POWER OF A 3×3 MATRIX, SUBGROUPS AND TILING

Juri Kirillov
Clare Hall, Herschel Road, Cambridge, United Kingdom

Received: 9/5/21, Accepted: 3/9/22 , Published: 4/4/22

Abstract

We obtain a formula for the nth power of a 3×3 matrix A in terms of A and its eigenvalues. Then we present a construction of a subgroup of the general linear group over the ring of polynomials and we discuss its connection with congruence subgroups and boundary invariants for tiling.

1. A Formula for the Power of a 3×3 Matrix

In [5], Ken Williams proved a formula for the nth power of a 2×2 matrix A with eigenvalues α and β:

$$A^n = \begin{cases} \alpha^n \left(\dfrac{A - \beta I}{\alpha - \beta} \right) + \beta^n \left(\dfrac{A - \alpha I}{\beta - \alpha} \right), & \text{if } \alpha \neq \beta \\ \alpha^{n-1}(nA - (n-1)\alpha I), & \text{if } \alpha = \beta. \end{cases} \tag{1}$$

Here I is the identity matrix. A number of combinatorial identities can be obtained from this formula [2]. Following the same method as in [5], we get a formula for a 3×3 matrix.

Theorem 1. *Let A be a 3×3 matrix with eigenvalues α, β and γ. Then we have:*

$$A^n = \begin{cases} \alpha^n \left(\dfrac{(A - \beta I)(A - \gamma I)}{(\alpha - \beta)(\alpha - \gamma)} \right) + \beta^n \left(\dfrac{(A - \alpha I)(A - \gamma I)}{(\beta - \alpha)(\beta - \gamma)} \right) + \gamma^n \left(\dfrac{(A - \alpha I)(A - \beta I)}{(\gamma - \alpha)(\gamma - \beta)} \right), \\ \quad \text{if all eigenvalues are different;} \\ \alpha^{n-2} \left(\alpha^2 I + n\alpha(A - \alpha I) + \dfrac{n(n-1)}{2}(A - \alpha I)^2 \right), \\ \quad \text{if all eigenvalues are equal;} \\ \alpha^n \left(I - \left(\dfrac{A - \alpha I}{\alpha - \beta} \right)^2 \right) + n\alpha^{n-1} \dfrac{(A - \alpha I)(A - \beta I)}{\alpha - \beta} + \beta^n \left(\dfrac{A - \alpha I}{\alpha - \beta} \right)^2, \\ \quad \text{if } \alpha = \gamma,\ \alpha \neq \beta. \end{cases}$$

Proof. As we know, matrix A satisfies its characteristic equation

$$(A-\alpha I)(A-\beta I)(A-\gamma I)=0.$$

In the first case, when all eigenvalues are different, let us put

$$X=\frac{(A-\beta I)(A-\gamma I)}{(\alpha-\beta)(\alpha-\gamma)}$$

$$Y=\frac{(A-\alpha I)(A-\gamma I)}{(\beta-\alpha)(\beta-\gamma)}$$

$$Z=\frac{(A-\alpha I)(A-\beta I)}{(\gamma-\alpha)(\gamma-\beta)}.$$

We can check that $X^2=X,\ Y^2=Y,\ Z^2=Z,\ \ XY=XZ=YZ=0$ and $A=\alpha X+\beta Y+\gamma Z$. It means that

$$A^n=\alpha^n X+\beta^n Y+\gamma^n Z.$$

In the second case, when all eigenvalues are equal ($\alpha=\beta=\gamma$), let us put

$$X=A-\alpha I.$$

Then $X^3=0$ and we get the following formula for matrix A^n:

$$A^n=(\alpha I+X)^n=\alpha^n I+n\alpha^{n-1}X+\alpha^{n-2}\frac{n(n-1)}{2}X^2.$$

In the third case, when two eigenvalues are equal but different from the third one ($\alpha=\gamma,\ \alpha\neq\beta$), let us put

$$X=\frac{A-\alpha I}{\alpha-\beta}.$$

Then $X^3=-X^2$ and it gives us a formula for A^n:

$$A^n=((\alpha-\beta)X+\alpha I)^n=$$

$$=X^2((\beta-\alpha)+\alpha)^n-X^2(\alpha^n+n\alpha^{n-1}(\beta-\alpha))+\alpha^n I+n\alpha^{n-1}(\alpha-\beta)X=$$

$$=\alpha^n(I-X^2)+n\alpha^{n-1}(\alpha-\beta)(X+X^2)+X^2\beta^n.$$

Also notice that

$$(\alpha-\beta)(X+X^2)=\frac{(A-\alpha I)(A-\beta I)}{\alpha-\beta}.$$

□

A different formula for a 3×3 matrix is given in [3], where the power of matrix is expressed in terms of its entries.

