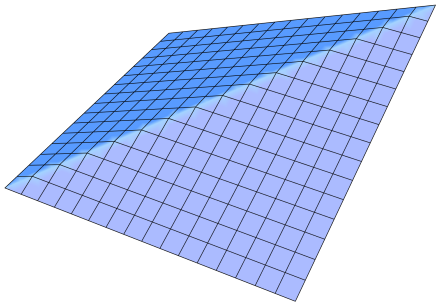


PMATH 336: Group Theory with Applications

Prof. Tyrone Ghaswala • Fall 2015 • University of Waterloo
MWF 9:30–10:20AM in MC 4064

Transcribed, LaTeXed, and edited by Rob Zimmerman

Note: These are personal lecture notes, not official course materials. They may contain errors (which by default you should attribute to me, Rob Zimmerman, rather than the course instructor). The permanent home of these — and all of my other lecture notes — is https://rob-zimmerman.github.io/coursenotes.

Contents

1 Group Examples and Basic Structure **3**
Group Theory with Applications . . . 3
Matrix Groups . . . 6
Group Axioms . . . 7
Basic Properties of Groups . . . 8
Dihedral Groups . . . 9
Symmetric Groups . . . 10

Classification of Groups . . . 13
Subgroups and Cosets . . . 15

2 Group Arithmetic and Homomorphisms 23
Fermat's Little Theorem . . . 24
More on Symmetric Groups . . . 24
Odd and Even Permutations . . . 27
Orders and Generators . . . 34
Homomorphisms . . . 34
Isomorphisms . . . 39

3 Quotients and Isomorphism Theorems 42
Normal Subgroups and Quotients . . . 42
The Quaternion Group . . . 47
The First Isomorphism Theorem . . . 49
Subgroup Lattices . . . 51
Correspondence Theorem . . . 53

4 Automorphism Groups 56
Conjugation . . . 58
Set-Theoretic Conventions . . . 60

5 Group Actions and Counting 62
Group Actions . . . 62
Cayley's Theorem . . . 64
Orbit-Stabilizer Theorem . . . 65
Equivalence Relations and Partitions . . . 68
Cauchy's Theorem . . . 70
Natural Actions on the Group Itself . . . 72
Counting Problems . . . 75
The Lemma That is Not Burnside's . . . 76

6 Symmetry Groups and Applications 79
Platonic Solids . . . 79
Rotational Symmetry Groups . . . 81
Generating Sets and Alternating Groups . . . 85
The Dodecahedron, Octahedron and Icosahedron . . . 89
Finite Abelian Groups . . . 91
Banach–Tarski Paradox . . . 97
Low-Dimensional Topology . . . 98

Appendix: Lecture and Tutorial Index **100**

Lecture 1 — Monday, September 14, 2015

1. Group Examples and Basic Structure

Group Theory with Applications

Group theory is the study of **symmetry**. How did it come to be? One of its historical origins is the work of Evariste Galois on the insolvability of the quintic by radicals, which he scribbled down on a piece of paper the night before the duel in which he tragically lost his life. We should be careful not to perish in the same manner.

We begin with examples of groups before giving the formal axioms.

Example 1.1 The integers under addition form the group

$$(\mathbb{Z}, +) = (\{\dots, -2, -1, 0, 1, 2, \dots\}, +).$$

Example 1.2 The set $\{-1, 1\}$ under multiplication is a group. Its Cayley table is

	-1	1
-1	1	-1
1	-1	1

The identity element is 1.

Example 1.3 The rational numbers under addition form the group $(\mathbb{Q}, +)$. The identity is 0, and the inverse of a/b under addition is $-a/b$.

Example 1.4 The nonzero rational numbers under multiplication form the group $(\mathbb{Q}^*, \cdot)$. The identity is 1, and the inverse of a/b is b/a. Here $a \neq 0$ by the definition $\mathbb{Q}^* = \mathbb{Q} \setminus \{0\}$.

Example 1.5 The complex numbers under addition form the group $(\mathbb{C}, +)$. The identity is 0, and the inverse of z under addition is $-z$.

Example 1.6 The nonzero complex numbers under multiplication form the group $(\mathbb{C}^*, \cdot)$. The identity is 1, and the inverse of z is $1/z$.

Example 1.7 The set $\{1, i, -1, -i\}$ is a group under multiplication. Here i is the usual imaginary unit, which satisfies $i^2 = i \cdot i = -1$.

We will see soon that the real general linear group is

$$GL_n(\mathbb{R}) = \{\mathbf{A} \in M_n(\mathbb{R}) : \mathbf{A} \text{ is invertible}\}.$$

An $n \times n$ matrix is invertible exactly when its determinant is nonzero, and the operation in this group is matrix multiplication. Matrix multiplication is not commutative in general: we can have $\mathbf{AB} \neq \mathbf{BA}$.

The same construction works over any field $\mathbb{F}$, giving the general linear group

$$GL_n(\mathbb{F}) = \{\mathbf{A} \in M_n(\mathbb{F}) : \det(\mathbf{A}) \neq 0\}.$$

Lecture 2 — Wednesday, September 16, 2015

The examples above come from familiar number systems. Modular arithmetic supplies another important class of examples.

The integers modulo n are

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}.$$

They come equipped with addition and multiplication modulo n.

Definition 2.1 An element $a \in \mathbb{Z}_n$ is called a **unit** if there exists an element $a^{-1} \in \mathbb{Z}_n$ such that $aa^{-1} = 1$.

Definition 2.2 The **group of units modulo n** is

$$\mathbb{Z}_n^* = \{a \in \mathbb{Z}_n : a \text{ is a unit}\}.$$

Example 2.3 In $\mathbb{Z}_9$, the units are the residue classes x for which we can solve

$$x \cdot x^{-1} \equiv 1 \pmod 9.$$

Thus

$$\mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}.$$

Recall from elementary number theory that $a \in \mathbb{Z}_n^*$ if and only if $\gcd(a, n) = 1$. This criterion lets us recognize units without explicitly searching for multiplicative inverses.

From these, we get two families of groups: $(\mathbb{Z}_n, +)$ and $(\mathbb{Z}_n^*, \cdot)$.

Definition 2.4 The operation table for a group is called a **Cayley table**.

Notation 2.5 When the operation is unambiguous, we will drop it from the notation of a group. For example, we may write $\mathbb{Z}_n$ instead of $(\mathbb{Z}_n, +)$.

Notation 2.6 When the operation is understood, we may also write ab instead of $a \cdot b$, for example.

Definition 2.7 Let G be a group. The **order** of G, denoted $|G|$, is the number of elements in G.

For example, $|\mathbb{Z}| = \infty$, $|\mathbb{Z}_n| = n$, $|\mathbb{Z}_4^*| = 2$, and $|\mathbb{Z}_n^*| = \phi(n)$, where ϕ is the Euler totient function.

Definition 2.8 Let G be a group. An element $e \in G$ is called an **identity** if $ae = ea = a$ for all $a \in G$.

Definition 2.9 Let G be a group with identity e. Suppose $a \in G$ and $b \in G$ satisfy $ab = ba = e$. Then b is called the **inverse** of a, and is denoted by a^{-1}.

Matrix Groups

Matrix groups provide a large and flexible source of examples.

Definition 2.10 The **real general linear group** is

$$GL_n(\mathbb{R}) := \{\mathbf{A} \in M_{n\times n}(\mathbb{R}) : \mathbf{A} \text{ is invertible}\}.$$

A matrix in $GL_n(\mathbb{R})$ is invertible exactly when its determinant is nonzero, and the group operation is matrix multiplication.

Exercise 2.11 If $\mathbf{B} = \begin{pmatrix} 1 & 2 \\ -1 & -1 \end{pmatrix}$ and $\mathbf{A} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix}$, then show $\mathbf{AB} \neq \mathbf{BA}$. Can you handle this?

Definition 2.12 Let $\mathbb{F}$ be a field. The **general general [sic] linear group over** $\mathbb{F}$ is

$$GL_n(\mathbb{F}) := \{\mathbf{A} \in M_{n\times n}(\mathbb{F}) : \det(\mathbf{A}) \neq 0\}.$$

Lecture 3 — Friday, September 18, 2015

The determinant criterion is easy to use in concrete computations, as the following modular example shows.

Example 3.1 Let

$$\mathbf{A} = \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \in M_{2\times 2}(\mathbb{Z}_{15}).$$

Then

$$\det(\mathbf{A}) = 1 \cdot 4 + (-2) \cdot 3 \equiv 1 \cdot 4 + 13 \cdot 3 \equiv 43 \equiv 13 \pmod{15}.$$

Is $13 \in \mathbb{Z}_{15}^*$? Certainly, since $\gcd(13, 15) = 1$. Therefore $\mathbf{A}$ is invertible over $\mathbb{Z}_{15}$. Its inverse is

$$\begin{aligned}
\mathbf{A}^{-1} &= \frac{1}{\det(\mathbf{A})} \begin{pmatrix} 4 & -2 \\ -3 & 1 \end{pmatrix} \\
&= \frac{1}{13} \begin{pmatrix} 4 & 13 \\ 12 & 1 \end{pmatrix} \\
&= 7 \begin{pmatrix} 4 & 13 \\ 12 & 1 \end{pmatrix} \\
&= \begin{pmatrix} 28 & 91 \\ 84 & 7 \end{pmatrix} \\
&\equiv \begin{pmatrix} 13 & 1 \\ 9 & 7 \end{pmatrix} \pmod{15}.
\end{aligned}$$

Indeed,

$$\begin{aligned}
\mathbf{A}\mathbf{A}^{-1} &= \begin{pmatrix} 1 & 2 \\ 3 & 4 \end{pmatrix} \begin{pmatrix} 13 & 1 \\ 9 & 7 \end{pmatrix} \\
&= \begin{pmatrix} 31 & 15 \\ 75 & 31 \end{pmatrix} \\
&\equiv \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \pmod{15} \\
&= \mathbf{I}.
\end{aligned}$$

Group Axioms

Definition 3.2 A **group** is a set G with a binary operation $\cdot$ such that the following hold:

1. For all $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;
2. There exists $e \in G$ such that $a \cdot e = e \cdot a = a$ for all $a \in G$;
3. For every $a \in G$, there exists $a^{-1} \in G$ such that $a \cdot a^{-1} = a^{-1} \cdot a = e$.

The axioms capture exactly the features of the examples we have been using: multiplication can be regrouped, there is an element that does nothing, and every element can be undone.

Definition 3.3 Two elements $a, b \in G$ **commute** if $ab = ba$. If every pair of elements of G commutes, then G is **abelian**.

Basic Properties of Groups

Proposition 3.4 In a group G, there is exactly one element $e \in G$ such that $ea = ae = a$ for all $a \in G$.

Proof. Suppose e and f are both identity elements. Since f is an identity, $fe = e$. Since e is an identity, $fe = f$. Therefore $e = f$. □

Proposition 3.5 Every element $a \in G$ has a unique inverse.

Proof. Suppose $b, c \in G$ are both inverses of a. Then $ab = ba = e$ and $ac = ca = e$. Hence

$$b = be = b(ac) = (ba)c = ec = c.$$

Therefore the inverse of a is unique. □

Proposition 3.6 Let $a, b, c \in G$. If $ab = ac$, then $b = c$. If $ba = ca$, then $b = c$.

Proof. If $ab = ac$, then multiplying on the left by a^{-1} gives

$$a^{-1}(ab) = a^{-1}(ac), \qquad (a^{-1}a)b = (a^{-1}a)c, \qquad \text{and} \qquad eb = ec,$$

and hence $b = c$. Similarly, if $ba = ca$, then multiplying on the right by a^{-1} gives

$$(ba)a^{-1} = (ca)a^{-1}, \qquad b(aa^{-1}) = c(aa^{-1}), \qquad \text{and} \qquad be = ce,$$

and hence $b = c$. □

Lecture 4 — Monday, September 21, 2015

We recall the group axioms. A group is a set G with a binary operation $\cdot$ such that:

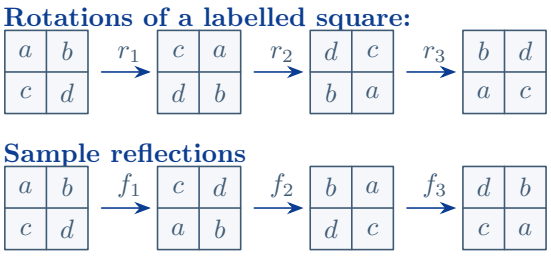
1. for any $a, b, c \in G$, $(a \cdot b) \cdot c = a \cdot (b \cdot c)$;
2. there exists $e \in G$ such that $ae = ea = a$ for all $a \in G$;
3. for every $a \in G$, there exists $a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = e$.

A binary operation on a set S is a function that takes two values of S and returns an element of S.

Dihedral Groups

For integers $n \geq 3$, we have a group D_n, the group of symmetries of a regular n-gon.

Example 4.1 The group D_4 is the group of symmetries of a square. Its operation is composition. The rotations and sample reflections in Figure 1 make the action concrete.



These pictures make it easy to track compositions in D_4.

FIGURE 1

Example 4.2 The composition $f_2 r_1$, in which r_1 is applied first, is shown in Figure 2.

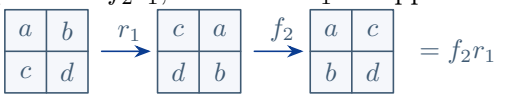


FIGURE 2

Example 4.3 Reversing the order gives the different composition $r_1 f_2$ shown in Figure 3.

FIGURE 3

The two final labelings differ, so $f_2 r_1 \neq r_1 f_2$. Therefore D_4 is not abelian.

Example 4.4 Find the order of D_n for general $n \geq 3$.

Solution. Every symmetry of a regular n-gon is either a rotation or a reflection. There are exactly n rotations, including the identity, and exactly n reflections, one for each axis of symmetry. Therefore

$$|D_n| = n + n = 2n.$$

□

Symmetric Groups

For each integer $n \geq 1$, we have the **symmetric group** S_n, which is sometimes also called a **permutation group**. The elements of S_n are the bijections from $\{1, 2, \ldots, n\}$ to itself, and the operation is composition, which we write as $*$. We can think of an element of S_n as a way to rearrange n objects.

One way to visualize an element of S_n is to draw two rows of n dots and join them so that every dot in the top row is connected to exactly one dot in the bottom row. Figure 4 shows two such elements and their composition.

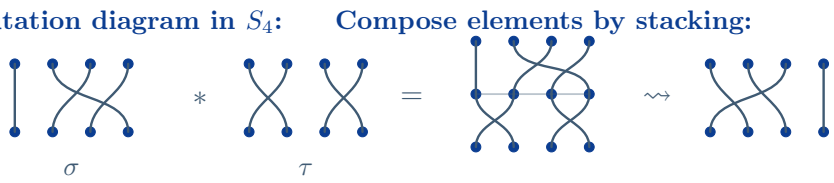


FIGURE 4

Diagrammatically, we compose two permutations by placing the second diagram under the first and following the strands.

Example 4.5 Prove that S_n is a group.

Solution. The set S_n consists of all bijections from $\{1, \ldots, n\}$ to itself, and the operation is composition. If $\sigma, \tau \in S_n$, then $\sigma * \tau$ is again a bijection, so S_n is closed under the operation. Associativity holds because composition of functions is associative. The identity map on $\{1, \ldots, n\}$ lies in S_n and acts as an identity element. Finally, every bijection has an inverse bijection, so each element of S_n has an inverse in S_n. Thus S_n is a group. □

Proposition 4.6 For every integer $n \geq 1$, we have $|S_n| = n!$.

Proof. A permutation of $\{1, \ldots, n\}$ is determined by choosing the image of 1, then the image of 2, and so on. There are n choices for the image of 1, then $n - 1$ choices for the image of 2, and continuing in this way gives

$$n(n-1)\cdots 2 \cdot 1 = n!$$

permutations. □

Braid groups provide another geometric family of examples. For $n \geq 1$, the braid group on n strands is denoted B_n, and its elements are called **braids**. The operation is given by stacking diagrams, in the same spirit that permutations compose by following one arrangement after another. Two braids represent the same element if one can be deformed into the other without moving the endpoints. Multiplication and deformation of braids are illustrated in Figure 5. A useful analogy is that B_n is to S_n as $\mathbb{Z}$ is to $\mathbb{Z}_n$.

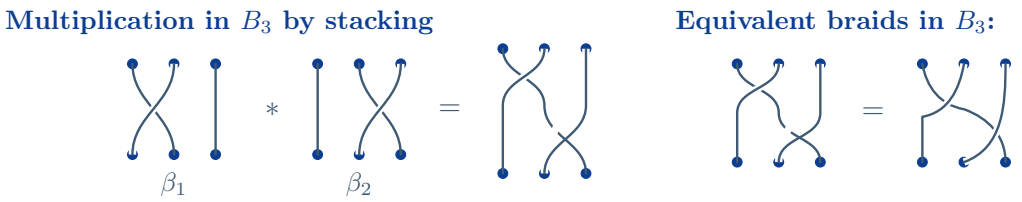


FIGURE 5

For more on braids, watch Braids - The Movie.

Lecture 5 — Wednesday, September 23, 2015

Definition 5.1 Let $(G, *)$ and $(H, \circ)$ be groups. The **direct product** of G and H is the group $(G \times H, \cdot)$, where

$$G \times H = \{(g, h) : g \in G,\ h \in H\}$$

and

$$(g_1, h_1) \cdot (g_2, h_2) = (g_1 * g_2, h_1 \circ h_2).$$

Direct products let us build larger groups from smaller ones while keeping the two operations independent. The projections onto the two coordinates remember the original factors.

Example 5.2 Find the identity element and inverses in $G \times H$. Prove that $G \times H$ is a group, and determine $|G \times H|$.

Solution. If e_G and e_H denote the identity elements of G and H, then (e_G, e_H) is the identity in $G \times H$, since

$$(g, h) \cdot (e_G, e_H) = (ge_G, he_H) = (g, h) = (e_G g, e_H h) = (e_G, e_H) \cdot (g, h).$$

The inverse of (g, h) is (g^{-1}, h^{-1}), because

$$(g, h) \cdot (g^{-1}, h^{-1}) = (gg^{-1}, hh^{-1}) = (e_G, e_H).$$

The reverse product is likewise $(g^{-1}g, h^{-1}h) = (e_G, e_H)$. Closure is immediate from the definition

of the operation, and associativity follows componentwise from associativity in G and H:

$$((g_1, h_1) \cdot (g_2, h_2)) \cdot (g_3, h_3) = (g_1(g_2 g_3), h_1(h_2 h_3)) = (g_1, h_1) \cdot ((g_2, h_2) \cdot (g_3, h_3)).$$

Therefore $G \times H$ is a group. If G and H are finite, then each element of $G \times H$ is an ordered pair (g, h) with $g \in G$ and $h \in H$, so

$$|G \times H| = |G|\,|H|.$$

□

Classification of Groups

A natural structural question is classification: up to isomorphism, which groups of order n can occur? For $n = 1$, there is only the trivial group.

For $n = 2$, examples include $\mathbb{Z}_2$, $\{1, -1\}$ under multiplication, and $\mathbb{Z}_4^*$. Their Cayley tables are compared in Figure 6.

$\mathbb{Z}_2$

$+$	0	1
0	0	1
1	1	0

$\{1, -1\}$

$\cdot$	1	-1
1	1	-1
-1	-1	1

$\mathbb{Z}_4^*$

$\cdot$	1	3
1	1	3
3	3	1

Generic table

$*$	$\circ$	$\square$
$\circ$	$\circ$	$\square$
$\square$	$\square$	$\circ$

FIGURE 6

Their Cayley tables are the same up to relabelling. To see why, suppose we have a group with two elements, $\circ$ and $\square$, and operation $*$.

Lemma 5.3 In any row or column of a Cayley table of a group, every element of the group appears exactly once.

Proof. Fix $a \in G$. If $ab = ac$, then cancellation gives $b = c$, so the entries in the row indexed by a are distinct. Since the row has $|G|$ entries and every entry lies in G, every element of G appears exactly once. The same argument, using right cancellation, applies to columns. □

For $n = 3$, examples include $\mathbb{Z}_3$, the rotation group $\{e, r_1, r_2\}$ of a labelled triangle, and the matrix

group $\{\mathbf{I}, \mathbf{A}, \mathbf{B}\}$, where

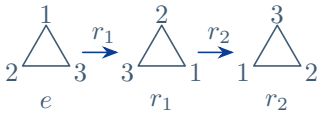
$$\mathbf{I} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \qquad \mathbf{A} = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}, \qquad \text{and} \qquad \mathbf{B} = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}.$$

Figure 7 compares the cyclic, geometric, and matrix models.

$\mathbb{Z}_3 = \{0, 1, 2\}$

$+$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Rotations of a labelled triangle



$\circ$	e	r_1	r_2
e	e	r_1	r_2
r_1	r_1	r_2	e
r_2	r_2	e	r_1

Matrix model

$\{\mathbf{I}, \mathbf{A}, \mathbf{B}\}$

$\cdot$	**I**	**A**	**B**
I	**I**	**A**	**B**
A	**A**	**B**	**I**
B	**B**	**I**	**A**

FIGURE 7

Relabelling $0 \leftrightarrow e \leftrightarrow \mathbf{I}$, $1 \leftrightarrow r_1 \leftrightarrow \mathbf{A}$, and $2 \leftrightarrow r_2 \leftrightarrow \mathbf{B}$ makes these three Cayley tables identical. This is the concrete reason that these three groups are isomorphic.

Suppose $G = \{e, a, b\}$. In the Cayley table

	e	a	b
e	e	a	b
a	a		
b	b		

,

the remaining entries are forced by the preceding lemma. Thus all groups of order 3 have the same Cayley table up to relabelling.

For now, we call two finite groups **isomorphic** if, after relabelling and reordering the elements, their Cayley tables are the same.

Editorial Note Finiteness only makes the Cayley-table comparison practical to display. The formal definition of isomorphism given later applies equally to infinite groups and expresses the same relabelling idea without requiring a finite table.

Thus all groups of order 1, 2, and 3 are unique up to isomorphism.

