Lecture 16

Examples of groups, II: Products and Subgroups

16.1 Goals

1. Understand what the direct product of two groups is.
2. Understand what a subgroup is, and know some examples of subgroups
3. Begin to see examples of group isomorphisms
4. See that automorphisms form a group (true to our philosophy of symmetries)

16.2 Products

We have seen groups in geometric settings (symmetries of mattresses) and algebraic settings (additive groups and groups of units coming from rings).

Today, we'll see ways to construct, and look for, new groups out of groups we already know.

Definition 16.2.1. Let G and H be groups. The *product group*, or *direct product* of G and H is the set $G \times H$ endowed with the following "componentwise" multiplication:

$$(g, h)(g', h') := (gg', hh').$$

We will not prove the following; you can prove it as an exercise if you are curious.

Proposition 16.2.2. Let G and H be groups. Then the product group $G \times H$ is indeed a group.

However, for the record: You can check that the identity element of $G \times H$ is the element (e_G, e_H) and the inverse to (g, h) is (g^{-1}, h^{-1}).

Remark 16.2.3. You already knew about the *set* called $G \times H$. What you're seeing today is that there is a way to naturally define a group operation on this set.

Remark 16.2.4. Using your previously knowledge of direct products: If G and H are finite sets with $\#G$ and $\#H$ elements in each, then $G \times H$ is a finite set with $(\#G) \times (\#H)$ elements.

Example 16.2.5. We have seen that $\mathbb{R}$ is a group under addition. Then the direct product group $\mathbb{R} \times \mathbb{R}$ has a group operation as follows:

$$(x, y) + (x', y') = (x + x', y + y').$$

This is the familiar vector addition in $\mathbb{R}^2$. So you secretly have already been playing with direct product groups.

Example 16.2.6. In the group $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$, we have that

$$(2, 2) + (1, 1) = (0, 3)$$

Example 16.2.7. In the group $\mathbb{Z} \times GL_2(\mathbb{R})$, we have that

$$(n, \begin{pmatrix} a & b \\ c & d \end{pmatrix})(n', \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix}) = (n + n', \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & cb' + dd' \end{pmatrix}).$$

Example 16.2.8. $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/7\mathbb{Z}$ is not isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/5\mathbb{Z}$ because the former has 14 elements, while the latter has 15 elements (hence there could be no bijection between them, let alone a group isomorphism).

Example 16.2.9. Both $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ and $\mathbb{Z}/4\mathbb{Z}$ have four elements. So there exists a bijection between these two sets. However, it turns out that these two groups are not isomorphic (Exercise 16.4.1). This is our first example showing that size alone does not characterize a group.

For some reason, this group comes up so often that it gets a name:

Definition 16.2.10. The group $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is called the *Klein four group*.

Notation 16.2.11. When considering direct products of groups of the form $\mathbb{Z}/n\mathbb{Z}$, it is very common to use the symbol $\oplus$ ("direct sum") instead of the symbol $\times$ (direct product). In this course, you do not need to worry about the difference. But just know that if you see the notation

$$\mathbb{Z}/n\mathbb{Z} \oplus \mathbb{Z}/m\mathbb{Z}$$

in another textbook, the notation represents the exact same group as $\mathbb{Z}/n\mathbb{Z} \times \mathbb{Z}/m\mathbb{Z}$.

However, a word of warning: An *infinite* direct sum—that is, the direct sum of infinitely many abelian groups—is not the same as an infinite product of groups. This has to do with the definitions of each, and we don't give the definition of an infinite direct sum.

16.3 Subgroups

Sometimes, we can find small groups sitting inside large groups.

Definition 16.3.1. Let G be a group, and $H \subset G$ a subset. We say that the subset is a *subgroup* of G if the following holds:

1. $e \in H$ (so H contains the identity element of G),
2. $g \in H \implies g^{-1} \in H$ (so H is closed under taking inverses in G), and
3. $g, g' \in H \implies gg' \in H$ (so H is closed under the group operation).

Example 16.3.2 (The trivial subgroup.)**.** Let G be any group, and let $H = \{e\}$ be the set containing only the identity element. Then H is a subgroup of G. This is called the trivial subgroup.

Likewise, let $H = G$. Then H is a subgroup (so any group is a subgroup of itself). This is also sometimes called a trivial subgroup of G, but less often.

Example 16.3.3. Let $G = \mathbb{Z}$ (under addition). Then the subset $H = 2\mathbb{Z}$ consisting of all even integers is a subgroup. This is because 0 is an even number (so H contains the identity element), the negative of an even number

is even (so H is closed under taking inverses), and the sum of two even numbers is even.

