Finite Permutation Groups

Peter Müller

July 1, 2013

Contents

1 Multiply transitive groups 1
2 Jordan sets 2
3 Sharply multiply transitive groups 4
4 Transitive groups of prime degree 7
5 Primitive groups with regular cyclic subgroup 10

1 Multiply transitive groups

Theorem 1.1. Let $\Omega$ be a finite set and $G \leq \text{Sym}(\Omega)$ be 2–transitive. Let $N \unlhd G$ be a minimal normal subgroup. Then one of the following holds:

(a) $N$ is regular and elementary abelian.

(b) $N$ is primitive, simple and not abelian.

Proof. First we show that $N$ is unique. Suppose that $M$ is another minimal normal subgroup of $G$, so $N \cap M = \{e\}$ and therefore $[N, M] = \{e\}$. Since non–trivial normal subgroups of the primitive group $G$ are transitive, we obtain that both $M$ and $N$ are transitive. Together with Lemma ??? and $M \leq C_G(N)$ and $N \leq C_G(M)$ we get that both $M$ and $N$ are regular. By Theorem ???, regular normal subgroups of finite 2–transitive groups are abelian. Hence $\langle M, N \rangle$ is abelian. But transitive abelian groups are regular, which forces $M = \langle M, N \rangle = N$.

If $N$ is regular, then we are done by Theorem ???.
So from now on we assume that $N$ is not regular. Pick $\omega \in \Omega$. As $G_\omega$ permutes transitively the $N_\omega$–orbits on $\Omega \setminus \{\omega\}$, we see that these $N_\omega$–orbits all have the same length. By Wielandt’s Lemma ???, we see that $N$ is primitive or a Frobenius group.

We start to analyze the case that $N$ is a Frobenius group. Let $F^*$ be the set of fixed point free elements of $N$. By Lemma ???, $|F^*| = n - 1$, where $n = |\Omega|$. Set

$$M = \{(\alpha, \beta, f) \mid \alpha, \beta \in \Omega, f \in F^*, \beta = \alpha f\}.$$ 

Note that for given $f$, there are $n$ choices for $\alpha$, and $\beta$ then is unique. So $|M| = n(n-1)$. There is a natural action of $G$ on $M$, for if $\beta = \alpha f$ and $g \in G$, then $\beta^g = \alpha^f g = \alpha^{gg^{-1}f}g = (\alpha^g)^f g$, so $(\alpha, \beta, f) \in M$ implies $(\alpha^g, \beta^g, f^g) \in M$. By the 2–transitivity of $G$, we see that for any $\alpha \neq \beta$ there is at least one $f \in F^*$ with $(\alpha, \beta, f) \in M$. As there are $n(n-1) = |M|$ such pairs, we see that $f$ is uniquely given by the pair $\alpha, \beta$, and that the elements of $F^*$ are conjugate. Let $p$ be a prime divisor of $\Omega$, and $f \in N$ be a element of order $p$. As $f$ has either 0 or at least $p > 1$ fixed points, we conclude that $f \in F^*$. So all elements of $F^*$ have order $p$, hence $\Omega$ is a power of $p$. By Lemma ???, the Frobenius kernel $F = F^* \cup \{e\}$ then is a subgroup of $N$. Let $g \in G$. Then $F^g \leq N$, and each element $\neq e$ in $F^g$ is fixed point free, hence $F^g \subseteq F$ and therefore $F^g = F$. So $F$ is a normal subgroup of $G$, and $F$ is regular, because $|F| = |\Omega|$. But we assumed that $G$ has no regular normal subgroup.

So we are left with the case that $N$ is primitive and not regular. We need to show that $N$ is simple. Suppose that this is not the case. Then $N$ has a minimal normal subgroups $S < N$. As $N$ is a minimal normal subgroup of $G$, there is an element $g \in G$ with $S \neq S^g$. So $S$ and $S^g$ are minimal normal subgroups of $N$, hence $S \cap S^g = \{e\}$ and therefore $[S, S^g] = \{e\}$. Again, the primitivity of $N$ implies that $S$ and $S^g$ are transitive, and as these groups centralize each other, they both are regular. We claim that $N = SS^g$. If that were not the case, then there were $h \in G$ with $S^h \not\leq SS^g$. Similarly as above, $[S^h, SS^g] = \{e\}$, so $SS^g$ we regular too, which is absurd. Thus $N = SS^g \cong S \times S$, so $|N| = |\Omega|^2$. Let $m$ be the common length of the $N_\omega$–orbits on $\Omega \setminus \{\omega\}$. So $m$ divides $|\Omega| - 1$. But $m$ also divides $|N_\omega|$, which divides $|\Omega| = |\Omega|^2$. However $|\Omega| - 1$ and $|\Omega|^2$ are relatively prime. This final contradiction proves the theorem.

