Matrices that are similar to their inverses

GRIGORE CĂLUGĂREANU

1. *Introduction*

In a group G, an element which is conjugate with its inverse is called *real*, i.e. the element and its inverse belong to the same *conjugacy class*. An element is called an *involution* if it is of order 2. With these notions it is easy to formulate the following questions.

1) Which are the (finite) groups all of whose elements are real ?
2) Which are the (finite) groups such that the identity and involutions are the only real elements ?
3) Which are the (finite) groups in which the real elements form a subgroup closed under multiplication?

According to specialists, these (general) questions cannot be solved in any reasonable way. For example, there are numerous families of groups all of whose elements are real, like the symmetric groups S_n. There are many solvable groups whose elements are all real, and one can prove that *any finite solvable group occurs as a subgroup of a solvable group whose elements are all real*.

As for question 2, note that in any Abelian group (conjugations are all the identity function), the only real elements are the identity and the involutions, and they form a subgroup. There are non-abelian examples as well, like a Suzuki 2-group.

Question 3 is similar to questions 1 and 2.

Therefore the abstract study of reality questions in finite groups is unlikely to have a good outcome. This may explain why in the existing bibliography there are only specific studies (see [1, 2, 3, 4]).

In this note, as another specific study, we determine the real elements of $GL_2(\mathbb{Z})$, i.e. we answer the following

Question: When is an invertible integral 2×2 matrix similar to its inverse?

These properties lead to some quadratic Diophantine equations, which may be solved using software on the Internet (e.g. [5]).

As examples will show, for an element u in a ring R, there are three possibilities:

u and u^{-1} are not conjugate,

or there are finitely many $v \in U(R)$ such that $u^{-1}v = vu$,

or there are infinitely many $v \in U(R)$ with $u^{-1}v = vu$. Notice that if $u^{-1}v = vu$ then also $-v \in U(R)$ has this property.

To simplify the wording we say that u has *zero index*, *finite index* or *infinite index* respectively (we neglect the $\pm$; e.g. u has index 3 means there are 6 different v, i.e. $\pm v_1, \pm v_2, \pm v_3$ such that $u^{-1}v_i = v_i u$, $i \in \{1, 2, 3\}$).

A trivial example of elements which are conjugate with their inverses are the *involutions*, i.e. order 2 elements, $u^2 = 1$ (indeed, then $u^{-1} = u$ and $v = u$).

It is easy to show that the property of being real is invariant under conjugations, i.e. if u is real and conjugate to v then v is (also) real.

However, real elements need not be conjugate.

Moreover, since there exist non-real elements, not every conjugacy class contains real elements. More precisely, in each conjugacy class either all elements are real or no element is real.

In a given group, it can be tricky to find the elements that are not real. For example, in [6], the group of unipotent upper triangular $n \times n$ matrices over the field $\mathbb{F}_q$, is considered, so that $U_n(\mathbb{F}_q)$ is a Sylow p-subgroup of the general linear group $GL_n(\mathbb{F}_q)$, where q is a power of a prime number p. The authors show that for sufficiently large n, there exist matrices in $U_n(\mathbb{F}_2)$ that are not real. In $U_{13}(\mathbb{F}_2)$, a matrix is given, and even if there is no direct proof of this, four independent computer calculations confirmed that this matrix is not real.

2. *Real matrices in* $\mathcal{M}_2(\mathbb{Z})$

First, it is easy to specify the involutory matrices U, such that $U^2 = I_2$. These are the four matrices $\begin{bmatrix} \pm 1 & 0 \\ 0 & \pm 1 \end{bmatrix}$ and the matrices $U_{ab} = \begin{bmatrix} a & b \\ \dfrac{1 - a^2}{b} & -a \end{bmatrix}$, for any a and $b \neq 0$ such that $b \mid (1 - a^2)$.

