MA294 Lecture

Timothy Kohl

Boston University

February 8, 2024

Group Isomorphisms

Observe that in parallel, in $\mathbb{Z}$ one has $m \cdot 1 + n \cdot 1 = (m+n) \cdot 1 = m + n$ and in C_∞ we have $x^m \cdot x^n = x^{m+n}$, i.e. the exponents in C_∞ add together just as the integers do in $\mathbb{Z}$.

Definition

If $(G_1, *_1)$ and $(G_2, *_2)$ are groups, then a bijection $\beta : G_1 \to G_2$ is an isomorphism if one has

$$\beta(g *_1 h) = \beta(g) *_2 \beta(h)$$

for all $g, h \in G_1$, and we call such a bijection β an isomorphism and write $G_1 \cong G_2$ and say G_1 and G_2 are isomorphic. (iso=same,morph=form)

Recall that a bijection $\beta : G_1 \to G_2$ is a function which is 1-1, namely that $\beta(x) = \beta(y)$ implies $x = y$ and onto, namely that for every $z \in G_2$ there exists $x \in G_1$ such that $\beta(x) = z$.

An isomorphism is therefore a bijection which 'respects' the group structures in both groups, so that, in some way, the groups G_1 and G_2 are equivalent (although not necessarily equal) as groups.

Our first example has already been explored but let's make it official.

$$(\mathbb{Z}, +) \cong (C_\infty, \cdot)$$

by virtue of the function $\beta : \mathbb{Z} \to C_\infty$ given by $\beta(m) = x^m$.

We can verify that β is a bijection.
If $\beta(m) = \beta(n)$ then $x^m = x^n$ which means

$$\begin{gathered} x^m \cdot x^{-n} = x^n x^{-n} \\ \downarrow \\ x^{m-n} = x^0 = 1 \\ \downarrow \\ m - n = 0 \\ \downarrow \\ m = n \end{gathered}$$

And that $\beta : \mathbb{Z} \to C_\infty$ is onto is pretty obvious.

As to respecting the two group structures, observe that
$\beta(m+n) = x^{m+n} = x^m \cdot x^n = \beta(m) \cdot \beta(n)$

and so β is a group isomorphism.

And just as we defined C_∞ as an infinite group consisting of distinct powers $\{x^i\}$ we can also define *the finite cyclic group or order (size) m* for any $m > 1$.

Definition

Let $C_m = \{1, x, \ldots, x^{m-1}\}$ with group operation $x^i \cdot x^j = x^{i+j \ mod \ m}$, namely add the exponents mod m.

For example $C_6 = \{1, x, x^2, x^3, x^4, x^5\}$ where, for instance, $x^3 \cdot x^4 = x^7 = x^1$ since $7 \equiv 1 \ (mod \ 6)$, and where, x^{-i} is $x^{m-i} = x^{6-i}$, e.g. $x^{-2} = x^4$.

And the following is not unexpected.

Theorem

The map $\beta : (\mathbb{Z}_m, +) \to (C_m, \cdot)$ given by $\beta(i) = x^i$ is an isomorphism of groups, namely $(\mathbb{Z}_m, +) \cong (C_m, \cdot)$.

Beyond cyclic groups, there are examples of groups that can be constructed by combining different groups together.

Definition

Given groups $(G_1, *_1)$ and $(G_2, *_2)$ their direct product is the group defined on the set $G_1 \times G_2 = \{(a, b) \mid a \in G_1 \text{ and } b \in G_2\}$ where the group operation is defined as follows:

$$(a, b) * (x, y) = (a *_1 x, b *_2 y)$$

namely the group operations in each coordinate are those of the individual G_i.

For example, the identity of $G_1 \times G_2$ is (e_1, e_2) where e_i is the identity of G_i since $(a, b) * (e_1, e_2) = (a *_1 e_1, b *_2 e_2) = (a, b)$.

Also, $(a, b)^{-1} = (a^{-1}, b^{-1})$ since

$$\begin{aligned}(a, b) * (a^{-1}, b^{-1}) &= (a * a^{-1}, b * b^{-1}) \\ &= (e_1, e_2)\end{aligned}$$

Note, if for a group G we define $|G|$ to be the size of G as a set, then if $|G_1|$ and $|G_2|$ are finite then it's pretty clear that

$$|G_1 \times G_2| = |G_1| \cdot |G_2|$$

which means that we can create groups of different sizes from smaller groups by joining them in a direct product.