Example 5.4 Prove that $\mathbb{Z}_2 \times \mathbb{Z}_2 \ncong \mathbb{Z}_4$. Prove that any group of order 4 is isomorphic to either $\mathbb{Z}_2 \times \mathbb{Z}_2$ or $\mathbb{Z}_4$.

Solution. First, $\mathbb{Z}_4$ contains an element whose repeated sums generate all four elements, namely 1. In contrast, every nonzero element of $\mathbb{Z}_2 \times \mathbb{Z}_2$ satisfies $x + x = (0, 0)$. Since isomorphisms preserve multiplication tables, these two groups cannot be isomorphic.

Now let G be a group of order 4. Suppose some $a \in G$ satisfies $a^2 \neq e$. We first show that $a^3 \neq e$. Otherwise e, a, a^2 would be distinct, and if b were the fourth element of G, left multiplication by a would permute e, a, a^2 cyclically. It would therefore have to fix b, which would give $ab = b$ and hence $a = e$, a contradiction. The elements e, a, a^2, a^3 are now distinct: the remaining possible equalities would force either $a = e$ or $a^2 = e$. They therefore exhaust G. Left multiplication by a sends the first three of them to a, a^2, a^3, so it must send a^3 to e. Thus $a^4 = e$, and $G = \langle a \rangle \cong \mathbb{Z}_4$.

Otherwise every nonidentity element squares to e. Writing $G = \{e, a, b, c\}$, we see that ab cannot be e, a, or b, so $ab = c$. The same argument shows $ba = c$, hence $ab = ba$. Similarly, $ac = ca = b$ and $bc = cb = a$. Thus the Cayley table of G agrees with that of $\mathbb{Z}_2 \times \mathbb{Z}_2$, so $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. □

Subgroups and Cosets

Roughly speaking, a subgroup is a group living inside another group. For example, $2\mathbb{Z} < \mathbb{Z}$: the even integers form a group under addition inside the group of all integers.

Example 5.5 Find all subgroups of $\mathbb{Z}_6$.

Solution. Any subgroup $H \leq \mathbb{Z}_6$ must contain 0. If $1 \in H$, then repeated addition gives every element of $\mathbb{Z}_6$, so $H = \mathbb{Z}_6$. The same is true if $5 \in H$, since $5 \equiv -1 \pmod 6$. If $2 \in H$, then H contains

$$0,\ 2,\ 2 + 2 = 4,$$

so $\{0, 2, 4\} \subseteq H$; this set is already closed under addition modulo 6, so it is a subgroup. Similarly, if $4 \in H$, then $2 = 4 + 4 \in H$, so we again obtain $\{0, 2, 4\}$. If $3 \in H$, then H contains $\{0, 3\}$, and this is closed under addition modulo 6. Therefore the subgroups of $\mathbb{Z}_6$ are

$$\{0\}, \qquad \{0, 3\}, \qquad \{0, 2, 4\}, \qquad \text{and} \qquad \mathbb{Z}_6.$$

□

Lecture 6 — Friday, September 25, 2015

We now make this informal picture precise.

Definition 6.1 Let $(G, \cdot)$ be a group. A **subgroup** $S \leq G$ is a subset $S \subseteq G$ such that $(S, \cdot)$ is itself a group.

Any group automatically comes with two subgroups: G itself, and $\{e\}$.

Definition 6.2 A subgroup $S \leq G$ such that $S \neq G$ and $S \neq \{e\}$ is called a **proper subgroup**.

Powers of a single element lead to another basic construction.

Definition 6.3 Let $a \in G$. For any $k \in \mathbb{Z}$, define $a^k \in G$ by

$$a^k = \begin{cases} a \cdot a \cdot \cdots \cdot a & \text{if } k > 0, \\ e & \text{if } k = 0, \\ (a^{-1}) \cdot \cdots \cdot (a^{-1}) & \text{if } k < 0. \end{cases}$$

In the first case there are k copies of a, and in the last case there are $-k$ copies of a^{-1}.

Example 6.4 Show that $a^n a^m = a^{n+m}$ for all $n, m \in \mathbb{Z}$. Show that $(a^n)^{-1} = a^{-n}$ for all $n \in \mathbb{Z}$.

Solution. If $n, m \geq 0$, then $a^n a^m = a^{n+m}$ follows directly from the definition of powers and associativity. If $m = -r < 0$ with $r > 0$, then for $n \geq r$ we have

$$a^n a^{-r} = a^{n-r}(a^r a^{-r}) = a^{n-r} = a^{n+m},$$

while for $n < r$ we have

$$a^n a^{-r} = (a^n a^{-n})a^{-(r-n)} = a^{-(r-n)} = a^{n-r} = a^{n+m}.$$

The case $n < 0 \leq m$ is similar, and if $n = -s < 0$ and $m = -r < 0$, then

$$a^n a^m = (a^{-1})^s (a^{-1})^r = (a^{-1})^{s+r} = a^{-(s+r)} = a^{n+m}.$$

Therefore $a^n a^m = a^{n+m}$ for all integers n and m.

Taking $m = -n$ gives

$$a^n a^{-n} = a^0 = e = a^{-n} a^n,$$

so a^{-n} is an inverse of a^n. By uniqueness of inverses, $(a^n)^{-1} = a^{-n}$. □

Definition 6.5 Let $a \in G$. The **order** of a, denoted $|a|$, is the smallest $k \in \mathbb{Z}^+$ such that $a^k = e$. If no such k exists, then we say that a has **infinite order**.

Definition 6.6 Let $a \in G$. The **subgroup generated by a**, denoted $\langle a \rangle$, is

$$\langle a \rangle = \{a^k : k \in \mathbb{Z}\}.$$

Proposition 6.7 For every $a \in G$, the order of a equals the order of its generated subgroup:

$$|a| = |\langle a \rangle|.$$

Proof. If $|a| = n < \infty$, then

$$\langle a \rangle = \{e, a, a^2, \ldots, a^{n-1}\}.$$

These elements are distinct: if $a^i = a^j$ with $0 \leq i < j < n$, then $a^{j-i} = e$, contradicting the minimality of n. Every other power reduces to one of them by division of its exponent by n. Hence $|\langle a \rangle| = n$.

If a has infinite order, then all the powers a^k, $k \in \mathbb{Z}$, are distinct, since $a^i = a^j$ with $i < j$ would give $a^{j-i} = e$. Thus $\langle a \rangle$ is infinite as well. □

Example 6.8 The set $\langle a \rangle$ is always a subgroup of G.

Example 6.9 If $G = \mathbb{Z}$, then

$$\langle 2 \rangle = 2\mathbb{Z} = \{\dots, -2, 0, 2, 4, \dots\}.$$

Example 6.10 If $G = S_3$ and $a \in S_3$ has order 2, then $a^2 = e$, so the subgroup generated by a is

$$\langle a \rangle = \{a, e\} \cong \mathbb{Z}_2.$$

For instance, if a swaps 1 and 2, the generated subgroup is shown in Figure 8.

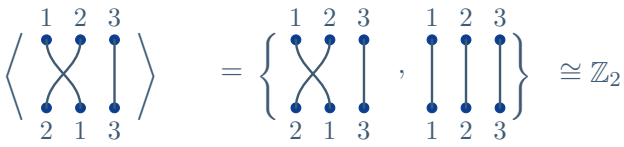


FIGURE 8

Example 6.11 Let $G = \mathbb{Z}_9^* = \{1, 2, 4, 5, 7, 8\}$. For the element 4, we have

k	$\dots$	-4	-3	-2	-1	0	1	2	3	4
4^k	$\dots$	7	1	4	7	1	4	7	1	4

and hence $\langle 4 \rangle = \{1, 4, 7\}$. Thus $|\langle 4 \rangle| = 3$.

Lecture 7 — Monday, September 28, 2015

We continue with subgroups, cosets, and Lagrange's theorem.

Example 7.1 Not every subgroup is generated by one element. Let $G = \mathbb{Z}_4 \times \mathbb{Z}_4$ and

$$H = \{(0,0), (2,0), (0,2), (2,2)\}.$$

Then $H < G$, but

$$\langle (0,0) \rangle = \{(0,0)\}, \qquad \langle (2,0) \rangle = \{(2,0), (0,0)\},$$

$$\langle(0,2)\rangle = \{(0,2),(0,0)\} \qquad \text{and} \qquad \langle(2,2)\rangle = \{(0,0),(2,2)\}.$$

Thus no single element of H generates all of H.

The following criterion is often the quickest way to verify that a subset is a subgroup.

Theorem 7.2 (Subgroup test) Let $(G,\cdot)$ be a group and let $H \subseteq G$ be a nonempty subset. Suppose the following hold:

1. For every $a, b \in H$, $a \cdot b \in H$.
2. For every $a \in H$, $a^{-1} \in H$.

Then H is a subgroup of G.

Proof. The condition (1) says that $\cdot$ restricts to a binary operation on H.

Since G is a group, $(ab)c = a(bc)$ for all $a, b, c \in H$, so associativity holds in H. Choose $a \in H$, which is possible because H is nonempty. By (2), we have $a^{-1} \in H$, and then (1) gives $aa^{-1} = e \in H$. Finally, (2) says that every element of H has its inverse in H. Therefore H is a group under the restricted operation, so $H \leq G$. □

The following examples suggest the statement of Lagrange's theorem.

G	H	$\lvert G\rvert$	$\lvert H\rvert$
$\mathbb{Z}_8$	$\langle 2\rangle$	8	4
$\mathbb{Z}_4 \times \mathbb{Z}_4$	$\{(0,0),(2,0),(0,2),(2,2)\}$	16	4
D_n	$\langle f\rangle$	$2n$	2
D_n	$\langle r\rangle$	$2n$	n
$\mathbb{Z}_9^*$	$\langle 2\rangle$	6	6
$\mathbb{Z}_9^*$	$\langle 8\rangle$	6	2
$GL_2(\mathbb{Z}_3)$	$SL_2(\mathbb{Z}_3)$	48	24

For $G = \mathbb{Z}_{12}$, the orders $|x|$ for $x \in \{0,1,2,3,4,5,6,7,8,9,10,11\}$ are

$$\{1,12,6,4,3,12,2,12,3,4,6,12\} = |\langle x\rangle|.$$

Cosets describe how a subgroup sits inside the ambient group by translating it through the group operation.

Example 7.3 Let $G = \mathbb{Z}$ and $H = 4\mathbb{Z} = \{\dots, -8, -4, 0, 4, 8, \dots\}$. Then

$$1 + 4\mathbb{Z} = \{\dots, -7, -3, 1, 5, 9, \dots\},$$

$$2 + 4\mathbb{Z} = \{\dots, -6, -2, 2, 6, 10, \dots\},$$

and

$$3 + 4\mathbb{Z} = \{\dots, -5, -1, 3, 7, \dots\}.$$

These are all the cosets. For example,

$$7 + 4\mathbb{Z} = -1 + 4\mathbb{Z} = 3 + 4\mathbb{Z}.$$

Example 7.4 Let $G = \mathbb{Z}_9$ and $H = \langle 3 \rangle = \{0, 3, 6\}$. Then

$$1 + H = \{1, 4, 7\}, \qquad 2 + H = \{2, 5, 8\}, \qquad \text{and} \qquad 3 + H = \{0, 3, 6\}.$$

There are three cosets.

Definition 7.5 Let G be a group, let $H \leq G$, and let $a \in G$. The set

$$aH := \{ah : h \in H\}$$

is called a **left coset** of H in G. The set

$$Ha := \{ha : h \in H\}$$

is called a **right coset** of H in G.

Definition 7.6 Let G be a group and let $H \leq G$. The **index** of H in G, denoted $[G : H]$, is the number of left cosets of H in G.

Example 7.7 Let $G = D_3$ and let $H = \langle f \rangle$ for any flip f. Write down all left and right cosets of H in G.

Solution. Write

$$D_3 = \{e, r, r^2, f, rf, r^2 f\},$$

where r is a rotation of order 3 and f is a flip. Then

$$H = \langle f \rangle = \{e, f\}.$$

The left cosets are

$$eH = H = \{e, f\}, \qquad rH = \{r, rf\}, \qquad \text{and} \qquad r^2 H = \{r^2, r^2 f\}.$$

For the right cosets, we use the relation $fr = r^{-1}f = r^2 f$. Thus

$$He = H = \{e, f\}, \qquad Hr = \{r, fr\} = \{r, r^2 f\}, \qquad \text{and} \qquad Hr^2 = \{r^2, fr^2\} = \{r^2, rf\}.$$

So the left and right cosets are different, which reflects the fact that $\langle f \rangle$ is not normal in D_3. □

Lecture 8 — Wednesday, September 30, 2015

We can now state and prove the basic divisibility result that governs subgroup orders.

Theorem 8.1 (Lagrange's theorem) Let G be a finite group, and let H be a subgroup of G. Then $|H|$ divides $|G|$.

Lemma 8.2 If $H \leq G$ and $a \in G$, then $|aH| = |H|$.

Proof. The map $H \to aH$ given by $h \mapsto ah$ is bijective. It is surjective by definition of aH, and it is injective by cancellation. Hence $|aH| = |H|$. □

Lemma 8.3 Suppose aH and bH are two left cosets of H in G. Then either $aH = bH$ or $aH \cap bH = \emptyset$.

Proof. If $aH \cap bH = \emptyset$, there is nothing to prove. Otherwise choose $x \in aH \cap bH$. Then

$x = ah_1 = bh_2$ for some $h_1, h_2 \in H$, so

$$b^{-1}a = h_2 h_1^{-1} \in H.$$

Write $b^{-1}a = h_3$. If $h \in H$, then

$$ah = (bh_3)h = b(h_3 h) \in bH,$$

so $aH \subseteq bH$. The same argument, with a and b interchanged, gives $bH \subseteq aH$. Hence $aH = bH$. □

Lemma 8.4 Every element $g \in G$ lies in some left coset of H.

Proof. Since $e \in H$, we have $g = ge \in gH$. □

Lemmas 8.3 and 8.4 show that the left cosets of H partition G.

Proof of Theorem 8.1. Let $\{a_1H, \ldots, a_kH\}$ be the set of left cosets of H in G. Since these cosets partition G,

$$|G| = |a_1H| + \cdots + |a_kH|.$$

By Lemma 8.2,

$$|H| = |a_1H| = \cdots = |a_kH|,$$

so $|G| = k|H|$. Therefore $|H|$ divides $|G|$. □

Porism 8.5 If G is a finite group and $H \leq G$, then

$$|H| = \frac{|G|}{[G : H]}.$$

Proof. By definition, $[G : H]$ is the number of left cosets of H in G. If $[G : H] = k$, then the proof of Theorem 8.1 shows that

$$|G| = k|H| = [G : H]\,|H|.$$

Since G is finite, dividing by $[G : H]$ gives

$$|H| = \frac{|G|}{[G : H]}.$$

□

Example 8.6 Let G be a group with $|G| = 15$. Let $H, K < G$ be distinct proper subgroups. Then $H \cap K = \{e\}$.

Solution. By Theorem 8.1, the proper subgroup orders $|H|$ and $|K|$ must be 3 or 5. Also, $H \cap K$ is a subgroup of both H and K. Since H and K are distinct proper subgroups, $H \cap K$ is a proper subgroup of each of them. Applying Theorem 8.1 inside H and K, and using that 3 and 5 are prime, gives $|H \cap K| = 1$. Therefore $H \cap K = \{e\}$. □

Definition 8.7 A group G is **cyclic** if there exists $a \in G$ such that $\langle a \rangle = G$. Such an element is called a **generator** of G.

Let G be a finite group and let $a \in G$. Since $\langle a \rangle \leq G$, Theorem 8.1 gives $|a| = |\langle a \rangle| \mid |G|$, and hence $a^{|G|} = e$. In particular, we have the following corollary:

Corollary 8.8 Every group of prime order is cyclic.

Proof. Let $|G| = p$ be prime and choose $a \in G \setminus \{e\}$. By Proposition 6.7 and Lagrange's theorem, the order $|a|$ divides p. Since $a \neq e$, its order is not 1, so $|a| = p$. Therefore $\langle a \rangle = G$, and G is cyclic. □

2. Group Arithmetic and Homomorphisms

Fermat's Little Theorem

Theorem 8.9 (Fermat's little theorem) If p is prime, then for any $a \in \mathbb{Z}$, $a^p \equiv a \pmod{p}$.

Proof. If $p \mid a$, then $a \equiv 0 \pmod{p}$, and the conclusion is immediate. Otherwise $\gcd(a, p) = 1$, so $a \in \mathbb{Z}_p^*$. Since $|\mathbb{Z}_p^*| = p - 1$, the preceding consequence of Theorem 8.1 gives

$$a^{p-1} \equiv 1 \pmod{p}.$$

Multiplying both sides by a gives $a^p \equiv a \pmod{p}$. □

Lecture 9 — Friday, October 02, 2015

More on Symmetric Groups

Definition 9.1 A **permutation** on a set X is a bijection $\sigma : X \to X$.

We think of elements of S_n as permutations of the set $\{1, \ldots, n\}$. Up to now, we have usually drawn them as permutation diagrams. If we label the dots from left to right, each such diagram determines a bijection $\sigma : \{1, \ldots, n\} \to \{1, \ldots, n\}$.

Cycle notation records what happens when we repeatedly apply a permutation to each element. In Figure 9, the element 1 maps to 4, and 4 maps back to 1. Likewise, 2 maps to 3, and 3 maps back to 2.

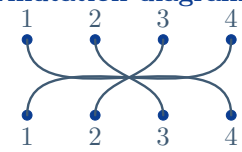
Repeated application of σ therefore produces the two disjoint cycles

$$1 \mapsto 4 \mapsto 1 \qquad \text{and} \qquad 2 \mapsto 3 \mapsto 2.$$

These cycles completely determine the permutation, so we write

$$\sigma = (14)(23).$$

A permutation diagram for σ:



$1 \mapsto 4 \mapsto 1$ *and* $2 \mapsto 3 \mapsto 2$.

FIGURE 9

More generally, every permutation can be written as a product of disjoint cycles.

Remark 9.2 Two conventions make cycle notation easier to read.

1. The number written first in a cycle does not change the permutation. For example, (123), (231), and (312) all describe the same cycle. In practice, we usually begin each cycle with the smallest entry.
2. We omit cycles of length 1 unless we are writing the identity permutation. Thus (1254) really means (1254)(3), while the identity is denoted by (1) regardless of which symmetric group we are using.

Definition 9.3 An n-cycle is a cycle of the form $(a_1 a_2 \dots a_n)$. A 2-cycle is called a **transposition**.

Example 9.4 The elements of S_3 are

$$(1), \qquad (12), \qquad (13), \qquad (23), \qquad (123), \qquad \text{and} \qquad (132).$$

Thus S_3 consists of the identity, three transpositions, and two 3-cycles.

Since elements of S_n are functions $\sigma : \{1, \dots, n\} \to \{1, \dots, n\}$, the group operation is composition of functions. Thus $\sigma\tau$ means that we perform τ first and then σ.

For example, let

$$\sigma = (1342) \qquad \text{and} \qquad \tau = (14).$$

Then

$$\tau(1) = 4, \qquad \tau(2) = 2, \qquad \tau(3) = 3, \qquad \text{and} \qquad \tau(4) = 1,$$

while

$$\sigma(1) = 3, \qquad \sigma(2) = 1, \qquad \sigma(3) = 4, \qquad \text{and} \qquad \sigma(4) = 2.$$

Therefore

$$(\sigma\tau)(1) = \sigma(\tau(1)) = \sigma(4) = 2 \qquad \text{and} \qquad (\sigma\tau)(2) = \sigma(\tau(2)) = \sigma(2) = 1,$$

$$(\sigma\tau)(3) = \sigma(\tau(3)) = \sigma(3) = 4 \qquad \text{and} \qquad (\sigma\tau)(4) = \sigma(\tau(4)) = \sigma(1) = 3.$$

Hence

$$\sigma\tau = (12)(34).$$

The strand diagram in Figure 10 records the same composition from right to left.

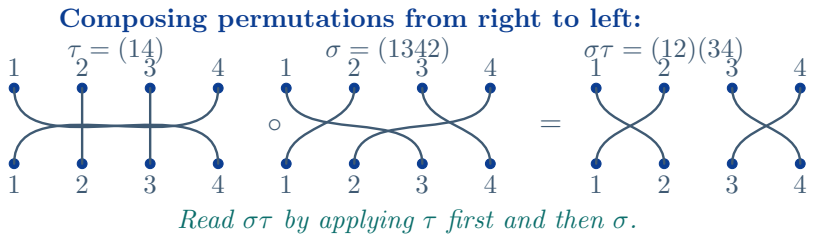


FIGURE 10

To multiply permutations in cycle notation, it is helpful to follow a consistent procedure.

1. Start with the smallest number that has not yet appeared in your answer, and write it as the first entry of a new cycle.
2. Move from the rightmost cycle to the leftmost cycle, updating that number at each stage.
3. Write down the resulting value, and continue until you return to the starting number. At that point, close the cycle.
4. Repeat this process until every number in $\{1, \ldots, n\}$ has been accounted for, omitting any 1-cycles.

For instance,

$$(12)(13)(14) = (1432) \qquad \text{and} \qquad (142)(123)(12)(23) = (13)(24).$$

The best way to become fluent with cycle notation is to practice these computations until the right-to-left composition becomes natural.

Lecture 10 — Monday, October 05, 2015

Odd and Even Permutations

Every permutation can be written as a product of transpositions. For example, if $\sigma = (123) \in S_4$ and $\tau = (12) \in S_4$, then

$$(123) = (13)(12) = (13)(14)(23)(14)(23)(12)$$

and

$$\tau = (12) = (34)(12)(34) = (12)(34)(12)(34) = (12)(23)(12)(23)(12).$$

Lemma 10.1 The identity permutation $(1) \in S_n$ cannot be written as a product of an odd number of transpositions.

Proof. Let

$$\Delta = \prod_{1 \le i < j \le n} (x_i - x_j).$$

A transposition swaps two variables and therefore changes the sign of Δ. Thus a product of an odd number of transpositions changes Δ to $-\Delta$. The identity permutation fixes Δ. Hence the identity permutation cannot be a product of an odd number of transpositions. □

Proposition 10.2 A permutation $\sigma \in S_n$ cannot be written as both a product of an even number of transpositions and a product of an odd number of transpositions.

