BULLETIN 13 (1), 1970

THE GROUP OF THE QUADRATIC RESIDUE TOURNAMENT

BY
MYRON GOLDBERG

1. **Introduction.** A *tournament* T_n is a set of n *nodes* $a_1, a_2, \ldots, a_n$ such that every pair (a_i, a_j) of distinct nodes is joined by exactly one of the oriented *edges* $\overrightarrow{a_i a_j}$ or $\overrightarrow{a_j a_i}$. If $\overrightarrow{a_i a_j}$ is in T_n, then we say that a_i *dominates* a_j and write $a_i \to a_j$.

The (automorphism) *group* $G(T_n)$ of a tournament T_n is the group of all permutations ϕ of the nodes of T_n such that $\phi(a) \to \phi(b)$ if and only if $a \to b$. It is known [9] that there exist tournaments whose group is abstractly isomorphic to a given group H if and only if H has odd order; thus all tournament groups are solvable, by the Feit-Thompson Theorem [7].

If we label $q=p^n$ nodes with the elements of the Galois field $GF(q)$ and let $a_i \to a_j$ if and only if $a_j - a_i$ is a square in $GF(q)$, then the resulting configuration will be a tournament when $q \equiv 3 (\text{mod } 4)$, that is, if n is odd and $p \equiv 3 (\text{mod } 4)$; we call this tournament the (quadratic) *residue tournament* R_q. Our main object here is to determine the group $G(R_q)$ of the residue tournament R_q.

The automorphism groups of certain other specific graphs and tournaments have been considered, for example, in [1], [2], [8]. References on the groups of graphs in general and tournaments in particular may be found in [11] and [10].

2. **Preliminary results.** Finding $G(R_q)$ is equivalent to finding all permutations ϕ of the elements of $GF(q)$ such that $a_i - a_j$ is a square in $GF(q)$ if and only if $\phi(a_i) - \phi(a_j)$ is a square in $GF(q)$. In what follows we shall use the terminology and notation of Wielandt [15], and we will not repeat any of the usual definitions here.

Let a be the power of a prime, say $a=p^k$. Let $\mathscr{T}(n, a)$ be the group of all permutations of $GF(a^n)$ of the form $x \to bx^\sigma$, where b is a non-zero element of $GF(a^n)$ and σ is an automorphism of $GF(a^n)$ over $GF(a)$. Let $GL(n, a)$ denote, as usual, the general linear group of all non-singular $n \times n$ matrices with entries in $GF(a)$. In a recent paper [12], D. S. Passman has proved the following result.

THEOREM 1. *Let $a=p^k$, where p is a prime, and suppose G is a solvable subgroup of $GL(n, a)$ such that*

$$\left.\frac{a^n-1}{a^m-1}\right| \, |G| \text{ for some divisor } m \neq n \text{ of } n.$$

Then either $G \leq \mathscr{T}(n, a)$ or else $(n, a) = (2, 3), (2, 5), (2, 7), (2, 11), (2, 23), (2, 47), (4, 3)$ or $(6, 2)$.

Received by the editors April 11, 1969.

https://doi.org/10.4153/CMB-1970-010-8 Published online by Cambridge University Press

Let $\mathscr{S}(n, p)$ denote the group of all permutations of the elements of $GF(p^n)$ of the form $x \rightarrow sx^\sigma + b$, where s is a non-zero square of $GF(p^n)$, σ is an automorphism of $GF(p^n)$ and b is arbitrary in $GF(p^n)$.

3. Main result

THEOREM 2. *If* $q = p^n \equiv 3 (\mathrm{mod}\ 4)$, *then* $G(R_q) = \mathscr{S}(n, p)$.

Proof. It is clear that $\mathscr{S}(n, p) \leq G(R_q)$. The non-trivial squares and non-squares of $GF(p^n)$ are the nodes dominated by 0 and dominating 0, respectively. Consequently, $\mathscr{S}_0(n, p)$, the subgroup of $\mathscr{S}(n, p)$ fixing 0, must permute the squares among themselves and the non-squares among themselves. Since $\mathscr{S}_0(n, p)$ is transitive on the $(q-1)/2$ squares and on the $(q-1)/2$ non-squares, it follows that $G(R_q)$ is 3/2-transitive; hence it is either primitive or Frobenius ([15] p. 25). When $n > 1$, the automorphism group of $GF(p^n)$ is non-trivial (fixing $GF(p)$), so that $G(R_q)$ is not Frobenius. When $n = 1$, $G(R_q)$ is also primitive because it is transitive of prime degree.

To show that $G(R_q) \leq \mathscr{S}(n, p)$ we first consider the case $n = 1$. Then $\mathscr{S}(1, p)$ is the group of $\binom{p}{2}$ permutations of the form $x \rightarrow sx + b$, since $GF(p)$ admits only the identity automorphism. For any $\alpha \neq \beta$ in $GF(p)$, it is well known [15, p. 5] that

$$|G(R_q)| = |\alpha^{G(R_q)}| \cdot |\beta^{G_\alpha(R_q)}| \cdot |G_{\alpha\beta}(R_q)|.$$

But $|G_{\alpha\beta}| = 1$ for a solvable transitive group G of prime degree, by a result of Galois [15, p. 29]. Consequently,

$$|G(R_q)| \leq p \cdot \frac{p-1}{2} \cdot 1 = \binom{p}{2},$$

so $G(R_q) = \mathscr{S}(1, p)$; this case may also be treated as a direct consequence of a classical theorem of Burnside (see, for example, Passman [13, p. 53]) which used the theory of group characters.