2 Jordan sets

**Definition 2.1.** Let $G$ act transitively on $\Omega$. A subset $\Delta \subseteq \Omega$ with $|\Delta| \geq 2$ is called a *Jordan set*, if the pointwise stabilizer of $\Omega \setminus \Delta$ in $G$ acts transitively
Remark 2.2. If $G$ is $k$-fold transitive $\Omega$, then any subset $\Delta$ with $|\Delta| \geq 2$ and $|\Omega \setminus \Delta| \leq k - 1$ is a Jordan set.

In the following we denote by $G(\Delta)$ the pointwise stabilizer of $\Omega \setminus \Delta$ in $\Delta$.

Lemma 2.3. Let $G$ act transitively on $\Omega$, and let $\Delta$ and $\Sigma$ be Jordan sets of $\Omega$. Then the following holds:

(a) If $\Delta \cap \Sigma \neq \emptyset$, then $\Delta \cup \Sigma$ is a Jordan set.

(b) Let $\Delta \subsetneq \Omega$ be a maximal Jordan set with respect to inclusion. Then $\Delta \cap \Sigma = \emptyset$ or $\Sigma \subset \Delta$ or $\Delta \cup \Sigma = \Omega$.

(c) Let $G$ be imprimitive, and $B$ be a nontrivial block which intersects $\Delta$ non-trivially. Then $\Delta \subseteq B$ or $B \subseteq \Delta$.

Proof. (a) Clearly $<G(\Delta), G(\Sigma)>$ fixes $\Omega \setminus (\Delta \cup \Sigma)$ pointwise. As $G(\Delta)$ and $G(\Sigma)$ are transitive on $\Delta$ and $\Sigma$, and $\Delta \cap \Sigma$ is not empty, we get that $<G(\Delta), G(\Sigma)>$ is transitive on $\Delta \cup \Sigma$.

(b) Clear by (a).

(c) Suppose that the assertion is false. Then there is

\[
\begin{align*}
\alpha & \in B \cap \Delta \\
\beta & \in B \setminus \Delta \\
\delta & \in \Delta \setminus B.
\end{align*}
\]

Pick $g \in G(\Delta)$ with $\alpha^g = \beta$. Note that $\delta \notin B$, but $\delta = \alpha^g \in B^g$, so $B \neq B^g$ and hence $B \cap B^g = \emptyset$. However, $\beta \notin \Delta$, so $\beta = \beta^g$ since $g \in G(\Delta)$. Therefore $\beta \in B \cap B^g$, a contradiction.

Lemma 2.4 (Rudio). Let $G$ act primitively on the finite set $\Omega$, and let $\Delta$ be a nonempty proper subset of $\Omega$. Then for any distinct $\alpha, \beta \in \Omega$ there is $g \in G$ with $\alpha \notin \Delta^g$, but $\beta \in \Delta^g$.

Proof. Without loss of generality we may and do assume that $G$ acts faithfully. In particular, $G$ is finite.

Set $U := \{g \in G \mid \beta \in \Delta^g\}$ and $B = \bigcap_{g \in U} \Delta^g$. We are done once we know that $B$ is a block, since then $B = \{\beta\}$ by primitivity of $G$, so there is $g \in U$ with $\alpha \notin \Delta^g$. 

3
We need to show that $B$ is a block. Let $x \in G$ be arbitrary, and assume that $B$ and $B^x$ have a nontrivial intersection. Pick $b \in B \cap B^x$. We need to show that $B = B^x$. We distinguish two cases:

(a) If $\beta \in B^x$, then $\beta \in \cap_{g \in U} \Delta^{gx}$, so $Ux \subset U$. But $U$ is a finite set, hence $Ux = U$. We obtain

$$B^x = \cap_{g \in U} \Delta^{gx} = \cap_{h \in U} \Delta^h = \cap_{h \in U} \Delta^h = B.$$ 

(b) Now suppose that $\beta \notin B^x$. Pick $y \in G$ with $b^y = \beta$. From $b \in B \cap B^x$ we get $\beta = b^y \in B^y \cap B^{xy}$, so $\beta \in B \cap B^y \cap B^{xy}$. Now $B = B^y$ and $B = B^{xy}$ by case (a), hence $B^y = B^{xy}$, and finally $B = B^x$.

\[
\square
\]

**Theorem 2.5 (Jordan).** Let $G \leq \text{Sym} (\Omega)$ act primitively on the finite set $\Omega$. Suppose that there is a proper Jordan set in $\Omega$. Then the action is $2$–transitive.

