A theorem on factorizable groups

By NOBORU ITO in Chicago (Illinois, U.S.A.) *)

To Professor Ladislaus Rédei on his seventieth birthday

The purpose of this note is to prove the following theorem.

Theorem. *Let a finite group $\mathfrak{G}$ be the product of two subgroups $\mathfrak{A}$ and $\mathfrak{B}$ such that* (1) *$\mathfrak{A}$ and $\mathfrak{B}$ have non-trivial centers*; (2) *if B is a non-identity element of $\mathfrak{B}$, then the centralizer of B in $\mathfrak{G}$ is contained in $\mathfrak{B}$. Then $\mathfrak{G}$ is not simple.*

Remark. Take $\mathfrak{G}$, $\mathfrak{A}$ and $\mathfrak{B}$ as the icosahedral group, a Sylow 5-subgroup and a tetrahedral subgroup respectively. Then all the conditions in the theorem except (1) to $\mathfrak{B}$ are satisfied. This shows that (1) applied to $\mathfrak{A}$ and (2) are not sufficient to imply the non-simplicity of $\mathfrak{G}$.

Notation. Let $\mathfrak{X}$ be a finite group. $Z(\mathfrak{X})$ denotes the center of $\mathfrak{X}$. For a prime p, $\mathfrak{X}_p$ denotes a Sylow p-subgroup of $\mathfrak{X}$. Let $\mathfrak{X}$ be a subset of $\mathfrak{X}$. $|\mathfrak{Y}|$ denotes the number of elements in $\mathfrak{Y}$. Ns $\mathfrak{Y}$ denotes the normalizer of $\mathfrak{Y}$ in $\mathfrak{X}$. Cs $\mathfrak{Y}$ denotes the centralizer of $\mathfrak{Y}$ in $\mathfrak{X}$. If $\mathfrak{Y}=\{Y\}$, Cs $Y=$Cs $\mathfrak{Y}$. For $X\in\mathfrak{X}$, $[X]$ denotes the conjugacy class of $\mathfrak{X}$ containing X. $\mathfrak{E}=\{E\}$ denotes the identity subgroup of $\mathfrak{X}$. Let $\mathscr{X}$ be a set of irreducible characters of $\mathfrak{X}$. Then $\Gamma(\mathscr{X})$ denotes the ring of rational integral linear linear combinations λ of characters in $\mathscr{X}$. $\Gamma_0(\mathscr{X})$ denotes the subring of $\Gamma(\mathscr{X})$ consisting of all λ with $\lambda(E)=0$. Let φ be a character of a subgroup $\mathfrak{Y}$. Then φ^* denotes the character of $\mathfrak{X}$ induced by φ. $1_{\mathfrak{X}}$ denotes the principal character of $\mathfrak{X}$.

Proof. Assume that the theorem is false. Let $\mathfrak{G}$ be a simple group satisfying all the conditions in the theorem.

(i) By a theorem of BURNSIDE ([3], p. 491) $|\mathfrak{B}|$ is not a prime power.

(ii) $\mathfrak{A}\cap\mathfrak{B}=\mathfrak{E}$. In fact, otherwise take $B(\neq E)\in\mathfrak{A}\cap\mathfrak{B}$. Then $Z(\mathfrak{A})\leqq$Cs $B\leqq\mathfrak{B}$. This shows that $\mathfrak{B}$ contains a normal subgroup of $\mathfrak{G}$ containing $Z(\mathfrak{A})$. This is a contradiction.

*) This work was partially supported by NSF GP 9584.

(iii) $\mathfrak{A}$ and $\mathfrak{B}$ are Hall subgroups of $\mathfrak{G}$. In fact, otherwise, let p be a common prime divisor of $|A|$ and $|\mathfrak{B}|$. We may assume that $\mathfrak{G}_p=\mathfrak{A}_p\mathfrak{B}_p$ ([3], p. 676). Then $\mathfrak{A}_p\neq\mathfrak{E}\neq\mathfrak{B}_p$. Take $P(\neq E)\in\mathfrak{B}_p$. Then $Z(\mathfrak{G}_p)\subseteqq \mathrm{Cs}\, P\subseteqq\mathfrak{B}$. Take $P^*(\neq E)\in Z(\mathfrak{G}_p)$. Then $\mathfrak{A}_p\subseteqq\mathfrak{G}_p\subseteqq \mathrm{Cs}\, P^*\subseteqq\mathfrak{B}$. This contradicts (ii).

