Moshe Mason Rubin
MATH 330 Homework #6
10 October 2016

Exercise 5.8. Show that A_{10} contains an element of order 15.

Proof. Consider $\sigma \in A_{10} \subset S_{10}$ given by $\sigma = (12345)(678)$, the product of two disjoint cycles. Then $\sigma \in A_{10}$ as σ is the product of two even permutations and Theorem 5.7 states A_{10} is a sub-group of S_{10}, therefore closed. Notice $(12345)^{-1} = (12345)^4$ and $(678)^{-1} = (678)^2$, and clearly $(12345)^{-1} \neq (678)^n$ and $(678)^{-1} \neq (12345)^m$ for any $(n, m) \in \mathbb{Z}^2$. Because $|A_{10}| = \frac{10!}{2}$ is finite, $|\sigma| \neq \infty$ as $\sigma^n \in A_{10}$ for all $n \in \mathbb{Z}$ by Theorem 5.7 that A_n is a sub-group of S_n. Then

$$\begin{aligned}
\sigma^{15} &= [(12345)(678)]^{15} \\
&= (12345)^{15}(678)^{15} \quad \text{by Proposition 5.2 (that disjoint cycles commute) and Theorem 3.8.3} \\
&= \left[(12345)^5\right]^3 \left[(678)^3\right]^5 \quad \text{by Theorem 3.8.2} \\
&= (id)^3 \, (id)^5 \\
&= id
\end{aligned}$$

So $\sigma = (12345)(678) \in A_{10}$ is an element of A_{10} of order 15. $\square$

Exercise 5.13. Let $\sigma = \sigma_1 \cdots \sigma_m \in S_n$ be the product of disjoint cycles. Prove that the order of σ is the least common multiple of the lengths of the cycles $\sigma_1, \ldots, \sigma_m$.

Proof. Let $|\sigma| = k$. So

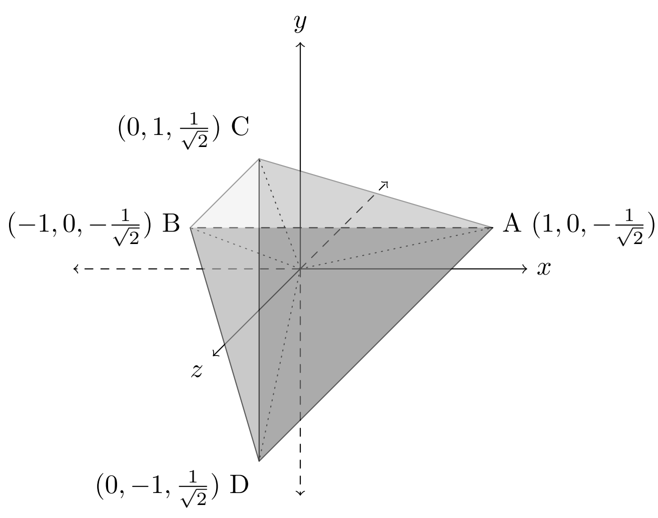
$$\begin{aligned}
\sigma^k &= (\sigma_1 \cdots \sigma_m)^k \\
&= \sigma_1^k \cdots \sigma_m^k \quad \text{by Proposition 5.2 (that disjoint cycles commute) and Theorem 3.8.3} \\
&= id \quad \text{because } \sigma^k = id \text{ as } |\sigma| = k
\end{aligned}$$

So $\sigma_i^k = id$ for $i \in ([1, m] \cap \mathbb{Z})$. So if So $\sigma_i^k = id$ then k must be a common multiple of the length of each σ_i. So the smallest k (that is, the order of σ) must be equal to the least common divisor of lengths of $\sigma_1, \ldots \sigma_m$ by definition of least common multiple. $\square$

Exercise 5.16. Find all group of rigid motions of a tetrahedron. Show that this is the same group as A_4.

Proof.

A regular tetrahedron centered at $(0, 0, 0)$ with each face an equilateral triangle of side length $\frac{\sqrt{6}}{2}$



Consider the position of face $ACD \to A'C'D'$ for each rigid motion of the tetrahedron. The point A may assume 4 distinct locations. Once A is fixed, C may assume one of 3 remaining distinct locations. Once A and C are chosen, D may assume only 1 distinct location. So the order is $4 \times 3 \times 1 = 12$. The group of rigid rotations is given by $\rho_A = \left(\begin{smallmatrix} A & B & C & D \\ A & D & B & C \end{smallmatrix}\right)$, $\rho_A^2 = \left(\begin{smallmatrix} A & B & C & D \\ A & C & D & B \end{smallmatrix}\right)$, $\rho_B = \left(\begin{smallmatrix} A & B & C & D \\ C & B & D & A \end{smallmatrix}\right)$, $\rho_B^2 = \left(\begin{smallmatrix} A & B & C & D \\ D & B & A & C \end{smallmatrix}\right)$, $\rho_C = \left(\begin{smallmatrix} A & B & C & D \\ B & D & C & A \end{smallmatrix}\right)$, $\rho_C^2 = \left(\begin{smallmatrix} A & B & C & D \\ D & A & C & B \end{smallmatrix}\right)$, $\rho_D = \left(\begin{smallmatrix} A & B & C & D \\ C & A & B & D \end{smallmatrix}\right)$, $\rho_D^2 = \left(\begin{smallmatrix} A & B & C & D \\ B & C & A & D \end{smallmatrix}\right)$, $\rho_{AB,BC} = \left(\begin{smallmatrix} A & B & C & D \\ B & A & D & C \end{smallmatrix}\right)$, $\rho_{AC,BD} = \left(\begin{smallmatrix} A & B & C & D \\ C & D & A & B \end{smallmatrix}\right)$, $\rho_{AD,BC} = \left(\begin{smallmatrix} A & B & C & D \\ D & C & B & A \end{smallmatrix}\right)$, and $id = \left(\begin{smallmatrix} A & B & C & D \\ A & B & C & D \end{smallmatrix}\right)$. By Proposition 5.8, $A_4 \subset S_4$ is of order $\frac{4!}{2} = 12$ and A_4 is given by

$$\begin{aligned}
A_4 &= \{id, (12)(13), (12)(14), (12)(34), (13)(12), (13)(14), (13)(24), (14)(12), (14)(13), (14)(23), (23)(24), (24)(23)\} \quad \text{by definition} \\
&= \{(24)(23), (23)(24), (14)(13), (13)(14), (14)(12), (12)(14), (13)(12), (12)(13), (12)(34), (13)(34), (14)(23), id\} \quad \text{by reordering} \\
&= \{(234), (243), (134), (143), (124), (142), (123), (132), (12)(34), (13)(24), (14)(23), id\} \quad \text{as } (a_i a_k)(a_i a_j) = (a_i a_k a_j).
\end{aligned}$$

Notice this matches the set A_4 as listed in Chapter 5, **Example 8.**
Since the order of the rigid motions of a tetrahedron equals the order of A_4, to show that the two groups are equivalent we must show that every rigid motion of a tetrahedron is the product even number of permutations. Label A, B, C, D as $1, 2, 3, 4$ respectively. Then

- (234) corresponds to ρ_A ((243) to ρ_A^2)
- (134) corresponds to ρ_B ((143) to ρ_B^2)
- (124) corresponds to ρ_C ((142) to ρ_C^2)
- (123) corresponds to ρ_D ((132) to ρ_D^2)
- $(12)(34)$ corresponds to $\rho_{AB,BC}$
- $(13)(24)$ corresponds to $\rho_{AC,BD}$
- $(14)(23)$ corresponds to $\rho_{AD,BC}$
- The identity id corresponds to itself

