18.701: Problem Set 3

Dmitry Kaysin

March 2020

Problem 1

Let $\mathbb{F}_p$ be a prime field, and let $V = \mathbb{F}_p^2$.

a) Prove that the number of bases of V is equal to the order of the general linear group $\mathrm{GL}_2(\mathbb{F}_p)$.

Proof. $B = \{(1,0),(0,1)\}$ is a basis of V, thus $\dim V = 2$. By Artin 3.5.9, any basis B' of V can be represented as $B' = BP$, where P is a unique invertible 2×2 matrix with entries in $\mathbb{F}_p$. Such matrices form the general linear group $\mathrm{GL}_2(\mathbb{F}_p)$. Therefore, the number of unique bases of V is equal to the order of $\mathrm{GL}_2(\mathbb{F}_p)$.

□

b) Prove that the order of the general linear group $\mathrm{GL}_2(\mathbb{F}_p)$ is

$$p(p+1)(p-1)^2,$$

and the order of the special linear group $\mathrm{SL}_2(\mathbb{F}_p)$ is

$$p(p+1)(p-1).$$

Proof. Order of $\mathrm{GL}_2(\mathbb{F}_p)$ is equal to the number of possible 2×2 matrices with entries in $\mathbb{F}_p$ and a non-zero determinant. We start from the first row. There are p^2 2-combinations with repetition from $\mathbb{F}_p = \{0, 1, \dots, p-1)\}$. Therefore, there are $p^2 - 1$ choices of how to compose the first row of the matrix (we exclude $(0,0)$). The second row can have any 2-combination with repetition from $\mathbb{F}_p$ except those that are equal to the first row multiplied by some $c \in \mathbb{F}_p$ (including 0). Therefore, there are $p^2 - p$ choices of how to compose the second row. We conclude that there are

$$(p^2-1)(p^2-p) = (p-1)(p+1)(p-1)p = p(p+1)(p-1)^2$$

choices of how to compose 2×2 invertible matrix with entries in $\mathbb{F}_p$, which is the order of $\mathrm{GL}_2(\mathbb{F}_p)$, as required.

Consider determinant homomorphism $\det : \mathrm{GL}_2(\mathbb{F}_p) \to \mathbb{F}_p^\times$, where $\mathbb{F}_p^\times$ is the multiplicative group of field $\mathbb{F}$. The special linear group $\mathrm{SL}_2(\mathbb{F}_p)$ is the kernel of det. By Lagrange's theorem:

$$|\mathrm{GL}_2(\mathbb{F}_p)| = |\ker \det| \cdot |\mathrm{im} \det| \tag{1}$$

We notice that homomorphism det is surjective, i. e. $\mathrm{im} \det = \mathbb{F}_p^\times$. Indeed, we can construct invertible matrix with determinant a for every $a \in \mathbb{F}_p^\times$:

$$\left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} : a \in F_n^\times \right\}$$

Therefore, $|\mathrm{im} \det| = |\mathbb{F}_p^\times| = p - 1$. Substituting to (1) we have:

$$\begin{gathered} p(p+1)(p-1)^2 = |\ker \det| \cdot (p-1), \\ |\ker \det| = p(p+1)(p-1). \end{gathered}$$

Therefore, order of $\mathrm{SL}_2(\mathbb{F}_p)$ is $p(p+1)(p-1)$, as required.

$\square$

Problem 2

Let GL denote the group $\mathrm{GL}_2(\mathbb{F}_3)$ of invertible matrices with entries modulo 3. This group operates on 2-dimensional vectors with entries mod 3 by matrix multiplication, as usual.

There are 9 vectors modulo 3, and four pairs $\pm v$ of nonzero vectors, namely

$$s_1 = \pm \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \quad s_2 = \pm \begin{pmatrix} 0 \\ 1 \end{pmatrix}, \quad s_3 = \pm \begin{pmatrix} 1 \\ 1 \end{pmatrix}, \quad s_4 = \pm \begin{pmatrix} 1 \\ -1 \end{pmatrix}.$$

The elements of GL permute the nonzero vectors, and they also permute the pairs of nonzero vectors. Sending a matrix to the permutation it defines gives us a homomorphism φ from GL to the symmetric group S_4 of permutations of $\{s_1, s_2, s_3, s_4\}$. For example, if $E = \left(\begin{smallmatrix} 1 & 1 \\ & 1 \end{smallmatrix}\right)$, then $\varphi(E)$ is the 3-cycle (s_2, s_3, s_4).

a) Show that φ is a surjective map, and determine its kernel.