2. A Subgroup of Matrices over Polynomials

Theorem 2. *The following set of matrices is a group over the ring of polynomials $F[a]$, where F is a field:*

$$G = \left\{ \begin{pmatrix} x_1a + x_2 & x_1 \\ -x_1a^2 + x_3a + x_4 & -x_1a + x_2 + x_3 \end{pmatrix} \Big| -x_1x_4 + x_2^2 + x_2x_3 \neq 0,\ x_j \in F \right\}.$$

Proof. Let us put

$$q_1 = \begin{pmatrix} x_1a + x_2 & x_1 \\ -x_1a^2 + x_3a + x_4 & -x_1a + x_2 + x_3 \end{pmatrix}$$

$$q_2 = \begin{pmatrix} y_1a + y_2 & y_1 \\ -y_1a^2 + y_3a + y_4 & -y_1a + y_2 + y_3 \end{pmatrix}.$$

Then

$$q_1q_2 = \begin{pmatrix} z_1a + z_2 & z_1 \\ -z_1a^2 + z_3a + z_4 & -z_1a + z_2 + z_3 \end{pmatrix}$$

where

$$\begin{aligned} z_1 &= x_1y_2 + x_1y_3 + x_2y_1 \\ z_2 &= x_1y_4 + x_2y_2 \\ z_3 &= -x_1y_4 + x_2y_3 + x_3y_2 + x_3y_3 + x_4y_1 \\ z_4 &= x_2y_4 + x_3y_4 + x_4y_2. \end{aligned} \tag{2}$$

This means that the set of matrices of type

$$M = \begin{pmatrix} x_1a + x_2 & x_1 \\ -x_1a^2 + x_3a + x_4 & -x_1a + x_2 + x_3 \end{pmatrix}$$

is closed under multiplication. The identity matrix is also present in this set. We can put

$$\begin{aligned} x_1 = x_3 = x_4 &= 0 \\ x_2 &= 1, \end{aligned}$$

and then M is the identity matrix. In this way we obtain a semigroup. Let us compute the inverse of matrix M:

$$(-x_1x_4 + x_2^2 + x_2x_3)M^{-1} = \begin{pmatrix} -x_1a + x_2 + x_3 & -x_1 \\ x_1a^2 - x_3a - x_4 & x_1a + x_2 \end{pmatrix}.$$

We can notice that this matrix has the same form, so it belongs to the set G. If

$$-x_1x_4 + x_2^2 + x_2x_3 \neq 0,$$

then the determinant is non-zero, and this set is a group. □

In this way we obtain that G is a subgroup of $GL_2(F[a])$. Here is another proof based on a more general construction.

Lemma 3. *Let $F[a]$ be the ring of polynomials over the field F. Then the following set of matrices is an F-subalgebra of $M_2(F[a])$:*

$$\{x_1u + x_2v + x_3uv + x_4vu \mid u^2 = 0, v^2 = 0, uv + vu = I, u, v \in M_2(F[a]), x_i \in F\}$$

where I is the identity matrix.

The proof is easy and is left to the reader. This F-algebra is isomorphic to the matrix algebra $A = M_2(F)$. It can be seen from the Peirce decomposition

$$A = eAe + eA(1-e) + (1-e)Ae + (1-e)A(1-e)$$

by taking e any idempotent of A, for example

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

Then we obtain

$$M_2(F) = \{x_1u_1 + x_2u_2 + x_3u_3 + x_4u_4 \mid x_i \in F\}$$

where

$$u_1 = \begin{pmatrix} 1 & 0 \\ 1 & 0 \end{pmatrix} \quad u_3 = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}$$
$$u_2 = \begin{pmatrix} -1 & 1 \\ -1 & 1 \end{pmatrix} \quad u_4 = \begin{pmatrix} 0 & 0 \\ -1 & 1 \end{pmatrix}.$$

We can see that $u_2^2 = u_3^2 = 0$ and $u_2u_3 + u_3u_2 = I$. Now if we put

$$u = \begin{pmatrix} a & 1 \\ -a^2 & -a \end{pmatrix} \quad v = \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix},$$

then the group of invertible elements in the F-algebra in Lemma 3 is the group we constructed in Theorem 2. So it is isomorphic to $GL_2(F)$. Let us give another proof of this result.

