



Title	A remark on conjugacy classes in simple groups
Author(s)	Nobusawa, Nobuo
Citation	Osaka Journal of Mathematics. 1981, 18(3), p. 749-754
Version Type	VoR
URL	https://doi.org/10.18910/11034
rights	
Note	

The University of Osaka Institutional Knowledge Archive : OUKA

<https://ir.library.osaka-u.ac.jp/>

The University of Osaka

Nobusawa, N.
Osaka J. Math.
18 (1981), 749-754

A REMARK ON CONJUGACY CLASSES IN SIMPLE GROUPS

NOBUO NOBUSAWA

(Received January 23, 1980)

Let A be a union of some conjugacy classes in a group. We define a binary operation on A by $a \circ b = b^{-1}ab$. It satisfies that (1) $a \circ a = a$, (2) $(a \circ b) \circ c = (a \circ c) \circ (b \circ c)$ and (3) a mapping $\sigma_a: x \rightarrow x \circ a$ is a permutation on A . Generally we call a binary system which satisfies the above three conditions a pseudosymmetric set. It is called a symmetric set if (4) σ_a has the order 2 is also satisfied. The set of all nilpotent elements in a Lie algebra is another example of a pseudosymmetric set, where $\sigma_a = \exp(\text{ad } a)$. The purpose of this note is to generalize the main result on the simplicity of a symmetric set given in [2] to the case of a pseudosymmetric set. As applications, three examples of conjugacy classes in simple groups A_n , $SL(V)$ and $Sp(V)$ will be discussed, from which we could derive a new proof of the simplicity of the corresponding groups A_n , $PSL(V)$ and $PSp(V)$.

Generally, let A be a pseudosymmetric set and define $G = G(A) = \langle \sigma_a | a \in A \rangle$, a group generated by σ_a . The above three conditions imply that G is a group of automorphisms of A . Note that if ρ is an automorphism of A , then $\sigma_a \rho = \rho^{-1} \sigma_a \rho$. $\{\sigma_a | a \in A\}$ is a union of conjugacy classes in G and hence is a pseudosymmetric set, and the mapping $\sigma: a \rightarrow \sigma_a$ is a homomorphism of A to the set. When σ is a monomorphism, we say that A is effective. When $A = a^G$ for an element a , we say that A is transitive. Let G' be the commutator subgroup of G . When A is transitive, $G' = \langle \sigma_a^{-1} \sigma_b | a, b \in A \rangle$, since $b = a^\rho$ with some element ρ in G and $\sigma_a^{-1} \sigma_b = \sigma_a^{-1} \rho^{-1} \sigma_a \rho \in G'$ and conversely $\sigma_a^{-1} \sigma_b^{-1} \sigma_a \sigma_b = \sigma_a^{-1} \sigma_c$ with $c = a^{\sigma_b}$. So, in this case, $G = \langle G', \sigma_a \rangle$ for any a . Also note that if A is a union of conjugacy classes in a group K and if A generates K , then $G \cong K/Z(K)$, where $Z(K)$ is the center of K .

Let A and B be pseudosymmetric sets and suppose that there exists a homomorphism f of A onto B . The inverse image $f^{-1}(b)$ for an element b in B is called a coset of f . Let $\{C_i\}$ be the set of all cosets of f . Then $\{C_i\}$ is a system of blocks of imprimitivity of the permutation group G , and if σ and ρ belong to the same coset, then $C_i^\sigma = C_i^\rho$ for every i . When $|B| > 1$ and f is not a monomorphism, we say that f is proper. A pseudosymmetric set A with $|A| > 2$ is called simple if it has no proper homomorphism. Note that if A is simple, then it is transitive. For, consider the canonical homomorphism $a \rightarrow a^G$

of A onto $B=\{a^G|a\in A\}$. Since A is simple, $|B|=1$ or the mapping is a monomorphism. In the former case, $A=a^G$ is transitive. In the latter case, $a=a^G$ for every a , i.e., G is trivial, which is impossible because $|A|>2$ implies that A has a proper homomorphism to the trivial pseudosymmetric set of two elements. The following theorem is established for a symmetric set in [2].