**Proof.** Let $\Delta \subsetneq \Omega$ be a maximal nontrivial Jordan set. Set $|\Delta| = k$ and $|\Omega| = n$. Fix $\alpha \in \Omega$. By Rudio’s Lemma, for any $\beta \in \Omega \setminus \{\alpha\}$ there is $g \in G$ with $\alpha \notin \Delta^g$, but $\beta \in \Delta^g$. Clearly, $\Delta^g$ is a proper Jordan set too. Let $D$ be the set of these sets $\Delta^g$. Note that any two members of $D$ intersect trivially by Lemma ???. So $\Omega \setminus \{\alpha\}$ is a disjoint union of the sets in $D$. In particular, $k$ divides $n - 1$. Set

$$M = \{ (\alpha, \Delta^x) | \alpha \in \Omega, x \in G, \alpha \notin \Delta^x \}.$$ 

Counting via $\alpha$ shows $|M| = n \cdot \frac{n-1}{k}$. Set $u := |\{\Delta^x | x \in G\}|$. Clearly $|M| = u \cdot (n - k)$, so

$$uk(n-k) = n(n-1).$$ 

From $k \mid n-1$ we get that the numbers $k, n-k$ and $n$ are pairwise relatively prime, so $k(n-k)$ divides $n - 1$. In particular, $k(n-k) \leq n - 1$. Together with $2 \leq k \leq n - 1$ this implies $k = n - 1$, so $\Omega = \Delta \cup \{\alpha\}$ for some $\alpha$. We get that $G_\alpha$ is transitive on $\Delta$, and the claim follows. \[
\square
\]

## 3 Sharply multiply transitive groups

Let $G$ act on the set $\Omega$. Set $\Omega^{(k)}$ be the set of $k$–tuples $(\omega_1, \omega_2 \ldots, \omega_k)$ with pairwise distinct entries. We say that $G$ is sharply $k$–fold transitive on $\Omega$ if $G$ acts regularly on $\Omega^{(k)}$.

Some easy consequences of this definition are:
If $G$ is transitive on $\Omega$, then $G$ is sharply $k$–fold transitive on $G$ if and only $G_\omega$ is sharply $(k - 1)$–fold transitive on $\Omega \setminus \{\omega\}$ for some (or any) $\omega \in \Omega$.

If $G$ is sharply $k$–fold transitive on the finite set $\Omega$ of size $n$, then $|G| = n(n - 1)(n - 2) \ldots (n - k + 1)$.

Clearly, a sharply 1–fold transitive group is just a group in its regular action. We list some examples of sharply $k$–fold transitive groups for $k \geq 2$:

- Let $K$ be a skewfield. Then $G = AGL(1, K)$ acts sharply 2–transitively on $K$.

- Let $K$ be field. Then $PGL(2, K)$ acts sharply 3–transitively on the set of 1–dimensional subspaces of $K^2$.

- If $|\Omega| = n < \infty$, then $\text{Sym}(\Omega)$ acts sharply $n$–transitively on $\Omega$. This action is also sharply $(n - 1)$–transitive. Furthermore, $\text{Alt}(\Omega)$ acts sharply $(n - 2)$–transitively on $\Omega$.

A Theorem of Tits shows that except for specific groups of degrees 11 and 12, there are no other cases of sharp $k$–transitivity for $k \geq 4$.

In the following $M_{11}$ denotes a hypothetical group which acts sharply 4–transitively on 11 points. Such a group indeed exists and is unique, which will not be shown here. (Remarks about Mathieu groups ???)

In the following we do not assume that $\Omega$ is finite. Before discussing the case $k \geq 4$, we look at the case $k = 4$ which serves as basis for an induction proof of the general case.

**Proposition 3.1** (Tits). Let $G$ act sharply 4–transitively on the set $\Omega$. Then $G$ is one of the following groups: $S_4$, $S_5$, $A_6$, $M_{11}$.

**Proof.** We will frequently show that an element from $G$ is the identity by showing that it has at least four fixed points.

Let 1, 2, 3, 4 be distinct elements from $\Omega$. Pick $t \in G$ with

$$1^t = 2, \quad 2^t = 1, \quad 3^t = 3, \quad 4^t = 4.$$ 

So $t^2$ has at least four fixed points, hence $t^2 = e$.

So $t$ is an involution. Set $H = G_1 \cap C_G(t)$. Clearly, $H$ acts on the fixed points of $t$. This action is faithful, because $h \in H$ fixes 1, and also 2 in view of $2^h = 1^h = 1^t = 1^t = 2$. So if $h$ fixes 3 and 4 too, then $h$ has four fixed points, hence $h = e$. 

5
On the other hand, $t$ has at most 3 fixed points, and if $|\Omega|$ is even, then $t$ has exactly 2 fixed points. From that we see that $|H| \leq 6$, and $|H| \leq 2$ if $|\Omega|$ is even.