Proof. Suppose

$$\sigma = (a_1 b_1) \dots (a_n b_n) = (c_1 d_1) \dots (c_m d_m),$$

where n is odd and m is even. Since every transposition is its own inverse,

$$[(a_1 b_1) \dots (a_n b_n)]^{-1} = (a_n b_n) \dots (a_1 b_1).$$

Therefore

$$(1) = (c_1 d_1) \dots (c_m d_m)(a_n b_n) \dots (a_1 b_1),$$

which writes the identity as a product of $m+n$ transpositions. Since $m+n$ is odd, this contradicts Lemma 10.1. □

This justifies the following definition.

Definition 10.3 If $\sigma \in S_n$ can be written as a product of an even number of transpositions, then σ is called an **even permutation**. Otherwise, σ is called an **odd permutation**.

Example 10.4 In S_3, the even permutations are (1), (123), and (132), while the odd permutations are (12), (13), and (23). The even permutations form a group, and there are equally many even and odd permutations.

Proposition 10.5 Let

$$A_n := \{\sigma \in S_n : \sigma \text{ is even}\}.$$

Then A_n is a subgroup of S_n.

Proof. We use the subgroup test (Theorem 7.2). The identity lies in A_n, so A_n is nonempty. If $\sigma, \tau \in A_n$, then each can be written as a product of an even number of transpositions, so $\sigma\tau$ can also be written as a product of an even number of transpositions. Hence $\sigma\tau \in A_n$. Finally, if

$$\sigma = (a_1 b_1) \dots (a_k b_k)$$

with k even, then

$$\sigma^{-1} = (a_k b_k) \dots (a_1 b_1),$$

so σ^{-1} is also even. Therefore $A_n \leq S_n$. □

Definition 10.6 The subgroup $A_n \leq S_n$ is called the **alternating group** on n elements.

Example 10.7 We have

$$A_3 = \{(1), (123), (132)\}.$$

Example 10.8 Let $n \geq 2$. Prove that an n-cycle is even if and only if n is odd. Prove that there are the same number of odd and even permutations in S_n. Conclude that $[S_n : A_n] = 2$.

Solution. An n-cycle can be written as a product of $n-1$ transpositions:

$$(a_1\, a_2\, \ldots\, a_n) = (a_1\, a_n)(a_1\, a_{n-1}) \cdots (a_1\, a_2).$$

Therefore an n-cycle is even if and only if $n-1$ is even, that is, if and only if n is odd.

To count even and odd permutations, fix a transposition $\tau = (1\,2)$. If σ is even, then $\tau\sigma$ is odd, and if σ is odd, then $\tau\sigma$ is even. Thus left multiplication by τ gives a bijection from the even permutations to the odd permutations. Hence there are equally many even and odd permutations in S_n.

Since A_n is the set of even permutations, we obtain

$$|A_n| = \frac{|S_n|}{2}.$$

Therefore

$$[S_n : A_n] = \frac{|S_n|}{|A_n|} = 2.$$

□

Since $|S_4| = 4! = 24$, we have $|A_4| = 24/2 = 12$. However, A_4 has no subgroup of order 6, as proved in Proposition 32.11. This gives a counterexample to the converse of Lagrange's theorem (Theorem 8.1).

The following question is the *Futurama problem*, from the episode "The Prisoner of Benda" (Season 6, Episode 10). The characters in the show have a machine that swaps their minds. For example, if $\sigma = (123)$, then the machine sends the mind in body 1 to body 2, the mind in body 2 to body 3, and the mind in body 3 to body 1. The question is how many more bodies they need to add to the machine so that they can undo any given permutation of their minds using distinct transpositions, each involving at least one of the new bodies.

Question 10.9 Let $\sigma \in S_n$. How many more numbers do you need to add to $\{1, 2, \ldots, n\}$ so that you can undo σ using distinct transpositions, each involving at least one of the new numbers?

Lecture 11 — Wednesday, October 07, 2015

We return to cyclic groups because their subgroup structure can be described very explicitly.

Definition 11.1 A group G is **cyclic** if there exists $a \in G$ such that $G = \langle a \rangle$. Such an element is called a **generator**.

Example 11.2 The group $\mathbb{Z}_n$ is generated by both 1 and -1, and may have other generators. Also,

$$\mathbb{Z}_{10}^* = \{1, 3, 7, 9\} = \{3^0, 3^1, 3^2, 3^3\} = \langle 3 \rangle$$

under multiplication. Further examples are

$$\mathbb{Z} = \langle 1 \rangle \qquad \text{and} \qquad 3\mathbb{Z} = \langle 3 \rangle \neq \mathbb{Z},$$

$$\{1, i, -1, -i\} = \langle i \rangle \qquad \text{and} \qquad \{(1), (123), (132)\} = \langle (123) \rangle.$$

For every $a \in G$, the subgroup $\langle a \rangle$ is cyclic.

Cyclic groups need not be finite.

Proposition 11.3 Cyclic groups are abelian.

Proof. Let $G = \langle a \rangle$. If $x, y \in G$, then $x = a^m$ and $y = a^n$ for some integers m, n. Hence

$$xy = a^m a^n = a^{m+n} = a^{n+m} = a^n a^m = yx.$$

Therefore G is abelian. □

Example 11.4 If $G = \mathbb{Z}$, then $\langle n \rangle \leq \mathbb{Z}$ for every $n \in \mathbb{Z}$. These are in fact all the subgroups of $\mathbb{Z}$.

Theorem 11.5 Every subgroup of a cyclic group is cyclic.

Proof. Let $G = \langle a \rangle$ and let $H \leq G$. If $H = \{e\}$, then $H = \langle e \rangle$ is cyclic. Assume $H \neq \{e\}$. Choose $b \in H$ with $b \neq e$. Since $G = \langle a \rangle$, we have $b = a^s$ for some nonzero integer s. Since H is a subgroup, $b^{-1} = a^{-s} \in H$, so some positive power of a lies in H.

Let m be the smallest positive integer such that $a^m \in H$. We claim that $H = \langle a^m \rangle$. Certainly $\langle a^m \rangle \subseteq H$. Conversely, choose $y \in H$. Since $G = \langle a \rangle$, there is an integer n such that $y = a^n$. By the division algorithm, write $n = qm + r$ with $0 \leq r < m$. Then

$$y = a^n = a^{qm+r} = (a^m)^q a^r,$$

so

$$a^r = (a^m)^{-q} y \in H.$$

By the minimality of m, we must have $r = 0$. Therefore $y = (a^m)^q \in \langle a^m \rangle$, so $H = \langle a^m \rangle$. □

Example 11.6 In $G = \mathbb{Z}_{12}$, we have

$$\langle 0 \rangle = \{0\}, \qquad \langle 1 \rangle = \mathbb{Z}_{12}, \qquad \text{and} \qquad \langle 2 \rangle = \{0, 2, 4, 6, 8, 10\},$$

$$\langle 3 \rangle = \{0, 3, 6, 9\}, \qquad \langle 4 \rangle = \{0, 4, 8\}, \qquad \text{and} \qquad \langle 6 \rangle = \{0, 6\}.$$

Lemma 11.7 Let G be a group, let $a \in G$, and suppose $|a| = n$. Then $a^k = e$ if and only if $n \mid k$.

Proof. *Forward implication.* Suppose $a^k = e$. By the division algorithm, write $k = qn + r$ with $0 \leq r < n$. Then

$$e = a^k = a^{qn+r} = (a^n)^q a^r = a^r.$$

Since n is the smallest positive exponent with $a^n = e$, we must have $r = 0$. Hence $n \mid k$.

Reverse implication. If $n \mid k$, then $k = qn$ for some integer q, and

$$a^k = a^{qn} = (a^n)^q = e.$$

□

Lemma 11.8 Let $G = \langle a \rangle$ and $|G| = n$. Then

$$|a^s| = \frac{n}{\gcd(n, s)}.$$

Proof. Let $d = \gcd(n, s)$, and write $n = dn'$ and $s = ds'$, where $\gcd(n', s') = 1$. For every positive integer k, Lemma 11.7 gives

$$(a^s)^k = e \quad \Longleftrightarrow \quad n \mid sk \quad \Longleftrightarrow \quad n' \mid k.$$

The smallest such k is $n' = n/d$, so $|a^s| = n/\gcd(n, s)$. □

Lecture 12 — Friday, October 09, 2015

We next sharpen this picture by describing exactly which subgroup orders occur in a cyclic group and by identifying its generators.

Recall Lemma 11.7: if $a \in G$ and $|a| = n$, then $a^k = e$ if and only if $n \mid k$. Also recall Lemma 11.8: if $G = \langle a \rangle$ and $|G| = n$, then $|a^s| = n/\gcd(n, s)$. These two facts will be repeatedly in the next theorem: powers return to the identity exactly at multiples of the order, and the order of a power is governed by the greatest common divisor.

Theorem 12.1 Let $G = \langle a \rangle$ and $|G| = n$. For every positive divisor d of n, there is exactly one subgroup $H \leq G$ with $|H| = d$, namely

$$H = \langle a^{n/d} \rangle.$$

Proof. If $d = 1$, then $H = \{e\}$ is the unique subgroup of order 1. Now suppose $d > 1$. By Lemma 11.8,

$$|a^{n/d}| = \frac{n}{\gcd(n, n/d)} = \frac{n}{n/d} = d,$$

so $\langle a^{n/d} \rangle$ is a subgroup of order d.

It remains to prove uniqueness. Let $K \leq G$ satisfy $|K| = d$. By Theorem 11.5, we have $K = \langle a^s \rangle$, where s is the smallest positive integer such that $a^s \in K$. By the Euclidean algorithm, there exist

integers u, v such that

$$\gcd(n, s) = un + vs.$$

Thus

$$a^{\gcd(n,s)} = (a^n)^u (a^s)^v \in K.$$

Since $1 \leq \gcd(n, s) \leq s$, the minimality of s forces $\gcd(n, s) = s$. Hence

$$d = |a^s| = \frac{n}{\gcd(n, s)} = \frac{n}{s}.$$

Therefore $s = n/d$, and so $K = \langle a^{n/d} \rangle$. □

Example 12.2 If $G = \mathbb{Z}_{100}$, then the possible subgroup orders are the positive divisors of 100:

$$100,\ 50,\ 25,\ 20,\ 10,\ 5,\ 4,\ 2,\ 1.$$

Proposition 12.3 Let $|G| = n$. The following are equivalent:

1. G is cyclic.
2. For any positive divisor d of n, there is at most one subgroup of order d.
3. For any positive divisor d of n, there is exactly one subgroup of order d.

Proof. By Theorem 12.1, (1) implies (3), and (3) immediately implies (2).

Now assume (2). Let N_d be the number of elements of order d in G. If $N_d > 0$, all elements of order d generate the same subgroup of order d, and that cyclic subgroup has exactly $\phi(d)$ generators. Hence $N_d \leq \phi(d)$. By Lagrange's theorem, every element of G has order dividing n, so

$$n = \sum_{d|n} N_d \leq \sum_{d|n} \phi(d) = n.$$

The last identity follows by partitioning the elements of the cyclic group $\mathbb{Z}_n$ according to their orders. Equality must therefore hold throughout, so $N_n = \phi(n) > 0$. Thus G contains an element of order n and is cyclic, proving (1). □

Orders and Generators

Recall Lemma 11.8: if $G = \langle a \rangle$ and $|G| = n$, then $|a^s| = n/\gcd(n, s)$.

Proposition 12.4 Let $G = \langle a \rangle$ and $|G| = n$. Then a^s generates G if and only if $\gcd(n, s) = 1$.

Proof. By Lemma 11.8,

$$|a^s| = \frac{n}{\gcd(n, s)}.$$

The element a^s generates G if and only if $|a^s| = |G| = n$, which holds if and only if $\gcd(n, s) = 1$. □

Lecture 13 — Wednesday, October 14, 2015

At this point, our main examples of groups include

$$\mathbb{Z},\ \mathbb{Z}_n,\ \mathbb{Z}_n^*,\ \mathbb{R},\ \mathbb{R}^*,\ \mathbb{Q},\ \mathbb{Q}^*,\ \mathbb{C},\ \mathbb{C}^*,\ GL_n(\mathbb{Z}_n),\ S_n,\ D_n,\ A_n,\ G \times H.$$

We have also studied groups of small order, subgroups, Lagrange's theorem, symmetric and alternating groups, and cyclic groups.

Homomorphisms

Homomorphisms give a way to compare groups.

$$\{(1), (1234), (13)(24), (1432)\} = \{(1234)^0, (1234)^1, (1234)^2, (1234)^3\} \leq S_4.$$

Define $\phi : \mathbb{Z}_4 \to S_4$ by $n \mapsto (1234)^n$. Then

$$\phi(n + m) = (1234)^{n+m} = (1234)^n(1234)^m = \phi(n) \cdot \phi(m).$$

In D_n, consider $\{e, r_1, \ldots, r_{n-1}\} \leq D_n$. Define $\phi : \mathbb{Z}_n \to D_n$ by $k \mapsto r_k$. Again, $\phi(k + \ell) = \phi(k)\phi(\ell)$.

Parity gives another example. Addition in $\mathbb{Z}_2$ records the familiar rules: even plus even and odd plus odd are even, while even plus odd is odd. Define

$$\phi : \mathbb{Z} \to \mathbb{Z}_2, \quad a \mapsto \begin{cases} 0 & \text{if } a \text{ is even,} \\ 1 & \text{if } a \text{ is odd.} \end{cases}$$

Then $\phi(a+b) = \phi(a) + \phi(b)$.

The cosets of $3\mathbb{Z} \leq \mathbb{Z}$ are

$$0 + 3\mathbb{Z}, \qquad 1 + 3\mathbb{Z}, \qquad \text{and} \qquad 2 + 3\mathbb{Z}.$$

The map $\phi : \mathbb{Z} \to \mathbb{Z}_3$ given by $k \mapsto k \pmod 3$ satisfies $\phi(n+m) = \phi(n) + \phi(m)$. More generally, there is a homomorphism $\mathbb{Z} \to \mathbb{Z}_n$ given by $k \mapsto k \pmod n$.

The parity of permutations gives a homomorphism

$$\phi : S_n \to \mathbb{Z}_2, \quad \sigma \mapsto \begin{cases} 0 & \text{if } \sigma \text{ is even,} \\ 1 & \text{if } \sigma \text{ is odd.} \end{cases}$$

Again, $\phi(\sigma\tau) = \phi(\sigma) + \phi(\tau)$.

The group D_4 also has a useful structure. If R denotes a rotation and F denotes a flip, then multiplication of types follows the table

	R	F
R	R	F
F	F	R

which is the Cayley table of $\mathbb{Z}_2$ after relabelling.

Definition 13.1 Let $(G, \cdot)$ and $(H, *)$ be groups. A **group homomorphism** is a function $\phi : G \to H$ such that

$$\phi(a \cdot b) = \phi(a) * \phi(b)$$

for all $a, b \in G$.

Thus a homomorphism is a map that preserves the group operation. It need not be injective or surjective, but it must carry products in the domain to products in the codomain.

Example 13.2 The map $\phi : \mathbb{R} \to \mathbb{R}^*$ given by $x \mapsto e^x$ is a homomorphism, since

$$\phi(x+y) = e^{x+y} = e^x e^y = \phi(x)\phi(y)$$

for all $x, y \in \mathbb{R}$.

Example 13.3 The determinant gives a homomorphism

$$\det : GL_n(\mathbb{Z}_k) \to \mathbb{Z}_k^*$$

because $\det(\mathbf{AB}) = \det(\mathbf{A})\det(\mathbf{B})$.

Example 13.4 If $L : V \to W$ is a linear map between vector spaces, then L is a homomorphism between the underlying abelian groups of V and W.

Example 13.5 The absolute value maps

$$|\cdot| : \mathbb{Q}^* \to \mathbb{Q}^* \qquad \text{and} \qquad |\cdot| : \mathbb{C}^* \to \mathbb{R}^*$$

are homomorphisms because $|ab| = |a||b|$.

Proposition 13.6 Let $\phi : G \to H$ be a homomorphism. Then $\phi(e_G) = e_H$ and $\phi(a^{-1}) = \phi(a)^{-1}$ for all $a \in G$.

Proof. We have

$$\phi(a) = \phi(e_G a) = \phi(e_G)\phi(a).$$

Multiplying on the right by $\phi(a)^{-1}$ gives $\phi(e_G) = e_H$. Also,

$$e_H = \phi(e_G) = \phi(aa^{-1}) = \phi(a)\phi(a^{-1}),$$

so $\phi(a^{-1})$ is an inverse of $\phi(a)$. By uniqueness of inverses, $\phi(a^{-1}) = \phi(a)^{-1}$. □

Proposition 13.7 Let G, H, K be groups, and let $\phi : G \to H$ and $\psi : H \to K$ be homomorphisms. Then $\psi \circ \phi : G \to K$ is a homomorphism.

Proof. For $a, b \in G$,

$$(\psi \circ \phi)(ab) = \psi(\phi(ab)) = \psi(\phi(a)\phi(b)) = \psi(\phi(a))\psi(\phi(b)).$$

Thus $(\psi \circ \phi)(ab) = (\psi \circ \phi)(a)(\psi \circ \phi)(b)$. □

Lecture 14 — Friday, October 16, 2015

The next basic invariants of a homomorphism are its kernel and image.

Definition 14.1 Let $\phi : G \to H$ be a homomorphism. The **kernel** of ϕ is the set

$$\ker(\phi) = \{g \in G : \phi(g) = e_H\} \subseteq G.$$

The **image** of ϕ is the set

$$\text{im}(\phi) = \{h \in H : \text{there exists } g \in G \text{ such that } \phi(g) = h\} \subseteq H.$$

Example 14.2 Consider $\det : GL_3(\mathbb{Z}_9) \to \mathbb{Z}_9^*$. Here the identity in $\mathbb{Z}_9^*$ is 1, so

$$\ker(\det) = \{\mathbf{A} \in GL_3(\mathbb{Z}_9) : \det(\mathbf{A}) = 1\}.$$

To determine the image, let $a \in \mathbb{Z}_9^*$. Then

$$\det \begin{pmatrix} a & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} = a,$$

so $a \in \text{im}(\det)$. Thus $\text{im}(\det) = \mathbb{Z}_9^*$.

Example 14.3 Let $\phi : \mathbb{Z}_4 \to S_4$ be given by $n \mapsto (1234)^n$. Then $\ker(\phi) = \{0\}$ and

$$\text{im}(\phi) = \{(1234)^n : n = 0, 1, 2, 3\} = \langle (1234) \rangle.$$

Example 14.4 Let G be a group and let $a \in G$. Define $\phi_a : \mathbb{Z} \to G$ by $n \mapsto a^n$. This is a homomorphism because

$$\phi_a(n+m) = a^{n+m} = a^n a^m = \phi_a(n)\phi_a(m)$$

for all $m, n \in \mathbb{Z}$. Then $\ker(\phi_a) = \{0\}$ if $|a| = \infty$, while $\ker(\phi_a) = k\mathbb{Z}$ if $|a| = k$. Also, $\text{im}(\phi_a) = \langle a \rangle$. This map is sometimes called the **exponential map**.

Example 14.5 Let G and H be groups. The **trivial homomorphism** is $\phi : G \to H$ given by $g \mapsto e_H$. Its kernel is G, and its image is $\{e_H\}$.

Proposition 14.6 If $\phi : G \to H$ is a homomorphism, then $\text{im}(\phi)$ is a subgroup of H.

Proof. By Proposition 13.6, $\phi(e_G) = e_H$, so $e_H \in \text{im}(\phi)$ and $\text{im}(\phi)$ is nonempty. Let $h_1, h_2 \in \text{im}(\phi)$. Then there exist $g_1, g_2 \in G$ such that $\phi(g_1) = h_1$ and $\phi(g_2) = h_2$. Therefore

$$\phi(g_1 g_2) = \phi(g_1)\phi(g_2) = h_1 h_2,$$

so $h_1 h_2 \in \text{im}(\phi)$. If $h \in \text{im}(\phi)$, choose $g \in G$ with $\phi(g) = h$. Then

$$\phi(g^{-1}) = \phi(g)^{-1} = h^{-1},$$

so $h^{-1} \in \text{im}(\phi)$. By the subgroup test (Theorem 7.2), $\text{im}(\phi) \leq H$. □

Proposition 14.7 If $\phi : G \to H$ is a homomorphism, then $\ker(\phi) \leq G$.

Proof. By Proposition 13.6, $\phi(e_G) = e_H$, so $e_G \in \ker(\phi)$. Let $g_1, g_2 \in \ker(\phi)$. Then

$$\phi(g_1 g_2) = \phi(g_1)\phi(g_2) = e_H e_H = e_H,$$

so $g_1 g_2 \in \ker(\phi)$. If $g \in \ker(\phi)$, then

$$\phi(g^{-1}) = \phi(g)^{-1} = e_H^{-1} = e_H,$$

so $g^{-1} \in \ker(\phi)$. By the subgroup test (Theorem 7.2), $\ker(\phi) \leq G$. □

Proposition 14.8 Let $\phi : G \to H$ be a homomorphism. Then ϕ is injective if and only if $\ker(\phi) = \{e_G\}$.

Proof. *Forward implication.* Suppose ϕ is injective. Since $\phi(e_G) = e_H$, the only element of G that can map to e_H is e_G. Hence $\ker(\phi) = \{e_G\}$.

Reverse implication. Suppose $\ker(\phi) = \{e_G\}$. If $\phi(g_1) = \phi(g_2)$, then

$$\phi(g_1 g_2^{-1}) = \phi(g_1)\phi(g_2)^{-1} = e_H.$$

Thus $g_1 g_2^{-1} \in \ker(\phi) = \{e_G\}$, so $g_1 = g_2$. Therefore ϕ is injective. □

Isomorphisms

Definition 14.9 An **isomorphism** between two groups G and H is a homomorphism $\phi : G \to H$ that is a bijection. If there exists an isomorphism $\phi : G \to H$, then G and H are **isomorphic**, and we write $G \cong H$.

