MATH 546, SPRING 2023

CONTENTS

1. Introductory remarks about the course.

Here are some preliminary remarks about the course.

(1) My name is Professor Kustin. (My last name rhymes with "Justin".)
(2) Be sure to look at the class website often. If you don't know the address, send an e-mail to me at kustin@math.sc.edu
(3) Quiz 1 on Wednesday, January 18 is one of the assigned HW problems from 1–6.
(4) The list of assigned HW is on my website. (I might add to the list or tinker with it, but, mainly my intention is to leave it alone and merely assign problems from it.)
(5) There is no textbook for the course. I will put class notes on the website. Use them however you like. (Maybe you want to read them before I give the lecture. Maybe you want to read them after you have heard the lecture. At any rate, if you miss class be sure to study them.) I have put the Homework assignments on the website. If you feel you want a book, I suggest the one by Beachy and Blair. I have used it a number of times. To some extent, I follow it. I have taken some homework problems from it. On the other hand, I skip the first 100 pages or so. I start with the definition of a group (which is in Chapter 3). There are some notational things in Beachy and Blair that irritate me. Also, when I first used Beachy and Blair, it was inexpensive; in the mean time, it has become more expensive.
(6) There will be an Exam or Quiz essentially every Wednesday. (The exact dates can be found on the syllabus which is on the website.) The exams and quizzes will be given at the end of class. When you finish your quiz or exam, **take a picture of your solution for your records** and give me your answers. I will send my comments back by way of e-mail. In general, I won't return papers.
(7) If you miss an exam or quiz or do poorly on an exam or quiz; don't worry about it. There will be plenty more chances for you to demonstrate competence. Be sure to learn how to do missed or wrong problem correctly. I'll surely ask about it again.
(8) To make the class work, please do the following.
    (a) Master every lecture.
    (b) Do every homework problem. I expect you to do the homework. Figure out proofs on your own. It serves very little purpose if you read the proof somewhere or if you wait for me to do it in class.
    (c) Ask questions. There are many ways to ask questions: raise your hand in class, send me an e-mail, leave me a note (either in my office or at the front of the classroom), etc. Do whatever works for you.
    (d) Learn from your mistakes.

(e) Don't give up.

(9) I assume that all of you have taken and done well in Math 300 and Math 544. Almost all of the problems in this course require you to prove a statement, or give an example, or make a calculation that has some theoretical content.

(10) **Learn every definition.** Learn the official definition (because that is what one uses to prove things). Also learn the intuitive idea behind each concept (because we are human beings and not robots).

(11) Similarly, learn the correct and complete statement of every theorem.

(12) Write precise and complete thoughts in complete sentences.

2. MATH 546 IS THE STUDY OF GROUPS.

Definition 2.1. A group $(G,*)$ is a set G together with one binary operation $*$, which satisfy the following properties.

(1) The group G is closed under the operation $*$. (If g_1 and g_2 are elements of G, then $g_1 * g_2$ is an element of G.)
(2) The operation $*$ associates. (If g_1, g_2, and g_3 are in G, then $g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$.)
(3) The group G has an identity element. (There exists an element $\mathrm{id} \in G$ with $g * \mathrm{id} = g$ and $\mathrm{id} * g = g$ for all $g \in G$.)
(4) Every element of G has an inverse. (If $g \in G$, then there is an element h in G with $g * h = \mathrm{id}$ and $h * g = \mathrm{id}$.)

If the operation $*$ also satisfies commutativity (that is, $g_1 * g_2 = g_2 * g_1$ for all g_1 and g_2 in G), then G is called an Abelian group.

2.2. Some of the examples I want to give involve fields. I do not want to define field at this time. Instead, I will remind you that some of our favorite fields are

- the field of rational numbers
$$(\mathbb{Q}, +, \times) = \{\tfrac{a}{b} \mid a \text{ and } b \text{ are integers with } b \neq 0\},$$
- the field of of real numbers $(\mathbb{R}, +, \times)$, and
- the field of complex numbers $(\mathbb{C}, +, \times)$, where
$$\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R} \text{ and } i^2 = -1\}.$$

2.A. **Examples of Groups.**

Examples 2.3. Here are some examples of groups.

Ex. 1. Let $\boldsymbol{k}$ be a field and n be a positive integer. Let $\mathrm{GL}_n(\boldsymbol{k})$ be the group[1] of invertible $n \times n$ matrices with entries from $\boldsymbol{k}$. The operation in $\mathrm{GL}(\boldsymbol{k})$ is matrix multiplication.

Notice that the product of two invertible matrices is invertible. (So, $\mathrm{GL}_n(\boldsymbol{k})$ is closed.)

Notice that the identity matrix (which has ones on the main diagonal and zeros elsewhere) is an identity element of $\mathrm{GL}_n(\boldsymbol{k})$.

You probably proved in Math 544 that matrix multiplication associates. (I want you to do a small special case of this as a homework problem).

Every invertible matrix has an inverse.

• Eventually, you will learn that every finite group G is a subgroup of $\mathrm{GL}_n(\boldsymbol{k})$ for some n and some $\boldsymbol{k}$. (I make a further comment about this in the next example.)

[1] "GL" stands for General Linear group.

Ex. 2. Let T be a set and $\mathrm{Sym}(T)$ be[2] the set of invertible functions $f : T \to T$. The operation in $\mathrm{Sym}(T)$ is composition.

One element of $\mathrm{Sym}(T)$ is $\mathrm{id} : T \to T$ with $\mathrm{id}(t) = t$ for all $t \in T$. Of course, this is the identity element of $\mathrm{Sym}(T)$.

The composition of two invertible functions is an invertible function; so T is closed.

Every invertible function has an inverse.

Function composition ALWAYS associates!! Indeed,

$$(f \circ (g \circ h))(x) \quad \text{and} \quad ((f \circ g) \circ h)(x)$$

both always[3] mean

$$f(g(h(x))).$$

• Eventually you will learn that every group is a subgroup of $\mathrm{Sym}(T)$ for some set T. (This is called Cayley's theorem.[4])

• If $T = \{1, 2, 3, \ldots, n\}$, then one usually writes S_n instead of $\mathrm{Sym}(T)$.

• At the end of the course we will write various notations for the elements of S_n. We could do that now, but I would much rather prove Theorems about groups than discuss the arithmetic of permutations.

For now I propose the "two-line" notation for describing permutations Let σ and τ be the following elements of S_3:

$$\sigma(1) = 2, \quad \sigma(2) = 1, \quad \sigma(3) = 3, \quad \text{and}$$

$$\tau(1) = 2, \quad \tau(2) = 3, \quad \tau(3) = 1.$$

If f is an element of S_3, then one relatively convenient way to record f is in the form

$$\begin{pmatrix} 1 & 2 & 3 \\ f(1) & f(2) & f(3) \end{pmatrix}.$$

If one uses this notation, then

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \quad \text{and} \quad \tau = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Furthermore, $\sigma \circ \tau$ is

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$$

[2] $\mathrm{Sym}(T)$ is called the symmetric group on T or the group of permutations of T. (I suppose one could call $\mathrm{Sym}(T)$ the the group of symmetries of T.)

[3] This is why association is a natural hypotheses in many algebraic situations.

[4] Once you know Cayley's Theorem, then you can easily show that every finite group is a subgroup of $\mathrm{GL}_n \boldsymbol{k}$. You need only show that $\mathrm{Sym}(\{1, 2, 3, \ldots, n\})$ is a subgroup of $\mathrm{GL}_n \boldsymbol{k}$. Can you do that?

because

$$1 \xrightarrow{\tau} 2 \xrightarrow{\sigma} 1$$
$$2 \xrightarrow{\tau} 3 \xrightarrow{\sigma} 3$$
$$3 \xrightarrow{\tau} 1 \xrightarrow{\sigma} 2$$

Ex. 3. $(\mathbb{Z},+)$, $(\mathbb{Q},+)$, $(\mathbb{R},+)$, $(\mathbb{C},+)$ all are Abelian groups.

Ex. 4. $(\mathbb{Q}\setminus\{0\},\times)$, $(\mathbb{R}\setminus\{0\},\times)$, $(\mathbb{C}\setminus\{0\},\times)$ all are Abelian groups.

Ex. 5. $(\mathbb{Z}\setminus\{0\},\times)$ is not a group.

Ex. 6. Let $\mathrm{Mat}_{2\times 2}\mathbb{Z}$ be the set of 2×2 matrices. Observe that $(\mathrm{Mat}_{2\times 2}\mathbb{Z},+)$ is an Abelian group, where $+$ means addition of matrices.

Ex. 7. $(\mathrm{Mat}_{2\times 2}\mathbb{Z},\times)$ is not a group.

Ex. 8. Let $\mathrm{SL}_2(\mathbb{Z}) = \{A \in \mathrm{Mat}_{2\times 2}\mathbb{Z} \mid \det A = 1\}$. Observe that $(\mathrm{SL}_2(\mathbb{Z}),\times)$ is a group, where $\times$ means matrix multiplication.

Ex. 9. (My main source for the discussion of rigid motions is the book by Artin [1].) A function $f:\mathbb{R}^2\to\mathbb{R}^2$ is called a rigid motion (or an isometry) if f preserves distance. (That is the distance between $f(P_1)$ and $f(P_2)$ is the same as the distance between P_1 and P_2 for all points P_1 and P_2 on the plane $\mathbb{R}^2$. Measure distance the usual way. If $P_i = (x_i, y_i)$, then the distance between P_1 and P_2 is $\sqrt{(x_2-x_1)^2+(y_2-y_1)^2}$.)

Notice that every rigid motion is an invertible function. Let f be a rigid motion. It is clear that f is one-to-one. If P_1 and P_2 are different elements of $\mathbb{R}^2$, then the distance between them is not zero; so the distance between $f(P_1)$ and $f(P_2)$ is not zero. Thus, $f(P_1)\neq f(P_2)$.

It takes a little more effort to see that f is onto.

First we show that f preserves angle. If P, Q and R are three points in the plane then $f(P)$, $f(Q)$, and $f(R)$ are three points in the plane and the sides of the triangle with vertices P, Q, and R have the same lengths as the triangle with vertices $f(P)$, $f(Q)$, and $f(R)$. Consequently, the two triangles are congruent and the corresponding angles are equal.

Let P be an arbitrary point in the plane. The points $f(0,0)$, $f(1,0)$ and $f(0,1)$ form a right angle in the plane; so there are numbers a and b so that P, $f(0,0)$ $f(a,0)$ and $f(0,b)$ form a rectangle. Observe that P and $f(a,b)$ are the only points with distance $|b|$ from $f(a,0)$, $|a|$ from $f(0,b)$ and $\sqrt{a^2+b^2}$ from $f(0,0)$. Conclude that P must equal $f(a,b)$.

Let $\mathscr{G}$ be the group of rigid motions of the plane. The operation in $\mathscr{G}$ is composition. Some elements in $\mathscr{G}$ are

- Fix a point P in the plane and rotate the plane by the angle θ.
- Fix a line in the plane and reflect the plane across the line.
- Fix a point (x_0,y_0) in the plane and translate the plane by (x_0,y_0). That is $f(x,y) = (x+x_0, y+y_0)$.

Here is an example. Let ρ be rotation of the plane counterclockwise by 90 degrees fixing the origin. Let σ be reflection of the plane across the x-axis. Let D_4 be[5] the smallest subgroup of $\mathscr{G}$ which contains σ and ρ.

Questions. (9a) What does $\sigma\rho$ do?
(9b) How many elements are in D_4? (Did you list every element? Are all of the elements on your list different?)
(9c) What do the elements of D_4 do to $A = (1,0)$, $B = (0,1)$, $C = (-1,0)$, $D = (0,-1)$?
(9d) What do the elements of D_4 do to the square with vertices A, B, C, D?
(9e) Give a geometric description of every element of D_4.
(9f) Record the multiplication table for D_4.
(9g) Notice that $\{\mathrm{id}, \rho^2, \sigma, \sigma\rho^2\}$ is a subgroup of D_4.

Answers. (9a) To focus our thinking, maybe we should ask what $\sigma\rho$ does to A, B, C, D, and to the square with vertices A, B, C, and D.

$$\begin{aligned} A &\xrightarrow{\rho} B \xrightarrow{\sigma} D \\ B &\xrightarrow{\rho} C \xrightarrow{\sigma} C \\ C &\xrightarrow{\rho} D \xrightarrow{\sigma} B \\ D &\xrightarrow{\rho} A \xrightarrow{\sigma} A \end{aligned}$$

We see that $\sigma \circ \rho$ is reflection[6] across $y = -x$.
(9b) We know $\rho^4 = \mathrm{id}$, $\sigma^2 = \mathrm{id}$, and $\sigma\rho$ is a reflection; so $(\sigma\rho)^2 = \mathrm{id}$; that is

$$\sigma\rho\sigma\rho = \mathrm{id}\,.$$

Multiply on the left by σ:

$$\rho\sigma\rho = \sigma.$$

Multiply on the right by ρ^3:

$$\rho\sigma = \sigma\rho^3.$$

Conclude that every element of D_4 has the form

$$\sigma^i\rho^j \text{ with } i \in \{0,1\} \text{ and } j \in \{0,1,2,3\}. \tag{2.3.1}$$

[5]The group D_4 is called a Dihedral group.