Let $P = \{ (\omega, \omega') \mid \omega \in \Omega, \omega \neq 1, 2, \omega \neq \omega' \}$ be the ordered orbits of $\langle t \rangle$ of length 2 distinct from $(1, 2)$ and $(2, 1)$.

We claim that $H$ acts transitively on $P$: Pick $(\omega, \omega')$ and $(\bar{\omega}, \bar{\omega}')$ in $P$, and choose $g \in G$ with $1^g = 1, 2^g = 2, \omega^g = \bar{\omega}, (\omega')^g = \bar{\omega}'$.

Of course $g \in G_1$. We are done once we know that $g \in C_G(t)$. Consider the commutator $c = g^{-1}t^{-1}gt$, and note that $t = t^{-1}$. We compute that $c$ fixes the points $1, 2, \bar{\omega}, \bar{\omega}'$:

\begin{align*}
1g^{-1}t^{-1}gt &= 1t^{-1}gt = 2gt = 2t = 1 \\
2g^{-1}t^{-1}gt &= 2t^{-1}gt = 1gt = 1t = 2 \\
\bar{\omega}g^{-1}t^{-1}gt &= \omega t^{-1}gt = \omega^t = \bar{\omega}t \\
(\omega')^g t^{-1}gt &= (\omega')^t = \omega^t = \bar{\omega}t
\end{align*}

This yields $g^{-1}t^{-1}g = e$, so $g \in H$.

Note that $|\Omega| = 2 + f + |P|$, where $f \in \{2, 3\}$ is the number of fixed points of $t$. We obtain $|\Omega| \leq 2 + 3 + 6 = 11$, and $|\Omega| \leq 2 + 2 + 2 = 6$ if $|\Omega|$ is even.

In order to finish the proof, we need to show that $|\Omega| \neq 7, 9$.

First suppose that $|\Omega| = 9$. Then $|P| = 4$. However, $H$ is isomorphic to a subgroup of $S_3$, and such a group cannot act transitively on a set of size 4.

So we are left to deal with $|\Omega| = 7$. In this case $t$ is a double transposition. But $G$ is 4–transitive on $\Omega$, so $G$ then contains all double transpositions from $\text{Sym}(\Omega)$. But $(1 2)(3 4) \cdot (1 2)(3 5) = (3 4 5)$, so $G$ also contains all 3–cycles, hence $G \geq \text{Alt}(\Omega)$, a contradiction.

**Lemma 3.2.** Let $G \leq \text{Sym}(\Omega)$ be transitive, and $|\Omega| = p$ be a prime. Then $|G| = pd(1 + pe)$ with $e \in N_0$ and a divisor $d$ of $p - 1$.

**Proof.** Let $C$ be a Sylow $p$–subgroup of $G$. Then $C$ has order $p$, is cyclic and regular on $\Omega$. Set $N = N_G(C)$. Note that $C = C_G(C)$, so $N/C$ is isomorphic to a subgroup of $\text{Aut}(C)$, a group of order $d \mid p - 1$. The number of Sylow $p$–subgroups of $G$ has the form $1 + pe$, and equals $[G : N]$ since they are all conjugate to $C$. The claim then follows from $|G| = [G : N][N : C]|C|$. □

**Lemma 3.3.** Suppose that $|\Omega| = 13$. Then $\text{Sym}(\Omega)$ does not contain a sharply 6–transitive group.
Proof. Suppose that $G \leq \text{Sym}(\Omega)$ is sharply 6–transitive. So $|G| = 13 \cdot 12 \cdot 11 \cdot 10 \cdot 9 \cdot 8$. By the previous lemma, $|G| = 13d(1 + 13e)$ for a divisor $d$ of 12. Writing $12 = dk$, we obtain $11 \cdot 10 \cdot 9 \cdot 8k = 1 + 13e$, hence $3k \equiv 1 \pmod{13}$. This yields $k \equiv 9 \pmod{13}$, contrary to $k$ being a divisor of 12.

In the following $M_{12}$ denotes a group which acts sharply 5–transitively on 12 points. We do not prove existence and uniqueness of such a group.

Theorem 3.4 (Tits). Suppose that $G$ act sharply $k$–transitively on the set $\Omega$ for $k \geq 4$. Then $\Omega$ is finite, and $G$ is one of the following groups: $S_n$ ($k = n$ or $k = n - 1$), $A_n$ ($k = n - 2$), $M_{11}$ ($k = 4$), $M_{12}$ ($k = 5$).

Proof. We know this result already for $k = 4$. Since a point stabilizer of a sharply $k$–transitive group is sharply $(k - 1)$–transitive on the remaining points, the result follows by induction and the fact from the previous lemma, that $M_{12}$ is not a point stabilizer of a sharply 6–transitive group on 13 elements.

