MA251 Algebra 1 - Week 9

Louis Li

April 3, 2023

1 Week 9

Question 1.

Calculate the SVD of the following matrices, that is find orthogonal matrices P, Q such that

$$\begin{pmatrix} D & 0 \\ 0 & 0 \end{pmatrix} = P^T A Q,$$

where $D = diag(\gamma_1, ..., \gamma_d)$ with $\gamma_1 \geq \gamma_2 \geq ... \geq \gamma_d > 0$.

$$A_1 = \begin{pmatrix} -\sqrt{2} & 0 \\ 0 & \sqrt{3} \end{pmatrix}, \quad A_2 = \begin{pmatrix} -1 & 5 \\ 5 & -1 \end{pmatrix}, \quad A_3 = \begin{pmatrix} 3 & 2 \\ -2 & -6 \\ -6 & 3 \end{pmatrix}.$$

Solution.

(a) For A_1, it is a diagonal matrix with real numbers, however we need to change the sign of the first entry and swap the entries so they go in the right order. We can change the orthonormal basis by sending $\mathbf{e}_1$ to $\mathbf{e}_2$ and $\mathbf{e}_2$ to $\mathbf{e}_1$. That means $P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$ and then

$$P^T A_1 P = \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} -\sqrt{2} & 0 \\ 0 & \sqrt{3} \end{pmatrix} \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} \sqrt{3} & 0 \\ 0 & -\sqrt{2} \end{pmatrix}.$$

Choose $Q = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$, we see that first of all Q is still orthogonal and second

$$P^T A_1 Q = \begin{pmatrix} \sqrt{3} & 0 \\ 0 & \sqrt{2} \end{pmatrix} = D,$$

so $A_1 = PDQ^T$, which is the SVD.

(b) Similarly, A_2 is a symmetric matrix, and hence it is diagonalisable by an orthogonal basis change. We find its eigenvalues are $\lambda_1 = -6$ and $\lambda_2 = 4$. For $\lambda = -6$, the corresponding eigenvector is $\mathbf{v}_1 = \begin{pmatrix} -1 \\ 1 \end{pmatrix}$. For $\lambda = 4$, the corresponding eigenvector is $\mathbf{v}_2 = \begin{pmatrix} 1 \\ 1 \end{pmatrix}$. Again, we need to make their length to be 1. Hence, the eigenvectors are $\mathbf{v}_1' = \frac{1}{\sqrt{2}} \begin{pmatrix} -1 \\ 1 \end{pmatrix}$ and $\mathbf{v}_2' = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 \\ 1 \end{pmatrix}$. Since they form an orthonormal basis, we choose $P = \begin{pmatrix} -\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \end{pmatrix}$ and

$$P^T A_2 P = D' = \begin{pmatrix} -6 & 0 \\ 0 & 4 \end{pmatrix}.$$

Again we need to change the sign in the top left entry, so choose $Q = \frac{1}{\sqrt{2}} \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix}$ instead, and this will sort out the minus sign on the -6. Therefore,

$$P^T A_2 Q = D = \begin{pmatrix} 6 & 0 \\ 0 & 4 \end{pmatrix},$$

so $A_2 = PDQ^T$, which is the SVD.

(c) For A_3, we follow the method of the finding SVD.

$$A_3^T A_3 = \begin{pmatrix} 3 & -2 & -6 \\ 2 & -6 & 3 \end{pmatrix} \begin{pmatrix} 3 & 2 \\ -2 & -6 \\ -6 & 3 \end{pmatrix} = \begin{pmatrix} 49 & 0 \\ 0 & 49 \end{pmatrix}.$$

Since the diagonal matrix, the eigenvalues are 49. Hence the singular values are $\sqrt{49} = 7$, and our diagonal matrix will be $D = \begin{pmatrix} 7 & 0 \\ 0 & 7 \\ 0 & 0 \end{pmatrix}$. We need to choose an orthonormal basis of $\mathbb{R}^2$ so that $A_3^T A_3$ is diagonal. However, since the matrix is already diagonal, so the standard basis $\mathbf{e}_1$ and $\mathbf{e}_2$ are the choices. Therefore, $Q = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Still like QR decomposition, define the columns of A_3 be $\mathbf{g}_1, \mathbf{g}_2$. Therefore,

$$\mathbf{f}_1 = \frac{\mathbf{g}_1}{|\mathbf{g}_1|} = \frac{1}{7} \begin{pmatrix} 3 \\ -2 \\ -6 \end{pmatrix}.$$

Choose $\mathbf{f}_2' = \mathbf{g}_2 - (\mathbf{g}_2 \mathbf{f}_1)\mathbf{f}_1$, we get

$$\mathbf{f}_2 = \frac{\mathbf{f}_2'}{|\mathbf{f}_2'|} = \frac{1}{7} \begin{pmatrix} 2 \\ -6 \\ 3 \end{pmatrix}.$$

We need to find another third vector which extends this to an orthonormal basis. We can solve a two simultaneous equations

$$\begin{cases} 3a - 2b - 6c &= 0 \\ 2a - 6b + 3c &= 0 \end{cases}.$$

Choose $\mathbf{f}_3' = \begin{pmatrix} 6 \\ 3 \\ 2 \end{pmatrix}$, which has length 7 then

$$\mathbf{f}_3 = \frac{\mathbf{f}_3'}{|\mathbf{f}_3'|} = \frac{1}{7} \begin{pmatrix} 6 \\ 3 \\ 2 \end{pmatrix}.$$

Then

$$P = \frac{1}{7} \begin{pmatrix} 3 & 2 & 6 \\ -2 & -6 & 3 \\ -6 & 3 & 2 \end{pmatrix}.$$

Then we check that

$$A_3 = PDQ^T,$$

which is the SVD.

