M403 - Fall 2013 - Enrique Areyan - HW6

50/50

① Consider the group $(\mathbb{Q},+)/(\mathbb{Z},+)$, the group of rationals under addition modulo the subgroup of integers. So an element of this group is a coset $a+\mathbb{Z}$ where a is a rational number.

(a) Find the order of the element $\frac{3}{4}+\mathbb{Z}$.

Solution: We want to find $n \geq 1$ such that $(\frac{3}{4}+\mathbb{Z})^n = e$, where e is the identity of $(\mathbb{Q},+)/(\mathbb{Z},+)$, i.e. $e = 0+\mathbb{Z}$. Take $n=4$, then. $(\frac{3}{4}+\mathbb{Z})^4 = (\frac{3}{4}+\mathbb{Z})+(\frac{3}{4}+\mathbb{Z})+(\frac{3}{4}+\mathbb{Z})+(\frac{3}{4}+\mathbb{Z}) = (4\cdot\frac{3}{4}+\mathbb{Z}) = 3+\mathbb{Z} = \mathbb{Z}$.

Hence, the order of $\frac{3}{4}+\mathbb{Z}$ is 4. ✓

(b) Show that every element of this group has finite order.

Pf: Let $a+\mathbb{Z} \in (\mathbb{Q},+)/(\mathbb{Z},+)$; so $a \in \mathbb{Q}$. Write $a = \frac{p}{q}$, for p,q integers, i.e., $\gcd(p,q)$, $q \neq 0$. Without loss of generality, write $\frac{p}{q}$ in lowest terms. Moreover Claim: $\Theta(a+\mathbb{Z}) = q$. Pf: $(a+\mathbb{Z})^q = (\frac{p}{q}+\mathbb{Z})^q = (q(\frac{p}{q})+\mathbb{Z}) = (p+\mathbb{Z}) = \mathbb{Z} = e$. Let $1<k<q$ be such that $(a+\mathbb{Z})^k = \mathbb{Z}$. Then, $k\cdot\frac{p}{q} \in \mathbb{Z}$, which means that $q \mid kp$, but $\gcd(q,p)=1$ so it must be that $q \mid k$ but $k<q$ so $q \nmid k$, a contradiction, there is no such k; so the order of $a+\mathbb{Z}$ is indeed q. ✓ +10

(c) Prove that the group is infinite

Pf: Consider the subset $S \subset (\mathbb{Q},+)/(\mathbb{Z},+)$ defined by $S = \{\frac{1}{n}+\mathbb{Z} \mid n \in \mathbb{N}\}$. Define the function $f: S \to \mathbb{N}$ by $f(\frac{1}{n}+\mathbb{Z}) = n$. Clearly f is a bijection, So in particular we can conclude that S is an infinite set. But $S \subset (\mathbb{Q},+)/$ so the group $(\mathbb{Q},+)/(\mathbb{Z},+)$ must be infinite and at least as big as $\mathbb{N}$. ✓ is cyclic.

(d) Prove that every finite subgroup of $(\mathbb{Q},+)/(\mathbb{Z},+)$ is cyclic.

Pf: Note that the group $(\mathbb{Q},+)/(\mathbb{Z},+)$ is abelian: Let $a+\mathbb{Z}, b+\mathbb{Z}$ be elements of this group, then $(a+\mathbb{Z})+(b+\mathbb{Z}) = (a+b)+\mathbb{Z} = (b+a)+\mathbb{Z} = (b+\mathbb{Z})+(a$ therefore, all subgroups of this group are abelian since they inherit the group operation. Let H be a finite subgroup of $(\mathbb{Q},+)/(\mathbb{Z},+)$. Then H is abelian. Moreover, by part (b), we know that every element of this group has finite order, so pick $a+\mathbb{Z} \in (\mathbb{Q},+)/(\mathbb{Z},+)$; the subgroup $\langle a+\mathbb{Z}\rangle$ is finite and cyclic. Any other finite subgroup must contain at least one element, say $b+\mathbb{Z}$. But then $(b+\mathbb{Z})+(c+\mathbb{Z}) = (b+c)+\mathbb{Z}$ would have to be in the group $\langle(b+c)+\mathbb{Z}\rangle$, and thus be cyclic. ✓

Hence, every finite subgroup is cyclic.

