Can. J. Math., Vol. XXIII, No. 4, 1971, pp. 679–685

ON PRIMITIVE SOLVABLE LINEAR GROUPS

C. R. B. WRIGHT

1. Introduction. Let V be a vector space over the field K. A group G of K-linear transformations of V onto itself is *primitive* in case no proper non-trivial subspace of V is G-invariant and V cannot be written as a direct sum of proper subspaces permuted among themselves by G. Equivalently, G is primitive on V in case G is irreducible and is not induced from a proper subgroup.

Suprunenko showed [**3**, Theorem 12, p. 28] that the n-dimensional general linear group $\mathrm{GL}(n, K)$ has a solvable primitive subgroup only if

(1) there is a divisor, m, of n such that K has an extension field of degree m containing a primitive p-th root of 1 for each prime p dividing n/m.

The main result of this note is the converse fact.

THEOREM 1. *If the field K and positive integer n satisfy* (1), *then* $\mathrm{GL}(n, K)$ *contains a solvable primitive subgroup.*

In [**3**, Chapter 1, p. 28], Suprunenko states that in Chapter 2 he will prove Theorem 1 in case K is algebraically closed and n is odd. The argument given in [**3**, Section II.4] is somewhat mysterious, but does apparently lead to the result claimed. The restriction on n is never specifically imposed, although it is tacitly used in the construction of the group Γ [**3**, p. 48], since for even n it is not enough to find symplectic groups; they must be orthogonal as well. It seems easier to produce a direct argument for general K and n than to try to disentangle the cross references and notation of [**3**] and build upon the special case it handles.

The outline of this argument is based on the treatment in [**3**] and consists of dealing with one prime-power factor of n at a time, using facts about finite symplectic and orthogonal groups and then pasting the results for the factors together. The prime 2 causes a certain amount of trouble at various stages and must sometimes be handled separately. (It appears that Suprunenko, in considering only symplectic groups, has overlooked one of the points at which 2 behaves differently from the odd primes.)

Notation is fairly standard. If K is a field, K^n is the direct sum of n copies of K and $\mathrm{M}(n, K)$ is the ring of $n \times n$ matrices over K. If $S \subseteq \mathrm{M}(n, K)$, then $[S]$ is the subspace of $\mathrm{M}(n, K)$ spanned by S. For every choice of n and K we denote the centre of $\mathrm{GL}(n, K)$ by Z and the identity by I.

Received November 17, 1970 and in revised form, April 1, 1971.

2. Some finite solvable irreducible linear groups. The proof of Theorem 3 in the next section hinges upon the existence of solvable irreducible subgroups of the symplectic groups $\mathrm{Sp}_{2n}(q)$ for q an odd prime-power and certain orthogonal groups $\mathrm{O}_{2n}(q)$ for q a power of 2. In this section we establish this existence by a method which handles both cases at once. For q odd or a power of 4 there is a somewhat more transparent construction (see [**3**, p. 48]) which consists of taking the wreath product of a 2-dimensional group with an n-cycle. The construction below, however, has the virtue of providing groups for all cases. (For background on symplectic and orthogonal groups see [**2**, sections II.9 and II.10].)

THEOREM 2. *Let q be a prime-power and let n be a natural number. If $q^n \geqq 3$, then* $\mathrm{GL}(2n, q)$ *contains an irreducible solvable subgroup which is symplectic if q is odd and preserves the form $x_1y_1 + \ldots + x_ny_n$ if q is even. If $q^n \geqq 5$, the subgroup can be chosen to be metacyclic.*

Proof. Since $\mathrm{Sp}_2(3) = \mathrm{SL}(2, 3)$, a solvable group, the result is correct if $q^n = 3$. If $n = 1$ and $q = 4$, a subgroup of order 5 in $\mathrm{SL}(2, 4)$ is irreducible and leaves x_1y_1 invariant.

Suppose that $q = n = 2$. Let

$$B = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}, \quad N = \begin{bmatrix} 1 & 0 & 0 & 1 \\ 0 & 1 & 1 & 0 \\ 0 & 1 & 0 & 0 \\ 1 & 0 & 0 & 0 \end{bmatrix}, \quad J = \begin{bmatrix} 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 0 \end{bmatrix}$$

in $\mathrm{GL}(4, 2)$. One can check that $J^2 = I$, $B^{-1}NB = N^{-1}$, $JBJ = B^{-1}$ and $JNJ = N^{-1}$, and that the group $\langle B, N, J\rangle$ is an irreducible subgroup of $\mathrm{GL}(4, 2)$ of order 36 leaving $x_1y_1 + x_2y_2$ invariant.