4 Transitive groups of prime degree

Theorem 4.1 (Burnside). Let $p$ be a prime number, $|\Omega| = p$, and $G \leq \text{Sym}(\Omega)$ be transitive. Then $G$ is either 2–transitive or a proper subgroup of $\text{AGL}_1(p)$ with respect to a suitable identification of $\Omega$ with $\mathbb{F}_p$.

The main tool is the following

Proposition 4.2. Let $U$ be a non-empty, proper subset of $\mathbb{F}_p \setminus \{0\}$. Let $\pi$ be a permutation of $\mathbb{F}_p$ such that $i - j \in U$ for $i, j \in \mathbb{F}_p$ implies $\pi(i) - \pi(j) \in U$. Then there are $a, b \in \mathbb{F}_p$ such that $\pi(x) = ax + b$ for all $x \in \mathbb{F}_p$.

In [Sch08] Schur gives a proof of this proposition in two steps. First he uses a precursor of his S-ring technique to show that if $1 \in U$, then $U$ is a subgroup of $\mathbb{F}_p \setminus \{0\}$. In the second step he shows that $\pi$ is linear. In this note we show that a small modification of his second step makes the first step unnecessary. See the remarks at the end for further comments.

Proof of Burnside’s theorem. Let $G$ be a transitive permutation group on $p$ elements. As $p$ divides the order of $G$, there is an element $\tau \in G$ of order $p$. We may assume that $G$ acts on $\mathbb{F}_p$, with $\tau(x) = x + 1$ for all $x \in \mathbb{F}_p$. So $G$ contains the group of translations $x \mapsto x + b$ for each $b \in \mathbb{F}_p$.

Suppose that $G$ is not doubly transitive. Then the stabilizer $G_0$ of 0 has at least 2 orbits on $\mathbb{F}_p \setminus \{0\}$. Let $U$ be one of these orbits. In order to show
that $U$ meets the assumptions of the proposition, pick $i, j$ with $i - j \in U$. Define $\sigma : x \mapsto \pi(x + j) - \pi(j)$, note that $\sigma \in G$, and $\sigma(0) = 0$, so actually $\sigma \in G_0$. Therefore $\pi(i) - \pi(j) = \sigma(i - j) \in U$.

So we may apply the proposition, which shows that $G$ is a subgroup of the group of permutations $x \mapsto ax + b$ with $a \in \mathbb{F}_p \setminus \{0\}, b \in \mathbb{F}_p$.

**Lemma 4.3.** Let $U$ be a subset of $m$ nonzero elements in a field. Then there is an integer $r$ with $1 \leq r \leq m$ with $\sum_{u \in U} u^r \neq 0$.

**Proof.** Write $U = \{u_1, u_2, \ldots, u_m\}$ and $\prod_{i=1}^m (X - u_i) = a_0 + a_1X + \cdots + a_{m-1}X^{m-1} + X^m$. Consider the matrix and the vectors

$$A = \begin{pmatrix} 1 & u_1 & \cdots & u_1^{m-1} \\ 1 & u_2 & \cdots & u_2^{m-1} \\ \vdots & \vdots & \ddots & \vdots \\ 1 & u_m & \cdots & u_m^{m-1} \end{pmatrix}, \quad a = \begin{pmatrix} a_0 \\ a_1 \\ \vdots \\ a_{m-1} \end{pmatrix}, \quad v = -\begin{pmatrix} u_1^n \\ u_2^n \\ \vdots \\ u_m^n \end{pmatrix}.$$

Then $a$ is the unique solution of the linear equation $Ax = v$. Therefore $A$ is invertible. In particular

$$\left(\sum_{u \in U} u \sum_{u \in U} u^2 \cdots \sum_{u \in U} u^m\right) = (u_1 \ u_2 \ \cdots \ u_m) A \neq 0,$$

and the claim follows. \qed

**Proof of the proposition.** By an iterated application of $\pi$ we see that $i - j \in U$ if and only if $\pi(i) - \pi(j) \in U$. In particular, replacing $U$ by its complement in $\mathbb{F}_p \setminus \{0\}$ preserves the assumption. Therefore we may and do assume $|U| \leq \frac{p-1}{2}$.

