Browning

Normal generators of finite groups

Defn. Say H is an "inner" G-group if H is a G-group such that the image of

say "left"

$G \longrightarrow \mathrm{Aut}\, H$ contains the inner-automorphisms of H. Assume H is finite.

1) Then if K is a subgroup of H, such that K is invariant under the action of G, K must be normal in H and so H/K is not only just a G-set but also in fact an inner G-group. Also K must be inner.

2) So H must have a composition series

$$H = H_0 \rhd H_1 \rhd H_2 \rhd \cdots \rhd H_m = (1)$$

where each H_{i+1} is a maximal (proper) G-invariant subgroup of H_i.

For such a series each H_i/H_{i+1} must not have any proper G-invariant subgroups other than (1).

3) If S ~~has~~ is an inner G-group which has no proper G-invariant subgroups other than (1) then any element of $S \setminus (1)$ generates S as a G-group.

4) If H is an inner G-group and if $(a_1, \ldots, a_n)$ ~~and $(b_1, \ldots, b_n)$~~ is a sequence of elements of H which generate H as a G-group then an elementary G-transformation

$$(a_1, \ldots a_n) \longrightarrow (a_1', \ldots, a_n')$$

is one of the following

I, permutation: $a_i \longmapsto a_{\pi(i)}$

II. inversion: $a_i \longmapsto a_i^{-1}$, $a_j \longmapsto a_j$, $j \neq i$.

III. multi: $a_i \longmapsto a_i a_j$, $j \neq i$, $a_k \longmapsto a_k$, $k \neq i$

IV. G-action: $a_i \longmapsto g \cdot a_i$, $a_j \longmapsto a_j$, $j \neq i$.

Say a G-<u>transformation</u> is a composition of these; write $(\underset{\sim}{a}) \xrightarrow{(G)} (\underset{\sim}{b})$. Then $(b_1, \ldots, b_n)$ necessarily also is a G-generating set for H, clearly.

5) <u>Lemma</u>. Suppose H has a G-generating set having n elements, say $(t_1, \ldots, t_n)$, where H is a finite inner G-group. Suppose $(a_1, \ldots, a_k)$ is a G-generating set with $k > n$. Then

$$(a_1, \ldots, a_k) \xrightarrow{(G)} (t_1, \ldots, t_n, 1, \ldots, 1).$$

<u>Proof</u>. By induction on the minimum length m of a composition series for H as in (2).

<u>Case m = 1</u>. H is then "G-simple" as in (3), so n must be 1 and $k > 1$. We may suppose $a_1 \neq 1$. Then

$$(a_1, a_2, \ldots) \xrightarrow{(G)} (a_1, \underbrace{1, \ldots}_{\text{all } 1\text{'s}})$$

because (a_1) already generates H as a G-group. Then

$$(a_1, 1, \ldots 1) \xrightarrow{(G)} (a_1, t_1, 1, \ldots)$$
$$\longrightarrow (t_1, a_1, 1 \ldots)$$
$$\longrightarrow (t_1, 1, 1, \ldots)$$

<u>Induction step</u>. Assume the Lemma holds for all such inner G-groups with composition series of length $m-1$. Let H be as in (2) with $K = H_{m-1}$ the last nontrivial term. Then by assumption the Lemma holds for

H/K. If $(\tau_1, \ldots, \tau_{n'})$ is a sequence of G-generators for H/K with n' minimal then certainly $n' \leq n$. So we have

$$(\bar{a}_1, \ldots, \bar{a}_k) \xrightarrow{(G)} (\tau_1, \ldots, \tau_{n'}, (1's))$$

$$(\bar{t}_1, \ldots, \bar{t}_n, (1's)) \xrightarrow{(G)} (\tau_1, \ldots, \tau_{n'}, (1's))$$

[Where $\bar{x}$ denotes x modulo K]

$$\therefore \quad (\bar{a}_1, \ldots, \bar{a}_k) \xrightarrow{(G)} (\bar{t}_1, \ldots, \bar{t}_n, (1's))$$

i.e. $$(a_1, \ldots, a_k) \xrightarrow{(G)} (t_1\alpha_1, \ldots, t_n\alpha_n, \alpha_{n+1}, \ldots, \alpha_k)$$

by mimicing the operations in H, where each α_i must lie in the normal subgroup K.