Theorem 4. *Let F be a field. The group*

$$G = \left\{ \begin{pmatrix} x_1a + x_2 & x_1 \\ -x_1a^2 + x_3a + x_4 & -x_1a + x_2 + x_3 \end{pmatrix} \Big| -x_1x_4 + x_2^2 + x_2x_3 \neq 0, \quad x_j \in F \right\}$$

is isomorphic to $GL_2(F)$. This isomorphism can be obtained by the map $a \to a_0 \in F$.

Proof. From the previous theorem we know that this map is a homomorphism, so we only need to show that it is a bijection. Every matrix can be uniquely represented in this form:

$$\begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix} = \begin{pmatrix} x_1a_0 + x_2 & x_1 \\ -x_1a_0^2 + x_3a_0 + x_4 & -x_1a_0 + x_2 + x_3 \end{pmatrix}$$

where

$$\begin{aligned} x_1 &= b_1 \\ x_2 &= a_1 - b_1a_0 \\ x_3 &= d_1 - a_1 + 2b_1a_0 \\ x_4 &= c_1 - b_1a_0^2 - (d_1 - a_1)a_0, \end{aligned}$$

so the map $a \to a_0$ is a bijection. □

From relations (2) we obtain that if $x_4 = y_4 = 0$, then $z_4 = 0$, so the matrices with $x_4 = 0$ form a subgroup G_1 of group G.

$$G_1 = \left\{ \begin{pmatrix} x_1a + x_2 & x_1 \\ -x_1a^2 + x_3a & -x_1a + x_2 + x_3 \end{pmatrix} \mid x_2(x_2 + x_3) \neq 0, \quad x_j \in F \right\}$$

If we put $x_3 = 0$, then the set of matrices obtained this way from the above construction is a subgroup of G_1. Let us denote it by G_2.

$$G_2 = \left\{ \begin{pmatrix} x_1a + x_2 & x_1 \\ -x_1a^2 & -x_1a + x_2 \end{pmatrix} \mid x_2 \neq 0, \ x_1, x_2 \in F \right\}$$

Therefore we obtain that $G_2 \subset G_1 \subset G$. Notice that G_2 is an abelian subgroup of $GL_2(F[a])$ and for any $a \in F$ it is an abelian subgroup of $GL_2(F)$.

Another subgroup of $GL_2(F[a])$ can be constructed as upper-triangular matrices where one element is a polynomial of degree less or equal to n:

$$G_3(n) = \left\{ \begin{pmatrix} b & f(a) \\ 0 & c \end{pmatrix} \Big| \, b, c \in F, \ bc \neq 0, f(a) \in F[a], \ deg(f(a)) \leqslant n \right\}.$$

3. Connection with Congruence Subgroups

The congruence subgroups of $\mathrm{SL}_2(\mathbb{Z})$ are defined in the following way (N is a positive integer). The principal congruence subgroup

$$\Gamma(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \ : \ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}$$

and congruence subgroups

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \ : \ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} * & * \\ 0 & * \end{pmatrix} \pmod{N} \right\}$$

$$\Gamma_1(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}) \ : \ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \equiv \begin{pmatrix} 1 & * \\ 0 & 1 \end{pmatrix} \pmod{N} \right\}.$$

A congruence subgroup of level N is a subgroup of $\mathrm{SL}_2(\mathbb{Z})$ that contains $\Gamma(N)$ for some integer N. As we know, $\Gamma(N)$ and $\Gamma_1(N)$ are normal subgroups, i.e.,

$$\Gamma(N) \triangleleft \Gamma_1(N) \triangleleft \Gamma_0(N) \subset \mathrm{SL}_2(\mathbb{Z}).$$

Let us consider groups $G_1(N)$ and $G_2(N)$ as subgroups of $\mathrm{SL}_2(\mathbb{Z})$:

$$G_1 = \left\{ \begin{pmatrix} xN+k & x \\ -xN^2 & -xN+k \end{pmatrix} \Big| \, x \in \mathbb{Z}, k = \pm 1 \right\} \subset \Gamma_0(N)$$

$$G_2 = \left\{ \begin{pmatrix} xN+1 & x \\ -xN^2 & -xN+1 \end{pmatrix} \Big| \, x \in \mathbb{Z} \right\} \subset \Gamma_1(N).$$

