RENDICONTI
del
SEMINARIO MATEMATICO
della
UNIVERSITÀ DI PADOVA

CHARLES S. HOLMES

Direct products with isomorphic lattices

Rendiconti del Seminario Matematico della Università di Padova, tome 45 (1971), p. 71-80
<http://www.numdam.org/item?id=RSMUP_1971__45__71_0>

DIRECT PRODUCTS WITH ISOMORPHIC LATTICES

CHARLES S. HOLMES *)

1. Introduction.

In [1] it was shown that if G and H are groups with isomorphic subgroup lattices, and G is the free product of subgroups A and B with amalgamated subgroup N a proper normal subgroup of A and B and if N does not have index 2 in both A and B, then G is isomorphic to H. Here we show the condition on indices is necessary.

Rottländer [2] has given examples of groups G and H which are non-isomorphic but have the same situation of subgroups. This means that there is a subgroup lattice isomorphism between the lattices of subgroups of G and H which preserves conjugacy and is strictly index preserving. It is shown here that for certain groups K the direct products $G \times K$ and $H \times K$ have a similar but weaker property in that the lattice isomorphism need not preserve conjugacy. In particular this is true, if K is abelian or K is the infinite dihedral group. When K is the infinite dihedral group, $G \times K$ is a free product with normal amalgamated subgroup of index two in both factors. That is, a free product with normal amalgamated subgroup of index two in both factors is not necessarily determined by its lattice of subgroups.

For the record we define here some of the less familiar terms used in this paper. Let G be a group. It is well known that the collection $L(G)$ of all subgroups of G is a lattice where for two subgroups A and B of G the meet of A and B is the set intersection $A \cap B$ and the join

*) Indirizzo dell'A.: Dept. of Mathematics, Miami University, Oxford, Ohio 45056, U.S.A.

of A and B is the subgroup $\langle A, B\rangle$ generated by the union $A \cup B$. For two groups G and H a lattice isomorphism from $L(G)$ onto $L(H)$ is called a projectivity from G onto H. H is called a projective image of G if there is a projectivity p from G onto H. In addition a group G is said to be determined by its subgroup lattice $L(G)$ if any projective image of G is isomorphic to G. Now let p be a projectivity from G onto H and let A, B, and C be subgroups of G. The projectivity p is said to preserve coniugacy provided pA is conjugate to pB in pC if and only if A is conjugate to B in C. Also p is strictly index preserving if the indices $[pB : pA]$ and $[B : A]$ are equal whenever A is a subgroup of B; p is index preserving when the indices are equal for cyclic B. A projectivity p from G onto H is situation preserving if p preserves coniugacy and is strictly index preserving. In this case G and H are said to have the same situation of subgroups. Throughout this paper we write $A \leq B$ if A is a subgroup of (the subgroup) B and $A \triangle B$ if A is a normal subgroup of B. By an infinite dihedral group we mean a proper free product of two groups of order two.

2. An Induction Principle.

It is easy to see that an isomorphism f from a group G onto a group H induces a projectivity from G onto H. That is, the map p from $L(G)$ onto $L(H)$ defined by $pK = fK$ for every subgroup K of G is a projectivity. Suppose now that f is a one to one map from a group G onto a group H. Certainly f induces a lattice isomorphism φ from the lattice of all subsets of G onto the lattice of all subsets of H. If p is the restriction of φ to $L(G)$, then p injects $L(G)$ into the set of all subsets of H. Thus p is a projectivity from G onto H if and only if p maps $L(G)$ onto $L(H)$.

INDUCTION PRINCIPLE. Let G and H be groups and f a map from G into H which is one to one and onto. The map f induces a projectivity from G onto H, if

a) $A \leq G$ implies $f(A) \leq H$, and

b) $B \leq H$ implies $f^{-1}(B) \leq G$.

A projectivity p induced by such a one to one and onto function f in this way is strictly index preserving if G is finite, and index preserving if G has no elements of infinite order. If G does have elements of infinite order, p is index preserving providing f restricted to any infinite cyclic subgroup C of G is an isomorphism of C into H.