[6]Possibly you are perfectly happy studying the problem point by point and guessing the answer. Possibly, you would rather have something that looks more official. In the second case, maybe you know that rotation counterclockwise by θ is the linear transformation $\begin{bmatrix} x \\ y \end{bmatrix} \mapsto \begin{bmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$ and reflection of the xy-plane across the line through the origin with angle θ is the linear transformation $\begin{bmatrix} x \\ y \end{bmatrix} \mapsto \begin{bmatrix} \cos 2\theta & \sin 2\theta \\ \sin 2\theta & -\cos 2\theta \end{bmatrix} \begin{bmatrix} x \\ y \end{bmatrix}$. You are welcome to use the matrices if you know and understand them. The intuitive approach is also fine.

Thus D_4 has at most 8 elements. One must still show that the eight elements of (2.3.1) are different.

One should answer (9b), (9c), and (9d) at the right pace. I'll just jump to (9e)

(9e)

element	action
id	identity
ρ	rotation by 90 degrees
ρ^2	rotation by 180 degrees
ρ^3	rotation by 270 degrees
σ	reflection across the x-axis
$\sigma\rho$	reflection across $y = -x$
$\sigma\rho^2$	reflection across the y-axis
$\sigma\rho^3$	reflection across the $y = x$

(9f)

	id	ρ	ρ^2	ρ^3	σ	$\sigma\rho$	$\sigma\rho^2$	$\sigma\rho^3$
id	id	ρ	ρ^2	ρ^3	σ	$\sigma\rho$	$\sigma\rho^2$	$\sigma\rho^3$
ρ	ρ	ρ^2	ρ^3	id	$\sigma\rho^3$	σ	$\sigma\rho$	$\sigma\rho^2$
ρ^2	ρ^2	ρ^3	id	ρ	$\sigma\rho^2$	$\sigma\rho^3$	σ	$\sigma\rho$
ρ^3	ρ^3	id	ρ	ρ^2	$\sigma\rho$	$\sigma\rho^2$	$\sigma\rho^3$	σ
σ	σ	$\sigma\rho$	$\sigma\rho^2$	$\sigma\rho^3$	id	ρ	ρ^2	ρ^3
$\sigma\rho$	$\sigma\rho$	$\sigma\rho^2$	$\sigma\rho^3$	σ	ρ^3	id	ρ	ρ^2
$\sigma\rho^2$	$\sigma\rho^2$	$\sigma\rho^3$	σ	$\sigma\rho$	ρ^2	ρ^3	id	ρ
$\sigma\rho^3$	$\sigma\rho^3$	σ	$\sigma\rho$	$\sigma\rho^2$	ρ	ρ^2	ρ^3	id

(9g) To see that $\{\mathrm{id}, \rho^2, \sigma, \sigma\rho^2\}$ is a subgroup of D_4 we need only check that this set is closed under composition. This is clear. Every element squares to the identity. If a, b, c are the non-identity elements then $ab = c$. All groups with four elements in which every element squares to the identity and the product of any two non-identity elements is the third non-identity element is called a Klein 4-group. The name honors Felix Klein.[7]

Ex. 10. Fix a positive integer n. Let ρ be the element of $\mathscr{G}$ which fixes the origin and rotates the plane counterclockwise by $\frac{2\pi}{n}$. Let Rot_n be the smallest subgroup[8] of $\mathscr{G}$ which contains ρ. The elements of G are $\mathrm{id}, \rho, \rho^2, \ldots, \rho^{n-1}$. Notice that $\rho^n = \mathrm{id}$ and

$$\rho^{j+an} = \rho^j$$

for all integers j and a.

[7] We will talk about the Klein bottle latter.

[8] If S is a subset of a group G, then the smallest subgroup of G which contains S is denoted $\langle S \rangle$. The subgroup $\langle S \rangle$ is called the subgroup of G generated by S.

2.B. **A short discussion of cyclic groups, the order of a group, the order of an element, and the subgroup of the group G generated by the set of elements S.**

Definition 2.4. Let G be a group. If there is an element $g \in G$ with every element of G equal to g^i for some[9] integer i, then G is called a cyclic group.

Example 2.5. If ρ is the rigid motion which fixes the origin and rotates the plane by $\frac{2\pi}{n}$ (counterclockwise), then the subgroup $\langle\rho\rangle$ of $\mathscr{G}$ is a cyclic group of order n.

(Please make sure you know what $\langle\ \rangle$ means and both meanings of the word order.)

Questions 2.6. (10a) Give an example of an infinite cyclic group.
(10b) What is the smallest non-cyclic group that we know?

Answers 2.7. (a) The group $(\mathbb{Z},+)$ and the subgroup of $(\mathbb{Q}\setminus\{0\},\times)$ generated by 2 both are infinite cyclic groups.

(b) The Klein four group is a small non-cyclic group. It is clear that every group with one element or two elements is cyclic. You can prove that every group with three elements IS cyclic (but it will be much easier once you know Lagrange's Theorem). Let G be a group with three distinct elements id, a, b. Observe ab can not equal a because, if $ab = a$, then b MUST be the identity element. Similarly if $ab = b$, then a MUST be the identity element. Thus, $ab = \mathrm{id}$.

Maybe this is enough to show that G is cyclic; but we can also calculate the exact value of a^2. Indeed, if $a^2 = a$, then we multiply both sides on the right by b to learn $a = \mathrm{id}$, which is not possible because a, b, id are distinct. If $a^2 = \mathrm{id}$, then multiply both sides on the right by b to learn $a = b$, which is also not possible. Thus, a^2 MUST be b. We have proven that every group with 3 elements is cyclic. (Lagrange's Theorem gives an easier proof.)

Continue with the Examples.

Ex. 11. Let n be a positive integer and $U_n = \{z \in \mathbb{C} \mid z^n = 1\}$. Observe the U_n is a group[10] under multiplication. Indeed, U_n is closed under multiplication. If $z \in U_n$, then z^{n-1} is also in U_n and z times z^{n-1} is equal to 1. Thus every element of U_n has an inverse.

So the question is: What is the multiplication in U_n? Is U_n a new group or is U_n essentially the same as an old group?

Here are the first few U_n's:

$$U_1 = \{1\}$$

[9] If $i = 0$ and g is an element of a group G, then g^0 means id; if $i = -1$, then g^{-1} means the inverse of g. If i is a positive integer, then g^{-i} means (the inverse of g)^i.

[10] The group U_n is called the group of n-th roots of one.

$$\begin{aligned}
U_2 &= \{-1,1\}\\
U_3 &= \{\cos\tfrac{2\pi}{3}+i\sin\tfrac{2\pi}{3},\cos\tfrac{4\pi}{3}+i\sin\tfrac{4\pi}{3},1\}\\
&= \{-\tfrac{1}{2}+\tfrac{\sqrt{3}}{2}i,-\tfrac{1}{2}-\tfrac{\sqrt{3}}{2}i,1\}\\
U_4 &= \{i,-1,-i,1\}\\
U_n &= \{\cos\tfrac{2\pi k}{n}+i\sin\tfrac{2\pi k}{n} \mid 0\le k\le n-1\}\\
&= \{e^{\frac{2k\pi}{n}} \mid 0\le k\le n-1\}.
\end{aligned}$$

I will draw a few of the groups U_n on the complex plane (where the horizontal axis is the number line for $\mathbb{R}$ and the vertical axis is the number line for $i\mathbb{R}$.) I will show Euler's argument for why

$$e^{i\theta} = \cos\theta + i\sin\theta.$$

We use Taylor's series to see this:

$$\begin{aligned}
e^z &= 1+z+\frac{z^2}{2!}+\frac{z^3}{3!}+\frac{z^4}{4!}+\frac{z^5}{5!}+\dots,\\
\cos(z) &= 1-\frac{z^2}{2!}+\frac{z^4}{4!}-\dots,\\
\sin(z) &= z-\frac{z^3}{3!}+\frac{z^5}{5!}+\dots,
\end{aligned}$$

for all complex numbers z. It follows that

$$\begin{aligned}
e^{i\theta} &= 1+(i\theta)+\frac{(i\theta)^2}{2!}+\frac{(i\theta)^3}{3!}+\frac{(i\theta)^4}{4!}+\frac{(i\theta)^5}{5!}+\dots\\
&= 1-\frac{\theta^2}{2!}+\frac{\theta^4}{4!}-\dots+i\left(\theta-\frac{\theta^3}{3!}+\frac{\theta^5}{5!}-\dots\right)\\
&= \cos\theta+i\sin\theta.
\end{aligned}$$

We see that U_n is a cyclic group of order[11] n. Later, when we have enough language, we will prove that the group U_n of n-th roots of is isomorphic to the rotation group Rot_n.

Ex. 12. Here is one more example of a group. Let

$$U = \{z = a+bi \in (\mathbb{C}\setminus\{0\},\times) \mid a^2+b^2 = 1\}.$$

We call U the unit circle group. Of course, U is equal to

$$\{e^{i\theta} \mid \theta\in\mathbb{R}\}.$$

This ends the list of examples which started on with Examples 2.3 on page 4.

[11] The order of a group is the number of elements in the group. The order of an element g in a group G is the order of the subgroup $\langle g\rangle$ in G. Notice that if the element g has finite order, then the order of g is the least positive integer exponent m with $g^m = \mathrm{id}$.

2.C. **Three elementary properties of groups.**

(1) If G is a group, then the identity element of G is unique.
(2) If G is a group and a is an element of G, then the inverse of a is unique.
(3) If G is a group and a is an element of G, then the inverse of the inverse of a is a.

Proof. (1) Suppose id and id' both are identity elements for $(G,*)$, then

$$\mathrm{id} = \mathrm{id} * \mathrm{id}' = \mathrm{id}'.$$

The left equality holds because id' is an identity element for G; hence, $a = a * \mathrm{id}'$ for all a in G. The right equality holds because id is an identity element for G; hence, $\mathrm{id} * b = b$ for all $b \in G$. At any rate $\mathrm{id} = \mathrm{id}'$.

(2) Suppose b and c both are inverses of a. Then

$$b = b * \mathrm{id} = b * (a * c) = (b * a) * c = \mathrm{id} * c = c.$$

The left most equality holds because id is the identity element of G. The second equality hold because c is an inverse of a. The next equality holds because the operation $*$ is associative. The second from the right equality holds because b is an inverse of a. The right most equality holds because id is the identity element of G.

At any rate, $b = c$.

(3) Suppose b is the inverse of a and c is the inverse of b. We will show that $c = a$. Observe that

$$a =_1 \mathrm{id} * a =_2 (c * b) * a =_3 c * (b * a) =_4 c * \mathrm{id} =_5 c.$$

The equality $=_1$ holds because id is the identity element of G. The equality $=_2$ holds because c is the inverse of b. The equality $=_3$ holds because the operation * associates. The equality $=_4$ holds because b is the inverse of a; and $=_6$ holds because id is the identity element of G.

At any rate, $c = a$ and the proof is complete. □

3. Lagrange's Theorem and left cosets.

Lagrange's Theorem is a labor saving device.

Once you know Lagrange's Theorem, then you automatically know that all groups with 2, 3, 5 ,7 elements are Abelian.

Once you know Lagrange's Theorem, then you automatically know that every subgroup of S_4 has 1, 2, 3, 4, 6, 8, 12, or 24 elements. This fact is helpful if you want to find the order of a particular subgroup of S_4. This fact is helpful if you are trying to show that a particular subgroup of S_4 is all of S_4. You don't have to demonstrate that all 24 elements of S_4 are in your subgroup. It suffices to demonstrate that 13 elements of S_4 are in the subgroup (as on HW 1.c).

Theorem 3.1. [Lagrange's Theorem] *Let G be a finite group and H be a subgroup of G. Then the number of elements in H divides the number of elements*[12] *of G.*

Corollary 3.2. *If g is an element of the finite group G, then the order*[13] *of g divides the order*[14] *of G.*

Corollary 3.3. *If G is a group with n elements and $g \in G$, then $g^n = \mathrm{id}$.*

Corollary 3.4. *If G is a finite group of prime order, then G is a cyclic group and every element of G, other than the identity element, generates*[15] *G.*

Question 3.5. *Consider Homework Question* 1.(c). *What is the subgroup of S_4 generated by $\{\sigma, \tau\}$? Give a complete answer. You may use Lagrange's Theorem.*

One uses left cosets to prove Lagrange's Theorem.

