8/19 Fall 2024, Howard Math 210

Modern Algebra I (1st semester graduate algebra)

Instructor: Sam Hopkins, sam.hopkins@howard.edu

Website: samuelfhopkins.com/classes/210.html

=

Class info:

- Meets MW 11:10 am - 12:30 pm in Douglass Hall #212
- Office Hrs: Tue 12-1pm or by appointment in Annex III #220 (email me to set up a time!)
- Text: Hungerford "Algebra" (email me if you need help getting a copy!)
- Grading: 40% 6 homeworks
  20% 2 inperson midterm exams
  20% one final exam

Collaboration on HWs is encouraged, but not on exams. Other than doing the assignments, I expect you to show up to class and participate. ☺

=

What is this class about?

You might think: algebra is a method for solving equations like

$$5x + 7y - 3z = 10.$$

Certainly linear algebra (which I assume you have taken a class in) is about solving linear equations. More generally commutative algebra concerns itself with polynomial equations like

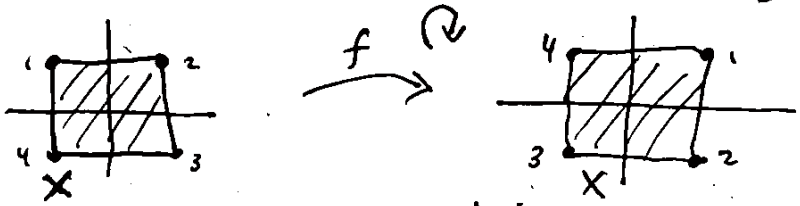
$$10x^3 - 2xy + 5x - 3y = 7.$$

Equations like this will be in the back of our mind during this semester (and we may return to them next semester), but since the 19th century algebra has evolved to be much more than a method for solving equations, and it is this "modern algebra" we will study this semester.

Modern algebra studies abstract mathematical objects defined by axioms, and attempts to classify them and understand their structure. These abstract objects capture disparate mathematical phenomena, and a key insight of modern algebra is that generalization is a powerful tool in math.

The first algebraic objects we will study are groups. Rather than give you the formal definition of a group right now, let me discuss where they come from. Given any mathematical object X, we can consider the collection $\mathrm{Aut}(X) = \{f: X \to X \mid f \text{ preserves the structure of } X\}$ of structure-preserving maps from X to itself, which is called the automorphism group of X.

For example, if X is a square in the plane, then one element of $\mathrm{Aut}(X)$ is rotation by 90° CCW:



Another automorphism would be rotation by 180°. And $\mathrm{Aut}(X)$ is more than just a set of maps, because we can compose two automorphisms to get another automorphism. For example, rotating by 90° twice is the same as rotating 180°. It is this composition product which gives $\mathrm{Aut}(X)$ the structure of a group.

But $\mathrm{Aut}(X)$ makes sense not just when X is a geometric object like a square, but also for differential eqn's, dynamical systems, etc. And can study all of these at once!

An important subfamily of groups, the abelian groups, serve a dual purpose as "counter systems" (think: tally marks) and lead to the other major algebraic structure we will study this semester: rings. Rings are abstractions of the number systems we are familiar with like the integers $\mathbb{Z}$, the rational numbers $\mathbb{Q}$, the real numbers $\mathbb{R}$, the complex numbers $\mathbb{C}$, etc. Rings have two operations: addition $+$ and multiplication $\times$.

For any family of algebraic structures (groups, rings, etc.), a very fruitful approach to understanding their structure is to study the structure-preserving maps between the members of this family. For example, we could try to map the symmetries of a 3-dimensional object to the symmetries of a 2D object:

$$\mathrm{Aut}\left(\text{  }\right) \longrightarrow \mathrm{Aut}\left(\text{}\right)$$

The collection of all structure-preserving maps between members of a family of mathematical objects form a category, and we may talk a little about categories in our study of groups and rings.

Modern algebra can be highly abstract, and it can be difficult to "visualize" the arguments we will make using the axioms. To counteract this, we will try to provide many concrete examples along the way. We will especially be interested in finite structures, which are already very interesting. When you feel stuck, seeing what things look like in a concrete, finite example is always a good idea!