3. Rottländer's Examples.

Here we study a construction (2) of classes of groups with the property that all groups in a class have the same situation of subgroups. The groups in a particular class are semi-direct products of an elementary abelian group of order p^2, where p is some prime, and a prime cyclic group of order q. More specifically any group G in this class has a representation of the form

$$G=\{a,\ b,\ c: 1=a^p=b^p=c^q=aba^{-1}b^{-1},\ cac^{-1}=a^r,\ cbc^{-1}=b^s\}$$

where $r^q \equiv s^q \equiv 1(p)$, $s \equiv r^u(p)$ and $u \not\equiv 0,1(q)$. Since the multiplicative group of residue classes modulo p has order $p-1$, $p \equiv 1(q)$. Other members of the class are determined by letting u range over the set $2, 3, \ldots, q-1$. Thus the class of groups is specified by the numbers p, q, and r while the number u specifies a group within the class. When it is understood that we are considering the class of groups determined by p, q, and r, it is convenient to let G_u designate the groups determined by u. We shall soon see that G_u is isomorphic to G_v if and only if $u \equiv v(q)$ or $uv \equiv (1)q$.

In this paragraph we state the basic properties of the group $G=G_u$ from the previous paragraph in order to facilitate the reading of this paper. These results can also be found in Rottländer's article (2). Any element of g can be written uniquely as a product. $g=a^kb^lc^m$ for some integers k, l, m, such that $0 \leqq k$, $l \leqq p-1$ and $0 \leqq m \leqq q-1$. Hence the order of G is p^2q. It is easy to see that the cyclic subgroups $\langle a \rangle$, and $\langle b \rangle$ generated by a and b respectively are normal subgroups of G. Hence the subgroup $\langle a,\ b \rangle$ generated by a and b is normal in G, and $\langle a,\ b \rangle$ is the only subgroup of G of order p^2. In addition $\langle a \rangle$ and $\langle b \rangle$ are the only normal subgroups of order p in G. The $p-1$ non-normal cyclic subgroups of order p in $\langle a,\ b \rangle$ fall into $(p-1)/q$ coniugacy classes of q groups each. In fact all groups conjugate to $\langle ab^x \rangle$ are of the form

$\langle ab^{xy}\rangle$ where $y\in\langle sr^{-1}\rangle=\langle r\rangle$ in the multiplicative group of integers modulo p. This is seen most easily by considering the following example

$$c\langle ab^x\rangle c^{-1}=\langle a^r b^{xs}\rangle=\langle ab^{xsr-1}\rangle.$$

A simple computation shows that any non-trivial element of G not in $\langle a, b\rangle$ has order q. Since there are $p^2q-p^2=p^2(q-1)$ elements of order q in G, there are p^2 subgroups of order q in G. These subgroups are all cojugate by the appropriate Sylow theorem. If an element g in G has order q, then the subgroups $\langle a, g\rangle$ and $\langle b, g\rangle$ have order pq. Furthemore these are the only subgroups of order pq in G. To be more specific if $g=a^kb^lc^m$ in the unique representation of g in G where $m\neq 0$, then g has order q and,

$$\langle a, g\rangle=\langle a, b^lc^m\rangle=\langle a, b^{l'}c\rangle$$

$$\langle b, g\rangle=\langle b, a^kc^m\rangle=\langle b, a^{k'}c\rangle$$

where l' and k' are appropriate integers. It is now easy to see that all subgroups pq containing a (or b) are conjugate in G to $\langle a, c\rangle$ ($\langle b, c\rangle$). Since $\langle a, c\rangle$ is not conjugate to $\langle b, c\rangle$, there are two conjugate classes of subgroups of order pq. In addition the subgroups of order q are conjugate in any group of order pg.

Suppose now that $G=G_u$ and H is a group isomorphic to G_v which for the sake of convenience has the presentation

$$H=\{\alpha, \beta, \gamma : \alpha^p=\beta^p=\gamma^q=\alpha\beta\alpha^{-1}\beta^{-1}, \gamma\alpha\gamma^{-1}=\alpha^r, \gamma\beta\gamma^{-1}=\beta^t\}$$

where $t=r^v$. If $uv\equiv 1(q)$, then it is easy to see that

$$\gamma^u\beta\gamma^{-u}=\beta^{t^u}=\beta^r,$$

and

$$\gamma^u\alpha\gamma^{-u}=\alpha^{r^u}.$$

Hence the map determined by

$$a\to\beta,\ b\to\alpha,\ c\to\gamma^u$$

is an isomorphism from G to H. On the other hand if f is an isomorphism from G onto H, then $f(a)$ is an element of $\langle\alpha\rangle$ or $\langle\beta\rangle$. It turns out that $f(a)\varepsilon\langle\alpha\rangle$ implies $u\equiv v(q)$ and that $f(a)\varepsilon\langle\beta\rangle$ implies $uv\equiv 1(q)$. The proof is simple although it is not necessarily the case $f(c)\varepsilon\langle\gamma\rangle$. However, $f(c)$ must conjugate α and β as a power of γ.

