18.701: Problem Set 1

Dmitry Kaysin

March 2020

Diagnostic Problem

Let a and b be elements of a group G. Prove that ab and ba have the same order.

Proof. Element of a group G has order n if $a^n = e$ where e is an identity element of G. Suppose ab has order n, then:

$$(ab)^n = e$$

By associativity of group operation:

$$\underbrace{a\ \overbrace{bab\cdots aba}^{(ba)\ n-1\text{ times}}\ b}_{(ab)\ n\text{ times}} = e$$

From this we have:

$$\begin{aligned}
a(ba)^{n-1}b &= e \\
a(ba)^{n-1}ba &= ea \\
a(ba)^n &= ea \\
a(ba)^n &= ae \\
a^{-1}a(ba)^n &= a^{-1}ae \\
(ba)^n &= e
\end{aligned}$$

□

Problem 1

Let A be an $n \times n$ matrix with integer entries a_{ij}. Prove that A is invertible and that its inverse A^{-1} has integer entries, if and only if $\det A = \pm 1$.

Proof. We know that for arbitrary square matrices A, B:

$$\det A \cdot \det B = \det AB$$

Square matrix A is invertible if and only if $\det A \neq 0$. Then A is invertible, thus:

$$\det A \cdot \det(A^{-1}) = \det I_n = 1$$

Forward direction: Looking at the basic formula for determinant, we conclude that matrix with integer entries has integer determinant. Since $\det(A^{-1})$ must be integer, we can see that $\det A$ is integer if and only if $\det(A^{-1}) = \pm 1$. Then $\det A = \pm 1$ as requested.

Backward direction: Suppose $\det A = \pm 1$. We know that:

$$A^{-1} = \frac{1}{\det A}(\operatorname{adj} A) = \pm(\operatorname{adj} A)$$

Entries of adjugate of A are derived from minors of A, which are determinants of smaller matrices composed from entries of A. Therefore adjugate of a matrix with integer entries itself has integer entries, thus A^{-1} must have integer entries. □

Problem 2

Consider a general system $AX = B$ on m linear equations in n unknowns, where m and n are not necessarily equal. The coefficient matrix A may have a left inverse L, a matrix such that $LA = I_n$. If so, we may try to solve the system as we learn to do in school:

$$AX = B, \quad LAX = LB, \quad X = LB.$$

But when we try to check our work by running the solution backward, we run into trouble: If $X = LB$, then $AX = ALB$. We seem to want L to be right inverse, which isn't what was given.
Exactly what does the sequence of steps above show? What would the existence of a right inverse show?

System of equations may have one or many solutions or may have no solutions. In our original equation $AX = B$ we implicitly assume existence of a solution. If no solution exists, all further operations are meaningless, i.e. X, which is equal to LB in the last expression is not guaranteed to solve original equation. If solution exists, our argument proves that it must be equal to LB.

On the other hand, if right inverse of A exists (denote it R) it is easy to see that $X = RB$ solves the original equation:

$$AX = B, \quad ARB = B, \quad B = B,$$

which confirms existence of a solution to $AX = B$. However, this is only one solution while we know that a system of equations may have infinitely many solutions.

As a side note, we conclude that if both left and right inverses exist, then the system of equations must have one and only one solution $LB = RB$. In this case L must be equal to R.

Problem 3

Denote R discrete region (finite set of integer lattice points) in the plane. Denote its boundary ∂R (the set of lattice points that are not in R, but which are at a distance 1 from some point of R). Thus R is the interior of the region $\overline{R} = R \cup \partial R$.
Find function f defined on $\overline{R}$ that is equal to β on the boundary, and that satisfies the discrete Laplace equation at all points in the interior:

$$f(u+1,v) + f(u-1,v) + f(u,v+1) + f(u,v-1) - 4f(u,v) = 0.$$

Denote x_{uv} value of f on interior point (u,v). Denote β_{uv} value of f on boundary point (u,v).

We can index interior points x_k and boundary points β_m using lexicographical order on (u,v).