Notice every rigid motion of is the product of an even number of permutations as for each $x \in \{\text{group of rigid motions of a tetrahedron}\}$, $x \in A_4$. So the group of rigid motions of a tetrahedron is the same as A_4 as

$$\begin{aligned}\{\text{group of rigid motions of a tetrahedron}\} &= \left\{\rho_A, \rho_A^2, \rho_B, \rho_B^2, \rho_C, \rho_C^2, \rho_D, \rho_D^2, \rho_{((AB)(BC))}, \rho_{((AC)(BD))}, \rho_{((AD)(BC))}\right\} \\ &\quad \text{from way above} \\ &= \{(234), (243), (134), (143), (124), (142), (123), (132), (12)(34), (13)(24), (14)(23), id\} \\ &\quad \text{from above} \\ &= \{id, (12)(34), (13)(24), (14)(23), (123), (132), (124), (142), (134), (143), (234), (243)\} \\ &\quad \text{by reordering} \\ &= A_4 \quad \text{as listed in Chapter 5, \textbf{Example 8.} and above}\end{aligned}$$

□

Exercise 5.19. Prove that D_n is non-abelian for $n \geq 3$.

Proof. By Theorem 5.10, we know that the group D_n consists of all products of the two elements r and s satisfying the relations

$$\begin{aligned} r^n &= id \\ s^2 &= id \\ srs &= r^{-1} \end{aligned}$$

for $n \geq 3$.
Let $n \geq 3$ and label r, s such that $r^n = id$ and $s^2 = id$, which is certainly possible by Theorem 5.10. Now assume for a contradiction of D_n is abelian. Then

$$\begin{aligned} srs = (sr)s = (rs)s &\quad \text{by assumption that } D_3 \text{ is abelian} \\ = r(ss) = rs^2 &\quad \text{by associativity of elements in } D_n \text{ as } D_n \text{ is a sub-group of } S_n \text{ by Theorem 5.9} \\ = r(id) &\quad \text{by Theorem 5.15 and chose of } s \in D_n \\ = r & \end{aligned}$$

However $srs = r$ is a contradiction to Theorem 5.10 that $srs = r^{-1}$ as this would imply

$$\begin{aligned} rr^{-1} = id &\implies r(srs) = id \quad \text{by Theorem 5.10} \\ &\implies r(r) = id \quad \text{by calculation above that } srs = r \\ &\implies r^2 = id \end{aligned}$$

and $r^2 = id$ cannot happen for $r \in D_n$ for $n \geq 3$ as r is necessarily of order n and $2 < n$. So our original assumption that D_n is abelian must be false, so D_n must be non-abelian for $n \geq 3$. □

Exercise 5.23. If σ is a cycle of odd length, prove that σ^2 is also a cycle.

Proof. Let $\sigma = (\sigma_1, \ldots, \sigma_k)$ for some odd integer k. Then σ may be written as $\sigma = (\sigma_1\sigma_k)(\sigma_1\sigma_{k-1})\cdots(\sigma_1\sigma_3)(\sigma_1\sigma_2)$, a finite product of transpositions. Then

$$\begin{aligned} \sigma^2 &= \left((\sigma_1\sigma_k)(\sigma_1\sigma_{k-1})\cdots(\sigma_1\sigma_3)(\sigma_1\sigma_2)\right)^2 \\ &= [(\sigma_1\sigma_k)(\sigma_1\sigma_{k-1})\cdots(\sigma_1\sigma_3)(\sigma_1\sigma_2)]\,[(\sigma_1\sigma_k)(\sigma_1\sigma_{k-1})\cdots(\sigma_1\sigma_3)(\sigma_1\sigma_2)] \quad \text{by definition of exponentiation} \end{aligned}$$

Then σ^2 is given by $\sigma^2(\sigma_\ell) = \sigma(\sigma(\sigma_\ell)) = \sigma(\sigma_{\ell+1}) = \sigma_{\ell+2}$ for $\ell = 1, 2, \ldots, k-2$. So $\sigma^2 : \sigma_1 \mapsto \sigma_3$, and $\sigma^2 : \sigma_3 \mapsto \sigma_5$, and eventually we will arrive at $\sigma^2 : \sigma_{k-2} \mapsto \sigma_k$ as k is an odd number. Then $\sigma^2(\sigma_k) = \sigma(\sigma_1) = \sigma_2$. $\sigma^2(\sigma_\ell) = \sigma(\sigma(\sigma_\ell)) = \sigma(\sigma_{\ell+1}) = \sigma_{\ell+2}$ for $\ell = 1, 2, \ldots, k-2$. So $\sigma^2 : \sigma_2 \mapsto \sigma_4$, and $\sigma^2 : \sigma_4 \mapsto \sigma_6$, and eventually we will arrive at $\sigma^2 : \sigma_{k-3} \mapsto \sigma_{k-1}$ as k is an odd number so $k-3$ is even. Then $\sigma_{k-1} \mapsto \sigma_1$ as $\sigma_1 \mapsto \sigma_3$ as before. So $\sigma^2 = (\sigma_3, \sigma_5, \ldots, \sigma_{k-2}, \sigma_k, \sigma_2, \sigma_4, \ldots, \sigma_{k-1}, \sigma_1)$ is a cycle. □

Exercise 5.26. Prove that any element in S_n can be written as a finite product of the following permutations.

(a) $(12),(13),\ldots,(1n)$ (b) $(12),(23),\ldots,(n-1,n)$ (c) $(12),(12\ldots n)$

Proof. Let $\sigma \in S_n$.

(a) Then by Theorem 5.3, σ can be written as the product of disjoint cycles $\sigma = a_1 a_2 \cdots a_k$. For $i = 1, \ldots k$, let $a_i = (\alpha_{i_1}, \ldots, \alpha_{i_\ell})$. Then $a_i : \alpha_{i_m} \mapsto \alpha_{i_{m+1}}$ for $m = 1, \ldots, \ell - 1$ and $a_i : \alpha_{i_\ell} \mapsto \alpha_1$. Consider $a_i' = (\alpha_{i_1} a_{i_\ell})(a_{i_1} a_{i_{\ell-1}}) \cdots (a_{i_1} a_{i_3})(a_{i_1} a_{i_2})$, which is a product of $(12),(13),\ldots,(1n)$. Then $a_i' : \alpha_{i_m} \mapsto \alpha_{i_{m+1}}$ for $m = 1, \ldots, \ell - 1$ and $a_i' : \alpha_{i_\ell} \mapsto \alpha_1$. So $a_i = a_i'$ for all i. So

$$\begin{aligned} \sigma &= a_1 a_2 \cdots a_k \\ &= a_1' a_2' \cdots a_k' \quad \text{as } a_i = a_i' \\ &= ((a_{1_1} a_{1_\ell}) \cdots (a_{1_1} a_{1_2}))\,((a_{2_1} a_{2_\ell}) \cdots (a_{2_1} a_{2_2})) \cdots ((a_{k_1} a_{k_\ell}) \cdots (a_{k_1} a_{k_2})) \end{aligned}$$

which is a product of $(12),(13),\ldots,(1n)$ ☐

Exercise 6.1. Suppose that G is a finite group with an element g of order 5 and an element h of order 7. Why must $|G| \geq 35$?