As a general remark, notice that the characteristic polynomial of an invertible matrix U over the integers, $p_U(X) = X^2 - \mathrm{Tr}(U)X \pm 1$ is rarely reducible over $\mathbb{Z}$: it is reducible if, and only if, $\mathrm{Tr}(U) \in \{0, \pm 2\}$. Indeed, $\Delta = \mathrm{Tr}^2(U) \pm 4$; for $+4$ the equation $x^2 + 4 = y^2$ has only the solutions $\pm(0, 2)$, and for -4 the equation $x^2 - 4 = y^2$ has only the solutions $\pm(2, 0)$. Hence we cannot expect eigenvalues, eigenvectors or Jordan normal form to solve our problem.

Examples show that the irreducibility of the characteristic polynomial (or the reducibility) does not characterise real matrices.

Also notice that for an invertible matrix $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$, we can always suppose $b \neq 0$ or $c \neq 0$, because otherwise U is diagonal and thus one of the four involutory matrices already mentioned.

Next, for the equality $U^{-1}V = VU$, with invertible U and V there are four possibilities: $\det U = \pm 1$ and $\det V = \pm 1$.

Here is a first result.

Theorem 1: Let $U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be invertible over $\mathbb{Z}$, $b \neq 0$ and $\det U = 1$. Then $U^{-1}V = VU$ with $V = \begin{bmatrix} x & y \\ z & t \end{bmatrix}$ and $\det V = 1$ if, and only if, the following conditions hold:

(i) there exists $y \in \mathbb{Z}$ such that $\big(\mathrm{Tr}\,(U)^2 - 4\big)y^2 - 4b^2$ is a square, say Y^2; this includes $|\mathrm{Tr}\,(U)| \geqslant 2$.

(ii) $2b$ divides $Y - (d - a)y$;

(iii) b divides $(d - a)x - cy$.

Actually $Y = 2bx + (d - a)y$, $bz = (d - a)x - cy$ and the conditions include $U = \pm I_2$.

Proof: Assume $U^{-1}V = VU$. Then $U^{-1} = \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ and the equality of the products gives

$$(d-a)x = cy + bz, b(x+t) = 0 = c(x+t), (d-a)t = -cy - bz.$$

The first and the fourth equations give $(d - a)(x + t) = 0$. Hence

(i) $x + t \neq 0$ gives obviously $b = c = 0$, $a = d = \pm 1$, so $U = \pm I_2$.

(ii) If $x + t = 0$, the second and third equations hold, $t = -x$, so the first and the fourth coincide.

Hence the conditions are $(d - a)x = cy + bz$ and $t = -x$, that is, a matrix U is similar to its inverse (with $\det V = 1$) if, and only if, $U = \pm I_2$ or there exist integers x, y, z with $x^2 + yz = -1$ such that $(d - a)x = cy + bz$.

This reduces to some quadratic Diophantine equations, depending on.

(1) $a \neq d$; $(d-a)x = cy + bz$ gives $(cy + bz)^2 + (d-a)^2yz + (d-a)^2 = 0$, i.e.

$$c^2y^2 + \big[(d - a)^2 + 2bc\big]yz + b^2z^2 + (d - a)^2 = 0.$$

(2) $b \neq 0$: $bz = (d-a)x - cy$ gives $bx^2 + y\big[(d-a)x - cy\big] = -b$, i.e.

$$bx^2 + (d - a)xy - cy^2 + b = 0$$

(3) $c \neq 0$: $cy = (d - a)x - bz$ gives $cx^2 + z\big[(d-a)x - bz\big] = -c$, i.e.

$$cx^2 + (d - a)xz - bz^2 + c = 0.$$

Since we assume $b \neq 0$, the reduction of the Diophantine equation (2) to its canonical form gives $[2bx + (d - a)y]^2 + 4b^2 = \big[(a + d)^2 - 4\big]y^2$ or $\big[(a + d)^2 - 4\big]y^2 - 4b^2 = [2bx + (d - a)y]^2$ or else

$$DX^2 = Y^2 + 4b^2$$

where $X = y$, $Y = 2bx + (d - a)y$ and $D = \mathrm{Tr}^2(Y) - 4$. From the

canonical form, clearly $D = \mathrm{Tr}^2(A) - 4 \geqslant 0$ (i.e. $|\mathrm{Tr}(U)| \geqslant 2$) is necessary in order to have real solutions.