Discrete Laplace equation in $\mathbb{R}^2$ implies that each x_k is equal to the average of neighbouring four points, or:

$$4x_k = \sum_{i \in I} x_i + \sum_{j \in J} \beta_j,$$

where I is the set of neighbouring interior points, and J is the set of neighbouring boundary points.

Using matrix form:

$$(4I_K - A_x)X = A_\beta B$$

where $K = |R|$ is an identity matrix of size equal to the number of interior points;
X is a column vector of unknown x_k; size $K \times 1$;
A_x is a square matrix with rows representing adjacency of interior points ($a_{ij} = 1$ if x_j is neighbour of x_i and $i \neq j$); size $K \times K$;
A_β is a matrix with rows representing, which boundary points are neighbouring each interior point ($a_{ij} = 1$ if β_j is neighbour of x_i); size $K \times M$, where $M = |\partial R|$ is the number of boundary points;
B is a column vector of β_m; size $M \times 1$.

a) When R is the set of five points $(0,0),(0,\pm 1),(\pm 1,0)$, there are eight boundary points. Write down the system of linear equations in this case, and solve the Dirichlet problem where β is the function on ∂R defined by $\beta_{uv}=0$ if $v \leq 0$ and $\beta_{uv}=1$ if $v>0$.

We set up the problem as follows:

$$\left(4\begin{pmatrix}1&0&0&0&0\\0&1&0&0&0\\0&0&1&0&0\\0&0&0&1&0\\0&0&0&0&1\end{pmatrix}-\begin{pmatrix}0&0&1&0&0\\0&0&1&0&0\\1&1&0&1&1\\0&0&1&0&0\\0&0&1&0&0\end{pmatrix}\right)X=$$

$$=\begin{pmatrix}1&1&1&0&0&0&0&0\\0&1&0&1&0&1&0&0\\0&0&0&0&0&0&0&0\\0&0&1&0&1&0&1&0\\0&0&0&0&0&1&1&1\end{pmatrix}\begin{pmatrix}0\\0\\1\\0\\1\\0\\1\\0\end{pmatrix}$$

Solving for X we have:

$$X=\begin{pmatrix}{}^{17}\!/_{48}\\{}^{5}\!/_{48}\\{}^{20}\!/_{48}\\{}^{41}\!/_{48}\\{}^{17}\!/_{48}\end{pmatrix}$$

b) The maximum principle states that a harmonic function takes on its maximal value on the boundary. Prove the maximum principle for discrete harmonic functions.

We assume that this proposition is made for a non-constant function.

Proof. Suppose non-constant f achieves maximum value on interior point k and $f(k)=x_k$. Then $x_k \geq p_i$ for all $i \in I$ where I is the set of neighbouring points of k (both of interior and of boundary). However in this case the Laplace equation holds only if $x_k=p_i$ for all $i \in I$. We proceed recursively for each p_i and conclude that value of f at all points of $\overline{R}$ is equal to x_k, which implies that f is constant. Contradiction. Therefore, non-constant f cannot achieve maximum value on interior point.

□

c) Prove that the discrete Dirichlet problem has a unique solution for every region R and every boundary function β.

Proof. We once again consider the system of linear equations representing the problem:

$$(4I_K - A_x)X = A_\beta B$$

Solution to non-homogeneous equation exists for any right-hand side and is unique if the only solution to homogeneous equation is a zero vector. Suppose, X is a solution to homogeneous system of equations

$$(4I_K - A_x)X = 0$$

We immediately see that $-X$ must also be a solution. Right-hand side being zero vector indicates that value of f at all points of R adjacent to boundary ∂R is equal to 0. Now consider R°, interior of R. From the maximum principle (part b) we know that f restricted to R attains maximum at the boundary of R°. From this we have that $f(p) \leq 0$ for all $p \in R^\circ$. Both X and $-X$ must satisfy this condition, thus:

$$x_i \leq 0 \quad \text{and} \quad -x_i \leq 0 \quad \text{for all entries } x_i \text{ of } X$$

Therefore each x_i must be equal to 0. From this we have that zero vector is the only solution to the homogeneous equation above.

