Algebra - Midterm 1 - Fall 2018 - NYU

All answers must be justified.

NAME:

Exercise 1 We recall that $GL_2(\mathbb{R})$ denotes the group of invertible 2×2 matrices with real coefficients. If $A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ is a 2×2 matrix, we recall that the transpose of A, denoted by A^T is the matrix $A^T := \begin{pmatrix} a & c \\ b & d \end{pmatrix}$, and that $(AB)^T = B^T A^T$. The identity matrix is denoted by I_2.

We let $O_2(\mathbb{R})$ be the subset of $GL_2(\mathbb{R})$ defined by

$$O_2(\mathbb{R}) := \left\{ A \in GL_2(\mathbb{R}), A^T A = I_2 \right\}.$$

Question 1. Show that $O_2(\mathbb{R})$ is a subgroup of $GL_2(\mathbb{R})$.

- We have $I_2^T \cdot I_2 = I_2 \cdot I_2 = I_2$ hence $I_2 \in O_2(\mathbb{R})$
- Let A be in $O_2(\mathbb{R})$, by definition $A^T \cdot A = I_2$ hence $A^T = A^{-1}$. We have $A \cdot A^{-1} = A^{-1} \cdot A = I_2$, in particular $A \cdot A^T = I_2$, but $A = (A^T)^T$, so $(A^T)^T \cdot A^T = I_2$, which means $A^T \in O_2(\mathbb{R})$, and thus $A^{-1} \in O_2(\mathbb{R})$
- Let A, B be in $O_2(\mathbb{R})$. Let us compute

$$\begin{aligned} (AB)^T AB &= B^T A^T A B \quad \text{(by the formula recalled above)} \\ &= B^T B \quad \text{(because } A \in O_2(\mathbb{R})\text{)} \\ &= I_2 \quad \text{(because } B \in O_2(\mathbb{R})\text{)} \end{aligned}$$

hence $AB \in O_2(\mathbb{R})$.

In conclusion, $O_2(\mathbb{R})$ is a subgroup of $GL_2(\mathbb{R})$

For any A in $O_2(\mathbb{R})$, we define the *commutator of* A as the subset

$$\mathrm{Comm}(A) := \{B \in O_2(\mathbb{R}),\ AB = BA\}.$$

In plain words, $\mathrm{Comm}(A)$ is the set of all matrices in $O_2(\mathbb{R})$ that commute with A.

Question 2. Compute $\mathrm{Comm}(I_2)$.

By definition, $\mathrm{Comm}(I_2) = \{ B \in O_2(\mathbb{R}),\ I_2 B = B \cdot I_2 \}$

$= \{ B \in O_2(\mathbb{R}),\ B = B \}$

So $\mathrm{Comm}(I_2) = O_2(\mathbb{R})$.

Question 3. For all A in $O_2(\mathbb{R})$, show that $\mathrm{Comm}(A)$ is a subgroup of $O_2(\mathbb{R})$. Let $A \in O_2(\mathbb{R})$

- We have $I_2 \cdot A = A \cdot I_2 = A$ so $I_2 \in \mathrm{Comm}(A)$
- If $B \in \mathrm{Comm}(A)$ we have $AB = BA$, so $B^{-1}A = AB^{-1}$ and $B^{-1} \in \mathrm{Comm}(A)$
- If B, C are in $\mathrm{Comm}(A)$, we have

$$ABC = BAC = BCA$$

(first $=$: because $AB = BA$; second $=$: because $AC = CA$)

thus $BC \in \mathrm{Comm}(A)$

In conclusion, $\mathrm{Comm}(A)$ is a subgroup of $O_2(\mathbb{R})$

Question 4. Let $A = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$. Show that A is in $O_2(\mathbb{R})$, compute its order and describe its commutator.

- We have $A^T = A$, and $A^T \cdot A = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, so $A \in O_2(\mathbb{R})$
- Since $A^T = A$ and $A^T \cdot A = I_2$, we have $A^2 = I_2$, so A has order 2.
- Let us describe its commutator. Let $B \in O_2(\mathbb{R})$, let us write $B = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$.

