18.701: Problem Set 2

Dmitry Kaysin

March 2020

Problem 1

Prove that, for $n \geq 3$, the three-cycles generate the alternating group A_n.

Proof. Since no three-cycle is a member of A_n with $n < 3$ we proceed for $n \geq 3$. Alternating group A_n is a group of even permutations of the set. Even permutation is a permutation that can be represented as a product of even number of transpositions (two-cycles). Consider arbitrary element $x \in A_n$. Using this presentation of x, combine two-cycles into pairs starting from the first one. Within each pair, transpositions are either disjoint or not disjoint. If they are disjoint, product of such pair of transposition can always be represented as product of 2 three-cycles.

$$(ab)(fg) = (ab)(bf)(bf)(fg) = (abf)(bfg)$$

If they are not disjoint, product of such pair of transpositions is equal to a three-cycle:

$$(ca)(ba) = (ac)(ab) = (ca)(ab) = (cab) = (abc)$$

Identity permutation can also be represented as product of 3 identical three-cycles.

Continuing for each pair of transpositions, we conclude that x can be represented as product of three-cycles, i.e. three cycles generate A_n.

□

Problem 2

Determine the center of $\mathrm{GL}_n(\mathbb{R})$.

Center of a group G (denote $Z(G)$) is the set of its elements that commute with each element of G. All invertible matrices form $\mathrm{GL}_n(\mathbb{R})$. As we know, elementary matrices representing row-addition and row-multiplication generate $\mathrm{GL}_n(\mathbb{R})$. Therefore, if any particular matrix commutes with each elementary matrix, it must commute with any element of $\mathrm{GL}_n(\mathbb{R})$ and, therefore, is an element of $\mathrm{Z}(\mathrm{GL}_n(\mathbb{R}))$.

Taking arbitrary matrix A, we notice that left-multiplication by any elementary matrix E operates on its rows, while right-multiplication operates on its columns, and only one row or column is affected.

We first consider elementary matrix $E^{\times}(i, \lambda)$ that multiplies i-th row or column by λ. For example, for $i = 1$:

$$E^{\times}(1, \lambda) \cdot A = \begin{bmatrix} \lambda a & \dots & \lambda x & \dots & \lambda y \\ \vdots & \ddots & & & \vdots \\ b & & \ddots & & * \\ \vdots & & & \ddots & \vdots \\ c & \dots & * & \dots & * \end{bmatrix}$$

$$A \cdot E^{\times}(1, \lambda) = \begin{bmatrix} \lambda a & \dots & x & \dots & y \\ \vdots & \ddots & & & \vdots \\ \lambda b & & \ddots & & * \\ \vdots & & & \ddots & \vdots \\ \lambda c & \dots & * & \dots & * \end{bmatrix}$$

For these matrices to be equal, the following must hold:

$$x = \lambda x, \quad y = \lambda y, \quad \dots$$

More generally, each non-diagonal entry $a_{ij} (i \neq j)$ must be equal to λa_{ij}. This is only possible if $a_{ij} = 0$.

We then consider elementary matrix $E^{+}(i, j, \lambda)$ that adds λ-multiple of i-th row or column to j-th row or column. For example, for $i = 1, j = 2$:

$$E^{\times}(1, \lambda) \cdot A = \begin{bmatrix} a & 0 & \dots & 0 \\ a & b & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & c \end{bmatrix}$$

$$A \cdot E^{\times}(1, \lambda) = \begin{bmatrix} a & 0 & \dots & 0 \\ b & b & & 0 \\ \vdots & & \ddots & \vdots \\ 0 & 0 & \dots & c \end{bmatrix}$$

For these matrices to be equal a must be equal to b. More generally, all diagonal entries must be equal. We conclude that matrices

$$D = \{\lambda I_n : \lambda \in \mathbb{R}\}$$

(matrices with the same diagonal entries) commute with elementary matrices $E^{\times}$ and E^{+}. Therefore, they must commute with every element of $\mathrm{GL}_n(\mathbb{R})$, thus $D = \mathrm{Z}(\mathrm{GL}_n(\mathbb{R}))$.

Problem 3

> Show that the functions $f = \dfrac{1}{x}$, $g = \dfrac{x-1}{x}$ generate a group of functions, the law of composition being composition of functions, that is isomorphic to the symmetric group S_3.

Proof. Denote $F = (\langle f, g \rangle, \circ)$, group generated by f, g. Identity element of F is function $h(x) = x$.