Theorem. *Let A be a pseudosymmetric set. If A is simple, then G' is the unique minimal normal subgroup of G . The converse is also true if A is effective and transitive.*

Proof. Suppose that A is simple. Let $K\neq 1$ be a normal subgroup of G , and B the set of all K -orbits. B is a pseudosymmetric set, and there is the canonical homomorphism $f: a\rightarrow a^K$. Since $K\neq 1$, f is not a monomorphism. Therefore, $|B|=1$, which implies that K is transitive on A . So, for any elements a and b , $a^\rho=b$ with ρ in K . Then, $\sigma_a\rho=\rho^{-1}\sigma_a\rho=\sigma_b$, and hence $\sigma_b^{-1}\sigma_a\in K$ as K is normal. Thus $G'\subset K$, which proves the first part of Theorem. Conversely, suppose that A is effective and transitive and that A is not simple. We want to show that there is a normal subgroup K such that $1\neq K\subsetneq G'$. Since A is not simple, there is a proper homomorphism f of A onto B with $|B|\geq 2$. f induces a homomorphism \bar{f} of G to $G(B)$ in a natural way: $f(a\circ b)=f(a)\circ f(b)=f(a)^{\bar{f}(\sigma_b)}$, or, more generally $f(a^\rho)=f(a)^{\bar{f}(\rho)}$. Let \bar{g} be the restriction of \bar{f} to G' . Let K be the kernel of \bar{g} . Since \bar{f} is not a monomorphism, there exist a and b such that $a\neq b$ and $f(a)=f(b)$. Then, $\bar{f}(\sigma_a)=\bar{f}(\sigma_b)$ and hence $\bar{g}(\sigma_a^{-1}\sigma_b)=1$. Thus $K\neq 1$. Note that $\sigma_a^{-1}\sigma_b\neq 1$ and $\in G'$ as A is effective and transitive. On the other hand, let $f(c)$ and $f(d)$ be two elements in B . Since A is transitive, $c^\tau=d$ with some τ in G . We may assume that τ is in G' . For, $G=\langle G', \sigma_c \rangle = \sum \sigma_c^i G'$ and we can replace τ by $\sigma_c^i\tau$. Then, $f(c)^{\bar{g}(\tau)}=f(c^\tau)=f(d)\neq f(c)$. Therefore, $\bar{g}(\tau)\neq 1$ and τ is not in K . $K\subsetneq G'$.

Corollary. *Let A be an effective and transitive pseudosymmetric set. Suppose $G'=G$. Then A is simple if and only if G is a simple group.*

In the following, we show some examples of simple pseudosymmetric sets. Although it is well known that the corresponding groups G are simple, we shall show the simplicity of A directly, thus giving a new proof of the simplicity of G (once we show $G'=G$).

EXAMPLE 1. We consider the alternating group A_n . ($n\geq 5$) Let A be the conjugacy class of the 3-cycle $(1, 2, 3)$. A consists of all 3-cycles and generates A_n . So, $G\cong A_n/Z(A_n)=A_n$. We shall show that A is simple. Let $\{C_i\}$ be the set of all cosets of a homomorphism of A to a pseudosymmetric set B . Assume that $|C_i|\geq 2$. Note that all C_i have the same cardinality as A is transitive. Let C be one of C_i .

(1) Suppose that $(1, 2, 3)$ and $(1, 2, 4)$ are both contained in C . It is not hard to check that the pseudosymmetric set C contains all (i, j, k) , $1 \leq i, j, k \leq 4$. Since $(1, 2, 3)^{\sigma} = (1, 2, 4) \in C$ where $\sigma = (3, 4, 5)$, we see that $(1, 2, 4)^{\sigma} = (1, 2, 5)$ is also contained in C due to the definition of a block of imprimitivity of a permutation group. So, C contains all (i, j, k) , $1 \leq i, j, k \leq 5$ by the above argument. Repeating this process, we have $C = A$.

(2) Suppose that $(1, 2, 3)$ and $(1, 4, 5) \in C$. Then, $(1, 2, 3)^{\sigma} = (4, 2, 3)$ is contained in C , where $\sigma = (1, 4, 5)$. Thus, by (1), $C = A$.

(3) Suppose that $(1, 2, 3)$ and $(2, 1, 3) \in C$. Let $\sigma = (1, 2, 3)$ and $\tau = (2, 1, 3)$. Then both $(2, 4, 5)^{\sigma} = (3, 4, 5)$ and $(2, 4, 5)^{\tau} = (1, 4, 5)$ are contained in $C' = C_i^{\sigma} = C_j^{\tau}$, where C_i contains $(2, 4, 5)$. Then $C' = A$ by (1).

