(SQUARE) ROOTS OF BOUNDED OPERATORS

BY PROF. MOHAMMED HICHEM MORTAD

Students may contact me at : **mhmortad@gmail.com** for any questions.

1. Basics

Definition. Let $A \in B(H)$. We say that $B \in B(H)$ is a **square root** of A if $B^2 = A$.

We can similarly define a cube root. Indeed, we say that $B \in B(H)$ is a **cube root** of some $A \in B(H)$ if $B^3 = A$.

More generally, we say that $B \in B(H)$ is a n**th root** of some $A \in B(H)$ if $B^n = A$ (where $n \in \mathbb{N}$).

Example 1.1. Let I be the identity 2×2 matrix, i.e.

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

Then I has infinitely many square roots. Indeed,

$$A_x = \begin{pmatrix} x & 1 \\ 1-x^2 & -x \end{pmatrix}$$

represents, for each $x \in \mathbb{R}$, a square root of I (as $A_x^2 = I$ whichever x).

In fact, I has infinitely many self-adjoint square roots! Just consider

$$A_x = \begin{pmatrix} x & \sqrt{1-x^2} \\ \sqrt{1-x^2} & -x \end{pmatrix}$$

where $x \in [-1, 1]$. Then

$$A_x^2 = I, \ \forall x \in [-1, 1].$$

Remarks.

1. Every self-adjoint operator has roots of any order.
2. More generally, normal operators have roots of any order. The proof in the finite dimensional setting is based on the Complex Spectral Theorem.

Example 1.2. A square root of

$$\begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}$$

is:

$$\begin{pmatrix} 1 & 0 \\ 0 & \sqrt{2} \end{pmatrix}.$$

Another one is:

$$\begin{pmatrix} -1 & 0 \\ 0 & \sqrt{2} \end{pmatrix}.$$

Are there more? The answer is yes!

Theorem 1.3. *Let A be an $n \times n$ matrix. Assume that A is defined over the complex field and that A has n pairwise distinct nonzero eigenvalues. Then A has exactly 2^n square roots.*

Proof. A way of establishing this result is via a proof by induction. Assume that an $n \times n$ matrix (already having n pairwise distinct nonzero eigenvalues) has 2^n square roots. Let A be an $(n+1) \times (n+1)$ matrix having $n+1$ pairwise distinct nonzero eigenvalues. Hence A is diagonalizable and so there exists an invertible matrix T such that

$$T^{-1}AT = \begin{pmatrix} \lambda_1 & 0 & 0 & \cdots & 0 \\ 0 & \lambda_2 & 0 & \cdots & 0 \\ \vdots & \ddots & \ddots & \ddots & \vdots \\ 0 & \cdots & 0 & \lambda_n & 0 \\ 0 & \cdots & \cdots & 0 & \lambda_{n+1} \end{pmatrix} := D$$

where λ_k, $k = 1, \cdots, n, n+1$ are pairwise different and nonzero. By the induction's assumption, the matrix having the eigenvalues λ_k, $k = 1, \cdots, n$ in its diagonal has 2^n square roots. Thus, it becomes clear that D has $2 \times 2^n = 2^{n+1}$ square roots (as also $\lambda_{n+1} \neq 0$) whereby A too has 2^{n+1} square roots, as wished. □

Remark. The fact that we have assumed that the eigenvalues have to be pairwise distincts and non zero is essential. For example, we saw above that the identity matrix on $\mathbb{C}^2$, which has two equal eigenvalues, has infinitely many square roots (and not only 2^2). Also, the matrix $A = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, which has one zero eigenvalue, has two square roots only!

Thanks to the spectral theorem for a normal matrix A, we may write $U^*AU = D$ where D is diagonal, and for some unitary U. Now, given the fact that we can easily find square roots of diagonal matrices, we may say the following:

Theorem 1.4. *A square root of a normal matrix A is of the form*

$$B = UCU^*$$

where C is a square root of D defined above.