We have $B \in \mathrm{Comm}(A) \Leftrightarrow BA = AB \Leftrightarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix}\begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}\begin{pmatrix} a & b \\ c & d \end{pmatrix}$

$$\Leftrightarrow \begin{pmatrix} -b & -a \\ -d & -c \end{pmatrix} = \begin{pmatrix} -c & -d \\ -a & -b \end{pmatrix} \Leftrightarrow \begin{matrix} b = c \\ d = a \end{matrix}$$

so $B \in \mathrm{Comm}(A) \Leftrightarrow B$ is in $O_2(\mathbb{R})$ and can be written as $\begin{pmatrix} a & c \\ c & a \end{pmatrix}$ for some a, c in $\mathbb{R}$

This is an acceptable answer.

$$\Leftrightarrow B = \begin{pmatrix} a & c \\ c & a \end{pmatrix} \text{ where } \begin{cases} a^2 + c^2 = 1 \\ ac = 0 \end{cases}$$

$$\Leftrightarrow B = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \text{ or } \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} \text{ or } \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \text{ or } \begin{pmatrix} 0 & -1 \\ -1 & 0 \end{pmatrix}$$

Exercise 2 We recall that a group G is said to be cyclic if there exists an element g in G such that the subgroup $\langle g \rangle$ generated by g is equal to G itself.

Question 1. Show that $\mathbf{Z}_2 \times \mathbf{Z}_3$ is cyclic, but that $\mathbf{Z}_2 \times \mathbf{Z}_2$ is not.

- let us consider $\langle (1,1) \rangle$ in $Z_2 \times Z_3$. The successive powers of $(1,1)$ are $(1,1)$; $(0,2)$; $(1,0)$; $(0,1)$; $(1,2)$; $(0,0)$

  so $\langle (1,1) \rangle = Z_2 \times Z_3$ and $Z_2 \times Z_3$ is thus cyclic.

- In $Z_2 \times Z_2$ we have

  $\langle (0,0) \rangle = \{(0,0)\}$

  $\langle (1,0) \rangle = \{(0,0); (1,0)\}$

  $\langle (0,1) \rangle = \{(0,0); (0,1)\}$

  $\langle (1,1) \rangle = \{(0,0); (1,1)\}$

  none of these are $Z_2 \times Z_2$, so there is no generator, $Z_2 \times Z_2$ is not cyclic.

Question 2. Let G, H be two groups. Assume that G is cyclic and that there exists an isomorphism from G to H. Prove that H is cyclic

Done in class.

Question 3. Let G be a group, and let g be in G. Someone tells you that there is **at most one** element of G not included in $\langle g \rangle$. Show that G is cyclic.

- If there is no element not included in $\langle g \rangle$, then G is cyclic and g is a generator.
- Let us assume there is exactly one element in G and not in $\langle g \rangle$, let us denote it by h. Consider $g \cdot h$.

  * Either $g \cdot h = h$, which means $g = e$. Then $\langle g \rangle = \{e\}$, and thus $G = \{e, h\}$ is isomorphic to Z_2, and is thus cyclic
  * Or $g \cdot h \neq h$. Since h is the only element not in $\langle g \rangle$, we must have $g \cdot h \in \langle g \rangle$, but since $g \in \langle g \rangle$ we have $h \in \langle g \rangle$, which is absurd.

The signature morphism Let $n \geq 2$. We recall that the "signature" or "parity" of a permutation σ in S_n is defined as

$$\varepsilon(\sigma) := \prod_{1 \leq i < j \leq n} \mathrm{Sign}\,(\sigma(j) - \sigma(i))\,,$$

where Sign denotes the sign ($+1$ or -1).

We have proven the following facts: $\varepsilon(\mathrm{Id}) = 1$, and if τ is a transposition, $\varepsilon(\tau) = -1$. The goal of this exercise is to prove that ε is a morphism, namely that for all permutations σ_1, σ_2, we have

$$\varepsilon(\sigma_1 \circ \sigma_2) = \varepsilon(\sigma_1)\varepsilon(\sigma_2).$$

Question 1. Show that

$$(13) = (23)(12)(23).$$

$(13) = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ and $(23)(12)(23)$

$= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$

$= \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$ so $(13) = (23)(12)(23)$

Question 2. For $i = 1, \ldots n-1$, we let τ_i be the transposition

$$\tau_i := (i(i+1))\,,$$

that switches two "neighbors" in $\{1, \ldots, n\}$. Prove that any transposition can be written as a product of these transpositions τ_i.