As we can see, G_1 and G_2 are not congruence subgroups because they do not contain $\Gamma(N)$. They are abelian groups, in particular:

$$G_1 \cong \mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$$

$$G_2 \cong \mathbb{Z}$$

where the generator of the free part is the matrix

$$\begin{pmatrix} N+1 & 1 \\ -N^2 & -N+1 \end{pmatrix}$$

and the torsion part is $-I$ (the identity matrix with minus sign). The group $\mathrm{SL}_2(\mathbb{Z})$ does not have abelian subgroups of finite index, and therefore G_1 and G_2 are not subgroups of finite index in $\mathrm{SL}_2(\mathbb{Z})$.

4. A Connection with Boundary Invariants for Tiling

Let $A = \langle x, y \rangle$ be the free group generated by two elements x, y. Given the tile τ in the square lattice, we can assign to it a word $\partial\tau \in A$ obtained by traversing the boundary of τ in the counterclockwise direction, where a step in the horizontal direction from left to right adds x and a step in the upward direction adds y. In the opposite directions x^{-1} and y^{-1} are added, respectively. For example, the boundary of pentomino Z is $x^2y^2xyx^{-2}y^{-2}x^{-1}y^{-1}$.

An introduction to boundary invariants can be found in [4] and [1]. It is often useful to find a map (a homomorphism) $A \to G$ to a particular group G, so that the

boundary of each tile in the given set would be trivial. Examples of this method are given in [4], where G is the symmetric group S_n.

However, the group G can also be a matrix group. Let us put

$$\begin{aligned} x &= \begin{pmatrix} s & s(p-s)-1 \\ 1 & p-s \end{pmatrix} \\ y &= \begin{pmatrix} 0 & -1 \\ 1 & q \end{pmatrix}, \end{aligned} \tag{3}$$

where

$$\begin{aligned} s &= -\sqrt{\frac{i-3}{2}} \\ p &= q = \sqrt{1+i} \\ i &= \sqrt{-1}. \end{aligned}$$

Then the boundary of pentomino Z is equal to the identity matrix for all orientations (translation, rotation and reflection).

Here is another invariant for pentomino Z based on the following group. Let

$$G = \langle m_z \mid z \in \mathbb{Z}[i] \rangle,$$

where

$$m_z = \begin{pmatrix} kz & 1 \\ 1-(kz)^2 & -kz \end{pmatrix}, \quad \text{if } z \in 2\mathbb{Z}[i] = \{2x+2yi \mid x, y \in \mathbb{Z}\},$$

$$m_z = \begin{pmatrix} kz & 1 \\ -1-(kz)^2 & -kz \end{pmatrix}, \quad \text{if } z \in (2\mathbb{Z}+1)[i] = \{2x+1+(2y+1)i \mid x, y \in \mathbb{Z}\}$$

and $k \in \mathbb{C}$. One can think of these matrices as being placed on the edges of the square lattice, and that z is equal to the corresponding complex number located at the midpoint of the edge. We can assume that the side of the square is 2 in its length, and 0 is located on the horizontal edge. Then horizontal edges have even coordinates and vertical edges have coordinates in the set $\{2x+1+(2y+1)i \mid x, y \in \mathbb{Z}\}$.

Example: the set of points along the boundary for pentomino Z is

$$\{0, 2, 3+i, 3+3i, 4+4i, 5+5i, 4+6i, 2+6i, 1+5i, 1+3i, 2i, -1+i\}.$$

Let τ be a polyomino placed in that lattice. Suppose that complex numbers on the boundary of τ form the set $A = \{z_1, z_2, ..., z_n\}$. Then the boundary of τ is

$$\partial\tau = \prod_{z \in A} m_z.$$

After a move by a (translation by $a \in \mathbb{Z}[i]$), the boundary of τ becomes

$$\prod_{z \in A} m_{z+a} = \prod_{j=1}^{n} \begin{pmatrix} k(z_j+a) & 1 \\ 1-(k(z_j+a))^2 & -k(z_j+a) \end{pmatrix}.$$

When squared, matrices m_z become scalar:

$$m_z^2 = \pm I.$$

Therefore, to obtain an invariant for polyomino τ we need to ensure that its boundary does not depend on a and it is equal to a scalar matrix, i.e., for any a we have

$$\prod_{z \in A} m_{z+a} = \pm I.$$

How can we find the value of k, so that the boundary is invariant under translation? Notice that matrix

$$\begin{pmatrix} z+a & 1 \\ c-(z+a)^2 & -(z+a) \end{pmatrix}$$

belongs to group G from Section 2 (we can put $x_1 = 1, x_2 = z, x_3 = -2z, x_4 = c - z^2$) and m_z is obtained by the substitution $a \to ka, z \to kz$. In this way, matrices m_z belong to the group isomorphic to G.