Two possibilities:

i) $\alpha_{n+1} = \cdots = \alpha_k = 1$. Then $(t_1\alpha_1, \ldots, t_n\alpha_n)$ G-generate ~~by the minimality of n, at least some $t_i\alpha_i \neq 1$~~

& so choosing any $x \in K \setminus (1)$, x can be expressed in terms of $t_1\alpha_1, \ldots t_n\alpha_n$ and operation by G so that

$$(t_1\alpha_1, \ldots, t_n\alpha_n, 1, \ldots 1) \xrightarrow{(G)} (t_1\alpha_1, \ldots, t_n\alpha_n, x, 1, \ldots 1)$$

so the case (i) ~~leads~~ reduces to the following case

ii) some α_i, $i \geq n+1$ is nontrivial. We may suppose it is α_{n+1} and call it x. x G-generates K by observation (3). So we have

$$(x, \alpha_{n+2}, \ldots) \xrightarrow{(G)} (x, 1, \ldots)$$ by

the first step and just the same way (expressing the α_i's, $i \leq n$ in terms of x & operations from G)

$$(t_1\alpha_1, \ldots, t_n\alpha_n, x, \alpha_{n+2}, \ldots) \to (t_1, \ldots, t_n, x, 1, \ldots)$$

But $(t_1, \dots, t_n)$ already G-generate so can be used to eliminate x. //.

6) <u>Definition</u>. Say $(a_1, \dots, a_k)$ is a G-generating set in <u>echelon form</u> for the finite inner G-group H if the following conditions hold:

(i) $(\underset{\sim}{a})$ is a G-generating set for H. (write $H = \langle \underset{\sim}{a} \rangle^G$)

Let $H_j = \langle a_j, \dots, a_k \rangle^G$, $j = 1, \dots, k$.

(ii) For each $j = 1, \dots, k-1$ require that H_{j+1} be minimal in H_j among all G-subgroups $K (\subset H_j)$ with the property that: K needs at most $k-j$ generators, and $\langle a_1, \dots, a_{j-1}, x, K \rangle^G = H$ for some $x \in H_j$

redundant, I think $\{$ (iii) $\langle a_j \rangle^G$ is maximal in H_j among all $\langle x \rangle^G$ such that $\langle a_1, \dots, a_{j-1}, x, H_{j+1} \rangle^G = H$.

7) Note that G-generating sets in echelon form exist.

8) <u>Theorem</u>. Say H, $H_1 = H$, $H_2, \dots, H_k$, $a_1, \dots, a_k$ are as in (6). Suppose $(b_1, \dots, b_\ell)$ is any G-generating set for H. Then

i) if $\ell > k$, $(b_1, \dots, b_\ell) \xrightarrow{(G)} (a_1, \dots, a_k, 1's)$

ii) if $\ell \le k$ $(b_1, \dots, b_\ell) \xrightarrow{(G)} (a_1, \dots, a_{\ell-1}, x)$ where $x \in H_\ell$, $\langle x \rangle^G = H_\ell$ (x depends on $(b_1, \dots, b_\ell)$)

Proof. We can reduce to the case (ii) by extending $(a_1, \ldots, a_k)$ by 1's if necessary. So assume $\ell \leq k$.

The proof is by induction on ℓ.

If $\ell = 1$ then for $k=1$ take $x = b_1$, while if $k > 1$ we must have $H_2 = (1)$ by (6) condition (ii). Thus $(a_1, a_2, \ldots) = (a_1, 1, 1, \ldots)$ in this case and $\langle a_1 \rangle^G = H = \langle b_1 \rangle^G$ so again take $x = b_1$.

Assume the Theorem for $\ell - 1$.

Assume $\ell \geq 2$. Factoring by H_2 obtain

$(\bar{b}_1, \ldots, \bar{b}_\ell)$, $(\bar{a}_1, 1, \ldots, 1)$

& by lemma (5) have

$$(\bar{b}_1, \ldots, \bar{b}_\ell) \xrightarrow{(G)} (\bar{a}_1, 1, \ldots, 1) \text{ in } H/H_2.$$

Lift to get (each $\beta_i \in H_2$)

$$(b_1, \ldots, b_\ell) \xrightarrow{(G)} (a_1\beta_1, \beta_2, \ldots, \beta_\ell).$$