(4) Suppose that $(1, 2, 3)$ and $(2, 1, 4) \in C$. Let $\sigma = (1, 2, 3)$ and $\tau = (2, 1, 4)$. Then both $(2, 3, 5)^{\sigma} = (3, 1, 5)$ and $(2, 3, 5)^{\tau} = (1, 3, 5)$ are contained in a coset C' , and $C' = A$ by (3).

(5) Suppose that $n \geq 6$ and that $(1, 2, 3)$ and $(4, 5, 6) \in C$. Let $\sigma = (1, 2, 3)$ and $\tau = (4, 5, 6)$. Then both $(2, 3, 4)^{\sigma} = (3, 1, 4)$ and $(2, 3, 4)^{\tau} = (2, 3, 5)$ are contained in a coset C' , and $C' = A$ by (2).

From the above, we can conclude that A is simple.

EXAMPLE 2 (For Examples 2 & 3, see [1]). Let V be a vector space over a field K . Let $\tau_{a,f}$ be a transvection: $x \rightarrow x - f(x)a$, where $a \neq 0$ and f is a non-zero linear function such that $f(a) = 0$. A pseudosymmetric set A is defined as follows. When $\dim V \geq 3$, let A be the set of all transvections. It is known in this case that A is a conjugacy class in $SL(V)$ and generates $SL(V)$. When $\dim V = 2$, let τ be a transvection represented by a matrix $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ with respect to some basis of V , and let A be the conjugacy class of τ in $SL(V)$. We show that A generates $SL(V)$ in this case. Then A is seen to be transitive. For $\lambda \neq 0$, we have

$$\begin{bmatrix} \lambda^{-1} & 0 \\ 0 & \lambda \end{bmatrix}^{-1} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \lambda^{-1} & 0 \\ 0 & \lambda \end{bmatrix} = \begin{bmatrix} 1 & \lambda^2 \\ 0 & 1 \end{bmatrix} \in A.$$

If $\text{char}(K) \neq 2$ or if K is finite, then $\mu = \alpha^2 - \beta^2 - \gamma^2$ has solutions α, β and γ in K for any given μ as we see easily. Then,

$$\begin{bmatrix} 1 & \alpha^2 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & \beta^2 \\ 0 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 1 & \gamma^2 \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & \mu \\ 0 & 1 \end{bmatrix} \in \langle A \rangle.$$

Then, also,

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}^{-1} \begin{bmatrix} 1 & \mu \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 0 \\ -\mu & 1 \end{bmatrix} \in \langle A \rangle.$$

We see that $\langle A \rangle = SL(V)$ in this case. Next, assume that $\text{char}(K) = 2$ and K

is infinite. Then,

$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix}^{-1} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \in A.$$

Hence,

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \in \langle A \rangle.$$

For any non-zero μ ,

$$\begin{bmatrix} \mu & 0 \\ 0 & \mu^{-1} \end{bmatrix}^{-1} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} \mu & 0 \\ 0 & \mu^{-1} \end{bmatrix} = \begin{bmatrix} 1 & \mu^{-2} \\ \mu^2 & 0 \end{bmatrix} \in \langle A \rangle.$$

Hence,

$$\begin{bmatrix} 1 & \mu^{-2} \\ \mu^2 & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} \mu^{-2} & 1 \\ 0 & \mu^2 \end{bmatrix} \in \langle A \rangle.$$

Therefore,

$$\begin{bmatrix} \mu^{-2} & 1 \\ 0 & \mu^2 \end{bmatrix} \begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix} \begin{bmatrix} \mu^{-2} & 1 \\ 0 & \mu^2 \end{bmatrix}^{-1} \begin{bmatrix} 1 & \lambda \\ 0 & 1 \end{bmatrix}^{-1} = \begin{bmatrix} 1 & \lambda(\mu^{-4}-1) \\ 0 & 1 \end{bmatrix} \in \langle A \rangle.$$

Since K is infinite, $\lambda(\mu^{-4}-1)$ can be any non-zero element in K . As in the first case, we can show $\langle A \rangle = SL(V)$. So, we can also conclude that for any $\langle a \rangle$ there exists $c \in \langle a \rangle$ and f such that $\tau_{c,f} \in A$ if $\dim V=2$.