Proof. The proof is easy. We have

$$B^2 = UCU^*UCU^* = UC^2U^* = UDU^* = A,$$

as wished. $\square$

Example 1.5. On $\mathbb{C}^2$, let

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

Then A is self-adjoint (but not positive) and has two distinct non zero eigenvalues and so A ought to have *four and only four* square root of any nature. To find them explicitly, we need to diagonalize A. We find

$$A = UDU^* \text{ where } D = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix} \text{ and } U = \begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Then D has four square roots given by

$$\begin{pmatrix} -1 & 0 \\ 0 & -i \end{pmatrix}, \begin{pmatrix} -1 & 0 \\ 0 & i \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & -i \end{pmatrix} \text{ and } \begin{pmatrix} 1 & 0 \\ 0 & i \end{pmatrix}.$$

The square roots of A are therefore

$$\frac{1}{2}\begin{pmatrix} -1-i & -1+i \\ -1+i & -1-i \end{pmatrix}, \frac{1}{2}\begin{pmatrix} -1+i & -1-i \\ -1-i & -1+i \end{pmatrix}, \frac{1}{2}\begin{pmatrix} 1-i & 1+i \\ 1+i & 1-i \end{pmatrix}$$

and

$$\frac{1}{2}\begin{pmatrix} 1+i & 1-i \\ 1-i & 1+i \end{pmatrix}.$$

Remark. As one observes none of the previous matrices is self-adjoint, let alone its positiveness. In other words, *all square roots in this example are non self-adjoint.*

However, ***a positive operator has one, and only one, positive square root.*** We have:

Theorem 1.6. *Let $A \in B(H)$ be positive. Then A possesses a* ***unique positive*** *square root denoted exclusively by $\sqrt{A}$ (or $A^{\frac{1}{2}}$). Moreover, if $B \in B(H)$ is such that $AB = BA$, then $\sqrt{A}B = B\sqrt{A}$.*

Remark. The proof in a finite dimensional space is easy. The proof to be given is longer, however, it bypasses the spectral theorem and it is valid for infinite dimensional spaces.

Proof.

(1) Observe first that since A is positive and $\|A\| \leq 1$, we have $0 \leq A \leq I$. Another equally important observation is that the sequence (B_n) is a "polynomial" of A. This implies that all of B_n are pairwise commuting.

Next, $B_0 = 0$ is evidently self-adjoint. So, assuming that B_n is self-adjoint (and recalling that A is self-adjoint), we can easily check that B_{n+1} too is self-adjoint. Therefore, all B_n are self-adjoint.

Now, we claim that $B_n \leq I$ for all n. This is obviously true for $n = 0$. Assume that $B_n \leq I$. Observing that $(I - B_n)^2 \geq 0$ (why?), we then have

$$I - B_{n+1} = I - B_n - \frac{1}{2}(A - B_n^2) = \frac{1}{2}(I - B_n)^2 + \frac{1}{2}(I - A) \geq 0.$$

To prove that (B_n) is increasing, observe first that $B_0 \leq \frac{1}{2}A = B_1$. Assuming that $B_n \geq B_{n-1}$, we may write

$$B_{n+1} - B_n = \frac{1}{2}[(I - B_{n-1}) + (I - B_n)](B_n - B_{n-1})$$

which, being a product of commuting positive operators, itself is positive.

Consequently, we have shown that

$$0 = B_0 \leq B_1 \leq \cdots \leq B_n \leq \cdots \leq I,$$

as needed.

(2) Since (B_n) is bounded monotone increasing, by Theorem **??** we know that (B_n) converges strongly to some self-adjoint $B \in B(H)$. Since each B_n is positive, we have

$$< Bx, x >= \lim_{n\to\infty} < B_n x, x >\geq 0$$

as strong convergence implies weak one. Thus, $B \geq 0$.

It remains to show that $B^2 = A$. Let $x \in H$. We have by hypothesis

$$B_{n+1}x = B_n x + \frac{1}{2}(Ax - B_n^2 x).$$

Passing to the strong limit and using $\|B_n^2 x - B^2 x\| \to 0$ (why?), we finally get $B^2 = A$, as required.