Preliminaries: Logic, Sets, functions, etc. (Hungerford's Intro)

Before we can introduce any algebraic structures, we need to review some preliminary material.

Logic A proposition is a statement that is either true or false but not both like "7 is a prime number" or "2+2=5." Given two propositions p, q we can form compound propositions "p and q" ($p \wedge q$) and "p or q" ($p \vee q$), with $p \wedge q$ being true when both p and q are true, and $p \vee q$ being true when at least one of p or q is true. The conditional $p \Rightarrow q$ ("if p then q" or "p implies q") is true unless p is false but q is true. "Not p" ($\neg p$) is true if p is false and false if p is true.

We will also use quantified statements of form $\forall x\ P(x)$ ("for all x in some domain of discourse, $P(x)$") or $\exists x\ P(x)$ ("there exists x such that $P(x)$") where $P(x)$ is a propositional formula. The meaning of these statements will be clear in context.

In general, I expect you to have some familiarity with basic mathematical proofs, including proof by contradiction and proof by induction. Proof-writing will be an important part of the class.

Sets Sets are the most basic mathematical objects. A set is a collection of objects. A set can be finite like $X = \{1, 2, 3\}$ or infinite like $\mathbb{N} = \{0, 1, 2, \ldots\}$. The notation $a \in X$ means that a is an element of X (belongs to X).

There is a formal, axiomatic approach to set theory where we define the universe of all sets in terms of the membership relation $\in$. But this is not a set theory course so we will not be so formal.

The important thing is what sets are there and especially what can we do with sets, how do we construct them.

First of all, two sets A and B are equal if and only if they have the same elements in them:

$$A = B \iff \forall x \quad x \in A \iff x \in B.$$

There is one special set called the empty set, denoted $\emptyset = \{\}$ that has no elements in it.

Sets can have other sets as elements. For instance, $X = \{\emptyset\}$ is a set, which is distinct from $\emptyset$ itself. (In fact, in the formal approach to set theory, all the elements of sets are in turn sets.)

Given two sets X and Y we can form their union $X \cup Y$, which is everything in X or in Y, and their intersection $X \cap Y$, everything in both X and in Y.

In fact, if A_i for $i \in I$ is any collection of sets indexed by some other set I, we can form the union $\bigcup_{i \in I} A_i$, which is everything in any A_i for some $i \in I$ and the intersection $\bigcap_{i \in I} A_i$ which is everything in all A_i for all $i \in I$.

E.g. Letting $A_n = [\frac{-1}{n}, \frac{1}{n}]$, a subset of real numbers in $\mathbb{R}$ for each $n \in \{1, 2, 3, \ldots\}$, we have $\bigcap_n A_n = \{0\}$.

Let us recall that we say A is a subset of B, written $A \subseteq B$, if for every x in A, also $x \in B$. Given any set A we can form its power set $\mathcal{P}(A)$, which is the set of all subsets of A.

E.g. if $A = \{1,2\}$ then $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{1,2\}\}$.

You are probably used to "set-builder notation", where we write things like

$A \cup B = \{x : x \in A \text{ or } x \in B\}$, $\mathcal{P}(A) = \{S : S \subseteq A\}$, etc.

Formally, the axiom of comprehension allows us to (try*) to form the set

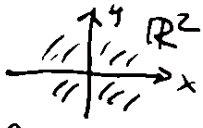
$X = \{A : P(A)\}$ where $P(A)$ is a propositional formula.

WARNING* Consider the "set"

$X = \{A : A \text{ is a set and } A \notin A\}$.

Do we have $X \in X$? If not, then we should, but if we do, then we shouldn't! This is called Russell's Paradox and shows that a very naive approach to set theory is flawed. Nevertheless, we only run into risks from things like Russell's paradox when we try to do "very infinite" constructions involving classes like all the sets. So from now on we will ignore this issue and use comprehension/set-builder notation in an unrestricted way.

