# GENERATING REFLECTIONS FOR $U(2, p^{2n})$. II, $p=2$

D. W. Crowe

(received October 17, 1963)

1. Introduction. It is known [4] that the finite two-dimensional unitary group $U(2, p^{2n})$ is generated by two reflections if $p \neq 2$. The present note completes that result by giving two generating reflections for $U(2, 2^{2n})$, $n > 1$. As in [4] this implies that the points of the "unit circle" $x\bar{x} + y\bar{y} = 1$ in the unitary plane over $GF(2^{2n})$, $n > 1$, are the vertices of a "regular unitary polygon" whose group of automorphisms is $U(2, 2^{2n})$.

The final section gives abstract definitions for the particular groups $U(2, 2^4)$ and $U(2, 5^2)$ in terms of their generating reflections.

The terminology is that of [4].

2. The generating reflections. As in [4] we write $q = 2^n$ and put $\delta = \lambda^{q-1}$, where $\lambda$ is a generator of the multiplicative group $GF^*(q^2)$ of $GF(q^2)$. For each $x \in GF(q^2)$, $\bar{x} = x^q$ by definition, so that $\delta\bar{\delta} = 1$. An element $r$ of $GF(q^2)$ is called real if $r = \bar{r}$. The real elements constitute a subfield $GF(q)$ of $GF(q^2)$. Since there are $q$ real elements in $GF(q^2)$ there are $q^2$ distinct elements of the form $a + b\delta$, $a, b$ real. Thus each element $x \in GF(q^2)$ has a unique representation $x = a + b\delta$, where $a$ and $b$ are real. In fact, by considering $x + \bar{x}$ and $x\delta + \overline{x\delta}$ it is found that

Canad. Math. Bull. vol. 7, no. 2, April 1964



https://doi.org/10.4153/CMB-1964-019-0 Published online by Cambridge University Press

$$a = (x\bar{\delta} + \bar{x}\delta)(\delta + \bar{\delta})^{-1},$$

$$b = (x + \bar{x})(\delta + \bar{\delta})^{-1}.$$

By analogy with [4] we hope to find two generating unitary reflections $R = \begin{pmatrix} x & y \\ \bar{y}\delta & \bar{x}\delta \end{pmatrix}$ and $S = \begin{pmatrix} 1 & 0 \\ 0 & \delta \end{pmatrix}$ each having characteristic roots $1, \delta$. In particular $x + \bar{x}\delta = 1 + \delta$. If $x = a + b\delta$ this reduces to $(a + b)(1 + \delta) = 1 + \delta$; hence $a + b = 1$. That is, the solutions to $x + \bar{x}\delta = 1 + \delta$ are all of the form $a + (a+1)\delta$, where $a$ is real. The only choice of $y$ which satisfies $x\bar{x} + y\bar{y} = 1$ (so that $R$ is unitary) and gives powers of $R$ analogous to those of [4] is $y = c + c\delta$, where $c = a + \sqrt{a}$. (In fact, to prove this one needs only to consider $R^2$.) It is readily verified by induction that for such a choice of $x$ and $y$,

$$R^k = \begin{pmatrix} x_k & y_k \\ y_k & u_k \end{pmatrix},$$

where $x_k = a + (a+1)\delta^k$, $y_k = c + c\delta^k$, and $u_k = a + 1 + a\delta^k$. $(k = 1, \ldots, q+1)$.

The symmetry of $R$ suggests that a suitable choice of $m$ may make the diagonal entries $x_1$ and $u_1\delta^{2m}$ of $S^m R S^m$ equal, and hence make $(S^m R S^m)^2$ scalar. Equating these, and solving for $a$, yields

$$a = (\delta + \delta^{2m})(1 + \delta + \delta^{2m} + \delta^{2m+1})^{-1},$$

which is always real. Then $(S^m R S^m)^2 = \delta^{2m+1} I$. We also take $2m+1$ relatively prime to $q + 1$ (e.g., $2m \equiv 3 \pmod{q+1}$ if $n > 1$). This guarantees that $(S^m R S^m)^2$ generates the centre (i.e., the cyclic group of scalar matrices $\delta^i I$, $i = 1, \ldots, q+1$) of $U(2, q^2)$. We write $P = S^{-(2m+1)}(S^m R S^m)^2$.

We proceed to verify that with this choice of $m$ (and hence $a$) the group $G = \{R, S\}$ generated by $R$ and $S$ has order



https://doi.org/10.4153/CMB-1964-019-0 Published online by Cambridge University Press

$|G| > q(q^2-1)(q+1)/2$. That is, the order of the subgroup $G$ of $U(2,q^2)$ is greater than half the known order of $U(2,q^2)$, so that $G \cong U(2,q^2)$. It is sufficient to verify that the matrices in $G$ have more than $q(q^2-1)/2$ distinct first rows, since left multiplication by powers of $S$ yields $q+1$ different matrices for each first row.