From now on suppose that $q^n \geqq 5$. Let V be $\mathrm{GF}(q^n)$ viewed as an n-dimensional space over $\mathrm{GF}(q)$. Let Z be a Singer cycle of $\mathrm{GF}(q^n)$ over $\mathrm{GF}(q)$ (see [**2**, p. 187]). For X in $\mathrm{GL}(n, q)$ let $X^* = (X^t)^{-1}$. Let

$$W = \begin{bmatrix} Z & 0 \\ 0 & Z^* \end{bmatrix}$$

in $\mathrm{GL}(2n, q)$ acting on $V \oplus V$. One can check that

$$W^t \cdot \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix} \cdot W = \begin{bmatrix} 0 & I \\ -I & 0 \end{bmatrix},$$

so that W is symplectic, and

$$W \cdot \begin{bmatrix} X \\ Y \end{bmatrix} = \begin{bmatrix} ZX \\ Z^* Y \end{bmatrix},$$

so that, since $(Z^*Y)^t \cdot (ZX) = Y^t \cdot X$, W preserves $x_1y_1 + \ldots + x_ny_n$.

Now Z has order $q^n - 1$ and acts irreducibly on V. Since Z and its transpose Z^t have the same invariant factor, $Z^t = P^{-1}ZP$ for some P in $\mathrm{GL}(n, q)$. Let

$$R = \begin{bmatrix} 0 & P \\ -P^* & 0 \end{bmatrix}.$$

A routine check shows that $R^{-1}WR = W^{-1}$ and that R is symplectic and sends $x_1y_1 + \ldots + x_ny_n$ to its negative. Let $G = \langle W, R\rangle$. Then G is metacyclic and is symplectic or orthogonal accordingly as q is odd or even.

Suppose that $Z^{-1} = Q^{-1}ZQ$ for some Q in $\mathrm{GL}(n, q)$. Then

$$Q \in N(\langle Z\rangle) = \langle Z\rangle \cdot \langle B\rangle,$$

where $B^{-1}ZB = Z^q$ (see [**2**, p. 187]). So $Z^{-1} = B^{-i}ZB^i$ for some i with $0 \leqq i < n$, and thus $q^n - 1$, the order of Z, divides $q^i + 1$. Easy calculation shows that $q^n \leqq 4$, contrary to assumption. Hence Z^{-1} and Z are not conjugate in $\mathrm{GL}(n, q)$, so that Z^* and Z are not either.

Viewed as a $\langle W\rangle$-module, $V \oplus V$ has the obvious irreducible submodules $V \oplus 0$ and $0 \oplus V$, which we have just shown are inequivalent. By the Jordan-Hölder Theorem these must be the only two W-submodules. Since R interchanges them, G acts irreducibly on $V \oplus V$, as desired.

3. The case $n = p^e$. This section uses the groups just constructed to help produce primitive solvable subgroups of $\mathrm{GL}(q, K)$ for $q = p^e$ a prime-power.

THEOREM 3. *Let p be a prime and let $q = p^e$. Let K be a field which contains a primitive p-th root of 1. If $q = 2$, suppose that -1 is a sum of two squares. Then $\mathrm{GL}(q, K)$ contains solvable subgroups B and W such that*

(a) $Z < B \lhd W$,

(b) $[B] = M(q, K)$,

(c) *B/Z is a chief factor of W of order q^2,*

(d) $B = C_W(B/Z)$.

Proof. Suppose first that $q > 2$. Let ϵ be a primitive p-th root of 1 in K. Let E be the subgroup of $\mathrm{GL}(p, K)$ generated by the matrices a and b, where

$$a = \begin{bmatrix} 0 & 1 & 0 & \ldots & 0 \\ 0 & 0 & 1 & \ldots & 0 \\ & & & \cdot & \\ & & & \cdot & \\ & & & \cdot & \\ 0 & 0 & 0 & \ldots & 1 \\ 1 & 0 & 0 & \ldots & 0 \end{bmatrix} \quad \text{and} \quad b = \begin{bmatrix} 1 & & & & & 0 \\ & \epsilon & & & & \\ & & \epsilon^2 & & & \\ & & & \cdot & & \\ & 0 & & & \cdot & \\ & & & & & \epsilon^{p-1} \end{bmatrix}.$$

