David Beydler
MATH 540A
Due: 10/3/07

1.1-28, 1.6-2, 13

1.1

28) [Let $(A, \star)$ and $(B, \circ)$ be groups and let $A \times B$ be their direct product (as defined in Example 6). Verify all the group axioms for $A \times B$:]

a) [prove that the associative law holds:
for all $(a_i, b_i) \in A \times B$, $i = 1, 2, 3$ $(a_1, b_1)[(a_2, b_2)(a_3, b_3)] = [(a_1, b_1)(a_2, b_2)](a_3, b_3)$]

__Pf__: Let $(a_i, b_i) \in A \times B$ for $i = 1, 2, 3$. Then

$$\begin{aligned}
(a_1 b_1)[(a_2, b_2)(a_3, b_3)] &= (a_1, b_1)\ (a_2 \star a_3, b_2 \circ b_3) \\
&= (a_1 \star (a_2 \star a_3), b_1 \circ (b_2 \circ b_3)) \\
&= ((a_1 \star a_2) \star a_3, (b_1 \circ b_2) \circ b_3) \\
&= (a_1 \star a_2, b_1 \circ b_2)(a_3, b_3) \\
&= [(a_1, b_1)(a_2, b_2)](a_3, b_3)
\end{aligned}$$

since A and B are groups

$\blacksquare$

b) [prove that $(1, 1)$ is the identity of $A \times B$]

__Pf__: Let $(a, b) \in A \times B$. Then

$$(1, 1)(a, b) = (1 \star a, 1 \circ b) = (a, b)$$

since 1 is the identity of A and 1 is the identity of B

and

$$(a, b)(1, 1) = (a \star 1, b \circ 1) = (a, b)$$

Thus, $(1, 1)$ is the identity of $A \times B$. $\blacksquare$

see next page

(1.1 cont) (28 cont)

c) [prove that the inverse of (a,b) is (a^{-1}, b^{-1})]

<u>Pf</u>: Let $(a,b) \in A \times B$. Then

$$(a,b)(a^{-1}, b^{-1}) = (a a^{-1}, b \circ b^{-1}) = (1, 1)$$

since a^{-1} is the inverse of a and b^{-1} is the inverse of b

and

$$(a^{-1}, b^{-1})(a, b) = (a^{-1} \ast a, b^{-1} \circ b) = (1, 1)$$

So, the inverse of (a,b) is (a^{-1}, b^{-1}). ▨

DB 3

$\boxed{1.6}$ 2) [If $\phi : G \to H$ is an isomorphism, prove that $|\phi(x)| = |x|$ for all $x \in G$. Deduce that any two isomorphic groups have the same number of elements of order n for each $n \in \mathbb{Z}^+$. Is the result true if ϕ is only assumed to be a homomorphism?]

Pf: Let $x \in G$. Suppose $|x| = n$. Then $x^n = e$. So, $\phi(x^n) = \phi(e)$. Since ϕ is an isomorphism we get $(\phi(x))^n = \phi(e)$. And since $\phi(e)$ is the identity of H, we get that $|\phi(x)| \leq n$. Now suppose that $|\phi(x)| < n$. Then there would be an $m < n$ such that $(\phi(x))^m = \phi(e)$. So, $\phi(x^m) = \phi(e)$. Since ϕ is an isomorphism we can apply ϕ^{-1} to both sides to get $x^m = e$. But this would contradict the fact that $|x| = n > m$, so $|\phi(x)| \not< n$. Thus, $|\phi(x)| = n = |x|$, as required. ▨

Let $\{x_1, \ldots, x_k\}$ be the entire list of elements of G with order n. Then $\{\phi(x_1), \ldots, \phi(x_k)\}$ also have order n. Now suppose that $h \in H$ had order n, but was not in $\{\phi(x_1), \ldots, \phi(x_k)\}$. Since ϕ is onto, there would be a $g \in G$ such that $\phi(g) = h$. So, $n = |h| = |\phi(g)| = |g|$. But then since $|g| = n$, we would have $g \in \{x_1, \ldots, x_k\}$, and $h \in \{\phi(x_1), \ldots, \phi(x_k)\}$, which is a contradiction. So if there are only k elements of order n in G, then there are k elements of order n in H. ▨

If ϕ is a homomorphism, then orders are not preserved. For example, let $\phi : \mathbb{Z}_4 \to \mathbb{Z}_4$ be defined by $\phi(x) = 0$. Then $|1| = 4$ in G, but $|\phi(1)| = 1$.

(1.6 cont) 13) [Let G and H be groups and let $\phi : G \to H$ be a homomorphism. Prove that the image of ϕ, $\phi(G)$ is a subgroup of H. Prove that if ϕ is injective then $G \cong \phi(G)$.]

Pf: Closure: Let $h_1, h_2 \in \phi(G)$. Then there are $g_1, g_2 \in G$ such that $\phi(g_1) = h_1$ and $\phi(g_2) = h_2$. So, $h_1 h_2 = \phi(g_1)\phi(g_2) = \phi(g_1 g_2)$, since ϕ is a homomorphism. Now since G is a group, $g_1 g_2 \in G$, so $\phi(g_1 g_2) \in \phi(G)$, so $h_1 h_2 \in \phi(G)$. Thus, $\phi(G)$ is closed.

Associativity: Since multiplication in H is associative, so is multiplication in $\phi(G) \subseteq H$.

Identity: Let $e \in G$ be the identity of G. Let $g \in G$ so $\phi(g) \in \phi(G)$. Then

$$\phi(g)\phi(e) = \phi(ge) = \phi(g), \text{ and}$$
$$\phi(e)\phi(g) = \phi(eg) = \phi(g).$$

So $\phi(e) \in H$ is the identity of H, and since $e \in G$, $\phi(e) \in \phi(G)$ (i.e. $\phi(G)$ has an identity).

Inverse: Let $g \in G$ so $\phi(g) \in \phi(G)$. Since G is a group, $g^{-1} \in G$, so $\phi(g^{-1}) \in \phi(G)$.
Since $\phi(g)\phi(g^{-1}) = \phi(gg^{-1}) = \phi(e)$, and

$$\phi(g^{-1})\phi(g) = \phi(g^{-1}g) = \phi(e),$$

$(\phi(g))^{-1} = \phi(g^{-1}) \in \phi(G)$.

Thus, $\phi(G)$ is a group. And since $\phi(G) \subseteq H$, $\phi(G)$ is a subgroup of H. $\blacksquare$

see next page

(1.6 cont) (13 cont)

Pf: Suppose ϕ is injective (1-1). Then since ϕ is also onto $\phi(G)$, $\phi: G \to \phi(G)$ is a bijection. This fact, combined with the fact that ϕ is a homomorphism, proves that ϕ is an isomorphism between G and $\phi(G)$. So, $G \cong \phi(G)$. ▨