Example 14.10 We show that $\mathbb{Z}_5 \cong \langle (12345) \rangle$. Define

$$\phi : \mathbb{Z}_5 \to \langle (12345) \rangle, \quad \phi(n) = (12345)^n.$$

This is a homomorphism. The only $n \in \mathbb{Z}_5$ such that $\phi(n) = (1)$ is $n = 0$, so $\ker(\phi) = \{0\}$. By Proposition 14.8, ϕ is injective. Also,

$$\begin{aligned} \langle (12345) \rangle &= \{(1), (12345), (13524), (14253), (15432)\} \\ &= \{(12345)^0, (12345)^1, (12345)^2, (12345)^3, (12345)^4\}, \end{aligned}$$

so ϕ is surjective. Therefore ϕ is an isomorphism, and $\mathbb{Z}_5 \cong \langle (12345) \rangle$.

Lecture 15 — Monday, October 19, 2015

Recall that an isomorphism $\phi : G \to H$ is a bijective homomorphism. This means that an isomorphism preserves the group operation and also matches the elements of the two groups one-to-one.

Example 15.1 The groups $\mathbb{Z}_2 \times \mathbb{Z}_2$ and $\mathbb{Z}_4$ are not isomorphic. Suppose, for contradiction, that there is an isomorphism

$$\phi : \mathbb{Z}_2 \times \mathbb{Z}_2 \to \mathbb{Z}_4.$$

Choose $a \in \mathbb{Z}_2 \times \mathbb{Z}_2$ such that $\phi(a) = 1$. Since $g^2 = e$ for all $g \in \mathbb{Z}_2 \times \mathbb{Z}_2$, we get

$$\phi(e) = \phi(a^2) = \phi(a)\phi(a) = 1 + 1 = 2.$$

This contradicts $\phi(e) = 0$. Therefore $\mathbb{Z}_2 \times \mathbb{Z}_2 \ncong \mathbb{Z}_4$.

Example 15.2 The groups $\mathbb{Z}_6$ and S_3 are not isomorphic. If $\phi : \mathbb{Z}_6 \to S_3$ were an isomorphism, then there would exist $a, b \in \mathbb{Z}_6$ such that $\phi(a) = (12)$ and $\phi(b) = (23)$. Since $\mathbb{Z}_6$ is abelian, $a + b = b + a$. However,

$$\phi(a + b) = \phi(a)\phi(b) = (12)(23) = (123),$$

while

$$\phi(b + a) = \phi(b)\phi(a) = (23)(12) = (132).$$

This is impossible, so $\mathbb{Z}_6 \ncong S_3$.

Example 15.3 Let G be abelian and let H be nonabelian. Prove that $G \ncong H$.

Solution. Suppose, for contradiction, that there were an isomorphism $\phi : G \to H$. If $x, y \in H$, write $x = \phi(a)$ and $y = \phi(b)$ for some $a, b \in G$. Since G is abelian,

$$xy = \phi(a)\phi(b) = \phi(ab) = \phi(ba) = \phi(b)\phi(a) = yx.$$

Thus every pair of elements of H commutes, so H is abelian. This contradicts the assumption that H is nonabelian. Therefore $G \ncong H$. □

Proposition 15.4 Let $G = \langle a \rangle$ and $H = \langle b \rangle$ be cyclic groups. Then $G \cong H$ if and only if $|G| = |H|$.

Proof. *Forward implication.* If $G \cong H$, then there is a bijection between G and H, so $|G| = |H|$.

Reverse implication. First suppose $|G| = |H| = n < \infty$. Then

$$G = \{a^0 = e, a^1, \ldots, a^{n-1}\} \qquad \text{and} \qquad H = \{b^0 = e, b^1, \ldots, b^{n-1}\}.$$

Define $\phi : G \to H$ by $\phi(a^s) = b^s$, where exponents are read modulo n. This is well-defined and satisfies

$$\phi(a^s a^t) = \phi(a^{s+t \pmod n}) = b^{s+t \pmod n} = b^s b^t,$$

so ϕ is a homomorphism. It is bijective because it sends the listed elements of G to the listed elements of H one-to-one.

If $|G| = |H| = \infty$, then every element of G has a unique expression a^k with $k \in \mathbb{Z}$, and every element of H has a unique expression b^k. The map $\phi(a^k) = b^k$ is again a bijective homomorphism. Hence $G \cong H$. □

Corollary 15.5 Let G be a cyclic group. If $|G| = n$, then $G \cong \mathbb{Z}_n$. If $|G| = \infty$, then $G \cong \mathbb{Z}$.

Proof. This follows from Proposition 15.4, since $\mathbb{Z}_n$ is cyclic of order n and $\mathbb{Z}$ is cyclic of infinite order. □

Corollary 15.6 Let p be prime, and let G and H be groups of order p. Then $G \cong H$.

Proof. By Lagrange's theorem (Theorem 8.1), any nonidentity element of G has order p, so G is cyclic. Similarly, H is cyclic. The result follows from Proposition 15.4. □

Proposition 15.7 Let G and H be groups. A homomorphism $\phi : G \to H$ is an isomorphism if and only if there exists a homomorphism $\psi : H \to G$ such that $\phi(\psi(h)) = h$ for all $h \in H$ and $\psi(\phi(g)) = g$ for all $g \in G$.

Proof. *Forward implication.* Suppose ϕ is an isomorphism. Since ϕ is bijective, it has an inverse function $\psi : H \to G$. We show that ψ is a homomorphism. Let $h_1, h_2 \in H$. Write $h_1 = \phi(g_1)$ and $h_2 = \phi(g_2)$. Then

$$\psi(h_1h_2) = \psi(\phi(g_1)\phi(g_2)) = \psi(\phi(g_1g_2)) = g_1g_2 = \psi(h_1)\psi(h_2).$$

The identities $\phi(\psi(h)) = h$ and $\psi(\phi(g)) = g$ hold because $\psi = \phi^{-1}$.

Reverse implication. Suppose such a homomorphism ψ exists. If $\phi(g_1) = \phi(g_2)$, then applying ψ gives $g_1 = g_2$, so ϕ is injective. For any $h \in H$, the identity $\phi(\psi(h)) = h$ shows that h lies in the image of ϕ, so ϕ is surjective. Thus ϕ is bijective, and hence an isomorphism. □

The homomorphism ψ in Proposition 15.7 is called the **inverse** of ϕ, and is denoted $\psi = \phi^{-1}$.

3. Quotients and Isomorphism Theorems

Normal Subgroups and Quotients

We have already seen that images and kernels of homomorphisms are subgroups. Conversely, every subgroup occurs as an image: if $H \leq G$, then the inclusion homomorphism $\iota : H \to G$ defined by $\iota(h) = h$ has image H. The more delicate question is which subgroups occur as kernels.

Lecture 16 — Wednesday, October 21, 2015

Question 16.1 Which subgroups can be kernels?

Example 16.2 Let $H = \{(1), (12)\} \leq S_3$. We show that H cannot be the kernel of a homomorphism with domain S_3. Suppose, for contradiction, that $\phi : S_3 \to K$ is a homomorphism and that $\ker(\phi) = H$. Since

$$(13) = (23)(12)(23)^{-1},$$

we have

$$\phi((13)) = \phi((23))\phi((12))\phi((23))^{-1} = \phi((23))e\phi((23))^{-1} = e.$$

Thus $(13) \in \ker(\phi)$, contradicting $\ker(\phi) = \{(1), (12)\}$. Therefore H cannot be a kernel.

The calculation in the preceding example isolates the obstruction. If $H = \ker(\phi)$, then for every $g \in G$ and every $h \in H$,

$$\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g)^{-1} = e,$$

so $ghg^{-1} \in H$.

Definition 16.3 Let $H \leq G$. We say that H is a **normal subgroup** of G if $ghg^{-1} \in H$ for every $g \in G$ and every $h \in H$. We write $H \trianglelefteq G$.

Proposition 16.4 Let $H \leq G$. The following conditions are equivalent:

1. For every $g \in G$ and every $h \in H$, we have $ghg^{-1} \in H$.
2. For every $g \in G$, we have $gHg^{-1} \subseteq H$.
3. For every $g \in G$, we have $gHg^{-1} = H$.
4. For every $g \in G$, we have $gH = Hg$.

Proof. The equivalence of (1) and (2) is only a change of notation. Condition (3) immediately implies (2). Conversely, assume (2). Applying it to g^{-1} gives $g^{-1}Hg \subseteq H$. Multiplying this inclusion on the left by g and on the right by g^{-1} gives

$$H \subseteq gHg^{-1}.$$

Together with $gHg^{-1} \subseteq H$, this gives $gHg^{-1} = H$. Thus (2) implies (3).

Finally, $gHg^{-1} = H$ is equivalent to $gH = Hg$, because multiplying $gHg^{-1} = H$ on the right by g gives $gH = Hg$, and multiplying $gH = Hg$ on the right by g^{-1} gives $gHg^{-1} = H$. □

We now know that if $H \leq G$ is the kernel of a homomorphism, then $H \trianglelefteq G$. The converse also holds, but showing it is much harder. The proof of this converse motivates the construction of quotient groups.

Suppose $\phi : G \to K$ is a homomorphism with kernel H. The map ϕ is constant on each left coset of H: if $g_1 = g_2 h$ for some $h \in H$, then $\phi(g_1) = \phi(g_2)$. Conversely, if $\phi(g_1) = \phi(g_2)$, then $g_2^{-1} g_1 \in H$, so g_1 and g_2 lie in the same left coset. Thus the fibres of ϕ are exactly the left cosets of H.

Because H is normal, its left and right cosets agree by Proposition 16.4. This lets us multiply cosets without depending on the representatives we choose. Indeed, if $g_1' = g_1 h_1$ and $g_2' = g_2 h_2$ for $h_1, h_2 \in H$, then normality gives $h_3 := g_2^{-1} h_1 g_2 \in H$, and hence

$$g_1' g_2' = g_1 h_1 g_2 h_2 = g_1 g_2 h_3 h_2 \in g_1 g_2 H.$$

This calculation motivates the following construction.

Definition 16.5 Let G be a group and let $H \trianglelefteq G$. The **quotient group** G/H is the set of left cosets of H in G, equipped with the multiplication

$$(g_1 H)(g_2 H) = g_1 g_2 H.$$

When no confusion can arise, we also write $[g]$ for the coset gH, so that $[g_1][g_2] = [g_1 g_2]$.

Proposition 16.6 If $H \trianglelefteq G$, then the multiplication on G/H is well-defined and makes G/H into a group.

Proof. Suppose $g_1 H = g_1' H$ and $g_2 H = g_2' H$. Then $g_1' = g_1 h_1$ and $g_2' = g_2 h_2$ for some $h_1, h_2 \in H$. Hence

$$g_1' g_2' = g_1 h_1 g_2 h_2 = g_1 g_2 (g_2^{-1} h_1 g_2) h_2.$$

Since H is normal, $g_2^{-1} h_1 g_2 \in H$, so $(g_2^{-1} h_1 g_2) h_2 \in H$. Thus $g_1' g_2' H = g_1 g_2 H$, proving that the multiplication is well-defined.

Associativity follows from associativity in G. The identity element is $H = eH$, since

$$(eH)(gH) = gH = (gH)(eH).$$

The inverse of gH is $g^{-1} H$, since

$$(gH)(g^{-1} H) = H = (g^{-1} H)(gH).$$

Therefore G/H is a group. □

Example 16.7 The quotient multiplication is not well-defined for $H = \{(1), (12)\} \leq S_3$. In S_3, we have $(1)H = (12)H$. If the rule $(g_1H)(g_2H) = g_1g_2H$ were well-defined, then multiplying both representatives by the same coset $(13)H$ would give

$$((1)H)((13)H) = ((12)H)((13)H).$$

However,

$$((1)H)((13)H) = (13)H \qquad \text{and} \qquad ((12)H)((13)H) = (12)(13)H = (132)H.$$

The cosets are different, since

$$(13)H = \{(13), (123)\} \qquad \text{and} \qquad (132)H = \{(132), (23)\}.$$

Thus this subgroup is not normal, and the quotient multiplication is not well-defined.

Definition 16.8 Let G be a group and let $H \trianglelefteq G$. The **quotient map** is the homomorphism

$$\pi : G \to G/H, \quad \pi(g) = gH.$$

The quotient map is a homomorphism because

$$\pi(g_1g_2) = (g_1g_2)H = (g_1H)(g_2H) = \pi(g_1)\pi(g_2).$$

Proposition 16.9 Let G be a group and let $H \leq G$. Then H is normal in G if and only if H is the kernel of some homomorphism with domain G.

Proof. *Forward implication.* Suppose $H \trianglelefteq G$. Let $\pi : G \to G/H$ be the quotient map. Then

$$\ker(\pi) = \{g \in G : gH = H\} = H.$$

Thus H is the kernel of a homomorphism.

Reverse implication. Suppose $H = \ker(\phi)$ for some homomorphism $\phi : G \to K$. If $h \in H$ and $g \in G$, then

$$\phi(ghg^{-1}) = \phi(g)\phi(h)\phi(g)^{-1} = \phi(g)e\phi(g)^{-1} = e.$$

Hence $ghg^{-1} \in \ker(\phi) = H$, so $H \trianglelefteq G$. □

Thus normal subgroups are exactly the subgroups that can occur as kernels.

Lecture 17 — Friday, October 23, 2015

Example 17.1 Since $\mathbb{Z}$ is abelian, $3\mathbb{Z} \trianglelefteq \mathbb{Z}$. The cosets are

$$0+3\mathbb{Z}, \qquad 1+3\mathbb{Z}, \qquad \text{and} \qquad 2+3\mathbb{Z}.$$

Therefore $|\mathbb{Z}/3\mathbb{Z}| = 3$, and the map

$$\phi : \mathbb{Z}/3\mathbb{Z} \to \mathbb{Z}_3, \quad \phi(x+3\mathbb{Z}) = x \pmod 3$$

is an isomorphism. More generally, the same construction gives $\mathbb{Z}/n\mathbb{Z} \cong \mathbb{Z}_n$.

Proposition 17.2 Let $H \trianglelefteq G$.

1. If G is abelian, then every subgroup of G is normal.
2. If G is finite, then $|G/H| = |G|/|H|$.
3. If G is abelian, then G/H is abelian.
4. If G is cyclic, then G/H is cyclic.

Proof. For (1), let $H \leq G$. If $g \in G$ and $h \in H$, then $ghg^{-1} = hgg^{-1} = h \in H$, so $H \trianglelefteq G$.

For (2), the elements of G/H are the left cosets of H, and every left coset has $|H|$ elements. Since the left cosets partition G, the number of cosets is $|G|/|H|$.

For (3), if G is abelian, then for $g_1, g_2 \in G$,

$$(g_1H)(g_2H) = g_1g_2H = g_2g_1H = (g_2H)(g_1H).$$

Thus G/H is abelian.

For (4), suppose $G = \langle a \rangle$. Every element of G/H has the form gH with $g = a^m$, so

$$gH = a^m H = (aH)^m.$$

Therefore $G/H = \langle aH \rangle$. □

Proposition 17.3 If $H \leq G$ and $[G : H] = 2$, then $H \trianglelefteq G$.

Proof. There are two left cosets of H and two right cosets of H. If $g \in H$, then $gH = H = Hg$. If $g \notin H$, then gH is the unique left coset different from H, and Hg is the unique right coset different from H. Since both are equal to $G \setminus H$, we have $gH = Hg$. Hence $gH = Hg$ for every $g \in G$, so $H \trianglelefteq G$ by Proposition 16.4. □

Corollary 17.4 For every $n \geq 2$, $A_n \trianglelefteq S_n$.

Proof. The even permutations and odd permutations in S_n have the same cardinality, so $[S_n : A_n] = 2$. The result follows from Proposition 17.3. □

Lecture 18 — Monday, October 26, 2015

Among groups of order 8, we have already seen $\mathbb{Z}_8$, D_4, $\mathbb{Z}_2 \times \mathbb{Z}_4$, and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$. There is one more group of order 8.

The Quaternion Group

William Hamilton introduced the quaternions in 1843 while looking for a multiplication on $\mathbb{R}^4$ analogous to complex multiplication on $\mathbb{R}^2$. Supposedly, he was struck by the idea while walking along the Royal Canal in Dublin, and etched the fundamental relations on a stone of the Brougham Bridge. We identify

$$(a, b, c, d) \in \mathbb{R}^4 \qquad \text{with} \qquad a + ib + jc + kd.$$

The multiplication is determined by

$$i^2 = j^2 = k^2 = ijk = -1.$$

From these relations we obtain

$$ij = k, \qquad jk = i, \qquad \text{and} \qquad ki = j,$$

and reversing the order introduces a minus sign:

$$ji = -k, \qquad kj = -i, \qquad \text{and} \qquad ik = -j.$$

Definition 18.1 The **quaternion group** is

$$Q_8 = \{1, -1, i, -i, j, -j, k, -k\},$$

with multiplication determined by the quaternion relations above.

Example 18.2 The relations give

$$i(-i) = -(i^2) = -(-1) = 1,$$

so $i^{-1} = -i$. Similarly, $j^{-1} = -j$ and $k^{-1} = -k$. The group Q_8 is nonabelian, since $ij = k$ while $ji = -k$.

Proposition 18.3 Every subgroup of Q_8 is normal.

Proof. The subgroups of Q_8 are

$$\{1\}, \qquad \{1, -1\}, \qquad \langle i \rangle, \qquad \langle j \rangle, \qquad \langle k \rangle, \qquad \text{and} \qquad Q_8.$$

The trivial subgroup and the whole group are normal. The subgroup $\{1, -1\}$ is central, hence normal. Each of $\langle i \rangle$, $\langle j \rangle$, and $\langle k \rangle$ has order 4, hence index 2, and is normal by Proposition 17.3. □

Up to isomorphism, the groups of order 8 are

$$\mathbb{Z}_8, \qquad D_4, \qquad \mathbb{Z}_2 \times \mathbb{Z}_4, \qquad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2, \qquad \text{and} \qquad Q_8.$$

The First Isomorphism Theorem

Example 18.4 Consider the **sign homomorphism**

$$\operatorname{sgn} : S_3 \to \mathbb{Z}_2, \quad \operatorname{sgn}(\sigma) = \begin{cases} 0, & \text{if } \sigma \text{ is even,} \\ 1, & \text{if } \sigma \text{ is odd.} \end{cases}$$

Then $\ker(\operatorname{sgn}) = A_3$ and $\operatorname{im}(\operatorname{sgn}) = \mathbb{Z}_2$. Since $[S_3 : A_3] = 2$, we have $S_3/A_3 \cong \mathbb{Z}_2$. Explicitly, the isomorphism is

$$\overline{\operatorname{sgn}} : S_3/A_3 \to \mathbb{Z}_2, \quad \overline{\operatorname{sgn}}(\sigma A_3) = \begin{cases} 0, & \text{if } \sigma \in A_3, \\ 1, & \text{if } \sigma \notin A_3. \end{cases}$$

Example 18.5 Consider the homomorphism

$$\phi : \mathbb{Z}_9 \to \mathbb{Z}_3, \quad \phi(n) = n \pmod 3.$$

Then $\ker(\phi) = \{0, 3, 6\}$ and $\operatorname{im}(\phi) = \mathbb{Z}_3$. Define

$$\overline{\phi} : \mathbb{Z}_9/\ker(\phi) \to \mathbb{Z}_3, \quad \overline{\phi}([n]) = \phi(n).$$

This is well-defined: if $[n] = [m]$, then $[n - m] = [0]$, so $n - m \in \ker(\phi)$. Hence

$$0 = \phi(n - m) = \phi(n) - \phi(m),$$

and therefore $\phi(n) = \phi(m)$. The map $\overline{\phi}$ is a homomorphism, is injective because its kernel is trivial, and is surjective because ϕ is surjective. Thus $\mathbb{Z}_9/\ker(\phi) \cong \mathbb{Z}_3$.

Theorem 18.6 (First isomorphism theorem) Let $\phi : G \to H$ be a homomorphism. Then

$$G/\ker(\phi) \cong \operatorname{im}(\phi).$$

Proof. Let $K = \ker(\phi)$. Define

$$\overline{\phi} : G/K \to \operatorname{im}(\phi), \quad \overline{\phi}(gK) = \phi(g).$$

We verify that $\overline{\phi}$ is an isomorphism.

First, $\overline{\phi}$ is well-defined. If $g_1K = g_2K$, then $g_2^{-1}g_1 \in K$, so

$$e = \phi(g_2^{-1}g_1) = \phi(g_2)^{-1}\phi(g_1),$$

and hence $\phi(g_1) = \phi(g_2)$.

Second, $\overline{\phi}$ is a homomorphism, since

$$\overline{\phi}((aK)(bK)) = \overline{\phi}(abK) = \phi(ab) = \phi(a)\phi(b) = \overline{\phi}(aK)\overline{\phi}(bK).$$

Third, $\overline{\phi}$ is injective. If $\overline{\phi}(gK) = e$, then $\phi(g) = e$, so $g \in K$, and therefore $gK = K$.

Finally, $\overline{\phi}$ is surjective onto $\operatorname{im}(\phi)$ by definition of image. Therefore $\overline{\phi}$ is an isomorphism. □

Corollary 18.7 Let $\phi : G \to H$ be a homomorphism, where G and H are finite. Then $|\operatorname{im}(\phi)|$ divides both $|G|$ and $|H|$.

Proof. By Proposition 14.6, $\operatorname{im}(\phi) \leq H$, so Lagrange's theorem (Theorem 8.1) gives $|\operatorname{im}(\phi)| \mid |H|$. By Theorem 18.6,

$$|\operatorname{im}(\phi)| = |G/\ker(\phi)| = \frac{|G|}{|\ker(\phi)|}.$$

Thus $|\operatorname{im}(\phi)|$ also divides $|G|$. □

The first isomorphism theorem is the group-theoretic analogue of the rank-nullity theorem from linear algebra: it measures the image by quotienting out exactly the part of the domain that maps to the identity.

