Similar matrices and equivalent polynomial matrices

Darij Grinberg

August 25, 2022

***

The purpose of this note is to prove a classical result in linear algebra: that two $m \times m$-matrices a and b over a commutative ring K are similar if and only if the polynomial matrices $tI_m - a$ and $tI_m - b$ (where I_m is the identity matrix, and t is a polynomial indeterminate) are equivalent (i.e., satisfy $(tI_m - a)\,p = q\,(tI_m - b)$ for two invertible polynomial matrices p and q).

Even better, we shall prove a generalization of this result, replacing the matrices a and b by two elements a and b of a (not necessarily commutative) ring R, and replacing the polynomial matrices $tI_m - a$ and $tI_m - b$ by the polynomials $t - a$ and $t - b$ in $R[t]$. Here, $R[t]$ denotes the polynomial ring over R in a single indeterminate t; we will define this object precisely in Definition 1.2.

Neither this generalization nor our proof is really new. The generalization was observed by @user20948 in a comment at MathOverflow (`https://mathoverflow.net/questions/66269/#comment866429_96046`), who proved it tersely but nicely using a commutative diagram of $R[t]$-modules and their quotients. The proof I give below is merely an elementary rewording of @user20948's proof – much less slick, but fully elementary and self-contained. A similar proof appears in [Gantma77, Chapter VI, §4–§5].

1. Notations and definitions regarding polynomials

Convention 1.1. In the following, rings are always understood to be associative and with unity, but not necessarily commutative.

We will use the concept of a polynomial ring $R[t]$ over a ring R that is not necessarily commutative. This notion is widely known in the case when R is commutative. The definition in the general case is more or less the same, except that certain shortcuts requiring are not available (e.g., the polynomial ring $R[t]$ is not an R-algebra in general, and we have to distinguish between left and right multiplication). Here is the general definition:

Definition 1.2. Let R be a ring. Then, $R[t]$ shall denote the ring of polynomials in a single indeterminate t over R. The definition of this ring is well-known when R is commutative; we use the same definition in the general case: A polynomial $p \in R[t]$ means an infinite sequence $(p_0, p_1, p_2, \ldots)$ of elements of R such that all but finitely many $n \geqslant 0$ satisfy $p_n = 0$. We define sums and products of such polynomials by the usual formulas:

$$(p_0, p_1, p_2, \ldots) + (q_0, q_1, q_2, \ldots) := (p_0 + q_0,\ p_1 + q_1,\ p_2 + q_2,\ \ldots);$$
$$(p_0, p_1, p_2, \ldots) \cdot (q_0, q_1, q_2, \ldots) := (r_0, r_1, r_2, \ldots),$$

where $r_n := \sum_{i=0}^{n} p_i q_{n-i}$ for each $n \geqslant 0$.

We identify each $a \in R$ with the polynomial $(a, 0, 0, 0, \ldots) \in R[t]$. This makes R into a subring of $R[t]$. Hence, a polynomial

$$p = (p_0, p_1, p_2, \ldots) \in R[t]$$

can be multiplied by an element $a \in R$ both from the left and from the right: namely,

$$\begin{aligned} ap &= (ap_0, ap_1, ap_2, \ldots) \qquad \text{and} \\ pa &= (p_0 a, p_1 a, p_2 a, \ldots). \end{aligned} \tag{1}$$

Now, define the indeterminate t as the sequence $(0, 1, 0, 0, 0, \ldots) \in R[t]$ (only the second entry is 1). Then, each polynomial $p = (p_0, p_1, p_2, \ldots) \in R[t]$ satisfies

$$p = \sum_{n \geqslant 0} p_n t^n = \sum_{n \geqslant 0} t^n p_n.$$

This is, of course, the standard way of writing polynomials.

