THE BRAUER-SUZUKI-WALL THEOREM

BY
HELMUT BENDER[1]

1. Introduction

It is the purpose of this note to present an alternate proof of the following fundamental result of Brauer, Suzuki, and Wall.

THEOREM (Brauer-Suzuki-Wall). *Let G be a finite group with an involution t and an abelian subgroup K of $H = C_G(t)$ containing t. Assume the following conditions*:

(i) $H = K\langle s\rangle$ *with an involution* $s \notin K$;
(ii) $C_K(s) = \langle t\rangle$, *and* $x^s = x^{-1}$ *for all* $x \in K$;
(iii) $K \cap K^g = 1$ *for all* $g \in G - H$;
(iv) *all involutions of G are conjugate to t.*

Then G has a subgroup Q of order q such that
(1) $|G| = q(q + 1)(q - 1)/2$;
(2) $C_G(x) = Q$ *for all* $x \in Q^{\#}$;
(3) $N_G(Q) = QD$ *with an abelian subgroup D of order* $(q - 1)/2$;
(4) *whenever* $1 \subset X \subseteq D$, *then* $N_G(X) = N_G(D) = D\langle u\rangle$ *with an involution* $u \notin D$ *inverting* D.

Considered as a permutation group on the set of conjugates of Q, G then satisfies the assumptions of a theorem of Zassenhaus (G is doubly transitive of degree $q + 1$, no non-identity element fixes three points, the stabilizer of two points is abelian of order $(q - 1)/2$ and is inverted by some involution). It follows that G is isomorphic to $PSL_2(q)$; see [6], or [4, Section 18], or [3, Section 13.3].

The original proof of the Brauer-Suzuki-Wall Theorem is contained in part II of [2]. See also [3, Sections 15.4 and 9.4].

By a transfer argument, condition (iv) can be replaced by the assumption that G has no subgroup of index 2.

In addition to the notation already introduced, we let $k = |K|$, and

$$i(x) = \textit{number of involutions} \quad u \neq x \quad \textit{in } G \textit{ satisfying} \quad x^u = x^{-1}, \quad \textit{for} \quad x \in G.$$

Note that $i(x)$ equals the number of ordered pairs (u, v) of involutions u, v satisfying $x = uv$. All other notation follows [3] and is standard. In particular $Q^{\#}$ denotes the set of non-identity elements in Q.

For $k = 2$ it is easily verified that every coset of H (a Sylow 2-subgroup of

Received October 12, 1973.

[1] This research was partially done at the University of Illinois at Chicago Circle and was supported by a National Science Foundation grant.

G) not lying in $N = N_G(H)$ contains exactly one involution, and hence that for each involution u outside N the subgroup $T = N \cap N^u$ has order $3 = |N:H|$ and is inverted by u; for example, see [3], Theorem 9.2.2.i.

Since then u is the only element of Hu normalizing T, it follows that $C_G(T) = T$. Hence either $G = N$, or $G - N$ contains exactly $3 \cdot 4$ involutions because N has 4 subgroups of order 3 and each is normalized by 3 involutions (if $G \neq N$). In the latter case, $3 \cdot 4 = |G:H| - |N:H|$, and hence $|G| = 60$.

For a beautiful discussion of a similar, but much more general situation, the reader is referred to [5].

In case $k = 4$, subgroups of order larger than $|H|$ are still available, namely the normalizers of elementary abelian subgroups of order 4. Again the desired conclusion can be obtained from a look at the distribution of involutions in the cosets of such a large subgroup. See for example [1, Section 3].

In the following, assume $k > 4$. Here elementary counting arguments have to be supplemented by some information on the order of G. A suitable lower bound would suffice, but the character argument in the next section will give the exact order of G, in terms of k and a sign $\varepsilon = \pm 1$.