The usual presentation of S_3 is as follows:

$$S_3 = \langle\, x, y \ \mid\ x^3 = 1,\ y^2 = 1,\ yx = x^2y \,\rangle.$$

Consider map $\varphi : S_3 \to F$ such that $x \longmapsto g$ and $y \longmapsto f$, then:

$$\begin{aligned}
&x^3 \longmapsto g^3; \quad g^3 = g \circ g \circ g = g \circ \frac{\frac{x-1}{x} - 1}{\frac{x-1}{x}} = g \circ \frac{1}{1-x} = \frac{\frac{1}{1-x} - 1}{\frac{1}{1-x}} = x = 1_F,\\
&y^2 \longmapsto f^2; \quad f^2 = f \circ f = \frac{1}{\frac{1}{x}} = x = 1_F,\\
&yx \longmapsto fg; \quad fg = f \circ g = \frac{1}{\frac{x-1}{x}} = \frac{x}{x-1},\\
&x^2y \longmapsto g^2f; \quad g^2f = g \circ g \circ f = g \circ \frac{\frac{1}{x} - 1}{\frac{1}{x}} = g \circ (1-x) = \frac{(1-x) - 1}{(1-x)} = \frac{x}{x-1},\\
&xy \longmapsto gf; \quad gf = g \circ f = 1 - x.
\end{aligned}$$

Since map φ preserves generating relations of S_3 after mapping to F, it must be a homomorphism. We also note that non-identity elements of S_3 (x, y, xy, yx, x^2y) map to non-identity elements of F, thus $\ker\varphi = 1_{S_3}$, φ is injective and an isomorphism. We conclude that F is isomorphic to S_3.

□

Problem 4

> Let S be a set with a law of composition. A partition $\Pi_1 \cup \Pi_2 \cup \cdots$ of S is compatible with the law of composition if for all i and j, the product set
>
> $$\Pi_i\Pi_j = \{xy \mid x \in \Pi_i, y \in \Pi_j\}$$
>
> is contained in a single subset Π_k of the partition.
> a) The set $\mathbb{Z}$ of integers can be partitioned into three sets [Pos], [Neg], [$\{0\}$]. Discuss the extent to which the laws of composition $+$ and $\times$ are compatible with this partition.

We check possible products of sets [Pos], [Neg], [{0}] for each law of composition, taking into account commutativity of the product of given sets, which stems from commutativity of + and × in $\mathbb{Z}$.

We first consider law of composition $+$:

$$\begin{gathered}
[\text{Pos}][\text{Pos}] = [\text{Pos}] \\
[\text{Neg}][\text{Neg}] = [\text{Neg}] \\
[\{0\}][\{0\}] = [\{0\}] \\
[\text{Pos}][\{0\}] = [\text{Pos}] \\
[\text{Neg}][\{0\}] = [\text{Neg}] \\
[\text{Pos}][\text{Neg}] = [\text{Pos}] \cup [\text{Neg}] \cup [\{0\}]
\end{gathered}$$

Product of [Pos] and [Neg] sets is not contained in any single set of partition, thus given partition is incompatible with $+$.

We then consider law of composition $\times$:

$$\begin{gathered}
[\text{Pos}][\text{Pos}] = [\text{Pos}] \\
[\text{Neg}][\text{Neg}] = [\text{Pos}] \\
[\{0\}][\{0\}] = [\{0\}] \\
[\text{Pos}][\{0\}] = [\{0\}] \\
[\text{Neg}][\{0\}] = [\{0\}] \\
[\text{Pos}][\text{Neg}] = [\text{Neg}]
\end{gathered}$$

Therefore given partition is compatible with $\times$.

b) Describe all partitions of integers that are compatible with the operation $+$.

Suppose partition $\Pi_0 \cup \Pi_1 \cup \cdots$ is compatible with $+$. Choose set Π_e that contains 0. We will prove that Π_e must be a subgroup of Z^+.

Proof. Closure: Consider product $\Pi_e\Pi_e$. Since $0 + 0 = 0 \in \Pi_e\Pi_e$ and 0 can be an element of only one set of partition:

$$\Pi_e\Pi_e = \Pi_e,$$

or equivalently: for any $a, b \in \Pi_e$

$$a + b \in \Pi_e$$

Inverses: Then consider arbitrary element $a \in \Pi_e$. Suppose its inverse $-a$ is an element of Π_{-a}. We know that $a + (-a) = 0 \in \Pi_e$, thus:

$$\Pi_e\Pi_{-a} = \Pi_e,$$

or equivalently: for any $a \in \Pi_e$

$$a + (-a) \in \Pi_e$$

Associativity follows from associativity of addition on $\mathbb{Z}$. Therefore, Π_e must be a group, specifically a subgroup of $\mathbb{Z}^+$.