Now the existence of the invertible matrix V with $U^{-1}V = VU$ (and $\det V = 1$) follows from the conditions (i)-(iii) in the statement of the theorem.

Examples: (All with $\det U = \det V = 1$.)

(a) *A real matrix of infinite index and irreducible characteristic polynomial*

$U = \begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}$ with $a = 2$, $b = c = d = 1$, so $\mathrm{Tr}(U) = 3$. Then $5y^2 - 4 = 1^2$ for $y = 1$ and for $Y = 1$, $Y - (d - a)y = 2$, $2b = 2$ so $x = 1$. Finally, $bz = (d - a)x - cy$ gives $z = -2$. Indeed,

$$U^{-1}V = \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix}\begin{bmatrix} 1 & 1 \\ -2 & -1 \end{bmatrix} = \begin{bmatrix} 3 & 2 \\ -5 & -3 \end{bmatrix}$$

$$= \begin{bmatrix} 1 & 1 \\ -2 & -1 \end{bmatrix}\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = VU.$$

In the above we have dealt with only one matrix V since it is easy to see that $5y^2 - 4$ is a square for $y = 1$.

Also $y = 2$, $Y = 4$ works: $2bx + (d - a)y = Y$ gives $x = 3$ and $bz = (d - a)x - cy$ gives $z = -5$. Indeed,

$$U^{-1}V = \begin{bmatrix} 1 & -1 \\ -1 & 2 \end{bmatrix}\begin{bmatrix} 3 & 2 \\ -5 & -3 \end{bmatrix} = \begin{bmatrix} 8 & 5 \\ -13 & -8 \end{bmatrix}$$

$$= \begin{bmatrix} 3 & 2 \\ -5 & -3 \end{bmatrix}\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix} = VU.$$

If we want to find all V (and so the index of U), we must first solve the other quadratic Diophantine equation $5y^2 - 4 = Y^2$. The solutions are $\pm(1, 1)$, $\pm(1, -1)$, $\pm(4, 2)$ and infinitely many other solutions given by recursion $x_{n+1} = 9x_n + 20y_n$, $y_{n+1} = 4x_n + 9y_n$, and also $x_{n+1} = 9x_n - 20y_n$, $y_{n+1} = -4x_n + 9y_n$. So U has *infinite index*. The characteristic polynomial, $p_U(x) = X^2 - 3X + 1$, is irreducible over $\mathbb{R}$.

(b) *Matrices in the same conjugacy class*

$U = \begin{bmatrix} 3 & 1 \\ -1 & 0 \end{bmatrix}$ is similar to the one in (a):

$$\begin{bmatrix} 2 & 1 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 3 & 1 \\ 2 & 1 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ 1 & 1 \end{bmatrix}\begin{bmatrix} 3 & 1 \\ -1 & 0 \end{bmatrix}.$$

Hence, from the invariance to similarity mentioned in the introduction, this U is also real with infinite index. Clearly U and V have the same trace,

determinant and characteristic polynomial. For instance $V = \begin{bmatrix} 2 & 1 \\ -5 & -2 \end{bmatrix}$ shows the reality property.

In order to simplify the statement of the next result, we first describe the invertible matrices U with $|\mathrm{Tr}(U)| < 2$. This is only possible with $\mathrm{Tr}(U) = 0$ or $\mathrm{Tr}(U) \in \{\pm 1\}$.

If $\mathrm{Tr}(U) = 0$, by the Cayley-Hamilton theorem, $U^2 = I_2$, so the involutory matrices are the matrices $U = \begin{bmatrix} a & b \\ -\dfrac{1+a^2}{b} & -a \end{bmatrix}$ for every $b \neq 0$ such that $b \mid (1 - a^2)$.

If $\mathrm{Tr}(U) = 1$, $\det U = 1$ then by the Cayley-Hamilton theorem, $U^2 - U + I_2 = 0_2$ or equivalently $U^{-1} = I_2 - U$. These are $U = \begin{bmatrix} a & b \\ \dfrac{a - a^2 - 1}{b} & 1 - a \end{bmatrix}$ for every $b \neq 0$ such that $b \mid (a^2 - a + 1)$.