(2)(a) Find all possible cycle structures for elements of S_5.

Solution: there are a total of 7 possible cycle structures for elements of S_5

e (identity), (1,2), (1,2)(3,4), (1,2,3)(4,5), (1,2,3), (1,2,3,4), (1,2,3,4,5)

(b) Find all possible orders for elements of S_5.

Solution: All possible orders are given by the lcm of the lenghts of each cycle in the cycle structure for elements of S_5 as show in (a):

Note that this are representatives elements, e.g, we could have (4,5) instead of (1,2) and so on.

cycle structure	order
e (identity)	lcm(1) = 1
(1,2)	lcm(2,1,1,1) = 2
(1,2)(3,4)	lcm(2,2,1) = 2
(1,2,3)(4,5)	lcm(3,2) = 6
(1,2,3)	lcm(3,1,1) = 3
(1,2,3,4)	lcm(4,1) = 4
(1,2,3,4,5)	lcm(5) = 5

All possible orders are: 1, 2, 3, 4, 5, 6

+10

(C) Find the number of elements in each conjugacy class in S_5

Solution: the key observation here is that conjugation preserves cycle structure in S_5 therefore, to count the number of elements in each conjugacy class with the same cycle structure it suffices to count the number of elements in conjugacy class

Note that the conjugacy classes partition S_5. Therefore $|S_5| = 5! = 120 = 1+10+15+20+20+30+24$; So each element of S_5 is accounted for.

cycle structure	# of elements in conjugacy class
e	$\boxed{1}$ (only itself)
(1,2)	there are 5 possible numbers for position 1 and 4 for position 2. But we have to adjust for the fact that (1,2)=(2,1) so, total = $\frac{5\times4}{2} = \boxed{1}$
(1,2)(3,4)	Same reasoning as before but divide by an extra 2 to account for order of transpositions, so t... is $(5\times4\times3\times2)/2\times2\times2 = \boxed{15}$
(1,2,3)(4,5)	$(5\times4\times3\times2\times1)/3\times2 = \boxed{20}$
(1,2,3)	$(5\times4\times3)/3 = \boxed{20}$
(1,2,3,4)	$(5\times4\times3\times2)/4 = \boxed{30}$
(1,2,3,4,5)	$(5\times4\times3\times2\times1)/5 = \boxed{24}$

M403 - Fall 2013 - Enrique Areyan - HW6

(2)(d) For each conjugacy class choose a representative of that class and describe its centralizer. (In each case it is a group you know or a product of groups you know).

Solution: As previously calculated there are 7 conjugacy classes: CHOOSE the following elements as class representatives:

e, $(1,2)$, $(1,2)(3,4)$, $(1,2,3)(4,5)$, $(1,2,3)$, $(1,2,3,4)$, $(1,2,3,4,5)$

By definition: $C_{S_5}((1,2)) = \{ g \in S_5 \mid \gamma g = g \gamma$, γ a transposition in S_5

Clearly, every element of S_5 commutes with e, so $C_{S_5}(e) = S_5$.

For transpositions (i,j) $1 \leq i < j \leq 5$. We would need

$g(i,j) = (i,j)g \Rightarrow g(i,j)g^{-1} = (i,j) \Rightarrow g$ is a permutation of S_5 that fixes both i,j. But these are exactly permutations over smaller sets. $C_{S_5}(\text{Class of } (1,2)) = S_3$; (take two elements out of S_5).