Proof. Let $g = (g_1 g_2 g_3 g_4 g_5)$ and $h = (h_1 h_2 h_3 h_4 h_5 h_6 h_7)$. By Corollary 6.6, the orders of g and h, (5 and 7 respectively) must divide the number of elements in G, so $|G|$ is 35 at least, or larger. ☐

Exercise 6.3. Prove or disprove: Every sub-group of the integers has finite index.

Proof. This is false. Let $H = \{1\}$. Then H is a sub-group of $\mathbb{Z}$ and $[\mathbb{Z} : H] = \#\mathcal{L}_H = \#\{g \cdot 1 : g \in \mathbb{Z}\} = \infty$ ☐

Exercise 6.5. List the left and right co-sets of the sub-groups in each of the following.

(a) $\langle 8 \rangle$ in $\mathbb{Z}_{24}$ (b) $\langle 3 \rangle$ in $U(8)$ (d) A_4 in S_4 (f) D_4 in S_4

Solution.

(a) The left and right co-sets of $\langle 8 \rangle$ in $\mathbb{Z}_{24}$ are the same as addition is commutative in $\mathbb{Z}_{24}$. So the left and right co-set are

$$\begin{array}{ccccccc} 0+\langle 8\rangle & = & 8+\langle 8\rangle & = & 16+\langle 8\rangle & = & \{0,8,16\} \\ 1+\langle 8\rangle & = & 9+\langle 8\rangle & = & 17+\langle 8\rangle & = & \{1,9,17\} \\ 2+\langle 8\rangle & = & 10+\langle 8\rangle & = & 18+\langle 8\rangle & = & \{2,10,18\} \\ 3+\langle 8\rangle & = & 11+\langle 8\rangle & = & 19+\langle 8\rangle & = & \{3,11,19\} \\ 4+\langle 8\rangle & = & 12+\langle 8\rangle & = & 20+\langle 8\rangle & = & \{4,12,20\} \\ 5+\langle 8\rangle & = & 13+\langle 8\rangle & = & 21+\langle 8\rangle & = & \{5,13,21\} \\ 6+\langle 8\rangle & = & 14+\langle 8\rangle & = & 22+\langle 8\rangle & = & \{6,14,22\} \\ 7+\langle 8\rangle & = & 15+\langle 8\rangle & = & 23+\langle 8\rangle & = & \{6,14,22\} \end{array}$$

(b) The left and right co-sets of $\langle 3 \rangle$ in $U(8)$ are the same as multiplication is commutative in $\mathbb{Z}_8$. $U(8) = \{1,3,5,7\}$ and $\langle 3 \rangle = \{1,3\}$, so the left and right co-sets are:

$$\begin{aligned} 1 \cdot \{3,1\} &= \{3,1\} \\ 3 \cdot \{3,1\} &= \{1,3\} \\ 5 \cdot \{3,1\} &= \{7,5\} \\ 7 \cdot \{3,1\} &= \{5,7\} \end{aligned}$$

(d) The order of A_4 in S_4 is 2, so the left co-sets equals the right co-sets. So the left and right co-sets of

$$A_4 = \{(234),(243),(134),(143),(124),(142),(123),(132),(12)(34),(13)(24),(14)(23),id\}$$

are

$$\begin{aligned} A_4 &= \{(234),(243),(134),(143),(124),(142),(123),(132),(12)(34),(13)(24),(14)(23),id\} \\ (12)A_4 &= \{(1234),(1243),(1342),(1432),(24),(14),(23),(34),(1324),(1423),(12)\} \end{aligned}$$

(f) From Chapter 5 **Example 9.**, $D_4 = \{(1234),(13)(24),(1432),id,(24),(13),(12)(34),(14)(32)\}$. So the left co-sets are

$$\begin{aligned} D_4 &= \{(1234),(13)(24),(1432),id,(24),(13),(12)(34),(14)(32)\} \\ (12)D_4 &= \{(12),(234),(2413),(143),(34),(1423),(132),(124)\} \\ (14)D_4 &= \{(14),(123),(1342),(243),(1243),(23),(134),(142)\} \end{aligned}$$

☐

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) $Hg_1^{-1} = Hg_2^{-1}$ (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):**

$$\begin{aligned}g_1 H \ = g_2 H &\iff g_1 \sim_{H,L} g_2, \quad \text{as } [x]_{\sim_{H,L}} = xH \\ &\iff g_1^{-1} g_2 \in H \quad \text{by definition of } \sim_{H,L} \\ &\iff g_1^{-1} \sim_{H,R} g_2^{-1} \quad \text{by definition of } \sim_{H,R} \\ &\iff Hg_1^{-1} = Hg_2^{-1}, \quad \text{as } [x]_{\sim_{H,R}} = Hx\end{aligned} \tag{1}$$

So $g_1 H = g_2 H \iff Hg_1^{-1} = Hg_2^{-1}$. □

(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):**

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

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

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

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 $\phi(a+bi) \cdot \phi(c+di) = \phi((a + bi) \times (c + di))$ where $\cdot$ is matrix multiplication and $\times$ is complex multiplication. So

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

So $\phi(a + bi) \cdot \phi(c + di) = \phi((a + bi) \times (c + di))$. 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 $s \in S_4$. □

Moshe Mason Rubin
MATH 330 Homework #8
7 November 2016

Exercise 9.9. Let $G = \mathbb{R} \setminus \{-1\}$ and define a binary operation on G by

$$a * b = a + b + ab.$$

Prove that G is a group under this operation. Show that $(G, *)$ is isomorphic to the multiplicative group of nonzero real numbers.

Proof. By **Exercise 3.7** from homework #2, $(G, *)$ is an abelian group.
The map $\phi : G \to \mathbb{R}^*$ given by $\phi(x) = 1 + x$ is clearly a bijection and well defined on each set. ϕ preserves group operations as for any $a, b \in G$,

$$\begin{aligned} \phi(a) \cdot \phi(b) &= (1 + a) \cdot (1 + b) \quad \text{by definition of } \phi \\ &= 1 + b + a + ab = a + b + ab + 1 \\ &= \phi(a + b + ab) \quad \text{by definition of } \phi \\ &= \phi(a * b) \quad \text{by definition of } * \end{aligned}$$

So $(G, *) \simeq (\mathbb{R}^*, \cdot)$. $\square$

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

Proof. Consider $(1, 12, 11, 10, 9, 8, 7, 6, 5, 4, 3, 2) \in D_{12}$ which has order 12. Because every element of S_4 has order less than or equal to 4, the two groups cannot be isomorphic by Theorem from class that $\operatorname{ord}[\phi(g_1)] = \operatorname{ord}(g_1)$. $\square$

Exercise 9.14. Show that the set of all matrices of the form $\left[\begin{smallmatrix} \pm 1 & k \\ 0 & 1 \end{smallmatrix}\right]$ is isomorphic to D_n where all entries in the matrix are in $\mathbb{Z}_n$.