The situations $\mathrm{Tr}(U) = 1$, $\det U = -1$ and $\mathrm{Tr}(U) = 1$, $\det U = \pm 1$ are analogous.

The following result refers to $|\mathrm{Tr}(U)| \geqslant 2$.

Theorem 2: Let $U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be invertible over $\mathbb{Z}$, $b \neq 0$, $|\mathrm{Tr}(U)| \geqslant 2$ and $\det U = 1$. Then $U^{-1}V = VU$ with $V = \begin{bmatrix} x & y \\ z & t \end{bmatrix}$ and $\det V = -1$ if, and only if, the following conditions hold:

(i) there exists $y \in \mathbb{Z}$ such that $(\mathrm{Tr}^2(U) - 4)y^2 + 4b^2$ is a square, say Y^2,

(ii) $2b$ divides $Y - (d - a)y$,

(iii) b divides $(d - a)x - cy$.

Actually $Y = 2bx + (d - a)y$, $bz = (d - a)x - cy$.

Proof: If $\det U = 1$, $\det V = -1$, the same computation as in the previous proof works until we have to use $xt - yz = -1$ for $t = -x$, that is, $x^2 + yz = 1$ (instead of -1).

This slightly modifies the quadratic Diophantine equations obtained there:

(1) $a \neq d$: $(d - a)x = cy + bz$ gives $(cy + bz)^2 + (d - a)^2 yz - (d - a)^2 = 0$, i.e.

$$c^2y^2 + [(d - a)^2 + 2bc]yz + b^2z^2 - (d - a)^2 = 0;$$

(2) $b \neq 0$: $bz = (d-a)x - cy$ gives $bx^2 + y\left[(d-a)x - cy\right] = b$, i.e.

$$bx^2 + (d-a)xy - cy^2 - b = 0;$$

(3) $c \neq 0$: $cy = (d-a)x - bz$ gives $cx^2 + z\left[(d-a)x - bz\right] = c$, i.e.

$$cx^2 + (d-a)xz - bz^2 - c = 0.$$

We continue with $b \neq 0$ and the canonical form is

$$[2bx + (d-a)y]^2 - 4b^2 = \left[(a+d)^2 - 4\right]y^2$$

or else $\left(\mathrm{Tr}^2(A) - 4\right)X^2 + 4b^2 = Y^2$ with $X = y$, $Y = 2bx + (d-a)y$.

Since $D = \mathrm{Tr}^2(A) - 4 \neq 0$ (i.e. $|\mathrm{Tr}(U)| \geqslant 2$), the existence of the invertible matrix V with $U^{-1}V = VU$ (and $\det V = 1$) follows from the conditions (i)-(iii) in the statement of the theorem.

More examples

(c) *A matrix which is not real with irreducible characteristic polynomial*

$U = \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix}$. When searching for V with $\det V = 1$, the Diophantine equation (2) is $2x^2 - 2xy - y^2 + 2 = 0$, with no integer solutions.

Actually, the canonical form here is $DX^2 = Y^2 + 4b^2$ i.e. $(2x-y)^2 + 4 = 3y^2$, and one can check directly that $3y^2 - 4$ is not a square, because of well-known properties: all even square numbers are divisible by 4, numbers of the form $4n + 2$ are not square numbers, all odd square numbers are of the form $4n + 1$, numbers of the form $4n + 3$ are not square numbers.

The characteristic polynomial, $p_X(U) = X^2 - 4X + 1 = (X-2)^2 - 3$, is irreducible over $\mathbb{Z}$.

When searching for V with $\det V = -1$, the Diophantine equation (2) is now $2x^2 - 2xy - y^2 - 2 = 0$, with no solutions. Therefore $U = \begin{bmatrix} 3 & 2 \\ 1 & 1 \end{bmatrix}$ is not real (not similar to its inverse).

(d) *There is no V with* $\det V = 1$ *but infinitely many V with* $\det V = -1$. The characteristic polynomial is reducible over $\mathbb{Z}$.