Definition 3.6. Let H be a subgroup of the group $(G, *)$ and let g be an element of G. Then the left coset of H in G determined by g is

$$g * H = \{g * h \mid h \in H\}.$$

Example 3.7. Find the left cosets of $H = \{\mathrm{id}, \sigma\}$ in $G = D_3$.

Recall from Homework that $D_3 = \{\mathrm{id}, \rho, \rho^2, \sigma, \sigma \circ \rho, \sigma \circ \rho^2\}$. The operation in D_3 is completely determined by $\sigma^2 = \mathrm{id}$, $\rho^3 = \mathrm{id}$, $\rho\sigma = \sigma\rho^2$.

---

[12] Recall that the number of elements in the group G is also known as the order of G.

[13] Recall that the order of g is the least positive power n with $g^n = \mathrm{id}$. The order of g is also equal to the number of elements in $\langle g \rangle$.

[14] Recall that the order of the group G is the number of elements in G.

[15] Let S be a subset of the group G. Recall that the subgroup of G generated by S is the smallest subgroup of G which contains S.

Answer 3.8. We see that

$$\begin{aligned}
\mathrm{id} * H &= \{\mathrm{id} * \mathrm{id}, \mathrm{id} * \sigma\} = \{\mathrm{id}, \sigma\} = H, \\
\sigma * H &= \{\sigma * \mathrm{id}, \sigma * \sigma\} = \{\sigma, \mathrm{id}\} = H, \\
\rho * H &= \{\rho * \mathrm{id}, \rho * \sigma\} = \{\rho, \sigma * \rho^2\} \\
\sigma * \rho^2 * H &= \{\sigma * \rho^2 * \mathrm{id}, \sigma * \rho^2 * \sigma\} = \{\sigma * \rho^2, \rho\} = \rho * H \\
\rho^2 * H &= \{\rho^2 * \mathrm{id}, \rho^2 * \sigma\} = \{\rho^2, \sigma * \rho\} \\
\sigma * \rho * H &= \{\sigma * \rho * \mathrm{id}, \sigma * \rho * \sigma\} = \{\sigma * \rho, \rho^2\}
\end{aligned}$$

We see that there are three left cosets of H in G. Each coset has two elements and each element of G is in exactly one coset.

$$\boxed{\begin{array}{c} \mathrm{id}, \sigma \\ \hline \rho, \sigma * \rho^2 \\ \hline \sigma * \rho, \rho^2 \end{array}}$$

Example 3.9. Find the left cosets of $H = \langle 5 \rangle$ in $G = (\mathbb{Z}, +)$.

Answer 3.10. Recall that H is the subgroup

$$\langle 5 \rangle = \{\ldots, -10, -5, 0, 5, 10, \ldots\}$$

of $(\mathbb{Z}, +)$. We see that

$$\begin{aligned}
&\vdots \\
-1 + H &= \{\ldots, -11, -6, -1, 4, 9, \ldots\} = 4 + H, \\
0 + H &= \{\ldots, -10, -5, 0, 5, 10, \ldots\} = H, \\
1 + H &= \{\ldots, -9, -4, 1, 6, 11, \ldots\}, \\
2 + H &= \{\ldots, -8, -3, 2, 7, 12, \ldots\}, \\
3 + H &= \{\ldots, -7, -2, 3, 8, 13, \ldots\}, \\
4 + H &= \{\ldots, -6, -1, 4, 9, 14, \ldots\}, \\
5 + H &= \{\ldots, -5, 0, 5, 10, 15, \ldots\} = H, \\
5 + H &= \{\ldots, -4, 1, 6, 11, 16, \ldots\} = 1 + H, \\
&\vdots
\end{aligned}$$

We see that there are five cosets left cosets of H in G. Furthermore, there is a one-to-one correspondence between the elements of $a + H$ and the elements of H for each $a \in G$.

Question 3.11. *What are the left cosets of the unit circle group*

$$U = \{e^{i\theta} = \cos\theta + i \sin\theta \mid \theta \in \mathbb{R}\}$$

in $(\mathbb{C} \setminus \{0\}, \times)$? *Answer this question with a picture*!

Question 3.12. *What are the left cosets of* $(\mathbb{R}^{positive}, \times)$ *in* $(\mathbb{C} \setminus \{0\}, \times)$? *Answer this question with a picture*!

Summary 3.13. *We consider the four examples discussed above. In each example, we have a group* $(G, *)$ *and a subgroup* H. *In all four examples, every element of* G *is in exactly one left coset of* H *in* G. *Furthermore, there is a one-to-one correspondence*[16] *between the elements of* H *and the elements of the coset* $g * H$, *for all* $g \in G$.

We prove that the observations we made in Summary 3.13 hold always. Then we use these observations to prove Lagrange's Theorem.

Lemma 3.14. *Let* H *be a subgroup of the group* $(G, *)$. *Then every element of* G *is in exactly one left coset of* H *in* G.

Proof. We prove two statements.

(1) Every element of G is in at least one left coset of H in G.
(2) Let g_1 and g_2 be elements of G. If the left cosets $g_1 * H$ and $g_2 * H$ have any elements in common, then $g_1 * H = g_2 * H$.

Here is the proof of (1). Let $g \in G$. Then $g \in g * H$. This completes the proof of (1).

The proof of (2) involves more writing. Suppose $g \in g_1 * H \cap g_2 * H$ for some $g, g_1, g_2 \in H$. In this case,

$$g = g_1 * h_1 \text{ and } g = g_2 * h_2 \text{ for some } h_1 \text{ in } H_1 \text{ and } h_2 \text{ in } H_2. \tag{3.14.1}$$

We must prove that $g_1 * H = g_2 * H$.

(a) We will show that every element of $g_1 * H$ is in $g_2 * H$.
(b) We will also show that every element of $g_2 * H$ is in $g_1 * H$.

Before we get to work, let us mine (3.14.1) which tells us

$$g_1 * h_1 = g = g_2 * h_2.$$

Multiply both sides of $g_1 * h_1 = g_2 * h_2$ on the right by the inverse of h_1 and associate and use the property of inverse to see that

$$g_1 = g_2 * (h_2 * h_1^{-1}). \tag{3.14.2}$$

Multiply both sides of $g_1 * h_1 = g_2 * h_2$ on the right by the inverse of h_2 and associate and use the property of inverse to see that

$$g_1 * (h_1 * h_2^{-1}) = g_2. \tag{3.14.3}$$

[16] Let S and T be two sets. A one-to-one correspondence between S and T is a pair of functions $f : S \to T$ and $g : T \to S$ so that $(f \circ g)(t) = t$ for all $t \in t$ and $(g \circ f)(s) = s$ for all $s \in S$. If there is a one-to-one correspondence between the two sets S and T and one of the sets is finite, then both sets are finite and the two sets have the same number of elements.

We prove (a). Let x be an arbitrary element if $g_1 * H$. It follows that $x = g_1 * h_3$ for some $h_3 \in H$. Use (3.14.2) to conclude that $x = \left(g_2 * (h_2 * h_1^{-1})\right) * h_3$. Thus, x is equal to $g_2 *$ (an element of H); hence $x \in g_2 * H$. This completes the proof of (a).

We prove (b). Let y be an arbitrary element if $g_2 * H$. It follows that $y = g_2 * h_4$ for some $h_4 \in H$. Use (3.14.3) to conclude that $y = \left(g_1 * (h_1 * h_2^{-1})\right) * h_3$. Thus, y is equal to $g_1 *$ (an element of H); hence $y \in g_1 * H$. This completes the proof of (b).

Now that we have established (a) and (b) we have established (2). This completes the proof of Lemma 3.14 □

Lemma 3.15. *If H is a subgroup of the group G and $g \in G$, then there is a one-to-one correspondence between the elements of H and the elements $g * H$.*

Proof. We exhibit two function $f_1 : H \to g * H$ and $f_2 : g * H \to H$ such that $(f_2 \circ f_1)$ is the identity function on H and $(f_1 \circ f_2)$ is the identity function on $g * H$.

It is obvious what f_1 and f_2 are, namely $f_1(h) = g * h$ and $f_2(g * h) = g^{-1} * (g * h)$, where g^{-1} is the inverse of g. We see that

$$(f_2 \circ f_1)(h) = f_2(g * h) = g^{-1} * (g * h) = h$$

and

$$(f_1 \circ f_2)(g * h) = f_1(g^{-1} * (g * h)) = f_1(h) = g * h.$$

This completes the proof. □

We now prove Lagrange's theorem.

Theorem. 3.1 *Let G be a finite group and H be a subgroup of G. The the number of elements in H divides the number of elements*[17] *of G.*

Proof. Let $|G|$ be the number of elements in G and $|H|$ be the number of elements in H. Lemma 3.15 tells us that all of the left cosets of H in G have the same number of elements. The coset $\mathrm{id} * H = H$ has $|H|$ elements; so every left coset of H in G has $|H|$ elements. Lemma 3.14 tells us that every element of G is in exactly one left coset of H in G. Let c be the number of left coset of H in G. We have shown that $|G| = c|H|$. □

Remark 3.16. It is reasonable to ask if the converse of Lagrange's Theorem is true. That is, suppose G is a group of order n and d is a positive integer which divides n. Does G have to have a subgroup of order d?

The answer is: NO! The smallest example is the group called A_4 which consists of twelve elements in S_4. The group A_4 does not have a subgroup of order 6. See Question 7.10.

On the other hand, the converse of Lagrange's Theorem does hold for cyclic groups and that is the topic of the next section.

[17] Recall that the number of elements in the group G is also known as the order of G.

4. THE SUBGROUPS OF A CYCLIC GROUP.

The next project is: What are the subgroups of a cyclic group?

Example 4.1.

- What are the subgroups of $\mathbb{Z}$?
  Some subgroups that come to mind[18] are:
  $$\langle 0\rangle, \quad \langle 1\rangle, \quad \langle 2\rangle, \quad \langle 3\rangle, \quad \langle 4\rangle, \quad \langle 5\rangle, \quad \text{etc.}$$
- What are the subgroups of U_{24}?
  Some subgroups that come to mind are
  $$U_1, \quad U_2, \quad U_3, \quad U_4, \quad U_6, \quad U_8, \quad U_{12}, \quad U_{24}.$$

Proposition 4.2. *Every subgroup of a cyclic group is cyclic.*

Proof. Let $G = \langle g\rangle$ be a cyclic and let H be a subgroup of G. If H consists only of the identity element, then H is certainly cyclic. Otherwise, there is some positive integer s with $g^s \in H$. Pick s to be the least positive integer with $g^s \in H$. We claim $H = \langle g^s\rangle$.

The inclusion $\supseteq$ is obvious.

We prove the inclusion $\subseteq$. Let $h = g^r$ be an arbitrary element of H. Write $r = \ell s + m$ for integers ℓ and m with $0 \leq m \leq s-1$. It follows that $g^m \in H$. We picked s to have the property that if $1 \leq i \leq s-1$, then $g^i \notin H$. Thus, $m = 0$ and

$$h = g^r = g^{\ell s+m} = g^{\ell s} = (g^s)^\ell \in \langle g^s\rangle.$$

□

Corollary 4.3. *If G is a finite cyclic group of order n, then G has exactly one subgroup of order d for each divisor d of n.*

Remark 4.4. In Example 4.1 we listed all of the subgroups of U_{24}.

Proof. Let $G = \langle g\rangle$. Fix a divisor d of n. Observe that $\langle g^{n/d}\rangle$ has order d. On the other hand, if H is a subgroup of G of order d, then the proof of Proposition 4.2 shows that $H = \langle g^s\rangle$ where s is the smallest positive exponent with g^s in H. Furthermore, the proof of Proposition 4.2 shows that this s must divide n (otherwise, there is a smaller exponent with g to that exponent is in H) and $\frac{n}{s}$ is the order of H. □

Definition 4.5. If a and b are integers, not both zero, then the
greatest common divisor of a and b is the largest integer d for which d divides a and d divides b.

Lemma 4.6. *If a and b are integers (not both zero), then the subgroup $\langle a,b\rangle$ is equal to $\langle d\rangle$ where d is the greatest common divisor of a and b.*

[18] I often write the subgroup $\langle n\rangle$ of $\mathbb{Z}$ as $n\mathbb{Z}$.

Proof. The subgroup $\langle a,b\rangle$ is not the zero subgroup; so there is some non-zero integer in $\langle a,b\rangle$; indeed, there is some positive integer in $\langle a,b\rangle$. Let d be the smallest positive integer in $\langle a,b\rangle$. We already proved that $\langle a,b\rangle = \langle d\rangle$. It remains to show that d is the greatest common divisor of a and b. The fact that a and b are in $\langle d\rangle$ guarantees that d divides both a and b. Furthermore, if d' divides both a and b, then d' divides d because $d \in \langle a,b\rangle$. Thus $d' \leq d$, and d is the largest integer which divides both a and b. □

5. Group homomorphisms, group isomorphisms, Cayley's Theorem.

Definition 5.1. If G and G' are groups then a function $\phi : G \to G'$ is a group homomorphism if

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

for all g_1, g_2 in G. The operation on the left takes place in G. The operation on the right takes place in G'.