One further set-theoretic construction is very useful. An ordered pair is something of the form (a, b), where order matters so that $(a, b) \neq (b, a)$ unless $a = b$. The (Cartesian) product $A \times B$ of two sets A and B is the set $A \times B = \{(a, b) : a \in A, b \in B\}$ of all ordered pairs where the 1st element is in A, 2nd element is in B.

E.g. $\mathbb{R} \times \mathbb{R} = \mathbb{R}^2$ is the usual Cartesian plane: 

If $A_1, A_2, \ldots, A_n$ are n sets we can likewise form the product $A_1 \times A_2 \times \cdots \times A_n$ consisting of all ordered n-tuples $(a_1, a_2, \ldots, a_n)$ with $a_i \in A_i$ $\forall i$.

In fact, if A_i for $i \in I$ is any collection of sets indexed by some set I we can also make sense of the product $\prod_{i \in I} A_i$, as we'll see below...

Functions A function $f: A \to B$ from one set A to another set B assigns to each $a \in A$ exactly one element $f(a) \in B$. The graph of $f: A \to B$ is $\{(a, f(a)) : a \in A\} \subseteq A \times B$. We can identify a function with its graph; under this identification a function $f: A \to B$ is any subset of $A \times B$ with the property that for each $a \in A$ there is exactly one $b \in B$ such that (a, b) is in the subset.

Notice how an ordered pair $(a, b) \in A \times B$ can be identified with a function $f: \{1, 2\} \to A \cup B$ such that $f(1) \in A$ and $f(2) \in B$. This identification

allows us to define $\prod_{i \in I} A_i$ (where A_i are sets indexed by $i \in I$) as the set of all functions $f: I \to \bigcup_{i \in I} A_i$ such that $f(i) \in A_i$ $\forall$ i.

The Axiom of Choice asserts that if $A_i \neq \emptyset$ $\forall i \in I$ then $\prod_{i \in I} A_i \neq \emptyset$ as well. In other words, the Axiom of Choice says that if all the A_i are nonempty, then we can "simultaneously" pick an element $a_i \in A_i$ for all of them. It is known that that the Axiom of Choice is independent of the other usual axioms of set theory. It's worth paying attention to when the axiom of choice is used because it is inherently "non-constructive" (you can't program a computer to do it). Nevertheless, we will freely use the axiom of choice without much commentary because it is needed for basic statements in algebra such as "Every vector space has a basis." Like with Russell's Paradox, it is only with "very infinite" constructions that there is an issue where the axiom of choice is really needed, and again the focus is on finite/concrete things in our class.

Riddle: Why is the axiom of choice needed to select one sock from an infinite # of pairs of socks, but not to select one shoe from ∞-many pairs of shoes?

8/21

Give a function $g: X \to Y$ and a function $f: Y \to Z$ we can form their composition $f \circ g: X \to Z$ given by $(f \circ g)(x) = f(g(x))$ for all $x \in X$.

E.g. If $f: \mathbb{Z} \to \mathbb{Z}$ is given by $f(x) = x^2 + 2x - 1$ and $g: \mathbb{Z} \to \mathbb{Z}$ is given by $g(x) = 3x + 2$ then $(f \circ g)(x) = (3x+2)^2 + 2(3x+2) - 1 = 9x^2 + 18x + 7$.

Importantly, composition of functions is associative:

$(f \circ g) \circ h = f \circ (g \circ h)$ $\forall$ $f: Y \to Z$, $g: X \to Y$, $h: W \to X$

We will discuss associativity much more soon...

There is a special function, the identity function $Id_X: X \to X$ for any set X, which is given by $Id_X(x) = x$ $\forall$ $x \in X$.

The identity function "gives you back what you put in."

A function $f: X \to Y$ is injective (or one-to-one) if $f(a) = f(b) \Rightarrow a = b$ for all $a, b \in X$.

A function $f: X \to Y$ is surjective (or onto) if for every $y \in Y$ there is some $x \in X$ with $f(x) = y$.

Theorem Let $f: X \to Y$ be a function with $X \neq \emptyset$.

i) f is injective if and only if it has a left inverse, i.e. there is $g: Y \to X$ with $g \circ f = Id_X$.

ii) f is surjective if and only if it has a right inverse, i.e. there is $h: Y \to X$ with $f \circ h = Id_Y$.

