Permutation groups of prime degree, a quick proof of Burnside’s theorem

Peter Müller
October 7, 2021

Abstract
A transitive permutation group of prime degree is doubly transitive or solvable. We give a direct proof of this theorem by Burnside which uses neither S-ring type arguments, nor representation theory.

In this note $\mathbb{F}_p$ is the field with $p$ elements, with $p$ a prime. The following proposition proves Burnside’s theorem in a few lines.

Proposition 1. 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 $\pi(i) = ai + b$ for all $i \in \mathbb{F}_p$.

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 $p$. Assume that $G$ acts on $\mathbb{F}_p$, with $\tau(i) = i + 1$ for all $i \in \mathbb{F}_p$. Suppose that $G$ is not doubly transitive. So $G$ has at least two orbits on the pairs $(i, j)$ with $i \neq j$. On the other hand, $\tau$ permutes cyclically the pairs $(i, j)$ with constant difference, so there is a non-empty proper subset $U$ of $\mathbb{F}_p \setminus \{0\}$ such that $\pi(i) - \pi(j) \in U$ for all $\pi \in G$ and $i, j$ with $i - j \in U$. By the proposition, $G$ is a subgroup of the group of permutations $i \mapsto ai + b$ with $a \in \mathbb{F}_p \setminus \{0\}, b \in \mathbb{F}_p$. In particular, $G$ is solvable.
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 $\{\pi(i + u) - \pi(i) \mid u \in U\} = U$, hence $\{\pi(i + u) \mid u \in U\} = \{\pi(i) + u \mid u \in U\}$. 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

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

Note that $f(X)^w$ is a polynomial of degree $nw$, so $X^{nw}$ is an $\mathbb{F}_p$-linear combination of the derivatives of $f(X)^w$. Thus we obtain

$$\sum_{u \in U} ((X + u)^{nw} - X^{nw}) = \sum_{k \geq 1} S(k) g_{w-k}(X),$$

where $g_k(X)$ is a polynomial of degree at most $\ell n$.

Let $r \geq 1$ be minimal with $S(r) \neq 0$. Then the degree of the right handside is at most $n(w - r)$.

Suppose that $r \leq nw$. Then the coefficient of $X^{nw-r}$ on the left handside is (up to a nonzero factor) $S(r)$. Since $S(r) \neq 0$, we must have $nw - r \leq n(w - r)$, so $n = 1$, and we are done.

It remains to consider $r - 1 \geq nw$. Suppose we have chosen $w$ maximal with $nw \leq p - 1$. Then $p - 1 < n(w + 1) \leq 2nw \leq 2(r - 1)$, so $r > (p + 1)/2$.

This shows $S(k) = 0$ for $k = 1, 2, \ldots, (p - 1)/2$. Therefore $|U| \geq (p + 1)/2$ (for instance because the van der Monde matrix of $U$ is not singular; or
because the first \((p - 1)/2\) elementary symmetric functions of \(U\) vanish, so a polynomial with zero set \(U\) has degree \(\geq (p + 1)/2\). This contradicts \(|U| \leq (p - 1)/2\).

**Remark.** Our proof is similar to the final step in 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]. The certainly most elegant 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]. A very concise and streamlined version of Wielandt’s proof is contained in [LMT93 6.7].

### References

[Sch08] I. Schur, *Neuer Beweis eines Satzes von W. Burnside*, Jahresbericht der Deutsch. Math.-Ver. (1908), 17, 171–176.
[Wie94] H. Wielandt, *Mathematische Werke/Mathematical works. Vol. 1*, Walter de Gruyter & Co., Berlin (1994).

IWR, Universität Heidelberg, Im Neuenheimer Feld 368, 69120 Heidelberg, Germany
E-mail: Peter.Mueller@iwr.uni-heidelberg.de