Definition 1. A **group homomorphism** is a function $f : G \to H$ that satisfies the following for all $x, y \in G$

$$f(xy) = f(x)f(y).$$

Definition 2. A function $f : G \to H$ is

- **injective** (or **one-to-one**) if no two distinct elements $x, y \in G$ satisfy $f(x) = f(y)$.
- **surjective** (or **onto**) if for every element $z \in H$, there is some $x \in G$ with $f(x) = z$.
- **bijective** if it is both injective and surjective

Proposition 3. *The following three conditions are equivalent for a function $f : G \to H$:*

- *f is bijective (i.e. both injective and surjective)*
- *f has an inverse $f^{-1} : H \to G$*
- *G and H are both finite and the same size and f is either injective or surjective*

Definition 4. An **isomorphism** of groups is a bijective function $f : G \to H$ that is also a group homomorphism. Two groups are **isomorphic** if there is some isomorphism between them. This is written as $G \approx H$.

Example 5. Consider the function $f : (\mathbb{R}, +) \to (\mathbb{R}^\times, \times)$ defined by $f(x) = 2^x$. This is a homomorphism since $f(x+y) = 2^{x+y} = 2^x 2^y = f(x)f(y)$. It is not an isomorphism since there is no x with $f(x) < 0$.

Example 6. Let $(\mathbb{R}^+, \times)$ be the group of positive real numbers with the operation of multiplication. This group is isomorphic to $(\mathbb{R}, +)$.

We can use the exact same function as in Example 5. The only difference is this time f is actually a bijection. This is true since $\log_2 : (\mathbb{R}^+, \times) \to (\mathbb{R}, +)$ is its inverse.

Definition 7. Take any two groups G, H. The **product group** $G \times H$ is the group whose elements are in the form (g, h) for $g \in G$ and $h \in H$. Multiplication is defined by

$$(g, h) \cdot (g', h') = (gg', hh').$$

Proposition 8. *The product group actually is a group.*

Proof. This group has identity $(1_G, 1_H)$ where $1_G \in G$ and $1_H \in H$ are the identities in their respective groups.

For an element $(g, h) \in G \times H$, it has inverse (g^{-1}, h^{-1}).

Finally, multiplication in the product group is associative since it is in the original groups.

$$\begin{aligned}((x_1, y_1) \cdot (x_2, y_2)) \cdot (x_3, y_3) &= (x_1 x_2, y_1 y_2) \cdot (x_3, y_3) \\ &= ((x_1 x_2) x_3, (y_1 y_2) y_3) \\ &= (x_1 (x_2 x_3), y_1 (y_2 y_3)) \\ &= (x_1, y_1) \cdot (x_2 x_3, y_2 y_3) \\ &= (x_1, y_1) \cdot ((x_2, y_2) \cdot (x_3, y_3))\end{aligned}$$

□

Example 9. The **Klein Four Group** V_4 is defined to be $\mathbb{Z}_2 \times \mathbb{Z}_2$. It has four elements $e = (0, 0)$, $a = (1, 0)$, $b = (0, 1)$, and $c = (1, 1)$. e is the identity and all other elements are their own inverses. Finally $ab = c$, $ac = b$, and $bc = a$.

Theorem 10 (Chinese Remainder Theorem)**.** *For m, n relatively prime integers,*

$$\mathbb{Z}_m \times \mathbb{Z}_n \approx \mathbb{Z}_{mn}$$

Proof. Define the function $f : \mathbb{Z}_{mn} \to \mathbb{Z}_m \times \mathbb{Z}_n$ that has

$$f(x) = (x \pmod{m}, x \pmod{n}).$$

Note that this is, in fact, a group homomorphism.

Since $\mathbb{Z}_{mn}$ and $\mathbb{Z}_m \times \mathbb{Z}_n$ both have size mn, by Proposition 3, all we need to do is to show that f is either injective or surjective to know that it is a bijection. The fact that f is surjective follows from the number theoretic version of the Chinese Remainder Theorem.

Lemma 11 (Chinese Remainder Theorem)**.** *For m, n relatively prime integers and $0 \le a < m$ and $0 \le b < n$, there is some $0 \le x < mn$ that satisfies*

$$\begin{aligned}x &\equiv a \pmod{m} \\ x &\equiv b \pmod{n}\end{aligned}$$

Proof. To satisfy the first equation, x has to be somewhere in the list $a, a + m, a + 2m, a + 3m, \cdots, a + (n - 1)m$. This list has n different numbers on it. We want to show that one of them has to be $b \pmod{n}$. To do this, what we will show is that all the numbers in this list are different $\pmod{n}$.

What we want to show is that no two numbers in the form $a + im$ and $a + jm$ are the same $\pmod{n}$, or equivalently that their difference isn't a multiple of n. Thus all we need to show is that for $0 \le i, j < n$ and $i \ne j$, $(i - j)m$ isn't a multiple of n.

There are a couple of ways to show this. One way is to note that the statement $n | (i - j)m$ is equivalent to saying $n | (i - j)$ since m and n are relatively prime. Another way is to see that we want $\gcd(n, (i - j)m) = n$, but $\gcd(n, (i - j)m) \le \gcd(n, (i - j)) \gcd(n, m)$, and $\gcd(n, m) = 1$ since they are relatively prime. In either case, what we get is that n must divide $i-j$, which is impossible since $|i-j| < n$ and $i \neq j$.

Therefore all the numbers in our list have a different residue $\pmod{n}$, so one of them must be $b \pmod{n}$, completing our proof. $\square$

By Lemma 11, for any $(a,b) \in \mathbb{Z}_m \times \mathbb{Z}_n$, there is some $x \in \mathbb{Z}_{mn}$ with $x \pmod{m} = a$ and $x \pmod{n} = b$ which means exactly that $f(x) = (a,b)$, so our function is surjective and thus a bijection. $\square$