Note that the indeterminate t commutes with every polynomial $p \in R[t]$, since multiplying p by t (in either order) is tantamount to shifting all coefficients of p by one position to the right: If $p = (p_0, p_1, p_2, \ldots) \in R[t]$, then

$$pt = tp = (0, p_0, p_1, p_2, \ldots). \tag{2}$$

Remark 1.3. The main difference between the general case (i.e., the case when R is arbitrary ring) and the classical commutative case (i.e., the case when R is a commutative ring) is that in the general case, it is not clear how to evaluate a polynomial $p = (p_0, p_1, p_2, \ldots) \in R[t]$ at a given element $a \in R$. Indeed, we can define the "left evaluation" $\sum_{n \geqslant 0} p_n a^n$ and the "right evaluation" $\sum_{n \geqslant 0} a^n p_n$, but these are in general not the same (unless a belongs to the center of R), and neither of them is as well-behaved as in the commutative case. (More on that below.)

Another difference is that, as mentioned above, $R[t]$ is not an R-algebra if R is not commutative (since the notion of an R-algebra does not exist in this case).

2. The claim

Recall that an element p of a ring R is called *invertible* if and only if it has an inverse (i.e., if there is an element $q \in R$ such that $pq = qp = 1$).

We need one more definition before we can state the main result:

Definition 2.1. Let R be a ring. Let a and b be two elements of R.

(a) We say that a and b are *conjugate* in R if there exists an invertible element $p \in R$ such that $ap = pb$.

(b) We say that a and b are *equivalent* in R if there exist invertible elements $p, q \in R$ such that $ap = qb$.

I'm not sure how standard the word "equivalent" is; I think other authors use "unit-equivalent" or "associate" for the same notion.

Our goal is to prove the following:

Theorem 2.2. Let R be a ring. Let $a, b \in R$ be two elements. Then, a and b are conjugate in R if and only if the polynomials $t - a$ and $t - b$ are equivalent in $R[t]$.

Before we prove this theorem, let us see how it can be used to prove the result promised at the beginning of this note:

Corollary 2.3. Let K be a ring. Let $a, b \in K^{m\times m}$ be two $m \times m$-matrices over K. Then, the matrices a and b are similar if and only if the matrices $tI_m - a$ and $tI_m - b$ in $(K[t])^{m\times m}$ are equivalent in $(K[t])^{m\times m}$. (Here, I_m denotes the $m \times m$-identity matrix.)

Proof of Corollary 2.3. The polynomial ring $K^{m\times m}[t]$ is known to be isomorphic to the matrix ring $(K[t])^{m\times m}$. Indeed, there is a ring isomorphism

$$\rho : K^{m\times m}[t] \to (K[t])^{m\times m}$$

that sends each polynomial $\sum\limits_{n\geqslant 0} A_n t^n \in K^{m\times m}[t]$ (with $A_n \in K^{m\times m}$ for all $n \geqslant 0$) to the matrix $\sum\limits_{n\geqslant 0} t^n A_n \in (K[t])^{m\times m}$ (where each A_n is now regarded as a matrix over $K[t]$). This isomorphism ρ sends the polynomial $t - a \in K^{m\times m}[t]$ to the matrix $tI_m - a \in (K[t])^{m\times m}$; that is, we have $\rho(t-a) = tI_m - a$. Similarly, $\rho(t-b) = tI_m - b$.

Conjugate elements of $K^{m\times m}$ are better known as similar matrices. Thus, we have the following chain of logical equivalences:

$$\begin{aligned}
&(\text{the matrices } a \text{ and } b \text{ are similar}) \\
&\iff \left(\text{the matrices } a \text{ and } b \text{ are conjugate in } K^{m\times m}\right) \\
&\iff \left(\text{the polynomials } t-a \text{ and } t-b \text{ are equivalent in } K^{m\times m}[t]\right) \\
&\qquad\qquad \left(\text{by Theorem 2.2, applied to } R = K^{m\times m}\right) \\
&\iff \left(\text{the matrices } \rho(t-a) \text{ and } \rho(t-b) \text{ are equivalent in } (K[t])^{m\times m}\right) \\
&\qquad\qquad \left(\begin{array}{c} \text{since } \rho \text{ is a ring isomorphism, and thus} \\ \text{two elements } c \text{ and } d \text{ of } K^{m\times m}[t] \\ \text{are equivalent in } K^{m\times m}[t] \text{ if and only if} \\ \text{their images } \rho(c) \text{ and } \rho(d) \text{ are equivalent in } (K[t])^{m\times m} \end{array}\right) \\
&\iff \left(\text{the matrices } tI_m - a \text{ and } tI_m - b \text{ are equivalent in } (K[t])^{m\times m}\right)
\end{aligned}$$