Proof: i). Let's prove the $\Rightarrow$ direction: if f is injective it has a left inverse g. The other direction is an (easy) exercise for you.
First, choose any $a_0 \in X$. We define $g: Y \to X$ by

$$g(b) = \begin{cases} \text{the unique } a \text{ with } f(a)=b & \text{if } b \text{ is in the image of } f \\ a_0 & \text{otherwise.} \end{cases}$$

Recall that the image of $f: X \to Y$ is the set of b such that $f(a)=b$ for some $a \in X$. Then we check that $(g \circ f)(a) = g(f(a)) = g(b) = a$ for all $a \in X$, so indeed g is a left-inverse of f.

ii): Again let's prove the $\Rightarrow$ direction, leaving the $\Leftarrow$ direction as an exercise. For each $b \in Y$, choose some $a \in X$ with $f(a)=b$ (this requires the axiom of choice!) and define $h: Y \to X$ by $h(b)=a$ for these choices for all $b \in Y$.
It is again easy to check $(f \circ h)(b) = b$ for all $b \in Y$, so h is a right-inverse of f as claimed. ☒

A function $f: X \to Y$ is a bijection if it is both an injection and a surjection.

Corollary A function $f: X \to Y$ between two nonempty sets X and Y is a bijection if and only if it has a two-sided inverse, i.e. there is $g: Y \to X$ with $g \circ f = Id_X$ and $f \circ g = Id_Y$.

Pf: Exercise for you to fill in details... ☒

Number systems As mentioned, we use notation
$\mathbb{N} = \{0, 1, 2, \ldots\}$ for the natural numbers (book does differently)
$\mathbb{Z} = \{\ldots, -1, 0, 1, 2, \ldots\}$ for the integers,
$\mathbb{Q} = \{\frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0\}$ for the rationals,
and $\mathbb{R} =$ for the reals.
We will not formally develop the theory of these number systems from scratch, but let us recall some important properties of the integers, especially regarding addition and multiplication.

Addition for $\mathbb{Z}$:
- is associative: $(a+b)+c = a+(b+c) \quad \forall a, b, c \in \mathbb{Z}$
- has an identity $0 \in \mathbb{Z}$: $a + 0 = 0 + a = a \quad \forall a \in \mathbb{Z}$
- has inverses $-a$: $a + (-a) = (-a) + a = 0 \quad \forall a \in \mathbb{Z}$
- is commutative: $a + b = b + a \quad \forall a, b \in \mathbb{Z}$.

Multiplication for $\mathbb{Z}$:
- is associative: $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b, c \in \mathbb{Z}$
- has an identity $1 \in \mathbb{Z}$: $a \cdot 1 = 1 \cdot a = a \quad \forall a \in \mathbb{Z}$
- distributes over addition: $a \cdot (b+c) = (a \cdot b) + (a \cdot c)$, $(b+c) \cdot a = (b \cdot a) + (c \cdot a) \quad \forall a, b, c \in \mathbb{Z}$
- is commutative: $a \cdot b = b \cdot a \quad \forall a, b \in \mathbb{Z}$.

These properties mean that $(\mathbb{Z}, +, \cdot)$ is a (commutative) ring.

One more thing about integers to recall:
$a = r \bmod n$ means $\exists k \in \mathbb{Z}$ such that
$a \cdot k + r = n$,
i.e. r is the remainder we get when dividing a by n.

Groups (Chapter 2 of Hungerford)

§1.1 Let G be a set. A binary operation $\cdot$ on G is a map $\cdot : G \times G \to G$. We usually write $\cdot$ "multiplicatively" and write $g \cdot h$ for image of $(g,h) \in G \times G$, but sometimes we write the operation "additively" as $g+h$ instead. We use usual notation for multiplication like $g^2 = g \cdot g$ and so on.