Similarly for $(1,2,3)$: $g \in C_{S_5}((1,2,3)) \Rightarrow g(1,2,3) = (1,2,3)g^{-1}$
$\Rightarrow g(1,2,3)g^{-1} = (1,2,3) \Rightarrow C_{S_5}((1,2,3)) = S_2$.

Clearly, the only element of S_5 that commutes with $(1,2,3,4,5)$ is e so $C_{S_5}((1,2,3,4,5)) = e$, the trivial group. A similar argument applies to $(1,2,3,4)$, since the only things that commute with it are 1-cycles, but these are the same as the identity, therefore

$C_{S_5}((1,2,3,4)) = S_1 = e$, the trivial group.

A similar reasoning follows for $(1,2)(3,4)$ and $(1,2,3)(4,5)$

M403 - Fall 2013 - Enrique Areyan - HW6

(3) Let G be a group and $Aut(G)$ denote the group of automorphisms of G: $Aut(G) = \{f: G \to G \mid f$ is an isomorphism$\}$.

Let for each $x \in G$, $I_x(g) = xgx^{-1}$ for all $g \in G$. Finally, $Inn(G) = \{I_x \mid x \in$

(a) Prove that <u>if</u> $x \in G$ and $\sigma \in Aut(G)$ <u>then</u> $\sigma I_x \sigma^{-1} = I_{\sigma(x)}$.

<u>Pf</u>: Let $x \in G$ and $\sigma \in Aut(G)$. Let $g \in G$. then

$(\sigma I_x \sigma^{-1})(g) = \sigma(I_x(\sigma^{-1}(g)))$ By definition of function composition

$= \sigma(x(\sigma^{-1}(g))x^{-1})$ By definition of I_x

$= (\sigma(x))[\sigma(\sigma^{-1}(g))](\sigma(x^{-1}))$ Since σ is an isomorphism.

$= \sigma(x)\, g\, \sigma(x^{-1})$ Since σ is the inverse of σ^{-1}

$= \sigma(x)\, g\, [\sigma(x)]^{-1}$ Again, σ is an isom. it preserves inverses

$= I_{\sigma(x)}(g)$ By definition of $I_{\sigma(x)}$

$\Rightarrow \sigma I_x \sigma^{-1} = I_{\sigma(x)}$.

(b) Prove that $Inn(G) \trianglelefteq Aut(G)$.

<u>Pf</u>: We want to show that: $\forall I_x \in Inn(G): \forall \sigma \in Aut(G): \sigma I_x \sigma^{-1} \overset{?}{\in} Inn(G)$

But we just proved in (a) that given $x \in G$ and $\sigma \in Aut(G)$, $\sigma I_x \sigma^{-1} = I_{\sigma(x)}$

Since σ is an isomorphism, $\sigma(x) \in G$. therefore $\sigma I_x \sigma^{-1} = I_{\sigma(x)} \in Inn(G)$

Which means that $Inn(G) \trianglelefteq Aut(G)$.

(c) Define a map $\alpha: G \to Inn(G)$ by $\alpha(x) = I_x$. Prove that α is a homomorphism and determine its kernel.

<u>Pf</u>: (i) α is a homomorphism: Let $x, y \in G$. Also, Let $g \in G$. Consider

$\alpha(xy)(g) = I_{xy}(g) = (xy)g(xy)^{-1} = (xy)g(y^{-1}x^{-1}) = x(ygy^{-1})x^{-1} = x\, I_y(g)\, x^{-1}$

$= I_x(I_y(g)) = (I_x \circ I_y)(g) = (\alpha(x) \circ \alpha(y))(g) \Rightarrow \alpha(xy) = \alpha(x)\alpha(y)$.

(ii) By definition: $Ker(\alpha) = \{x \in G \mid \alpha(x) = e$, where e is the identity of $Inn($

the identity of $Inn(G)$ is such that for any $I_x \in Inn G$: $eI_x = I_x e =$

clearly $e = I_e$, since $I_e I_x(g) = I_e(xgx^{-1}) = exgx^{-1}e^{-1} = xgx^{-1} = I_x(g)$.