(since $\rho(t-a) = tI_m - a$ and $\rho(t-b) = tI_m - b$). This proves Corollary 2.3. □

3. Right evaluations

The trick to the proof of Theorem 2.2 is the following definition:

Definition 3.1. Let R be a ring, and let $a \in R$ be arbitrary. Then, we let $r_a : R[t] \to R$ be the map that sends each polynomial $(p_0, p_1, p_2, \ldots) \in R[t]$ (with $p_0, p_1, p_2, \ldots \in R$) to $\sum\limits_{n\geqslant 0} a^n p_n$.

This map r_a can be called the *right evaluation map at a*, since it "evaluates" polynomials at $t = a$. But this shouldn't be taken too literally; in particular, it is not always true that any two polynomials $p, q \in R[t]$ satisfy $r_a(pq) = r_a(p) \cdot r_a(q)$. (However, this equality still holds if a lies in the center of R.)

The following property of r_a is straightforward:

Proposition 3.2. Let R be a ring, and let $a \in R$ be arbitrary. Then, the map $r_a : R[t] \to R$ is a right R-linear map, i.e., a homomorphism of right R-modules.

Proof of Proposition 3.2. If $p = (p_0, p_1, p_2, \ldots)$ and $q = (q_0, q_1, q_2, \ldots)$ are two polynomials in $R[t]$ (with $p_0, p_1, p_2, \ldots \in R$ and $q_0, q_1, q_2, \ldots \in R$), then their sum is $p+q = (p_0+q_0,\ p_1+q_1,\ p_2+q_2,\ \ldots)$, and thus the definition of r_a yields

$$\begin{aligned} r_a(p+q) &= \sum_{n\geqslant 0} \underbrace{a^n(p_n+q_n)}_{=a^n p_n + a^n q_n} = \sum_{n\geqslant 0}(a^n p_n + a^n q_n) \\ &= \underbrace{\sum_{n\geqslant 0} a^n p_n}_{\substack{=r_a(p) \\ \text{(by the definition of } r_a)}} + \underbrace{\sum_{n\geqslant 0} a^n q_n}_{\substack{=r_a(q) \\ \text{(by the definition of } r_a)}} \\ &= r_a(p) + r_a(q). \end{aligned}$$

Thus, the map r_a respects addition.

If $p = (p_0, p_1, p_2, \ldots)$ is a polynomial in $R[t]$ (with $p_0, p_1, p_2, \ldots \in R$), and if $c \in R$, then

$$\begin{aligned} pc &= (p_0, p_1, p_2, \ldots)\, c && (\text{since } p = (p_0, p_1, p_2, \ldots)) \\ &= (p_0 c, p_1 c, p_2 c, \ldots) && (\text{by (1), applied to } c \text{ instead of } a), \end{aligned}$$

and thus the definition of r_a yields

$$r_a(pc) = \sum_{n\geqslant 0} a^n p_n c = \underbrace{\sum_{n\geqslant 0} a^n p_n}_{\substack{=r_a(p) \\ \text{(by the definition of } r_a)}} \cdot c = r_a(p)\cdot c.$$

Thus, the map r_a is right R-linear (since we already know that r_a respects addition). This proves Proposition 3.2. □

We will also need the following properties of r_a:

Proposition 3.3. Let R be a ring, and let $a \in R$ be arbitrary. Let $s \in R[t]$. Then:

(a) We have $r_a(sc) = r_a(s)\,c$ for any $c \in R$.

(b) We have $r_a(st) = a r_a(s)$.