2. The order of G

The abelian group K has k linear characters, two of which are fixed by s (namely those having $[s, K]$, a subgroup of index 2 in K, in their kernel). Each of the values 1 and -1 is assumed by $k/2$ characters on t. Since $k/2 - 2 \geq 6/2 - 2 = 1$, K has linear characters ρ and σ not fixed by s such that $\rho(t) = 1$ and $\sigma(t) = -1$.

Then ρ^H and σ^H are distinct irreducible characters of H of degree 2. Let $\alpha = (1_K - \rho)^H$ and $\beta = (\rho - \sigma)^H$. Then

$$\alpha(1) = \beta(1) = 0, \qquad \alpha(t) = 0, \qquad \beta(t) = 4,$$
$$(\alpha, \alpha) = 3, \qquad (\beta, \beta) = 2, \qquad (\alpha, \beta) = -1.$$

It is an easily verified but basic fact due to Brauer and Suzuki that these relations remain valid if α and β are replaced by α^* and β^*, the generalized characters of G induced by α and β (moreover, α^* and β^* coincide with α and β on K, respectively); for example, see [3, Theorem 4.4.6]. Here it is essential that K is a t. i. subgroup with normalizer H (condition (iii)), and that α and β vanish outside $K^{\#}$.

By Frobenius reciprocity, $(\alpha^*, 1_G) = 1$ and $(\beta^*, 1_G) = 0$. It follows that

$$\alpha^* = 1_G + \gamma - \lambda, \qquad \beta^* = \varphi - \gamma$$

where γ, λ, and φ are distinct non-trivial irreducible characters of G, or negatives of such characters.

For the class function i defined in the previous section we have the formula

$$i = |G|\,|H|^{-2} \sum \frac{\chi(t)^2}{\chi(1)}\,\chi$$

where χ ranges over all irreducible characters of G; see [3, 9.4.2], and remember that characters always assume real (in fact integral) values on involutions. Clearly, this formula remains valid if any χ is replaced by its negative.

It follows that

$$(\alpha^*, i) = |G||H|^{-2}(1 + \gamma(t)^2/\gamma(1) - \lambda(t)^2/\lambda(1))$$

and

$$(\beta^*, i) = |G||H|^{-2}(\varphi(t)^2/\varphi(1) - \gamma(t)^2/\gamma(1)).$$

Next we compute these two inner products directly. Let $\delta = \alpha^*$ or β^*. Since δ vanishes on elements not conjugate to an element of $K^{\#}$, and $i(x) = k$ for all $x \in K^{\#}$ (the involutions contributing to $i(x)$ are exactly those in $H - K = Ks$, and Ks consists of involutions, by condition (ii)), we conclude

$$(\delta, i) = |G|^{-1}\textstyle\sum_{g\in G} \delta(g)i(g)$$

$$= |G|^{-1}|G:N_G(K)|\, k\textstyle\sum_{g\in K} \delta(g) = |H|^{-1}k^2(1_K, \delta|_K).$$

This together with

$$\alpha^*|_K = \alpha|_K = 1_K - \rho + (1_K - \rho)^s \quad\text{and}\quad \beta^*|_K = \beta|_K = \rho - \sigma + (\rho - \sigma)^s$$

yields

$$(\alpha^*, i) = 2|H|^{-1}k^2 \quad\text{and}\quad (\beta^*, i) = 0.$$

Comparing the two expressions for our inner products, we see that

$$2k^2 = |G:H|(1 + \gamma(t)^2/\gamma(1) - \lambda(t)^2/\lambda(1))$$

and

$$0 = \varphi(t)^2 - \gamma(t)^2$$

(because $\varphi(1) = \gamma(1)$). Since $\varphi(t) - \gamma(t) = \beta^*(t) = \beta(t) = 4$, the latter relation implies $\varphi(t) = 2$ and $\gamma(t) = -2$. Then $1 + \gamma(t) - \lambda(t) = \alpha^*(t) = 0$ yields $\lambda(t) = -1$.