Finally, assume that a $C \in B(H)$ commutes with A, i.e. $AC = CA$. We must show that $BC = CB$. Since C commutes with A, we may easily show that C commutes with B_n too, that is, $CB_n x = B_n Cx$ (for all n and all x). On the one hand, we clearly see that $B_n Cx \to BCx$. On the other hand, invoking the (sequential) continuity of C, we have that $CB_nx \to CBx$. By uniqueness of the strong limit, we get

$$BCx = CBx,\ \forall x \in H,$$

as desired.

(3) If $A = 0$, then $B = 0$ will do. So if $A \neq 0$, considering $T = \frac{A}{\|A\|}$ gives $0 \leq T \leq 1$. Then, apply what we have already done above.

(4) *The proof of uniqueness here, although not being complicated, is not as direct as one is used to with other theorems.*

We have already shown that $B^2 = A$. Assume that there is another positive $C \in B(H)$ such that $C^2 = A$. We must show that $Bx = Cx$ for all $x \in H$. Observe first that A plainly commutes with C. By Question (2), C commutes with B as well, i.e. $BC = CB$. This tells us that

$$(B + C)(B - C) = B^2 - C^2 = A - A = 0.$$

So, if we let $x \in H$ and set $y = (B - C)x$, then

$$< By, y > + < Cy, y >=< (B+C)y, y >=< (B+C)(B-C)x, y >= 0.$$

Because both B and C are positive, we obtain (cf. Exercise **??**)

$$< By, y >=< Cy, y >= 0.$$

By (2) again, $B \geq 0$ has a square root which we denote by D, say. That is, $D^2 = B$. Therefore,

$$\|Dy\|^2 =< Dy, Dy >=< D^2y, y >=< By, y >= 0$$

and so $Dy = 0$. This implies that $By = D^2y = D(0) = 0$.

Using also a square root of C, we may similarly show that $Cy = 0$. Consequently,

$$\|Bx - Cx\|^2 =< (B - C)x, (B - C)x >=< (B - C)y, x >= 0.$$

Accordingly, $B = C$, i.e. we have proven that the positive A can *only have one* positive square root, marking the end of the proof.

□

Corollary 1.7. *Let A and B be two positive operators on a complex Hilbert space H. If A and B commute, then AB (and hence BA) is positive. Moreover,*

$$(AB)^{\frac{1}{2}} = A^{\frac{1}{2}}B^{\frac{1}{2}}.$$

Proof. Since A is positive, it admits a unique positive square root, which we denote by P (that is $P^2 = A$). Since B commutes with A, it commutes with P as well.

Let $x \in H$. We may write (remembering that positive operators are necessarily self-adjoint)

$$< ABx, x >=< P^2Bx, x >=< PBx, Px >=< BPx, Px >\geq 0$$

as B is positive. Therefore, $AB \geq 0$.

Since A and B are positive, both $A^{\frac{1}{2}}$ and $B^{\frac{1}{2}}$ exist and are well-defined. Since A and B also commute, AB is positive and it makes sense then to define $(AB)^{\frac{1}{2}}$. If we come to show that

$$(A^{\frac{1}{2}}B^{\frac{1}{2}})^2 = AB,$$

then by the uniqueness of the square root, the desired result follows.

Now since A and B commute, so do their square roots and we have

$$(A^{\frac{1}{2}}B^{\frac{1}{2}})^2 = A^{\frac{1}{2}}B^{\frac{1}{2}}A^{\frac{1}{2}}B^{\frac{1}{2}} = A^{\frac{1}{2}}A^{\frac{1}{2}}B^{\frac{1}{2}}B^{\frac{1}{2}} = AB.$$

The proof is complete. □

Remark. We give an example showing the importance of the commutativity of A and B for the result to hold. Let

$$A = \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix} \text{ and } B = \begin{pmatrix} 1 & 1 \\ 1 & 3 \end{pmatrix}.$$

Then both A and B are positive.