(c) We have $r_a((t-a)\,s) = 0$.

(d) There exists a polynomial $\overline{s} \in R[t]$ such that $s = r_a(s) + (t-a)\,\overline{s}$.

Proof of Proposition 3.3. Write the polynomial $s \in R[t]$ in the form $s = (s_0, s_1, s_2, \ldots)$. Thus, the definition of r_a yields $r_a(s) = \sum_{n\geqslant 0} a^n s_n$.

(a) This follows immediately from Proposition 3.2.

(b) From $s = (s_0, s_1, s_2, \ldots)$, we obtain $st = (0, s_0, s_1, s_2, \ldots)$ (by (2), applied to $p = s$). Setting $s_{-1} := 0$, we can rewrite this as

$$st = (s_{-1}, s_0, s_1, s_2, \ldots).$$

Hence, the definition of r_a yields

$$\begin{aligned} r_a(st) &= \sum_{n \geqslant 0} a^n s_{n-1} = a^0 \underbrace{s_{0-1}}_{=s_{-1}=0} + \sum_{n \geqslant 1} \underbrace{a^n}_{=aa^{n-1}} s_{n-1} \\ &= \underbrace{a^0 0}_{=0} + \sum_{n \geqslant 1} aa^{n-1} s_{n-1} = \sum_{n \geqslant 1} aa^{n-1} s_{n-1} \\ &= \sum_{n \geqslant 0} aa^n s_n \qquad \left(\begin{array}{c} \text{here, we have substituted } n \\ \text{for } n-1 \text{ in the sum} \end{array} \right) \\ &= a \underbrace{\sum_{n \geqslant 0} a^n s_n}_{\substack{=r_a(s) \\ \text{(by the definition of } r_a)}} = ar_a(s). \end{aligned}$$

This proves Proposition 3.3 **(b)**.

(c) From $s = (s_0, s_1, s_2, \ldots)$, we obtain $as = (as_0, as_1, as_2, \ldots)$. Thus, the definition of r_a yields

$$r_a(as) = \sum_{n \geqslant 0} \underbrace{a^n a}_{\substack{=a^{n+1} \\ =aa^n}} s_n = \sum_{n \geqslant 0} aa^n s_n = a \underbrace{\sum_{n \geqslant 0} a^n s_n}_{\substack{=r_a(s) \\ \text{(by the definition of } r_a)}} = ar_a(s).$$

Now, (2) (applied to $p = s$) yields $st = ts$. Hence, $(t-a)s = \underbrace{ts}_{=st} - as = st - as$. Therefore,

$$\begin{aligned} r_a((t-a)s) &= r_a(st - as) \\ &= \underbrace{r_a(st)}_{\substack{=ar_a(s) \\ \text{(by Proposition 3.3 (b))}}} - \underbrace{r_a(as)}_{=ar_a(s)} \qquad \text{(by Proposition 3.2)} \\ &= ar_a(s) - ar_a(s) = 0. \end{aligned}$$

This proves Proposition 3.3 **(c)**.

(d) The element t of $R[t]$ commutes with a (since $ta = (0, a, 0, 0, 0, \ldots) = at$). Hence, the equality

$$x^n - y^n = (x-y) \sum_{k=0}^{n-1} x^k y^{n-1-k}$$

(which holds for any two commuting elements x and y and any $n \geqslant 0$) can be applied to $x = t$ and $y = a$. Thus, for any $n \geqslant 0$, we have

$$t^n - a^n = (t - a) \sum_{k=0}^{n-1} t^k a^{n-1-k}. \tag{3}$$

Subtracting the equality $r_a(s) = \sum_{n \geqslant 0} a^n s_n$ from the equality $s = (s_0, s_1, s_2, \ldots) = \sum_{n \geqslant 0} t^n s_n$, we obtain