Then E is extraspecial of order p^3 generated by elements of order p, with $[a, b] = \epsilon I$. Let X be the Kronecker product $X = E \otimes \ldots \otimes E \leqq \mathrm{GL}(q, K)$.

https://doi.org/10.4153/CJM-1971-075-6 Published online by Cambridge University Press

Then X is extraspecial of order $p^{2e+1} = q^2 \cdot p$ with derived group $\langle \epsilon I \rangle = X \cap Z$. Let $B = XZ$. Then $[B] = [X]$.

We now show that $[X] = M(q, K)$, from which (*b*) will follow. Suppose that $0 = \sum_{i=1}^{m} x_i k_i$ is a K-dependence relation among elements $x_1, \ldots, x_m$ of X lying in different cosets of X'. Then $m \geqq 2$ and $x_1 x_2^{-1} \notin Z(X)$, so that $1 \neq [x_1 x_2^{-1}, y]$ for some y in X and hence $[x_1, y] \neq [x_2, y]$. Then

$$0 = y^{-1}\left(\sum_{i=1}^{m} x_i k_i\right) y - \sum_{i=1}^{m} x_i k_i [x_1, y]$$

yields a shorter dependence relation than the given one. It follows that $\dim_K([X]) \geqq [X : X'] = p^{2e} = q^2$, so $[X] = M(q, K)$.

Using [**2**, Sätze III.13.7 and III.13.8 and Bemerkungen 13.9], it is not hard to see that the group of automorphisms of X fixing $X \cap Z$ is isomorphic to the group of GF(p)-linear transformations of X/X' leaving invariant the bilinear form f and quadratic form g defined by

$$[x, y] = \epsilon^{f(x,y)} \quad \text{and} \quad x^p = \epsilon^{g(x)}.$$

This group is $\mathrm{Sp}_{2e}(p)$ if p is odd and is the orthogonal group of degree $2e$ leaving invariant $x_1 y_1 + \ldots + x_e y_e$ if $p = 2$. In either case, by Theorem 2, X has a solvable group G of automorphisms acting irreducibly on X/X' and centralizing X'. By linearity, G extends to a group (which we also call G) of K-algebra automorphisms of $[X]$.

Now $[X] = [B] = M(q, K)$, a central simple K-algebra. By [**1**, Theorem 7.2c], every automorphism of $[B]$ is inner. Hence G is a group of inner automorphisms of $M(q, K)$ normalizing B and acting irreducibly on B/Z. Let $H/Z = G$, with $H \leqq \mathrm{GL}(q, K)$, and let $W = HB$. Then B/Z is a chief factor of W of order q^2, as claimed in (c), and W is solvable. Moreover, $C_W(B/Z) = B \cdot C_H(B/Z) = B \cdot Z = B$. This completes the proof in case $q > 2$.

Now suppose that $q = 2$ and that $-1 = \alpha^2 + \beta^2$ for some α and β in K. Let

$$a = \begin{bmatrix} \alpha & \beta \\ \beta & -\alpha \end{bmatrix} \qquad b = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix},$$

$$x = \begin{bmatrix} \alpha & \beta + 1 \\ \beta - 1 & -\alpha \end{bmatrix} \quad \text{and} \quad y = \begin{bmatrix} -\beta & \alpha + 1 \\ \alpha - 1 & \beta \end{bmatrix}.$$

Then $a^2 = b^2 = (ab)^2 = -I$, so that $\langle a, b \rangle$ is quaternion of order 8, $x^2 = -2I$, $y^2 = -2I$, $(xy)^3 = 8I$ and $x^{-1}ax = b$, $x^{-1}bx = -a$, $y^{-1}ax = -a$, $y^{-1}bx = ab$. Let $B = \langle a, b \rangle Z$ and $W = B\langle x, y \rangle$. Then $W/Z \cong S_4$ and the conditions (a)–(d) are easy to verify. The proof of Theorem 3 is complete.