Lecture 19 — Wednesday, October 28, 2015

The first isomorphism theorem is one of the most useful tools for proving that two groups are isomorphic, especially when one of them is given as a quotient.

Example 19.1 Let $H = \{1, -1\} \trianglelefteq Q_8$. Then

$$Q_8/H \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Proof. Define $\phi : Q_8 \to \mathbb{Z}_2 \times \mathbb{Z}_2$ by

$$\phi(1) = \phi(-1) = (0,0), \qquad \phi(i) = \phi(-i) = (1,0),$$

$$\phi(j) = \phi(-j) = (1,1) \qquad \text{and} \qquad \phi(k) = \phi(-k) = (0,1).$$

Using the multiplication rules in Q_8, we check that $\phi(xy) = \phi(x) + \phi(y)$ for all $x, y \in Q_8$, so ϕ is a homomorphism. It is surjective, and its kernel is exactly $\{1, -1\} = H$. Therefore the first isomorphism theorem gives

$$Q_8/H \cong \text{im}(\phi) = \mathbb{Z}_2 \times \mathbb{Z}_2.$$

□

Subgroup Lattices

We can often learn interesting structural information about a group by looking at how its subgroups sit inside one another. The resulting diagram is called the **subgroup lattice**. We place larger subgroups higher in the picture, and we connect two subgroups when one contains the other with no subgroup strictly between them.

Example 19.2 The subgroups of S_3 are

$$\{(1)\}, \qquad H_1 = \{(1), (12)\}, \qquad H_2 = \{(1), (13)\}, \qquad H_3 = \{(1), (23)\},$$

$$H_4 = \{(1), (123), (132)\} \qquad \text{and} \qquad S_3.$$

Example 19.3 The subgroups of $\mathbb{Z}_6$ are

$$\{0\}, \qquad \langle 3 \rangle = \{0, 3\}, \qquad \langle 2 \rangle = \{0, 2, 4\}, \qquad \text{and} \qquad \mathbb{Z}_6.$$

The subgroup lattices of S_3 and $\mathbb{Z}_6$ are compared in Figure 11.

FIGURE 11

Example 19.4 Because $\mathbb{Z}_{12}$ is cyclic, it has exactly one subgroup of order d for each divisor d of 12. Thus its proper nontrivial subgroups are

$$\langle 2\rangle, \qquad \langle 3\rangle, \qquad \langle 4\rangle, \qquad \text{and} \qquad \langle 6\rangle.$$

The resulting lattice is shown in Figure 12.

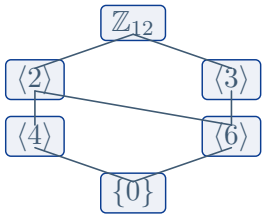


FIGURE 12

Notice that $|\langle 4\rangle| = 3$ and $|\langle 2\rangle| = 6$. Since $\langle 2\rangle$ is cyclic of order 6, it has a subgroup of order 3. Because there is only one subgroup of order 3 in $\mathbb{Z}_{12}$, it must be $\langle 4\rangle$, so $\langle 4\rangle \leq \langle 2\rangle$. Similar order arguments recover the rest of the lattice. Also, because $\langle 6\rangle \trianglelefteq \mathbb{Z}_{12}$ and $\mathbb{Z}_{12}/\langle 6\rangle$ is cyclic of order 6, the part of the lattice above $\langle 6\rangle$ has the same shape as the subgroup lattice of $\mathbb{Z}_6$.

Example 19.5 The proper nontrivial subgroups of Q_8 are

$$\langle -1\rangle = \{1, -1\}, \qquad \langle i\rangle = \{1, i, -1, -i\}, \qquad \langle j\rangle = \{1, j, -1, -j\},$$

$$\text{and} \quad \langle k\rangle = \{1, k, -1, -k\}.$$

The proper nontrivial subgroups of $\mathbb{Z}_2 \times \mathbb{Z}_2$ are the three order-2 subgroups

$$H_1 = \{(0,0), (1,0)\}, \qquad H_2 = \{(0,0), (0,1)\}, \qquad \text{and} \qquad H_3 = \{(0,0), (1,1)\}.$$

Figure 13 makes the different containment patterns visible.

FIGURE 13

We already know that $Q_8/\langle -1 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Notice that the part of the subgroup lattice of Q_8 lying above $\langle -1 \rangle$ has the same shape as the subgroup lattice of $\mathbb{Z}_2 \times \mathbb{Z}_2$. This is the phenomenon explained by the correspondence theorem.

Exercise 19.6 As further practice, draw subgroup lattices for several groups of the form $\mathbb{Z}_n$, and also sketch the infinite subgroup lattice of $\mathbb{Z}$ from the top downward.

Lecture 20 — Friday, October 30, 2015

Correspondence Theorem

Definition 20.1 Let $\phi : G \to H$ be a homomorphism. If $S \subseteq G$, then

$$\phi(S) = \{\phi(s) : s \in S\}$$

is the **image** of S. If $T \subseteq H$, then

$$\phi^{-1}(T) = \{g \in G : \phi(g) \in T\}$$

is the **preimage** of T.

Lemma 20.2 Let $\phi : G_1 \to G_2$ be a homomorphism. If $H_1 \leq G_1$, then $\phi(H_1) \leq G_2$. If $H_2 \leq G_2$, then $\phi^{-1}(H_2) \leq G_1$.

Proof. Since $e \in H_1$, we have $\phi(e) = e \in \phi(H_1)$. If $x = \phi(a)$ and $y = \phi(b)$ lie in $\phi(H_1)$, with $a, b \in H_1$, then

$$xy^{-1} = \phi(a)\phi(b)^{-1} = \phi(ab^{-1}) \in \phi(H_1),$$

because $ab^{-1} \in H_1$. Hence $\phi(H_1) \leq G_2$.

For the preimage, $e \in \phi^{-1}(H_2)$ since $\phi(e) = e \in H_2$. If $a, b \in \phi^{-1}(H_2)$, then $\phi(a), \phi(b) \in H_2$, so

$$\phi(ab^{-1}) = \phi(a)\phi(b)^{-1} \in H_2.$$

Thus $ab^{-1} \in \phi^{-1}(H_2)$, and therefore $\phi^{-1}(H_2) \leq G_1$. □

Theorem 20.3 (Correspondence theorem) Let $\phi : G_1 \to G_2$ be a surjective homomorphism, and let $K = \ker(\phi)$. There is a one-to-one correspondence

$$\{H \leq G_1 : K \leq H \leq G_1\} \longleftrightarrow \left\{\overline{H} \leq G_2\right\}$$

given by

$$H \mapsto \phi(H) \qquad \text{and} \qquad \overline{H} \mapsto \phi^{-1}(\overline{H}).$$

Furthermore, this correspondence has the following properties:

1. If $K \leq H_1, H_2 \leq G_1$, then $H_1 \leq H_2$ if and only if $\phi(H_1) \leq \phi(H_2)$.
2. If $K \leq H \leq G_1$, then $[G_1 : H] = [G_2 : \phi(H)]$.

Proof. By Lemma 20.2, images and preimages of subgroups under ϕ are subgroups. If $\overline{H} \leq G_2$, then $K \leq \phi^{-1}(\overline{H})$ because $\phi(k) = e \in \overline{H}$ for every $k \in K$. Thus both assignments are well-defined.

The two assignments are inverse to each other. If $\overline{H} \leq G_2$, then surjectivity of ϕ gives

$$\phi(\phi^{-1}(\overline{H})) = \overline{H}.$$

If $K \leq H \leq G_1$, then $H \subseteq \phi^{-1}(\phi(H))$. Conversely, if $a \in \phi^{-1}(\phi(H))$, then $\phi(a) = \phi(b)$ for some $b \in H$. Hence

$$\phi(b^{-1}a) = e,$$

so $b^{-1}a \in K \subseteq H$. Since $b \in H$, this implies $a \in H$. Therefore $\phi^{-1}(\phi(H)) = H$.

For (1), the forward implication is immediate: if $H_1 \leq H_2$, then $\phi(H_1) \leq \phi(H_2)$.

Reverse implication. Suppose $\phi(H_1) \leq \phi(H_2)$, and let $x \in H_1$. Then $\phi(x) \in \phi(H_2)$, so $\phi(x) = \phi(y)$ for some $y \in H_2$. Thus

$$y^{-1}x \in \ker(\phi) = K \subseteq H_2.$$

Since $y \in H_2$, we get $x \in H_2$. Hence $H_1 \leq H_2$.

For (2), define a map from the set of left cosets of H in G_1 to the set of left cosets of $\phi(H)$ in G_2 by

$$\Psi(gH) = \phi(g)\phi(H).$$

This map is well-defined. If $g_1H = g_2H$, then $g_2^{-1}g_1 \in H$, so $\phi(g_2)^{-1}\phi(g_1) \in \phi(H)$, and hence $\phi(g_1)\phi(H) = \phi(g_2)\phi(H)$. It is injective because if $\phi(g_1)\phi(H) = \phi(g_2)\phi(H)$, then $\phi(g_2^{-1}g_1) \in \phi(H)$, so $g_2^{-1}g_1 \in \phi^{-1}(\phi(H)) = H$, and therefore $g_1H = g_2H$. It is surjective because, for every $g' \in G_2$, surjectivity of ϕ gives $g \in G_1$ with $\phi(g) = g'$, and then $\Psi(gH) = g'\phi(H)$. Thus the two coset sets have the same cardinality, so $[G_1 : H] = [G_2 : \phi(H)]$. □

Lecture 21 — Monday, November 02, 2015

Corollary 21.1 Let G and H be groups with $G \cong H$. Then:

1. G and H have isomorphic subgroup lattices.
2. For each positive integer k, the groups G and H have the same number of subgroups of index k.

Proof. Let $\phi : G \to H$ be an isomorphism. Then ϕ is surjective and $\ker(\phi) = \{e\}$. Applying Theorem 20.3 with $G_1 = G$, $G_2 = H$, and $K = \{e\}$ gives a bijection

$$\{L \leq G\} \longleftrightarrow \{M \leq H\}, \quad L \mapsto \phi(L), \qquad \text{and} \qquad M \mapsto \phi^{-1}(M),$$

which preserves inclusion by (1). Hence the subgroup lattices are isomorphic. The same theorem also gives

$$[G : L] = [H : \phi(L)]$$

for every subgroup $L \leq G$, so this correspondence preserves subgroup index. Therefore G and H have the same number of subgroups of index k for each k. □

Corollary 21.2 Let G be a group and let $K \trianglelefteq G$. There is a one-to-one correspondence between subgroups of G containing K and subgroups of G/K, and this correspondence preserves inclusion and index.

Proof. Apply Theorem 20.3 to the quotient map

$$\pi : G \to G/K, \quad \pi(g) = gK.$$

This map is surjective and has kernel K, so all conclusions of the correspondence theorem apply directly. □

The previous corollary explains a pattern that appears repeatedly in examples: the subgroup lattice of G/K is exactly the portion of the subgroup lattice of G lying above K.

Corollary 21.3 Every quotient of a finite cyclic group is cyclic.

Proof. Let $G = \langle a \rangle$ be finite cyclic, and let $K \trianglelefteq G$. If $\pi : G \to G/K$ is the quotient map, then

$$G/K = \langle \pi(a) \rangle,$$

because every coset has the form $\pi(a^m) = \pi(a)^m$. Hence G/K is cyclic. □

4. Automorphism Groups

Automorphisms of a group are best interpreted as symmetries of the group's internal structure.

Definition 21.4 Let G be a group. An **automorphism** of G is an isomorphism $\phi : G \to G$. The set of all automorphisms of G is denoted by $\mathrm{Aut}(G)$.

Definition 21.5 For a group G, define the **identity automorphism**

$$\mathrm{id}_G : G \to G, \quad g \mapsto g.$$

The map id_G is always an automorphism, so $\mathrm{Aut}(G)$ is never empty.

Proposition 21.6 For every group G, the set $\mathrm{Aut}(G)$ is a group under composition.

Proof. If $\phi, \psi \in \mathrm{Aut}(G)$, then both are bijective homomorphisms, so $\phi \circ \psi$ is again a bijective homomorphism and therefore lies in $\mathrm{Aut}(G)$. Thus composition is a binary operation on $\mathrm{Aut}(G)$. Associativity follows from associativity of function composition.

The identity element is id_G, since $\mathrm{id}_G \circ \phi = \phi \circ \mathrm{id}_G = \phi$ for every $\phi \in \mathrm{Aut}(G)$.

Finally, let $\phi \in \mathrm{Aut}(G)$. Because ϕ is an isomorphism, it has an inverse map $\phi^{-1} : G \to G$ that is also a homomorphism. Hence $\phi^{-1} \in \mathrm{Aut}(G)$ and

$$\phi \circ \phi^{-1} = \phi^{-1} \circ \phi = \mathrm{id}_G \,.$$

Therefore every element has an inverse, so $\mathrm{Aut}(G)$ is a group under composition. □

Lecture 22 — Wednesday, November 04, 2015

Example 22.1 Let

$$V = \mathbb{Z}_2 \times \mathbb{Z}_2 = \{e, a, b, c\},$$

where a, b, c are the three nonidentity elements. Then

$$a^2 = b^2 = c^2 = e, \qquad ab = c, \qquad ac = b, \qquad \text{and} \qquad bc = a.$$

An automorphism of V permutes the three nonidentity elements, giving a homomorphism

$$\mathrm{Aut}(V) \to S_{\{a,b,c\}} \cong S_3.$$

This homomorphism is injective because an automorphism of V is determined by its values on a, b, c. It is surjective because any permutation of a, b, c preserves the displayed multiplication rules. Therefore

$$\mathrm{Aut}(\mathbb{Z}_2 \times \mathbb{Z}_2) \cong S_3.$$

The same computation appears in linear form as $GL_2(\mathbb{Z}_2) \cong S_3$. For example,

$$\begin{bmatrix} 0 & 1 \\ 1 & 1 \end{bmatrix} \begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} b \\ a+b \end{bmatrix}.$$

Thus this matrix sends $(1,0)$ to $(0,1)$, sends $(0,1)$ to $(1,1)$, and sends $(1,1)$ to $(1,0)$, which is a 3-cycle on the nonzero elements of $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Conjugation

Example 22.2 Let $\tau = (23) \in S_3$, and define $\phi_\tau : S_3 \to S_3$ by $\phi_\tau(\sigma) = \tau\sigma\tau^{-1}$. Then ϕ_τ acts by relabelling the entries of cycles:

$$\begin{array}{lll} (1) \mapsto (1), & (12) \mapsto (13), & (13) \mapsto (12), \\ (23) \mapsto (23), & (123) \mapsto (132), & (132) \mapsto (123). \end{array}$$

More generally, for any group G and any $a \in G$, the map

$$\phi_a : G \to G, \quad \phi_a(g) = aga^{-1},$$

is an automorphism.

Definition 22.3 Let G be a group and let $a \in G$. The map $\phi_a(g) = aga^{-1}$ is called **conjugation by a**. An automorphism of this form is called an **inner automorphism**. The set of all inner automorphisms is denoted by $\mathrm{Inn}(G)$.

Example 22.4 For Q_8, conjugation by i gives

$$\phi_i(i) = i, \qquad \phi_i(j) = iji^{-1} = -j, \qquad \text{and} \qquad \phi_i(k) = iki^{-1} = -k.$$

Also,

$$\phi_i(g) = igi^{-1} = (-i)g(-i)^{-1} = \phi_{-i}(g),$$

so $\phi_i = \phi_{-i}$. Similarly, $\phi_j = \phi_{-j}$ and $\phi_k = \phi_{-k}$. Together with the identity inner automorphism, this gives

$$|\mathrm{Inn}(Q_8)| = 4,$$

and in fact

$$\mathrm{Inn}(Q_8) \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \cong Q_8/\langle -1 \rangle.$$

Definition 22.5 The **center** of a group G is

$$Z(G) = \{a \in G : ag = ga \text{ for all } g \in G\}.$$

For example, $Z(Q_8) = \langle -1 \rangle$.

Theorem 22.6 For every group G,

$$G/Z(G) \cong \mathrm{Inn}(G).$$

Proof. Define

$$\Psi : G \to \mathrm{Inn}(G), \quad \Psi(a) = \phi_a.$$

For $a, b, g \in G$,

$$\phi_{ab}(g) = (ab)g(ab)^{-1} = a(bgb^{-1})a^{-1} = \phi_a(\phi_b(g)),$$

so $\phi_{ab} = \phi_a \circ \phi_b$. Hence Ψ is a homomorphism.

The map is surjective by definition of $\mathrm{Inn}(G)$. Its kernel is exactly $Z(G)$: if $a \in \ker(\Psi)$, then $\phi_a = \mathrm{id}_G$, so $aga^{-1} = g$ for all g, equivalently $ag = ga$ for all g, hence $a \in Z(G)$. Conversely, if $a \in Z(G)$, then $aga^{-1} = g$ for all g, so $\phi_a = \mathrm{id}_G$ and $a \in \ker(\Psi)$.

Therefore $\ker(\Psi) = Z(G)$, and the first isomorphism theorem yields

$$G/Z(G) \cong \mathrm{Inn}(G).$$

□

Corollary 22.7 If G is abelian, then $\mathrm{Inn}(G) = \{\mathrm{id}_G\}$.

Proof. If G is abelian, then $Z(G) = G$. Apply Theorem 22.6. □

Proposition 22.8 For every group G, the subgroup $\mathrm{Inn}(G)$ is normal in $\mathrm{Aut}(G)$.

Proof. Let $\psi \in \mathrm{Aut}(G)$ and $\phi_a \in \mathrm{Inn}(G)$. For each $g \in G$,

$$(\psi\phi_a\psi^{-1})(g) = \psi(a\psi^{-1}(g)a^{-1}) = \psi(a)g\psi(a)^{-1} = \phi_{\psi(a)}(g).$$

Thus $\psi\phi_a\psi^{-1} = \phi_{\psi(a)} \in \mathrm{Inn}(G)$, so $\mathrm{Inn}(G) \trianglelefteq \mathrm{Aut}(G)$. □

Definition 22.9 The **outer automorphism group** of G is

$$\mathrm{Out}(G) := \mathrm{Aut}(G)/\mathrm{Inn}(G).$$

Some standard facts for orientation are

$$\mathrm{Aut}(\mathbb{Z}_n) \cong \mathbb{Z}_n^\times, \qquad \text{and} \qquad \mathrm{Aut}(\mathbb{Z}_p^n) \cong GL_n(\mathbb{Z}_p),$$

and

$$\mathrm{Out}(S_n) \cong \begin{cases} \{e\}, & n \neq 6, \\ \mathbb{Z}_2, & n = 6. \end{cases}$$

Lecture 23 — Friday, November 06, 2015

Set-Theoretic Conventions

We recall the following set-theoretic language when discussing group actions. A function $f : X \to Y$ is **injective** if $f(x_1) = f(x_2)$ forces $x_1 = x_2$, and it is **surjective** if every element of Y is equal to $f(x)$ for some $x \in X$. A **bijection** is a function that is both injective and surjective.

An **equivalence relation** on a set X is a relation that is reflexive, symmetric, and transitive. The **equivalence class** of $x \in X$ is the set of all elements equivalent to x, and the equivalence classes partition X.

Proposition 23.1 Let $f : S \to T$ be a function between nonempty sets. Then the following hold:

1. f is injective if and only if it has a left inverse, that is, a function $g : T \to S$ such that $g \circ f = \mathrm{id}_S$.
2. f is surjective if and only if it has a right inverse, that is, a function $h : T \to S$ such that $f \circ h = \mathrm{id}_T$.
3. f is a bijection if and only if it has an inverse, that is, a function $k : T \to S$ such that $k \circ f = \mathrm{id}_S$ and $f \circ k = \mathrm{id}_T$.

Proof. For (1), suppose first that $g : T \to S$ satisfies $g \circ f = \mathrm{id}_S$. If $f(s_1) = f(s_2)$, then

$$s_1 = g(f(s_1)) = g(f(s_2)) = s_2,$$

so f is injective. Conversely, suppose f is injective. Choose an element $s_0 \in S$. Define $g : T \to S$ by

$$g(t) = \begin{cases} s, & t = f(s) \text{ for some } s \in S, \\ s_0, & t \notin f(S). \end{cases}$$

This is well-defined because injectivity makes the element s with $t = f(s)$ unique. Thus $g(f(s)) = s$ for all $s \in S$, so $g \circ f = \mathrm{id}_S$.

For (2), suppose first that $h : T \to S$ satisfies $f \circ h = \mathrm{id}_T$. If $t \in T$, then $t = f(h(t))$, so f is surjective. Conversely, suppose f is surjective. For each $t \in T$, the fibre $f^{-1}(\{t\})$ is nonempty; using the axiom of choice, choose an element $h(t) \in f^{-1}(\{t\})$. Then $f(h(t)) = t$ for every $t \in T$, so $f \circ h = \mathrm{id}_T$.

For (3), if $k : T \to S$ satisfies both identities, then (1) shows that f is injective and (2) shows that f is surjective, hence f is a bijection. Conversely, if f is a bijection, then for each $t \in T$ there is a unique $s \in S$ such that $f(s) = t$. Define $k(t) = s$. Then $k(f(s)) = s$ for all $s \in S$ and $f(k(t)) = t$ for all $t \in T$, so k is an inverse of f. □

Yes, we used the axiom of choice. Deal with it.

Proposition 23.2 Let G be a group and let $a \in G$. The map $f_a : G \to G$ defined by $f_a(g) = ag$ is a bijection.

Proof. The inverse of f_a is $f_{a^{-1}}$, since for any $g \in G$,

$$f_{a^{-1}}(f_a(g)) = a^{-1}(ag) = (a^{-1}a)g = eg = g,$$

and similarly,

$$f_a(f_{a^{-1}}(g)) = a(a^{-1}g) = (aa^{-1})g = eg = g.$$

Therefore, f_a is a bijection. □

Lecture 24 — Monday, November 09, 2015

5. Group Actions and Counting

Group Actions

Up to this point, we have studied groups as abstract algebraic objects. Group actions let us study them through the permutations they induce on concrete sets.

