Isomorphism of groups

The historically first isomorphism between groups, and still an important one, is the isomorphism between $[\mathbb{R}; +]$ and $[\mathbb{R}^+; \times]$, where $\mathbb{R}$ is the set of real numbers and $\mathbb{R}^+$ is the set of positive real numbers. Napier's insight, embeddded in the slide rule he invented, was that if you want to multiply two positive numbers, you can add the two numbers' logarithms together and then exponentiate the sum. That is,

$$x \times y = 10^{\log x + \log y}$$

(where I use log to mean the base ten logarithm, also called the common logarithm). We can rewrite this in terms of the quantities $a = \log x$ and $b = \log y$:

$$10^a \times 10^b = 10^{a+b}.$$

Note that the operation f that (for all a) sends a to 10^a is a bijection between $\mathbb{R}$ and $\mathbb{R}^+$. We can rewrite the previous formula as

$$f(a) \times f(b) = f(a + b)$$

or, writing $+$ as $*_1$ and $\times$ as $*_2$,

$$f(a) *_2 f(b) = f(a *_1 b).$$

More generally, we say that a map f from G_1 to G_2 (where $[G_1; *_1]$ and $[G_2; *_2]$ are groups) is an *isomorphism* of groups if (a) f is a bijection and (b) $f(a *_1 b) = f(a) *_2 f(b)$ for all a, b in G_1.

(This should remind you of the definition of an isomorphism of graphs: we say that a map f from V_1 to V_2 (where (V_1, E_1) and (V_2, E_2) are graphs) is an *isomorphism* of graphs if f is a bijection and

$$\{v, w\} \in E_1 \Leftrightarrow \{f(v), f(w)\} \in E_2$$

for all v, w in E_1.)

Let's look at other examples.

An isomorphism from $[\{0, 1\}; +_2]$ to $[\{+1, -1\}; \times]$ is given by the map f from $\{0, 1\}$ to $\{+1, -1\}$ satisfying $f(0) = +1$ and $f(1) = -1$, i.e., the map $f(a) = (-1)^a$. This is a bijection, and it's easy to check property (b): $f(a *_1 b) = f(a +_2 b) = (-1)^{a+_2 b} = (-1)^{a+b} = (-1)^a \times (-1)^b = f(a) *_2 f(b)$.

The groups $[\{0,1\};+_2]$ and $[\{+1,-1\};\times]$ are isomorphic to each other and also to $[\{F,T\};\mathrm{XOR}]$. In fact, all 2-element groups are isomorphic to these groups. To see why, let e be the identity element of some 2-element group $[G;*]$, and let f be the other element. We have $e*e=e$ and $e*f=f$ and $f*e=f$, so we're forced to have $f*f=e$. (One way to see this is to remember that f must have an inverse; since e isn't an inverse of f, the only other element of G, namely f, must be the inverse of f.) So the map that sends e to 0 and f to 1 is an isomorphism from $[G;*]$ to $[\mathbb{Z}_2;+_2]$.

An isomorphism from $[\{0,1,2,3\};+_4]$ to $[\{+1,+i,-1,-i\};\times]$ is given by the map f satisfying $f(a)=(i)^a$. You can check this by drawing the addition table for $\mathbb{Z}_4$; then replacing 0, 1, 2, and 3 by $+1$, $+i$, -1, and $-i$ respectively; and lastly checking that this new table coincides with the multiplication table for $\{+1,+i,-1,-i\}$. (For more insight into why this works, show that $(i)^{a+_4 b}=(i)^a\times(i)^b$.)

If two algebraic structures are isomorphic, then every "intrinsic" property of one (such as being associative or being commutative) automatically carries over to the other. For example, suppose that $[G_1;*_1]$ is commutative, and suppose that $[G_2;*_2]$ is isomorphic to $[G_1;*_1]$. To show that $[G_2;*_2]$ is commutative as well, we reason as follows: for all x,y in G_2, there exist a,b in G_1 such that $x=f(a)$ and $y=f(b)$, and therefore

$$\begin{aligned} x*_2 y &= f(a)*_2 f(b) \\ &= f(a*_1 b) \text{ (because } f \text{ is an isomorphism)} \\ &= f(b*_1 a) \text{ (because } *_1 \text{ is commutative)} \\ &= f(b)*_2 f(a) \text{(because } f \text{ is an isomorphism)} \\ &= y*_2 x, \end{aligned}$$

proving that $[G_2;*_2]$ is commutative as claimed.

Another property that is preserved by isomorphism is finiteness. If $[G_1,*_1]$ is isomorphic to $[G_2,*_2]$, then either G_1 and G_2 are both finite (and of the same cardinality) or else G_1 and G_2 are both infinite. That's because the isomorphism f is a bijection (property (a)).

Another property that is preserved by isomorphism is the property of being cyclic. $[\mathbb{Z};+]$ is a cyclic group, but $[\mathbb{Z}^2;+]$ is not. So the two groups are not isomorphic. On the other hand, the infinite groups $[\mathbb{Z};+]$ and $[2\mathbb{Z};+]$ are isomorphic, even though the second is a subgroup of the first! An isomorphism from $[\mathbb{Z};+]$ to $[2\mathbb{Z};+]$ is given by the function f satisfying $f(a)=2a$ for all a. This function is a bijection from $\mathbb{Z}$ to $2\mathbb{Z}$.