Now the other relation, after multiplication by $\gamma(1)\lambda(1)$, reads

$$2k^2\gamma(1)\lambda(1) = |G:H|f \quad\text{with}\quad f = \gamma(1)\lambda(1) + 4\lambda(1) - \gamma(1).$$

Clearly, H is a Hall subgroup of G. Hence $|G:H|$ divides $\gamma(1)\lambda(1)$. From

$$1 + \gamma(1) - \lambda(1) = \alpha^*(1) = 0$$

it is immediate that the greatest common divisor $(\lambda(1), f)$ of $\lambda(1)$ and f is 1, whence $\lambda(1)$ divides $|G:H|$, and in particular is odd.

Being a multiple of $2k^2$, $f = \gamma(1)(\lambda(1) - 1) + 4\lambda(1)$ is divisible by 8. Hence $\gamma(1)$ is not divisible by 4. Thus, $(\gamma(1), f) = 2$, whence $\gamma(1)/2$ must be a divisor of $|G:H|$.

Now it is clear that

$$|G:H| = \lambda(1)\gamma(1)/2.$$

Hence

$$4k^2 = f = \gamma(1)(\lambda(1) - 1) + 4\lambda(1)$$

$$= (\lambda(1) - 1)^2 + 4\lambda(1) = (\lambda(1) + 1)^2.$$

Thus $2k\varepsilon = \lambda(1) + 1$ with $\varepsilon = \pm 1$. Then $\gamma(1) = \lambda(1) - 1 = 2k\varepsilon - 2$. So we get

$$|G{:}H| = (2k\varepsilon - 1)(k\varepsilon - 1) = (2k - \varepsilon)(k - \varepsilon).$$

Replacing ε by $-\varepsilon$ yields

$$|G{:}H| = (2k + \varepsilon)(k + \varepsilon) \quad \text{with } \varepsilon = \pm 1.$$

In the following, let $q = 2k + \varepsilon$, and note that

$$|G| = q(q + 1)(q - 1)/2.$$

3. Completion of the proof

Since all elements of $H - K$ are conjugate to t, the set K^G equals H^G and contains the centralizer of any of its non-identity elements.

Consider the function $(u, v) \to uv$ from the set of all pairs of involutions into G. Each element $x \in G$ is assigned to $i(x)$ pairs. Since $i(1) = |G{:}H|$ and $i(x) = k$ for $x \in K^{\#}$, the $|G{:}H|(k - 1) + 1$ elements of $K^G = H^G$ are assigned to $|G{:}H| + |G{:}H|(k - 1)k$ pairs.

Hence there exists an element $x \notin H^G$ such that

$$\begin{aligned} i(x) &\geq \frac{|G{:}H|^2 - |G{:}H| - |G{:}H|(k - 1)k}{|G| - 1 - |G{:}H|(k - 1)} \\ &> \frac{|G{:}H| - 1 - (k - 1)k}{|H| - (k - 1)} \\ &= \frac{(2k + \varepsilon)(k + \varepsilon) - 1 - (k - 1)k}{2k - (k - 1)} \\ &= \frac{k^2 + 3k\varepsilon + k}{k + 1} \\ &= k + 3\varepsilon \frac{k}{k + 1}. \end{aligned}$$

In the following, F denotes the centralizer of a suitable element $x \notin H^G$ for which $i(x) > k + 3\varepsilon k/(k + 1)$ and $x^t = x^{-1}$.

We let $M = N_G(F)$, $f = |F|$, and $n = |M{:}F|$.

3.1. (i) $F = C_G(a)$ *and* $a^t = a^{-1}$ *for all* $a \in F^{\#}$,

(ii) $M = F(K \cap M)$,

(iii) $F \cap M^g = 1$ *for all* $g \in G - M$,

(iv) $f \geq k - 1$ *if* $\varepsilon = -1$, *and* $f \geq k + 3$ *if* $\varepsilon = 1$.