A group homomorphism which is one-to-one and onto is called a group isomorphism.

Elementary Properties. Let $\phi : G \to G'$ be a group homomorphism. The following statements hold.

(a) If id is the identity element of G, then $\phi(\mathrm{id})$ is the identity element of G'.
(b) The homomorphism ϕ carries the inverse of g to the inverse of $\phi(g)$ for all $g \in G$.

Proof. (a) Observe that $\mathrm{id} = \mathrm{id} * \mathrm{id}$; so

$$\phi(\mathrm{id}) = \phi(\mathrm{id} * \mathrm{id}) = \phi(\mathrm{id}) * \phi(\mathrm{id}).$$

Now multiply both sides of the equation by the inverse of $\phi(\mathrm{id})$, to learn that

$$\mathrm{id}' = \phi(\mathrm{id}),$$

where id' is the identity element in G'.

(b) Let g be an element of G and let g^{-1} be the inverse of g in G. Observe that $g * g^{-1} = \mathrm{id}$; hence,

$$\phi(g) * \phi(g^{-1}) = \phi(\mathrm{id}) = \mathrm{id}'.$$

Multiply both sides of the equation on the left by $(\phi(g))^{-1}$ to obtain the result. □

Example 5.1.1. The function $\phi : (\mathbb{R}, +) \to (\{r \in \mathbb{R} \mid 0 < r\}, \times)$, given by $\phi(r) = e^r$ is a group isomorphism because

$$\phi(r_1 + r_2) = e^{r_1 + r_2} = e^{r_1} e^{r_2} = \phi(r_1)\phi(r_2).$$

ϕ is surjective. Take s in the target. Observe that $\ln s$ is in the source and

$$\phi(\ln s) = e^{\ln s} = s.$$

ϕ is injective. Suppose r_1 and r_2 are in the source with $\phi(r_1) = \phi(r_2)$. Then $e^{r_1} = e^{e_2}$. Apply ln to both sides to learn that $r_1 = r_2$.

Example 5.1.2. The function $\phi : (\mathbb{R}, +) \to U$, which is given by

$$\phi(\theta) = e^{i\theta}$$

is a surjective group homomorphism which is not injective.

Example 5.1.3. Recall the group $\mathscr{G}$ of rigid motions of the plane. Let Rot be the subset of $\mathscr{G}$ which consists of all rotations which fix the origin. In particular, for each real number θ, let ρ_θ be the rigid motion which fixes the origin and rotates the plane counterclockwise by the angle θ radians. Observe that Rot is a subgroup of $\mathscr{G}$. Observe that $\phi : U \to \text{Rot}$, which is given by

$$\phi(e^{i\theta}) = \rho_\theta,$$

is a function. That is, check that if $e^{i\theta} = e^{i\theta'}$, then $\rho_\theta = \rho_{\theta'}$. Observe that ϕ is a group isomorphism.

5.A. **When are two cyclic groups isomorphic?**

Observation 5.2. *Two cyclic groups are isomorphic if and only if they have the same order.*

Proof.
($\Rightarrow$) This direction is clear. An isomorphism is always a bijection.

($\Leftarrow$) We treat two cases: infinite cyclic groups and finite cyclic groups.

• We show that every infinite cyclic group is isomorphic to $(\mathbb{Z}, +)$. (This is good enough because the relation "are isomorphic" is an equivalence relation on the set of groups. You should prove this, if necessary.[19]) If G is a cyclic group with generator g and operation $*$, then

$$\phi : \mathbb{Z} \to G,$$

given by $\phi(j) = g^j$, is an isomorphism. Of course,

$$g^j \text{ means } \begin{cases} \underbrace{g * g * \cdots * g}_{j \text{ times}}, & \text{if } 0 < j, \\ \text{identity element}, & \text{if } j = 0, \\ \underbrace{g^{-1} * g^{-1} * \cdots * g^{-1}}_{|j| \text{ times}}, & \text{if } j < 0. \end{cases}$$

(Please check, if necessary, that $\phi(j+k) = \phi(j) * \phi(k)$, ϕ is one-to-one, and ϕ is onto.)

• Suppose $A = \langle a \rangle$ and $B = \langle b \rangle$ are both cyclic groups of order n, where n is a finite positive integer. The elements of A are $\{a^j | 0 \le j \le n-1\}$ and the elements of B are $\{b^j | 0 \le j \le n-1\}$, where a^0 is the identity element of A and b^0 is the identity element of B. It is clear that

$$\phi : A \to B,$$

[19] A relation $(\sim)$ on the set S is an equivalence relation if it is reflexive ($s \sim s$ for all $s \in S$), symmetric ($s \sim s' \implies s' \sim s$, for all $s, s' \in S$) and transitive ($s \sim s'$ and $s' \sim s''$ for $s, s', s'' \in S$ implies $s \sim s''$).

given by $\phi(a^j) = b^j$, for $0 \leq j \leq n-1$, is a bijection. We show that ϕ is a homomorphism. If $0 \leq i, j \leq n-1$, then $i+j = k+rn$ for some integers k and r with $0 \leq k \leq n-1$. Observe that

$$\phi(a^i \cdot a^j) = \phi(a^{i+j}) = \phi(a^{k+rn}) = \phi(a^k \cdot (a^n)^r) = \phi(a^k) = b^k = b^{k+rn} = b^{i+j}$$
$$= b^i \cdot b^j = \phi(a^i) \cdot \phi(a^j).$$

□

5.B. **Cayley's Theorem.** On the first day of class, I defined group and then I started to give a long list of examples of groups. The second example was the Symmetric group on the set T, denoted $\mathrm{Sym}(T)$. Recall that if T is a set, then the set of invertible functions $f : T \to T$ under the operation composition is a group called the Symmetric group on T. I said that every group "is" a subgroup of $\mathrm{Sym}(T)$ for some T and this result is called Cayley's Theorem. Now that we have the proper language, lets state the Theorem correctly and prove it.

Theorem 5.3. (Cayley) *Every group G is isomorphic to a subgroup of* $\mathrm{Sym}(G)$.

Proof. Let G be a group. If $g \in G$, then let $g_L : G \to G$ be the function $g_L(g_1) = gg_1$ for all $g_1 \in G$. Notice that g_L is a permutation of G!

Let $G_L = \{g_L : G \to G \mid g \in G\}$.

Observe $(G_L, \circ)$ is a subgroup of $\mathrm{Sym}(G)$.

- If $h, g \in G$, then $h_L \circ g_L = (hg)_L$. (So G_L is closed under $\circ$.)
- If id is the identity element of G, then id_L is the identity element of G_L.
- If $g \in G$, then $(g^{-1})_L = (g_L)^{-1}$.
- Function composition always associates.

Observe that $\phi : G \to G_L$, which is defined by $\phi(g) = g_L$, is a group isomorphism. Indeed,

- we already saw that $\phi(hg) = \phi(h) \circ \phi(g)$,
- if g_L is an arbitrary element of G_L, for some $g \in G$, then $g_L = \phi(g)$,
- if $\phi(g) = \phi(h)$, then the functions g_L and h_L of G_L are equal. In particular, if id is the identity element of G, then

$$g = g\,\mathrm{id} = g_L(\mathrm{id}) = h_L(\mathrm{id}) = h\,\mathrm{id} = h.$$

□

Corollary 5.4. *If G is a group of order*[20] *n, then G is isomorphic to a subgroup of S_n.*

Of course, there is more nothing to prove. The proof we gave also establishes the Corollary.

On the first day of class I promised that

[20]The order of a group is the number of elements in the group.

Theorem 5.5. *Every finite group is isomorphic to a subgroup of* $\mathrm{GL}_n(\mathbb{R})$ *for some* n.

Now that we know a proof of Lagrange's Theorem, we also know a proof of Theorem 5.5, provided we can prove

Observation 5.6. *The group* S_n *is isomorphic to a subgroup of* $\mathrm{GL}_n(\mathbb{R})$.

Problem 5.7. Prove Observation 5.6.

Example 5.8. Lets use Cayley's Theorem to exhibit S_3 as a subgroup of S_6. Write S_3 as

$$a_1 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}, \quad a_2 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}, \quad a_3 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix},$$
$$a_4 = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}, \quad a_5 = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}, \quad \text{and} \quad a_6 = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}.$$

Observe that

$$(a_2)_L : S_3 \to S_3$$

is

$$\begin{aligned}
a_1 &\mapsto a_2 \\
a_2 &\mapsto a_1 \\
a_3 &\mapsto \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = a_6 \\
a_4 &\mapsto \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = a_5 \\
a_5 &\mapsto \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = a_4 \\
a_6 &\mapsto \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = a_3.
\end{aligned}$$

So $(a_2)_L = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_1 & a_6 & a_5 & a_4 & a_3 \end{pmatrix}$. Similarly,

$$(a_5)_L : S_3 \to S_3$$

is

$$\begin{aligned}
a_1 &\mapsto a_5 \\
a_2 &\mapsto \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = a_3 \\
a_3 &\mapsto \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = a_4 \\
a_4 &\mapsto \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = a_2 \\
a_5 &\mapsto \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = a_6 \\
a_6 &\mapsto \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix} = a_1.
\end{aligned}$$

So $(a_5)_L = \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_5 & a_3 & a_4 & a_2 & a_6 & a_1 \end{pmatrix}$

In Homework 1.a, you saw that S_3 is generated by a_2 and a_5. Thus, the proof of Cayley's theorem shows that S_3 is isomorphic to the subgroup of S_6 which is generated by

$$\begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_2 & a_1 & a_6 & a_5 & a_4 & a_3 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} a_1 & a_2 & a_3 & a_4 & a_5 & a_6 \\ a_5 & a_3 & a_4 & a_2 & a_6 & a_1 \end{pmatrix}.$$

Example 5.9. This is a more interesting example. Does there exist an 8-element group

$$\{\mathrm{id}, a, a^2, a^3, b, ab, a^2b, a^3b\}$$

which satisfies

$$a^4 = \mathrm{id}, \quad a^2 = b^2, \quad \text{and} \quad ba = a^3b?$$

Step 1. If there exists such a group; it could only have one multiplication table

(5.9.1)

	id	a	a^2	a^3	b	ab	a^2b	a^3b
id	id	a	a^2	a^3	b	ab	a^2b	a^3b
a	a	a^2	a^3	id	ab	a^2b	a^3b	b
a^2	a^2	a^3	id	a	a^2b	a^3b	b	ab
a^3	a^3	id	a	a^2	a^3b	b	ab	a^2b
b	b	a^3b	a^2b	ab	a^2	a	id	a^3
ab	ab	b	a^3b	a^2b	a^3	a^2	a	id
a^2b	a^2b	ab	b	a^3b	id	a^3	a^2	a
a^3b	a^3b	a^2b	ab	b	a	id	a^3	a^2

We still do not know if this multiplication associates and we certainly do not know if all eight names are distinct.

Here is my plan. Let T be the set that consists of the eight elements

$$T = \{g_1, g_2, g_3, g_4, g_5, g_6, g_7, g_8\}.$$

Pretend that pretend$-G$ is a group whose elements are $\mathrm{id}, \alpha, \alpha^2, \alpha^3, \beta, \alpha\beta, \alpha^2\beta, \alpha^3\beta$ and which satisfy the relations $\alpha^4 = \mathrm{id}$, $\beta^2 = \alpha^2$, $\beta\alpha = \alpha^3\beta$. Pretend that

$$\begin{aligned} &g_1 \text{ behaves like } \mathrm{id}, \\ &g_2 \text{ behaves like } \alpha, \\ &g_3 \text{ behaves like } \alpha^2, \\ &g_4 \text{ behaves like } \alpha^3, \\ &g_5 \text{ behaves like } \beta, \\ &g_6 \text{ behaves like } \alpha\beta, \\ &g_7 \text{ behaves like } \alpha^2\beta, \\ &g_8 \text{ behaves like } \alpha^3\beta \end{aligned}$$

We use the idea in the proof of Cayley's Theorem to find permutations a and b in $\mathrm{Sym}(T)$ which satisfy: $a^4 = \mathrm{id}$, $b^2 = a^2$, $ba = a^3b$. **If we are lucky**, the permutations a^ib^j, with $0 \le i \le 3$ and $0 \le j \le 1$, are distinct. In this case, we will have

found a **real subgroup** of $\mathrm{Sym}(T)$ with 8 distinct elements whose multiplication table is (5.9.1).