Now we are in a position to show that A is simple. Let $\{C_i\}$ be the set of all cosets of a homomorphism where $|C_i| \geq 2$. First, we prove that there is a coset C which contains two elements $\tau_{a,f}$ and $\tau_{b,g}$ such that $f(b) \neq 0$. For it, let σ and ρ be two elements in some coset. There is a hyperplane H such that $H^\sigma \neq H^\rho$, since otherwise $\sigma\rho^{-1}$ fixes every line and hence $\sigma=\rho$ as both σ and ρ are transvections. So, we can choose an element c in H such that $c^\sigma \notin H^\rho$. Let h be a linear function defining H ; $H=H_h=\{x \mid h(x)=0\}$. Let $a=c^\rho$, $b=c^\sigma$, $f=h^\rho$ and $g=h^\sigma$. Let $C=C_i^\sigma$, where C_i is a coset containing $\tau_{c,h}$. Note that we can make $\tau_{c,h} \in A$ if $\dim V=2$ by the above remark. Note also $C_i^\sigma=C_i^\rho$ as σ and ρ belong to the same coset. C satisfies the above condition. For, $f(b)=h^\rho(b)=h(b^{\rho^{-1}}) \neq 0$ as $b \notin H^\rho$. C contains $\tau_{c,h}^\rho=\tau_{a,f}$ and $\tau_{c,h}^\sigma=\tau_{b,g}$. Next, we prove that, for every line $\langle d \rangle$, C contains an element $\tau_{d',*}$ such that $d' \in \langle d \rangle$. For it, we may assume that $d \notin \langle a \rangle \cup \langle b \rangle$. If $d \notin H_f$, we can choose φ is $SL(V)$ such that φ is the identity on H_f and that $b^\varphi \in \langle d \rangle$. Note that $f(b) \neq 0$ implies $b \notin H_f$. φ fixes $\tau_{a,f}$ as it is a unimodular linear transformation acting identically on H_f . Therefore, $C^\varphi=C$. Since $\tau_{b,g}^\varphi \in C$, we can let $d'=b^\varphi$. If $d \in H_f$ and $d \notin H_g$, we can choose ξ in $SL(V)$ such that ξ is the identity on H_g and that $d^\xi \notin H_f$. Since ξ fixes $\tau_{b,g}$ this time, $C^\xi=C$. From the above, we can find d_0 such that $\tau_{d_0,*} \in C$ and that $d_0 \in \langle d^\xi \rangle$. So, in

this case, let $d'=d_a^{\xi^{-1}}$. Finally, suppose that $d \in H_f \cap H_g$. In this case, we can choose ξ in $SL(V)$ such that ξ induces a unimodular linear transformation on H_f , $a^\xi = a$ and $d^\xi \notin H_g$. It follows that $\tau_{a,f}^\xi = \tau_{a,f}$ since $\xi \in SL(V)$ and its restriction on H_f is a unimodular linear transformation of H_f . Hence, $C^\xi = C$. Then, as above, we can show the existence of a required element d' . It is now easy to conclude that $C = A$. For, let $\tau_{d',*}$ be given as above. $\tau_{d,f}$ and $\tau_{d',*}$ are commutative as $d' \in \langle d \rangle$. For every d , $\tau_{d,f}$ leaves C fixed. Since A is transitive, this implies $C = A$. We have proven that A is simple.

EXAMPLE 3. Suppose that V has a non-singular symplectic metric (x, y) . Let $\sigma_{a,\lambda}$ be a symplectic transvection: $x \mapsto x + \lambda(x, a)a$, where a is a non-zero element in V and λ is a non-zero element in K . We define a pseudosymmetric set A by $A = \{\sigma_{a,1} \mid a \in V^* = V - \{0\}\}$. We want to show that A generates $Sp(V)$ and that A is simple. In order to show that A generates $Sp(V)$, first suppose that $\text{char}(K) \neq 2$ or that K is finite. Since $\sigma_{\lambda a,1} = \sigma_{a,1}^2$ and $\sigma_{a,1}^{-1} = \sigma_{a,-1}$, we can show that $\langle A \rangle$ contains all $\sigma_{a,\mu}$ as in Example 2. Thus, $\langle A \rangle = Sp(V)$ in this case, since $\sigma_{a,\mu}$ generate $Sp(V)$. Next, suppose that $\text{char}(K) = 2$ and that K is infinite. We reduce our problem to the case of $\dim 2$ and solve it. To show $\sigma_{a,\lambda} \in \langle A \rangle$, consider $V' = \langle a, a' \rangle$, a hyperbolic plane. Let $V = V' \oplus V''$ be an orthogonal decomposition. Then $\sigma_{a,\lambda} = \sigma'_{a,\lambda} \oplus 1_{V''}$, where $\sigma'_{a,\lambda}$ is a symplectic transvection on V' . Now, $Sp(V') = SL(V') = PSL(V')$ because K is infinite and $\text{char}(K) = 2$. (See [1], p. 174.) If we let $A' = \{\sigma'_{c,1} \mid c \in V'^*\}$, then $\langle A' \rangle$ is a normal subgroup of $SL(V')$ and hence $\langle A' \rangle = Sp(V')$, since the latter is a simple group by the above. This implies that $\sigma_{a,\lambda} \in \langle A' \rangle \oplus 1_{V''} \subset \langle A \rangle$. Thus, A generates $Sp(V)$.