Therefore, solution to the discrete Dirichlet problem exists for any region R and boundary values β and such solution is unique.

□

Problem 4

a) Prove that the elementary matrices of the first (row-addition) and third (row-multiplication) types generate $\mathrm{GL}_n(\mathbb{R})$.

Proof. Group $\mathrm{GL}_n(\mathbb{R})$ consists of (square) invertible matrices. We know that any invertible matrix can be transformed into identity matrix via a series of matrix multiplications by elementary matrices (row-multiplication, row-addition, row-switching). We note that any row-switching transformation $T_{i,j}$ can be represented as a series of row multiplications and row additions:

$$T_{i,j} = D_i(-1) \cdot L_{i,j}(1) \cdot L_{j,i}(-1) \cdot L_{i,j}(1)$$

Therefore for arbitrary $A \in \mathrm{GL}_n(\mathbb{R})$:

$$E_k \cdots E_3 E_2 E_1 A = I_n,$$

where E_i is either row-multiplication or row-addition transformation.

Inverse of row-multiplication transformation is row-multiplication transformation; inverse of row-addition transformation is row-addition transformation, thus:

$$(E_k \cdots E_3 E_2 E_1)^{-1}(E_k \cdots E_3 E_2 E_1)A = (E_k \cdots E_3 E_2 E_1)^{-1} I_n$$
$$A = E_1^{-1} E_2^{-1} E_3^{-1} \cdots E_k^{-1} I_n,$$

where each E_i^{-1} is either row-multiplication or row-addition transformation. We also note that identity matrix I_n is equal to row-multiplication transformation matrix $D_1(1)$.

Therefore any matrix in $\mathrm{GL}_n(\mathbb{R})$ can be represented by elementary matrices that corresponding to row-multiplication and row-addition transformations. Row-multiplication and row-addition matrices are themselves elements of $\mathrm{GL}_n(\mathbb{R})$, thus they generate $\mathrm{GL}_n(\mathbb{R})$.

□

> b) Prove that the elementary matrices of the first type generate $\mathrm{SL}_n(\mathbb{R})$. Do the 2×2 case first.

Proof. We notice that left-multiplication by elementary matrix of the first type results in adding multiple of one row to another one. On the other hand, right-multiplication by elementary matrix of the first type results in adding multiple of one column to another one.

For the purpose of convenience we shall call elementary matrix of the first type L-matrices for the rest of this exercise. We first note that any L-matrix (assuming a row/column is not added to itself) has determinant of 1. Thus L-matrices and their inverses are elements of $\mathrm{SL}_n(\mathbb{R})$. Consider arbitrary 2×2 matrix, $a, b, c, d \in \mathbb{R}$:

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

We notice that we can transform A into an identity matrix using only left multiplication by L-matrices. We start with:

$$\begin{pmatrix} 1 & {}^{(1-a)}\!/_{c} \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & {}^{d-(ad-bc)}\!/_{c} \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & {}^{(d-1)}\!/_{c} \\ c & d \end{pmatrix},$$

with the last equality being true because $ad - bc = \det A$ and $\det A = 1$ since $A \in \mathrm{SL}_2(\mathbb{R})$. We continue with the transformations:

$$\begin{pmatrix} 1 & 0 \\ -c & 1 \end{pmatrix} \begin{pmatrix} 1 & {}^{(d-1)}\!/_{c} \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & {}^{(d-1)}\!/_{c} \\ 0 & {}^{-c(d-1)}\!/_{c} + d \end{pmatrix} = \begin{pmatrix} 1 & {}^{(d-1)}\!/_{c} \\ 0 & 1 \end{pmatrix},$$

with the last term being an L-matrix. Summarizing, we have

$$L_2 L_1 A = L_3 I$$
$$A = L_1^{-1} L_2^{-1} L_3 I,$$

where I is a 2×2 identity matrix. Since inverse of an L-matrix is itself an an L-matrix, we conclude that 2×2 L-matrices generate $\mathrm{SL}_2(\mathbb{R})$.