$$\begin{aligned} s - r_a(s) &= \sum_{n \geqslant 0} t^n s_n - \sum_{n \geqslant 0} a^n s_n = \sum_{n \geqslant 0} \underbrace{(t^n s_n - a^n s_n)}_{=(t^n - a^n) s_n} \\ &= \sum_{n \geqslant 0} \underbrace{(t^n - a^n)}_{\substack{= (t-a) \sum_{k=0}^{n-1} t^k a^{n-1-k} \\ \text{(by (3))}}} s_n = \sum_{n \geqslant 0} (t - a) \left(\sum_{k=0}^{n-1} t^k a^{n-1-k} \right) s_n \\ &= (t - a) \underbrace{\sum_{n \geqslant 0} \left(\sum_{k=0}^{n-1} t^k a^{n-1-k} \right) s_n}_{\substack{\text{This sum is well-defined,} \\ \text{since all but finitely many} \\ \text{of its addends are 0 (because} \\ \text{all but finitely many } n \text{ satisfy } s_n = 0)}} . \end{aligned}$$

Thus, there exists a polynomial $\overline{s} \in R[t]$ such that $s - r_a(s) = (t - a)\overline{s}$ (namely, $\overline{s} = \sum_{n \geqslant 0} \left(\sum_{k=0}^{n-1} t^k a^{n-1-k} \right) s_n$). In other words, there exists a polynomial $\overline{s} \in R[t]$ such that $s = r_a(s) + (t - a)\overline{s}$. This proves Proposition 3.3 **(d)**. □

4. Proof of Theorem 2.2

We are now ready to prove Theorem 2.2:

Proof of Theorem 2.2. $\Longrightarrow$: Assume that a and b are conjugate in R. We must show that the polynomials $t - a$ and $t - b$ are equivalent in $R[t]$.

Since a and b are conjugate in R, there exists an invertible element $r \in R$ such that $ar = rb$ (by the definition of "conjugate"). Consider this r. Then, $r \in R \subseteq R[t]$, and furthermore the element r is invertible in $R[t]$ (since r is invertible in R). In the ring $R[t]$, we have

$$(t - a) r = \underbrace{tr}_{\substack{= rt \\ \text{(by (2), applied} \\ \text{to } p = r)}} - \underbrace{ar}_{= rb} = rt - rb = r(t - b).$$

Thus, there exist invertible elements $p, q \in R[t]$ such that $(t-a)p = q(t-b)$ (namely, $p = r$ and $q = r$). In other words, the polynomials $t-a$ and $t-b$ are equivalent in $R[t]$ (by the definition of "equivalent"). This proves the "$\Longrightarrow$" direction of Theorem 2.2.

$\Longleftarrow$: Assume that the polynomials $t-a$ and $t-b$ are equivalent in $R[t]$. We must show that a and b are conjugate in R.

We have assumed that the polynomials $t-a$ and $t-b$ are equivalent in $R[t]$. In other words, there exist invertible elements $p, q \in R[t]$ such that

$$(t-a)p = q(t-b) \tag{4}$$

(by the definition of "equivalent"). Consider these p and q. Note that p and q are invertible; thus, p^{-1} and q^{-1} are invertible as well.

We now claim that

$$r_a(q) \cdot r_b\left(q^{-1}\right) = 1. \tag{5}$$

[*Proof of* (5): Proposition 3.3 **(a)** (applied to $s = q$ and $c = r_b(q^{-1})$) yields

$$r_a\left(q r_b\left(q^{-1}\right)\right) = r_a(q) \cdot r_b\left(q^{-1}\right). \tag{6}$$

However, Proposition 3.3 **(d)** (applied to b and q^{-1} instead of a and s) yields that there exists a polynomial $\overline{s} \in R[t]$ such that $q^{-1} = r_b(q^{-1}) + (t-b)\overline{s}$. Consider this $\overline{s}$. Then, solving the equality $q^{-1} = r_b(q^{-1}) + (t-b)\overline{s}$ for $r_b(q^{-1})$, we find

$$r_b\left(q^{-1}\right) = q^{-1} - (t-b)\overline{s}.$$

Thus,

$$q \underbrace{r_b\left(q^{-1}\right)}_{=q^{-1}-(t-b)\overline{s}} = q\left(q^{-1} - (t-b)\overline{s}\right) = 1 - \underbrace{q(t-b)}_{\substack{=(t-a)p \\ \text{(by (4))}}}\overline{s} = 1 - (t-a)p\overline{s}.$$