Example 24.1 The dihedral group D_5 acts on the vertices of a regular pentagon. Each symmetry of the pentagon gives a bijection from the set of vertices to itself.

Example 24.2 The Rubik's cube group acts on the set of states of a Rubik's cube.

Example 24.3 The group $GL_2(\mathbb{R})$ acts on $\mathbb{R}^2$ in the usual way:

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax + by \\ cx + dy \end{pmatrix}.$$

Since every matrix in $GL_2(\mathbb{R})$ is invertible, each element acts as a bijection on $\mathbb{R}^2$.

Example 24.4 Let G be the group of rotational symmetries of a regular tetrahedron. Then G acts on its 4 vertices. The identity is the only element that fixes every vertex; such an action is called **faithful**.

The same group also acts on the 3 lines joining midpoints of opposite edges. This action is not faithful, since a 180° rotation about one of these lines fixes all 3 lines.

Example 24.5 The group S_n acts on $\{1, \ldots, n\}$ by evaluation: $\sigma \cdot i = \sigma(i)$.

Example 24.6 Every group acts on itself by left multiplication. If $a \in G$, define $f_a : G \to G$ by $f_a(g) = ag$. Since left multiplication is a bijection, this gives a permutation of the underlying set of G.

In particular, if $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ and X is the underlying set of G, then the action by left multiplication gives a homomorphism $G \to S_X$. Since $|X| = 4$, we have $S_X \cong S_4$, so $\mathbb{Z}_2 \times \mathbb{Z}_2$ is isomorphic to a subgroup of S_4.

Definition 24.7 Let X be a set. We write S_X for the **permutation group of X**, that is, the group of bijections $X \to X$ under composition.

If $|X| = n$, then $S_X \cong S_n$.

Definition 24.8 Let G be a group and let X be a set. We say that G **acts on** X, and write $G \curvearrowright X$, if there is a function

$$\cdot : G \times X \to X$$

such that $e \cdot x = x$ for every $x \in X$, and

$$(gh) \cdot x = g \cdot (h \cdot x)$$

for every $g, h \in G$ and every $x \in X$.

For each $g \in G$, the action determines a function

$$\psi_g : X \to X, \quad \psi_g(x) = g \cdot x.$$

Proposition 24.9 For each $g \in G$, the map ψ_g is a bijection.

Proof. The inverse of ψ_g is $\psi_{g^{-1}}$. Indeed, for $x \in X$,

$$\psi_{g^{-1}}(\psi_g(x)) = g^{-1} \cdot (g \cdot x) = (g^{-1}g) \cdot x = e \cdot x = x,$$

and similarly $\psi_g(\psi_{g^{-1}}(x)) = x$. Hence ψ_g is bijective. □

Thus a group action assigns a permutation of X to each element of G in a way that respects the group structure.

Proposition 24.10 Let G be a group and let X be a set. Group actions of G on X are equivalent to homomorphisms $G \to S_X$.

Proof. *Forward implication.* Suppose $G \curvearrowright X$. For $g \in G$, define $\psi_g : X \to X$ by $\psi_g(x) = g \cdot x$. By Proposition 24.9, each ψ_g lies in S_X. Define $\phi : G \to S_X$ by $\phi(g) = \psi_g$. Then for $x \in X$,

$$\phi(gh)(x) = \psi_{gh}(x) = (gh) \cdot x = g \cdot (h \cdot x) = \psi_g(\psi_h(x)).$$

Thus $\phi(gh) = \phi(g)\phi(h)$, so ϕ is a homomorphism.

Reverse implication. Suppose $\phi : G \to S_X$ is a homomorphism. Define

$$g \cdot x = \phi(g)(x).$$

Then

$$e \cdot x = \phi(e)(x) = \mathrm{id}_X(x) = x$$

and

$$(gh) \cdot x = \phi(gh)(x) = (\phi(g)\phi(h))(x) = g \cdot (h \cdot x).$$

Therefore this rule defines an action of G on X. □

Cayley's Theorem

Theorem 24.11 (Cayley's theorem) Every group is isomorphic to a subgroup of a symmetric group.

Proof. Let G be a group, and let $X = G$. Define an action of G on itself by left multiplication:

$$g \cdot x = gx.$$

This is a group action, since $e \cdot x = ex = x$ and

$$g \cdot (h \cdot x) = g \cdot (hx) = (gh)x = (gh) \cdot x.$$

Let $\phi : G \to S_X$ be the associated homomorphism. If $\phi(g)$ is the identity permutation, then $g \cdot x = x$ for every $x \in X$. Taking $x = e$ gives $g = e$. Thus $\ker(\phi) = \{e\}$, so ϕ is injective. Therefore $G \cong \text{im}(\phi)$, and $\text{im}(\phi) \leq S_X$. □

Corollary 24.12 If $|G| = n$, then G is isomorphic to a subgroup of S_n.

Proof. Apply Theorem 24.11 to the action of G on itself by left multiplication, and note that $S_X \cong S_n$ since $|X| = |G| = n$. □

This is one reason the symmetric groups are so important: every finite group appears inside one of them.

Lecture 25 — Wednesday, November 11, 2015

Orbit-Stabilizer Theorem

Example 25.1 Let G be the group of rotational symmetries of a cube. We can count $|G|$ in several equivalent ways:

1. There are 6 choices for the image of a face and then 4 choices for the rotation about that face, so $|G| = 6 \cdot 4 = 24$.
2. There are 8 choices for the image of a vertex and then 3 choices for the image of an adjacent edge, so $|G| = 8 \cdot 3 = 24$.
3. There are 12 choices for the image of an edge and then 2 choices for its orientation, so

$|G| = 12 \cdot 2 = 24$.

4. There are 24 choices for the image of a directed edge, so $|G| = 24$.

Equivalently, the same group acts naturally on the set of faces, on the set of vertices, on the set of edges, and on the set of directed edges.

Definition 25.2 Let $G \curvearrowright X$. For $x \in X$, the **orbit** of x is

$$O_x = \{g \cdot x : g \in G\}.$$

The **stabilizer** of x is

$$S_x = \{g \in G : g \cdot x = x\}.$$

The orbit records where the point can move under the action, while the stabilizer records which group elements leave the point fixed. The orbit-stabilizer theorem relates these two complementary pieces of information.

Proposition 25.3 Let $G \curvearrowright X$ and let $x \in X$. Then $S_x \leq G$.

Proof. Since $e \cdot x = x$, we have $e \in S_x$. If $g, h \in S_x$, then $h \cdot x = x$, so applying h^{-1} gives $h^{-1} \cdot x = x$. Hence

$$(gh^{-1}) \cdot x = g \cdot (h^{-1} \cdot x) = g \cdot x = x.$$

Thus $gh^{-1} \in S_x$, and therefore $S_x \leq G$. □

Example 25.4 Let S_4 act on $\{1, 2, 3, 4\}$ in the usual way, and consider $4 \in X$. Its orbit is

$$O_4 = \{1, 2, 3, 4\},$$

because for each $a \in X$, the transposition $(4a)$ sends 4 to a. Its stabilizer is

$$\mathrm{Stab}_{S_4}(4) = \{\sigma \in S_4 : \sigma(4) = 4\} = \{(1), (12), (13), (23), (123), (132)\},$$

which is isomorphic to S_3 through its action on $\{1, 2, 3\}$.

Theorem 25.5 (Orbit-stabilizer theorem) Let $G \curvearrowright X$ and let $x \in X$. Then

$$[G : S_x] = |O_x|.$$

In particular, if G is finite, then

$$|G| = |S_x|\,|O_x|.$$

Proof. Let

$$T = \{gS_x : g \in G\}$$

be the set of left cosets of S_x. Define

$$\Phi : T \to O_x, \quad \Phi(gS_x) = g \cdot x.$$

This map is well-defined: if $gS_x = hS_x$, then $h^{-1}g \in S_x$, so $(h^{-1}g) \cdot x = x$. Applying h gives $g \cdot x = h \cdot x$.

The map Φ is surjective by definition of O_x. It is injective because if $g \cdot x = h \cdot x$, then $(h^{-1}g) \cdot x = x$, so $h^{-1}g \in S_x$, and hence $gS_x = hS_x$. Thus Φ is a bijection, so $[G : S_x] = |O_x|$. If G is finite, then $[G : S_x] = |G|/|S_x|$, which gives $|G| = |S_x|\,|O_x|$. □

Example 25.6 We compute $|GL_2(\mathbb{Z}_3)|$ using the natural action on $\mathbb{Z}_3^2$. Let

$$\boldsymbol{v} = \begin{pmatrix} 1 \\ 0 \end{pmatrix}.$$

The orbit of $\boldsymbol{v}$ is the set of nonzero vectors in $\mathbb{Z}_3^2$, because an invertible matrix may have any nonzero vector as its first column. Thus

$$|O_{\boldsymbol{v}}| = 3^2 - 1 = 8.$$

The stabilizer of $\boldsymbol{v}$ consists of invertible matrices whose first column is $\boldsymbol{v}$, namely

$$S_{\boldsymbol{v}} = \left\{ \begin{pmatrix} 1 & c \\ 0 & d \end{pmatrix} : c \in \mathbb{Z}_3,\ d \in \mathbb{Z}_3^\times \right\}.$$

There are 3 choices for c and 2 choices for d, so $|S_{\boldsymbol{v}}| = 6$. By Theorem 25.5,

$$|GL_2(\mathbb{Z}_3)| = |O_{\boldsymbol{v}}|\,|S_{\boldsymbol{v}}| = 8 \cdot 6 = 48.$$

Lecture 26 — Friday, November 13, 2015

Equivalence Relations and Partitions

Example 26.1 On $\mathbb{Z}$, define $a \sim b$ if $a - b \in 7\mathbb{Z}$. This identifies integers that are congruent modulo 7. The equivalence classes partition $\mathbb{Z}$:

$$[0] = \{\dots, -7, 0, 7, \dots\}, \qquad [1] = \{\dots, -6, 1, 8, \dots\}, \qquad [2] = \{\dots, -5, 2, 9, \dots\},$$

and similarly for the remaining congruence classes.

Example 26.2 Let

$$X = \{1, 2, 3, 4, 5, 6\}, \qquad Y_1 = \{1, 2\}, \qquad Y_2 = \{3, 4, 6\}, \qquad \text{and} \qquad Y_3 = \{5\}.$$

Define $a \sim b$ if a and b lie in the same subset Y_i. Then $\sim$ is reflexive, symmetric, and transitive, and the sets Y_1, Y_2, Y_3 are exactly its equivalence classes.

Definition 26.3 Let X be a set. An **equivalence relation** on X is a relation $\sim$ satisfying:

1. **Reflexivity**: $x \sim x$ for every $x \in X$.
2. **Symmetry**: if $x \sim y$, then $y \sim x$.
3. **Transitivity**: if $x \sim y$ and $y \sim z$, then $x \sim z$.

The **equivalence class** of $x \in X$ is

$$[x] = \{y \in X : y \sim x\},$$

and the set of equivalence classes is denoted by $X/\!\sim$.

Definition 26.4 A **partition** of a set X is a collection of nonempty subsets $\{Y_i\}_{i \in I}$ such

that $Y_i \cap Y_j = \emptyset$ whenever $i \neq j$, and

$$\bigcup_{i \in I} Y_i = X.$$

Proposition 26.5 Equivalence relations on X are equivalent to partitions of X.

Proof. *Forward implication.* Suppose $\sim$ is an equivalence relation on X. Every $x \in X$ lies in $[x]$, so the equivalence classes cover X. If $[x] \cap [y] \neq \emptyset$, choose $z \in [x] \cap [y]$. Then $z \sim x$ and $z \sim y$, so symmetry and transitivity give $x \sim y$. It follows that an element is equivalent to x exactly when it is equivalent to y, so $[x] = [y]$. Hence distinct equivalence classes are disjoint, and the equivalence classes partition X.

Reverse implication. Suppose $\{Y_i\}_{i \in I}$ is a partition of X. Define $a \sim b$ if a and b lie in the same part Y_i. This relation is reflexive because every element lies in some part, symmetric by definition, and transitive because if $a, b \in Y_i$ and $b, c \in Y_j$, then $b \in Y_i \cap Y_j$, so $Y_i = Y_j$ and $a, c \in Y_i$. Therefore $\sim$ is an equivalence relation, and its equivalence classes are the parts of the partition. □

Example 26.6 Let G be a group and let $H \leq G$. Define $g_1 \sim g_2$ if $g_1^{-1} g_2 \in H$. This is an equivalence relation on G: reflexivity follows from $g^{-1} g = e \in H$; symmetry follows because $g_1^{-1} g_2 \in H$ implies $(g_1^{-1} g_2)^{-1} = g_2^{-1} g_1 \in H$; and transitivity follows because

$$g_1^{-1} g_3 = (g_1^{-1} g_2)(g_2^{-1} g_3) \in H$$

whenever $g_1^{-1} g_2$ and $g_2^{-1} g_3$ lie in H. The equivalence class of g is

$$[g] = \{x \in G : g^{-1} x \in H\} = gH.$$

Thus the left cosets of H partition G.

Example 26.7 The group $GL_2(\mathbb{Z}_2)$ acts on $\mathbb{Z}_2^2$ by matrix multiplication. The zero vector is fixed by every matrix, so

$$O_{(0,0)} = \{(0, 0)\}.$$

The three nonzero vectors form a single orbit, so

$$O_{(1,0)} = \mathbb{Z}_2^2 \setminus \{(0,0)\}.$$

Example 26.8 Let $\mathbb{Z}_2$ act on $\{1,2,3,4,5,6\}$ through the homomorphism $\phi : \mathbb{Z}_2 \to S_6$ that sends the nonidentity element to $(12)(34)$. The orbits are

$$\{1,2\}, \qquad \{3,4\}, \qquad \{5\}, \qquad \text{and} \qquad \{6\}.$$

Proposition 26.9 Let $G \curvearrowright X$. Then the set of orbits $\{O_x : x \in X\}$ partitions X.

Proof. Define $x \sim y$ if there is some $g \in G$ such that $g \cdot x = y$. This is an equivalence relation. Reflexivity follows from $e \cdot x = x$. Symmetry follows because if $g \cdot x = y$, then $x = g^{-1} \cdot y$. Transitivity follows because if $g \cdot x = y$ and $h \cdot y = z$, then

$$(hg) \cdot x = h \cdot (g \cdot x) = h \cdot y = z.$$

By Proposition 26.5, the equivalence classes partition X. The equivalence class of x is

$$[x] = \{y \in X : y \sim x\} = \{y \in X : y = g \cdot x \text{ for some } g \in G\} = O_x.$$

Therefore the orbits partition X. □

Cauchy's Theorem

Theorem 26.10 (Cauchy's theorem) Let G be a finite group, and let p be a prime dividing $|G|$. Then there is an element $g \in G$ with $|g| = p$.

Lecture 27 — Monday, November 16, 2015

Proof. Let

$$X = \{(g_1, \ldots, g_p) \in G^p : g_1 g_2 \cdots g_p = e\}.$$

The first $p-1$ entries determine the last one, so $|X| = |G|^{p-1}$. Since p divides $|G|$, it follows that p divides $|X|$.

The group $\mathbb{Z}_p$ acts on X by cyclic shifts:

$$1 \cdot (g_1, \ldots, g_p) = (g_p, g_1, \ldots, g_{p-1}).$$

This action is well-defined. Indeed, if $g_1 \cdots g_p = e$, then $g_1 \cdots g_{p-1} = g_p^{-1}$, and hence

$$g_p g_1 \cdots g_{p-1} = g_p g_p^{-1} = e.$$

Every orbit under this action has size either 1 or p, by Theorem 25.5. Since $|X|$ is divisible by p, the number of singleton orbits is divisible by p. A tuple has a singleton orbit exactly when all its entries are equal:

$$(g_1, \ldots, g_p) = (g, g, \ldots, g).$$

The tuple $(e, e, \ldots, e)$ is one such tuple, so there must be at least one more. Therefore there is some $g \neq e$ such that

$$(g, g, \ldots, g) \in X.$$

This means $g^p = e$. Hence $|g|$ divides p, and since $g \neq e$, we conclude $|g| = p$. □

For $p = 3$, the cyclic action is

$$0 \cdot (a, b, c) = (a, b, c), \qquad 1 \cdot (a, b, c) = (c, a, b), \qquad \text{and} \qquad 2 \cdot (a, b, c) = (b, c, a).$$

Lemma 27.1 If g and h commute and $\gcd(|g|, |h|) = 1$, then $|gh| = |g|\,|h|$.

Proof. Let $m = |g|$ and $n = |h|$. Since g and h commute,

$$(gh)^{mn} = g^{mn} h^{mn} = e,$$

so $|gh|$ divides mn. Conversely, suppose $(gh)^r = e$. Then $g^r = h^{-r}$ lies in $\langle g\rangle \cap \langle h\rangle$. The order of any element in this intersection divides both m and n, so it is 1. Hence $g^r = e$ and $h^r = e$, so m and n both divide r. Since $\gcd(m, n) = 1$, mn divides r. Therefore $|gh| = mn$. □

Corollary 27.2 Let G be abelian and let $|G| = pq$, where p and q are distinct primes. Then G is cyclic.

Proof. By Cauchy's theorem, there are elements $g, h \in G$ with $|g| = p$ and $|h| = q$. Since G is abelian, g and h commute. By Lemma 27.1,

$$|gh| = pq.$$

Thus gh generates G, so G is cyclic. □

Natural Actions on the Group Itself

Example 27.3 Let G be a finite group and let

$$X = \{T \subseteq G : |T| = k\}.$$

Then G acts on X by left multiplication:

$$g \cdot T = gT = \{gt : t \in T\}.$$

If T is a subgroup, then the stabilizer of T under this action is exactly T. Indeed, every $t \in T$ satisfies $tT = T$, so $T \subseteq S_T$. Conversely, if $gT = T$, then $g = ge \in gT = T$, so $g \in T$. Hence $S_T = T$. Applying the orbit-stabilizer theorem to this action gives another route to Lagrange's theorem.

There are three especially natural actions of a group G on itself:

$$g \cdot x = gx, \qquad g \cdot x = xg^{-1}, \qquad \text{and} \qquad g \cdot x = gxg^{-1}.$$

The first is left multiplication, the second is right multiplication, and the third is conjugation. The right multiplication rule is an action because

$$(gh) \cdot x = x(gh)^{-1} = xh^{-1}g^{-1} = g \cdot (h \cdot x),$$

and $e \cdot x = xe^{-1} = x$.

Example 27.4 Under left multiplication, S_3 acts transitively on itself: for any $\sigma \in S_3$, we have $\sigma \cdot (1) = \sigma$. The same is true for right multiplication.

Example 27.5 Consider the conjugation action of S_3 on itself. The conjugates of (12) are

a	$a(12)a^{-1}$
(1)	(12)
(12)	(12)
(13)	(23)
(23)	(13)
(123)	(23)
(132)	(13)

Therefore

$$O_{(12)} = \{(12), (13), (23)\} \qquad \text{and} \qquad S_{(12)} = \{(1), (12)\}.$$

The remaining conjugacy classes and stabilizers are

$$O_{(1)} = \{(1)\} \qquad \text{and} \qquad S_{(1)} = S_3,$$

and

$$O_{(123)} = \{(123), (132)\} \qquad \text{and} \qquad S_{(123)} = \{(1), (123), (132)\}.$$

Thus elements in the same orbit can have different stabilizers; for example, $O_{(12)} = O_{(13)}$, but $S_{(12)} \neq S_{(13)}$.

Definition 27.6 Let G act on itself by conjugation. The orbit of g under this action is called the **conjugacy class** of g and is denoted by K_g. The stabilizer of g under this action is called the **centralizer** of g and is denoted by C_g.

Thus

$$K_g = \{aga^{-1} : a \in G\} \qquad \text{and} \qquad C_g = \{a \in G : ag = ga\}.$$

Example 27.7 For the conjugation action of Q_8 on itself, the central elements 1 and -1

have singleton conjugacy classes:

$$K_1 = \{1\}, \qquad K_{-1} = \{-1\}, \qquad \text{and} \qquad C_1 = C_{-1} = Q_8.$$

The remaining conjugacy classes are

$$K_i = \{i, -i\}, \qquad K_j = \{j, -j\}, \qquad \text{and} \qquad K_k = \{k, -k\},$$

and the corresponding centralizers are

$$C_i = \langle i \rangle, \qquad C_j = \langle j \rangle, \qquad \text{and} \qquad C_k = \langle k \rangle.$$

Proposition 27.8 For every group G,

$$Z(G) = \bigcap_{g \in G} C_g.$$

Proof. An element $a \in G$ lies in the intersection of all centralizers exactly when $ag = ga$ for every $g \in G$, which is exactly the condition $a \in Z(G)$. □

Lecture 28 — Wednesday, November 18, 2015

Counting Problems

Question 28.1 How many ways can we colour the vertices of a square with two black dots and two white dots?

There are $\binom{4}{2} = 6$ colourings before identifying colourings that differ only by rotation. Figure 14 labels the six colourings and displays their rotation orbits.

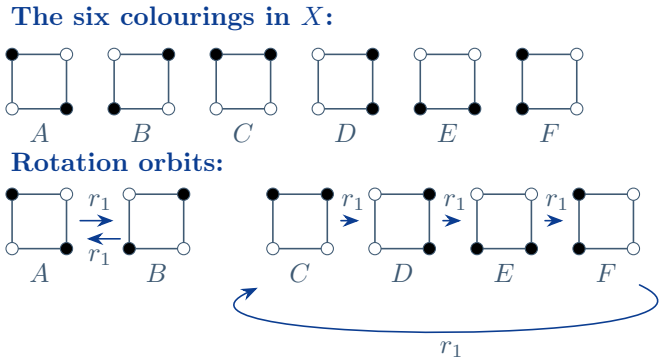


FIGURE 14

Let $H = \{e, r_1, r_2, r_3\} \leq D_4$ be the rotation subgroup, and let X be the set of these six colourings. The group H acts on X by rotating the square. There are two orbits: adjacent black vertices and opposite black vertices.