(iv) $\mathfrak{B}$ is a T.I. set. Namely if $X^{-1}\mathfrak{B}X\neq\mathfrak{B}$ for $X\in\mathfrak{G}$, then $X^{-1}\mathfrak{B}X\cap\mathfrak{B}=\mathfrak{E}$. In fact, otherwise, take $B(\neq E)\in X^{-1}\mathfrak{B}X\cap\mathfrak{B}$. Then $Z(X^{-1}\mathfrak{B}X)\subseteqq \mathrm{Cs}\, B\subseteqq\mathfrak{B}$. So $X^{-1}\mathfrak{B}X\subseteqq \mathrm{Cs}\, Z(X^{-1}\mathfrak{B}X)\subseteqq\mathfrak{B}$. Thus $X^{-1}\mathfrak{B}X=\mathfrak{B}$. This is a contradiction.

(v) $\mathrm{Ns}\,\mathfrak{B}$ is a Frobenius group with $\mathfrak{B}$ the kernel. In fact, if $\mathrm{Ns}\,\mathfrak{B}=\mathfrak{B}$, then by (iv) and by a theorem of FROBENIUS ([3], p. 495) $\mathfrak{G}$ is not simple. Thus $\mathrm{Ns}\,\mathfrak{B}\neq\mathfrak{B}$. Let $\mathfrak{C}$ be a complement of $\mathfrak{B}$ in $\mathrm{Ns}\,\mathfrak{B}$ ([3], p. 126). Then by the condition (2) on $\mathfrak{B}$ and by (iii) no element $(\neq E)$ of $\mathfrak{C}$ commutes with an element $(\neq E)$ of $\mathfrak{B}$. Hence we get our assertion ([3], p. 497).

By a theorem of THOMPSON ([3], p. 499) $\mathfrak{B}$ is nilpotent.

(vi) By (iv) and (v) we are in a position to apply the theory of exceptional characters. Let $\mathcal{S}$ be the set of irreducible characters of $\mathrm{Ns}\,\mathfrak{B}$ which do not have $\mathfrak{B}$ in their kernel. Then the induction map $*$ is a linear isometry from $\Gamma_0(\mathcal{S})$ into the character ring of $\mathfrak{G}$ such that $\lambda^*(E)=0$ for $\lambda\in\Gamma_0(\mathcal{S})$ ([2], (23. 1), (25. 4)). If $|\mathfrak{C}|+1 = |\mathfrak{B}|$, then $|\mathfrak{B}|$ must be a prime power. This contradicts (i). Hence ($\mathfrak{C}$, *) is coherent ([2], (31. 6)). Namely $*$ can be extended to a linear isometry $^{\mathscr{C}}$ from $\Gamma(\mathcal{S})$ into the character ring of $\mathfrak{G}$.

(vii) Let χ be an irreducible component of $1_{\mathfrak{A}}^*$. Assume that $\chi\neq 1_{\mathfrak{G}}$ and that $\pm\chi\notin\mathcal{S}^{\mathscr{C}}$. Then there exists a rational integer c such that $\chi(B)=c$ for every $B(\neq E)\in\mathfrak{B}$. We show that

$$\chi(E) = |\mathfrak{B}|-1.$$

In fact, since

$$\sum_{B\in\mathfrak{B}}\chi(B)1_{\mathfrak{B}}(B) = \chi(E)+c(|\mathfrak{B}|-1) = m|\mathfrak{B}|,$$

where m is a non-negative integer, we obtain that

$$\chi(E)-c = (m-c)|\mathfrak{B}|.$$

Since $\chi(E)\leqq|\mathfrak{B}|-1$ and since $\mathfrak{G}$ is simple, we see that

$$\chi(E)>|c|,\ 0>c,\ m-c = 1,\ m=0 \quad\text{and}\quad c=-1.$$

Thus $\chi(E) = |\mathfrak{B}|-1$. This implies that the permutation representation of $\mathfrak{G}$ induced by $\mathfrak{A}$ is doubly transitive ([2], (9. 6)). Here we notice that $1_{\mathfrak{A}}^*$ is the character of this permutation representation.

Now let A be an element of $Z(\mathfrak{A})$ of order p, a prime. Then since $1_{\mathfrak{A}}^*$ is doubly transitive, $1_{\mathfrak{A}}^*(A)=1$. If $X^{-1}AX\in\mathfrak{A}$ for $X\in\mathfrak{G}$, then X fixes the "point" $\mathfrak{A}$. Hence $X\in\mathfrak{A}$ and $X^{-1}AX=A$.

