From similarity over $\mathbb{C}$ to $\mathbb{Q}$

Seewoo Lee

February 15, 2022

This is a problem from Berkeley's preliminary exam.

Theorem 1. *Let A, B be $n \times n$ matrices with coefficients in $\mathbb{Q}$. For any field extension K of $\mathbb{Q}$, we say that A and B are similar over K if $A = PBP^{-1}$ for some $n \times n$ invertible matrix P with coefficients in K. Prove that A and B are similar over $\mathbb{Q}$ if and only if they are similar over $\mathbb{C}$.*

Proof. (This is a proof from the original solution of the exam.) The *only if* part is trivial, and we will show the *if* part. Let $P = (x_{ij})$. The condition that A and B are similar over $\mathbb{C}$ is equivalent to the statement that the system of equation

$$AP = PB, \quad \det(P) \neq 0$$

has a solution in $(x_{ij}) \in \mathbb{C}^{n^2} \simeq M_{n\times n}(\mathbb{C})$. We need to show that the system has a solution in $\mathbb{Q}^{n^2}$.

Let $V \subset \mathbb{Q}^{n^2}$ be a space of solution of $AP = PB$ and let $W \subset \mathbb{C}^{n^2}$ be a space of solution of the same equation. Then we have a natural isomorphism $W \simeq V \otimes_{\mathbb{Q}} \mathbb{C}$. (The system of equation is just a linear equation over $\mathbb{Q}$). Since $W \neq 0$, $V \neq 0$ and we have a rational solution.

Now we have to consider the condition $\det(P) \neq 0$. Take a basis of V over $\mathbb{Q}$, and identify V with $\mathbb{Q}^m$ for some m. Then this basis also gives an identification $W = \mathbb{C}^m$. Now the restriction of $\det(P)$ to V becomes a polynomial $f(y_1, \dots, y_m)$ of m variables with rational coefficients via the identification. By the condition, f is not identically zero over $\mathbb{C}$, so it is not the zero polynomial. Hence, we can find an element of $\mathbb{Q}^m$ at which f is nonzero, and this element gives the desired solution in $\mathbb{Q}^{n^2}$ of the equation. □

As you can see in the proof, this theorem holds for any arbitrary field extension K/F of characteristic zero. More precisely, if A, B are $n \times n$ matrices over a characteristic zero field F which are similar over a field K, then it is also similar over F. However, you can't apply the same proof for characteristic p cases, since there exist nonzero polynomials which have 0 values at every points. (For example, $x^p - x \in \mathbb{F}_p[x]$ is a nonzero polynomial which became 0 when we evaluates at $a \in \mathbb{F}_p$.) But the result is still true for any field extension, and we are going to introduce some other proofs that are posed in this MSE post.

proof 2. Actually, this is a direct consequence of existence of a rational canonical form.

Theorem 2 (Rational canonical form)**.** *Let F be a field and $A \in M_{n\times n}(F)$. Then there exists $Q \in \mathrm{GL}_n(F)$ s.t. $A = QLQ^{-1}$, where $L = \mathrm{diag}(L(f_1), \dots, L(f_k))$ and $L(f)$ is a companion matrix of a polynomial f, i.e.*

$$L(f) = \begin{pmatrix} 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$$

where $f(x) = a_0 + a_1 + \cdots + a_{n-1}x^{n-1} + x^n$.

The existence follows from the structure theorem of the finitely generated module over PID (and $F[x]$ is a PID for any field F). Consider F^n as $F[x]$-module where x acts as multiplication by A, then we have a decomposition

$$F^n \simeq F[x]/(f_1(x)) \oplus F[x]/(f_2(x)) \oplus \cdots \oplus F[x]/(f_r(x))$$

as invariant subspaces with $f_1|f_2|\cdots|f_r$. Note that such decomposition is unique up to isomorphism, hence rational canonical form is also unique.

It is known that two matrices are similar if and only if their rational canonical form are same. So if A and B are similar (over K), they have a same rational canonical form, so they are similar over F. □

proof 3. This proof only applies when F is not a finite field. (not finished) □