$U = \begin{bmatrix} -62 & 147 \\ -27 & 64 \end{bmatrix}$. As for V with $\det V = 1$, equation (2) is $147x^2 + 126xy + 27y^2 + 174 = 3\left[(7x + 3y)^2 + 7^2\right] = 0$, with no integer solutions.

The characteristic polynomial $p_X(U) = X^2 - 2X + 1 = (X-1)^2$ is reducible over $\mathbb{Z}$.

As for V with $\det V = -1$, the Diophantine equation (2) is $147x^2 + 126xy + 27y^2 - 147 = 0$, and has infinitely many solutions: $(-1 + 3s, -7s)$ or $(1 + 3s, -7s)$.

Further, we need $bz = (d-a)x - cy$ to be solvable for z, i.e., $147z = 126x + 27y$.

Now $147z = 126(\pm 1 + 3s) - 27 \cdot 7s$ reduces to $21z = 18(\pm 1 + 3s) - 27s$ or $7z = 6(\pm 1 + 3s) - 9s = 3(\pm 2 + 3s)$, for which it is necessary (and sufficient) $7 \mid 2 + 3s$ or equivalently $3s = 7k \mp 2 = 6k + k \mp 2$. Hence for $+$: $k - 2 = 3l$, $s = 7l + 4$ and $V = \begin{bmatrix} 21l + 13 & -49l - 28 \\ 9l + 6 & -21l - 13 \end{bmatrix}$ $[\det V = -1]$, and for $-$: $V = \begin{bmatrix} 21l - 13 & -49l + 28 \\ 9l - 6 & -21l + 13 \end{bmatrix}$.

Both $U^{-1}V = VU$ are verified, so U has *infinite index*. U is similar to U^{-1} by infinitely many different V, all with $\det V = -1$, but there are no V with $\det V = 1$.

(e) *A real matrix of index* 3 *with irreducible characteristic polynomial*

$U = \begin{bmatrix} 3 & 13 \\ -1 & -4 \end{bmatrix}$. First notice that equation (2) for $\det V = 1$ has no integer solutions.

Secondly, equation (2) for $\det V = -1$ becomes $13x^2 - 7xy + y^2 - 13 = 0$ which has 12 solutions: $\pm(3, 8)$, $\pm(1, 7)$, $\pm(4, 15)$, $\pm(1, 0)$, $\pm(4, 13)$, $\pm(3, 13)$.

Further we need $bz = (d-a)x - cy$ to be solvable for z, i.e., $13z = -7x + y$. Only the first three $(\pm)$ pairs verify so we get $V = \pm\begin{bmatrix} 3 & 8 \\ -1 & -3 \end{bmatrix}, \pm\begin{bmatrix} 1 & 7 \\ 0 & -1 \end{bmatrix}, \pm\begin{bmatrix} 4 & 15 \\ -1 & -4 \end{bmatrix}$. Hence this U has index 3.

(f) *A real matrix of infinite index and characteristic polynomial reducible over* $\mathbb{Z}$

$U = \begin{bmatrix} 1 & 4 \\ -1 & -3 \end{bmatrix}$. Now (2) for $\det V = -1$ is

$$4x^2 - 4xy + y^2 - 4 = 0 = (2x + y)^2 - 4,$$

which has infinitely many integer solutions: $(\pm 1 + s, 2s)$.

We need these to verify $bz = (d - a)x - cy$, i.e. $4z = -4x + y$. This is clearly verified if, and only if, $s = 2l$ while $x = \pm 1 + 2l$, $y = 4l$, $z = \mp 1 - l$ and $t = -x = \mp 1 - 2l$.

Hence $V = \begin{bmatrix} \pm 1 + 2l & 4l \\ \pm 1 - l & \mp 1 - 2l \end{bmatrix}$ with $\det V = -1$, i.e. U has infinite index. The characteristic polynomial is reducible over $\mathbb{Z}$: $p_X(U) = X^2 + 2X + 1 = (X + 1)^2$.