□

Thus, Π_e is either $[\{0\}]$, $[\mathbb{Z}]$ or $[\mathbb{Z}a]$ where $a \in \mathbb{N}$. From this we have the following possible partitions of $\mathbb{Z}$ that are compatible with $+$:

- Partition by singletons: $\bigcup_{q \in \mathbb{Z}} [\{q\}]$;
- Single-set partition: $[\mathbb{Z}]$;
- Cosets of $\mathbb{Z}a$ for $a \in \mathbb{N}$:

$$\bigcup_{n \in [0,1,\ldots,a-1]} \Big[\{ka \mid k \in \mathbb{Z}\} + n \Big]$$

Problem 5

a) Prove that every group of even order contains an element of order 2.
b) Prove that every group of order 21 contains an element of order 3.

Proof. We first prove that group G of order m contains an element of order p such that p is prime and p divides m. Choose arbitrary element $a \in G$. Order of cyclical subgroup $\langle a \rangle$ must divide order of G by Lagrange's theorem (Artin 2.8.9), i.e.:

$$\big|\langle a \rangle\big| = pk, \quad k \in \mathbb{N}$$

From this we have:

$$\underbrace{aa \cdots aa}_{pk \text{ times}} = 1, \quad \underbrace{a^k a^k}_{p \text{ times}} = 1, \quad (a^k)^p = 1$$

and we have element a^k of order p.

Conclusion for $p = 2$ and $p = 3$ follows immediately.

□

Problem 6

Prove that two matrices

$$E = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \quad E' = \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}$$

generate the group $\mathrm{SL}_2(\mathbb{Z})$ of all integer matrices with determinant 1. Remember that the subgroup they generate consists of all elements that can be expressed as products using the four elements E, E', E^{-1}, E'^{-1}.

Consider arbitrary element of $\mathrm{SL}_2(\mathbb{Z})$:

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

such that $\det A = ad - bc = 1$. We will further refer to the bottom-left element (a_{21}) of any matrix as c and to the bottom-right element (a_{22}) of any matrix as d.

Claim. Matrix A can be column-reduced via right-multiplications by matrices E, E' and their inverses to a matrix A' with $c = 0$ and $d > 0$.

Proof. Our strategy will be to perform Euclidean algorithm on the bottom row of A via column reduction.

First we will transform A into a matrix such that both c and d are non-negative. If $c < 0$ and $d > 0$ we right-multiply by $(E'E^{-1}E')$:

$$A(E'E^{-1}E') = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} b & -a \\ d & -c \end{pmatrix}$$

If $d < 0$ and $c > 0$ we right-multiply by $(E'E^{-1}E')^{-1}$:

$$A(E'E^{-1}E')^{-1} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix} = \begin{pmatrix} -b & a \\ -d & c \end{pmatrix}$$

If both c and d are negative we right-multiply by $(E'E^{-1}E')^2$:

$$A(E'E^{-1}E')^2 = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} -a & -b \\ -d & -c \end{pmatrix}$$

Now with both c and d non-negative, if $c \leq d$ we right-multiply A by E^{-n} where $n = \left\lfloor \frac{d}{c} \right\rfloor$:

$$AE^{-n} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b - an \\ c & d - cn \end{pmatrix}$$

where c is a quotient and $(d - cn)$ is a remainder after the first iteration of Euclidean algorithm. If $c > d$ we right-multiply A by $(E')^{-n}$ where $n = \left\lfloor \frac{c}{d} \right\rfloor$:

$$AE'^{-n} = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & 0 \\ -n & 1 \end{pmatrix} = \begin{pmatrix} a - bn & b \\ c - dn & d \end{pmatrix}$$

where d is a quotient and $(c - dn)$ is a remainder after the first iteration of Euclidean algorithm.

We proceed and after a finite number of iterations we have either $c = 0, d > 0$ or $d = 0, c > 0$. In the former case we have our conclusion. Otherwise, we further right-multiply by $(E'E^{-1}E')$ in order to arrive at matrix A':

$$A' = \begin{pmatrix} a & b \\ c & 0 \end{pmatrix} (E'E^{-1}E') = \begin{pmatrix} -b & a \\ 0 & c \end{pmatrix}$$

We notice that $\det\left(\begin{smallmatrix} a & b \\ c & 0 \end{smallmatrix}\right) = 1$, therefore $-bc = 1$ and since $c > 0$, we have $b = -1$; thus

$$A' = \begin{pmatrix} 1 & a \\ 0 & c \end{pmatrix}$$

and we have A' as requested.

□

Corollary. Since $c = 0$ and $d > 0$ for A', then $\det A' = ad = 1$, therefore $a = d = 1$ and $A = E^k$ for some $k \in \mathbb{Z}$ and:

$$\begin{aligned} AE_1E_2 \cdots E_n &= A' = E^k \\ A &= E^k E_n^{-1} \cdots E_2^{-1} E_1^{-1}, \end{aligned}$$

i.e. any element $A \in \mathrm{SL}_2(\mathbb{Z})$ can be represented as a product of matrices E, E' and their inverses. Thus E and E' generate $\mathrm{SL}_2(\mathbb{Z})$.