The nature of the direct product is not always so obvious, but at least we can work out the details if we know the stucture of each 'component'.

Example: Let $C_2 = \{1, x\}$ the cyclic group of order 2 and let $C_3 = \{1, y, y^2\}$ be the cyclic group of order 3.

We use the symbol 'y' in C_3 to prevent confusion with the 'x' in C_2.

So $x^2 = 1$ and $y^3 = 1$ and therefore

$$C_2 \times C_3 = \{(1,1), (1,y), (1,y^2), (x,1), (x,y), (x,y^2)\}$$

is a group with 6 elements.

So what is the nature of this group?

i.e. Is this group isomorphic to a group we *know*?

Again, the multiplication in $C_2 \times C_3$ is 'coordinate-wise', for example $(x, y)(1, y^2) = (x \cdot 1, y \cdot y^2) = (x, 1)$, and $(x, y)^{-1} = (x^{-1}, y^{-1}) = (x, y^2)$.

CLAIM: $C_2 \times C_3 \cong C_6$

How?

The key observation we want to make is that C_6, being cyclic, is generated by a single element of order 6, namely $C_6 = \langle z \rangle = \{1, z, z^2, z^3, z^4, z^5\}$, specifically every element is a power of a *single element*.

Define

$$\beta : C_6 = \{1, z, .., z^5\} \to C_2 \times C_3 = \{(1,1), (1,y), (1,y^2), (x,1), (x,y), (x,y^2)\}$$

by $\beta(z) = (x, y)$. (What does this mean?)

Defining $\beta(z) = (x, y)$ implies that
$\beta(z^2) = \beta(z \cdot z) = \beta(z)\beta(z) = (x, y)(x, y) = (x^2, y^2) = (1, y^2)$.

Keeping going in this direction we have
$\beta(z^3) = \beta(z^2 \cdot z) = \beta(z^2) \cdot \beta(z) = (1, y^2)(x, y) = (x, y^3) = (x, 1)$.

Keeping going we get $\beta(z^4) = \beta(z^3)\beta(z^1) = (x, 1)(x, y) = (1, y)$, and
$\beta(z^5) = (x, y^2)$.

That is, $\beta(z) = (x, y)$ implies $\beta(z^k) = (x, y)^k$, and it follows that β is 1-1 and onto.

Given that $2 \cdot 3 = 6$, this example makes one wonder if $C_m \times C_n \cong C_{mn}$?

The answer is, not generally, except in the following case.

Theorem

$C_m \times C_n \cong C_{mn}$ if and only if $gcd(m, n) = 1$.

Proof.

(Sketch - The book has the full proof.)

If $C_m = \langle x \rangle$ and $C_n = \langle y \rangle$ where $gcd(m, n) = 1$ then one can prove that $|(x, y)| = mn$. (Exercise!)

As such, if $C_{mn} = \langle z \rangle$ one can define $\beta : C_{mn} \to C_m \times C_n$ by $\beta(z) = (x, y)$ which is 1-1 and onto and preserves the group structure, because if $\beta(z) = (x, y)$ then $\beta(z^i) = (x, y)^i = (x^i, y^i)$. □

For perspective, let's consider the group $C_2 \times C_2$ which we can represent as $\mathbb{Z}_2 \times \mathbb{Z}_2$ which is actually the usual way this group is examined.

As $\mathbb{Z}_2 = \{0, 1\}$ then let $V = \mathbb{Z}_2 \times \mathbb{Z}_2 = \{(0, 0), (0, 1), (1, 0), (1, 1)\}$.

This group is *not* isomorphic to $\mathbb{Z}_4$, in particular because

$$\mathbb{Z}_4 = \langle 1 \rangle = \{0, 1, 1 + 1, 1 + 1 + 1\}$$

while in contrast, V is not generated by a single element, since $(1, 0) + (1, 0) = (0, 0)$, $(0, 1) + (0, 1) = (0, 0)$, and $(1, 1) + (1, 1) = (0, 0)$. That is, every element except the identity has order 2.

V is called the Klein-4 group (Vierergruppe), although there are several 'versions' of this group, which are all isomorphic, but this one is fairly concrete.