You may argue by induction on the "distance" between the elements of the transposition, and let yourself be inspired by Question 2.

Let us prove that for any $r \geq 1$, for any $j \in \{1, \ldots, n-r\}$, the transposition $(j\,(j+r))$ can be written as a product of the τ_i's.

* If $r = 1$, it is one of the τ_i's!
* Assume it is true for some $r \geq 1$, and consider $(j\,(j+r+1))$.

We write, as in question 1

$$(j\,(j+r+1)) = \underbrace{(j+r, j+r+1)}_{\text{one of the } \tau_i\text{'s}}\,(j\,(j+r))\,\underbrace{(j+r, j+r+1)}_{\text{one of the } \tau_i\text{'s}}$$

$(j\,(j+r))$ can be written as a product of the τ_i's by induction hypothesis.

So $(j\,(j+r+1))$ can be written as a product of the τ_i's.

Question 3. Deduce that every permutation in S_n can be written as product of the transpositions τ_i.

We know by a result from class that every permutation can be written as a product of transpositions. From Question 2, we know every transposition is a product of the τ_i's. Thus every permutation is a product of the τ_i's.

Question 4. Show that, in order to prove that ε is a group morphism, it is enough to prove that for any permutation σ and for any $i \in \{1, \dots, n-1\}$, we have

$$\varepsilon(\sigma \circ \tau_i) = -\varepsilon(\sigma). \qquad (*)$$

(hence the whole result boils down to this very easy computation that you can do at home.)

We prove the following: for any permutation σ_1, for any $k \geq 1$, if σ_2 is a product of k transpositions τ_i, then $\varepsilon(\sigma_1 \circ \sigma_2) = \varepsilon(\sigma_1)\varepsilon(\sigma_2)$

* $k = 1$ follows from $(*)$
* Assume it is true for $k \geq 1$. Write σ_2 as $\sigma_2' \circ \tau_i$, where σ_2' is the product of at most k transpositions τ_i and τ is one of them.

We have $\varepsilon(\sigma_1 \circ \sigma_2) = \varepsilon(\sigma_1 \circ \sigma_2' \circ \tau) = \varepsilon((\sigma_1 \circ \sigma_2') \circ \tau)$

$= \varepsilon(\sigma_1 \circ \sigma_2')\,\varepsilon(\tau)$ (by $*$)

$= \underbrace{\varepsilon(\sigma_1)\varepsilon(\sigma_2')}_{\text{by induction hypothesis}}\varepsilon(\tau) = \varepsilon(\sigma_1)\underbrace{\varepsilon(\sigma_2)}_{\text{by } *}$.

Since, by Question 3, every σ_2 is a product of the τ_i's, we have proven the result.

Question 5. Compute (with minimal justification) the parity of the following permutations:

1. $(123)(456)(123456)$
2. $(12)(234)^{-1}(12345)(34)^{-1}$
3. (123456789).

Parity of a cycle of length L = parity of $L-1$
Parity of σ = parity of σ^{-1}. Hence

1) $1 \cdot 1 \cdot (-1) = -1$
2) $(-1) \cdot 1 \cdot (1) \cdot (-1) = 1$
3) 1.

Bonus question: compute the center of S_n for $n \geq 3$.

It is trivial. Let $\sigma \in S_n$ be different from the identity.
Let $a \in \{1, \dots, n\}$ such that $\sigma(a) \neq a$; denote $b = \sigma(a)$.

- If $\sigma(b) \neq a$, let $\tau = (ab)$.

We have $\sigma \circ \tau(a) = \sigma(b)$ and $\tau \circ \sigma(a) = \tau(b) = a$
since $\sigma(b) \neq a$, $\sigma \circ \tau \neq \tau \circ \sigma$ so σ, τ don't commute.

- If $\sigma(b) = a$, since $n \geq 3$ we can take $c \neq a, b$.
Let $\tau = (ac)$. We have
$\sigma \circ \tau(b) = \sigma(b) = a$
$\tau \circ \sigma(b) = \tau(a) = c$ but $a \neq c$
hence $\sigma \circ \tau \neq \tau \circ \sigma$ and σ, τ don't commute.