$I_x I_e(g) = I_x(ege^{-1}) = I_x(g)$. therefore, we can re

our definition: $Ker(\alpha) = \{x \in G \mid \alpha(x) = I_e\}$. Let $x \in G$ be such that $\alpha(x) =$

But by definition $\alpha(x) = I_x = I_e$. this leads our thinking to the followin
claim: $Ker(\alpha) = Z(G)$.

Pf: $(\subseteq)$ Let $x \in Ker(\alpha)$. then, for any $g \in G$, $I_x(g) = g$. So then, let $g \in$
$gx = I_x(gx) = x(gx)x^{-1} = (xg)(xx^{-1}) = xg \Rightarrow x \in Z(G)$.

$(\supseteq)$ Let $y \in Z(G)$. By definition, for any $g \in G$: $gy = yg$. Let $g \in G$:
$I_y(g) = y(g)y^{-1} = (yg)y^{-1} = (gy)y^{-1} = g(yy^{-1}) = g \Rightarrow y \in Ker(\alpha)$.

(d) Prove that the quotient group $G/Z(G)$ is isomorphic to $Inn(G)$.

Pf: First note that α is onto. By definition, for each $x \in G$ we have the automorphism I_x. Moreover, we proved in (c) that α is a homomorphi therefore, by the first isomorphism theorem its kernel is isomorphic to its image. As a diagram:

+10

$$\begin{tikzcd} G \arrow[r, "\alpha"] \arrow[d, "\pi"'] & Inn(G) \\ Ker(\alpha) = G/Z(G) \arrow[ur, dashed, "\varphi"'] & \end{tikzcd}$$

$\varphi \circ \pi = \alpha$; by first isom. theorem

So we have a unique isomorphism $\varphi : G/Z(G) \to Inn(G)$, such that $\varphi \circ \pi = \alpha$.

---

(4) (a). Prove that S_n is generated by $(1,2)$ and $(1,2,\dots,n)$, i.e., $S_n = \langle \{(1,2),(1,2,\dots$

Pf: It suffices to show that we can produce all transpositions with elemen from $\{(1,2),(1,2,\dots,n)\}$. Then, by theorem showed in class, any permutation can be writen as the product of transpositions and we will be done.

By another proposition showed in class, we know that conjugation preserves cycle structure. therefore, conjugating $(1,2)$ by the cycle $(1,2,\dots,n)$ will yield another transposition. So, if we conjugate $(1,2)$ by the n-cycle repeatedly we will get all transpositions of the form:

$$(1,2,\dots,n)(1,2)(n,n-1,\dots,1) = (1)(2,3)(4)\cdots(n) = (2,3).$$
$$(1,2,\dots,n)(2,3)(n,n-1,\dots,1) = (1)(2)(3,4)(5)\cdots(n) = (3,4)$$
$$\vdots$$
$$(1,2,\dots,n)(n-1,n)(n,n-1,\dots,1) = (1,n)(2)(3)\cdots(n-1) = (1,n) = (n,1).$$

this shows that repeated conjugation produces the following transposit[ions] $(1,2),(2,3),(3,4),\ldots,(n,1)$. Note that these are the same as: $(2,1),(3,2),\ldots,(1,n)$. Finally, we can get any transposition from the above type of transposition. Without loss of generality, let us write a transposition (i,j) where $1 \le i < j \le n$ as follow:

+10

$$(i,j) = (i,i+1)(i+1,i+2)\cdots(j-1,j)(n-1,j)\cdots(i+2,i+1)(i+1\ i).$$

therefore, you can generate all transpositions, which shows that $\langle\{(1,2),(1,2,\ldots,n)\}\rangle = S_n$.

(b) Let $1 \le i < j \le n$. Find necessary and sufficient conditions on i,j so that (i,j) and $(1,2,\ldots,n)$ generate S_n.