Proof. We first find the kernel of φ. We compose 2×4 matrix from column-vectors that represent s_1, s_2, s_3 and s_4:

$$S = \left[\pm \begin{pmatrix} 1 \\ 0 \end{pmatrix} \; \pm \begin{pmatrix} 0 \\ 1 \end{pmatrix} \; \pm \begin{pmatrix} 1 \\ 1 \end{pmatrix} \; \pm \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right]$$

Matrix $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ such that $A \in \ker \varphi$ must preserve vectors (s_1, s_2, s_3, s_4), thus:

$$AS = S,$$

up to a sign of each vector. Multiplying:

$$\begin{aligned} &\left[\begin{pmatrix} \pm a \\ 0 \end{pmatrix} \; \begin{pmatrix} 0 \\ \pm d \end{pmatrix} \; \begin{pmatrix} (\pm a) + (\pm b) \\ (\pm c) + (\pm d) \end{pmatrix} \; \pm \begin{pmatrix} (\pm a) + (\pm b) \\ (\pm c) - (\pm d) \end{pmatrix} \right] = \\ &\qquad\qquad = \left[\pm \begin{pmatrix} 1 \\ 0 \end{pmatrix} \; \pm \begin{pmatrix} 0 \\ 1 \end{pmatrix} \; \pm \begin{pmatrix} 1 \\ 1 \end{pmatrix} \; \pm \begin{pmatrix} 1 \\ -1 \end{pmatrix} \right] \end{aligned}$$

From the first and the second vectors we can see that $a = \pm 1$, $b = 0$, $c = 0$, $d = \pm 1$. From the third vector we can see that $a = d$. We conclude that elements

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

form the kernel of φ. As per Lagrange's theorem:

$$|\mathrm{GL}| = |\ker \varphi| \cdot |\operatorname{im} \varphi|$$

Using the result of Problem 1, the order of GL is 48, thus

$$48 = 2 \cdot |\operatorname{im} \varphi|$$
$$|\operatorname{im} \varphi| = 24$$

The order of symmetric group S_4 is $4! = 24$, therefore $|\operatorname{im} \varphi| = |S_4|$ and φ must be surjective.

□

b) Determine the subgroup of GL that corresponds, by the Correspondence Theorem, to the alternating subgroup A_4 of S_4.

The special linear group $\mathrm{SL}_2(\mathbb{F}_3)$ corresponds to A_4.

Proof. Denote $\mathrm{SL} = \mathrm{SL}_2(\mathbb{F}_3)$. Using the result of Problem 1, the order of $\mathrm{SL}_2(\mathbb{F}_3)$ is 24. By the Correspondence Theorem, since φ is onto S_4 and $\ker \varphi \leq \mathrm{SL}$, there exists a subgroup G of S_4 such that $G = \varphi(\mathrm{SL})$ and

$$|\mathrm{SL}| = |\ker \varphi| \cdot |\varphi(\mathrm{SL})|$$
$$24 = 2 \cdot |\varphi(\mathrm{SL})|$$
$$|\varphi(\mathrm{SL})| = |G| = 12.$$

We remember that the special linear group SL is generated by elementary row-addition matrices of the form:

$$\begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ a & 1 \end{pmatrix}, \quad a \in \mathbb{F}_3,\ a \neq 0.$$

We check images of elementary matrices under φ:

$$\varphi\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} = (s_2 s_3 s_4), \quad \varphi\begin{pmatrix}1 & -1\\ 0 & 1\end{pmatrix} = (s_2 s_4 s_3),$$
$$\varphi\begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix} = (s_1 s_3 s_4), \quad \varphi\begin{pmatrix}1 & 0\\ -1 & 1\end{pmatrix} = (s_1 s_4 s_3).$$

We can see that images of the generators of SL are 3-cycles, even permutations, each distinct element of A_4 of order 3.