We may also check that

$$AB = \begin{pmatrix} 1 & 1 \\ 2 & 6 \end{pmatrix},$$

i.e. AB is not positive because it is not even self-adjoint and

$$AB = \begin{pmatrix} 1 & 1 \\ 2 & 6 \end{pmatrix} \neq \begin{pmatrix} 1 & 2 \\ 1 & 6 \end{pmatrix} = BA.$$

Proposition 1.8. *Let* $A, B \in B(H)$ *be such that* $0 \leq A \leq B$. *Then*

$$\sqrt{A} \leq \sqrt{B}.$$

A proof is based upon the following fairly standard result whose proof may be consulted in Theorem 3.1.69 in [2]:

Theorem 1.9. *Let* $A, B \in B(H)$. *Then*

$$\forall x \in H : \ \|Ax\| \leq \|Bx\| \Longleftrightarrow \exists K \in B(H) \text{ contraction } : A = KB.$$

Now, we prove Proposition 1.8.

Proof. Let $x \in H$. Since $0 \leq A \leq B$, we have for all $x \in H$

$$0 \leq < Ax, x > \leq < Bx, x > \Longleftrightarrow 0 \leq < \sqrt{A}x, \sqrt{A}x > \leq < \sqrt{B}x, \sqrt{B}x >$$

and so (for all x)

$$0 \leq \|\sqrt{A}x\|^2 \leq \|\sqrt{B}x\|^2.$$

So, by Theorem 1.9, we know that $\sqrt{A} = K\sqrt{B}$ for some contraction $K \in B(H)$. Since $\sqrt{A}$ is self-adjoint, it follows that $K\sqrt{B}$ too is self-adjoint, i.e. $K\sqrt{B} = \sqrt{B}K^*$. Since $\sqrt{B} \geq 0$, by Reid's inequality we obtain:

$$< \sqrt{A}x, x > = < \sqrt{B}K^* x, x > \leq < \sqrt{B}x, x >,$$

that is,

$$\sqrt{A} \leq \sqrt{B},$$

as required. □

2. Exercises

Exercise 1. *Find matrices without any square root.*

Solution. Let

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

Then A does not have any square root. To see this, assume that A has a square root, B say, which is a 2×2 matrix of the form

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

Then

$$B^2 = A \Longleftrightarrow \begin{pmatrix} a^2 + bc & ab + bd \\ ac + cd & bc + d^2 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix}$$

and hence

$$\begin{cases} a^2 + bc = 0, \\ ab + bd = 1, \\ ac + cd = 0, \\ bc + d^2 = 0. \end{cases}$$

The previous system has no solution (as the reader may easily check) meaning that A has no square root.

We give another example to use a different approach. Let

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

Then

$$A^2 = \begin{pmatrix} 0 & 0 & 1 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix} \text{ and } A^3 = \begin{pmatrix} 0 & 0 & 0 \\ 0 & 0 & 0 \\ 0 & 0 & 0 \end{pmatrix}.$$

Assume that A has a square root B, that is, $B^2 = A$. Hence $B^6 = A^3 = 0$, i.e. B is nilpotent. Since B is a 3×3 matrix, its index cannot exceed 3. Therefore, $B^3 = 0$, but this is just not consistent with $B^4 = A^2 \neq 0$. Thus A has no square root.

Exercise 2. *Find a square root of $A + I$ where*

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

Solution. Clearly, $A^3 = 0$. Inspired by the Taylor expansion series of $\sqrt{1+x}$, we conjecture that a square root of $A + I$ is

$$I + \frac{1}{2}A - \frac{1}{8}A^2 = \underbrace{\begin{pmatrix} 1 & \frac{1}{2} & \frac{3}{8} \\ 0 & 1 & \frac{1}{2} \\ 0 & 0 & 1 \end{pmatrix}}_{:=B}.$$

This is in effect the case as we can readily check that $B^2 = A + I$.

