10-29-1993

Direct products.

Definition. Let G and H be groups. The **direct product** $G \times H$ of G and H is the set of all ordered pairs $\{(g, h) | g \in G, h \in H\}$ with the operation

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

Remarks. The identity element is $(1, 1)$, the pair consisting of the identity elements of G and H. Inverses are given by $(g, h)^{-1} = (g^{-1}, h^{-1})$. The product is associative, since it is associative in each component.

Note that if G and H are abelian, I'll use additive notation as usual.

$$(g_1, h_1) + (g_2, h_2) = (g_1 + g_2, h_1 + h_2)$$

$$\text{Inverses: } -(g, h) = (-g, -h)$$

$$\text{Identity: } (0, 0) \ \square$$

Examples.

1. If G and H are finite, then $|G \times H = |G||H|$. For example, $|\mathbb{Z}_5 \times \mathbb{Z}_6| = 30$. $\square$

2. If G and H are abelian, so is $G \times H$. $\square$

3. $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_4$ are *not* isomorphic.

   One reason is that $\mathbb{Z}_4$ is cyclic of order 4, while every element of $\mathbb{Z}_2 \times \mathbb{Z}_2$ has order 2. $\square$

4. Construct 4 different groups of order 8.

   The group D_4 of symmetries of the square is nonabelian. The groups $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbf{Z}_2$, and $\mathbb{Z}_8$ are abelian. Of the abelian groups, $\mathbb{Z}_8$ is cyclic of order 8, $\mathbb{Z}_4 \times \mathbb{Z}_2$ has an element of order 4 but is not cyclic, and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbf{Z}_2$ has only elements of order 2. It follows that the three abelian groups I've listed are distinct.

   In fact, there are 5 groups of order 8. The fifth is the group Q of the **quaternions**. It consists of the set $\{\pm 1, \pm i, \pm j, \pm k\}$ with the multiplication table

	1	-1	i	$-i$	j	$-j$	k	$-k$
1	1	-1	i	$-i$	j	$-j$	k	$-k$
-1	-1	1	$-i$	i	$-j$	j	$-k$	k
i	i	$-i$	-1	1	k	$-k$	$-j$	j
$-i$	$-i$	i	1	-1	$-k$	k	j	$-j$
j	j	$-j$	$-k$	k	-1	1	i	$-i$
$-j$	$-j$	j	k	$-k$	1	-1	$-i$	i
k	k	$-k$	j	$-j$	$-i$	i	-1	1
$-k$	$-k$	k	$-j$	j	i	$-i$	1	-1

With this description, it might be tedious to check associativity. But you can also think of Q as the subgroup of $GL(2, \mathbb{C})$ (2×2 complex matrices with nonzero determinant) generated by

$$\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}, \qquad \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}.$$

Since matrix multiplication is associative — to be proved later! — the multiplication here is associative. However, in this case you'd have to verify that the subgroup in question has order 8.

Note also that I haven't proved that these descriptions are equivalent — that is, that they give rise to isomorphic groups. $\square$

Definition. Let m and n be positive integers. The **least common multiple** $[m,n]$ of m and n is the smallest positive integer divisible by m and n.

Remark. Since mn is divisible by m and n, the set of positive multiples of m and n is nonempty. Hence, it has a smallest element, by well-ordering. It follows that the least common multiple of two positive integers is always defined. For example, $[18,30] = 90$.

The following result follows from the Fundamental Theorem of Arithmetic. Do you see how?

Lemma. Let m and n be positive integers. Then

$$mn = (m,n)[m,n]. \square$$

Proposition. The element $(1,1)$ has order $[m,n]$ in $\mathbb{Z}_m \times \mathbb{Z}_n$.

Proof.

$$[m,n](1,1) = ([m,n],[m,n]).$$

The first component is 0, since it's divisible by m; the second component is 0, since it's divisible by n. Hence, $[m,n](1,1) = (0,0)$.

Next, I must show that $[m,n]$ is the smallest positive integer which kills $(1,1)$. Suppose $k(1,1) = (0,0)$, so $(k,k) = (0,0)$. Consider the first components. $k = 0$ in $\mathbb{Z}_m$ means that $m \mid k$; likewise, the second components show that $n \mid k$. Since k is a common multiple of m and n, it must be greater than or equal to the least common multiple $[m,n]$: that is, $k \geq [m,n]$. This proves that $[m,n]$ is the order of $(1,1)$. $\square$

Example. In $\mathbb{Z}_4 \times \mathbb{Z}_6$, the element $(1,1)$ has order $[4,6] = 12$. On the other hand, the element $(1,1) \in \mathbb{Z}_5 \times \mathbb{Z}_6$ has order 30. Since $\mathbb{Z}_5 \times \mathbb{Z}_6$ has order 30, the group is cyclic; in fact, $\mathbb{Z}_5 \times \mathbb{Z}_6 \approx \mathbb{Z}_{30}$. $\square$

