125. Note on Groups with Involutions.

By Masayoshi NAGATA.
Nagoya University.

(Comm. by Z. SUETUNA, M.J.A., Dec. 12, 1952.)

Let G be a group with an involution under which only the identity is invariant. As is well known, if G is a Lie group then G is abelian. So, a question arises: Is such G always abelian? But it is not valid as will be shown in the following.

The main purpose of the present note is to give some sufficient conditions for such G to be abelian.

Theorem. *Let G be a group with an involution σ for which it holds that if $g^\sigma=g(g\in G)$ then $g=1$. Then G is abelian if G satisfies one of the following conditions:*

a) Every element of G is of finite order[1][2].

b) For every element g of G, there exists an element h of G such that $g=h^2$ and, furthermore, when $g=(k^\sigma)^{-1}k^{-1}k^\sigma k$ for some $k\in G$ (in this case it is evident that $g^\sigma=g^{-1}$), there exists an element h of G such that $h^\sigma=h^{-1}$, $g=h^2$[3].

c)[4] *For an arbitrary element g of G, the subgroup generated by g and g^σ is nilpotent.*

Proof. We have only to prove that $g^\sigma=g^{-1}$ for any element g of G.

I) We first prove the case a). Set $a=g^{-1}g^\sigma$. Then it is evident that $a^\sigma=a^{-1}$. Therefore the order n of a is odd: Indeed, if $a^{2m}=1$ then $a^m=1$ because $(a^m)^\sigma=a^{-m}=a^m$. Taking a natural number d such that $2d\equiv1$ (mod. n), we set $b=a^d$, $c=gb$. Then since $b^\sigma=b^{-1}$ and $b^2=a$, we have $c^\sigma=gab^{-1}=gb=c$, which implies $c=1$. Therefore $g^{-1}g^\sigma=a=g^{-2}$, whence $g^\sigma=g^{-1}$.

II) Next we prove the case b). Set $a=hh^\sigma$, taking an element h of G such that $h^2=g$. Further we set $b=a^{-1}a^\sigma(=(h^\sigma)^{-1}h^{-1}h^\sigma h)$. By our assumption, we see, as in the proof I), that $a^\sigma=a^{-1}$. This shows $h^\sigma h=(h^\sigma)^{-1}h^{-1}$, therefore $(h^2)^\sigma=h^{-2}$, i.e., $g^\sigma=g^{-1}$.

III) Before proving the case c), we construct a non-abelian group G_0 which has an involution σ_0 as σ in our theorem and then

1) It was proved by H. Zassenhaus that if G is a finite group of odd order then G is abelian in his paper "*Kenzeichnung endlicher Gruppen als Permutations-gruppen*", Hamburg. Abhand. 11 (1936), pp. 17-43.

2) It is sufficient that $g^{-1}g^\sigma$ is of finite order for any $g\in G$.

3) For this, one of the followings is sufficient: i) g is of finite order, ii) if $h_1{}^2=h_2{}^2=g$ then $h_1{}^{-1}h_2$ is in the center of G.

4) The validity o fthis case was suggested by N. Ito.

we prove a lemma.

Example 1. Let H_0 be a free abelian group generated by y_i (i runs over all rational integers). Let G_0 be a group generated by H_0 and an element x under the relation $x^{-1}y_ix=y_{i+1}^{-1}$ (for all i).

We can define an involution σ_0, as was required, by $x^{\sigma_0}=xy_0$, $y_i^{\sigma_0}=y_i^{-1}$ (for all i).

Lemma. *Let G be a group with an involution σ as in our theorem. If the commutator group H of G is abelian, then for any element g of G the subgroup K generated by g and g^σ is a homomorphic image of G_0 in our Example 1. Further the involution σ for K is induced from σ_0.*

Proof. Set $g^{-1}g^\sigma=b_0$ and we set $g^{-i}b_0g^i=b_i$ (for all rational integers i). Then we have only to prove that $b_0b_i=b_ib_0$ for all $i<0$.