Anyhow left multiplication by α sends

$$\mathrm{id} \to \alpha \to \alpha^2 \to \alpha^3 \to \mathrm{id} \quad \text{and} \quad \beta \to \alpha\beta \to \alpha^2\beta \to \alpha^3\beta \to \beta.$$

So, left multiplication by α corresponds to the permutation

$$a = \begin{pmatrix} g_1 & g_2 & g_3 & g_4 & g_5 & g_6 & g_7 & g_8 \\ g_2 & g_3 & g_4 & g_1 & g_6 & g_7 & g_8 & g_5 \end{pmatrix} \in \mathrm{Sym}(T)$$

$\mathrm{Sym}(T)$. Also, left multiplication by β sends

$$\mathrm{id} \to \beta \to \alpha^2 \to \alpha^2\beta \to \mathrm{id} \quad \text{and} \quad \alpha \to \alpha^3\beta \to \alpha^3 \to \alpha\beta \to \alpha.$$

So, left multiplication by β corresponds to the permutation

$$b = \begin{pmatrix} g_1 & g_2 & g_3 & g_4 & g_5 & g_6 & g_7 & g_8 \\ g_5 & g_8 & g_7 & g_6 & g_3 & g_2 & g_1 & g_4 \end{pmatrix} \in \mathrm{Sym}(T)$$

It is now easy to see that

$$\begin{aligned}
\mathrm{id} &= \begin{pmatrix} g_1 & g_2 & g_3 & g_4 & g_5 & g_6 & g_7 & g_8 \\ g_1 & g_2 & g_3 & g_4 & g_5 & g_6 & g_7 & g_8 \end{pmatrix} \\
a &= \begin{pmatrix} g_1 & g_2 & g_3 & g_4 & g_5 & g_6 & g_7 & g_8 \\ g_2 & g_3 & g_4 & g_1 & g_6 & g_7 & g_8 & g_5 \end{pmatrix} \\
a^2 &= \begin{pmatrix} g_1 & g_2 & g_3 & g_4 & g_5 & g_6 & g_7 & g_8 \\ g_3 & g_4 & g_1 & g_2 & g_7 & g_8 & g_5 & g_6 \end{pmatrix} \\
a^3 &= \begin{pmatrix} g_1 & g_2 & g_3 & g_4 & g_5 & g_6 & g_7 & g_8 \\ g_4 & g_1 & g_2 & g_3 & g_8 & g_5 & g_6 & g_7 \end{pmatrix} \\
b &= \begin{pmatrix} g_1 & g_2 & g_3 & g_4 & g_5 & g_6 & g_7 & g_8 \\ g_5 & g_8 & g_7 & g_6 & g_3 & g_2 & g_1 & g_4 \end{pmatrix} \\
ab &= \begin{pmatrix} g_1 & g_2 & g_3 & g_4 & g_5 & g_6 & g_7 & g_8 \\ g_6 & g_5 & g_8 & g_7 & g_4 & g_3 & g_2 & g_1 \end{pmatrix} \\
a^2b &= \begin{pmatrix} g_1 & g_2 & g_3 & g_4 & g_5 & g_6 & g_7 & g_8 \\ g_7 & g_6 & g_5 & g_8 & g_1 & g_4 & g_3 & g_2 \end{pmatrix} \\
a^3b &= \begin{pmatrix} g_1 & g_2 & g_3 & g_4 & g_5 & g_6 & g_7 & g_8 \\ g_8 & g_7 & g_6 & g_5 & g_2 & g_1 & g_4 & g_3 \end{pmatrix}
\end{aligned}$$

are distinct and satisfy $a^4 = 1$, $b^2 = a^2$, $ba = a^3b$.

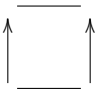
6. Normal subgroups, quotient groups, and the First Isomorphism Theorem.

Make identifications to create new objects. Example 1. Surfaces.

One major technique that distinguishes Mathematics from many other disciplines is that in Mathematics one can take a perfectly good thing and one can pretend one part of the original thing is equal to some other part of the original thing and thereby create a brand new perfectly good thing.

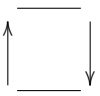
The first example that comes to mind is the study of surfaces. One can start with a rectangular surface

and pretend that each point on the left side is the same as the corresponding point in the right side.



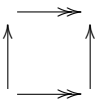
Now one has a cylinder.

Or one can start with a rectangular surface and pretend that each point on the left side is the same as the corresponding point in the right side measured in the opposite direction.



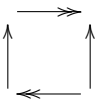
Now one has a Möbius bond.

One can make identifications on a rectangular surface



and create a torus.

One can make identifications on a rectangular surface



and create a Klein bottle.

The cylinder, the Möbius band, and the torus can all be built in 3-space. The Klein bottle can not be built in 3-space but it makes just as much sense to a Mathematician as the other three surfaces.

Make identifications to create new objects. Example 2. Groups.

Start with a group G. Pick out two elements g_1 and g_2. Our goal is to create a new group $\bar{G}$ which is as much like G as possible, but in which the image of g_1 in $\bar{G}$ is equal to the image of g_2 in $\bar{G}$. Lets write $\bar{g}_1$ in place of "the image of g_1 in $\bar{G}$".

Notice first that we are putting a relation $\sim$ on G and saying that $\bar{g}_1 = \bar{g}_2$ in $\bar{G}$ if and only if $g_1 \sim g_2$ in G. What kind of relations $\sim$ in G will give rise to groups $\bar{G}$?

(1) The relation $\sim$ better be an equivalence relation because $=$ in $\bar{G}$ is an equivalence relation. (See the footnote 19 on page 19 for the definition of an equivalence relation, if necessary.)
(2) If g_1, g_2, and g_3 are elements of G with $g_1 \sim g_2$, then one must have $g_1 g_3 \sim g_2 g_3$.
(3) In particular, $g_1 \sim g_2$ if and only if $g_1 g_2^{-1} \sim \mathrm{id}$ where id is the identity element of G.
(4) Hence, it suffices to figure out which elements g in G satisfy $g \sim \mathrm{id}$. Let $N = \{g \in G \mid g \sim \mathrm{id}\}$.
(5) Observe that N must be a subgroup.
(6) Observe that if $n \in N$ and g is an arbitrary element of G, then
$$gng^{-1} \sim g\,\mathrm{id}\,g^{-1} = \mathrm{id};$$
hence gng^{-1} must be in N.

Definition 6.1. If N is a subgroup of G and $gng^{-1} \in N$ for all $n \in N$ and $g \in G$, then G is called a normal subgroup of G.[21]

Remark. Sometimes it is easier to make sense of words than symbols. Here is Definition 6.1 expressed in words. A subgroup N of the group G is a normal subgroup if N is closed under conjugation by elements of G.

Examples 6.2. (a) If G is an Abelian group, then every subgroup of G is a normal subgroup.
(b) If G is an arbitrary group and N is a subgroup of the center of G then N is a normal subgroup of G.
(c) If N is a subgroup of the group G and[22] $|N| = \frac{1}{2}|G|$, then N is a normal subgroup of G. (Another way to state this result is: "Every subgroup of index 2 is normal." Indeed, the index of a subgroup H in the group G is the number of left cosets of H in G.)

Proof. Let N be a subgroup of G of index two. Notice that if g is an element of G which is not in N, then

(6.2.1) $\qquad G$ is the disjoint union of the left cosets $N \cup gN$.

We show that N is a normal subgroup of G. Take $n \in N$ and $g \in G$. If $g \in N$, then it is obvious that $gng^{-1} \in N$. Henceforth, $g \notin N$. We assume

[21] The symbols "$N \triangleleft G$" mean "N is a normal subgroup of G".
[22] We are using $|\ |$ to mean "the number of elements in".

that $gng^{-1} \notin N$. We will reach a contradiction. If $gng^{-1} \notin N$, then by (6.2.1) $gng^{-1} \in gN$; hence $ng^{-1} \in N$ and $g^{-1} \in N$, which is impossible. □

(d) If N is a subgroup of the group G and N is the only subgroup of G with order equal to the order of N, then N is a normal subgroup of G.

Proof. In this case, for each $g \in G$, gNg^{-1} is a subgroup of G of order equal to the order of N. It follows from the hypothesis that $gNg^{-1} = N$. □

(e) $\langle \rho \rangle \triangleleft D_4$, (because $\langle \rho \rangle$ has index two)

(f) $\langle \rho^2 \rangle \triangleleft D_4$ because $\langle \rho^2 \rangle$ is the center of D_4.

(g) $\langle \sigma \rangle$ is not a normal subgroup of D_4 because

$$\rho^{-1}\sigma\rho = \rho^3\sigma\rho = \sigma\rho^2$$

and $\sigma\rho^2 \notin \langle \sigma \rangle$.

(h) Let Q be the group with eight elements $a^i b^j$ with $i \in \{0,1,2,3\}$ and $j \in \{0,1\}$, $a^4 = \mathrm{id}$, $a^2 = b^2$, and $ba = a^3 b$. (Example 5.9 shows that the group Q exists.) The element a^2 of Q is the only element of order 2. It follows from (d) that $\langle a^2 \rangle$ is a normal subgroup of Q.

There is also another way to see that $\langle a^2 \rangle \triangleleft Q_8$. If G is a group, then the <u>center</u> of G is

$$Z(G) = \{g \in G \mid gh = hg \text{ for all } h \in G\}.$$

It is true (and easy to see) that

$$Z(G) \triangleleft G$$

for all groups G. Furthermore, one can verify that $Z(Q_8) = \langle a^2 \rangle$.

(i) The subgroup $\left\langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \right\rangle$ of S_3 is not normal because

$$\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix} \notin \left\langle \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} \right\rangle.$$

(j) The subgroup

$$V_4 = \left\{ \mathrm{id}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 4 & 3 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 3 & 4 & 1 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix} \right\} \tag{6.2.2}$$

is a normal subgroup of S_4, A_4, and D_4. (See Example 7.9 for a QUICK proof.)

(k) Let $\phi : G \to G'$ be a group homomorphism and let

$$\ker\phi = \{g \in G \mid \phi(g) \text{ is equal to the identity element of } G'\}.$$

Then $\ker\phi$ is a normal subgroup of G.

Proof. Check that $\ker\phi$ is closed under the operation of G. Check that if g is in $\ker\phi$, then $g^{-1} \in \ker\phi$. Check that $\ker\phi$ is closed under conjugation. □

The key property of a normal subgroup:

Proposition 6.3. *If N is a normal subgroup of G, and S is the set of left cosets of N in G, then*

$$S \times S \to S,$$

given by $aN \times bN \mapsto abN$ is a (well-defined) function.

Proof. Suppose $a_1N = a_2N$ and $b_1N = b_2N$. We must show that $a_1b_1N = a_2b_2N$ for some a_1, a_2, b_1, b_2 in G. We are told $a_1 = a_2n_1$ and $b_1 = b_2n_2$ for some n_1, n_2 in N.

We see that

$$a_1b_1 = a_2n_1b_2n_2 = a_2b_2b_2^{-1}n_1b_2n_2 = a_2b_2 \text{ times an element of } N.$$

We conclude that $a_1a_2N = a_2b_2N$. □

Quiz Wednesday on HW 19, 20, 27, 33, 38, 39.

Quiz Wednesday March 29 on HW 40, 41, 42, 49, 50, 54, 55.

Exam Wednesday, April 5 on Day 1 until To Be Announced.

Your questions

$\frac{G}{N}$

Let $(G,*)$ be a group and N be a normal subgroup of G. Then the set of left cosets of N in G forms a group with operation $(g_1 * N) * (g_2 * N) = g_1 * g_2 * N$. This new group is denoted $\frac{G}{N}$ and is called a quotient group. In particular, $\frac{G}{N}$ is the quotient of G by N.

The plan for today.

1. What is $\frac{(\mathbb{Z},+)}{5\mathbb{Z}}$?
2. What is $\frac{(\mathbb{R},+)}{\mathbb{Z}}$?
3. What is $\frac{(\mathbb{C}\setminus\{0\},\times)}{U}$?
4. What is $\frac{(S_4,\circ)}{V_4}$, where V_4 is the subgroup

$$\left\{\begin{pmatrix}1&2&3&4\\1&2&3&4\end{pmatrix},\begin{pmatrix}1&2&3&4\\2&1&4&3\end{pmatrix},\begin{pmatrix}1&2&3&4\\3&4&1&2\end{pmatrix},\begin{pmatrix}1&2&3&4\\4&3&2&1\end{pmatrix}\right\}?$$

5. Recall that $\langle\sigma\rangle$ is not a normal subgroup of $(S_3,\circ)$, where

$$\sigma=\begin{pmatrix}1&2&3\\2&1&3\end{pmatrix}.$$

Why does can't we make the left cosets of $\langle\sigma\rangle$ in S_3 into group using the same procedure?

We get to work.