Throughout the remainder of this paper we assume that $G=\langle a, b, c\rangle$ and $H=\langle\alpha, \beta\ \gamma\rangle$, as above, and in addition that G is not isomorphic to H. The smallest possible order that G and H can possibly have then is 605 when $p=11$ and $q=5$. We now provide a diagram of the subgroup lattice of one of the groups of order 605. Please note that the diagram is not a Hasse diagram of the subgroup lattice. The points are non-trivial cyclic subgroups; the lines are proper groups of composite order as in a projective plane over a prime field. So in a certain sense the subgroup lattice of these groups is two-dimensional.

It is possible to literally see that G and H have the same situation of subgroups by looking at the diagram in the example. Though a little more involved it is possible to construct a function f from G to H which induces a situation preserving projectivity from G to H. The results of this paper are proved by extending this function to larger groups. The important thing to note is that the subgroup $\langle a, b^l c\rangle$ of G is isomorphic to the subgroup $\langle\alpha\ \beta^l\gamma\rangle$ of H under the correspondence $a\rightarrow\alpha$, $b^l c\rightarrow\beta^l\gamma$. Thus we are led to define f by $f(a^m b^n)=\alpha^m\beta^n$ and $f(a^k(b^l c)^m)=$ $=\alpha^k(\beta^l\gamma)^m$. In other words we take f so that its restriction to the subgroups $\langle a, b\rangle$ and $\langle a, b^l c\rangle$ for $l=0, 1, \ldots, p-1$ is an isomorphism. The map f is obviously one to one and onto from G to H. In order to show that f induces a projectivity p it suffices to show that $f\langle b, a^n c\rangle=\langle\beta, \alpha^n\gamma\rangle$. Let

$$g=a^k(b^l c)^m\in\langle b,\ a^n c\rangle=\langle b,\ a^k c^m\rangle.$$

This means that $\langle a^n c\rangle=\langle a^k c^m\rangle$ and also that $\langle\alpha^n\gamma\rangle=\langle a^k\gamma^m\rangle$. Then

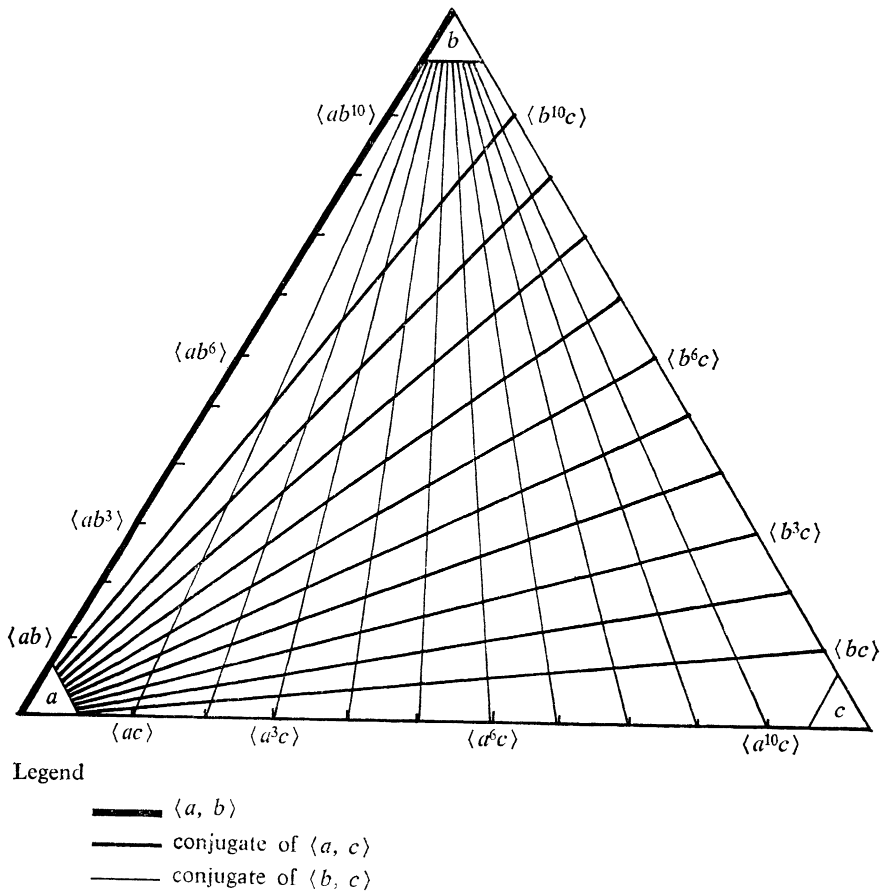
$$f(g)=\alpha^k(\beta^l\gamma)^m\in\langle\beta,\ \alpha^k\gamma^m\rangle=\langle\beta,\ \alpha^n\gamma\rangle.$$

