iff g_1 \in g_2 H \quad \text{by } \mathbf{(d)} \\ &\iff g_1 = g_2 h \quad \text{for some } h \text{ in } H \\ &\iff g_2^{-1} g_1 \in H \\ &\iff g_1 \sim_{H,L} g_2 \quad \text{by definition of } \sim_{H,L} \text{ and fact that } \sim_{H,L} \text{ is symmetric} \\ &\iff g_1 H = g_2 H, \quad \text{as } [x]_{\sim_{H,R}} = Hx\end{aligned}$$

So $g_1 H \subseteq g_2 H \iff g_1 H = g_2 H$. □

(a) $\iff$ (c): I kind of think of this as the definition, through a proof is given in (1). □

Exercise 6.17. Suppose that $[G : H] = 2$. If a and b are not in H, show that $ab \in H$.

Proof. Clearly $id \in H$ as H is a sub-group. Let $H = \{h_1, \ldots, h_n, id\}$ such that $a, b \notin H$. Consider $aH = \{ah_1, \ldots, ah_n, a\}$. Since $[G : H] = 2$ we have that $aH = G \setminus H$ by theorem from class. Clearly $ab \notin aH$ as $ah_i \neq ab$ for any i by assumption that $b \notin H$. So $ab \notin G \setminus H \implies ab \in H$ (as ab must be in G because G is closed). □

Exercise 6.20. Let H and K be sub-groups of a group G. Define a relation $\sim$ on G by $a \sim b$ if there exists an $h \in H$ and a $k \in K$ such that $hak = b$. Show that this relation is an equivalence relation. The corresponding equivalence classes are ***double co-sets***. Compute the double co-sets of $H = \{(1), (123), (132)\}$ in A_4.

Proof.

Reflexive: As H and K are sub-groups, clearly $id \in H$ and $id \in K$. So let $h = k = id$. Then $id \cdot a \cdot id = a$, so $\sim$ is reflexive. ✓

Symmetric: Because they are sub-groups, H and K are closed under inverses. So

$$\begin{aligned} a \sim b \iff hak = b &\iff ak = h^{-1}b \quad \text{by left multiplying by } h^{-1}, \text{ as } h^{-1} \in H \\ &\iff a = h^{-1}bk^{-1} \quad \text{by left multiplying by } k^{-1}, \text{ as } k^{-1} \in k \\ &\iff b \sim a \end{aligned}$$

So $a \sim b \iff b \sim a$, so $\sim$ is symmetric. ✓

Transitive: $a \sim b$ and $b \sim c$ means there exists $h_1, h_2 \in H$ and $k_1, k_2 \in K$ such that $h_1ak_1 = b$ and $h_2bk_2 = c$. So

$$\begin{aligned} a \sim b \text{ and } b \sim c &\iff h_1ak_1 = b \text{ and } h_2bk_2 = c \\ &\implies h_2\left(h_1ak_1\right)k_2 = c \quad \text{by substitution} \\ &\implies \left(h_2h_1\right)a\left(k_1k_2\right) = c \quad \text{by associativity in groups} \\ &\iff a \sim c \quad \text{as } h_2h_1 \in H \text{ and } k_1k_2 \in H \end{aligned}$$

So $a \sim b$ and $b \sim c \implies a \sim c$, so $\sim$ is transitive. ✓

So $\sim$ is an equivalence relation. So for $x \in G$,

$$\begin{aligned} [x] &:= \{y \in G \text{ such that } x \sim y\} \\ &= \{y \in G \text{ such that } hxk = y \text{ for some } h \in H, k \in K\} \\ &= \{hxk \text{ for some } h \in H, k \in K\} \end{aligned}$$

So the double co-sets of $H = \{(1), (123), (132)\}$ in A_4 are

$$\begin{aligned} H(1)H &= \{h_1h_2 | h_1, h_2 \in H\} \\ &= \{(1), (123), (132)\} \end{aligned}$$

and

$$\begin{aligned} &H(234)H \\ &= \{h_1(234)h_2 | h_1, h_2 \in H\} \\ &= \{(234), (234)(123), (234)(132), (123)(234), (123)(234)(123), (123)(234)(132), (132)(234), (132)(234)(123), (132)(234)(132)\} \\ &= \{(234)(13)(24), (142), (12)(34), (243), (143), (134), (124), (14)(23)\} = A_4 \setminus H \end{aligned}$$

□

Exercise 9.2. Prove that $\mathbb{C}^*$ is isomorphic to the sub-groups of $GL_2(\mathbb{R})$ consisting of matrices of the form

$$\begin{bmatrix} a & b \\ -b & a \end{bmatrix}$$

Proof. Let $\phi : \mathbb{C}^* \to \left\{\left[\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right] | a^2 + b^2 \neq 0\right\}$ be given be $a + bi \mapsto \left[\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right]$. Then ϕ forms a bijection between the sets $\mathbb{C}^*$ and $\left\{\left[\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right] | a^2 + b^2 \neq 0\right\}$.
To show the group operations are conserved, I will show $\phi(a+bi) \cdot \phi(c+di) = \phi\left((a + bi) \times (c + di)\right)$ where $\cdot$ is matrix multiplication and $\times$ is complex multiplication. So

$$\begin{aligned} \phi\left(a + bi\right) \cdot \phi\left(c + di\right) &= \begin{bmatrix} a & b \\ -b & a \end{bmatrix} \cdot \begin{bmatrix} c & d \\ -d & c \end{bmatrix} \quad \text{by definition of } \phi : \mathbb{C}^* \to \left\{\left[\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right] | a^2 + b^2 \neq 0\right\} \\ &= \begin{bmatrix} ac - bd & ad + bc \\ -\left(ad + bc\right) & ac - bd \end{bmatrix} \quad \text{by matrix multiplication} \\ &= \phi\left((ac - bd) + (ad + bc)i\right) \quad \text{by definition of } \phi : \mathbb{C}^* \to \left\{\left[\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right] | a^2 + b^2 \neq 0\right\} \\ &= \phi\left((a + bi) \times (c + di)\right) \end{aligned}$$

So $\phi(a + bi) \cdot \phi(c + di) = \phi\left((a + bi) \times (c + di)\right)$. So $(C^*, \times) \simeq \left(\left\{\left[\begin{smallmatrix} a & b \\ -b & a \end{smallmatrix}\right] | a^2 + b^2 \neq 0\right\}, \cdot\right)$. □

Exercise 9.12. Prove that S_4 is not isomorphic to D_{12}.

Proof. Although S_4 and D_{12} each have 24 elements, by Theorem 5.10, there exists $r \in D_{12}$ with $|r| = 12$, but no such element in S_4 as $|s| \leq 4$ for all $s \in S_4$. □