1. Observe that $\frac{\mathbb{Z}}{5\mathbb{Z}}$ has five elements:

$$0+5\mathbb{Z},\quad 1+5\mathbb{Z},\quad 2+5\mathbb{Z},\quad 3+5\mathbb{Z},\quad \text{and}\quad 4+5\mathbb{Z}.$$

Also,

$0+5\mathbb{Z}$ is the identity element;

$1+5\mathbb{Z}$ plus $1+5\mathbb{Z}$ equals $2+5\mathbb{Z}$;

$1+5\mathbb{Z}$ plus $1+5\mathbb{Z}$ plus $1+5\mathbb{Z}$ equals $3+5\mathbb{Z}$;

$1+5\mathbb{Z}$ plus $1+5\mathbb{Z}$ plus $1+5\mathbb{Z}$ plus $1+5\mathbb{Z}$ equals $4+5\mathbb{Z}$;

$1+5\mathbb{Z}$ plus $1+5\mathbb{Z}$ plus $1+5\mathbb{Z}$ plus $1+5\mathbb{Z}$ plus $1+5\mathbb{Z}$ equals $0+5\mathbb{Z}$;

Indeed $\frac{\mathbb{Z}}{5\mathbb{Z}}$ is a cyclic group of order five.

2. The cosets of $\frac{\mathbb{R}}{\mathbb{Z}}$ are

$$\{r+\mathbb{Z} \mid r \text{ is a real number with } 0\le r<1\}.$$

We have listed each coset exactly once!

If r_1 and r_2 are real numbers with $0\le r_1,r_2<1$, then

$$r_1+\mathbb{Z} \text{ plus } r_2+\mathbb{Z} \text{ equals } r_1+r_2+\mathbb{Z}$$

and if we want we write

$$r_1 + r_2 = n + q$$

where n is an integer and q is a real number with $0 \leq q < 1$. In this language $r_1 + r_2 + \mathbb{Z} = q + \mathbb{Z}$ in $\frac{\mathbb{R}}{\mathbb{Z}}$.

3. The cosets of $\frac{\mathbb{C}\backslash\{0\}}{U}$ are

$$\{rU \mid 0 < r \text{ and } r \text{ is a real number.}\}$$

We have listed each coset exactly once. This group "seems" to be the "same" as $(\mathbb{R}^{\text{pos}}, \times)$.

4. How many elements does $\frac{S_4}{V_4}$ have?

(There are six cosets of V_4 in S_4?)

How many groups do we know with six elements?

(I know the cyclic group of order six and S_3.)

Which one is more likely to be $\frac{S_4}{V_4}$?

Is there some way we can use the names from S_3 as we name the cosets of V_4 in S_4?

That is, notice that $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 2 & 1 & 3 & 4 \end{pmatrix}$ is the only element of σV_4 which leaves 4 alone.

In fact each coset of V_4 in S_4 has at most one element that leaves 4 alone.

This proves that

$$\frac{S_4}{V_4} = \{\alpha V_4 \mid \alpha \in S_4 \text{ and } \alpha(4) = 4\}.$$

We have reason to think that $\frac{S_4}{V_4}$ might be isomorphic to S_3.

5. Let $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ and $\rho = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. Recall that $\sigma^2 = \text{id}$, $\rho^3 = \text{id}$, and $\sigma\rho\sigma\rho = \text{id}$.

The coset $\rho\langle\sigma\rangle$ is equal to $\{\rho, \sigma\rho^2\}$ (because, $\rho\sigma = \sigma\rho^2$). So,

$$\boxed{\rho\langle\sigma\rangle = \sigma\rho^2\langle\sigma\rangle}.$$

The coset $\rho^2\langle\sigma\rangle$ is equal to $\{\rho^2, \sigma\rho\}$ (because, $\rho^2\sigma = \sigma\rho$). So

$$\boxed{\rho^2\langle\sigma\rangle = \sigma\rho\langle\sigma\rangle}.$$

However

$$\rho\rho^2\langle\sigma\rangle \textbf{Does not equal } \sigma\rho^2\sigma\rho\langle\sigma\rangle.$$

The coset on the left is $\text{id}\langle\sigma\rangle = \{\text{id}, \sigma\}$. The coset on the right is $\rho^2\langle\sigma\rangle = \{\rho^2, \sigma\rho\}$.

Theorem 6.4. *If N is a normal subgroup of G, and $\frac{G}{N}$ is the set of left cosets of N in G, then $(\frac{G}{N}, *)$ is a group with operation*

$$(aN) * (bN) = abN.$$

Proof. The operation $aN * bN = abN$ MAKES SENSE by Proposition 6.3. The rest of the properties must be checked – but they are easy!

The identity element of $\frac{G}{N}$ is $\mathrm{id}N$ because if aN is any element of S, then $\mathrm{id}N * aN = \mathrm{id}\,aN = aN$ and $aN * \mathrm{id}N = a\,\mathrm{id}N = aN$.

The operation in $\frac{G}{N}$ is closed: if a and b are elements of G, then aN and bN are elements of $\frac{G}{N}$ and $aN * bN$ is equal to abN which is an element of $\frac{G}{N}$.

The operation in $\frac{G}{N}$ associates: if a, b, and c are elements of G, then aN, bN and cN are elements of S and

$$(aN*bN)*cN = (abN)*cH = ((ab)c)*N = (a(bc))*N = (aN)*(bcN) = aN*(bN*cN).$$

The inverse of aN is $a^{-1}N$ where a^{-1} is the inverse in G of the element a of G. □

Here are two more minor properties of normal subgroups.

Observation 6.5. *Assume that N is a normal subgroup of the group G. Then the following statements hold:*

(a) *$gN = Ng$, for all $g \in N$, and*
(b) *$gN = \{h \in G \mid gh^{-1} \in N\}$, for all $g \in G$.*

Proof. (a) Let $g \in N$. We first show that $gN \subseteq Ng$. Take a typical element of gN, namely gn for some $n \in N$. Oberve that

$$gn = gng^{-1}g \in Ng.$$

Now we show that $Ng \subseteq gN$. A typical element of Ng has the form ng for some $n \in N$. Observe that

$$ng = gg^{-1}ng \in gN.$$

(b) Fix an element $g \in G$. We first show $gN \subseteq \{h \in G \mid gh^{-1} \in N\}$.

Each element of gN is of the form gn for some n in N. We must show that $g(gn)^{-1}$ is in N. But $g(gn)^{-1} = gn^{-1}g^{-1}$, which indeed is in N because n^{-1} is in the normal subgroup N.

Now we show that $\{h \in G \mid gh^{-1} \in N\} \subseteq gN$.

Take $h \in G$ with $gh^{-1} = n$, for some $n \in N$. We must show that $h \in gN$. We see that

$$n^{-1}g = h;$$

hence

$$h = n^{-1}g = g(g^{-1}n^{-1}g) \in gN.$$ □

Theorem 6.6. [The First Isomorphism Theorem.] *Let $\phi : G \to G'$ be a group homomorphism.*

(a) *If N is a normal subgroup of G and $N \subseteq \ker\phi$, then ϕ induces a group homomorphism $\bar{\phi} : \frac{G}{N} \to G'$, with*

$$\bar{\phi}(\bar{g}) = \phi(g).$$

(b) *The homomorphism*

$$\bar{\phi} : \frac{G}{\ker\phi} \to \operatorname{im}\phi$$

is an isomorphism.

Remark 6.7. It is very difficult to produce homomorphisms from random groups. To create such a homomorphism, I usually view the random group as a quotient of a well-understood group, I create a homomorphism from the well understood group, and then I apply the First Isomorphism Theorem.

For example when we proved that all cyclic groups of order n are isomorphic, we gave an unpleasant argument. The "correct" argument is to show that any group of order n is isomorphic to $\frac{\mathbb{Z}}{n\mathbb{Z}}$:

Let G be a cyclic group of order n with generator g. (Call the operation in G "times".) Define $\phi : \mathbb{Z} \to G$ with $\phi(r) = g^r$. This is a homomorphism. Apply the First Isomorphism Theorem to conclude that $\bar{\phi} : \frac{\mathbb{Z}}{n\mathbb{Z}} \to G$ is an isomorphism.

Proof of the First Isomorphism Theorem, Theorem 6.6.

We must show that $\bar{\phi}$ of (a) **is a legitimate function.** Once we do that, then everything else is obvious.

Suppose that g_1 and g_2 are elements of G with $\bar{g}_1 = \bar{g}_2$ in $\frac{G}{N}$. We must show that $\phi(g_1) = \phi(g_2)$.

The hypothesis $\bar{g}_1 = \bar{g}_2$ in $\frac{G}{N}$ guarantees that

$$g_1 g_2^{-1} \in N \subseteq \ker\phi.$$

It follows that $\phi(g_1 g_2^{-1})$ is the identity element of G'; and therefore, $\phi(g_1) = \phi(g_2)$. □

Example 6.8. The groups $\frac{\mathbb{R}}{\mathbb{Z}}$ and U are isomorphic.

Proof. Consider the homomorphism $\phi : \mathbb{R} \to U$, which is given by $\phi(\theta) = e^{2\pi i\theta}$. Apply the First Isomorphism Theorem. □

Example 6.9. The groups $\frac{U}{U_2}$ and U are isomorphic.

Proof. Consider the homomorphism $\phi : U \to U$, which is given by $\phi(u) = u^2$. Apply the First Isomorphism Theorem. □

Example 6.10. The groups $\frac{U}{U_n}$ and U are isomorphic.

Proof. Consider the homomorphism $\phi : U \to U$, which is given by $\phi(u) = u^n$. Apply the First Isomorphism Theorem. □

Example 6.11. Recall the subgroup V_4 of S_4 which is given in (6.2.2). I promised that Example 7.9 gives a quick proof that $V_4 \triangleleft S_4$. Assuming this is true, we prove that the groups $\frac{S_4}{V_4}$ and S_3 are isomorphic.

Proof. This one is sneaky. I do not know any homomorphisms from $S_4 \to S_3$. Instead, I propose that we consider $\phi : S_3 \to \frac{S_4}{V_4}$ to be the composition of the following two homomorphisms[23]:

$$S_3 \xrightarrow{\text{inclusion}} S_4 \xrightarrow{\text{natural quotient map}} \frac{S_4}{V_4}.$$

So, ϕ is automatically a homomorphism.

Observe that the kernel of ϕ is (id) because (id) is the only element of

$$V_4 \cap S_3.$$

Thus ϕ is an injection.[24]

An injective function from a six element set to a six element set is necessarily surjective. □

Example 6.12. Let $T = \{x_1, x_2, x_3\}$ be a set with three variables. Consider the polynomial $\Delta = (x_2 - x_1)(x_3 - x_1)(x_3 - x_2)$ in $\mathbb{Z}[x_1, x_2, x_3]$. Observe that if $\sigma \in \mathrm{Sym}(T)$, then $\sigma(\Delta)$ is equal to either Δ or $-\Delta$. Indeed σ is also an element of $\mathrm{Sym}\{\Delta, -\Delta\}$. Let T' be the name of the set $\{\Delta, -\Delta\}$. Observe that

$$\phi : \mathrm{Sym}(T) \to \mathrm{Sym}(T'),$$

given by $\phi(\sigma) = \sigma|_{T'}$, is a legitimate group homomorphism. Observe that ϕ is onto. Observe that the kernel of ϕ is

$$A_3 = \left\{ \begin{pmatrix} x_1 & x_2 & x_3 \\ x_2 & x_3 & x_1 \end{pmatrix}, \quad \begin{pmatrix} x_1 & x_2 & x_3 \\ x_3 & x_1 & x_2 \end{pmatrix}, \quad \begin{pmatrix} x_1 & x_2 & x_3 \\ x_1 & x_2 & x_3 \end{pmatrix} \right\}.$$

Conclude that $\frac{S_3}{A_3} \cong S_2$.

Problem 6.13. Mimic Example 6.12 in the situation where $T = \{x_1, x_2, x_3, x_4\}$. Which polynomial plays the role of Δ? Which elements of $\mathrm{Sym}(T)$ are in the kernel of ϕ. You might find it helpful to use cycle notation as described in section 7.A.

Example 6.14. Recall that $\mathrm{O}_n(\mathbb{R}) = \{M \in \mathrm{GL}_n(\mathbb{R}) \mid MM^{\mathrm{T}} = \mathrm{id}\}$. It follows that if $M \in \mathrm{O}_n(\mathbb{R})$, then $\det M$ is equal to 1 or -1. Recall, also that $\mathrm{SO}_n(\mathbb{R})$ is the subgroup of $\mathrm{O}_n(\mathbb{R})$, which consists of all matrices of determinant 1. Then the groups $\frac{\mathrm{O}_n(\mathbb{R})}{\mathrm{SO}_n(\mathbb{R})}$ and U_2 are isomorphic.

[23] If N is a normal subgroup of the group G, then the function $\phi : G \to \frac{G}{N}$, which is given by $\phi(g) = \bar{g}$, for all $g \in G$, is a group homomorphism. This homomorphism is called the natural quotient map.

[24] Have I ever said out loud that the homomorphism ϕ is an injection if and only if the kernel of ϕ consists of the identity element? At any rate, it is true, easy to prove, and very useful.