More generally, if n is any integer, then the subset

$$n\mathbb{Z}$$

consisting of all multiplies of n is a subgroup.

Example 16.3.4. Let $G = \mathbb{Q}$ (under addition). Fix a positive integer n, and define a subset

$$\frac{1}{n}\mathbb{Z}$$

to be the set of all rational numbers that can be written as $\frac{a}{n}$ for some integer n. (For example, 0 can be written as $\frac{0}{n}$ and 1 can be written as $\frac{n}{n}$. Of course, $\frac{1}{n}$ is also an element of $\frac{1}{n}\mathbb{Z}$.)

Then $\frac{1}{n}\mathbb{Z}$ is a subgroup of $\mathbb{Q}$.

Example 16.3.5. Recall that given a matrix A, its *transpose* is the matrix A^T whose (i,j)th entry is the (j,i)th entry of A. (When A is a square matrix, you can visualize its transpose as obtained by "flipping" A about its diagonal. This has the effect of turning the columns/rows of A into the rows/columns of A^T.)

We let

$$O_n(\mathbb{R})$$

denote the set of those invertible matrices for which $A^{-1} = A^T$. This is called the *orthogonal group*, or *real orthogonal group* (with n often left implicit).

Then it turns out that $O_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$ (Exercise 16.4.2).

Example 16.3.6. Recall that given a two-by-two matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$$

then the *determinant* of A is the real number $ad - bc$. Let

$$SL_2(\mathbb{R})$$

denote set of all matrices whose determinant is equal to 1. Then $SL_2(\mathbb{R})$ is a subgroup of $GL_2(\mathbb{R})$.

More generally, one can define $SL_n(\mathbb{R})$ to be the set of all n-by-n matrices with determinant equal to 1. (Because this is not a linear algebra class, I won't assume that you know how to define the determinant of a general n-by-n matrix.) Then $SL_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$.

$SL_n(\mathbb{R})$ is called the *special linear group*, or the *real special linear group*.

16.4 Exercises

Exercise 16.4.1. 1. Suppose that G is a group for which every element g satisfies $g^2 = e$. Prove that if H is isomorphic to G, then for every element $h \in H$, $h^2 = e_H$.

2. Prove that $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ is not isomorphic to $\mathbb{Z}/4\mathbb{Z}$.

Exercise 16.4.2. Prove that $O_n(\mathbb{R})$ is a subgroup of $GL_n(\mathbb{R})$.

Exercise 16.4.3. Prove that $SL_2(\mathbb{R})$ is a subgroup of $GL_2(\mathbb{R})$. Hint: $\det(AB) = \det(A)\det(B)$.

Exercise 16.4.4. Consider a 2-by-2 matrix

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix}.$$

Prove that $A \in O_2(\mathbb{R})$ if and only if all of the following are satisfied:

(a) $a^2 + c^2 = 1$ and $b^2 + d^2 = 1$ (so that the columns of A are vectors of norm 1).

(b) The inner product of the vector (a, c) with the vector (b, d) is zero (so that the columns of A are orthogonal to each other).

(In other words, the columns of A are *orthonormal*.)

If you like, you can prove more generally that an n-by-n matrix A is an element of $O_n(\mathbb{R})$ if and only if the columns of A are orthonomal.

Exercise 16.4.5. Fix an integer $n \geq 1$, and consider the group $n\mathbb{Z}$ (Example 16.3.3).

(a) Show that $n\mathbb{Z}$ is isomorphic to $\mathbb{Z}$ (as groups).

(b) Let m be any integer ≥ 1. Show that $m\mathbb{Z}$ and $n\mathbb{Z}$ are isomorphic.

Exercise 16.4.6. Suppose that G is a group, and g is an element of G satisfying the following: There exists some $h \in G$ so that $h^n = g$.

(a) Let $f : G \to K$ be a group isomorphism. Prove that there exists an element $k \in K$ for which $k^n = \phi(g)$.

(b) Prove that $\mathbb{Z}$ is not isomorphic to $\mathbb{Q}$.

By the way: $\mathbb{Z}$ and $\mathbb{Q}$ are another example of two groups with the same cardinality that are not isomorphic.

Exercise 16.4.7. Recall the Klein four group (Definition 16.2.10).

(a) Write out the group operation table of the Klein four group. (This will be a 4-by-4 "addition table.")

(b) Show that the Klein four-group is isomorphic to the symmetries of a (non-square) mattress (Section 14.4).