Applying the map r_a to this equality, we find

$$\begin{aligned} r_a\left(q r_b\left(q^{-1}\right)\right) &= r_a(1 - (t-a)p\overline{s}) \\ &= \underbrace{r_a(1)}_{\substack{=1 \\ \text{(this follows easily} \\ \text{from the} \\ \text{definition of } r_a)}} - \underbrace{r_a((t-a)p\overline{s})}_{\substack{=0 \\ \text{(by Proposition 3.3 (c),} \\ \text{applied to } p\overline{s} \text{ instead of } s)}} \qquad \text{(by Proposition 3.2)} \\ &= 1 - 0 = 1. \end{aligned}$$

Comparing this with (6), we obtain $r_a(q) \cdot r_b(q^{-1}) = 1$. Thus, (5) is proven.]

Now, we notice a symmetry slightly hidden in our setting: If we multiply both sides of the equality (4) by q^{-1} on the left and by p^{-1} on the right, then we obtain $q^{-1}(t-a)\,pp^{-1} = q^{-1}q\,(t-b)\,p^{-1}$. This simplifies to $q^{-1}(t-a) = (t-b)\,p^{-1}$ (since $q^{-1}(t-a)\underbrace{pp^{-1}}_{=1} = q^{-1}(t-a)$ and $\underbrace{q^{-1}q}_{=1}(t-b)\,p^{-1} = (t-b)\,p^{-1}$).

In other words,

$$(t-b)\,p^{-1} = q^{-1}(t-a)\,.$$

This equality has the same form as (4), but with the elements b, a, p^{-1} and q^{-1} playing the roles of a, b, p and q. Hence, we can prove the equality

$$r_b\left(q^{-1}\right)\cdot r_a\left(\left(q^{-1}\right)^{-1}\right) = 1$$

using the same reasoning that we used to prove (5) (but with a, b, p and q replaced by b, a, p^{-1} and q^{-1}). Since $\left(q^{-1}\right)^{-1} = q$, this equality rewrites as

$$r_b\left(q^{-1}\right)\cdot r_a(q) = 1.$$

Combining this equality with (5), we conclude that the elements $r_a(q)$ and $r_b\left(q^{-1}\right)$ are mutually inverse in R. Thus, the element $r_a(q) \in R$ is invertible.

Finally, applying the map r_a to both sides of (4), we obtain

$$\begin{aligned} r_a((t-a)\,p) &= r_a\left(\underbrace{q\,(t-b)}_{=qt-qb}\right) = r_a(qt-qb) \\ &= \underbrace{r_a(qt)}_{\substack{=ar_a(q) \\ \text{(by Proposition 3.3 (b),} \\ \text{applied to } s=q)}} - \underbrace{r_a(qb)}_{\substack{=r_a(q)b \\ \text{(by Proposition 3.3 (a),} \\ \text{applied to } s=q \text{ and } c=b)}} \qquad \text{(by Proposition 3.2)} \\ &= ar_a(q) - r_a(q)\,b. \end{aligned}$$

Hence,

$$ar_a(q) - r_a(q)\,b = r_a((t-a)\,p) = 0$$

(by Proposition 3.3 **(c)**, applied to $s = p$). In other words, $ar_a(q) = r_a(q)\,b$. Since $r_a(q) \in R$ is invertible, this shows that there exists an invertible element $z \in R$ such that $az = zb$ (namely, $z = r_a(q)$). In other words, a and b are conjugate in R. This proves the "$\Longleftarrow$" direction of Theorem 2.2. The proof of Theorem 2.2 is thus complete. □

References

[Gantma77] F. R. Gantmacher, *The Theory of Matrices, volume 1*, AMS Chelsea Publishing 1977.