Proof. Let $S = \left\{\left[\begin{smallmatrix} \pm 1 & k \\ 0 & 1 \end{smallmatrix}\right] : k \in \mathbb{Z}_n\right\}$. Notice for any $\left[\begin{smallmatrix} \pm 1 & k \\ 0 & 1 \end{smallmatrix}\right] \in S$, we have

$$\begin{bmatrix} \pm 1 & k \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & k \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \pm 1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^k \begin{bmatrix} \pm 1 & 0 \\ 0 & 1 \end{bmatrix}$$

and $\left[\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right]^2 = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$. So $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$ and $\left[\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$ generate S. Furthermore, $\left[\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right]$ has order n, and $\left[\begin{smallmatrix} -1 & 0 \\ 0 & 1 \end{smallmatrix}\right]$ has order 2, and

$$\begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & -1 \\ 0 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}^{-1}$$

By Theorem 5.10, D_n is generated by all the products of $r, s \in D_n$ such that $r^n = s^2 = id$ and $srs = r^{-1}$. Define $f : S \to D_n$ by $f\left(\left[\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix}\right]\right) = r^k$ and $f\left(\left[\begin{smallmatrix} -1 & k \\ 0 & 1 \end{smallmatrix}\right]\right) = r^k s$. To check that f preserves group operations, there are four cases to check:

1. $f\left(\left[\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 & \ell \\ 0 & 1 \end{smallmatrix}\right]\right) = f\left(\left[\begin{smallmatrix} 1 & k+\ell \\ 0 & 1 \end{smallmatrix}\right]\right) = r^{k+\ell} = r^k r^\ell = f\left(\left[\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix}\right]\right) \cdot f\left(\left[\begin{smallmatrix} 1 & \ell \\ 0 & 1 \end{smallmatrix}\right]\right)$. ✓
2. $f\left(\left[\begin{smallmatrix} -1 & k \\ 0 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 & \ell \\ 0 & 1 \end{smallmatrix}\right]\right) = f\left(\left[\begin{smallmatrix} -1 & k-\ell \\ 0 & 1 \end{smallmatrix}\right]\right) = r^{k-\ell} s = r^k r^{-\ell} s = \cdots = \cdots = f\left(\left[\begin{smallmatrix} -1 & k \\ 0 & 1 \end{smallmatrix}\right]\right) \cdot f\left(\left[\begin{smallmatrix} 1 & \ell \\ 0 & 1 \end{smallmatrix}\right]\right)$. ✓
3. $f\left(\left[\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} -1 & \ell \\ 0 & 1 \end{smallmatrix}\right]\right) = f\left(\left[\begin{smallmatrix} -1 & k+\ell \\ 0 & 1 \end{smallmatrix}\right]\right) = r^{k+\ell} s = r^k r^\ell s = r^k \left(r^\ell s\right) = f\left(\left[\begin{smallmatrix} 1 & k \\ 0 & 1 \end{smallmatrix}\right]\right) \cdot f\left(\left[\begin{smallmatrix} -1 & \ell \\ 0 & 1 \end{smallmatrix}\right]\right)$. ✓
4. $f\left(\left[\begin{smallmatrix} -1 & k \\ 0 & 1 \end{smallmatrix}\right]\left[\begin{smallmatrix} -1 & \ell \\ 0 & 1 \end{smallmatrix}\right]\right) = f\left(\left[\begin{smallmatrix} 1 & k-\ell \\ 0 & 1 \end{smallmatrix}\right]\right) = r^{k-\ell} = r^k r^{-\ell} = r\,(srs)^\ell \cdots = \cdots = f\left(\left[\begin{smallmatrix} -1 & k \\ 0 & 1 \end{smallmatrix}\right]\right) \cdot f\left(\left[\begin{smallmatrix} 1 & \ell \\ 0 & 1 \end{smallmatrix}\right]\right)$. ✓

$\square$

Exercise 10.2. Find all the sub-groups of D_4. Which sub-groups are normal? What are all the factors groups of D_4 up to isomorphisms?

Proof. The sub-groups are $D_4 = \left\{id, \rho, \rho^2, \rho^3, s, \rho s, \rho^2 s, \rho^3 s\right\} = \{id, (1234), (13)(24), (1432), (24), (12)(34), (13), (14)(23)\}$ are

1. $\{id\}$
2. $\{id, \rho^2\}$
3. $\{id, s\}$
4. $\{id, \rho s\}$
5. $\{id, \rho^2 s\}$
6. $\{id, \rho^3 s\}$
7. $\{id, \rho, \rho^2, \rho^3\}$
8. $\{id, \rho^2, s, \rho^2 s\}$
9. $\{id, \rho^2, \rho s, \rho^3 s\}$
10. D_4

1. $\{id\}$ is normal.
2. $\{id, \rho^2\}$ is normal as $(1234)\{id, \rho^2\} = \{(1234), (1432)\} = \{id, \rho^2\}(1234)$ and $(24)\{id, \rho^2\} = \{(24), (13)\} = \{id, \rho^2\}(24)$ and $(12)(34)\{id, \rho^2\} = \{(12)(34), (14)(23)\} = \{id, \rho^2\}(12)(34)$. ✓
3. $\{id, s\}$ is not normal as $(1234)\{id, s\} = \{(1234), (12)(34)\} \neq \{(1234), (14)(23)\} = \{id, s\}(1234)$.
4. $\{id, \rho s\}$ is not normal as $(1234)\{id, \rho s\} = \{(1234), (13)\} \neq \{(1234), (24)\} = \{id, \rho s\}(1234)$
5. $\{id, \rho^2 s\}$ is not normal as $\rho \circ (\rho^2 s) = \rho^3 s \neq \rho s = (\rho^2 s) \circ \rho$.
6. $\{id, \rho^3 s\}$ is not normal as $\rho \circ (\rho^3 s) = s \neq \rho^2 s = (\rho^3 s) \circ \rho$.
7. $\{id, \rho, \rho^2, \rho^3\}$ is normal as $s\{id, \rho, \rho^2, \rho^3\} = \{s, \rho^3 s, \rho^2 s, \rho s\} = \{id, \rho, \rho^2, \rho^3\}s$. ✓
8. $\{id, \rho^2, s, \rho^2 s\}$ is normal as $\rho\{id, \rho^2, s, \rho^2 s\} = \{\rho, \rho^3, \rho s, \rho^3 s\} = \{id, \rho^2, s, \rho^2 s\}\rho$. ✓
9. $\{id, \rho^2, \rho s, \rho^3 s\}$ is normal as $\rho\{id, \rho^2, \rho s, \rho^3 s\} = \{\rho, \rho^3, \rho^2 s, s\}$. ✓
10. D_4 is normal.

2. The factor group $D_4/\{id, \rho^2\} = \{\{id, \rho^2\}, \{\rho, \rho^3\}, \{s, \rho^2 s\}, \{\rho s, \rho^3 s\}\}$.
7. The factor group $D_4/\{id, \rho, \rho^2, \rho^3\} = \{\{id, \rho, \rho^2, \rho^3\}, \{s, \rho^3 s, \rho^2 s, \rho s\}\}$.
8. $D_4/\{id, \rho^2, s, \rho^2 s\} = \{\{id, \rho^2, s, \rho^2 s\}, \{\rho, \rho^3, \rho s, \rho^3 s\}\}$.
9. $D_4/\{id, \rho^2, \rho s, \rho^3 s\} = \{\{id, \rho^2, \rho s, \rho^3 s\}, \{\rho, \rho^3, \rho^2 s, s\}\}$.

□

Exercise 10.7. Prove or disprove: If H is a normal sub-group of G such that H and G/H are abelian, then G is abelian.