Consider arbitrary element $B \in \mathrm{SL}$, which can be represented as a product of elementary matrices:

$$B = E_1 \cdot E_2 \cdots E_n$$

Consider its image under φ:

$$\varphi(B) = \varphi(E_1 \cdot E_2 \cdots E_n)$$
$$\varphi(B) = \varphi(E_1) \cdot \varphi(E_2) \cdots \varphi(E_n)$$

Each $\varphi(E_k)$ above is a 3-cycle. Product of arbitrary number of 3-cycles is an even permutation, thus an element of A_4. Therefore, $\varphi(\mathrm{SL}) \leq A_4$. Since $|\varphi(\mathrm{SL})| = |A_4|$, we conclude that $\varphi(\mathrm{SL}) = A_4$ and SL corresponds to A_4.

□

c) Determine the subgroup of S_4 that corresponds to the subgroup of GL of upper triangular matrices.

Proof. Denote $U \leq \mathrm{GL}$, the subgroup of upper triangular matrices in GL:

$$\begin{pmatrix}a & b\\ 0 & c\end{pmatrix}$$

We first find the order of U. Since U must be invertible, $a \neq 0$ and $c \neq 0$. Therefore, there are 2 choices of a, 2 choices of c and 3 choices of b, for the total of 12 possible matrices in U. Therefore, $|U| = 12$.

We notice that $\ker\varphi \leq U$, therefore the Correspondence Theorem applies, and there must exist a subgroup $\varphi(U) \leq S_4$ of order 6.

There are 4 subgroups of order 6 in S_4, specifically groups of permutations of $\{s_1, s_2, s_3\}, \{s_2, s_3, s_4\}, \{s_1, s_2, s_4\}$ and $\{s_1, s_3, s_4\}$, each of which is isomorphic to the symmetric group S_3.

We check image of one of the elements of U under φ:

$$\varphi\begin{pmatrix}1 & 1\\ 0 & 1\end{pmatrix} = (s_2 s_3 s_4),$$

which is an element of the group of permutations of $\{s_2, s_3, s_4\}$. Therefore, U corresponds to the group of permutations of $\{s_2, s_3, s_4\}$, which is isomorphic to S_3.

□

Problem 3

Let $a = (a_1, \dots a_k)$ and $b = (b_1, \dots b_k)$ be points in k-dimensional space $\mathbb{R}^k$. A path from a to b is a continuous function on the unit interval $[0, 1]$ with values in $\mathbb{R}^k$, a function $X : [0, 1] \to \mathbb{R}^k$, sending $t \mapsto X(t) = (x_1(t), \dots x_k(t))$, such that $X(0) = a$ and $X(1) = b$. If S is a subset of $\mathbb{R}^k$ and if a and b are in S, define $a \sim b$ if a and b can be joined by a path lying entirely in S.
a) Show that $\sim$ is an equivalence relation on S. Be careful to check that any paths you construct stay within the set S.

Proof. We first check reflexivity. Consider $X : t \mapsto a$, constant function. $X(t)$ is continuous; $X([0, 1]) \subseteq S$ since $a \in S$; and $X(0) = X(1) = a$. Therefore, $a \sim a$.

We then check symmetry. Consider points $a, b \in S$ such that $a \sim b$. There must exist continuous function $X(t)$ such that $X[0, 1] \subseteq S$ and $X(0) = a, X(1) = b$. Consider function $Y(t) = X(1 - t)$. We notice that $Y(t)$ is a composition of continuous functions $f(t) = (1 - t)$ and $X(t)$, thus it must be continuous; $Y[0, 1] = X[0, 1] \subseteq S$; $Y(0) = X(1) = b$, $Y(1) = X(0) = a$. Therefore, $b \sim a$.

Lastly, we check transitivity. Consider points $a, b, c \in S$ such that $a \sim b$, $b \sim c$. There must exist continuous function $X(t)$ such that $X[0, 1] \subseteq S$ and $X(0) = a, X(1) = b$ and function $Y(t)$ such that $Y[0, 1] \subseteq S$ and $Y(0) = b, Y(1) = c$. Consider function $Z(t)$:

$$Z(t) = \begin{cases} X(2t), & \text{if } t \in [0, 0.5], \\ Y(2t - 1), & \text{if } t \in (0.5, 1]. \end{cases}$$

This is a piecewise function that is continuous since both X and Y are continuous on $[0, 1]$ and $X(1) = Y(0)$. We also notice that $Z[0, 1] = X[0, 1] \cup Y(0, 1] \subseteq S$ and $Z(0) = X(0) = a$, $Z(1) = Y(1) = c$. Therefore, $a \sim c$.

