Homework 7

Anthony Jones

1a) To show that $G \times H$ is a group, we must prove that the closed, associative, inverse, and identity properties exist.

Let $(g_1, h_1), (g_2, h_2) \in G \times H$. Observe, by definition, the direct product of the two:

$$(g_1, h_1)(g_2, h_2) = (g_1 \cdot g_2, h_1 \circ h_2).$$

Since $(G, \cdot)$ and $(H, \circ)$ are both groups, $g_1 \cdot g_2 \in G$ and $h_1 \circ h_2 \in H$. Thus

$$(g_1 h_1)(g_2, h) \in G \times H.$$

Let $\overset{a=}{(g_a, h_a)}, \overset{b=}{(g_b, h_b)}, \overset{c=}{(g_c, h_c)} \in G \times H$.

By definition

$$\begin{aligned}(ab)c &= (g_a \cdot g_b, h_a \circ h_b)(g_c, h_c) \\ &= (g_a \cdot g_b \cdot g_c, h_a \circ h_b \circ h_c)\end{aligned}$$

$$\begin{aligned}a(bc) &= (g_a, h_a)(g_b \cdot g_c, h_b \circ h_c) \\ &= (g_a \cdot g_b \cdot g_c, h_a \circ h_b \circ h_c) = (ab)c.\end{aligned}$$

Let $e = (I_G, I_H) \in G \times H$. Observe

$$\begin{aligned}(g_1, h_1)(e) &= (g_1 \cdot I_G, h_1 \circ I_H) \\ &= (g_1, h_1)\end{aligned}$$

$$\begin{aligned}(e)(g_1, h_1) &= (I_G \cdot g_1, I_H \circ h_1) \\ &= (g_1, h_1)\end{aligned}$$

1a) Finally, let $g, g^{-1} \in G$ and $h, h^{-1} \in H$ make the elements $(g,h) \in G \times H$ and $(g^{-1}, h^{-1}) \in G \times H$. Observe

$$\begin{aligned}(g,h)(g^{-1},h^{-1}) &= (g \cdot g^{-1}, h \circ h^{-1}) \\ &= (I_G, I_H) \\ &= e \in G \times H \quad \text{and}\end{aligned}$$

$$\begin{aligned}(g^{-1},h^{-1})(g,h) &= (g^{-1} \cdot g, h^{-1} \circ h) \\ &= (I_G, I_H) \\ &= e \in G \times H.\end{aligned}$$

Thus the inverse of any element pair of G and H is the pair of inverses of those elements, which exist as G and H are both groups.

- - - - - - - - - - - - - - - - -

Thus $G \times H$ is closed and associative under direct product operation, and both the identity and inverse exists within $G \times H$. Hence $G \times H$ is a group.

Homework 7

Anthony Jones

1b) Let $G' \leq G$ and $H' \leq H$ be subgroups.

Consider $a, b \in G' \times H'$ given by

$$a = (g_a, h_a); \quad g_a \in G', h_a \in H' \text{ and}$$

$$b = (g_b, h_b); \quad g_b \in G', h_b \in H'.$$

Finally, consider b^{-1}, given by

$$b^{-1} = [(g_b, h_b)]^{-1} = (g_b^{-1}, h_b^{-1}).$$

The direct product $ab^{-1} = (g_a \cdot g_b^{-1}, h_a \circ h_b^{-1})$ is an element of $G' \times H'$ if $g_a \cdot g_b^{-1} \in G'$ and $h_a \circ h_b^{-1} \in H'$. Because both G' and H' are subgroups, we know that this is true as $g_a, g_b \in G'$ and $h_a, h_b \in H'$. Thus

$$ab^{-1} = (g_a \cdot g_b^{-1}, h_a \circ h_b^{-1}) \in G' \times H',$$

and by the same proposition 3.1.2,

$$G' \times H' \leq G \times H.$$

Homework 7

Anthony Jones

1c) Yes. Let $G^\Delta \times H^\Delta \leq G \times H$ be any arbitrary subgroup. Consider $a = (g_{a\Delta}, h_{a\Delta}), b = (g_{b\Delta}, h_{b\Delta}) \in G^\Delta \times H^\Delta$.