Remark: If in $GL_2(\mathbb{Z})$ we write $A = \begin{bmatrix} 3 & 13 \\ -1 & -4 \end{bmatrix}$, $B = \begin{bmatrix} 1 & 4 \\ -1 & -3 \end{bmatrix}$, using the previous two examples, these are real, but they are not conjugate: $AX = XB$

for $X = \begin{bmatrix} x & y \\ z & t \end{bmatrix}$ amounts to a homogeneous linear system which has only the zero solution (its 4×4 determinant is -1).

Finally, a surprising result

Theorem 3: Let $U = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ be invertible over $\mathbb{Z}$, $b = 0$ and $\det U = -1$. Then $U^{-1}V = VU$ with invertible $V = \begin{bmatrix} x & y \\ z & t \end{bmatrix}$ if, and only if. U is involutory.

Proof: If $\det U = -1$ then $U^{-1} = \begin{bmatrix} -d & b \\ c & -a \end{bmatrix}$ and $(a + d)x = -cy + bz$, $b(-x + t) = 0$, $c(x - t)$, $(a + d)t = cy - bz$. The first and the fourth of these equations give $(a + d)(x + t) = 0$.

Case 1: If $a + d = 0$ then by the Cayley-Hamilton theorem, $U^2 - I_2 = 0_2$, that is $U = U^{-1}$, an involutory matrix.

Case 2: If $a + d \neq 0$ and $x + t = 0$ then $t = -x$ and the above system becomes $(a + d)x = -cy + bz$, $-bx = dy$, $cx = az$.
(a) If both $b \neq 0 \neq c$, we can eliminate x and since $ad - bc = -1$ we get $(d^2 - 1)y + b^2z = 0$, $c^2y + (a^2 - 1)z = 0$.

If $\det\begin{bmatrix} d^2 - 1 & b^2 \\ c^2 & a^2 - 1 \end{bmatrix} \neq 0$ the system has only the zero solution. Hence also $x = t = 0$ but $V = 0_2$ is not invertible.

If $\det\begin{bmatrix} d^2 - 1 & b^2 \\ c^2 & a^2 - 1 \end{bmatrix} \neq 0$, from $bc = ad + 1$ and $(a^2 - 1)(d^2 - 1) = b^2c^2$ we obtain $(a + d)^2 = 0$ which is impossible.

(b) Suppose $b \neq 0$ and $c = 0$; since $cx = az$, a cannot be zero (otherwise U is not invertible), so $z = 0$. Hence $(a + d)x = 0$ and so $x = 0$, but then V is not invertible.

(c) $b = 0$, $c \neq 0$ is analogous.

(d) $b = c = 0$ reduces to diagonal matrices (the four involutory matrices mentioned the beginning of this section).

Remark: Since the equality $U^{-1}V = VU$ does not use V^{-1} (and also $xt - yz = \pm 1$ is not used), the above theorem covers both $\det V = +1$ an $\det V = -1$.

References

1. J. L. Berrgren, Finite groups in which every element is conjugate to its inverse, *Pac. J. of Math.* **28** (1969) pp. 289-293.
2. R. Gow, Groups whose characters are rational-valued, *J. of Algebra* **40** (1) (1976) pp. 280–299.
3. R. Gow, Properties of the characters of the finite general linear group related to the transpose-inverse involution, *Proc. London Math. Soc.* (3) **47** (1983) (3) pp. 493-506.
4. P. Hegedüs, Groups where each element is conjugate to its certain power, *Cent. Eur. J. Math.* **11** (10) (2013) pp. 1742-1749.
5. D. Alpern, Generic two integer variable equation solver, available at https://www.alpertron.com.ar/QUAD.HTM
6. I. M. Isaacs, D. Karagueuzian, Conjugacy in groups of upper triangular matrices, *J. of Algebra* **202** (1998) pp. 704-711.
7. W. C. Brown, *Matrices over commutative rings*, Monographs and textbooks in pure and applied mathematics. New York, M. Dekker, (1993).

10.1017/mag.2020.13

GRIGORE CĂLUGĂREANU

Dept. of Mathematics, Babes-Bolyai University, 1 Kogălniceanu Street, 400084, Cluj-Napoca, Romania

e-mail: *calu@math.ubbcluj.ro*