We conclude that $\sim$ is an equivalence relation.

□

b) A subset S is path connected if $a \sim b$ for any two points a and b in S. Show that every subset S is partitioned into path-connected subsets with the property that two points in different subsets cannot be connected by a path in S.

Proof. Equivalence relation $\sim$ on S induces a partition on S. Sets in a partition represent different equivalence classes and are disjoint. This means that every point of S belongs to one and only one of the partition sets and for any $a, b \in S$ that belong to different sets of the partition, $a \nsim b$. From the definition of path-connectedness, such points cannot be connected by a path in S.

□

Problem 4

The set of $n \times n$ matrices can be identified with the space $\mathbb{R}^{n\times n}$. Let G be a subgroup of $\mathrm{GL}_n(\mathbb{R})$. With the notation of the previous exercise, prove:
a) If A, B, C and D are in G, and if there are paths in G from A to B and from C to D, then there is a path in G from AC to BD.

Proof. We say that function $\varphi : [0,1] \to \mathrm{GL}_n(\mathbb{R})$ is continuous if φ is continuous in each of its entries. Since $A \sim B$, there exists function $X : [0,1] \to G$ such that $X(0) = A$, $X(1) = B$ and $\rho \circ X$ is continuous on $[0,1]$. Since $C \sim D$, there exists function $Y : [0,1] \to G$ such that $Y(0) = C$, $Y(1) = D$ and $\rho \circ Y$ is continuous on $[0,1]$.

Since G is a subgroup, AC, AD, and BD must be elements of G.

We first prove that $AC \sim AD$ with a path $f : t \mapsto AY(t)$. We notice that $f(0) = AY(0) = AC$ and $f(1) = AY(1) = AD$ (endpoints match). We know that Y is continuous on $[0,1]$. Left-multiplication by A is a linear map, thus continuous function. Composition of continuous functions is continuous, thus f is continuous on $[0,1]$. We also notice that for any $t \in [0,1] : Y(t) \in G$. Then $AY(t) \in G$. Therefore, $f[0,1] = A \cdot Y[0,1] \subseteq G$ (path is in G). We conclude that $AC \sim AD$.

We then prove that $AD \sim BD$ with a path $g : t \mapsto X(t)D$. We notice that $g(0) = X(0)D = AD$ and $g(1) = X(1)D = BD$ (endpoints match). We know that X is continuous on $[0,1]$. Right-multiplication by D is a linear map, thus continuous function. Composition of continuous functions is continuous, thus g is continuous on $[0,1]$. We also can see that $g[0,1] = X[0,1] \cdot D \subseteq G$ via the same reasoning as above (path is in G). We conclude that $AD \sim BD$.

Since $AC \sim AD$ and $AD \sim BD$, by transitivity, $AC \sim BD$.

□

b) The set of matrices that can be joined to the identity I forms a normal subgroup of G. (It is called the connected component of G).

Proof. Consider set $H \subseteq \mathrm{GL}_n(\mathbb{R})$ such that for all $A \in H : A \sim I$, where I is the identity element of $\mathrm{GL}_n(\mathbb{R})$. We note that $I \sim I$ by reflexivity. Thus, H contains the identity element.

For arbitrary $A \in H$

$$I \sim A,$$

then, by the result of part a):

$$A^{-1} \sim AA^{-1} = I.$$

Thus, H contains inverses.

For arbitrary $A, B \in H$:

$$A \sim I \sim B \sim B^{-1},$$

then, by the result of part a):

$$AB \sim B^{-1}B, \qquad AB \sim I.$$

Thus, H is closed under matrix multiplication.

Therefore, H is a subgroup of $\mathrm{GL}_n(\mathbb{R})$.

We will now prove that H is normal. Consider arbitrary $A \in H$ and $C \in \mathrm{GL}_n(\mathbb{R})$.

$$\begin{gathered} A \sim I, \\ CA \sim CI, \\ CAC^{-1} \sim CIC^{-1}, \\ CAC^{-1} \sim I, \\ CAC^{-1} \in H. \end{gathered}$$

Thus, H is normal.

□

Problem 5

a) The group $\mathrm{SL}_n(\mathbb{R})$ is generated by elementary matrices of the first type (row addition). Use this fact to prove that $\mathrm{SL}_n(\mathbb{R})$ is path-connected.