For the general case of matrices of size $n \times n$, we proceed by induction on n with $n = 2$ being the induction basis. Suppose any $(n-1)$-size square matrix can be reduced to identity matrix via a series of left-multiplications by L-matrices. Consider $n \times n$ matrix A. We will provide examples for $n = 3$. Start with reducing top-left $(n-1) \times (n-1)$ submatrix of A to identity matrix:

$$A \to \begin{pmatrix} 1 & 0 & a_{13} \\ 0 & 1 & a_{23} \\ a_{31} & a_{32} & a_{33} \end{pmatrix}$$

Determinant of this transformed matrix is equal to:

$$a_{nn} - \left(a_{1n}a_{n1} + a_{2n}a_{n2} + \cdots + a_{(n-1)n}a_{n(n-1)}\right) = 1 \tag{1}$$

since matrix is an element of $\mathrm{SL}_n(\mathbb{R})$.

We proceed with reducing all entries of the n-th row to 0. After this series of transformation bottom-right entry becomes equal to $a_{nn} - (a_{1n}a_{n1} + a_{2n}a_{n2} + \cdots + a_{(n-1)n}a_{n(n-1)})$, which is equal to 1 by (1): We proceed with the transformations and reduce $a_{1n}, a_{2n}, \cdots, a_{(n-1)n}$ to 0:

$$\begin{pmatrix} 1 & 0 & a_{13} \\ 0 & 1 & a_{23} \\ 0 & 0 & 1 \end{pmatrix} \to \begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

We've arrived to an $n \times n$ identity matrix, which concludes the proof.

□

Problem 5

By definition, English words have the same pronunciation if their phonetic spellings in the dictionary are the same. The homophonic group $\mathcal{H}$ is generated by the letters of the alphabet, subject to the following relations: English words with the same pronunciation represent equal elements of the group. Thus $be = bee$, and since $\mathcal{H}$ is a group, we can cancel be to conclude that $e = 1$. Try to determine the group $\mathcal{H}$.

Proof. We examine a few (British English) homophones to better understand the structure of the group $\mathcal{H}$ (source):

$$\begin{gathered} be = bee, \quad e = 1; \\ sea = see, \quad a = e, \quad a = 1; \\ sale = sail, \quad sl = sil, \quad i = 1; \\ feel = fill, \quad fl = fll, \quad l = 1; \end{gathered}$$

$$plum = plumb, \quad b = 1;$$
$$medal = meddle, \quad d = 1;$$
$$die = dye, \quad i = y, \quad y = 1;$$
$$hour = our, \quad h = 1;$$
$$knight = night, \quad k = 1;$$
$$sole = soul, \quad u = 1;$$
$$son = sun, \quad o = u; \quad o = 1$$
$$flour = flower, \quad ou = we, \quad w = 1;$$
$$right = write, \quad rgt = rt, \quad g = 1;$$
$$scene = seen, \quad scn = sn, \quad c = 1;$$
$$cell = sell, \quad c = s, \quad s = 1;$$
$$bard = barred, \quad rd = rrd, \quad r = 1;$$
$$tacks = tax, \quad cks = x, \quad x = 1;$$
$$boos = booze, \quad s = ze, \quad z = 1;$$
$$tough = tuff, \quad h = ff, \quad draft = draught, \quad f = h = ff, \quad f = 1$$
$$faze = phase, \quad f = p, \quad p = 1;$$
$$profit = prophet, \quad h = 1;$$
$$genes = jeans, \quad j = 1;$$
$$band = banned, \quad n = 1;$$
$$peak = pique, \quad q = 1;$$
$$metal = mettle, \quad t = 1;$$
$$links = lynx, \quad x = 1;$$
$$dammed = damned, \quad m = 1;$$
$$chivvy = chivy, \quad v = 1.$$

Therefore, group $\mathcal{H}$ is trivial.

□