Remark. More generally, consider $(x_1, \ldots, x_n) \in G_1 \times \ldots \times G_n$, and suppose x_i has order r_i in G_i. (The G_i's need not be cyclic.) Then $(x_1, \ldots, x_n)$ has order $[r_1, \ldots, r_n]$. $\square$

Corollary. If $(m,n) = 1$, then $\mathbb{Z}_m \times \mathbb{Z}_n \approx \mathbb{Z}_{mn}$. $\square$

Remark. More generally, if m_1, ..., m_k are pairwise relatively prime, then

$$\mathbb{Z}_{m_1} \times \ldots \times \mathbb{Z}_{m_k} \approx \mathbb{Z}_{m_1 \cdots m_k}. \square$$

Proof. If $(m,n) = 1$, then $[m,n] = mn$. Then $(1,1)$ has order mn, but $|\mathbb{Z}_m \times \mathbb{Z}_n| = mn$. Therefore, $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic of order mn, so it must be isomorphic to $\mathbb{Z}_{mn}$. $\square$

Examples.

1. $\mathbb{Z}_5 \times \mathbb{Z}_6 \approx \mathbb{Z}_{30}$. However, $\mathbb{Z}_2 \times \mathbb{Z}_2 \not\approx \mathbb{Z}_4$, as noted above. $\square$

2. The element $(2,4,4)$ in $\mathbb{Z}_4 \times \mathbb{Z}_{12} \times \mathbb{Z}_6$ has order $[2,3,3] = 6$. $\square$

3. Let $G = \mathbb{Z} \times \mathbb{Z}$. G is the set of points (m,n) in the plane with integer coordinates.

Consider the subgroup $H = \langle (1,2) \rangle$. An arbitrary element of H is a multiple of $(1,2)$, hence has the form $(x,2x)$ for $x \in \mathbb{Z}$. You can think of H as the points on the line $y = 2x$ having integer coordinates.

What are the cosets of H? A typical coset has the form $(a,b) + \langle (1,2) \rangle$. However, since $(a,2a) \in H$, this coset is also

$$(a,b) - (a,2a) + H = (0, b-2a) + H.$$

It is evident that the number $b - 2a$ can take on any integer value as a and b vary over all integers. Hence, a typical coset of H can be written as $(0, c) + H$ for $c \in \mathbb{Z}$. Since $H = \{(x, 2x) \mid x \in \mathbb{Z}\}$,

$$(0, c) + H = \{(x, 2x + c) | x \in \mathbb{Z}\}.$$

Geometrically, this is the integer points on the line with slope 2 and y-intercept c.

From this discussion, it's clear that the cosets of H are (the integer points on) the lines with slope 2. This is a nice illustration of how the cosets of a subgroup partition the group.

Since G is abelian, H is automatically normal, and the set of cosets G/H forms a group. What is it? That is, what is a "known" group isomorphic to G/H?

From our discussion above, the cosets of H are "parametrized" by the y-intercepts of the slope 2 lines. Since such a y-intercept can be any integer point on the y-axis, it's reasonable to suspect that $G/H \approx \mathbb{Z}$. I'll try to construct an isomorphism.

To construct an isomorphism out of the quotient G/H, use the First Isomorphism Theorem. I need a map ϕ from G onto $\mathbb{Z}$ which kills $H = \langle(1, 2)\rangle$. Since G is ordered pairs (x, y), I'm trying to define $\phi((x, y))$. How can I do this so as to "kill" things of the form $(x, 2x)$? Well, what characterizes $(x, 2x)$ things is that the second component (y) is twice the first (x); that is, $y = 2x$, or $y - 2x = 0$. Define

$$\phi((x, y)) = y - 2x.$$

If x and y are integers, so is $y - 2x$, so there is indeed a map $\phi : \mathbb{Z} \times \mathbb{Z} \to \mathbb{Z}$. I must check that ϕ is a homomorphism, that it maps onto $\mathbb{Z}$, and that $\ker \phi = H$.

First,

$$\phi((a, b) + (c, d)) = \phi(a + c, b + d) = (b + d) - 2(a + c) = (b - 2a) + (d - 2c) = \phi((a, b)) + \phi((c, d)).$$

Therefore, ϕ is a homomorphism.

If $z \in \mathbb{Z}$, then $\phi((0, z)) = z$. Therefore, ϕ maps onto.

Finally, if $(x, 2x) \in H$, then $\phi((x, 2x)) = 2x - 2x = 0$. Therefore, $H \subset \ker \phi$. Suppose conversely that $(x, y) \in \ker \phi$, so $\phi((x, y)) = 0$. This means that $y - 2x = 0$, or $y = 2x$. Hence, $(x, y) = (x, 2x) \in H$. It follows that $\ker \phi \subset H$, so $H = \ker \phi$.