Def'n Let $G = (G, \cdot)$ be a set with a binary operation.

i) G is a semigroup if the product $\cdot$ is associative, $(a \cdot b) \cdot c = a \cdot (b \cdot c) \quad \forall a, b, c \in G$.

ii) G is a monoid if it is a semigroup and there exists an identity element $e \in G$: $a \cdot e = e \cdot a = a \quad \forall a \in G$.

iii) G is a group if it is a monoid and for each $a \in G$ there is an inverse element a^{-1} satisfying $a \cdot a^{-1} = a^{-1} \cdot a = e$.

iv) If G is a semigroup/monoid/group we say it is abelian (or commutative) if $a \cdot b = b \cdot a$ for all $a, b \in G$.

E.g. $\mathbb{Z}_{>0} = \{1, 2, 3, \ldots\}$ with addition $+$ forms a commutative semigroup, $\mathbb{N}$ with $+$ forms a commutative monoid (0 is the identity), and $\mathbb{Z}$ with $+$ (or $\mathbb{Q}$ w/ $+$ or $\mathbb{R}$ w/ $+$) forms an abelian group. For this reason abelian groups often use additive instead of multiplicative notation.

Theorem Let G be a monoid and suppose e_1 and $e_2 \in G$ are both identity elements. Then $e_1 = e_2$. In other words, the identity is unique.

Pf: Since e_1 is an identity, $e_1 a = a$ for all $a \in G$, in particular $e_1 e_2 = e_2$. But since e_2 is an identity, $a e_2 = a$ for all $a \in G$, in particular $e_1 e_2 = e_1$. So $e_1 = e_1 e_2 = e_2$. ☒

Remark Same argument shows that if $(G, \cdot)$ has a "right-identity" e_1 and a "left-identity" e_2 then $e_1 = e_2$ is a two-sided identity (and is unique)!

Theorem Let G be a group. Then for each $g \in G$ its inverse g^{-1} is unique.

Pf: Exercise for you. Similar to previous thm. ☒

Another exercise for you is to show that if G is a semigroup and we have any list $a_1, a_2, \ldots, a_n$ of elements of G (allowing repetition), then any way we parenthesize the product

$$a_1 \cdot a_2 \cdot \cdots \cdot a_n$$

evaluates to the same answer, so we don't have to write any parentheses.

Eg: $((a_1 \cdot a_2) \cdot a_3) \cdot a_4) = ((a_1 \cdot a_2) \cdot (a_3 \cdot a_4)) = (a_1 \cdot (a_2 \cdot (a_3 \cdot a_4)))$

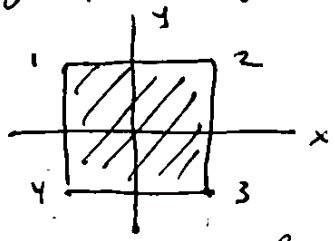
Similarly, if G is an abelian semigroup then

$$a_1 + a_2 + \cdots + a_n = a_{\sigma(1)} + a_{\sigma(2)} + \cdots + a_{\sigma(n)}$$

for any permutation σ of $1, 2, \ldots, n$.

Some examples of groups to have in mind:

E.g. Consider the group of "symmetries of a square":



In other words, functions from this square to itself that preserve distances between points. Call the collection of these symmetries D_4 (for "dihedral") and note $D_4 = \{e, R_{90°}, R_{180°}, R_{270°}, F_x, F_y, F_{13}, F_{24}\}$, where e is the identity, $R_{90°}$ = rotation by 90° ← clockwise, etc., F_x = flip over x-axis, F_{13} = flip over diagonal, etc. Then D_4 is a group if we define $g \cdot h = g \circ h$ for $g, h \in D_4$. E.g. $F_x \cdot R_{90°} = F_{24}$ and $R_{90°} \cdot F_x = F_{13}$, so D_4 is not abelian. Note each $g \in D_4$ is determined by where it sends the vertices 1, 2, 3, 4.