Suppose that there exists a q-subgroup $\mathfrak{Q}$ of $\mathfrak{G}$ such that $q \neq p$ and A induces a non-trivial automorphism of $\mathfrak{Q}$. If q divides $|\mathfrak{B}|$, then we may assume that $\mathfrak{Q} \subseteqq \mathfrak{B}$: A normalizes Cs $\mathfrak{Q}$. Let $\mathfrak{R}$ be the Sylow q-complement of $\mathfrak{B}$. Then since $\mathfrak{B} \supseteqq \supseteqq \mathrm{Cs}\,\mathfrak{Q} \supseteqq \mathfrak{R}$, A normalizes $\mathfrak{R}$ and hence $\mathfrak{B}$. Then Ns $\mathfrak{B}$ contains a normal subgroup of $\mathfrak{G}$ containing $\mathfrak{A}$. This is a contradiction. Therefore q divides $|\mathfrak{A}|$. A normalizes Cs $\mathfrak{Q}$. Since Cs $\mathfrak{Q}$ contains some conjugate of $Z(\mathfrak{A})$, there exists a Sylow p-subproup $\mathfrak{D}(\neq \mathfrak{E})$ of Cs $\mathfrak{Q}$ such that A normalizes $\mathfrak{D}$. Obviously $A \notin \mathfrak{D}$. $\mathfrak{D}$ contains some conjugate $Y^{-1}AY$ of A. Thus $A^{-1}Y^{-1}AY \neq E$ is a p-element. Since $A \in Z(\mathfrak{A})$, we have that

$$[A^{-1}][A] = |\mathfrak{B}|[E] + r[A^{-1}Y^{-1}AY],$$

where r is a positive integer.[1]) Since $\chi(A)=0$, this implies that $\chi(A^{-1}Y^{-1}AY)$ is a negative integer. Hence $l_{\mathfrak{A}}^*(A^{-1}Y^{-1}AY) \leqq 0$. Since $A^{-1}Y^{-1}AY$ is a p-element, this is a contradiction. Therefore there exists no subgroup such as $\mathfrak{Q}$. Hence by a theorem of SHULT ([4]) $\mathfrak{G}$ is not simple. Thus for every irreducible component $\zeta \neq l_{\mathfrak{G}}$ of $l_{\mathfrak{A}}^*$ we must have $\pm\zeta \in \mathscr{S}^{\mathscr{C}}$.

(viii) Now we can follow an arguement due to Burnside as follows ([1], § 151). Put $\mathscr{S} = \{\zeta_i,\ 1 \leqq i \leqq s\}$ with $s = |\mathscr{S}|$. If $s=2$, then $|\mathfrak{B}|$ is a prime power against (i). Hence $s \geqq 3$. By ([2], (23. 1)) and by the coherence of $(\mathscr{S}, {}^*)$ we have the following equation:

(a) $$(e_j\zeta_i - e_i\zeta_j)^* = e_j\zeta_i^* - e_i\zeta_j^* = e_j\zeta_i^{\mathscr{C}} - e_i\zeta_j^{\mathscr{C}},$$

where $1 \leqq i, j \leqq s$ and $e_k = \zeta_k(E)/|\mathfrak{C}|$ for $k=1, \dots, s$. (a) implies that

$$\sum_{X \in \mathfrak{G}} 1_{\mathfrak{A}}^*(X)\left(e_j\zeta_i^{\mathscr{C}}(X) - e_i\zeta_j^{\mathscr{C}}(X)\right) = 0.$$

Therefore the decomposition of $l_{\mathfrak{A}}^*$ into its irreducible components has the following form:

(b) $$1_{\mathfrak{A}}^* = 1_{\mathfrak{G}} + m\sum_{i=1}^{s} e_i\zeta_i^{\mathscr{C}},$$

where m is a rational integer. By (b) we see that $\zeta_i^{\mathscr{C}}(E) > 0$ for all i or $\zeta_i^{\mathscr{C}}(E) < 0$ for all i.

We show that $|\zeta_j^{\mathscr{C}}(E)| \geqq \zeta_j(E)$ for all j. By (a) and by the Frobenius reciprocity theorem ([2], (9. 4)), this is obvious, if $\zeta_j^{\mathscr{C}}(E) > 0$ or if $-\zeta_j^{\mathscr{C}}$ appears as an irreducible component of ζ_j^*. Hence we may assume that $\zeta_j^{\mathscr{C}}(E) < 0$ and that $-\zeta_j^{\mathscr{C}}$ does not appear as an irreducible component of ζ_j^*. Then by (a) we see that $-\zeta_j^*$ appears as an irreducible component of ζ_i^* with the multiplicity $\zeta_i(E)/\zeta_j(E)$, where $j \neq i$. This implies that $\zeta_i(E) \geqq \zeta_j(E)$ and that $|\zeta_j^{\mathscr{C}}(E)| \geqq \zeta_i(E)$([2], (9. 4)).