Proof. Any elementary matrix

$$E_a = \begin{pmatrix} 1 & a \\ 0 & 1 \end{pmatrix}, \qquad \text{for } a \in \mathbb{R}$$

can be joined to I, the identity matrix, via the path

$$\varphi : \, t \longmapsto I + \begin{pmatrix} 0 & at \\ 0 & 0 \end{pmatrix}$$

Thus, $E_a \sim I$. The same is true for elementary matrices E_a^T.

Any matrix $A \in \mathrm{SL}_n(\mathbb{R})$ can be represented as a product of elementary matrices E_a and E_a^T:

$$A = E_k \cdots E_2 E_1 I.$$

Using the result of Problem 4 a):

$$\begin{aligned} I &\sim I, \\ E_1 \cdot I &\sim I \cdot I, \\ E_2 \cdot E_1 \cdot I &\sim I \cdot I \cdot I, \\ &\cdots \\ A &\sim I. \end{aligned}$$

Thus, $\mathrm{SL}_n(\mathbb{R})$ is path-connected.

$\square$

> Show that $\mathrm{GL}_n(\mathbb{R})$ is a union of two path-connected subsets and describe them.

Proof. In this exercise we will use the group notation with lowercase letters representing elements of the group, i.e. matrices; e being the identity element of $\mathrm{GL}_n(\mathbb{R})$; and uppercase letters representing subgroups of $\mathrm{GL}_n(\mathbb{R})$.

Consider homomorphism $\varphi = \mathrm{sgn} \circ \det$, where (sgn) is a sign function and (det) is a determinant homomorphism. One can easily see that φ is indeed a homomorphism that sends $\mathrm{GL}_n(\mathbb{R})$ to $\mathbb{Z}_2$.

Denote H^+, the set $\{x \in \mathrm{GL}_n(\mathbb{R}) : \varphi(x) = 1\}$ (matrices with positive determinant). Denote H^-, the set $\{x \in \mathrm{GL}_n(\mathbb{R}) : \varphi(x) = -1\}$ (matrices with negative determinant). H^+ is a kernel of φ. Therefore, by the first isomorphism theorem, $\mathrm{GL}_n(\mathbb{R})\backslash H^+ \cong \mathbb{Z}_2$. Thus, there are only two elements in $\mathrm{GL}_n(\mathbb{R})\backslash H^+$, specifically H^+ and its coset H^-.

We will first show that H^+ is path-connected. As we have seen in the Problem 5 a), $\mathrm{SL}_n(\mathbb{R})$ is path-connected. To prove H^+ is path-connected it suffices to show that any matrix $a \in H^+$ can be path-connected to some matrix $c \in \mathrm{SL}_n(\mathbb{R})$. Consider function

$$f : t \longmapsto \begin{pmatrix} (1-t) + t\dfrac{1}{\det a} & 0 \\ 0 & 1 \end{pmatrix}$$

We claim that function $f(t)a$ for $t \in [0,1]$ is the required path. Indeed

$$f(0)a = ea = a, \quad \det f(1)a = \det\left({}^1\!/_{\det a}\right) \cdot \det a = 1,$$

thus $f(1)a = c$, where c is some element of $\mathrm{SL}_n(\mathbb{R})$. Every $f(t)$ has positive determinant, thus every $f(t)a$ is in H^+. Finally, $f(t)$ is continuous and right-multiplication is continuous, thus $f(t)a$ is continuous. Therefore, $a \sim c \sim e$ and we conclude that H^+ is path-connected.

We will now show that H^- is path-connected. Consider arbitrary $b \in H^-$. Since H^- is a coset of H^+, there exists $a \in H^+$ such that $b = xa$ for some $x \in H^-$. We know that $a \sim e$. By the result of Problem 4 a):

$$xa \sim xe, \quad b \sim xe.$$

Since $xe \in H^-$, we conclude that all elements of H^- can be path-connected via xe, thus H^- is path-connected. We also note that no two elements $b \in H^-$, $a \in H^+$ are path-connected, otherwise, b would be path-connected to e and by the result of the Problem 4 b), b would be an element of H^+, while H^- and H^+ are disjoint.

We conclude that both H^+ and H^- are path-connected and they together partition $\mathrm{GL}_n(\mathbb{R})$, as requested.

$\square$