Since $b_0=g^{-1}g^\sigma$, $gb_0g^{-1}=g^\sigma b_0(g^\sigma)^{-1}$. Set $c=b_0gb_0^{-1}g^{-1}$. Then since $c\in H$, $c^\sigma=c^{-1}$. Therefore $gb_0g^{-1}b_0^{-1}=c^{-1}=c^\sigma=b_0^{-1}g^\sigma b_0(g^\sigma)^{-1}=b_0^{-1}gb_0g^{-1}$, i.e., $b_{-1}b_0=b_0b_{-1}$. Now assuming that i) $g^nb_0g^{-n}=(g^n)^\sigma b_0(g^{-n})^\sigma$ and ii) $b_{-n}b_0=b_0b_{-n}(n\geq 1)$, we prove that i)′ $g^{n+1}b_0g^{-n-1}=(g^{n+1})^\sigma b_0(g^{-n-1})^\sigma$ and ii)′ $b_{-n-1}b_0=b_0b_{-n-1}$.

i)′: $(g^{n+1})^\sigma b_0(g^{-n-1})^\sigma=g^\sigma(g^n)^\sigma b_0(g^{-n})^\sigma(g^{-1})^\sigma=gb_0g^nb_0g^{-n}(b_0^{-1}g^{-1})$ (by i))
$=g^{n+1}b_0g^{-n-1}$ (by ii)).

ii)′: Set $d=b_0g^{n+1}b_0^{-1}g^{-n-1}$. Then since $d\in H$, $d^\sigma=d^{-1}$. Therefore $g^{n+1}b_0g^{-n-1}b_0^{-1}=d^{-1}=d^\sigma=b_0^{-1}(g^{n+1})^\sigma b_0(g^{-n-1})^\sigma=b_0^{-1}g^{n+1}b_0g^{-n-1}$, i. e., $b_{-n-1}b_0=b_0b_{-n-1}$.

IV) Now we prove the case c). We have only to prove that the subgroup K generated by g and g^σ is abelian. Thus we may assume that $G=K$. Then since G is nilpotent, we may assume that the commutator group of G is abelian. Thus, by our lemma, there exists a normal subgroup N of G_0, in our Example 1, such that $G\cong G_0/N$, where σ is induced from σ_0.

Since $x^{-1}y_i^{-1}xy_i=y_iy_{i+1}$, $x^{-1}(y_iy_{i+1})^{-1}xy_iy_{i+1}=y_iy_{i+1}^2y_{i+2}$, $\cdots x^{-1}(y_iy_{i+1}^{c_{1,n}}y_{i+2}^{c_{2,n}}\cdots y_{i+r}^{c_{r,n}}\cdots y_{i+n-1}^{c_{n-1,n}}y_{i+n})^{-1}xy_iy_{i+1}^{c_{1,n}}y_{i+2}^{c_{2,n}}\cdots y_{i+n}=y_iy_{i+1}^{c_{1,n+1}}\cdots y_{i+r}^{c_{r,n+1}}\cdots y_{i+n}^{c_{n,n+1}}y_{i+n+1},\cdots$, where $c_{r,s}=\binom{s}{r}$ (combination), the nilpotency of G implies that there exists a natural number k such that if $n=2^k$ then

$$y_iy_{i+1}^{c_{1,n}}\cdots y_{i+r}^{c_{r,n}}\cdots y_{i+n-1}^{c_{n-1,n}}y_{i+n}\in N \quad \text{(for all } i\text{)}.$$

Since for this n, $c_{1,n}$, $\cdots$, $c_{n-1,n}$ are even, we see that $b_ib_{i+n}=h_i^2$ for an element h_i of H_0N/N. Therefore $g^{2n}h$ is invariant under σ by a suitable element h of H_0N/N, which implies $g^{2n}\in H_0N/N$. Let now M be a maximal abelian subgroup containing H_0N/N. Then we have only to prove that if $a^2\in M(a\in G)$ then $a\in M$ (because $2n=2^{k+1}$). Since $a^{-1}a^\sigma\in H_0N/N$ and since $a^2\in M$ we have $c=aa^\sigma$ is in M, whence $c^\sigma=c^{-1}$. Since $aa^\sigma a=ca=ac^\sigma=ac^{-1}$, we see that $a^{-1}c^{-1}ac=c^2$, $a^{-1}c^{-2^l}ac^{2^l}=c^{2^{l+1}}$. By the nilpotency of G, we have $c^{2^r}=1$ for some r. Since $c\in M$, c must be identity, which implies $a^\sigma=a^{-1}$. The same holds for any am ($m \in M$), i.e., $(am)^{\sigma}=(am)^{-1}$. Therefore $a^{-1}m^{-1}=m^{-1}a^{-1}$, i.e., $am=ma$. This shows a is commutative with every element of M. Thus a must be in M because of the maximality of M.

Q. E. D.

V) In closing this note, we add two more examples of non-abelian groups each of which has an involution as in our theorem.

Example 2. Let G be a free group generated by two elements x and y and let σ be defined by $x^{\sigma}=y$, $y^{\sigma}=x$.

Example 3. Let G be a group generated by two elements x and y under the relation $yxy=x$[5]. Let σ be defined by $y^{\sigma}=y^{-1}$, $x^{\sigma}=x^{-1}y$.

5) We may add a more relation $x^2=1$.