Counterexample. Let $G = S_3$ and $H = A_3$. S_3 is non-abelian. By Corollary 9.4, $A_3 \simeq \mathbb{Z}_3$, so A_3 *is* abelian. We must show A_3 is normal and S_3/A_3 is abelian:
A_3 is normal as for any $\sigma \in S_3$, $\sigma A_3 \sigma^{-1}$ is even whether σ is even or odd. So $\sigma A_3 \sigma^{-1} \subseteq A_3$, so A_3 is normal by Theorem 10.1.2. ✓
To show S_3/A_3 is abelian, notice by Lagrange's Theorem, $[S_3 : A_3] = \frac{|S_3|}{|A_3|} = \frac{6}{3} = 2$. By Theorem 10.2, $|S_3/A_3| = [S_3 : A_3]$. By Corollary 9.4, since $|S_3/A_3| = 2$ and 2 is prime, $S_3/A_3 \simeq \mathbb{Z}_2$, so S_3/A_3 is abelian. ✓ □

Exercise 10.11. If a group G has exactly one sub-group H of order k, prove that H is normal in G.

Proof. By **Exercise 3.54** from homework #4, gHg^{-1} is a sub-group of G. By the assumption that H is the only sub-group of G, we have that $H = gHg^{-1}$. By Theorem 10.1.3, $H = gHg^{-1} \implies H$ is a normal subgroup of G. □

Exercise 10.12. Define the ***centralizer*** of an element g in a group G to be the set

$$C(g) = \{x \in G : xg = gx\}.$$

Show that $C(g)$ is a sub-group of G. If g generates a normal sub-group of G, prove that $C(g)$ is normal in G.

Proof. For $C(g) \subseteq G$ to be a sub-group of G, it is sufficient to show

1. For all $a, b \in C(g)$, $a \circ b \in C(g)$.
2. There exists $e \in C(g)$ such that $a \circ e = a = e \circ a$ for all $a \in C(g)$.
3. For all $a \in C(g)$ there exists $a^{-1} \in C(g)$ such that $a \circ a^{-1} = e = a^{-1} \circ a$.

1. Consider $a, b \in C(g)$. Then $a, b \in G$ as $C(g) \subseteq G$. Then

$$\begin{aligned}
(ab)x &= a(bx) && \text{by associativity of elements of } G \\
&= a(xb) && \text{by assumption that } b \in C(g) \\
&= (ax)b && \text{by associativity of elements of } G \\
&= (xa)b && \text{by assumption that } a \in C(g) \\
&= x(ab) && \text{by associativity of elements of } G
\end{aligned}$$

   So $ab \in C(g)$. ✓

2. Because $e \in G$ by definition commutes with every element of G, $e \in C(g)$. ✓

3. Consider $c \in C(g)$. Then $c \in G$ and $c^{-1} \in G$ as G is a group and $C(g) \subseteq G$. Then

$$\begin{aligned}
c \in C(g) &\implies cx = xc \\
&\implies c^{-1}cxc^{-1} = c^{-1}xcc^{-1} \quad \text{by left and right multiplying by } c^{-1} \\
&\implies xc^{-1} = c^{-1}x \quad \text{by condensing the “}c^{-1}c\text{” and “}cc^{-1}\text{” terms}
\end{aligned}$$

   So $c \in C(g) \implies c^{-1} \in C(g)$. ✓

So $C(g)$ is a sub-group of G.
Because $C(g)$ us clearly abelian, it follows that the left and right co-sets must be equal, and $C(g)$ must be normal. □

Exercise 11.2. Which of the following maps are homomorphisms? If the map is a homomorphism, what is the kernel?

(a) $\phi : \mathbb{R}^* \to GL_2(\mathbb{R})$ defined by

$$\phi(a) = \begin{bmatrix} 1 & 0 \\ 0 & a \end{bmatrix}$$

(b) $\phi : \mathbb{R} \to GL_2(\mathbb{R})$ defined by

$$\phi(a) = \begin{bmatrix} 1 & 0 \\ a & 1 \end{bmatrix}$$

(c) $\phi : GL_2(\mathbb{R}) \to \mathbb{R}$ defined by

$$\phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = a + d$$

(d) $\phi : GL_2(\mathbb{R}) \to \mathbb{R}^*$ defined by

$$\phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = ad - bc$$

(e) $\phi : \mathbb{M}_2(\mathbb{R}) \to \mathbb{R}$ defined by

$$\phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = b$$

Proof.

(a) ϕ is a homomorphism as for $a, b \in \mathbb{R}^*$,

$$\phi(a)\phi(b) = \begin{bmatrix} 1 & 0 \\ 0 & a \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 0 & b \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 0 & ab \end{bmatrix} = \phi(ab)$$

and $\ker \phi := \{x \in \mathbb{R}^* \text{ such that } \phi(x) = id\} = \{1\}$. □

(b) ϕ is not a homomorphism as

$$\phi(a)\phi(b) = \begin{bmatrix} 1 & 0 \\ a & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ b & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ a+b & 1 \end{bmatrix} \neq \phi(ab).$$

□

(c) ϕ is not a homomorphism as

$$\phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}\right) = \phi\left(\begin{bmatrix} a\alpha + b\gamma & a\beta + b\delta \\ c\alpha + d\gamma & c\beta + d\delta \end{bmatrix}\right) = a\alpha + b\gamma + c\beta + d\delta \neq a\alpha + a\delta + d\alpha + d\delta = \phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right)\phi\left(\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}\right).$$

(d) ϕ is a homomorphism as

$$\begin{aligned}\phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}\right) = \phi\left(\begin{bmatrix} a\alpha + b\gamma & a\beta + b\delta \\ c\alpha + d\gamma & c\beta + d\delta \end{bmatrix}\right) &= (a\alpha + b\gamma)(c\beta + d\delta) - (a\beta + b\delta)(c\alpha + d\gamma) \\ &= ac\alpha\beta + ad\alpha\delta + bc\beta\gamma + bd\gamma\delta - ac\alpha\beta - ad\beta\gamma - bc\alpha\delta - bd\gamma\delta \\ &= ad\alpha\delta + bc\beta\gamma - ad\beta\gamma - bc\gamma\delta \\ &= (ad - bc)(\alpha\delta - \beta\gamma) = \phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right)\phi\left(\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}\right)\end{aligned}$$

and $\ker\phi := \{M \in GL_2(\mathbb{R}) \text{ such that } \phi(A) = 1\} = SL_2(\mathbb{R})$. □

(e) ϕ is not a homomorphism as

$$\phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}\right) = \phi\left(\begin{bmatrix} a\alpha + b\gamma & a\beta + b\delta \\ c\alpha + d\gamma & c\beta + d\delta \end{bmatrix}\right) = a\beta + b\delta \neq b\beta = \phi\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right)\phi\left(\begin{bmatrix} \alpha & \beta \\ \gamma & \delta \end{bmatrix}\right).$$ □

Exercise 11.17. If H and K are normal sub-groups of G and $H \cap K = \{e\}$, prove that G is isomorphic to a sub-group of $G \setminus H \times G \setminus K$.

Proof. content... □

Homework exercises I cited:

Exercise 3.7 Let $S = \mathbb{R} \setminus \{-1\}$ and define a binary operation on S by $a * b = a + b + ab$. Prove that $(S, *)$ is an abelian group. An *abelian group* is a group G such that $a * b = b * a$ for all $a, b \in G$.