By 6(ii) we must have $\langle \beta_2, \ldots, \beta_\ell \rangle^G = H_2$ (since $\langle \beta_2, \ldots, \beta_\ell \rangle^G \subset H_2$ & $\langle \beta_2, \ldots, \beta_\ell, \underset{(\ell+1)}{1}, \ldots, \underset{(k)}{1} \rangle \subset H_2$ and H_2 is minimal with respect to existence of $k-1$ generators and an additional generator x ∋ $\langle x, H_2 \rangle^G = H$. Here x could be $a_1\beta_1$)

Then $\beta_2, \ldots, \beta_\ell$ can be used to eliminate the β_1 appearing in $a_1\beta_1$

So $(b_1, \ldots, b_\ell) \rightarrow (a_1, \beta_2, \ldots, \beta_\ell)$

& by induction $(\beta_2, \ldots, \beta_\ell) \rightarrow (a_2, \ldots, a_{\ell-1}, x)$ with $x \in H_\ell$.

(It is clear that $(a_2, \ldots, a_k)$ is in echelon form)

9) <u>Corollary</u>. With H, $(a_1, \ldots, a_k)$ as in (6) say a_n is the last nontrivial a_i. Then $(a_1, \ldots, a_n)$ is a G-generating set for H of minimum cardinality.

<u>Proof</u>: Let $(t_1, \ldots, t_m)^G = H$, m smallest.

Applying the Theorem $\exists$ $x \in H_m$ $\ni$ $\langle a_1, \ldots, a_{m-1}, x\rangle^G = H$,

where $\langle x\rangle^G = H_m \doteq \langle a_m, (a_{m+1}, \ldots, a_k)\rangle^G$.

$(k \geq m)$

But then by (6 iii), as H_{m+1} could be (1) & H_{m+1} is minimal $\therefore$ $H_{m+1} = 1$ and $a_{m+1} = a_{m+2} = \ldots = a_k = 1$.

So certainly $n = m$.

10) Corollary to (5): If $\langle x_1, \ldots, x_n ; r_1, \ldots, r_m\rangle$ is the trivial group and $F = F(x_1, \ldots x_n) \twoheadrightarrow G$ where G is finite <u>then</u>

~~$(\bar{x}_1, \ldots, \bar{x}_n) \cdots (\bar{r}_1, \ldots, \bar{r}_n)$~~

~~$(x_1, \ldots, x_n) \not\rightarrow (r_1, \ldots, r_n)$ by () transformations~~

$(\bar{x}_1, \ldots, \bar{x}_n) \xrightarrow{(G)}\!\!\!\!\!\!/\ \ (\bar{r}_1, \ldots, \bar{r}_n)$

$\overset{(\text{by } (5))}{\Longrightarrow}$ G can't be normally generated by $\leq n-1$ elements, so $n =$ min. no. of generators <u>and</u> of normal generators

$\Longleftrightarrow$ $Ab\,G$ can't be generated by $\leq n-1$ elements

Proof: $(\Rightarrow)$: Say $Ab\,G$ can be generated by $ab\,y_1, \ldots, ab\,y_{n-1}$. We can use unimodular transformations to affect:

$(ab\,\bar{x}_1, \ldots, ab\,x_n) \longrightarrow (ab\,y_1, \ldots, ab\,y_{n-1}, ab\,1)$.

Thus we can assume $\cancel{ab}\,\bar{x}_i = \cancel{ab}\,y_i$,
$1 \le i \le n-1$, $ab\,\bar{x}_n = 1$.

~~The~~ Let K be the normal subgroup of G generated by $\bar{x}_1, \dots, \bar{x}_{n-1}$.
We assume G can't be normally generated by $n-1$ elements so that $G \ne K$.
but $G/K = (\bar{x}_n)$ is cyclic $\therefore$ commutative,
$\therefore$ $\bar{x}_n \notin [G, G]$ $\therefore$ $ab\,\bar{x}_n \ne 1$ contradiction.

($\Leftarrow$) Clear since ~~also~~ the following inequalities hold

min. no. of generators of $Ab\,G$
$\le$ min. no. of normal generators of G
$\le$ min. no of ordinary generating set for G.

II) Therefore if $(x_1, \dots, x_n) \not\to (r_1, \dots, r_m)$ (by Q-transformations) is to be detected in a finite group G, G must have the properties

i) min. no. of gen.s of $Ab\,G$ = min no. for G

ii) $G^{(n)}$ is ~~exactly~~ never trivial
where $G^{(n)} = [G^{(n-1)}, G^{(n-1)}]$, $G^{(0)} = G$.
(result of note to Joan Birman)