This example suggests two useful averaging formulas. First, if N is the number of orbits, then

$$N = \frac{1}{|G|} \sum_{x \in X} |S_x|.$$

For the square example, this gives

$$N = \frac{1}{4}(2 + 2 + 1 + 1 + 1 + 1) = 2.$$

Here the first two terms come from the colourings A and B, which are fixed by the half-turn r_2,

while the remaining four colourings have trivial stabilizer.

Definition 28.2 Let $G \curvearrowright X$. For $g \in G$, the **fixed set** of g is

$$X_g = \{x \in X : g \cdot x = x\}.$$

For the same square action,

$$X_e = X, \qquad X_{r_1} = \emptyset, \qquad X_{r_2} = \{A, B\}, \qquad \text{and} \qquad X_{r_3} = \emptyset.$$

Thus

$$\frac{1}{4}\sum_{g \in H} |X_g| = \frac{1}{4}(6 + 0 + 2 + 0) = 2.$$

This is not a coincidence.

The Lemma That is Not Burnside's

Theorem 28.3 (The lemma that is not Burnside's, or Burnside's lemma) Let G be a finite group acting on a finite set X, and let N be the number of orbits. Then

$$N = \frac{1}{|G|}\sum_{g \in G} |X_g|.$$

Proof. Let

$$T = \{(g, x) \in G \times X : g \cdot x = x\}.$$

Counting first by group elements gives

$$|T| = \sum_{g \in G} |X_g|.$$

Counting first by elements of X gives

$$|T| = \sum_{x \in X} |S_x|.$$

By Theorem 25.5,

$$|S_x| = \frac{|G|}{|O_x|}.$$

If O is an orbit, then $O_x = O$ for every $x \in O$, so

$$\sum_{x \in O} \frac{|G|}{|O_x|} = \sum_{x \in O} \frac{|G|}{|O|} = |G|.$$

Summing over the N orbits gives $|T| = N|G|$. Therefore

$$\sum_{g \in G} |X_g| = N|G|,$$

and the desired formula follows. □

Question 28.4 How many ways can we number an eight-sided die?

The rotational symmetry group of the octahedron has order 24: if x is a face, then $|O_x| = 8$ and $|S_x| = 3$, so Theorem 25.5 gives $|G| = 24$. Let X be the set of numberings of the eight faces with the numbers $1, \ldots, 8$. Then $|X| = 8!$.

The identity fixes all 8! numberings. No nonidentity rotation fixes a numbering, because the numbers on the faces are all distinct. Hence Burnside's lemma gives

$$N = \frac{1}{24} \sum_{g \in G} |X_g| = \frac{8!}{24} = 1680.$$

Lecture 29 — Friday, November 20, 2015

Example 29.1 How many necklaces can we make with 5 beads, where each bead can be either black or white? Model a necklace as a colouring of the vertices of a regular pentagon using black and white. Let

$$G = D_5 = \{e, r_1, r_2, r_3, r_4, f_1, f_2, f_3, f_4, f_5\}$$

act on the set X of all such colourings. Then $|X| = 2^5 = 32$.

The group action and its fixed sets are illustrated in Figure 15.

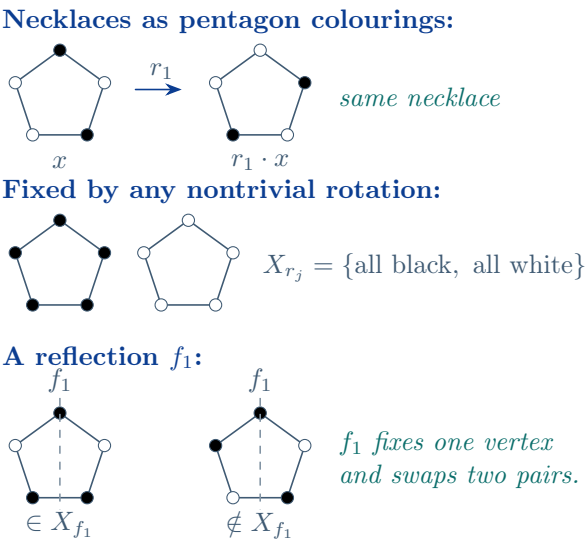


FIGURE 15

The identity fixes all colourings, so $|X_e| = 32$. A nontrivial rotation fixes exactly the two constant colourings, so

$$|X_{r_1}| = \cdots = |X_{r_4}| = 2.$$

Each reflection fixes one vertex and swaps two pairs of vertices. Therefore a colouring fixed by a reflection is determined by three independent colour choices: the fixed vertex and one colour for each swapped pair. Hence

$$|X_{f_i}| = 2^3 = 8$$

for each $i = 1, \ldots, 5$. By Burnside's lemma,

$$N = \frac{1}{|D_5|} \sum_{g \in D_5} |X_g| = \frac{1}{10}(32 + 4 \cdot 2 + 5 \cdot 8) = 8.$$

Thus there are 8 binary necklaces with 5 beads, up to dihedral symmetry.

Lecture 30 — Monday, November 23, 2015

Proposition 30.1 If $K \leq H \leq G$ and the relevant indices are finite, then

$$[G : K] = [G : H][H : K].$$

In particular, if $[G : H] = 1$, then $H = G$.

Proof. Choose representatives $\{g_i\}_{i\in I}$ for the left cosets of H in G, and representatives $\{h_j\}_{j\in J}$ for the left cosets of K in H. Then the elements $g_i h_j$ represent the left cosets of K in G. Indeed, every $g \in G$ can be written as $g = g_i h$ with $h \in H$, and then $h = h_j k$ with $k \in K$, so $g = g_i h_j k$. The representation is unique up to the chosen cosets, so the number of left cosets of K in G is $|I||J| = [G : H][H : K]$.

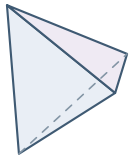
If $[G : H] = 1$, then H is the only left coset of H in G, so every element of G lies in H. Hence $H = G$. □

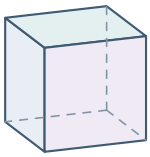
6. Symmetry Groups and Applications

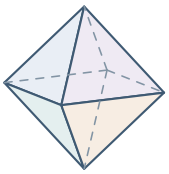
Platonic Solids

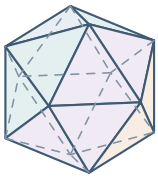
Definition 30.2 A **Platonic solid** is a convex polyhedron such that every face is the same regular polygon and every vertex has the same number of faces meeting at it.

The five Platonic solids are displayed together in Figure 16: the tetrahedron, cube, octahedron, icosahedron, and dodecahedron.


Tetrahedron


Cube


Octahedron


Icosahedron

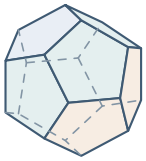

Dodecahedron

FIGURE 16

Let V, E, and F denote the numbers of vertices, edges, and faces, respectively.

	Tetrahedron	Cube	Octahedron	Icosahedron	Dodecahedron
V	4	8	6	12	20
E	6	12	12	30	30
F	4	6	8	20	12

Fact 30.3

1. These five are the *only* Platonic solids.
2. For any convex polyhedron, $V - E + F = 2$.

Definition 30.4 The **dual** of a polyhedron is formed by creating a vertex for each face of the original polyhedron and joining two new vertices by an edge exactly when the corresponding faces are adjacent.

Platonic solid	Dual
Tetrahedron	Tetrahedron
Cube	Octahedron
Octahedron	Cube
Icosahedron	Dodecahedron
Dodecahedron	Icosahedron

Rotational Symmetry Groups

We study rotational symmetry groups by finding useful actions on finite sets. For a tetrahedron, let G act on the set of 4 vertices. If v is a vertex, then $|O_v| = 4$ and $|S_v| = 3$, so Theorem 25.5 gives

$$|G| = |O_v|\,|S_v| = 12.$$

The same method gives the following table. The stabilizer contribution is the number of rotations about the chosen feature, and the orbit contribution is the number of possible images of that feature.

Platonic solid	Order of the rotational symmetry group
Tetrahedron	12
Cube	24
Octahedron	24
Icosahedron	60
Dodecahedron	60

Definition 30.5 An action $G \curvearrowright X$ is **faithful** if the identity is the only element of G that fixes every point of X.

Proposition 30.6 Let $G \curvearrowright X$, and let $\phi : G \to S_X$ be the corresponding homomorphism. The action is faithful if and only if ϕ is injective.

Proof. *Forward implication.* Suppose the action is faithful. If $\phi(g) = \mathrm{id}_X$, then $g \cdot x = x$ for every $x \in X$, so $g = e$. Thus $\ker(\phi) = \{e\}$, and ϕ is injective.

Reverse implication. Suppose ϕ is injective. If g fixes every point of X, then $\phi(g) = \mathrm{id}_X = \phi(e)$. Since ϕ is injective, $g = e$. Therefore the action is faithful. □

For the tetrahedron, let G be the rotational symmetry group and let $X = \{1, 2, 3, 4\}$ be the set of vertices. The natural action $G \curvearrowright X$ is faithful, since a rotation fixing every vertex is the identity. The 12 rotations consist of the identity, the two nonidentity rotations about each vertex-opposite-face axis, and the three 180° rotations about axes through midpoints of opposite edges.

Lecture 31 — Wednesday, November 25, 2015

We now describe the tetrahedron action explicitly. Let G be the rotational symmetry group of a regular tetrahedron, and let

$$X = \{\text{vertices of the tetrahedron}\} = \{1, 2, 3, 4\}.$$

The natural action $G \curvearrowright X$ gives a homomorphism $\phi : G \to S_4$.

The vertex labelling used below is shown in Figure 17.

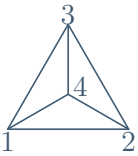


FIGURE 17

The elements of G are the identity e, the rotations r_i and r_i^2 for each $i \in \{1, 2, 3, 4\}$, and the rotations d_2, d_3, d_4. Here r_i and r_i^2 are the 120° and 240° rotations about the axis through the ith vertex and the centre of the opposite face. The rotation d_i, for $i \in \{2, 3, 4\}$, is the 180° rotation about the axis through the midpoint of the edge joining 1 to i and the midpoint of the opposite edge. Thus $|G| = 12$.

The identity fixes every vertex. The rotations r_i and r_i^2 fix the vertex i and cycle the other three vertices. The rotations d_2, d_3, d_4 interchange two pairs of vertices. Explicitly,

$$\begin{array}{lll} \phi(e) = (1), & \phi(r_1) = (2\,3\,4), & \phi(r_1^2) = (2\,4\,3), \\ \phi(r_2) = (1\,4\,3), & \phi(r_2^2) = (1\,3\,4), & \phi(r_3) = (1\,2\,4), \\ \phi(r_3^2) = (1\,4\,2), & \phi(r_4) = (1\,3\,2), & \phi(r_4^2) = (1\,2\,3), \\ \phi(d_2) = (1\,2)(3\,4), & \phi(d_3) = (1\,3)(2\,4), & \phi(d_4) = (1\,4)(2\,3). \end{array}$$

Proposition 31.1 The rotational symmetry group of a tetrahedron is isomorphic to A_4.

Proof. The action of G on the vertices is faithful, since a rotation fixing every vertex is the identity. Hence the associated homomorphism $\phi : G \to S_4$ is injective by Proposition 30.6. The displayed list shows that every element of $\mathrm{im}(\phi)$ is an even permutation, so $\mathrm{im}(\phi) \leq A_4$. Since

$|\operatorname{im}(\phi)| = |G| = 12$ and $|A_4| = 12$, it follows that $\operatorname{im}(\phi) = A_4$. Therefore $G \cong A_4$. □

The tetrahedron also acts on

$$Y = \{\text{lines joining midpoints of opposite edges}\}.$$

There are three such lines. The elements e, d_2, d_3, d_4 fix every element of Y, so the associated homomorphism $\psi : G \to S_Y \cong S_3$ has kernel

$$\ker(\psi) = \{e, d_2, d_3, d_4\}.$$

Under the isomorphism in Proposition 31.1, this kernel gives a proper nontrivial normal subgroup of A_4. Thus A_4 is not simple.

Next let G be the rotational symmetry group of a cube. Then $|G| = 24$. Let

$$X = \{\text{lines joining opposite vertices of the cube}\}.$$

There are four such lines, and the action $G \curvearrowright X$ is faithful: a rotation fixing all four body diagonals is the identity.

The elements of G can be organized by their rotation axes. The identity fixes all four elements of X. The rotations by 90°, 180°, and 270° about axes through opposite faces give 9 elements, and they fix no element of X. The rotations by 120° and 240° about axes through opposite vertices give 8 elements, and each fixes exactly one element of X. Finally, the 180° rotations about axes through midpoints of opposite edges give 6 elements, and each fixes two elements of X while switching the other two.

Proposition 31.2 The rotational symmetry group of a cube is isomorphic to S_4.

Proof. The faithful action on the four body diagonals gives an injective homomorphism $\phi : G \to S_4$ by Proposition 30.6. Since $|G| = 24 = |S_4|$, this injective homomorphism is also surjective. Hence $G \cong S_4$. □

Example 31.3 Write down the isomorphism in Proposition 31.2 explicitly, as in the tetrahedron computation above.

Solution. Let d_1, d_2, d_3, d_4 be the four body diagonals of the cube, where

$$d_1 = \overline{(1,1,1)(-1,-1,-1)}, \quad d_2 = \overline{(1,1,-1)(-1,-1,1)},$$
$$d_3 = \overline{(1,-1,1)(-1,1,-1)}, \quad d_4 = \overline{(-1,1,1)(1,-1,-1)}.$$

If G is the rotation group of the cube, define

$$\phi : G \to S_4$$

by letting $\phi(g)$ be the permutation induced by the action of g on the set $\{d_1, d_2, d_3, d_4\}$. In other words, $\phi(g)(i) = j$ when $g(d_i) = d_j$. This is exactly the homomorphism used in the proof of Proposition 31.2.

With this labeling, a 90° rotation about the z-axis sends

$$d_1 \mapsto d_4 \mapsto d_3 \mapsto d_2 \mapsto d_1,$$

so it corresponds to $(1\,4\,3\,2)$. A 120° rotation about the diagonal d_1 fixes d_1 and cycles the other three diagonals, so it corresponds to $(2\,3\,4)$. A 180° rotation about the x-axis interchanges d_1 with d_4 and d_2 with d_3, so it corresponds to $(1\,4)(2\,3)$. Thus the isomorphism sends each cube rotation to the permutation it induces on the four body diagonals, and this identifies the cube rotation group with S_4. □

The inclusion $A_4 < S_4$ has a geometric interpretation. A cube contains two regular tetrahedra, obtained by choosing alternating vertices. The cube rotation group acts on the set of these two tetrahedra, and the subgroup preserving each tetrahedron is the rotational symmetry group of one tetrahedron.

Proposition 31.4 We have $\mathrm{Aut}(Q_8) \cong S_4$.

Proof. Identify i, j, k with the three positive coordinate-axis directions of a cube. A cube rotation sends the ordered right-handed frame (i, j, k) to another ordered right-handed frame chosen from $\{\pm i, \pm j, \pm k\}$. The images satisfy the same quaternion relations, so the rotation induces an automorphism of Q_8. This gives an injective homomorphism from the cube rotation group into $\mathrm{Aut}(Q_8)$: a rotation acting trivially on $\{\pm i, \pm j, \pm k\}$ is the identity. Consequently,

$$|\,\mathrm{Aut}(Q_8)| \geq 24.$$

For the reverse bound, an automorphism ℓ fixes 1 and -1 and is determined by $\ell(i)$ and $\ell(j)$, because $\ell(k) = \ell(i)\ell(j)$. There are six possible images of i, namely $\pm i, \pm j, \pm k$. Once $\ell(i)$ is chosen, the element $\ell(j)$ must be one of the four elements of order 4 outside $\langle \ell(i) \rangle$; otherwise the images would not generate Q_8. Hence

$$|\operatorname{Aut}(Q_8)| \leq 6 \cdot 4 = 24.$$

The injective homomorphism from the cube rotation group is therefore an isomorphism. By Proposition 31.2, $\operatorname{Aut}(Q_8) \cong S_4$. □

Example 31.5 A 180° rotation about the i-axis gives the automorphism

$$\ell(i) = i, \qquad \ell(j) = -j, \qquad \text{and} \qquad \ell(k) = -k.$$

This is the same automorphism as conjugation by i.

Lecture 32 — Friday, November 27, 2015

Generating Sets and Alternating Groups

We briefly return to generating sets because they provide an efficient route to a structural fact about A_n. For example, the set

$$S = \{(1,0), (0,1)\} \subseteq \mathbb{Z}_3 \times \mathbb{Z}_2$$

generates $\mathbb{Z}_3 \times \mathbb{Z}_2$, since every $(a, b) \in \mathbb{Z}_3 \times \mathbb{Z}_2$ can be written as a sum of a copies of $(1, 0)$ and b copies of $(0, 1)$.

Definition 32.1 Let G be a group, and let $H \leq G$. A **generating set** for H is a subset $S \subseteq H$ such that every subgroup $K \leq G$ containing S also contains H. In this case, we say that S generates H.

Example 32.2 Prove that $\mathbb{Z}$ is generated by $\{1\}$.

Solution. Let $H \leq \mathbb{Z}$ and suppose $1 \in H$. Since H is closed under addition and inverses, it contains every integer multiple of 1. Hence $H = \mathbb{Z}$, so $\{1\}$ generates $\mathbb{Z}$. □

Example 32.3 Prove that $\mathbb{Z}$ is generated by $\{-1\}$.

Solution. Let $H \leq \mathbb{Z}$ and suppose $-1 \in H$. Then $1 = -(-1) \in H$, so the previous example implies that $H = \mathbb{Z}$. Therefore $\{-1\}$ generates $\mathbb{Z}$. □

Example 32.4 Prove that $\mathbb{Z}$ is generated by $\{2, 3\}$.

Solution. Let $H \leq \mathbb{Z}$ with $2, 3 \in H$. Then

$$1 = 3 - 2 \in H.$$

By the first example, $H = \mathbb{Z}$. Therefore $\{2, 3\}$ generates $\mathbb{Z}$. □

Example 32.5 Prove that S_n is generated by the set of all transpositions.

Solution. Every permutation can be written as a product of disjoint cycles, and every cycle can be written as a product of transpositions:

$$(a_1\, a_2\, \ldots\, a_k) = (a_1\, a_k)(a_1\, a_{k-1}) \ldots (a_1\, a_2).$$

Thus every element of S_n is a product of transpositions. Therefore any subgroup of S_n containing all transpositions must be all of S_n, so the transpositions generate S_n. □

Example 32.6 Prove that S_n is generated by $\{(1\,2), (1\,2\,\cdots\,n)\}$.

Solution. Let

$$\tau = (1\,2) \qquad \text{and} \qquad c = (1\,2\,\cdots\,n).$$

For each $k = 1, \ldots, n-1$,

$$c^{k-1}\tau c^{-(k-1)} = (k\ k+1).$$

So the subgroup generated by τ and c contains all adjacent transpositions. But every transposition

can be written as a product of adjacent transpositions, for example

$$(i\,j) = (i\;i+1)\dots(j-2\;j-1)(j-1\;j)(j-2\;j-1)\dots(i\;i+1)$$

when $i < j$. Hence this subgroup contains all transpositions, and by the previous example it is all of S_n. Therefore $\{(1\,2), (1\,2\,\cdots\,n)\}$ generates S_n. □

Example 32.7 Prove that D_n is generated by $\{r, f\}$ for any reflection f.

Solution. Let $H \leq D_n$ contain r and a reflection f. Then H contains all powers

$$e, r, r^2, \dots, r^{n-1}.$$

Since $f \in H$, it also contains

$$f,\; rf,\; r^2f,\; \dots,\; r^{n-1}f.$$

These are exactly the elements of D_n, so $H = D_n$. Therefore $\{r, f\}$ generates D_n. □

Example 32.8 Prove that Q_8 is generated by $\{i, j\}$.

Solution. The subgroup containing i and j must also contain

$$i^2 = j^2 = -1 \qquad \text{and} \qquad ij = k.$$

Hence it contains

$$1,\; -1,\; \pm i,\; \pm j,\; \pm k,$$

which are all the elements of Q_8. Therefore $\{i, j\}$ generates Q_8. □

Example 32.9 Prove that $\mathbb{Z}_n \times \mathbb{Z}_m$ is generated by $\{(1,0), (0,1)\}$.

Solution. Let $H \leq \mathbb{Z}_n \times \mathbb{Z}_m$ contain $(1,0)$ and $(0,1)$. If $(a,b) \in \mathbb{Z}_n \times \mathbb{Z}_m$, then

$$(a,b) = a(1,0) + b(0,1).$$

Since H is closed under the group operation, $(a,b) \in H$. Thus $H = \mathbb{Z}_n \times \mathbb{Z}_m$, so $\{(1,0), (0,1)\}$ generates $\mathbb{Z}_n \times \mathbb{Z}_m$. □

We first identify a convenient generating set for A_n, and then use it to prove that A_n is the unique subgroup of index 2 in S_n.

Lemma 32.10 For $n \geq 2$, the group A_n is generated by all 3-cycles in S_n.

Proof. Let S be the set of all 3-cycles in S_n, and let $H \leq S_n$ be a subgroup containing S. We show that $A_n \leq H$.

Every element of A_n can be written as a product of an even number of transpositions, so it is enough to show that the product of any two transpositions can be written as a product of 3-cycles. If the two transpositions share one entry, then their product is a 3-cycle. For instance,

$$(a\,b)(a\,c) = (a\,c\,b).$$

If the two transpositions are disjoint, then

$$(a\,b)(c\,d) = (a\,c\,b)(a\,c\,d).$$

Thus every element of A_n is a product of 3-cycles. Since all 3-cycles lie in H, we have $A_n \leq H$. Therefore the 3-cycles generate A_n. □

Proposition 32.11 The group A_4 has no subgroup of order 6.

Proof. Suppose that $H \leq A_4$ has order 6. Then $[A_4 : H] = 2$, so $H \trianglelefteq A_4$ by Proposition 17.3, and the quotient A_4/H has order 2. Let $\pi : A_4 \to A_4/H$ be the quotient map. If τ is a 3-cycle, then

$$\pi(\tau)^3 = H \qquad \text{and} \qquad \pi(\tau)^2 = H.$$

Consequently $\pi(\tau) = H$, so every 3-cycle lies in H. By Lemma 32.10, the 3-cycles generate A_4. Hence $H = A_4$, contradicting $|H| = 6$. □

Lemma 32.12 Every subgroup of index 2 in S_n contains all 3-cycles.