[1]) The usefulness of this equation we owe to Professor H. WIELANDT.

Now since $\sum_{i-1}^{s} \zeta_i(E)^2 = |\mathfrak{B}|\,|\mathfrak{C}| - |\mathfrak{C}|$, (b) implies that $|m|=1$ and $|\zeta_i^{\mathfrak{C}}(E)| = \zeta(E_i)$. Then since $s \geqq 3$, we obtain that $\zeta_i^{\mathfrak{C}}(E) > 0$ and that $\zeta_i^{\mathfrak{C}}$ restricted to Ns $\mathfrak{B}$ is equal to ζ_i. $(i=1, \ldots, s)$.

By a) we obtain that

$$e_j \zeta_i^{\mathfrak{C}}(A) = e_i \zeta_j^{\mathfrak{C}}(A)$$

for every element A of $\mathfrak{G}$ which is not conjugate to some element $(\neq E)$ of $\mathfrak{B}$. Since the number of characters ζ_i with $\zeta_i(E) = |\mathfrak{C}|$ equals $((\mathfrak{B}:\mathfrak{B}')-1)/|\mathfrak{C}|$, where $\mathfrak{B}'$ denotes the commutator subgroup of $\mathfrak{B}$, we may assume that $\zeta_1(E) = \zeta_2(E) = |\mathfrak{C}|$. Then

$$\zeta_i^{\mathfrak{C}}(A) = e_i \zeta_1^{\mathfrak{C}}(A)$$

for all i. Now by (b) be obtain that

$$\text{(c)} \qquad 1_{\mathfrak{A}}^*(A) = 1 + t\zeta_1^{\mathfrak{C}}(A)$$

for every element A of $\mathfrak{G}$ which is not conjugate to some element $(\neq E)$ of $\mathfrak{B}$, where $t = (|B|-1)/|\mathfrak{C}|$. Let $\mathfrak{G}(i)$ be the set of elements G in $\mathfrak{G}$ such that $l_{\mathfrak{A}}^*(G) = i$. Since $t \geqq s \geqq 3$, by (c) we see that $\mathfrak{G}(0)$ coincides with the set of elements of $\mathfrak{G}$ which are conjugate to elements $(\neq E)$ of $\mathfrak{B}$. Then we have that

$$\sum_{B \in \mathfrak{G}(0)} \zeta_1^{\mathfrak{C}}(B) = (\mathfrak{A}:\mathfrak{C}) \sum_{B \in \mathfrak{B}-\{E\}} \zeta_1(B) = -|\mathfrak{A}|$$

and that

$$\sum_{B \in \mathfrak{G}(0)} \zeta_1^{\mathfrak{C}}(B)\overline{\zeta_2^{\mathfrak{C}}(B)} = (\mathfrak{A}:\mathfrak{C}) \sum_{B \in B-\{E\}} \zeta_1(B)\overline{\zeta_2(B)} = -|\mathfrak{A}|\,|\mathfrak{C}|.$$

Finally, since $\sum_{G \in \mathfrak{G}} \zeta_1^{\mathfrak{C}}(G) = \sum_{G \in \mathfrak{G}} \zeta_1^{\mathfrak{C}}(G)\overline{\zeta_2^{\mathfrak{C}}(G)} = 0$, by (c) we obtain that

$$\text{(d)} \qquad -|\mathfrak{A}| + |\mathfrak{G}(t+1)| + 2|\mathfrak{G}(2t+1)| + \ldots + |\mathfrak{C}| = 0$$

and

$$\text{(e)} \qquad -|A|\,|\mathfrak{G}| + |\mathfrak{G}(t+1)| + 4|\mathfrak{G}(2t+1)| + \ldots + |\mathfrak{C}|^2 = 0.$$

(d) and (e) enforce $\mathfrak{G}(t+1)$, $\mathfrak{G}(2t+1)$, ... to be empty. Hence $|\mathfrak{A}| = |\mathfrak{C}|$ and $\mathfrak{A} = \mathfrak{C}$. This is a contradiction.

Bibliography

[1] W. Burnside, *Theory of groups of finite order* (Cambridge, 1911).
[2] W. Feit, *Characters of finite groups* (New York, 1967).
[3] B. Huppert, *Endliche Gruppen.* I (Berlin—Heidelberg—New York, 1967).
[4] E. Shult, Some analogues of Glauberman's Z^*-theorem, *Proc. Amer. Math. Soc.*, **17** (1966), 1186—1190.

DEPARTMENT OF MATHEMATICS
UNIVERSITY OF ILLINOIS AT CHICAGO CIRCLE

(Received October 14, 1970)