Associative For all $a, b, c \in G$, $(a * b) * c = a * (b * c)$.

$$\begin{aligned}(a * b) * c &= (a * b) + c + (a * b)c \quad \text{by definition of } a * b \\ &= (a + b + ab) + c + (a + b + ab)c \quad \text{by definition of } a * b \\ &= a + b + c + ab + ac + bc + abc \\ &= a + (b + c + bc) + a(b + c + bc) \\ &= a + (b * c) + a(b * c) \quad \text{by definition of } a * b \\ &= a * (b * c) \quad \text{by definition of } a * b\end{aligned}$$

Identity element There exists an element $e \in G$ such that for any $a \in G$, $e * a = a * e = a$.
For any a, let $b = 0$. Then $a * b = a + 0 + a(0) = a = 0 + a + 0(a) = b * a$. So $b = 0$ is the identity element such that $a * 0 = 0 * a$ for all $a \in G$.

Inverse element For each element $a \in G$ there exists an $a^{-1} \in G$ such that $a * a^{-1} = a^{-1} * a = e$.
We know from above that $e = 0$. So given $a \in G$,

$$\begin{aligned}a + b + ab &= 0 \\ \implies b(1 + a) + a &= 0 \\ \implies b &= \frac{-a}{1 + a}\end{aligned}$$

which is defined for all $x \in S$. So $b = \frac{-a}{1+a}$ is the unique inverse element a^{-1} to each a such that $a * a^{-1} = a^{-1} * a = e$.

Commutative For all $a, b \in G$, $a * b = b * a$.

$$\begin{aligned} a * b &= a + b + ab \\ &= b + a + ab \quad \text{by commutative property of addition} \\ &= b + a + ba \quad \text{by commutative property of multiplication} \\ &= b * a \quad \text{by definition} \end{aligned}$$

So $(S, *)$ is an abelian group. □

Exercise 3.54. Let H be a sub-group of G. If $g \in G$, show that $gHg^{-1} := \left\{g^{-1}hg : h \in H\right\}$ is also a sub-group of G.

Proof. By theorem from class, for $gHg^{-1} \subseteq G$ to be a sub-group of G, it is sufficient to show

1. For all $a, b \in gHg^{-1}$, $a \circ b \in gHg^{-1}$.
2. There exists $e \in gHg^{-1}$ such that $a \circ e = a = e \circ a$ for all $a \in gHg^{-1}$.
3. For all $a \in gHg^{-1}$ there exists $a^{-1} \in gHg^{-1}$ such that $a \circ a^{-1} = e = a^{-1} \circ a$.

Notice that gHg^{-1} is necessarily a subset of G as every element in H is contained in G (by assumption that H is a sub-group of G). So $g, h, g^{-1} \in G$. Furthermore, every element in gHg^{-1} is of the form $g^{-1}hg$, and G is closed by assumption that G is a group. So $gHg^{-1} \subseteq G$.
Let $a, b \in gHg^{-1}$. Then $a = g^{-1}h_a g$ and $b = g^{-1}h_b g$ for some $h_a, h_b \in H$.

1. Consider

$$\begin{aligned} ab &= \left(g^{-1}h_a g\right)\left(g^{-1}h_b g\right) \\ &= \left(g^{-1}h_a\right)\left(gg^{-1}\right)\left(h_b g\right) \quad \text{by associativity of elements of } G \\ &= \left(g^{-1}h_a\right)(e)\left(h_b g\right) \quad \text{by definition of } g^{-1} \\ &= \left(g^{-1}h_a\right)\left(h_b g\right), \quad \text{by definition of } e \\ &= g^{-1}\left(h_a h_b\right) g \quad \text{by associativity of elements of } G \end{aligned}$$

and $(h_a h_b) \in H$ as H was assumed to be a sub-group, so H is closed. So $ab = g^{-1}\left(h_a h_b\right) g$ is of the form $g^{-1}hg$ for some $h \in H$. So gHg^{-1} is closed.

2. By assumption that H is a sub-group of G, $e \in H$. So $\left(g^{-1}eg\right) \in gHg^{-1}$ and

$$\begin{aligned} g^{-1}eg &= g^{-1}g \quad \text{by definition of } e \\ &= e, \quad \text{by definition of } g^{-1}. \end{aligned}$$

So $\left(g^{-1}eg\right) \in gHg^{-1}$ and $g^{-1}eg = e$. so $e \in gHg^{-1}$.

3. By Proposition 3.4, if $a = g^{-1}h_a g$ then $a^{-1} = g^{-1}h_a^{-1}g$. So $a^{-1} \in gHg^{-1}$ if $h_a^{-1} \in H$, and h_a^{-1} is necessarily an element of H by assumption that H is a sub-group of G. So $a \in gHg^{-1} \implies a^{-1} \in gHg^{-1}$.

So this shows that gHg^{-1} is a sub-group of G. □

Moshe Mason Rubin
MATH 330 Homework #9
23 November 2016

Exercise 11.10. If $\phi : G \to H$ is a group homomorphism and G is cyclic, prove that $\phi(G)$ is also cyclic.

Proof. Let γ be a generator for G. Then for each $g \in G$, $g = \gamma^n$ for some $n \in \mathbb{N}$. Then

$$\begin{aligned}\phi(g) &= \phi(\gamma^n) \quad \text{because } \gamma \text{ generates } G \\ &= \phi\left(\underbrace{\gamma \cdot \gamma \cdot \ldots \cdot \gamma}_{n \text{ times}}\right) \\ &= \underbrace{\phi(\gamma) \circ \phi(\gamma) \circ \cdots \circ \phi(\gamma)}_{n \text{ times}} \quad \text{as } \phi \text{ is a homomorphism so } \phi(g_1 \cdot g_2) = \phi(g_1) \circ \phi(g_2) \\ &= \phi^n(\gamma)\end{aligned}$$

So for all $\phi(g) \in \phi(G)$, we have $\phi(g) = \phi^n(\gamma)$ for some $n \in \mathbb{N}$. So $\phi(\gamma)$ generates $\phi(G)$; so $\phi(G)$ is cyclic. □

Lemma 11.1. *If G_1, G_2 are groups with an isomorphism $\phi : G_1 \to G_2$ and there exists $g_1 \in G_1$ such that* $\operatorname{ord}(g_1) = n$ *for some $n \in \mathbb{N}$. Then* $\operatorname{ord}(\phi(g_1)) = n$.

Proof. If $g_1^n = e_1$ then

$$\begin{aligned}e_2 &= \phi(e_1) \quad \text{by Proposition 1.11.1} \\ &= \phi(g_1^n) \quad \text{because } \operatorname{ord}(g_1) = n \\ &= \phi^n(g_1) \quad \text{because } \phi \text{ is an isomorphism}\end{aligned}$$

So $\operatorname{ord}(\phi(g_1)) = n$. □

Exercise 11.14. Prove or disprove: $\mathbb{Q}/\mathbb{Z} \simeq \mathbb{Q}$.