Fix $i \in \mathbb{F}_p$. For $u \in U$ we have $(i + u) - i \in U$, hence $\pi(i + u) - \pi(i) \in U$. As $\pi$ is a permutation, the elements $\pi(i + u) - \pi(i)$ are different for different $u$. Thus $\{\pi(i + u) - \pi(i) | u \in U\} = U$, hence $\{\pi(i + u) | u \in U\} = \{\pi(i) + u | u \in U\}$. In particular, for $w \in \mathbb{N}$ we obtain

$$\sum_{u \in U} \pi(i + u)^w = \sum_{u \in U} (\pi(i) + u)^w.$$

Let $f(X) \in \mathbb{F}_p[X]$ be the polynomial of degree $n \leq p - 1$ with $f(i) = \pi(i)$ for all $i \in \mathbb{F}_p$. Suppose $wn \leq p - 1$. Then $\sum_{u \in U} f(X + u)^w - \sum_{u \in U} (f(X) + u)^w$ is a polynomial of degree $< p$ which vanishes identically on $\mathbb{F}_p$, thus

$$\sum_{u \in U} f(X + u)^w - \sum_{u \in U} (f(X) + u)^w = 0.$$
Setting $S_k = \sum_{u \in U} u^k$, we obtain

$$\sum_{u \in U} (f(X + u)^w - f(X)^w) = \sum_{k=1}^w \binom{w}{k} S_k f(X)^{w-k}.$$ 

Let $r \geq 1$ be minimal with $S_r \neq 0$. Then the right hand side has degree $n(w - r)$ if $r \leq w$, or vanishes if $r > w$.

$f(X)^w$ is a polynomial of degree $nw < p$. For $0 \leq \nu \leq nw$, the $\nu$th derivative $(f(X)^w)^{(\nu)}$ has degree $nw - \nu$. Thus there are $a_0, a_1, \ldots, a_{nw} \in \mathbb{F}_p$ such that

$$X^{nw} = \sum_{\nu=0}^{nw} a_{\nu} (f(X)^w)^{(\nu)},$$

where $a_0 \neq 0$. This yields

$$\sum_{u \in U} ((X + u)^{nw} - X^{nw}) = \sum_{\nu=0}^{nw} a_{\nu} \left( \sum_{k=1}^w \binom{w}{k} S_k f(X)^{w-k} \right)^{(\nu)}.$$ 

So

$$\sum_{u \in U} ((X + u)^{nw} - X^{nw})$$ is 0 or has degree $n(w - r)$. (1)

The previous lemma gives $r \leq |U| \leq \frac{p-1}{2}$.

Suppose we have chosen $w$ maximal with $nw \leq p - 1$. Then $p - 1 < n(w + 1) \leq 2nw$, so $nw > \frac{p-1}{2} \geq r$. Thus $nw - r > 0$, and (1) has degree $nw - r$ as one sees from expanding $(X + u)^{nw}$. We obtain $nw - r = n(w - r)$, so $n = 1$, and we are done.

Remark. Our proof resembles the final step of Schur’s proof in [Sch08]. However, the main part of his proof consists in showing that if $1 \in U$, then $U$ is a subgroup of $\mathbb{F}_p \setminus \{0\}$. Thus if $1 \leq k \leq w < |U|$, then $S_k = 0$, so $\sum_{u \in U} f(X + u)^w = |U| f(X)^w$, which produces a contradiction similarly as above. See also [DM96, 3.5] for a modern version of this proof.

In [DKM92] the authors give an S-ring argument to show that $U$ is a group. From there they however proceed with geometric arguments, and use facts about lacunary polynomials to conclude that $\pi$ is a linear function.

Burnside’s original proof uses complex character theory, see [Bur11].

Another proof is due to Wielandt, who studies the ring of $G$-invariant functions from $\mathbb{F}_p$ to $\mathbb{F}_p$. See [Wie94, pages 273–296], [HB82, XII, §10]. Concise and streamlined version of Wielandt’s proof are contained in [LMT93, 6.7] and [FJ05, 21.7].
5 Primitive groups with regular cyclic subgroup

We study finite primitive permutation groups with a cyclic regular subgroup. In a long and difficult paper from 1933 I. Schur [Sch33] invented a new technique to prove that such a group has either prime degree, or is doubly transitive. Later Wielandt [Wie64] gave a different version of Schur’s technique and proved the slightly more general

**Theorem 5.1** (Schur). Let \( G \) be a primitive permutation group of degree \( n \), and \( A \) be a regular abelian subgroup. Suppose that \( n \) is not prime, and that \( A \) contains a cyclic Sylow \( p \)-subgroup for some prime divisor \( p \) of \(|A|\). Then \( G \) is doubly transitive.

Because of its importance for the monodromy groups of polynomials and the beauty of its proof, we give a self-contained account in the following. Our presentation is influenced by [DM96]. For a variant confer [LMT93].