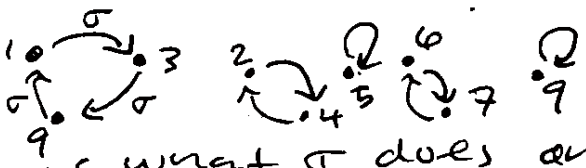
8/26 E.g. Let X be any set. Let $\mathrm{Sym}(X)$ denote the set of all bijections $f: X \to X$, which we make into a group by letting $g \cdot h = g \circ h$ for $g, h \in \mathrm{Sym}(X)$. This is called the Symmetric group on the set X. If X is infinite, then $\mathrm{Sym}(X)$ is infinite. But if X is finite, then $\mathrm{Sym}(X)$ is finite, and we may as well take $X = \{1, 2, \ldots, n\}$ and then we denote $S_n = \mathrm{Sym}(X)$, the n^{th} finite Symmetric group.

Def'n If G is a finite group, its **order** is the cardinality of G as a set, i.e., the # of elements of G.

The order of the symmetric group S_n is $n!$. This is because we can view the elements of S_n as **permutations** of $\{1, 2, 3, \ldots, n\}$. Recall that we can write a permutation $\sigma \in S_n$ in **two-line notation** as $\sigma = \begin{pmatrix} 1 & 2 & 3 & \cdots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \cdots & \sigma(n) \end{pmatrix}$. For example

$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\ 3 & 4 & 9 & 2 & 5 & 7 & 6 & 8 & 1 \end{pmatrix} \in S_9$ sends 1 to 3, 2 to 4, etc.

We can represent this same permutation as a *functional digraph*:



where the arrow tells us what σ does and in this way we see (exercise) that every permutation also decomposes as a disjoint union of **cycles** $a_1 \to a_2 \to \cdots \to a_k$, leading to **cycle notation**.

$\sigma = (1, 3, 9)(2, 4)(5)(6, 7)(8)$ in our example says one 3-cycle in σ is $1 \to 3 \to 9$, etc.

E.g. Let $\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = (1, 2, 3) \in S_3$.
and $\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = (1, 2)(3)$

Then $\pi\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ ≠

and $\sigma\pi = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$,

So S_3 is also non-abelian (it is the smallest non-abelian group).

Quotient groups

Recall that a (binary) relation R on a set X is any subset of $X \times X$, where we write xRy for $x, y \in X$ to mean (x,y) is in our subset ("x is related to y").
An equivalence relation R on X satisfies:

- reflexivity: $xRx \quad \forall x \in X$
- symmetry: $xRy \Leftrightarrow yRx \quad \forall x, y \in X$
- transitivity: xRy and $yRz \Rightarrow xRz \quad \forall x, y, z \in X$.

Given an equivalence relation R on X, the equivalence class of $a \in X$, denoted $\bar{a} = \{b \in X : aRb\}$, is all elements related to a.
The equivalence classes of R partition the set X.

Theorem Let G be a semigroup and suppose $\sim$ is an equivalence relation such that whenever $b_1 \sim b_2$, $a_1 \sim a_2$ then $a_1 b_1 \sim a_2 b_2$ for all $a_1, a_2, b_1, b_2 \in G$.
Then the set of equivalence classes of $\sim$ on G, $G/\sim$, has a semigroup structure where $\bar{a} \cdot \bar{b} = \overline{ab}$.
If G is a monoid, then so is $G/\sim$ with identity $\bar{e}$.
If G is a group, then so is $G/\sim$ with $\bar{g}^{-1} = \overline{g^{-1}}$ $\forall g \in G$.
Pf: Straightforward exercise.

E.g. Consider the group $(\mathbb{Z}, +)$. Let $n \in \{1, 2, 3, \ldots\}$ and define the equivalence relation $\sim$ on $\mathbb{Z}$ where $a \sim b$ is $a - b \equiv 0 \bmod n$ (i.e. $a \equiv b \bmod n$).
Then $\sim$ satisfies the above theorem's condition, so $(\mathbb{Z}/\sim, +)$ is a group, which we denote $\mathbb{Z}/n\mathbb{Z}$.

Recall that $\{0, 1, 2, \ldots, n-1\}$ are representatives of the equivalence classes of $\sim$, and we can understand the group structure of $\mathbb{Z}/n\mathbb{Z}$ in terms of "modular arithmetic" (or "clock arithmetic") on $\{0, 1, 2, \ldots, n-1\}$: $a + b = c$ if $a + b \equiv c \bmod n$.