Some condition on K is needed if $q = 2$. To see this, let K be an arbitrary ordered field and suppose that G is a primitive solvable subgroup of GL$(2, K)$

for which Z is a maximal abelian normal subgroup. Let B/Z be a chief factor of G. (Since G/Z is finite, such a factor certainly exists.) It is not hard to see that $|B/Z|$ divides 4, and since B is non-abelian, B/Z is a 4-group. Say $B = \langle a, b\rangle Z$ with $a^2 = \alpha I$, $b^2 = \beta I$ and $(ab)^2 = \gamma I$, with α, β, γ in K. Since $[a, b] \neq I$, $[a, b] = -I$, and $\gamma = -\alpha\beta$. At least one of α, β and γ is negative. Unless all three are, B/Z contains a proper normal subgroup of G/Z. Thus each of α, β and γ is negative. Easy calculation shows that for some x, y, z, u, v and w in K

$$a = \begin{bmatrix} x & y \\ z & -x \end{bmatrix} \quad \text{and} \quad b = \begin{bmatrix} u & v \\ w & -u \end{bmatrix},$$

with $x^2 + yz = \alpha$, $u^2 + vw = \beta$. Then

$$ab = \begin{bmatrix} xu + yw & * \\ * & zv + xu \end{bmatrix},$$

and so $xu + yw = -zv - xu$. Then

$$\begin{aligned} 0 &= 2xuyv + y^2vw + yzv^2 \\ &= 2xuyv + y^2(\beta - u^2) + v^2(\alpha - x^2) \\ &= -(yu - vx)^2 + y^2\beta + v^2\alpha, \end{aligned}$$

a non-positive element since α and β are negative. Thus $v = y = (yu - vx) = 0$, a contradiction to $x^2 + yz = \alpha < 0$.

4. General n and the proof of Theorem 1. This section puts together primitive subgroups of $\mathrm{GL}(q, K)$ for the prime-powers q dividing n to get a primitive subgroup of $\mathrm{GL}(n, K)$ which is the direct product of the pieces.

It is not true in general that if G and H are primitive subgroups of $\mathrm{GL}(n, K)$ and $\mathrm{GL}(m, K)$, respectively, then $G \otimes H$ is a primitive subgroup of $\mathrm{GL}(nm, K)$. For example, if K is the real field and both G and H are the multiplicative complex field viewed as embedded in $\mathrm{GL}(2, K)$, then G and H are primitive (see Theorem 6) but $G \otimes H$ is not irreducible, let alone primitive. So the proof of Theorem 4 must make use not only of the primitivity of the factors but also of some of the special properties noted in Theorem 3.

THEOREM 4. *Let $q_1, \ldots, q_t$ be powers of distinct primes and let $n = q_1 \ldots q_t$. Suppose that for $i = 1, \ldots, t$, $\mathrm{GL}(q_i, K)$ contains subgroups B_i and W_i satisfying*

(a) $Z < B_i \lhd W_i$,

(b) $[B_i] = M(q_i, K)$, *and*

(c) B_i/Z *is a chief factor of* W_i *of order* q_i^2.

Then $W = W_1 \otimes \ldots \otimes W_t$ is a primitive subgroup of $\mathrm{GL}(u, K)$.

If $B_i = C_{W_i}(B_i/Z)$ for each i, then $B = C_W(B/Z)$ and Z is a maximal abelian normal subgroup of W.

Proof. Let $B = B_1 \otimes \ldots \otimes B_t$. By (a) and (b), $Z < B \lhd W$ and $[B] = M(n, K)$. Moreover, by (c), B/Z is abelian and has $B_1/Z, \ldots, B_t/Z$ as its W-chief factors. Since $q_1, \ldots, q_t$ are relatively prime, by the Jordan-Hölder Theorem the only W-normal subgroups between Z and B are of form $B_i \otimes \ldots \otimes B_j$.

Let $V = K^n$ viewed naturally as a KW-module. Since $[W] = M(n, K)$, W is irreducible on V. Suppose that $V = V_1 \oplus \ldots \oplus V_k$ is a decomposition of V into blocks of imprimitivity for W with $k \geqq 2$. Let Y be the kernel of the permutation representation of W on the set of blocks. Then $Z \leqq B \cap Y < W$. Since $V = BV_1$, B is transitive. Thus $B/B \cap Y$ is a transitive abelian group and so $[B : B \cap Y] = k$. But $[B : B \cap Y]$ is a product of factors q_i^2, by the paragraph above. Since $n = k \cdot \dim V_1$ and n is not divisible by q_i^2, we have a contradiction. It follows that W is primitive on V.

