SIMILARITY OF MATRICES OVER FINITE RINGS

J. POMFRET

Abstract. It is shown that questions of similarity of certain invertible matrices over a finite ring can be reduced to questions of similarity over finite fields through the application of canonical epimorphisms.

Suprunenko has shown in [3] that two invertible matrices over $\mathbb{Z}/\mathbb{Z}_m$ whose orders are relatively prime to $m$ are similar if and only if their canonical images are similar over the fields $\mathbb{Z}/\mathbb{Z}_p$ for each prime divisor $p$ of $m$. An analogous result holds for invertible matrices over any finite commutative ring with identity.

Preliminaries. If $R$ is a finite commutative ring with identity, then $R$ is uniquely a ring direct product of finite local rings [1, Theorem 8.7, p. 90]. Suppose that $R=\prod_{i=1}^{t} R_i$, where $R_i$ is a finite local ring with maximal ideal $M_i$. Each $R_i$ has cardinality $p_i^t$ for some prime $p$ and has associated with it a canonical projection,

$$h_i: R_i \rightarrow R_i/M_i = GF(p_i^t).$$

Setting $k_i=GF(p_i^t)$ we will say that the finite fields $\{k_i:i=1, 2, \cdots, t\}$ are the fields associated with $R$.

Observe that the decomposition of $R$ carries over to the general linear group of degree $n$ over $R$ yielding $GL_n(R)\cong\prod_{i=1}^{t} GL_n(R_i)$. Furthermore, for each $i$, the projection $h_i$ induces an epimorphism,

$$h_i: GL_n(R_i) \rightarrow GL_n(k_i).$$

If $GL_n(R_i)$ is taken as the group of $n$ by $n$ invertible matrices over $R_i$, then $h_i$ is simply reduction modulo $M_i$. Note that the kernel of $h_i$, $K_i$, has cardinality a power of $p_i$ and thus is a solvable group.

The following corollary to P. Hall's extension of the Sylow theorems [2, Theorem 9.3.1, p. 141] is the key result needed for Theorems 1 and 2.

Observation. Let $G$ be a finite group with solvable normal subgroup $K$ and let $G=G/K=\langle g | g \in G \rangle$. Let $\alpha$ and $\beta$ be elements of $G$ with $(|\alpha|, |K|)=1=(|\beta|, |K|)$. Then $\bar{\alpha} \sim \bar{\beta}$ implies $\alpha \sim \beta$. 

Received by the editors April 12, 1972.


Key words and phrases. Similarity, finite local ring, finite solvable group.
Proof. Since $\bar{a} = \gamma^{-1}\bar{b}\gamma$ for some $\gamma$ it follows that $\langle a \rangle_K = \langle \gamma^{-1}\beta\gamma \rangle_K$. By P. Hall's theorem it follows that $\langle a \rangle$ and $\langle \gamma^{-1}\beta\gamma \rangle$ are conjugate in $\langle a \rangle_K$. Thus there is a $\mu$ in $K$ and $r > 0$ such that $\mu^{-1}\gamma^{-1}\beta\gamma\mu = \alpha^r$. Hence $\bar{a}^r = \gamma^{-1}\bar{b}\gamma = \bar{a}$ and, since $a$ and $\bar{a}$ have the same order, $\alpha = \alpha^r$. Therefore $\alpha = (\gamma\mu)^{-1}\beta(\gamma\mu)$ and $\alpha \sim \beta$.

The theorems.

Theorem 1. Let $R$ be a finite local ring with maximal ideal $M$ and $R/M = GF(p^n) = k$. Let $\alpha$, $\beta$ be elements of $GL_n(R)$ with $(|\alpha|, p) = 1$ and $(|\beta|, p) = 1$. Then $\alpha$ is similar to $\beta$ if and only if $\alpha$ is similar to $\beta$ modulo $M$.

Proof. This follows from the Observation by noting that the kernel, $K$, of $h:GL_n(R) \rightarrow GL_n(R/M)$ is solvable with cardinality a power of $p$.

Theorem 2. Let $R$ be a finite commutative ring with identity and let the cardinality of $R$ be $m$. Two elements $\alpha$ and $\beta$ of $GL_n(R)$ satisfying $(|\alpha|, m) = (|\beta|, m) = 1$ are similar if and only if their canonical images over the Galois fields associated with $R$ are similar.

Proof. This follows from Theorem 1 directly by means of the sequence of epimorphisms

$$GL_n(R) = \prod_{i=1}^t GL_n(R_i) \xrightarrow{\pi_i} GL_n(R_i) \xrightarrow{h_i} GL_n(k_i).$$

Bibliography


Department of Mathematics, Clemson University, Clemson, South Carolina 29631

Current address: Department of Mathematics, Bloomsburg State College, Bloomsburg, Pennsylvania 17815