Proof. $x \notin H^G$ implies $F \cap H^G = 1$, as remarked above. Hence all involutions of M are fixed-point-free on F, and thus invert every element of F. In particular, F is abelian. For the same reason, $C_G(a)$ is abelian for all $a \in F^{\#}$. This proves (i). For (ii) note that the product of any two involutions of M lies in $C_G(F) = F$. Clearly, (i) forces F to be a Hall subgroup of

G, and implies $F \cap F^g = 1$ for $g \in G - M$; this gives (iii). From (i) we also conclude $f = i(x)$; since f is odd, (iv) is immediate.

3.2. *One of the following holds*:
(i) $|G:H| = f(k+1)$ *and* $|G:M| = f(2k/n) - f + 1$,
(ii) $|G:H| - |G:M| \leq f(k+1) - (f(2k/n) - f + 1)$ *and*
$$|G:M| \geq f(2k/n) + 1.$$

Proof M contains f involutions. Let u be one of them. Then $C_M(u)$ is conjugate to $K \cap M$ and has order n. Let $g \in C_G(u) - C_M(u)$.

Since $F \cap M^g = 1$, and all subgroups of K are normal in H, it follows that $C_M(u) = M \cap M^g$. Note that $M^e = M^g$ for all $e \in Mg$. We conclude that the coset Mg contains n elements of $C_G(u)$, but no element commuting with any other involution of M. In addition, any involution $y \in Mg$ centralizes u because y normalizes $M \cap M^y = M \cap M^g$.

Hence there are $f(2k - n)$ elements outside M, among them fk involutions, commuting with an involution of M; they fall in $f(2k - n)/n$ cosets of M, which contain no further involutions. In addition, we have the coset M.

If there are no more cosets of M, then (i) holds. Otherwise, there are at least f more cosets because F (in fact M) acts without fixed-points on those additional cosets. This yields $|G:M| \geq f(2k/n) + 1$.

An additional coset can contain only one involution, as any involution inverting a non-identity element of M commutes with some involution in M. Hence $|G:H| - f(k+1)$, the number of involutions in the additional cosets, is not larger than the number of those cosets, which is $|G:M| - (f(2k/n) - f + 1)$.

3.3. *Assume case* (i) *of* (3.2). *Then the conclusion of the theorem holds with* $Q = F$ *and* $D = K$.

Proof. $f(k+1) = |G:H| = (2k+\varepsilon)(k+\varepsilon)$ implies
$$\varepsilon = 1 \quad \text{and} \quad f = 2k + 1 = q.$$
We have
$$|G:M| = f(2k/n) - f + 1 = (2k+1)(2k/n) - 2k = (k+1)2k/n + 2k^2/n - 2k.$$
On the other hand, $|G:H| = f(k+1)$ yields $|G:M| = (2k/n)(k+1)$.

Hence $2k^2/n - 2k = 0$, i.e. $k = n$.

Thus $N_G(F) = M = FK$ and $|K| = (q-1)/2$. Now the conditions (1)–(4) in the theorem are clear.

3.4. *Without loss*, $f = k - 1$, $n = 2$, *and* $\varepsilon = -1$.

Proof. By (3.3), we may assume that case (ii) of (3.2) holds.

If $|M| \leq |H|$, then $2f \leq nf = |M| \leq |H| = 2k$ together with (3.1.iv) yields the assertion.

Thus assume $|M|/|H| - 1 > 0$. Then the two inequalities in (3.2.ii) yield

$$\begin{aligned} f(2k/n)(nf/2k - 1) &< |G:M|(|M|/|H| - 1) \\ &= |G:H| - |G:M| < f(k+1) - f(2k/n) + f. \end{aligned}$$

This gives $f < k + 2$. Hence $\varepsilon = -1$ and $f \geq k - 1$, by (3.1.iv). Then $f = k - 1$ because $k + 1$ does not divide $|G:H| = (2k-1)(k-1)$.

Finally, $n = |K \cap M|$ divides both $k = |K|$ and $|F| - 1 = k - 2$, since $K \cap M$ is a subgroup of K acting fixed-point-freely on F. Thus $n = 2$.