By the First Isomorphism Theorem, $G/H \approx \mathbb{Z}$. □

When a group G is isomorphic to the direct product of groups H and K, you can think of G as "factored" from the inside as well as externally. That is, there are subgroups $H', K' < G$ such that $G = H'K'$ in a particularly nice way.

Theorem. Let $H, K < G$. The following statements are equivalent:

1. $G = HK$, $H, K \triangleleft G$, and $H \cap K = \{1\}$.
2. There is an isomorphism $\phi : H \times K \to G$ such that $\phi((h, 1)) = h$ and $\phi((1, k)) = k$.

Proof. $(1 \Rightarrow 2)$ Suppose statement 1 holds. Define a map $\phi : H \times K \to G$ by $\phi((h, k)) = hk$.

Before proving that ϕ is a homomorphism, I'll prove the following claim: If $h \in H$ and $k \in K$, then $hk = kh$. To see this, observe that $h(kh^{-1}k^{-1}) \in H$, since $kh^{-1}k^{-1} \in H$ by normality of H, and that $(hkh^{-1})k^{-1} \in K$, since $hkh^{-1} \in K$ by normality of K.

Therefore, $hkh^{-1}k^{-1} \in H \cap K = \{1\}$, so $hk = kh$. This proves the claim.

Now I'll prove that ϕ is a homomorphism.

$$\phi((h_1, k_1)(h_2, k_2)) = \phi((h_1h_2, k_1k_2)) = h_1h_2k_1k_2 = h_1k_1h_2k_2 = \phi((h_1, k_1))\,\phi((h_2, k_2)).$$

(I used the claim to do $h_2k_1 = k_1h_2$ in the middle.) Therefore, ϕ is a homomorphism.

Next, I'll show ϕ is an isomorphism by constructing an inverse. I'd like to define the inverse by $\phi(hk) = (h, k)$. Since $G = HK$, every element of G *can* be written in the form hk, where $h \in H$ and $k \in K$. However, to ensure that ψ is well-defined, I must check that every element of G can be written *uniquely* as hk. (A different representation for the same element might yield a different ordered pair as the output of ψ.)

Suppose, then, that $h_1k_1 = h_2k_2$, where $h_1, h_2 \in H$ and $k_1, k_2 \in K$. Then

$$h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K = \{1\}.$$

It follows that $h_1 = h_2$ and $k_1 = k_2$, so the representation is indeed unique.

Now $\psi : G \to H \times K$ defined by $\psi(hk) = (h, k)$ is well-defined. It obviously inverts ϕ, so ϕ is an isomorphism.

Finally, by definition of ϕ,

$$\phi((h,1)) = h, \qquad \phi((1,k)) = k.$$

This completes the proof that $1 \Rightarrow 2$.

($2 \Rightarrow 1$) Suppose there is an isomorphism $\phi : H \times K \to G$ such that $\phi((h,1)) = h$ and $\phi((1,k)) = k$. I'll show that the three parts of statement 1 hold.

If $g \in G$, then $g = \phi((h,k))$, since ϕ is onto. Therefore, $g = hk$, where $h \in H$ and $k \in K$. Hence, $G = HK$.

It is easy to verify that $H \times \{1\}$ and $\{1\} \times K$ are normal subgroups of $H \times K$. For example,

$$(h,k)(h',1)(h^{-1},k^{-1}) = (hh'h^{-1}, 1) \in H \times \{1\}$$

shows that $H \times \{1\} \triangleleft H \times K$.

Now ϕ is surjective, so it carries normal subgroups to normal subgroups. Since $\phi(H \times \{1\}) = H$ and $\phi(\{1\} \times K) = K$, it follows that $H, K \triangleleft G$.

Finally, suppose $h = k \in H \cap K$. Then

$$\phi((h,1)) = h = k = \phi((1,k)).$$

However, ϕ is injective, so $(h,1) = (1,k)$, and therefore $h = k = 1$. Therefore, $H \cap K = \{1\}$. □

Examples.

1. $\mathbb{Z}_{10} \approx \mathbb{Z}_2 \times \mathbb{Z}_5$. The theorem says that $\mathbb{Z}_{10}$ is the "internal" direct product of subgroups of order 2 and 5. Those subgroups are $\langle 5\rangle$ and $\langle 2\rangle$, respectively. In this situation, the three properties of statement 1 of the theorem are:

a. $\mathbb{Z}_{10} = \langle 5\rangle + \langle 2\rangle$.

b. $\langle 5\rangle, \langle 2\rangle \triangleleft \mathbb{Z}_{10}$.

c. $\langle 5\rangle \cap \langle 2\rangle = \{0\}$.

Note the change to additive notation! □

2. Direct products are useful tools, but not every group can be decomposed into a direct product of subgroups. For example, S_3 is not a direct product of a subgroup of order 2 and a subgroup of order 3. Such subgroups would be isomorphic to $\mathbb{Z}_2$ and $\mathbb{Z}_3$, respectively, and their direct product would therefore be abelian. However, S_3 is *not* abelian. □