By proposition 3.1.2 it follows that

$$ab^{-1} = (g_{a\Delta} \cdot g_{b\Delta}^{-1}, h_{a\Delta} \circ h_{b\Delta}^{-1}) \in G^\Delta \times H^\Delta.$$

Therefore, there exists some elements $m \in G^\Delta$ and $n \in H^\Delta$ for which

$$m = g_{a\Delta} \cdot g_{b\Delta}^{-1} \text{ and}$$
$$n = h_{a\Delta} \circ h_{b\Delta}^{-1}.$$

Finally, observe that for any element $\emptyset \in G^\Delta \times H^\Delta$, its constructors $g_{\emptyset\Delta}$ and $h_{\emptyset\Delta}$ must exist in G^Δ and H^Δ respectively. That is shown by

$$\forall \emptyset \in G^\Delta \times H^\Delta \; E \; g_{\emptyset\Delta} \in G^\Delta, h_{\emptyset\Delta} \in H^\Delta \text{ and}$$

$$\forall g_{\emptyset\Delta}, h_{\emptyset\Delta} \; E \; \emptyset = (g_{\emptyset\Delta}, h_{\emptyset\Delta}) \in G^\Delta \times H^\Delta.$$

Thus, by extension, there exists an m for any elements $g_{a\Delta} \in G^\Delta$, $g_{b\Delta}^{-1} \in G^\Delta$ and n for $h_{a\Delta} \in H^\Delta$, $h_{b\Delta}^{-1} \in H^\Delta$. Thus by proposition 3.1.2, these groups must also be subgroups $G^\Delta \leq G$ and $H^\Delta \leq H$.

Homework 7

Anthony Jones

1d) Let $a \in Z(G \times H)$ and $x \in G \times H$.

Then $ax = xa$, by definition. Thus

$$(g_a \cdot g_x,\ h_a \circ h_x) = (g_x \cdot g_a,\ h_x \circ h_a), \text{ where}$$

$$a = (g_a, h_a);\ g_a \in G,\ h_a \in H \text{ and}$$
$$x = (g_x, h_x);\ g_x \in G,\ h_x \in H.$$

Therefore, the constructor elements g_a and h_a must have the properties

$$g_a \cdot g_x = g_x \cdot g_a \text{ and}$$
$$h_a \circ h_x = h_x \circ h_a,\ \forall x \in G \times H.$$

Thus the constructor elements g_a and h_a are ~~the ~~ elements of the center of G and H respectively.

Thus $Z(G \times H) = Z(G) \times Z(H)$.

1e) If $G \times H$ is abelian then ~~$G \times H = Z(G \times H)$~~ $G \times H = Z(G \times H) = Z(G) \times Z(H)$ from above. Therefore every combination of G and H must be in $Z(G) \times Z(H)$: Thus $G = Z(G)$ and $H = Z(H)$, meaning both are abelian.

If G and H are abelian, then likewise

$$Z(G \times H) = Z(G) \times Z(H) = (G) \times (H) = G \times H$$

and so $G \times H$ is also abelian.

Homework 7

Anthony Jones

2) K is characteristic in G if $\phi(K) \subseteq K$ for every $\phi \in Aut(G)$. [HW 6]

Observe that any element $a \in K$ must be in the intersection of automorphisms of G applied to H. Consider the trivial automorphism of G, mapping any element to itself. This identity morphism denoted f follows that $a \in f(H)$, by definition, and therefore $a \in H$. Thus $K \subseteq H$.

Now observe that, by extension, any image of an $\phi \in Aut(G)$ applied on K is contained within the image of ϕ applied on H:

Let $a \in K$. As $K \subseteq H$, $a \in H$. Therefore $\phi(a) \in im(\phi|_H)$, so $im(\phi|_K) \subseteq im(\phi|_H)$.

Finally, consider $n \in \phi(K)$ for $\phi \in Aut(G)$. As we have displayed above, $n \in im(\phi|_H)$. But we can also consider any other arbitrary $\pi \in Aut(G)$ and observe using the same logic $n \in im(\pi|_H)$. Thus $n \in \bigcap_{\phi \in Aut(G)} \phi(H)$ and hence $\phi(K) \subseteq K$.

Therefore K is characteristic in G.

Homework 7

Anthony Jones

3) We will use Induction to prove:

Base

We know that the trivial subgroup $H = \{1\} \leq G$ and $|H| = p^0 = 1$.
By Cauchy's theorem, we also know that $\exists K \leq G$ such that $|K| = p^1 = p$.
It follows that $H \trianglelefteq K$ as $H = \{1\}$.