Before we show the simplicity of A , we show that A is transitive. V^* is clearly a pseudosymmetric set by $ab = a^{\sigma_b,1}$. A mapping $f: a \mapsto \sigma_{a,1}$ is a homomorphism of V^* onto A , and $f^{-1}(\sigma_{a,1}) = \{\pm a\}$. It suffices to show that V^* is transitive. Fix a , and let x be an arbitrary element in V^* . If $(a, x) \neq 0$, then $a+x = a^{\sigma_x, \lambda}$, where $\lambda = (a, x)^{-1}$. Therefore, $a+x$ belongs to the G^* -orbit of a where $G^* = G(V^*)$. Then x belongs to the G^* -orbit of $a+x$, which is equal to the G^* -orbit of a , since $(a+x, -a) \neq 0$ and $(a+x) + (-a) = x$. If $(a, x) = 0$, we can choose y such that $(a, y) \neq 0$ and $(y, x) \neq 0$. For, let $V' = \langle a, a' \rangle$ as before. If $(a', x) \neq 0$, let $y = a'$. If $(a', x) = 0$, let $\langle x, x' \rangle$ be a hyperbolic plane which is orthogonal to V' . Let $y = a' + x'$. Thus, x is in the G^* -orbit of y , which is equal to the G^* -orbit of a . We have shown that A is transitive. Now we are in a position to prove that A is simple. Let $\{C_i\}$ be the set of cosets as before, where $|C_i| \geq 2$. Let $C_i^* = f^{-1}(C_i)$. Let C^* be one of C_i^* .

(1) Suppose that C^* contains a and b such that $(a, b) \neq 0$. Since $C^{\sigma_b, \lambda} = C^*$ for any λ as $\sigma_{b,\lambda}$ fixes b , C^* contains all $a + \mu b$. So, more generally, C^*

contains $\alpha a + \beta b$ for any α and β . For any c in V^* , $(\alpha a + \beta b, c) = 0$ for some $\alpha a + \beta b$ in V^* , which implies that $\sigma_{c,\lambda}$ leaves $\alpha a + \beta b$ fixed. Therefore, C^* is left fixed by any $\sigma_{c,\lambda}$. Since V^* is transitive, this implies $C^* = V^*$, or $C = A$. A is simple in this case.

(2) Suppose that C^* contains a and b such that $(a, b) = 0$ and $a \notin \langle b \rangle$. Then, we can express $b = \alpha a + d$ with a non-zero element d in V'' , where $V = V' \oplus V''$ (orthogonal), since $(a, b) = 0$ and $a \notin \langle b \rangle$. Now, let c be an element in V'' such that $(d, c) \neq 0$. Since $\sigma_{c,\lambda}$ fixes a , C^* is left fixed by $\sigma_{c,\lambda}$. Then, $b^{\sigma_{c,\lambda}} \in C^*$, which implies that $b + c \in C^*$. Since $(b, b + c) \neq 0$, we have $C = A$ by (1).

(3) Suppose that C^* contains a and αa , where $\alpha \neq \pm 1$. Let b be an element such that $(a, b) \neq 0$. Let C_i^* be a coset which contains b . Then, $C_i^{*\sigma_{a,1}} = C_i^{*\sigma_{\alpha a,1}}$, which contains $d = b^{\sigma_{a,1}} = b + (b, a)a$ and $e = b^{\sigma_{\alpha a,1}} = b + \alpha^2(b, a)a$. Since $d \notin \langle e \rangle$, we can apply (1) or (2) and get that $\{C_i\} = \{A\}$, or A is simple.

REMARK. If we consider $PSL(V)$ and $PSp(V)$, the “effective” condition is satisfied.

References

- [1] E. Artin: Geometric algebra, Interscience, New York, 1961.
- [2] H. Nagao: *A remark on simple symmetric sets*, Osaka J. Math. **16** (1979), 349–352.

Department of Mathematics
University of Hawaii
Honolulu, Hawaii 96822
U.S.A.