In the following we assume the hypotheses of the Theorem. Let \( \Omega \) be the set \( G \) acts on. Pick \( \omega \in \Omega \). The regular action of \( A \) allows us to identify \( \Omega \) with the elements of \( A \), where we identify \( a \) with \( \omega^a \). This way we obtain a regular action of \( G \) on \( A \), where the subgroup \( A \) acts in its regular action on itself. In order to avoid a confusion with the notation for conjugation, we write \( a \star g \) for the image of \( a \in A \) under \( g \in G \) instead of \( a^g \). If \( b \in A \), then obviously \( a \star b = ab \). Also,

\[
1 \star (ag) = (1 \star a) \star g = a \star g = 1 \star (a \star g) \quad \text{for all } a \in A, \ g \in G. \tag{2}
\]

Let \( p \) be a prime such that, according to the hypothesis, \( A \) has a cyclic \( p \)-Sylow subgroup. So \( A \) has a unique subgroup of order \( p \), call it \( P \).

We will work with the group algebra \( R \) of \( A \) over \( \mathbb{F}_p \). As an \( \mathbb{F}_p \)-space, this is the space of mappings \( \lambda : A \rightarrow \mathbb{F}_p \). Addition and multiplication in \( R \) are defined as follows:

\[
(\lambda + \mu)(a) := \lambda(a) + \mu(a)
\]
\[
(\lambda \mu)(a) := \sum_{b,c \in A} \lambda(b) \mu(c) \quad \text{if } b \cdot c = a
\]

It is straightforward to verify that this makes \( R \) into a ring with unity. We use a more convenient notation, by writing \( \lambda_a \) instead of \( \lambda(a) \) and by identifying \( \lambda \in R \) with the formal linear combination \( \sum_{a \in A} \lambda_a a \).

We extend the action of \( G \) on \( A \) to \( R \) by linearity, and again write \( r \star g \) for \( g \in G \) applied to \( r \in R \).
For a subset $\Gamma \subseteq A$ we denote by $[\Gamma]$ the element $\sum_{\gamma \in \Gamma} \gamma \in R$. For $r \in R$, let $\text{supp}(r)$ be the support of $r = \sum \lambda_a a$, which is the set of those $a \in A$ with $\lambda_a \neq 0$. Let $G_1$ be the stabilizer of $1 \in A$, and denote by $C_R(G_1)$ the subset of elements of $R$ which are fixed by $G_1$. Let $A_1 = \{1\}, A_2, \ldots, A_N$ be the orbits of $G_1$ on $A$. Of course, we aim to prove that $N = 2$.

Lemma 5.2. The following holds.

(a) $C_R(G_1)$ is an $\mathbb{F}_p$-subspace of $R$ with basis $[A_1], [A_2], \ldots, [A_N]$.

(b) If $\Gamma \subseteq A$ is $G_1$-invariant, then $(\Gamma a) * g = \Gamma a * g$ for all $a \in A$, $g \in G_1$.

(c) If $\Gamma, \Delta \subseteq A$ are $G_1$-invariant, then so is $\Gamma \Delta$.

(d) $C_R(G_1)$ is a subring of $R$.

(e) If $B$ is a $G_1$-invariant subgroup of $A$, then $B = \{1\}$ or $B = A$.

(f) $<\text{supp}(c)> = 1$ or $A$ for each $c \in C_R(G_1)$.

(g) Let $\Gamma \subseteq A$ be $G_1$-invariant. Then $[\Gamma]^p = [\Gamma \cap P]^1$.

(h) For each $i = 1, 2, \ldots, N$ we have $|A_i \cap P| \geq 1$ and $A_i \setminus P$ is a union of cosets of $P$ in $A$.

Proof. To (a). If $c = \sum_{a \in A} \lambda_a a \in C_R(G_1)$, then $c * g = c$ for all $g \in G_1$ implies $\lambda_a = \lambda_b$ if $a, b$ lie in the same $G_1$-orbit. From this conclude the claim.

To (b). From $1 * (ag) = 1 * (a * g)$ (see (2)) we get $h \in G_1$ with $ag = h(a * g)$. So, for $\gamma \in \Gamma$ we obtain from a repeated application of (2) and noting that $\gamma a, \gamma * h, a * g \in A$ the following:

$$
(\gamma a) * g = 1 * (\gamma ag)
= 1 * (\gamma h(a * g))
= 1 * ((\gamma * h)(a * g))
= (\gamma * h)(a * g).
$$

If $\gamma$ runs through $\Gamma$, then so does $\gamma * h$, and (b) follows.

To (c). Let $a$ run through $\Delta$ and use (b).

To (d). In virtue of (a) we need to show that $[A_i][A_j] \in C_R(G_1)$ for all $i, j$. For $g \in G_1$ we get from (b) that if $b \in A_j$, then $(A_i b) * g = A_i (b * g)$, hence $([A_i]b) * g = [A_i](b * g)$. Now take the sum over $b \in A_j$, and note that $b * g$ runs through $A_j$. 11
To (e). If \( h \in G_1 \) then \( B \ast h = B \) by assumption. As \( G = G_1 A \), any \( g \in G \) has the form \( g = ha \) with \( h \in G_1 \) and \( a \in A \). So \( B \ast g = (B \ast h) \ast a = B \ast a = Ba \). So the coset \( Ba \) either equals \( B \), or is disjoint from \( B \). We see that \( B \) is a block with respect to the action of \( G \) on \( A \). However, this action is primitive, forcing \( |B| = 1 \) or \( B = A \).