Proof. Define $\phi : \mathrm{O}_n(\mathbb{R}) \to U_2$ by $\phi(M) = \det M$ for $M \in \mathrm{O}_n(\mathbb{R})$. Apply the First Isomorphism Theorem. □

Definition 6.15. Let $(G_1, *_1), \ldots, (G_n, *_n)$ be groups. Then the direct product of $G_1, \ldots, G_n$ is the group $(\prod_{i=1}^n G_i, *)$ or $(G_1 \times G_2 \times \cdots \times G_n, *)$. The elements of $\prod_{i=1}^n G_i$ are n-tuples $(g_1, \ldots, g_n)$ with $g_i \in G_i$, the operation in $(\prod_{i=1}^n G_i, *)$ is

$$(g_1, \ldots, g_n) * (g_1', \ldots, g_n') = (g_1 *_1 g_1', g_2 *_2 g_2', \ldots, g_n *_n g_n').$$

Remark 6.16. The direct product of $G_1, \ldots, G_n$ is also called the direct sum of $G_1, \ldots, G_n$. If one is using the name direct sum, one would usually write

$$\bigoplus_{i=1}^n G_i = G_1 \oplus \ldots \oplus G_n.$$

One can form the direct product and direct sum of infinitely many groups; however when one has infinitely many groups then the direct product and the direct sum are no longer the same.

Example 6.17. The following 5 groups all have order 8. None of these groups are isomorphic to any other group in the list:

$$\frac{\mathbb{Z}}{\langle 8\rangle}, \quad \frac{\mathbb{Z}}{\langle 4\rangle} \oplus \frac{\mathbb{Z}}{\langle 2\rangle}, \quad \frac{\mathbb{Z}}{\langle 2\rangle} \oplus \frac{\mathbb{Z}}{\langle 2\rangle} \oplus \frac{\mathbb{Z}}{\langle 2\rangle}, \quad D_4, \quad \text{and} \quad Q_8,$$

where Q_8 is the Quaternion group of Example 5.9.

Problem 6.18. Prove that none of the above groups are isomorphic to any other group on the list. Keep in mind that if two groups are isomorphic, then either they are both Abelian or they are both non-Abelian. Also keep in mind that if two groups are isomorphic then they both have the same number of order j for each j.

Example 6.19. If r and s are relatively prime integers[25] then

$$\frac{\mathbb{Z}}{rs\mathbb{Z}} \cong \frac{\mathbb{Z}}{r\mathbb{Z}} \oplus \frac{\mathbb{Z}}{s\mathbb{Z}}.$$

This assertion is usually called the Chinese Remainder Theorem.

Lemma 6.19.1. *If r and s are integers with greatest common divisor [26] d, then there exist integers a and b with $ar + bs = d$.*

Proof. We proved in Proposition 4.2 that the smallest subgroup of $\mathbb{Z}$ that contains r and s, denoted $\langle r, s\rangle$, is cyclic. Let t be the name of the generator; so $\langle r, s\rangle = \langle t\rangle$. The integer $-t$ also generates $\langle r, s\rangle$. So change t to negative t, if necessary. We may assume that t is positive and $\langle r, s\rangle = \langle t\rangle$. The fact that $t \in \langle r, s\rangle$ ensures that $t = ar + bs$ for some integers a and b. We need only show that t is the greatest

[25] The integers r and s are relatively prime if their greatest common divisor is 1. Recall the definition of greatest common divisor from Definition 4.5.

[26] Recall the definition of "greatest common divisor" from Definition 4.5. In particular, the greatest integer that divides both r and s is the greatest common divisor of r and s.

common divisor of a and b. The fact that $\langle r,s\rangle \subseteq \langle t\rangle$ ensures that t is a common factor of r and s. On the other hand, the equation $t = ar + bs$ guarantees that every common factor of r and s also divides t. $\square$

Now prove the assertion of (6.19). Define $\phi : \mathbb{Z} \to \frac{\mathbb{Z}}{r\mathbb{Z}} \oplus \frac{\mathbb{Z}}{s\mathbb{Z}}$ by $\phi(n) = (\bar{n}, \bar{n})$. Observe that ϕ is a homomorphism.

We prove that ϕ is surjective. We know from Lemma 6.19.1 that there are integers a and b with $ra + bs = 1$. Observe that $\phi(1 - ar) = (\bar{1}, \bar{0})$ and $\phi(1 - bs) = (\bar{0}, \bar{1})$. Every element in the target can be written in terms of $(\bar{1}, \bar{0})$ and $(\bar{0}, \bar{1})$. We conclude that ϕ is surjective.

Observe that $\langle rs\rangle \subseteq \ker\phi$. Apply the first part of the First Isomorphism Theorem to conclude that

$$\bar{\phi} : \frac{\mathbb{Z}}{\langle rs\rangle} \to \frac{\mathbb{Z}}{r\mathbb{Z}} \oplus \frac{\mathbb{Z}}{s\mathbb{Z}}$$

is a group homomorphism. A surjective function from a set with rs elements to a set with rs elements is necessarily injective.

7. Cycle notation for permutations, even and odd permutations, the Alternating group A_n, and A_4 does not have a subgroup of order six.

7.A. **Cycle notation.** When we write

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 1 & 3 & 2 & 4 \end{pmatrix} \quad \text{and} \quad \tau = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 2 & 1 \end{pmatrix},$$

we write way too much (There is no need to write the top line and isn't there a better way to say that σ does not move either 1 or 4.) and we have NO INSIGHT into what the permutations are doing.

I now propose that we write σ as $(2,3)$ and τ as $(1,4)(2,3)$. The idea is that $(2,3)$ says $2 \mapsto 3 \mapsto 2$ and nothing else happens and $(1,4)(2,3)$ means that

$$1 \mapsto 4 \mapsto 1, \quad 2 \mapsto 3 \mapsto 2, \quad \text{and} \quad \text{nothing else happens.}$$

In a similar manner in cycle notation

$$\begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 4 & 1 & 5 \end{pmatrix}$$

is written as $(1,2,3,4)$ which means

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

The symbols

$$(2,3), \quad (1,4), \quad \text{and} \quad (1,2,3,4)$$

are each known as cycles.

A cycle with j entries has order j. Disjoint cycles commute.

Every element of S_n can be written as a product of disjoint cycles.

Example 7.1. Write $(1,3,5)(4,1,7)(3,2,6)$ as a product of disjoint cycles. Here is my thinking:

$$\begin{aligned} &1 \mapsto 7 \\ &7 \mapsto 4 \\ &4 \mapsto 1 \mapsto 3 \\ &3 \mapsto 2 \\ &2 \mapsto 6 \\ &6 \mapsto 3 \mapsto 5 \\ &5 \mapsto 1 \end{aligned}$$

So, $(1,3,5)(4,1,7)(3,2,6) = (1,7,4,3,2,6,5)$.

7.B. **Every permutation in S_n is equal to a product of transpositions.**

Definition 7.2. A transposition is a 2-cycle.

Proof. Observe that

$$(1,2,3,\ldots,r) = (1,r)(1,r-1)\cdots(1,4)(1,3)(1,2).$$

□

7.C. **The notion of even and odd permutation makes sense.**

Observation 7.3. *Suppose that permutation σ in S_n is a product of a transpositions and also is a product of b transpositions. We claim that a and b are both even or a and b are both odd.*

Proof. It suffices to show that $(-1)^a = (-1)^b$. Consider the homomorphism

$$\phi : \mathrm{Sym}(\{x_1, \ldots, x_n\}) \to \mathrm{Sym}(\{\Delta, -\Delta\})$$

of Example 6.12, where

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

Claim 7.4. *If (k,ℓ) in S_n, then $(k,\ell)\Delta = -\Delta$.*

Proof of claim. It does no harm to assume that $k < \ell$. Observe that

$$\Delta = \Big(\prod_{\substack{i<j \\ \{i,j\}\cap\{k,\ell\}=\emptyset}} (x_j - x_i) \Big) \Big(\prod_{i<k} (x_k - x_i)(x_\ell - x_i) \Big) \Big(\prod_{k<i<\ell} (x_i - x_k)(x_\ell - x_i) \Big) \Big(\prod_{\ell<i} (x_i - x_\ell)(x_i - x_k) \Big) (x_\ell - x_k).$$

$$(k,\ell)(\Delta) = \Big(\prod_{\substack{i<j \\ \{i,j\}\cap\{k,\ell\}=\emptyset}} (x_j - x_i) \Big) \Big(\prod_{i<k} (x_\ell - x_i)(x_k - x_i) \Big) \Big(\prod_{k<i<\ell} (x_i - x_\ell)(x_k - x_i) \Big) \Big(\prod_{\ell<i} (x_i - x_k)(x_i - x_\ell) \Big) (x_\ell - x_k).$$

The four factors inside $\Big(\quad \Big)$ remain unchanged. The factor $(x_\ell - x_k)$ has changed to $(x_k - x_\ell) = -(x_\ell - x_k)$. The claim is established. □

The observation follows readily, because

$$\sigma(\Delta) = (-1)^a \Delta \quad \text{and} \quad \sigma(\Delta) = (-1)^b \Delta.$$

The polynomial Δ in $\mathbb{Z}[x_1, \ldots, x_n]$ is not identically zero; hence $(-1)^a = (-1)^b$, as desired. □

Definition 7.5. If the element σ of S_n is equal to the product of an even number of transpositions, then σ is called an even permutation and if σ is equal to the product of an odd number of transpositions, then σ is called an odd permutation.

7.D. **Define the Alternating group and calculate its order.**

Definition 7.6. The alternating group A_n is the following subgroup of S_n:

$$A_n = \{\sigma \in S_n | \sigma \text{ is an even permutation}\}.$$

Observation 7.7. *If $2 \leq n$, then A_n has order $\frac{n!}{2}$.*

Proof. All of the odd permutations of S_n are in the coset $(1,2)A_n$. Indeed, S_n is the disjoint union of the cosets $(1)A_n \cup (1,2)A_n$. We saw, when we proved Lagrange's Theorem that all cosets of A_n in S_n have the same number of elements. It follows that the order of A_n is $\frac{1}{2}$ the order of S_n. (Of course, S_n has $n!$ elements.) □

7.E. **Calculate $\sigma(a_1,\dots,a_r)\sigma^{-1}$ and observe that the Klein 4-group is a normal subgroup of S_4.**

Observation 7.8. *If σ and $(a_1,\dots,a_r)$ are permutations in S_n, then*

$$\sigma(a_1,\dots,a_r)\sigma^{-1} = (\sigma(a_1),\dots,\sigma(a_r)).$$

Proof. Observe that $\sigma(a_1,\dots,a_r)\sigma^{-1}$ and $(\sigma(a_1),\dots,\sigma(a_r))$ are the exact same function. Each one sends $\sigma(a_i)$ to $\sigma(a_{i+1})$ for $1 \le i \le r-1$, $\sigma(a_r)$ to $\sigma(a_1)$, and leaves

$$\{1,\dots,n\} \setminus \{\sigma(a_1),\dots,\sigma(a_r)\}$$

completely alone. □

Example 7.9. The subgroup $V_4 = \{(1),(1,2)(3,4),(1,3)(2,4),(1,4)(2,3)\}$ of S_4 is closed under conjugation. In other words, if $\sigma \in S_4$ and $\tau \in V_4$, then $\sigma\tau\sigma^{-1}$ is in V_4.

Question 7.10. *Prove that A_4 does not have a subgroup of order six.*

7.F. **Loose ends.** There are a few loose ends that I would like to tie up today.

1. How do we know that none of the groups
$$\frac{\mathbb{Z}}{\langle 8\rangle}, \quad \frac{\mathbb{Z}}{\langle 4\rangle} \oplus \frac{\mathbb{Z}}{\langle 2\rangle}, \quad \frac{\mathbb{Z}}{\langle 2\rangle} \oplus \frac{\mathbb{Z}}{\langle 2\rangle} \oplus \frac{\mathbb{Z}}{\langle 2\rangle}, \quad D_4, \quad \text{and} \quad Q_8,$$
are isomorphic to any other group on the list? (This is Problem 6.22 from the class notes.)
2. How do we know that if σ is in S_n and σ is the product of a transpositions and σ is also the product of b transpositions, then a and b are both even or both odd? (This is the point of Problem 6.17 from the class notes.)
3. How do we know that $V_4 = \{(12)(34),(13)(24),(14)(23),(1)\}$ is a normal subgroup of S_4? (It is obvious that V_4 is a subgroup of S_4. The question is how do we know that V_4 is closed by conjugation by elements of S_4.) (I promised this in the class notes in Example 6.15.)
4. How do we know that A_4 does not have any subgroups of order six? (I first told you this as an example of why the converse of Lagrange's Theorem is not true. This is the smallest such example.)
5. How do we know that the subgroup of S_4 generated by $\sigma = (12)$ and $\tau = (1234)$ is all of S_4? (I first asked you this in HW 0.c.iii. It is still messy; but at least you have a hope using cycle notation.)

We get to work.

