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, embedded 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)).

If G_1 and G_2 are groups, and e_1 is the identity element of G_1 and e_2 is the identity element of G_1, then any isomorphism from G_1 to G_2 (if one exists) must have the property that $f(e_1)=e_2$. That's because the relation $e_1*_1 e_1=e_1$ implies $f(e_1*_1 e_1)=f(e_1)$, and the left hand side of that equation can be rewritten as $f(e_1)*_2 f(e_1)$ because f is an isomorphisim. So

$f(e_1) *_2 f(e_1) = f(e_1)$; that is, if we write $f(e_1)$ as y, y satisfies $y *_2 y = y$. But this implies that $y = e_2$. So $f(e_1) = e_2$.

Using a similar proof, one can show that the number of solutions to the equation $x^n = e_1$ in G_1 must be equal to the number of solutions to the equation $y^n = e_2$ in G_2. This is related to the claim made in class that the order sequence of G_1 and the order sequence of G_2 must be the same if the two groups are isomorphic.

To prove that two groups are isomorphic, we exhibit an isomorphism between them. (Sometimes one has to explicitly prove that the function one has exhibited is an isomorphism, but other times this step is routine and may be omitted.) To prove that two groups G and G' are NOT isomorphic, we give some invariant that takes on different values for G and G'. One example would be $|G|$ (the order of G). Another would be the number of elements of G satisfying $x * x = e$ (or $x^3 = e$ etc.). Another would be the number of subgroups H of G such that H has order n. Yet another would be the order sequence.

A variant of the idea of isomorphism is the idea of homomorphism. We say that a map f from G_1 to G_2 (where $[G_1; *_1]$ and $[G_2; *_2]$ are groups) is a *homomorphism* of groups if

(*) $\quad f(a *_1 b) = f(a) *_2 f(b)$ for all a, b in G_1.

Compare this with the definition of isomorphism: we've dropped the condition that f is a bijection.

(For fans of math terminology, I'll mention that in the case where the groups G_1 and G_2 are the same group, an isomorphism is called an *automorphism* and a homomoprhism is called an *endomorphism*. But you don't need to know that.)

An example of a homomorphism is the function f from $\mathbb{Z}$ to $\mathbb{Z}_2$ that sends every even integer to 0 and sends every odd integer to 1. You can check that $f(a + b) = a +_2 b$ for all integers a, b. This means that if you want to know the remainder when you divide $a + b$ by 2, compute the remainder r that you get when you divide a by 2 and the remainder s that you get when you divide b by 2 and then compute $r +_2 s$.

Note that if f is a homomorphism, then the formula $f(a *_1 b) = f(a) *_2 f(b)$ extends to bigger formulas like like $f(a *_1 b *_1 c) = f(a) *_2 f(b) *_2 f(c)$.

As an application of this, go back to the homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_2$ discussed two paragraphs ago. If you have n integers $a_1, a_2, \ldots, a_n$, then $f(a_1 + a_2 + \ldots + a_n) = a_1 +_2 a_2 +_2 \ldots +_2 a_n$. Since each a_i is 0 or 1, this right hand sum is just a sum of k 1's, where k is the number of odd terms in

the sum $a_1 + a_2 + \ldots + a_n$. If you think about it for a minute, and maybe try some examples, you'll see that this tells us that the sum $a_1 + a_2 + \ldots + a_n$ is even when k is even and odd when k is odd. This relates to a fact that got mentioned in the lecture notes for chapter 9: in any simple graph, the number of vertices of odd degree must be even because the sum of the degrees (being equal to twice the number of edges) must be even.

The homomorphism from $\mathbb{Z}$ to $\mathbb{Z}_2$ isn't an isolated example; for any positive integer m there's a homomorphism f from $\mathbb{Z}$ to $\mathbb{Z}_m$ that sends each $n \in \mathbb{Z}$ to the remainder when n is divided by m (keeping in mind that even when n is negative the remainder is required to lie between 0 and $m - 1$). When m is 10, $f(n)$ is the last decimal digit of n (when n is positive); in this case, property (*) says that last decimal digit of the sum of two numbers equals what you get when you take just the last decimal digits of the two numbers, add them, divide the sum by ten, and take the remainder.

I'll conclude with two examples of homomorphisms related to Exercise 11.7.8(a) from the textbook. The operation abs$(\cdot)$ from $[\mathbb{R}^*, \times]$ to $[\mathbb{R}^+, \times]$ that sends x to $|x|$ is a homomorphism because abs(x $\times$ y) = abs(x) $\times$ abs(y) (that is, $|xy| = |x||y|$) for all nonzero x, y. Likewise, the operation sign$(\cdot)$ from $[\mathbb{R}^*, \times]$ to $[\{1, -1\}, \times]$ that sends x to $+1$ if x is positive and -1 if x is negative is a homomorphism because $\text{sign}(xy) = \text{sign}(x)\text{sign}(y)$ for all nonzero x, y.