Product Groups

Liming Pang

**Definition 1.** $G$ and $G'$ are groups. Define their **product group** to be the set of all ordered pairs $(g, g')$, where $g \in G$ and $g' \in G'$, with law of composition $(g_1, g'_1)(g_2, g'_2) = (g_1g_2, g'_1g'_2)$. The product group is denoted by $G \times G'$.

There are injective maps of $G$ and $G'$ into $G \times G'$ by

\[ i_1 : G \rightarrow G \times G' \]
\[ g \mapsto (g, 1_{G'}) \]

and

\[ i_2 : G' \rightarrow G \times G' \]
\[ g' \mapsto (1_G, g') \]

Also there are surjective projections:

\[ G \times G' \rightarrow G \]
\[ (g, g') \mapsto g \]

and

\[ G \times G' \rightarrow G' \]
\[ (g, g') \mapsto g' \]

**Lemma 2.** The images of the inclusions, $i_1(G)$ and $i_2(G')$ are normal subgroups in $G \times G'$.

**Exercise 3.** Prove the Lemma.
Given a group $G$ and two subgroups $H$ and $K$, we construct the product group $H \times K$, and there is a map:

$$f : H \times K \rightarrow G$$

$$(h, k) \mapsto hk$$

We see the image of $f$ is $HK = \{hk \in G | h \in H, k \in K\}$. Now we are going to study when the above function is an isomorphism, that is, when $G$ is isomorphic to a direct product of two of its subgroups.

**Theorem 4.** $G$ is a group, $H$ and $K$ are its subgroups. Then

$$f : H \times K \rightarrow G$$

defined above is an isomorphism if and only if $H \cap K = \{1\}$, $HK = G$ and $H, K$ are normal subgroups of $G$.

**Proof.** If $f : H \times K \rightarrow G$ is an isomorphism, then normal subgroups map to normal subgroups. Since $H \times \{1\}$ and $\{1\} \times K$ are normal subgroups in $H \times K$, their images, $H$ and $K$, are normal subgroups in $G$.

The image of $f$ is $HK$, and $f$ is an isomorphism, so $HK = G$.

Suppose $H \cap K \neq \{1\}$, then there exists $g \in H \cap K, g \neq 1$. But then $f(g, 1) = g = f(1, g)$, contradict to $f$ is an isomorphism. We conclude $H \cap K = \{1\}$.

Conversely, if $H \cap K = \{1\}$, $HK = G$ and $H, K$ are normal subgroups of $G$, then $f$ is injective: if $f(h_1, k_1) = f(h_2, k_2)$, then $h_1k_1 = h_2k_2$, $h_2^{-1}h_1 = k_2k_1^{-1} \in H \cap K = \{1\}$, we get $h_1 = h_2$ and $k_1 = k_2$.

The assumption $HK = G$ implies $f$ is surjective.

It remains to check $f$ is a homomorphism. $f((h_1, k_1)(h_2, k_2)) = f(h_1h_2, k_1k_2) = h_1h_2k_1k_2$. It suffices to prove $hk = kh$ for any $h \in H$ and $k \in K$. $hk = kh$ if and only if $hkh^{-1}k^{-1} = 1$. Observe that $hkh^{-1}k^{-1} = (hkh^{-1})k^{-1}$. $K$ is a normal subgroup, so $hkh^{-1}k^{-1} \in K$. Similarly we can show $hkh^{-1}k^{-1} \in H$, and by the fact $H \cap K = \{1\}$, we conclude $hkh^{-1}k^{-1} = 1$, i.e., $hk = kh$.

**Corollary 5.** $r$ and $s$ are relatively prime positive integers, then a cyclic group of order $rs$ is isomorphic to the product of a cyclic group of order $r$ and a cyclic group of order $s$. 

2
Proof. $G = < x >$ is a cyclic group of order $rs$. Consider $H = < x^s >$ and $K = x^r$. $|x^r| = s$ and $|x^s| = r$, so $H$ is a cyclic group of order $r$ and $K$ is a cyclic group of order $s$.

Since $r$ and $s$ are relatively prime, we see $|H \cap K| = \{1\}$, so $H \cap K = \{1\}$. $r$ and $s$ are relatively prime implies there exists integers $k$ and $l$ such that $rk + sl = 1$. So for any $m \in \mathbb{Z}$, $m = rkm + slm$. This means

$$x^m = x^{rkm+slm} = (x^s)^{lm}(x^r)^{km} \in HK$$

so $G = HK$.

$H$ and $K$ are normal subgroups in $G$ since $G$ is cyclic, in particular, it is abelian.

Applying the theorem above, we can conclude $G \cong H \times K$. \qed

Remark 6. We know a cyclic group of order $n$ is isomorphic to $\mathbb{Z}/n\mathbb{Z}$, so given relatively prime numbers $r$ and $s$, the above corollary can be expressed as

$$\mathbb{Z}/rs\mathbb{Z} \cong \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$$

And the isomorphism can be explicitly given by

$$\mathbb{Z}/rs\mathbb{Z} \longrightarrow \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$$

$$\bar{k}_{rs} \mapsto \bar{k}_r \times \bar{k}_s$$

This is called the **Chinese Reminder Theorem** (group version). It implies that the system of congruence equations

$$\begin{cases} 
  x \equiv a \pmod{r} \\
  x \equiv b \pmod{s}
\end{cases}$$

has a unique solution up to congruence modulo $rs$ if $r$ and $s$ are relatively prime.

Later when we discuss about ring theory, we will show the ring version of the theorem, and the group version describes parts of the results in the ring version.

**Exercise 7.** Prove the map defined in the above remark

$$\mathbb{Z}/rs\mathbb{Z} \longrightarrow \mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$$

$$\bar{k}_{rs} \mapsto \bar{k}_r \times \bar{k}_s$$

is well-defined, then show it is an isomorphism.
Example 8. Recall that the Klein Four Group $k_4 = \{1, a, b, c\}$ has multiplication table

<table>
<thead>
<tr>
<th></th>
<th>1</th>
<th>a</th>
<th>b</th>
<th>c</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td>1</td>
<td>a</td>
<td>b</td>
<td>c</td>
</tr>
<tr>
<td>a</td>
<td>a</td>
<td>1</td>
<td>c</td>
<td>b</td>
</tr>
<tr>
<td>b</td>
<td>b</td>
<td>c</td>
<td>1</td>
<td>a</td>
</tr>
<tr>
<td>c</td>
<td>c</td>
<td>b</td>
<td>a</td>
<td>1</td>
</tr>
</tbody>
</table>

Consider the cyclic subgroups $< a >$ and $< b >$. Both of them are of order 2.

$< a > \cap < b > = \{1\}$ since $< a > = \{1, a\}$, $< b > = \{1, b\}$

$< a > < b > = K_4$: $1.1 = 1, a.1 = a, 1.b = b, a.b = c$

The multiplication table implies $K_4$ is abelian, so $< a >$ and $< b >$ are normal subgroups.

We conclude $K_4 \cong < a > \times < b > \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$

This example in particular tells us that in the corollary above, if we delete the condition $r$ and $s$ being relatively prime, then the product of two cyclic groups may not be a cyclic group.

Exercise 9. If $x \in G$ and $y \in G'$ such that $|x| = m$, $|y| = n$, then what is the order of $|(x, y)|$ as an element of $G \times G'$?

Exercise 10. Show that If $r, s$ are not relatively prime, then $\mathbb{Z}/r\mathbb{Z} \times \mathbb{Z}/s\mathbb{Z}$ is not isomorphic to $\mathbb{Z}/rs\mathbb{Z}$. 