1. The groups $\frac{\mathbb{Z}}{\langle 8\rangle}$, $\frac{\mathbb{Z}}{\langle 4\rangle} \oplus \frac{\mathbb{Z}}{\langle 2\rangle}$, and $\frac{\mathbb{Z}}{\langle 2\rangle} \oplus \frac{\mathbb{Z}}{\langle 2\rangle} \oplus \frac{\mathbb{Z}}{\langle 2\rangle}$ are Abelian. The groups D_4 and Q_8 are not Abelian. If two groups are isomorphic then they are both Abelian or neither one is Abelian.

The group $\frac{\mathbb{Z}}{\langle 8\rangle}$ has an element of order 8; neither of the groups $\frac{\mathbb{Z}}{\langle 4\rangle}\oplus\frac{\mathbb{Z}}{\langle 2\rangle}$ nor $\frac{\mathbb{Z}}{\langle 2\rangle}\oplus\frac{\mathbb{Z}}{\langle 2\rangle}\oplus\frac{\mathbb{Z}}{\langle 2\rangle}$ has an element of order 8.

The group $\frac{\mathbb{Z}}{\langle 4\rangle}\oplus\frac{\mathbb{Z}}{\langle 2\rangle}$ has an element of order four, but $\frac{\mathbb{Z}}{\langle 2\rangle}\oplus\frac{\mathbb{Z}}{\langle 2\rangle}\oplus\frac{\mathbb{Z}}{\langle 2\rangle}$ does not have an element of order four.

The group D_4 has many elements of order two. The group Q_8 has only one element of order two.

2. This is Observation 7.3 from above.

Observation. 7.3 *Suppose that permutation σ in S_n is a product of a transpositions and also is a product of b transpositions. We claim that a and b are both even or a and b are both odd.*

Proof. It suffices to show that $(-1)^a=(-1)^b$. Consider the homomorphism

$$\phi:\mathrm{Sym}(\{x_1,\dots,x_n\})\to\mathrm{Sym}(\{\Delta,-\Delta\})$$

of Example 6.12, where

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

Claim. *If (k,ℓ) in S_n, then $(k,\ell)\Delta=-\Delta$.*

Proof of claim. It does no harm to assume that $k<\ell$. Observe that

$$\Delta=\Big(\prod_{\substack{i<j\\ \{i,j\}\cap\{k,\ell\}=\emptyset}}(x_j-x_i)\Big)\Big(\prod_{i<k}(x_k-x_i)(x_\ell-x_i)\Big)\Big(\prod_{k<i<\ell}(x_i-x_k)(x_\ell-x_i)\Big)\Big(\prod_{\ell<i}(x_i-x_\ell)(x_i-x_k)\Big)(x_\ell-x_k).$$

$$(k,\ell)(\Delta)=\Big(\prod_{\substack{i<j\\ \{i,j\}\cap\{k,\ell\}=\emptyset}}(x_j-x_i)\Big)\Big(\prod_{i<k}(x_\ell-x_i)(x_k-x_i)\Big)\Big(\prod_{k<i<\ell}(x_i-x_\ell)(x_k-x_i)\Big)\Big(\prod_{\ell<i}(x_i-x_k)(x_i-x_\ell)\Big)(x_\ell-x_k).$$

The four factors inside $\Big(\ \Big)$ remain unchanged. The factor $(x_\ell-x_k)$ has changed to $(x_k-x_\ell)=-(x_\ell-x_k)$. The claim is established. □

The observation follows readily, because

$$\sigma(\Delta)=(-1)^a\Delta\quad\text{and}\quad\sigma(\Delta)=(-1)^b\Delta.$$

The polynomial Δ in $\mathbb{Z}[x_1,\dots,x_n]$ is not identically zero; hence $(-1)^a=(-1)^b$, as desired. □

3. We must show that V_4 is closed under conjugation. But this is obvious: $\sigma(1)\sigma^{-1}=(1)\in V_4$ and

$$\sigma(ab)(cd)\sigma^{-1}=(\sigma(a)\sigma(b))(\sigma(c)\sigma(d)),$$

which is in V_4 for all $\{a,b,c,d\}=\{1,2,3,4\}$ and all σ in S_4.

4. The group A_4 has twelve elements; namely

$$(1),(123),(132),(124),(142),(134),(143),(234),(243),(12)(34),(13)(24),(14)(23).$$

We argue by contradiction. Suppose that H is a subgroup of A_4 of order 6, then H has index 2 in A_4; consequently, H is a normal subgroup of A_4. The subgroup H must contain a three cycle (because all of the elements of A_4, except 4 are three cycles.) So, $\sigma = (i, j, k) \in H$ for three distinct integers i, j, k between 1 and 4 and $\sigma^{-1} = (ikj) \in H$. Let ℓ be the fourth integer between 1 and 4. Observe that

$$(i\ell j)(ijk)(ij\ell) = (ik\ell) \in H$$

and

$$(ik\ell)^{-1} = (i\ell k) \in H.$$

Similarly,

$$(i\ell j)(i\ell k)(ij\ell) = (jk\ell) \in H$$

and

$$(jk\ell)^{-1} = (j\ell k) \in H.$$

At this point H contains at least 7 elements. We have reached a contradiction; because H contains exactly six elements.

We conclude that H does not exist.

5. Let H be the smallest subgroup of S_4 which contains $\sigma = (12)$ and $\tau = (1234)$. We show that all six transpositions (ij) are in H. Every element of S_4 is a product of transpositions.

Keep in mind that $(1234)^{-1} = (1432)$.

Observe that

$$\begin{aligned}
(1432)(12)(1234) &= (14) \in H, \\
(1432)(14)(1234) &= (34) \in H, \\
(1432)(34)(1234) &= (23) \in H, \\
(14)(12)(14) &= (24) \in H, \text{ and} \\
(23)(12)(23) &= (13) \in H.
\end{aligned}$$

The proof is complete.

8. Rings and Fields.

Definition 8.1. Let $(R,+,\times)$ be a set on with two operations. These operations are called "addition" and "multiplication". Then R is a ring if the following properties hold:

(i) $(R,+)$ is an Abelian group, (The additive identity is usually called 0.)
(ii) multiplication in R associates,
(iii) R has a multiplicative identity, (usually called 1)
(iv) and the distributive law

$$(a+b)c = ac+bc \quad \text{and} \quad a(b+c) = ab+ac$$

holds.

If multiplication commutes in R, then R is called a commutative ring.

If R is a commutative ring and $(R\setminus\{0\},\times)$ is an Abelian group, then R is called a field.

Examples 8.2. (1) $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ all are commutative rings. Indeed, $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$ all are fields. The ring $\mathbb{Z}$ is not a field.

(2) $\frac{\mathbb{Z}}{\langle n\rangle}$ is a commutative ring. We better make sure that multiplication makes sense. That is, if a,b,c,d are integers, $a+\langle n\rangle = b+\langle n\rangle$ in $\frac{\mathbb{Z}}{\langle n\rangle}$, and $c+\langle n\rangle = d+\langle n\rangle$ in $\frac{\mathbb{Z}}{\langle n\rangle}$, then

$$ac+\langle n\rangle = ad+\langle n\rangle$$

in $\frac{\mathbb{Z}}{\langle n\rangle}$.

Proof. The hypothesis $a+\langle n\rangle = b+\langle n\rangle$ guarantees that $a = b+rn$ for some integer r. The hypothesis that $c+\langle n\rangle = d+\langle n\rangle$ guarantees that $c = d+sn$ for some integer s. It follows that

$$ac = (b+rn)(d+sn) = bd+n(rd+sb+rsn);$$

and therefore, $ac+\langle n\rangle = bd+\langle n\rangle$, as desired. □

(3) If R is a commutative ring, then $R[x]$, which is the set of polynomials

$$\{r_0+r_1x+\cdots+r_nx^n \mid r_i \in R\},$$

is also a commutative ring.

(4) If R is a commutative ring then and r is an element of R, then r is called a unit if r has a multiplicative inverse in R. If R is a commutative ring, then the set of units in R is a group.

Question: For example, what is the group of units in $\frac{\mathbb{Z}}{\langle 6\rangle}$?

Answer: $\{1+\langle 6\rangle, 5+\langle 6\rangle\}$. This group is cyclic of order two. The element $5+\langle 6\rangle$ generates the group.

Question: What is the group of units in $\frac{\mathbb{Z}}{\langle 5\rangle}$?

Answer: $\{1+\langle 5\rangle, 2+\langle 5\rangle, 3+\langle 5\rangle, 4+\langle 5\rangle\}$. This group is cyclic and is generated by $u = 2+\langle 5\rangle$. Indeed, $u^2 = 4+\langle 5\rangle$, $u^3 = 3+\langle 5\rangle$, $u^4 = 1+\langle 5\rangle$. So, $\frac{\mathbb{Z}}{\langle 5\rangle}$ is a field with 5 elements. (In fact, every finite field has p^n elements for some positive prime integer p and some positive integer n. Furthermore, up to isomorphism, there is exactly one field with p^n elements.)

Question: What is the group of units in $\frac{\mathbb{Z}}{\langle 12\rangle}$?

Answer: $\{1+\langle 12\rangle, 5+\langle 12\rangle, 7+\langle 12\rangle, 11+\langle 12\rangle\}$. This is a Klein four-group.

(5) The ring $\mathrm{Mat}_{2\times 2}(R)$ is a non-commutative ring, for any commutative ring R. The elements of $\mathrm{Mat}_{2\times 2}(R)$ are the two by two matrices with entries from R.

(6) I will show you the field with 4 elements. Start with $\frac{\mathbb{Z}}{\langle 2\rangle}$. Write $\bar{0}$ instead of $0+\langle 2\rangle$ and $\bar{1}$ instead of $1+\langle 2\rangle$. Let R be the polynomial ring $\frac{\mathbb{Z}}{\langle 2\rangle}[x]$. The elements of $R = \frac{\mathbb{Z}}{\langle 2\rangle}[x]$ are polynomials of the form $\bar{a}_0 + \bar{a}_1 x + \cdots + \bar{a}_n x^n$, where each a_i is either 0 or one. Let f be the polynomial $x^2 + x + \bar{1}$ in R. (I picked f to be a polynomial of degree 2 which does not have any roots in $\frac{\mathbb{Z}}{\langle 2\rangle}$.) Let $(fR, +)$ be the subgroup $fR = \{fg \mid g \in R\}$ of $(R, +)$. Observe that the set of cosets

$$\frac{R}{fR}$$

is a ring. (As always we need to make sure that multiplication makes sense. Suppose r_1 and r_2 are elements of R with the cosets $r_1 + fR$ and $r_2 + fR$ equal and r_3 and r_4 are elements of R with the cosets $r_3 + fR$ and $r_4 + fR$ equal. We must show that the cosets

$$r_1 r_3 + fR \quad \text{and} \quad r_2 r_4 + fR$$

are equal. Of course, this is not hard. The hypothesis $r_1 + fR = r_2 + fR$ in $\frac{R}{fR}$ guarantees that there is an element h_1 in R with $r_1 = r_2 + fh_1$. The hypothesis that $r_3 + fR = r_4 + fR$ are equal in $\frac{R}{fR}$ guarantees that there is an element h_2 in R with $r_3 = r_4 + fh_2$. Now we see that

$$r_1 r_3 = (r_2 + fh_1)(r_4 + fh_2) = r_2 r_4 + f(h_1 r_4 + r_2 h_2 + fh_1 h_2);$$

hence the cosets $r_1 r_3 + fR$ and $r_2 r_4 + fR$ are equal in $\frac{R}{fR}$.)

Notice that $\frac{R}{fR}$ has exactly four elements. These elements are $\bar{0} + fR$, $\bar{1} + fR$, $\bar{1}x + fR$, and $\bar{1} + \bar{1}x + fR$. Observe that $(\frac{R}{fR}, +)$ is a Klein 4-group and $(\frac{R}{fR} \setminus \{0\}, \times)$ is a cyclic group of order three. Indeed,

$$(x + fR) \times (x + fR) = x^2 + fR = x + 1 + fR \quad \text{and}$$

$$(x + fR) \times (x + 1 + fR) = x^2 + x + fR = 1 + fR.$$

So $\frac{R}{fR}$ is a (actually the) field with 4 elements. It is usually called $\mathbb{GF}(4)$, the Galois Field with 4 elements. One constructs the Galois Field $\mathbb{GF}(p^n)$ with p^n elements in a similar manner for all positive prime integers p and all positive integers n.

I copied this sentence from Wikipedia: "Finite fields are fundamental in a number of areas of mathematics and computer science, including number theory, algebraic geometry, Galois theory, finite geometry, cryptography and coding theory."

REFERENCES

[1] M. Artin, *Algebra*, Prentice Hall, Inc., Englewood Cliffs, NJ, 1991.
[2] J. Beachy and W Blair, *Abstract Algebra* Book by John A. Beachy and William D. Blair