3.5. (i) *The set $Y = G - H^G - F^G$ consists of two conjugate classes of G;*
(ii) *if $y \in Y$, then y is not conjugate to y^{-1};*
(iii) *if $y \in Y$, then $C_G(y)$ has order $2k - 1$ and is a p-group, p a prime.*

Proof. By (3.4),

$$|G| = (2k-1)(k-1)\cdot 2k, \quad |F| = k - 1, \quad \text{and} \quad |N_G(F)| = 2(k-1).$$

Hence

$$\begin{aligned} |Y| &= |G| - |G:H|(k-1) - |G:N_G(F)|(f-1) - 1 \\ &= (2k-1)(k-1)\cdot 2k - (2k-1)(k-1)(k-1) \\ &\qquad - (2k-1)k(k-2) - 1 \\ &= (2k-1)(2k^2 - 2k - k^2 + 2k - 1 - k^2 + 2k) - 1 \\ &= (2k-1)(2k-1) - 1 \\ &= 4k(k-1). \end{aligned}$$

On the other hand, if $y \in Y$, then $|y^G| = 2k(k-1)m$ with an odd integer m, because $|C_G(y)|$ divides $2k - 1$.

This yields (i) and (iii). If $y^t = y^{-1}$, then $i(y) \geq |C_G(y)| = 2k - 1$, whence $C_G(y)$ satisfies the same assumptions as F. This would imply $|C_G(y)| = 2k + 1$ or $k - 1$, see the proofs of (3.3) and (3.4), a contradiction. Now (ii) is immediate.

3.6. *Let $X \neq 1$ be a p-subgroup of G, and P a Sylow p-subgroup of $N = N_G(X)$. Then $P \lhd N = PD$ with D conjugate to a subgroup of F or K.*

Proof. Let $r \neq p$ be a prime divisor of $|N|$, and R a Sylow r-subgroup of N. By (3.5.ii), N has odd order. Since both F and K are t. i. subgroups of G, and have index 2 in their normalizer, $N_N(R)$ is conjugate to a subgroup of F or K. In particular, $N_N(R)$ is abelian. Then Burnside's transfer theorem yields a normal complement of R in N.

This proves that P is normal in N, and that N/P is abelian. Now the Frattini argument gives $N = PN_N(R)$.

3.7. *A Sylow p-subgroup of G is disjoint from its conjugates.*

Proof. Let X be maximal among the intersections of two distinct Sylow

p-subgroups. Then $N_G(X)$ has no normal Sylow p-subgroup. By (3.6), $X = 1$.

3.8. *The conclusion of the theorem holds with Q a suitable Sylow p-subgroup of G, and $D = F$.*

Proof. Choose a subgroup Q of order $2k - 1 = q$ in such a way that $N_G(Q) = QD$ with D a subgroup of F or K; see (3.6).

By (3.7), elements of Q conjugate in G are already conjugate in $N_G(Q)$. Then (3.5) implies that Q is abelian and that

$$|D| = (q-1)/2 = k - 1 = |F|.$$

This completes the proof.

References

1. H. Bender, *Finite groups with large subgroups*, Illinois J. Math. vol. 18 (1974), pp. 223–228 (this issue).
2. R. Brauer, M. Suzuki, and G. E. Wall, *A characterization of the one-dimensional unimodular groups over finite fields*, Illinois J. Math., vol. 2 (1958), pp. 718–745.
3. D. Gorenstein, *Finite groups*, Harper and Row, New York, 1968.
4. N. Ito, *Frobenius and Zassenhaus groups*, Lecture notes. University of Illinois at Chicago Circle, 1969.
5. M. Suzuki, *Two characteristic properties of (ZT)-groups*, Osaka Math. J., vol. 15 (1963), pp. 143–150.
6. H. Zassenhaus, *Kennzeichnung endlicher linearer Gruppen als Permutationsgruppen*, Hamb. Abh., vol. 11 (1936), pp. 17–40.

Universität
Kiel, West Germany