□

Question 2.

Show that if $\phi : G \to H$ is an isomorphism, then $|g| = |\phi(g)|$ for all $g \in G$.

Proof.

Suppose that the order of g is n and by isomorphism of g, then

$$n\phi(g) = \phi(g) + ... + \phi(g) = \phi(g + g + ...g) = \phi(ng) = \phi(0) = 0.$$

Hence, $|\phi(g)|\,|n$. Suppose $|\phi(g)|$ is a proper divisor of n, say m. Then $0 = m\phi(g) = \phi(mg)$, but since ϕ is an isomorphism and hence in particular it is a bijection. Therefore, $\phi(mg) = 0$ if and only if $mg = 0$, which contradicts n being the order of g. □

Question 3.

What is the order of the cyclic subgroup generated by mg for general m (without the assumption that $m|n$)?

Solution.

Consider the elements of the subgroup: $\{zmg|z \in \mathbb{Z}\} = 0, mg, 2mg, ...$ This will not repeat until we hit 0. Since if $rmg = smg$ for some $r < s$, then $(s - r)mg = 0$ and so we would have seen 0 already. Therefore, the size of this subgroup is the least positive integer r such that $rmg = 0$. Hence, $n = |g|\,|rm$. The least positive integer r for which this is true is $\frac{n}{\gcd(n,m)}$. □

Question 4.

How many elements of order 2 are there in the following groups? How about elements of order 3?

(a) $\mathbb{C}^\times$ (under multiplication);

(b) $\mathbb{Z}$;

(c) $\mathbb{Z}/m$ for any positive integer $m > 0$.

Solution.

(a) For order 2, we need all elements g that are not 1, but $g^2 = 1$. Therefore, only $g = -1$ satisfies this condition. For order 3, we need all elements g that are not 1, but $g^3 = 1$. Hence, we have

$$\begin{aligned} g^3 &= 1 \\ g &= e^{i\frac{0+2\pi k}{3}} \\ g &= e^{i\frac{2\pi}{3}} \text{ or } e^{i\frac{4\pi}{3}}. \end{aligned}$$

(b) For order 2, we need elements g that are not 1 but $2g = 0$. As $g \in \mathbb{Z}$, this is impossible as it implies that $g = 0$. Similar for order 3, no elements of order 2 or 3 in $\mathbb{Z}$.

(c) Since $\mathbb{Z}/m$ is a quotient group defined as the set of integers $\{0, 1, ..., m-1\}$ modulo m, therefore it has order m. By Lagrange's theorem, it has an element of order n where $n|m$. The elements of order 2 are integers r between 1 and $m-1$ with $2r = 0 \mod m$. This means $2r$ needs to be divisible by m and for r in $1, ..., m-1$, we see that $r = \frac{m}{2}$ is the only solution. Thus we have exactly one element of order 2 when m is even and 0 elements of order 2 when m is odd.

Similarly, for $n = 3$, we find 0 elements of order 3 when m is not divisible by 3 and 2 elements when m is divisible by 3.

□

Question 5.

Show that the group of non-zero complex numbers $\mathbb{C}^\times$ under the operation of multiplication has finite cyclic subgroups of all possible orders.

Proof.

The subgroup generated by a primitive nth root of unity, which is $e^{\frac{2\pi i}{n}}$, will be cyclic of order n. □

Question 6.

Let G be an abelian group and let H and K be two subgroups with $H \leq K$.

(a) Show that K/H is a subgroup of G/H;

(b) Define a map $\phi : G/H \to G/K$ by $\phi(H+g) = K+g$. Check this is a group homomorphism;

(c) Use part (ii) and the first isomorphism theorem to prove that $\frac{G/H}{K/H} \cong G/K$.

Proof.

(a) Since the coset $H+0 \in K/H$, and for all cosets $H+k_1, H+k_2$, $(H+k_1)-(H+k_2) \in K/H$. Therefore K/H is non-empty. Since $(H+k_1)-(H+k_2) = H+(k_1-k_2)$ which is another coset of H in K. In fact, K/H is a group since H is a subgroup of K and so it must be a subgroup of G/K since it is contained in it.

(b) First we need to check it is well-defined. Take two different coset representatives of $g+H$, say g and $g+h$, do we have the same answer for $\phi(H+g)$? Since $H \leq K$, so $h \in K$ and $\phi(H+g) = K+g$ and thus $K+g = K+g+h$.

Then

$$\begin{aligned}\phi((H+g_1)+(H+g_2)) &= \phi(H+g_1+g_2)\\ &= K+g_1+g_2\\ &= (K+g_1)+(K+g_2)\\ &= \phi(H+g_1)+\phi(H+g_2).\end{aligned}$$

(c) We need to check that ϕ is surjective and has kernel K/H. It is surjective since any coset $g+K$ is mapped to by $H+g$. Note that

$$K = \phi(H+g) = K+g$$

if and only if $g \in K$. Therefore the kernel of ϕ consists of all cosets $H+k$ for $k \in K$, which is K/H.

□