Induction

~~Let $H \leq G$ with order p^k. By Lagrange's theorem,~~ Let $H \trianglelefteq G$ with order p^k and ~~$N \leq G$ with order p^{k-1}, where $H \trianglelefteq N$~~.
It follows from the third isomorphism theorem that there is a one-to-one correspondence of subgroups of G containing H and the subgroups of G/H. We know from Lagranges theorem that $|G/H| = |G|/|H|$ which is p^{n-k}. Because $k \leq n$, we know that for $k < n$ there exists at least one subgroup generated by an element of G/H with order p, using Cauchy's Theorem. Therefore there exists at least one subgroup of G containing H that is order P ~~containing H~~ $\times |H|$. Thus there exists a subgroup $K \trianglelefteq G$ with order p^{k+1}.

Finally it follows that this $H \trianglelefteq K$ As from Corollary 5.1.10 any subgroup with index $p | n$ is normal.

Therefore, for all $0 \leq k \leq n$ there exists subgroups with order p^k for which the group of order p^k is normal to p^{k+1}.

Homework 7

Anthony Jones

4) To show semidirect product as a group we must prove all four conditions:

<u>Closed</u>: Let $a, b \in (G \rtimes_\phi H)$ with
$a = (g_1, h_1)$ and $b = (g_2, h_2)$.

Then $ab = (g_1 \phi(h_1)(g_2), h_1 h_2)$.

Observe, firstly, that $h_1 h_2 \in H$ as H is a group. Now consider $g_1 \phi(h_1)(g_2)$: $\phi(h_1)$ defines an automorphism of G as shown in the group homomorphism. Therefore $\phi(h_1)(g_2) \in G$, as $\phi(h_1)$ maps g_2 to some other element in G. Finally, if we consider $(g_1)(\phi(h_1)(g_2))$, we can see that this is a product of two elements of G. Thus $g_1 \phi(h_1)(g_2) \in G$, and so $(G \rtimes_\phi H)$ is closed.

<u>Identity</u>: Consider $(I_G, I_H) \in (G \rtimes_\phi H)$:

$$
\begin{aligned}
(I_G, I_H)(g,h) &= (I_G \phi(I_H)(g), I_H \cdot h) \\
&= (g, h) \quad \text{and} \\
(g,h)(I_G, I_H) &= (g \phi(h)(I_G), h \cdot I_H) \\
&= (g \cdot I_G, h) = (g, h).
\end{aligned}
$$

An identy having an automorphism applied yields the identity, so $\phi(1) = 1$. Likewise the identity automorphism maps every g to itself, $\phi_I(g) = g$.

Homework 7 AJ

4) <u>Inverse</u>: Let $(a,b) \in (G \rtimes_\phi H)$.

Observe that as $\phi(a^{-1}a) = \phi(a^{-1})\phi(a)$, and $\phi(1) = 1$, we know that, similarly, $\phi(\phi(b^{-1}))(b) = b^{-1}b = 1$.

Thus, consider $(\phi(b^{-1})(a^{-1}), b^{-1})$:

$\phi(b^{-1})(a^{-1}) \in G$ and $b^{-1} \in H$ so this is contained in $(G \rtimes_\phi H)$.

$$(a,b)(\phi(b^{-1})(a^{-1}), b^{-1}) =$$
$$= (a\phi(b)(\phi(b^{-1})(a^{-1}), bb^{-1})$$
$$= (a\ \phi(bb^{-1})(a^{-1}), I_H)$$
$$= (a\ \phi(I_H)(a^{-1}), I_H)$$
$$= (aa^{-1}, I_H) = (I_G, I_H) = 1.$$

<u>Associ.</u>: $[(a,b)(g,h)](c,d) = (a\phi(b)(g), bh)(c,d)$
$$= (a[\phi(b)(g)][\phi(bh)(c)], bhd)$$
$$= (a[\phi(b)(g)][\phi(b)(\phi(h)(c)], bhd)$$
$$= (a\phi(b)(g\phi(h)c), bhd)$$
$$= (a,b)[(g\phi(h)(c), hd)]$$
$$= (a,b)[(g,h)(c,d)]$$