Suppose now that $n > 1$. Let A be a minimal normal subgroup of the primitive, solvable group $G = G(R_q)$. Then A is an elementary abelian p-group of order p^n ([15] p. 28). Since G is primitive, G_0 is maximal. Every normal subgroup of a primitive group is transitive, so A is not contained in G_0; hence $G = AG_0$. It is not difficult to show that A is its own centralizer $C(A)$ in G since A is regular and abelian. Consequently, $G_0 \approx G/C(A)$ and this is isomorphic to a subgroup of Aut A, the automorphism group of A (see Scott [14] p. 50; Dixon [5], [6], [7] used these observations to treat other problems). Since Aut A is isomorphic to $GL(n, p)$ [14, p. 125], we may regard G_0 as being a solvable subgroup of $GL(n, p)$.

Now let $m \neq n$ be any divisor of n. Clearly $(p^n - 1)/(p^m - 1)$ is an integer, since it is the index of the multiplicative group of $GF(p^m)$ in the multiplicative group of $GF(p^n)$. Since $\mathscr{S}_0(n, p) \leq G_0$ we have

$$|G_0| = t\,|\mathscr{S}_0(n, p)| = tn\frac{p^n - 1}{2}$$

for some odd integer t, and it follows easily that $(p^n-1)/(p^m-1)$ divides $|G_0|$. Therefore, the hypotheses of Theorem 1 are satisfied (when $k=1$), and since n is odd we may conclude that $G_0 \leq \mathscr{T}(n,p)$.

Now $G_0 \neq \mathscr{T}(n,p)$ because $\mathscr{T}(n,p)$ is transitive on the non-zero elements of $GF(p^n)$. Since $\mathscr{S}_0(n,p)$ is of index 2 in $\mathscr{T}(n,p)$, it follows that $G_0 = \mathscr{S}_0(n,p)$. Hence

$$|G| = |A|\,|G_0| = p^n \cdot n \cdot \frac{p^n-1}{2} = |\mathscr{S}(n,p)|,$$

and since $\mathscr{S}(n,p) \leq G$ we have that $G = G(R_q) = \mathscr{S}(n,p)$. This completes the proof of Theorem 2.

4. An application

THEOREM 3. *Let F be a finite field, where $|F| = p^n \equiv 3 \pmod 4$, and let ϕ be a permutation of F which fixes the elements of the prime field K of F; a necessary and sufficient condition that ϕ be an automorphism of F is that $\phi(a)-\phi(b)$ is a square in F if and only if $a-b$ is a square in F.*

Proof. If ϕ is an automorphism of F then the condition is clearly necessary.

Theorem 2 says that the set of permutations of F satisfying the conditon forms the group $G = \mathscr{S}(n,p)$. But the only elements of G which fix K are of the form $x \to x^\sigma$, where σ belongs to Aut F, since all others move either 0 or 1. This completes the proof of Theorem 3.

It can be shown that Theorem 2 is actually a special case of a result due to W. M. Kantor (unpublished) which is stated without proof in the recent book by Dembowski [3, p. 98].

ACKNOWLEDGEMENT

I would like to thank Professors R. D. Bercov and S. K. Sehgal for helpful conversations concerning the material in this paper, and also the referee for suggestions to improve its presentation.

REFERENCES

1. B. Alspach, M. Goldberg and J. W. Moon, *The group of the composition of two tournaments*, Math. Magazine **41** (1968), 77–90.

2. E. F. Assmus, Jr. and H. F. Mattson, Jr., *Research to develop the algebraic theory of codes.* AFCRL-68-0478, Scientific Report, Air Force Cambridge Research Laboratory, Bedford, Mass., Sept., 1968.

3. P. Dembowski, *Finite geometries*, Springer-Verlag, 1968.

4. J. D. Dixon, *The fitting subgroup of a linear solvable group*, Australian Math. Soc. J. **7** (1967), 417–424.

5. ———, *The maximum order of the group of a tournament*, Canad. Math. Bull. **10** (1967), 503–505.

6. ———, *The solvable length of a solvable linear group*, Math. Z. **107** (1968), 151–158.

7. W. Feit and J. G. Thompson, *The solvability of groups of odd order*, Pac. J. Math. **13** (1963), 775–1029.

8. R. Frucht, *Die Gruppe des Petersenschen Graphen und des Katensysteme der regulären Polyeder*, Comment. Math. Helv. **69** (1937), 217–223.

9. J. W. Moon, *Tournaments with a given automorphism group*, Can. J. Math. **16** (1964), 485–489.

10. ———, *Topics on Tournaments*, Holt, Rinehart and Winston, 1968.

11. O. Ore, *Theory of Graphs*, A. M. S. Colloq. Pub., Providence, 1962.

12. D. S. Passman, *P-solvable doubly transitive permutation groups*, Pac. J. Math. **26** (1968). 555–577.

13. ———, *Permutation groups*, Benjamin, 1968.

14. W. R. Scott, *Group theory*, Prentice Hall, 1964.

15. H. Wielandt, *Finite permutation groups*, Academic Press, 1964.

University of Alberta,
Edmonton, Alberta