Hence $f\langle b, a^n c\rangle\leq\langle\beta, \alpha^n\gamma\rangle$. Since $f\langle b, a^n c\rangle$ contains pg elements, the sets are equal. By our remarks following the statement of the induction principle we have that p is strictly index preserving. The fact that p preserves conjugacy follows from our classification of conjugate sub-

Diagram of $L(G)$, $G = G_u$

$p = 11$, $q = 5$, $r = 4$

$u = 2, 3,$ or 4



groups in listing the properties of G. In particular $\langle ab^x \rangle$ is conjugate to $\langle ab^y \rangle$ in G if and only if x and y are from the same coset $\langle sr^{-1} \rangle = \langle r \rangle = \langle tr^{-1} \rangle$ in the multiplicative group of integers modulo p if and only if $\langle \alpha\beta^x \rangle$ is conjugate to $\langle \alpha\beta^y \rangle$ in H. We have proved the following lemma.

LEMMA. The map $f : G \rightarrow H$ defined by $f(a^k(b^l c)^m) = \alpha^k(\beta^l\gamma)^m$ and $f(a^k b^l) = \alpha^k\beta^l$ for appropriate k, l, and m induces a situation preserving projectivity from G onto H.

4. The Fundamental Theorem.

Let G and H be as in the previous section. Let K be some group. Must $G \times K$ and $H \times K$ have the same situation of subgroups? No. In fact if K is any proper free group, then $G \times K$ and $H \times K$ are free products with normal amalgamated subgroups which by the results in (1) are determined by their lattices of subgroups. Thus if $H \times K$ is a projective image of $G \times K$, then $G \times K$ and $H \times K$ are isomorphic and by a simple argument on the order of elements G and H are isomorphic. However the following result shows how it is possible in certain cases to extend the map f from G onto H given in the previous section to all of $G \times K$ so that the extended map induces an index preserving projectivity from $G \times K$ onto $H \times K$. In the next section we give several examples.

THEOREM. Suppose:

a) Any subgroup of $G \times K$ which is not contained in $\langle a, b \rangle \times K$ or $\langle a, b^l c \rangle \times K$ $(l = 0, 1, \ldots, p-1)$ contains b.

b) Any subgroup of $H \times K$ which is not contained in

$$\langle \alpha, \beta \rangle \times K \text{ or } \langle \alpha, \beta^l\gamma \rangle \times K (l = 0, 1, \ldots, p-1) \text{ contains } \beta.$$

Then there is a projectivity from $G \times K$ onto $H \times K$ which is strictly index preserving.

PROOF. Define a map f from $G \times K$ onto $H \times K$ by $f(a^k b^l h) = \alpha^k \beta^l h$ and $f(a^k(b^l c)^m h) = \alpha^k(\beta^l\gamma)^m h$, where $h \in K$. Then f maps $G \times K$ one to one and onto $H \times K$. In addition f maps the subgroups

$$\langle a, b \rangle \times K \text{ or } \langle a, b^l c \rangle \times K \ (l = 0, 1, \ldots, p-1)$$

isomorphically onto the subgroups

$$\langle \alpha, \beta \rangle \times K \text{ or } \langle \alpha, b^l\gamma \rangle \times K,$$

respectively.

Suppose now that D is a subgroup of $G \times K$ which is not contained in

$$\langle a,\ b \rangle \times K \text{ or } \langle a,\ b^l c \rangle \times K \ (l=0,\ 1,\ \ldots,\ p-1).$$

By a.,

$$D=\langle b,\ D' \rangle, \text{ where } D' \leq \langle a,\ c \rangle \times K.$$

We shall show that $fD=\langle \beta,\ fD' \rangle$. Let

$$g=a^k(b^l c)^m h \in \langle b,\ a^k c^m h \rangle \leq \langle b,\ D' \rangle.$$

Then

$$f(g)=\alpha^k(\beta\gamma)^m h \in \langle \beta,\ \alpha^k \gamma^m h \rangle \leq \langle \beta,\ fD' \rangle$$

since $f(a^k c^m h)=(\alpha^k \gamma^m h \in fD')$. A similar argument shows that

$$f^{-1}\langle \beta,\ fD' \rangle \leq \langle b,\ f^{-1}(fD') \rangle = \langle b,\ D' \rangle.$$

The desired equality follows from the fact that

$$\langle \beta,\ fD' \rangle = f(f^{-1}\langle \beta,\ fD' \rangle) \leq f\langle b,\ D' \rangle \leq \langle \beta,\ fD' \rangle.$$

This shows in particular that for any subgroup M of $G \times K$,

$$fM \leq H \times K.$$

In a similar way f^{-1} can be shown to map subgroups of $H \times K$ to subgroups of $G \times K$. By the induction principle f induces a projectivity p from $G \times K$ onto $H \times K$.