Remark. More generally and by the same token, we may give an nth root of $A + I$ ($n \geq 2$). Indeed, one (nth) root is given by

$$B = I + \frac{1}{n}A + \frac{\frac{1}{n}(\frac{1}{n} - 1)}{2}A^2 = \begin{pmatrix} 1 & \frac{1}{n} & \frac{n+1}{2n^2} \\ 0 & 1 & \frac{1}{n} \\ 0 & 0 & 1 \end{pmatrix},$$

that is, $B^n = A$ (which could be verified by a proof by induction).

Exercise 3. *Can you provide an operator having only one square root?*

Solution. This is impossible for a simple reason. If B is a *non-zero* square root of a given operator A, i.e. $B^2 = A$, then $-B$ too is another square root of A as

$$(-B)^2 = B^2 = A.$$

Remark. Therefore, the number of (non-zero) square roots is always even.

Exercise 4. *([3]) Let $T \in B(H)$ be such that $T^2 = 0$. Show that if* $\text{Re}\, T \geq 0$ *(or* $\text{Im} T \geq 0$*), then T is normal and so $T = 0$.*

Solution. Write $T = A+iB$ where $A, B \in B(H)$ are self-adjoint where $A = \operatorname{Re} T$ and $B = \operatorname{Im} T$. Then clearly

$$T^2 = A^2 - B^2 + i(AB + BA).$$

So, if $T^2 = 0$, then

$$A^2 - B^2 + i(AB + BA) = 0 \Longrightarrow \begin{cases} A^2 = B^2, \\ AB = -BA. \end{cases}$$

Hence, if $A \geq 0$ (a similar argument works when $B \geq 0$), then

$$AB = -BA \Longrightarrow A^2B = -ABA = BA^2 \Longrightarrow AB = BA$$

(by Theorem 1.6). Therefore, T is normal. Accordingly,

$$\|T\|^2 = \|T^2\| = 0 \Longrightarrow T = 0,$$

as suggested.

The next exercise provides a generalization as well as a different proof.

Exercise 5. *([1]) Let $T = A + iB$ be a finite square matrix and let $n \geq 2$. Show that if $T^n = 0$ and $A \geq 0$ (or $B \geq 0$), then $T = 0$.*

Solution. Let $\dim H < \infty$. The proof uses a trace argument. First, assume that $A \geq 0$. Clearly, the nilpotence of T does yield $\operatorname{tr} T = 0$. Hence

$$0 = \operatorname{tr}(A + iB) = \operatorname{tr} A + i \operatorname{tr} B.$$

Since A and B are self-adjoint, we know that $\operatorname{tr} A, \operatorname{tr} B \in \mathbb{R}$. By the above equation, this forces $\operatorname{tr} B = 0$ and $\operatorname{tr} A = 0$. The positiveness of A now intervenes to make $A = 0$. Therefore, $T = iB$ and so T is normal. Thus, and as alluded above,

$$0 = \|T^n\| = \|T\|^n,$$

thereby, $T = 0$.

In the event $B \geq 0$, reason as above to obtain $T = A$ and so $T = 0$, as wished.

3. More exercises

Exercise 6. *Show that an invertible matrix over $\mathbb{C}$ has always a square root. Is this result still valid over $\mathbb{R}$?*

Exercise 7. *Let $T \in B(H)$ be a normal operator. As is known, T could have infinitely many square roots.*

Show that it can occur that two (normal) square roots of T do not commute.

Exercise 8. *Give an operator $A \in B(H)$ having a square root but A does not have a cube root.*

Exercise 9. *Provide an operator $A \in B(H)$ without any square root but A has a cube root.*

References

[1] N. Frid, M. H. Mortad, When Nilpotence Implies Normality of Bounded Linear Operators, (submitted). arXiv:1901.09435.

[2] M. H. Mortad, *An Operator Theory Problem Book*, World Scientific Publishing Co., (2018). https://doi.org/10.1142/10884. ISBN: 978-981-3236-25-7 (hardcover).

[3] M. H. Mortad, On the Existence of Normal Square and Nth Roots of Operators, *The Journal of Analysis*, (to appear).