Proof. Consider $\frac{1}{2} + \mathbb{Z} \in \mathbb{Q}/\mathbb{Z}$ which has order 2 as $\left(\frac{1}{2} + \mathbb{Z}\right) + \left(\frac{1}{2} + \mathbb{Z}\right) = 1 + \mathbb{Z} \equiv \mathbb{Z}$ and $\mathbb{Z}$ is the identity in $\mathbb{Q}/\mathbb{Z}$. Consider for a contradiction that there exists a non-zero $q \in \mathbb{Q}$ with order 2. That is, $q + q = 0 \iff 2q = 0$ which has no solution in $\mathbb{Q} \setminus \{0\}$. So there is no element of order 2 in $\mathbb{Q}$. So by Lemma 11.1, the two groups cannot be isomorphic. □

Exercise 11.5 (Addition Exercises: Automorphism #5)**.** Let G be a group and i_g be an inner automorphism of G, and define a map

$$\psi : G \to \operatorname{Aut}(G)$$

by

$$g \mapsto i_g.$$

Prove that this map is a homomorphism with image $\operatorname{Inn}(G)$ and kernel $Z(G)$. Use this result to conclude that

$$G/Z(G) \simeq \operatorname{Inn}(G).$$

Proof. Recall

$$\begin{aligned}\operatorname{Aut}(G) &:= \{\text{all isomorphisms } \phi : G \to G\} \\ \text{Given } g \in G, \quad i_g : G \to G &\text{ by } \quad x \mapsto gxg^{-1} \\ \operatorname{Inn}(G) &:= \{i_g \text{ for all } g \in G\} \\ Z(G) &:= \{x \in G : gx = xg \text{ for all } g \in G\}\end{aligned}$$

ψ is a homomorphism as

$$\begin{aligned}\psi(g_1 \cdot g_2) &= i_{g_1 \cdot g_2}(x) \quad \text{by definition of } \psi \\ &= (g_1 \cdot g_2) \cdot (x) \cdot (g_1 \cdot g_2)^{-1} \quad \text{by definition of } i_g \\ &= (g_1 \cdot g_2) \cdot (x) \cdot \left(g_2^{-1} \cdot g_1^{-1}\right) \\ &= g_1 \cdot \left(g_2 \cdot x \cdot g_2^{-1}\right) \cdot g_1^{-1} \quad \text{because } G \text{ is a group so elements associate} \\ &= g_1 \cdot (i_{g_2}(x)) \cdot g_1^{-1} \quad \text{by definition of } i_g \\ &= (i_{g_1} \circ i_{g_2})(x) \quad \text{by definition of } i_g\end{aligned}$$

So ψ is a homomorphism.
The image of ψ is clearly $\operatorname{Inn}(G)$ as $\operatorname{Im}(\psi) := \{\psi(g) \text{ for all } g \in G\} = \{i_g \text{ for all } g \in G\} =: \operatorname{Inn}(G)$.
$\ker(\psi) := \{g \in G : \psi(g) = id\}$ and $\psi(g) = id \iff gxg^{-1} = x \iff gx = xg$. So $\ker(\psi) = Z(G)$.
By the First Isomorphism Theorem, $G/\ker(\psi) \simeq \operatorname{Im}(\psi)$, so we have $G/Z(G) \simeq \operatorname{Inn}(G)$. □

Exercise 13.3. Find all of the abelian groups of order 720 up to isomorphism.

Solution. $720 = 2^4 \cdot 3^2 \cdot 5$, so, by The Fundamental Theorem of Finite Abelian Groups, all of the abelian groups of order 720 up to isomorphism are:

1. $\mathbb{Z}_2^4 \times \mathbb{Z}_3^2 \times \mathbb{Z}_5$
2. $\mathbb{Z}_4 \times \mathbb{Z}_2^2 \times \mathbb{Z}_3^2 \times \mathbb{Z}_5$
3. $\mathbb{Z}_4^2 \times \mathbb{Z}_3^2 \times \mathbb{Z}_5$
4. $\mathbb{Z}_8 \times Z_2 \times \mathbb{Z}_3^2 \times \mathbb{Z}_5$
5. $\mathbb{Z}_{16} \times \mathbb{Z}_3^2 \times \mathbb{Z}_5$
6. $\mathbb{Z}_2^4 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
7. $\mathbb{Z}_4 \times \mathbb{Z}_9 \times \mathbb{Z}_3^2 \times \mathbb{Z}_5$
8. $\mathbb{Z}_4^2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
9. $\mathbb{Z}_8 \times Z_2 \times \mathbb{Z}_9 \times \mathbb{Z}_5$
10. $\mathbb{Z}_{16} \times \mathbb{Z}_9 \times \mathbb{Z}_5$ □

Exercise 13.5. Show that the infinite direct product $G = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \cdots$ is not finitely generated.

Proof. Suppose for a contradiction that G is finitely generated and has n generators. Because G is abelian and every element is of order 2, so $|G| \leq 2^n$, which is a contradiction to the assumption that G is infinite. □

Exercise 13.14. Let G be a solvable group. Prove that any sub-group of G is also solvable.

Proof. content... □

Exercise 14.2. Computer all the X_g and all G_x for each of the following permutation groups.

(a) $X = \{1, 2, 3\}$,
$G = S_3 = \{(1), (12), (13), (23), (123), (132)\}$

(b) $X = \{1, 2, 3, 4, 5, 6\}$,
$G = \{(1), (12), (345), (354), (12)(345), (12)(354)\}$

Solution. Recall $X_g := \{x \in X \text{ such that } gx = x\}$ and $G_x := \{g \in G \text{ such that } gx = x\}$

(a)
- $X_{(1)} = X$
- $X_{(12)} = \{3\}$
- $X_{(13)} = \{2\}$
- $X_{(23)} = \{1\}$
- $X_{(123)} = X_{(132)} = \emptyset$
- $G_1 = \{(1), (23)\}$
- $G_2 = \{(1), (13)\}$
- $G_3 = \{(1), (12)\}$

(b)
- $X_{(1)} = X$
- $X_{(12)} = \{3, 4, 5, 6\}$
- $X_{(345)} = X_{(354)} = \{1, 2, 6\}$
- $X_{(12)(345)} = X_{(12)(354)} = \{6\}$
- $G_1 = G_2 = \{(345), (354)\}$
- $G_3 = G_4 = G_5 = \{(1), (12)\}$
- $G_6 = G$

□

Exercise 14.5. Let $G = A_4$ and suppose that G acts on itself by conjugation; that is, $(g, h) \mapsto ghg^{-1}$.

(a) Determine the conjugacy classes (orbits) of each element of G.

(b) Determine all the isotropy sub-groups for each element of G.

Proof. Recall if $\sigma = (\sigma_1, \ldots, \sigma_n)$ and $\tau = (\tau_1, \ldots, \tau_n)$ are permutations then $\tau\sigma\tau^{-1} = (\tau(\sigma_1), \ldots, \tau(\sigma_n))$.

(a) $A_4 = \{(234), (243), (134), (143), (124), (142), (123), (132), (12)(34), (13)(24), (14)(23), id\}$, so

- $\mathcal{O}_{id} = \{id\}$
- $\mathcal{O}_{(234)} = \{(234), (423), (241), (213), (431), (132), (314), (124), (143), (412), (321), (234)\} = \{(234), (124), (132), (143)\}$
- $\mathcal{O}_{(243)} = \{(324), (243), (214), (231), (413), (123), (341), (142), (134), (421), (312), (243)\} = \{(243), (142), (123), (134)\}$

- $\mathcal{O}_{(12)(34)} = \{(13)(42), (14)(23), (32)(41), (42)(13), (24)(31), (41)(32), (23)(14), (31)(24), (12)(34), (43)(12), (43)(12), (12)(34)\} = \{(13)(24), (14)(23), (12)(34)\}$

(b) Recall given an element $x \in G$, G_x is the isotropy sub-group defined by $G_x := \{g \in G \text{ such that } gx = x\}$

□

Exercise 16.1. Which of the following sets are rings with respect to the usual operations of addition and multiplication? If the set is a ring, is it also a field?

(b) $\mathbb{Z}_{18}$

(c) $\mathbb{Q}\left(\sqrt{2}\right) = \left\{a + b\sqrt{2} : a, b \in \mathbb{Q}\right\}$

(d) $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) = \left\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\right\}$

(e) $\mathbb{Z}\left[\sqrt{3}\right] = \left\{a + b\sqrt{3} : a, b \in \mathbb{Z}\right\}$

(f) $R = \left\{a + b\sqrt[3]{3} : a, b \in \mathbb{Q}\right\}$

Proof.