In fact, there are $q(q+1)^2/2$ distinct first rows in the matrices $R^k P^i S^j$ $(k = 1, \ldots, q/2;\ i,j=1,\ldots,q+1)$. For if two first entries of $R^k P^i$ are equal, say $x_k \delta^i = x_r \delta^s$, we have, on multiplying each side by its conjugate and simplifying, $\delta^k + \bar{\delta}^k = \delta^r + \bar{\delta}^r$. This can be written $(\delta^{k+r}+1)(\delta^k+\delta^r) = 0$. But $\delta^{k+r} \neq 1$ in the range considered, hence $k = r$. Thus there are $q(q+1)/2$ different first entries in rows of $R^k P^i$. Since in $R^k P^i S^j$ each first row has its second (non-zero) entry multiplied by the $q+1$ powers of $\delta$ we have the required result. It is summarized in the

THEOREM. The group $U(2,q^2)(q = 2^n, n > 1)$ is generated by the two (unitary) reflections

$$R = \begin{pmatrix} a + (a+1)\delta & c + c\delta \\ c + c\delta & a + 1 + a\delta \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & \delta \end{pmatrix}.$$

Here $\delta = \lambda^{q-1}$, $a = (\delta + \delta^{2m})(1 + \delta + \delta^{2m} + \delta^{2m+1})^{-1}$ (where $2m \equiv 3 \bmod q+1$), and $c = a + \sqrt{a}$.

We note that $U(2,2^2)$ is <u>not</u> generated by unitary reflections, for the only reflections are diagonal matrices, which generate a group of order 9, while $U(2,2^2)$ has order 18.

## 3. Defining relations for $U(2,2^4)$ and $U(2,5^2)$.

i) $U(2,2^4)$. Taking $m = 1$, so that $2m + 1 \equiv 3(\bmod 2^2 + 1)$, we have $a = \lambda^5$, where $\lambda$ generates $GF^*(2^4)$ and satisfies



https://doi.org/10.4153/CMB-1964-019-0 Published online by Cambridge University Press

$\lambda^4 \equiv \lambda + 1 \pmod 2$. (It is convenient to use the table on p. 160 of [1].) Then

$$R = \begin{pmatrix} \lambda^7 & \lambda^{14} \\ \lambda^{14} & \lambda \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & \lambda^3 \end{pmatrix}$$

generate $U(2, 2^4)$, of order 300. They satisfy

$$(1) \qquad R^5 = I, \quad RSR = SRS.$$

This is an abstract definition [2, p. 96] of the group $5[3]5$, of order 600, in which $(RS)^{30} = I$ and $(RS)^{15} \neq I$. However, in our group $(RS)^3 = (RSR)(SRS) = (SRS)^2$ is scalar, of period $5 = 2^2 + 1$, so that $(RS)^{15} = I$. Since

$$(2) \qquad R^5 = (RS)^{15} = I, \quad RSR = SRS$$

defines a group of order less than 600 it must define $U(2, 2^4)$.

ii) $U(2, 5^2)$. The group $U(2, 5^2)$ of order 720 is generated by [4, p. 501]

$$R = \frac{1}{2}\begin{pmatrix} 1+\delta & 1-\delta \\ 1-\delta & 1+\delta \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & \delta \end{pmatrix}.$$

If we take $\delta = \lambda^4$, where $\lambda$ satisfies $\lambda^2 \equiv 2\lambda + 2 \pmod 5$ [1, p. 159] then

$$R = \begin{pmatrix} \lambda^{23} & \lambda^2 \\ \lambda^2 & \lambda^{23} \end{pmatrix}, \quad S = \begin{pmatrix} 1 & 0 \\ 0 & \lambda^4 \end{pmatrix}.$$

These satisfy

$$(3) \qquad R^6 = I, \quad R^2S^2R^2S^2R^2 = S^2R^2S^2R^2S^2,$$

and

$$(4) \qquad RS = S^2R^{-2}S^{-2}R^2(S^2R^2)^{-10}.$$



https://doi.org/10.4153/CMB-1964-019-0 Published online by Cambridge University Press

To show that (3) and (4) together constitute an abstract definition of $U(2, 5^2)$ we note that the subgroup $\{T, U\}$ generated by $T = R^2$, $U = S^2$ is of order $\leq 360$, since $T^3 = I$, $TUTUT = UTUTU$ is an abstract definition of the group 3[5]3 of order 360 of automorphisms of a regular complex polygon (see [2], [4]). Enumeration of the (two) cosets [3, p. 12] of $\{T, U\}$ in the group defined by (3) and (4) shows that the latter group has order $\leq 720$. Hence it is exactly $U(2, 5^2)$.

## REFERENCES


1. A. A. Albert, Fundamental concepts of higher algebra, Chicago, 1956.

2. H. S. M. Coxeter, The symmetry groups of the regular complex polygons, Arch. der Math. 13 (1962), 86-97.

3. H. S. M. Coxeter and W. O. J. Moser, Generators and relations for discrete groups, Berlin-Gottingen-Heidelberg, 1957.

4. D. W. Crowe, Generating reflections for $U(2, p^{2n})$, Proc. Amer. Math. Soc. 13 (1962), 500-502.

5. G. C. Shephard, Regular complex polytopes, Proc. Lond. Math. Soc. (3) 2 (1952), 82-97.


---


This paper was prepared while the author was supported, in part, by N. S. F. Contract 86-5036.





https://doi.org/10.4153/CMB-1964-019-0 Published online by Cambridge University Press