Proof. Let $H \leq S_n$ satisfy $[S_n : H] = 2$. By Proposition 17.3, $H \trianglelefteq S_n$, so S_n/H has order 2.

Hence $(\sigma H)^2 = H$ for every $\sigma \in S_n$, which means that $\sigma^2 \in H$ for every $\sigma \in S_n$. Since

$$(a\,b\,c) = (a\,c\,b)^2,$$

every 3-cycle lies in H. □

Theorem 32.13 For $n \geq 2$, the subgroup A_n is the unique subgroup of index 2 in S_n.

Proof. Let $H \leq S_n$ satisfy $[S_n : H] = 2$. By Lemma 32.12, H contains all 3-cycles. Hence Lemma 32.10 gives $A_n \leq H$. But $|H| = |S_n|/2 = |A_n|$, so $H = A_n$. □

The Dodecahedron, Octahedron and Icosahedron

Let G be the rotational symmetry group of a dodecahedron. Then $|G| = 60$. We use the natural action of G on the set X of the five cubes inscribed in the dodecahedron.

Lecture 33 — Monday, November 30, 2015

The action of the dodecahedron rotation group on the five inscribed cubes is faithful. The elements of G can be counted by their rotation axes. The identity fixes every element of X. The axes through midpoints of opposite faces give 6 axes, each with 4 nonidentity rotations, for 24 elements; each such rotation fixes no element of X. The axes through opposite edges give 15 axes, each with 1 nonidentity rotation, for 15 elements; each such rotation fixes exactly one element of X. The axes through opposite vertices give 10 axes, each with 2 nonidentity rotations, for 20 elements; each such rotation fixes exactly two elements of X.

Proposition 33.1 The rotational symmetry group of the dodecahedron is isomorphic to A_5.

Proof. The faithful action on the five inscribed cubes gives an injective homomorphism

$$\phi : G \to S_5.$$

Thus $\operatorname{im}(\phi) \leq S_5$ and $|\operatorname{im}(\phi)| = |G| = 60$. Therefore $\operatorname{im}(\phi)$ has index 2 in S_5. By Theorem 32.13,

the unique subgroup of index 2 in S_5 is A_5, so $\text{im}(\phi) = A_5$. Since ϕ is injective, $G \cong A_5$. □

Proposition 33.2 The rotational symmetry group of the octahedron is isomorphic to S_4, and the rotational symmetry group of the icosahedron is isomorphic to A_5.

Proof. Rotations of a Platonic solid induce rotations of its dual, giving an isomorphism between their rotational symmetry groups. The octahedron is dual to the cube, so Proposition 31.2 implies that the octahedron has rotational symmetry group S_4. The icosahedron is dual to the dodecahedron, so Proposition 33.1 implies that the icosahedron has rotational symmetry group A_5. □

We have therefore identified the rotational symmetry groups of all five Platonic solids.

Platonic solid	Rotational symmetry group
Tetrahedron	A_4
Cube	S_4
Octahedron	S_4
Dodecahedron	A_5
Icosahedron	A_5

This raises the natural converse question: which finite groups occur as rotational symmetry groups in $\mathbb{R}^3$?

Definition 33.3 The **special orthogonal group** is

$$SO(3) = \{\mathbf{A} \in GL_3(\mathbb{R}) : \mathbf{A}^T\mathbf{A} = \mathbf{I} \text{ and } \det(\mathbf{A}) = 1\}.$$

Editorial Note The orthogonality condition $\mathbf{A}^T\mathbf{A} = \mathbf{I}$ is essential. Without it, the group is merely the special linear group $SL_3(\mathbb{R})$, which is much larger than $SO(3)$ and contains many more finite subgroups.

In other words, which finite groups are isomorphic to subgroups of $SO(3)$? We already know that A_4, S_4, and A_5 occur.

For $n = 2$, the group D_2 is isomorphic to

$$\{e, r, f_1, f_2\} \cong \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Geometrically, this group can be realized as a rotational symmetry group by taking the three nonidentity elements to be 180° rotations about three mutually perpendicular axes.

Fact 33.4 Every finite subgroup of $SO(3)$ is isomorphic to one of

$$A_4, \qquad A_5, \qquad S_4, \qquad D_n, \qquad \text{or} \qquad \mathbb{Z}_n$$

for some $n \geq 2$.

Finite Abelian Groups

We end the course by asking which finite abelian groups can occur.

Lecture 34 — Wednesday, December 02, 2015

Recall that if $|G| = 4$, then the abelian possibilities are $G \cong \mathbb{Z}_4$ and $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$. Also, if G is abelian and $|G| = pq$ for distinct primes p and q, then $G \cong \mathbb{Z}_{pq}$.

These examples suggest that finite abelian groups are assembled from cyclic pieces. The classification theorem below makes this precise and explains why prime powers are the natural building blocks.

Proposition 34.1 For positive integers n and m,

$$\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$$

if and only if $\gcd(n, m) = 1$.

Proof. The element $(1, 1) \in \mathbb{Z}_n \times \mathbb{Z}_m$ has order $\operatorname{lcm}(n, m)$. If $\gcd(n, m) = 1$, then this order is nm, so $\mathbb{Z}_n \times \mathbb{Z}_m$ is cyclic of order nm and is therefore isomorphic to $\mathbb{Z}_{nm}$.

Conversely, if $\mathbb{Z}_n \times \mathbb{Z}_m \cong \mathbb{Z}_{nm}$, then $\mathbb{Z}_n \times \mathbb{Z}_m$ has an element of order nm. The order of any

element (a, b) divides $\operatorname{lcm}(n, m)$, so nm divides $\operatorname{lcm}(n, m)$. Since $\operatorname{lcm}(n, m)$ divides nm, we get $\operatorname{lcm}(n, m) = nm$, and hence $\gcd(n, m) = 1$. □

The next question is whether every finite abelian group can be built as a direct product of cyclic groups.

The model for an internal direct product is the external product $G \times H$. Inside $G \times H$, define

$$\overline{G} = \{(g, e) : g \in G\} \qquad \text{and} \qquad \overline{H} = \{(e, h) : h \in H\}.$$

Then $\overline{G}, \overline{H} \trianglelefteq G \times H$ and $\overline{G} \cap \overline{H} = \{e\}$.

Proposition 34.2 Let G be finite, and let $H_1, H_2 \trianglelefteq G$. If $H_1 \cap H_2 = \{e\}$ and $|H_1|\,|H_2| = |G|$, then

$$G \cong H_1 \times H_2.$$

Proof. For $h_1 \in H_1$ and $h_2 \in H_2$, consider the commutator

$$c := h_1 h_2 h_1^{-1} h_2^{-1}.$$

Since $H_1 \trianglelefteq G$, we have $h_2 h_1 h_2^{-1} \in H_1$, so $c \in H_1$. Similarly, $c \in H_2$. Thus $c \in H_1 \cap H_2 = \{e\}$, so $h_1 h_2 = h_2 h_1$.

Define $\Phi : H_1 \times H_2 \to G$ by

$$\Phi(h_1, h_2) = h_1 h_2.$$

Because elements of H_1 commute with elements of H_2, the map Φ is a homomorphism. If $\Phi(h_1, h_2) = e$, then $h_1 = h_2^{-1} \in H_1 \cap H_2 = \{e\}$, so $h_1 = h_2 = e$. Hence Φ is injective.

Finally, the finite domain $H_1 \times H_2$ and codomain G have the same order by hypothesis. Since Φ is injective, it is therefore surjective as well. Hence $G \cong H_1 \times H_2$. □

Example 34.3 In the additive group $\mathbb{Z}_6$, the subgroups $\langle 3 \rangle$ and $\langle 2 \rangle$ satisfy

$$\mathbb{Z}_6 \cong \langle 3 \rangle \times \langle 2 \rangle \cong \mathbb{Z}_2 \times \mathbb{Z}_3.$$

By Proposition 34.1, this is also isomorphic to $\mathbb{Z}_6$.

Notation 34.4 The notation $\langle H_1, \ldots, H_k \rangle$ means the subgroup generated by $H_1 \cup \cdots \cup H_k$.

Corollary 34.5 Let G be finite, and let $H_1, \ldots, H_k \trianglelefteq G$. If

$$H_i \cap \langle H_1, \ldots, H_{i-1}, H_{i+1}, \ldots, H_k \rangle = \{e\}$$

for each i, and if $|H_1| \cdots |H_k| = |G|$, then

$$G \cong H_1 \times \cdots \times H_k.$$

Proof. For $j = 1, \ldots, k$, let $K_j := \langle H_1, \ldots, H_j \rangle$. Since each H_i is normal in G, each K_j is normal in G. For $j \geq 2$, we have

$$H_j \cap K_{j-1} = \{e\},$$

because $K_{j-1} \subseteq \langle H_1, \ldots, H_{j-1}, H_{j+1}, \ldots, H_k \rangle$. Hence

$$|K_j| = \frac{|K_{j-1}|\,|H_j|}{|K_{j-1} \cap H_j|} = |K_{j-1}|\,|H_j|.$$

Inductively, $|K_k| = |H_1| \cdots |H_k| = |G|$, so $K_k = G$.

If $i \neq j$, $a \in H_i$, and $b \in H_j$, then the commutator $aba^{-1}b^{-1}$ lies in both H_i and H_j, and therefore is e. Thus elements from distinct factors commute. Define

$$\Phi : H_1 \times \cdots \times H_k \to G, \quad \Phi(h_1, \ldots, h_k) = h_1 \cdots h_k.$$

The pairwise commutativity of different factors makes Φ a homomorphism, and surjectivity follows from $K_k = G$. For injectivity, suppose $\Phi(h_1, \ldots, h_k) = e$. Then

$$h_1 = (h_2 \cdots h_k)^{-1} \in H_1 \cap \langle H_2, \ldots, H_k \rangle = \{e\},$$

so $h_1 = e$. Cancelling and repeating gives $h_2 = \cdots = h_k = e$. Thus $\ker(\Phi) = \{e\}$, so Φ is injective. Therefore $G \cong H_1 \times \cdots \times H_k$. □

Example 34.6 In $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$, let

$$H_1 = \{(0,0,0), (1,0,0)\}, \qquad H_2 = \{(0,0,0), (0,1,0)\},$$
$$\text{and} \quad H_3 = \{(0,0,0), (0,0,1)\}.$$

Then

$$\langle H_1, H_2, H_3 \rangle = \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Theorem 34.7 (Classification of finite abelian groups) Let G be a finite abelian group. Then

$$G \cong \mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}}$$

for primes p_i and integers $n_i \geq 1$. Furthermore, this decomposition is unique up to permutation of the factors. That is,

$$\mathbb{Z}_{q_1^{m_1}} \times \cdots \times \mathbb{Z}_{q_k^{m_k}} \cong \mathbb{Z}_{r_1^{s_1}} \times \cdots \times \mathbb{Z}_{r_\ell^{s_\ell}}$$

if and only if $k = \ell$ and there is a permutation $\sigma \in S_k$ such that

$$q_i = r_{\sigma(i)} \qquad \text{and} \qquad m_i = s_{\sigma(i)}$$

for each $i = 1, \ldots, k$.

Proof sketch. The proof proceeds as follows.

1. Write $|G| = p_1^{a_1} \cdots p_n^{a_n}$ with $p_i \neq p_j$ when $i \neq j$. Define

   $$G_i = \{g \in G : g^{p_i^{a_i}} = e\}.$$

   Then $G_i \leq G$ and $|G_i| = p_i^{a_i}$.
2. Show that $G \cong G_1 \times \cdots \times G_n$.
3. Show that each G_i is isomorphic to a product of cyclic groups of p_i-power order:

   $$G_i \cong \mathbb{Z}_{p_i^{b_1}} \times \cdots \times \mathbb{Z}_{p_i^{b_m}}.$$

   This is the hard part of the proof.
4. Conclude the existence statement by combining the decompositions of the G_i.
5. Prove the uniqueness statement.

□

Example 34.8 If G is a finite abelian group of order 27, then

$$G \cong \mathbb{Z}_{27}, \qquad G \cong \mathbb{Z}_9 \times \mathbb{Z}_3, \qquad \text{or} \qquad G \cong \mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3.$$

Example 34.9 If G is a finite abelian group of order

$$36 = 2^2 \cdot 3^2,$$

then G is isomorphic to one of

$$\mathbb{Z}_{2^2} \times \mathbb{Z}_{3^2}, \qquad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_{3^2}, \qquad \mathbb{Z}_{2^2} \times \mathbb{Z}_3 \times \mathbb{Z}_3, \qquad \text{or} \qquad \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_3.$$

The cyclic group $\mathbb{Z}_{36}$ appears in the first case, since Proposition 34.1 gives

$$\mathbb{Z}_{2^2} \times \mathbb{Z}_{3^2} \cong \mathbb{Z}_{4 \cdot 9} = \mathbb{Z}_{36}.$$

Example 34.10 The group $\mathbb{Z}_{40} \times \mathbb{Z}_{15}$ is abelian, and the classification theorem rewrites it as

$$\begin{aligned} \mathbb{Z}_{40} \times \mathbb{Z}_{15} &= \mathbb{Z}_{2^3 \cdot 5} \times \mathbb{Z}_{3 \cdot 5} \\ &\cong \mathbb{Z}_{2^3} \times \mathbb{Z}_5 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \\ &\cong \mathbb{Z}_{120} \times \mathbb{Z}_5. \end{aligned}$$

If G and H have different numbers of elements of order k for some k, then $G \ncong H$. The converse is not true in general.

Example 34.11 The groups $Q_8 \times \mathbb{Z}_2$ and $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ are not isomorphic. The test based on element orders above does not fully classify arbitrary finite groups, but it does classify finite abelian groups.

Example 34.12 Write down all finite abelian groups. Prove, without using Theorem 34.7, that if G is a group with $|G| = 8$ and $g^2 = e$ for every $g \in G$, then

$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

Solution. By Theorem 34.7, the finite abelian groups are exactly the finite direct products of

cyclic groups whose orders are prime powers:

$$\mathbb{Z}_{p_1^{n_1}} \times \cdots \times \mathbb{Z}_{p_k^{n_k}}.$$

Now suppose $|G| = 8$ and $g^2 = e$ for every $g \in G$. Then for any $a, b \in G$,

$$e = (ab)^2 = abab.$$

Multiplying on the left by a and on the right by b gives $ba = ab$, so G is abelian.

Choose $a \neq e$. Then $\langle a \rangle = \{e, a\}$ has order 2. Choose $b \notin \langle a \rangle$. Since every element has square e, the four elements

$$e,\ a,\ b,\ ab$$

are distinct, so they form a subgroup of order 4. Choose $c \notin \{e, a, b, ab\}$. Then the eight elements

$$e,\ a,\ b,\ c,\ ab,\ ac,\ bc,\ abc$$

are distinct: any equality between two of them would force one of a, b, or c to lie in the subgroup generated by the other two, contrary to the choice of b and c. Since $|G| = 8$, these are all the elements of G.

Define

$$\phi : \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2 \to G$$

by

$$\phi(i, j, k) = a^i b^j c^k.$$

Because G is abelian and every element has order 2, this is a homomorphism. Its image contains all eight elements listed above, so it is surjective. Since the domain also has 8 elements, ϕ is bijective. Therefore

$$G \cong \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2.$$

□

Lecture 35 — Friday, December 04, 2015

Banach–Tarski Paradox

The **Banach–Tarski paradox** says, roughly, that a ball in $\mathbb{R}^3$ can be cut into finitely many pieces and then rearranged by rigid motions to form two balls congruent to the original. Figure 18 gives a deliberately schematic picture of the claim.

A cartoon of the Banach–Tarski paradox

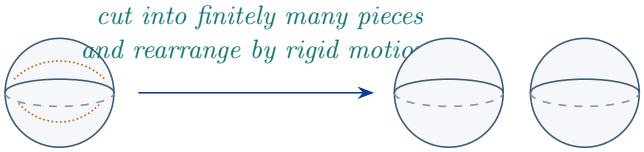


FIGURE 18

The **free group** F_2 consists of reduced words in the alphabet

$$\{a, a^{-1}, b, b^{-1}\},$$

with operation given by concatenation followed by cancellation. For example,

$$(aba)(bab) = ababab.$$

Let

$$S(a) = \{\text{reduced words beginning with } a\}.$$

Similarly define $S(a^{-1})$, $S(b)$, and $S(b^{-1})$. Then

$$F_2 = \{e\} \cup S(a) \cup S(a^{-1}) \cup S(b) \cup S(b^{-1}).$$

Also,

$$F_2 = aS(a^{-1}) \cup S(a) \qquad \text{and} \qquad F_2 = bS(b^{-1}) \cup S(b).$$

This is a paradoxical decomposition. The Banach–Tarski paradox is a consequence of the axiom of choice.

Low-Dimensional Topology

A **2-manifold** is a space that looks locally like $\mathbb{R}^2$. Such spaces come with a group invariant called the **fundamental group**. To define it, choose a basepoint and consider loops starting and ending at that point. The operation is concatenation of loops, and two loops represent the same element if one can be continuously deformed into the other while keeping the basepoint fixed.

Notation 35.1 The notation $\pi_1(X)$ denotes the fundamental group of X.

The loop pictures in Figure 19 compare the torus, concatenation, and the sphere.

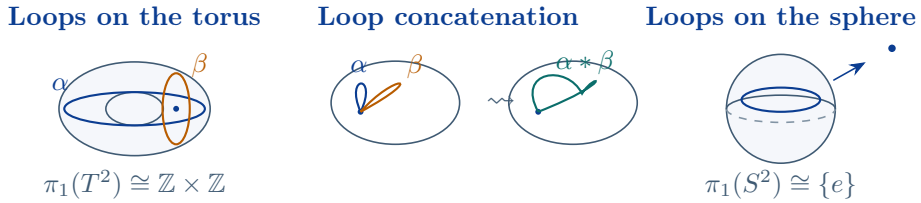


FIGURE 19

For the torus T^2 and the sphere S^2, we have

$$\pi_1(T^2) \cong \mathbb{Z} \times \mathbb{Z}, \qquad \text{and} \qquad \pi_1(S^2) \cong \{e\}.$$

Question 35.2 Is the torus homeomorphic to the sphere?

They are not homeomorphic, and the fundamental group gives a rigorous obstruction: their fundamental groups are not isomorphic.

A 3-manifold is a space that looks locally like $\mathbb{R}^3$. The group $\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$ is generated by

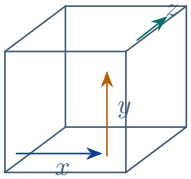
$$\{(1,0,0),(0,1,0),(0,0,1)\},$$

and

$$\mathbb{Z} \times \mathbb{Z} \times \mathbb{Z} \cong \pi_1(S^1 \times S^1 \times S^1).$$

Figure 20 shows the three independent loop directions geometrically.

The 3-torus as $S^1 \times S^1 \times S^1$



$\pi_1(S^1 \times S^1 \times S^1)$ has three independent loop directions, so $\pi_1(S^1 \times S^1 \times S^1) \cong \mathbb{Z}^3$.

FIGURE 20

Fact 35.3 Let

$$S^n = \{x \in \mathbb{R}^{n+1} : \|x\| = 1\}.$$

For $n \geq 2$, we have $\pi_1(S^n) \cong \{e\}$.

Question 35.4 (Poincaré conjecture) Is every closed 3-manifold X with $\pi_1(X) \cong \{e\}$ homeomorphic to S^3?

The answer is yes, by Perelman's 2003 proof of the Poincaré conjecture.

Groups that are also manifolds in a compatible way are called **Lie groups**. The torus $S^1 \times S^1$ is a Lie group. The spheres $S^0 \cong \mathbb{Z}_2$, S^1, and S^3 are Lie groups; the group structure on S^3 comes from the unit quaternions, with Q_8 sitting inside it. These are the only spheres that are Lie groups, a fact related to **de Rham cohomology**.

Appendix: Lecture and Tutorial Index

1. Lecture 1 — Monday, September 14, 2015
2. Lecture 2 — Wednesday, September 16, 2015
3. Lecture 3 — Friday, September 18, 2015
4. Lecture 4 — Monday, September 21, 2015
5. Lecture 5 — Wednesday, September 23, 2015
6. Lecture 6 — Friday, September 25, 2015
7. Lecture 7 — Monday, September 28, 2015
8. Lecture 8 — Wednesday, September 30, 2015
9. Lecture 9 — Friday, October 02, 2015
10. Lecture 10 — Monday, October 05, 2015
11. Lecture 11 — Wednesday, October 07, 2015
12. Lecture 12 — Friday, October 09, 2015
13. Lecture 13 — Wednesday, October 14, 2015
14. Lecture 14 — Friday, October 16, 2015
15. Lecture 15 — Monday, October 19, 2015
16. Lecture 16 — Wednesday, October 21, 2015
17. Lecture 17 — Friday, October 23, 2015
18. Lecture 18 — Monday, October 26, 2015
19. Lecture 19 — Wednesday, October 28, 2015
20. Lecture 20 — Friday, October 30, 2015
21. Lecture 21 — Monday, November 02, 2015
22. Lecture 22 — Wednesday, November 04, 2015
23. Lecture 23 — Friday, November 06, 2015
24. Lecture 24 — Monday, November 09, 2015
25. Lecture 25 — Wednesday, November 11, 2015
26. Lecture 26 — Friday, November 13, 2015

27. Lecture 27 — Monday, November 16, 2015
28. Lecture 28 — Wednesday, November 18, 2015
29. Lecture 29 — Friday, November 20, 2015
30. Lecture 30 — Monday, November 23, 2015
31. Lecture 31 — Wednesday, November 25, 2015
32. Lecture 32 — Friday, November 27, 2015
33. Lecture 33 — Monday, November 30, 2015
34. Lecture 34 — Wednesday, December 02, 2015
35. Lecture 35 — Friday, December 04, 2015