(b) $\mathbb{Z}_{18}$ is a ring; however it is not a field because not every every element has an inverse.

(c) $\mathbb{Q}\left(\sqrt{2}\right) = \left\{a + b\sqrt{2} : a, b \in \mathbb{Q}\right\}$ is both a ring and a field: the inverse of any given $a + b\sqrt{2} \in \mathbb{Q}\left(\sqrt{2}\right)$ is given by $\frac{a}{a^2-2b^2} + \frac{b}{2b^2-a^2}\sqrt{2}$. Notice this is always well defined except when $a^2 - 2b^2 = 0$, which cannot be the case because $a, b \in \mathbb{Q}$.

(d) $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right) = \left\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} : a, b, c, d \in \mathbb{Q}\right\}$ is a ring but not a field. $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$ is closed as one can check that

$$\begin{aligned}\left(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}\right)\left(\alpha + \beta\sqrt{2} + \gamma\sqrt{2} + \delta\sqrt{2}\right) &= (a\alpha + 2b\beta + 3c\gamma + 6d\delta) + (b\alpha + a\beta + 3d\gamma + 3c\delta)\sqrt{2} \\ &\quad + (c\alpha + 2d\beta + a\gamma + 2b\delta)\sqrt{3} + (d\alpha + c\beta + b\gamma + a\delta)\sqrt{6} \\ &\in \mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)\end{aligned}$$

However, $\mathbb{Q}\left(\sqrt{2}, \sqrt{3}\right)$ is not closed under inverses so it is not a field.

(e) $\mathbb{Z}\left[\sqrt{3}\right] = \left\{a + b\sqrt{3} : a, b \in \mathbb{Z}\right\}$ is a ring but not a field.

(f) $R = \left\{a + b\sqrt[3]{3} : a, b \in \mathbb{Q}\right\}$ is a ring but not a field. □

Exercise 16.2. Let R be the ring of 2×2 matrices of the form

$$\begin{bmatrix} a & b \\ 0 & 0 \end{bmatrix},$$

where $a, b \in \mathbb{R}$. Show that although R is a ring that has no identity, we can find a sub-ring S of R with an identity.

Proof. Consider $S := \{\left[\begin{smallmatrix} c & 0 \\ 0 & 0 \end{smallmatrix}\right] \text{ such that } c \in \mathbb{R}\} \subseteq R$. By Proposition 16.2, to show that $S \subseteq R$ is a sub-ring of R, it is sufficient to show

1. $S \neq \emptyset$
2. $rs \in S$ for all $r, s \in S$
3. $r - s \in S$ for all $r, s \in S$

1. $S \neq \emptyset$ as $\left[\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right] \in S$. ✓
2. S is closed under multiplication as for $\left[\begin{smallmatrix} c & 0 \\ 0 & 0 \end{smallmatrix}\right], \left[\begin{smallmatrix} \gamma & 0 \\ 0 & 0 \end{smallmatrix}\right] \in S$, $\left[\begin{smallmatrix} c & 0 \\ 0 & 0 \end{smallmatrix}\right]\left[\begin{smallmatrix} \gamma & 0 \\ 0 & 0 \end{smallmatrix}\right] = \left[\begin{smallmatrix} c\gamma & 0 \\ 0 & 0 \end{smallmatrix}\right] \in S$. ✓
3. S is closed under subtraction as for $\left[\begin{smallmatrix} c & 0 \\ 0 & 0 \end{smallmatrix}\right], \left[\begin{smallmatrix} \gamma & 0 \\ 0 & 0 \end{smallmatrix}\right] \in S$, $\left[\begin{smallmatrix} c & 0 \\ 0 & 0 \end{smallmatrix}\right] - \left[\begin{smallmatrix} \gamma & 0 \\ 0 & 0 \end{smallmatrix}\right] = \left[\begin{smallmatrix} c-\gamma & 0 \\ 0 & 0 \end{smallmatrix}\right] \in S$. ✓

So S is a sub-ring of R. Furthermore, S is a sub-ring with unity as for any $\left[\begin{smallmatrix} c & 0 \\ 0 & 0 \end{smallmatrix}\right] \in S$, $\left[\begin{smallmatrix} c & 0 \\ 0 & 0 \end{smallmatrix}\right]\left[\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right] = \left[\begin{smallmatrix} 1 & 0 \\ 0 & 0 \end{smallmatrix}\right]\left[\begin{smallmatrix} c & 0 \\ 0 & 0 \end{smallmatrix}\right] = \left[\begin{smallmatrix} c & 0 \\ 0 & 0 \end{smallmatrix}\right]$. □

Exercise 16.3. List or characterize all of the units in each of the following rings.

(a) $\mathbb{Z}_{10}$

(b) $\mathbb{Z}_{12}$

(c) $\mathbb{Z}_7$

(d) $\mathbb{M}_2(\mathbb{Z})$, the 2×2 matrices with entries in $\mathbb{Z}$

(e) $\mathbb{M}_2(\mathbb{Z}_2)$, the 2×2 matrices with entries in $\mathbb{Z}_2$.

Proof. (a) The units of $\mathbb{Z}_{10}$ are $\{x \in \mathbb{Z}_{10} \text{ such that } \gcd(10, x) = 1\} = \{1, 3, 7, 9\}$.

(b) The units of $\mathbb{Z}_{12}$ are $\{x \in \mathbb{Z}_{12} \text{ such that } \gcd(12, x) = 1\} = \{1, 5, 7, 11\}$.

(c) The units of $\mathbb{Z}_7$ are $\{x \in \mathbb{Z}_7 \text{ such that } \gcd(7, x) = 1\} = \mathbb{Z}_7$ as 7 is prime.

(d) The units of $\mathbb{M}_2(\mathbb{Z})$ are $GL_2(\mathbb{Z})$

(e) The units of $\mathbb{M}_2(\mathbb{Z}_2)$ are $GL_2(\mathbb{Z}_2) = \mathbb{M}_2(\mathbb{Z}_2) \setminus \{\left[\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right], \left[\begin{smallmatrix} 1 & 1 \\ 1 & 1 \end{smallmatrix}\right]\}$ □

Exercise 16.4. Find all of the ideals in each of the following rings. Which of these ideals are maximal and which are prime?

(a) $\mathbb{Z}_{18}$

(b) $\mathbb{Z}_{25}$

Proof.

(a) The ideals of $\mathbb{Z}_{18}$ are $\{0\}, \mathbb{Z}_{18}, 2\mathbb{Z}_{18}, 3\mathbb{Z}_{18}, 6\mathbb{Z}_{18}$, and $9\mathbb{Z}_{18}$.

(b) The ideals of $\mathbb{Z}_{25}$ are $\{0\}, \mathbb{Z}_5$, and $\mathbb{Z}_{25}$.

□

Exercise 16.9. What is the characteristic of the field formed by the set of matrices

$$F = \left\{ \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}, \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix}, \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}, \begin{bmatrix} 0 & 0 \\ 0 & 0 \end{bmatrix} \right\}$$

with entries in $\mathbb{Z}_2$?

Proof. The characteristic of F is 2 because $2r = \left[\begin{smallmatrix} 0 & 0 \\ 0 & 0 \end{smallmatrix}\right]$ for all $r \in F$. □