Now suppose that $B_i = C_{W_i}(B_i/Z)$ for each i. Then

$$C_W(B/Z) = C_{W_1}(B_1/Z) \otimes \ldots \otimes C_{W_t}(B_t/Z) = B.$$

If U is an abelian normal subgroup of W with $Z \leqq U$, then since each non-trivial group $B_i \otimes \ldots \otimes B_j$ is non-abelian, $U \cap B = Z$ and

$$U \leqq C_W(B/Z) = B,$$

so $U = Z$.

THEOREM 5. *Let n be a positive integer. Suppose that the field K contains a primitive p-th root of 1 for each prime divisor p of n and that -1 is a sum of two squares in K if $n \equiv 2 \pmod 4$. Then $\mathrm{GL}(n, K)$ contains a primitive solvable subgroup with Z as a maximal abelian normal subgroup.*

Proof. This follows from the last two theorems.

Although Theorem 1 loses its content if K is finite, Theorem 5 does not, and we get the following fact.

COROLLARY. *Let q be a prime-power and n a positive integer. Suppose that n divides some power of $q - 1$. Then $\mathrm{GL}(n, q)$ contains a primitive solvable subgroup with Z as maximal abelian normal subgroup.*

To prove Theorem 1 we need an elementary fact which seems to have been repeatedly used without mention in [**3**].

THEOREM 6. *Let K be a field and let K' be an extension of K of finite degree m. View $\mathrm{GL}(n/m, K')$ as a subgroup of $\mathrm{GL}(n, K)$. If G is a primitive subgroup of $\mathrm{GL}(n/m, K')$ which contains its centre, Z', then G is a primitive subgroup of $\mathrm{GL}(n, K)$.*

Proof. Let $V = (K')^{n/m} = K^n$. Suppose that $V = V_1 \oplus \ldots \oplus V_t$ is a decomposition into K-subspaces permuted by G. Then Z' also permutes $V_1, \ldots, V_t$, and for each s, $K'V_s$ has the form $V_i \oplus \ldots \oplus V_j$. Since the K'-subspaces $K'V_s$ are permuted by G and G acts primitively on V, $V = K'V_1$.

For $0 \neq a \in K'$, $aV_1 \in \{V_1, \ldots, V_t\}$. Thus

$$V = K'V_1 = \sum_{a \in K'} aV_1 = \bigoplus_{i=1}^{t} a_i V_1$$

for some $a_1, \ldots, a_t$ independent in K' over K, with $a_1 = 1$. Let

$$b = a_1 + \ldots + a_t.$$

Then $b \neq 0$, and $bV_1 = a_j V_1$ for some j. Hence,

$$(b - a_j)V_1 \subseteq a_j V_1 \cap \sum_{i \neq j} a_i V_1 = 0,$$

and so $b = a_j$ and $t = 1$, as desired.

We can now prove Theorem 1.

Proof of Theorem 1. By Theorem 6 we need only find a divisor, m, of n and an extension K' of degree m over K such that $\mathrm{GL}(n/m, K')$ contains a primitive solvable group. By hypothesis there exist m and K' such that K' contains a primitive p-th root of 1 for each prime p dividing n/m. By Theorem 5, $\mathrm{GL}(n/m, K')$ contains a primitive solvable group except perhaps if $n/m \equiv 2 \pmod 4$ and -1 is not a sum of two squares in K'. But in that case K' has an extension K'' of degree 2 obtained by adjoining a root of $x^2 + 1$, and $\mathrm{GL}(n/2m, K'')$ contains a primitive solvable group, as desired.

As a final note, the primitive groups produced above are absolutely irreducible. This follows from the fact that they are generated by certain fixed finite sets of matrices in a finite extension of the prime field of K. If K' is an extension of K and G is one of our primitive subgroups of $\mathrm{GL}(n, K)$, then G is an irreducible subgroup of $\mathrm{GL}(n, K')$ and, moreover, $G \cdot Z'$ is primitive.

References

1. E. Artin, C. J. Nesbitt and R. M. Thrall, *Rings with minimum condition* (University of Michigan Press, Ann Arbor, 1946).
2. B. Huppert, *Endliche Gruppen* I (Springer Verlag, Berlin-Heidelberg-New York, 1967).
3. D. Suprunenko, *Soluble and nilpotent linear groups*, Translations of Mathematical Monographs No. 9 (Amer. Math. Soc., Providence, 1963).

University of Oregon,
Eugene, Oregon