Solution: claim: Let $1 \le i < j \le n$, the transposition $(i\ j)$ and $(1,2,\ldots,n)$ generate S_n if and only if $\gcd(j-i,n)=1$.

Pf: ($\Rightarrow$) Suppose that $(i\ j)$ and $(1,2,\ldots,n)$ generate S_n. Let $\sigma \in S_n$. We know that σ can be written as a product of transpositions $\sigma = \pi_1\pi_2\cdots\pi_k$; Moreover, the permutation is either even or odd so $k=2p+1$ or $k=2p$. Also, suppose that $\gcd(j-i,n)=d>1$.

If $d>1$, then $(i\ j)$ together with $(1,2,\ldots,n)$ won't be able to generate all of S_n. In fact, $\langle (i\ j)(1,2,\ldots,n)\rangle \le S_n$. the reason is that repeated conjugation of (i,j) by $(1,2,\ldots,n)$ will not generate all transpositions of the kind $(1\ 2),(2\ 3),\ldots,(n,1)$, but only a subset of these. therefore, we won't be able to generate all transpositions and hence all of S_n.

($\Leftarrow$) Suppose that $\gcd(j-i,n)=1$. Let $(i\ j)\in S_n$ and $(1,2,\ldots,n)\in S_n$. Following a similar reasoning as in (a), take $(i\ j)$ and conjugate it repeatedly by $(1,2,\ldots,n)$. Since $\gcd(j-i,n)=1$, eventually we will get all permutations of the kind $(1,2)(2,3)\cdots(n,1)$ (maybe not in the order). From these produce all transpositions to be able to generate S_n.

therefore, $S_n = \langle\{(i,j),(1,2,\ldots,n)\}\rangle \Leftrightarrow \gcd(j-i,n)=1,\quad j>i.$

(5) (a) Prove that $GL_3(\mathbb{R})$ is isomorphic to $\mathbb{R}^\times \times SL_3(\mathbb{R})$.

Pf: Consider the following function:

$$f: GL_3(\mathbb{R}) \longrightarrow \mathbb{R}^\times \times SL_3(\mathbb{R}), \text{ for } M \in GL_3(\mathbb{R}) \text{ given by:}$$

$$f(M) = \left(\det(M), \frac{1}{[\det(M)]^{1/3}} \cdot M\right).$$

First note that this is a well-defined function on its range since

(i) $M \in GL_3(\mathbb{R}) \Rightarrow \det(M) \neq 0$, so $\frac{1}{[\det(M)]^{1/3}} \in \mathbb{R}$.

(ii) $\det\left(\frac{1}{[\det(M)]^{1/3}} \cdot M\right) = \left[\frac{1}{[\det(M)]^{1/3}}\right]^3 \cdot \det(M) = \frac{1}{\det(M)} \cdot \det(M) = 1. \Rightarrow \frac{1}{[\det(M)]^{1/3}} \cdot M \in S$

claim: f is a homomorphism. Pf. Let $M_1, M_2 \in GL_3(\mathbb{R})$. then:

$$f(M_1M_2) = \left(\det(M_1M_2), \frac{1}{[\det(M_1M_2)]^{1/3}} \cdot (M_1M_2)\right) = \left(\det(M_1)\det(M_2), \frac{1}{[\det(M_1)\det(M_2)]^{1/3}}(M_1M_2)\right)$$

$$= \left(\det(M_1)\det(M_2), \left[\frac{1}{[\det(M_1)]^{1/3}} M_1\right]\left[\frac{1}{[\det(M_2)]^{1/3}} M_2\right]\right)$$ by properties of det and algebra of matrices

$$= \left(\det(M_1), \frac{1}{[\det(M_1)]^{1/3}} M_1\right) \circ \left(\det(M_2), \frac{1}{[\det(M_2)]^{1/3}} \cdot M_2\right)$$

$$= f(M_1) \circ f(M_2).$$

Claim: f is a bijection. Pf:

(i) f is 1-1. Let $M_1, M_2 \in GL_3(\mathbb{R})$ be such that $f(M_1) = f(M_2)$. then by definition of f

$$\left(\det(M_1), \frac{1}{[\det(M_1)]^{1/3}} \cdot M_1\right) = \left(\det(M_2), \frac{1}{[\det(M_2)]^{1/3}} \cdot M_2\right)$$

$$\Rightarrow \det(M_1) = \det(M_2) \text{ and } \frac{1}{[\det(M_1)]^{1/3}} M_1 = \frac{1}{[\det(M_2)]^{1/3}} M_2$$

$$\Rightarrow \frac{1}{[\det(M_1)]^{1/3}} M_1 = \frac{1}{[\det(M_1)]^{1/3}} M_2 \Rightarrow M_1 = M_2 \quad (\text{since } \det(M_1) = \det(M_2)).$$

(ii) f is onto. Let $(x, A) \in \mathbb{R}^\times \times SL_3(\mathbb{R})$. So $x \in \mathbb{R}, x \neq 0$, $A \in SL_3(\mathbb{R}) \Rightarrow \det(A) = 1$. Pick $M \in GL_3(\mathbb{R})$ to be such that $M = x^{1/3} \cdot A$. then:

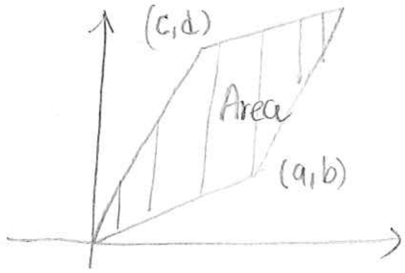
$$f(A) = f(x^{1/3}A) = \left(\det(x^{1/3}A), \frac{1}{[\det(x^{1/3}A)]^{1/3}} x^{1/3}A\right) = \left((x^{1/3})^3 \det(A), \frac{1}{[(x^{1/3})^3 \det(A)]^{1/3}} \cdot x^{1/3} A\right)$$

$$= \left(x \cdot 1, \frac{1}{x^{1/3}} \cdot x^{1/3} \cdot A\right) = (x, A).$$

(i) & (ii) $\Rightarrow$ f is a bijection. Is also a homomorphism. So, f is an isomorphism, $\Rightarrow$ $GL_3(\mathbb{R}) \cong \mathbb{R}^\times \times SL_3$

(5)(b) this is not true if you replace 3 by 2. What's the explanation - no proof required.

Solution: the group $Gl_2(\mathbb{R})$ is the group of all invertible 2x2 matrices, i.e., matrices with determinat distinct from zero. If a matrix (2x2), has determinat other than zero, its determinat represent the signed area of the parallelepiped spanned by the rows of the matrix interpreted as vectors.



$$Area = \det\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) \neq 0.$$

+10

If $Gl_2(\mathbb{R}) \cong \mathbb{R}^\times \times Sl_3(\mathbb{R})$ then the area of the parallelepiped spanned by each matrix in $GL_2(\mathbb{R})$ would be mapped into two different pieces of information $(\mathbb{R}^\times, SL_2(\mathbb{R}))$; but the area of any element of $SL_2(\mathbb{R})$ is one and by properties of determinants, if $A \in GL_2(\mathbb{R})$ $\det(aA) = a^2 \det(A)$; so it won't be possible to cover all of the product group $\mathbb{R}^\times \times SL_2(\mathbb{R})$ by members of $GL_2(\mathbb{R})$.

this is precisely the reason why it works in the 3-dimensional case. In this case, the volume of the parallelepiped is mapped into a real number which is possible because if $M \in Gl_3(\mathbb{R})$, then $\det(aM) = a^3 \det(M)$; and $(\;)^3$ is a bijection; whereas $(\;)^2$ is not

Hence, the function f as defined in 5(a) would not work in this case.