So after a move by a, the boundary depends on a only as a quadratic polynomial. We can equate the matrix ∂Z to a scalar matrix and solve the corresponding system of equations in k.

Let us put

$$k = \frac{1}{2}\sqrt{i-1}.$$

Then the boundary of pentomino Z is equal to the identity matrix with minus sign for all orientations, i.e.,

$$\partial Z = -I.$$

5. Commutator of Matrix Powers

Theorem 5. *Suppose that x and y are 2×2 matrices over the field F and their powers commute: $x^w y^z = y^z x^w$. Then one of these powers is a scalar matrix or x and y commute.*

Proof. We have to consider 3 cases:

1. Matrices x and y have different eigenvalues, α, β with $\alpha \neq \beta$ and α_1, β_1 with $\alpha_1 \neq \beta_1$.

2. One of the matrices has different eigenvalues but the other one has an eigenvalue with multiplicity two.

3. Both matrices have eigenvalues with multiplicity two.

Let us consider the first case as the other two are proved in a similar way. Suppose that x and y are given as follows:

$$x = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad y = \begin{pmatrix} a_1 & b_1 \\ c_1 & d_1 \end{pmatrix}.$$

Using the formula (1), we obtain

$$xy - yx = \begin{pmatrix} bc_1 - b_1c & ab_1 - a_1b + bd_1 - b_1d \\ -ac_1 + a_1c - cd_1 + c_1d & -bc_1 + b_1c \end{pmatrix}$$

$$\begin{aligned}(\alpha - \beta)(\alpha_1 - \beta_1)(x^w y^z - y^z x^w) \\ = -(\alpha^w - \beta^w)(\beta_1^z - \alpha_1^z) \begin{pmatrix} bc_1 - b_1c & ab_1 - a_1b + bd_1 - b_1d \\ -ac_1 + a_1c - cd_1 + c_1d & -bc_1 + b_1c \end{pmatrix}.\end{aligned}$$

It follows that

$$x^w y^z - y^z x^w = \frac{(\alpha^w - \beta^w)(\alpha_1^z - \beta_1^z)}{(\alpha - \beta)(\alpha_1 - \beta_1)}(xy - yx).$$

When matrix x has different eigenvalues (α and β) and y has eigenvalue α_1 with multiplicity two, we have:

$$x^w y^z - y^z x^w = \frac{z(\alpha^w - \beta^w)\alpha_1^{z-1}}{\alpha - \beta}(xy - yx).$$

And in case x has eigenvalue α with multiplicity two and y has eigenvalue β with multiplicity two, we have:

$$x^w y^z - y^z x^w = (\alpha^{w-1}\beta^{z-1}wz)(xy - yx).$$

□

Recall that the commutator of two matrices A and B is denoted by $[A, B] = AB - BA$. Then we see that for 2×2 matrices the commutator of their powers $[x^w, y^z]$ differs from the commutator $[x, y]$ only by a scalar multiple.

Acknowledgement. I would like to thank Uzi Vishne for his useful comments.

References

[1] J. H. Conway, J. C. Lagarias, Tilings with polyominoes and combinatorial group theory, *J. Combin. Theory Ser. A* **53** (1990), 183–208.

[2] J. Mc Laughlin, Combinatorial identities deriving from the nth power of a 2×2 matrix, *Integers* **4** (2004), A19.

[3] N. Na Chanta, P. Rochanakul, A combinatorial formula for powers of 3×3 matrices and some combinatorial identities, *Thai J. Math.* **18** (2020), no. 1, 372–383.

[4] M. Reid, Tile homotopy groups, *Enseign. Math.* (2) **49** (2003), no. 1-2, 123–155.

[5] K. S. Williams, The nth power of a 2×2 matrix (in Notes), *Math. Magazine* Vol.**65**, No.5 (1992), p. 336.