Finally p is strictly index preserving, because if

$$D=\langle b,\ D' \rangle \leq E=\langle b,\ E' \rangle$$

where

$$D' \leq E' \leq \langle a,\ c \rangle \times K,$$

then

$$[E : D]=[E' : D'].$$

Corollary. Suppose any subgroup of $G \times K(H \times K)$ is the direct product of its projections in $G(H)$ and K. Then $G \times K$ and $H \times K$ have the same situation of subgroups.

PROOF. It suffices to show that the projectivity p from the previous theorem preserves conjugacy. This follows from the fact that the restrictions of f to G and K preserve conjugacy.

5. Examples.

In this section we study groups K such that $G \times K$ and $H \times K$ satisfy conditions a and b of the theorem. Suppose K is an arbitrary group. Let D be a subgroup of $G \times K$ which is not contained in

$$\langle a,\ b \rangle \times K \text{ or } \langle a,\ b^l c \rangle \times K \ (l=0,\ 1,\ \dots\ (p-1)).$$

Then the projection of D onto the factor G in $G \times K$ must be G or one of the subgroups

$$\langle b,\ a^l c \rangle \cdot (l=0,\ 1,\ \dots,\ p-1)$$

Hence there are two elements h, k in K such that bh and $a^l ck$ are elements in D for some l. If h has finite order m and m is not a multiple of p then $(bh)^m = b^m h^m = b^m$ a generator of $\langle b \rangle$. If all elements in K have order relatively prime to p, then conditions a and b of the theorem must always hold. This observation gives our first example.

EXAMPLE 1. If all elements in K have finite order which is relatively prime to p, then $G \times K$ and $H \times K$ have the same lattice of subgroups. Consider again the elements bh and $a^l ck$ from above. Note that

$$(a^l ck)(bh)(a^l ck)^{-1} = (cbc^{-1})(khk^{-1}) = b^s(khk^{-1}) \in D.$$

If $khk^{-1}=h$, then $b^s h \in D$ and also $b^x h$ where $x=s^2,\ s^3,\ \dots,\ s^{q-1}$. Since $q \geq 5$, $(b^x h)(bh)^{-1} = b^{x-1}$ is a generator of $\langle b \rangle$, for some x. Thus we have our second example.

EXAMPLE 2. If K is abelian, then $G \times K$ and $H \times K$ have the same lattice of subgroups.

Our third example where K is an infinite dihedral group is related to the other two examples through the fact that in the infinite dihedral group any non-trivial element either has order two or infinity and that any two elements of infinite order commute. Returning to the situation bh, $a^l ck \in D$, we have $b \in D$ immediately if h has order two. Similarly if k has order two, then $a^l c \in D$ and by conjugation $b \in D$. However if h and k both have infinite order, then $b \in D$ by conjugation.

EXAMPLE 3. If K is the infinite dihedral group, then $G \times K$ and $H \times K$ have the same lattice of subgroups.

Furthermore we have that $G \times K$ and $H \times K$ are not isomorphic in any of the three examples. For if $G \times K$ were isomorphic to $H \times K$, then G can be identified with some subgroup of $H \times K$. Suppose in fact that this is done. In all three examples G is not a subgroup of K. Indeed in all three examples G has trivial intersection with K. This is most obvious when K is the infinite dihedral group, because then K has no elements of order p or q. When K is abelian, K is the center of $H \times K$. Since G has trivial center, $G \cap K = 1$. When the order of the elements of K are relatively prime to p, as in Example 1, then any non-trivial element in $G \cap K$ would have order q and would commute with any element of order p in $H \times K$. Again $G \cap K = 1$. Therefore the projection of $H \times K$ onto H maps G isomorphically onto H. This is the desired contradiction.

Finally it is easy to see that the idea in Example 1 could be extended to give an example for the corollary. That is, if K is a group in which every element has finite order relatively prime to p and q, then $G \times K$ and $H \times K$ have the same situation of subgroups.

BIBLIOGRAPHY

[1] HOLMES, C. S.: *Projectivities of Free Products*, Rend. Semi. Mat. Univ. Padova, 42 (1969) 341-387.

[2] ROTTLÄNDER, A.: *Nachweis der Existenz nicht-isomorpher Gruppen von gleicher Situation der Untergruppen*, Math. Zeitschrift 28 (1928) 641-653.

Manoscritto pervenuto in redazione il 10 febbraio 1970.