To (f). For \( c \in C_R(G_1) \) let \( S \) be the support of \( c \), and \( B \) the group generated by \( S \). Note that \( S \) is \( G_1 \)-invariant. Then \( B = \bigcup_{i=0}^{\infty} S^i \), and \( B \) is \( G_1 \)-invariant by (c). The assertion follows from (e).

To (g). Clearly \( [\Gamma] \in C_R(G_1) \). As the support of \([\Gamma]^p\) consists of \( p \)-th powers of \( A \), and the set of \( p \)-th powers of \( A \) is a proper subgroup of \( A \), we see that the group generated by the support of \([\Gamma]^p\) is a proper subgroup of \( A \), hence is trivial by (f). So \([\Gamma]^p\) is a multiple of 1, and the coefficient of 1 is the number of \( \gamma \in \Gamma \) with \( \gamma^p = 1 \), and the claim follows.

To (h). Let \( \Gamma \) be one of the \( A_i \). Pick \( \gamma \in \Gamma \setminus P \). Then \( \gamma^p \neq 1 \), and the number of elements \( \delta \in \Gamma \) with \( \gamma^p = \delta^p \) must be divisible by \( p \) as a consequence of (g). So this number is at least \( p \). On the other hand, as \( A \) is abelian, \( \gamma^p = \delta^p \) implies \( \delta \in P\gamma \), so there are at most \( |P| = p \) such elements \( \delta \). It follows that the set of \( \delta \in \Gamma \) with \( \delta^p = \gamma^p \) is precisely \( P\gamma \). In particular, \( P\gamma \subseteq \Gamma \). We see that \( \Gamma \setminus P \) is a union of cosets of \( P \).

It remains to show that \( \Gamma \) contains an element from \( P \). Suppose wrong. Then, by what we saw, \( \Gamma \) is a union of cosets of \( P \), hence \( P \subseteq B := \{b \in A | \ \Gamma b = \Gamma \} \). Clearly \( B \) is a subgroup of \( A \) of order \( > 1 \). Furthermore, \( B \) is \( G_1 \) invariant by (b). So \( B = A \) by (f). But this implies the nonsense \( A = \Gamma A = \Gamma \not\subseteq A \). \( \square \)

Now we are ready to prove the theorem. Suppose that \( G \) is not doubly transitive. Then there exists a \( G_1 \)-orbit \( \Gamma \) different from \( A_1 = \{1\} \) such that \( \mu := |\Gamma \cap P| \leq (p-1)/2 \). Set \( S = \{a \in A | Pa \subseteq \Gamma \} \). By (h) we know that \( \Gamma \) is the disjoint union of \( \Gamma \cap P \) and the sets \( Pa, a \in S \). Taking sums, we get

\[ [\Gamma] = [\Gamma \cap P] + [P]r, \]

with \( r = |S| \). For \( v \in P \) we have \( v[P] = [P] \), hence \( [P]^2 = p[P] = 0 \) and \([\Gamma \cap P][P] = \mu[P] \). Now \( c := ([\Gamma] - \mu 1)^2 \in C_R(G_1) \) by (d). We compute

\[ c = ([\Gamma \cap P] - \mu 1 + [P]r)^2 \]
\[ = ([\Gamma \cap P] - \mu 1)^2 + 2([\Gamma \cap P][P] - \mu[P])r + [P]^2r^2 \]
\[ = ([\Gamma \cap P] - \mu 1)^2, \]

so the support of \( c \) is contained in \( P \). Since \( P < A \), we get \( \text{supp}(c) \subseteq \{1\} \) by (f). So \( ([\Gamma \cap P] - \mu 1)^2 = [\Gamma \cap P]^2 - 2\mu[\Gamma \cap P] + \mu^21 \) is a multiple of 1. By (h), there is \( \gamma \in \Gamma \cap P \), so \( \mu \geq 1 \) and \( \gamma \neq 1 \). Let \( \rho \) be the number of appearances
of $\gamma$ in the expansion of $[\Gamma \cap P]^2$. Clearly $\rho \leq \mu$. But by the above, $p$ divides $\rho - 2\mu$, a contradiction to $-p < -2\mu \leq \rho - 2\mu \leq \mu - 2\mu < 0$.

**Remark.** There are also versions of the theorem for certain non-abelian regular groups $A$, see the references given in [Wie64, §25].

**References**