In particular, note that $\mathbb{Z}/n\mathbb{Z}$ is a finite group of order n. It is an abelian group, of course.

Product groups

Def'n Given two groups G and H, their direct product $G \times H$ is the group with elements in $G \times H$ and with $(g_1, h_1) \cdot (g_2, h_2) = (g_1 g_2, h_1 h_2)$.

The identity is (e_G, e_H), the inverses are $(g, h)^{-1} = (g^{-1}, h^{-1})$.

In the case when G and H are abelian, we also call this construction the direct sum and denote the group by $G \oplus H$.

Def'n Two groups G and H are isomorphic if there is a bijection $\varphi : G \to H$ such that $\varphi(x \cdot y) = \varphi(x) \cdot \varphi(y)$ $\forall x, y \in G$.

i.e. they have the "same group structure."

Write $G \cong H$ if G is isomorphic to H.

If G, H are finite groups of order n and m, respectively, then $G \times H$ is finite of order $n \cdot m$.

Exercise Show $\mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$.

Exercise Is $\mathbb{Z}/4\mathbb{Z}$ isomorphic to $\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$?

Explain why or why not!

Homomorphisms (§1.2 of Hungerford)

Def'n A map $\varphi: G \to H$ between two groups (or semigroups...) G and H is called a homomorphism if $\varphi(ab) = \varphi(a)\varphi(b)$ $\forall a, b \in G$. If φ is injective it is called a monomorphism, if it is surjective it is called an epimorphism, and if it is bijective it is called an isomorphism.

It is easy to see that if $f: G \to H$ and $g: H \to K$ are homomorphisms, then so is $g \circ f: G \to K$. (We will see later that this means groups form a category...)

A key idea in algebra is: to understand an algebraic object, understand maps to/from it that are structure-preserving.

8/28

E.g. For any $n \in \mathbb{Z}_{>0}$, there is the canonical epimorphism $\varphi: \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$ given by $\varphi(x) = \overline{x}$ $\forall x \in \mathbb{Z}$. We will see later this is true for all "quotient groups."

E.g. For any $n, k \in \mathbb{Z}_{>0}$, there is a monomorphism $\varphi: \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/kn\mathbb{Z}$ given by $\varphi(\overline{x}) = \varphi(\overline{kx})$ $\forall \overline{x} \in \mathbb{Z}/n\mathbb{Z}$.

A monomorphism can be seen as a way of embedding the "multiplication table" of one group G into another H:

$n=3, k=2$

$\mathbb{Z}/3\mathbb{Z} \hookrightarrow$

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

$\mathbb{Z}/6\mathbb{Z}$ ↵

+	0	1	2	3	4	5
0	0	1	2	3	4	5
1	1	2	3	4	5	0
2	2	3	4	5	0	1
3	3	4	5	0	1	2
4	4	5	0	1	2	3
5	5	0	1	2	3	4

Defn A homomorphism $\varphi: G \to G$ from a group G to itself is called an endomorphism, and if it is an isomorphism it is called an automorphism.

There is always the "trivial" automorphism $Id: G \to G$ (identity map) for any G.

E.g. If G is an abelian group, then $x \mapsto x^n$ (or $x \mapsto n \cdot x$ in additive notation) is an endomorphism of G, for any $n \in \mathbb{Z}$. For $n = -1$, $x \mapsto x^{-1}$ (or $x \mapsto -x$ in additive notation) is an automorphism

Exercise: Show that for any group G, the collection of automorphisms of G, denoted $Aut(G)$, forms a group where the product is composition.

Defn Let $\varphi: G \to H$ be a homomorphism between groups G and H.
The image of φ, $Im(\varphi)$, is the set $\{\varphi(x) : x \in G\} \subseteq H$.
The kernel of φ, $Ker(\varphi)$, is the set $\{x \in G : \varphi(x) = e\} \subseteq G$.

Theorem Let $\varphi: G \to H$ be a homomorphism.
i) φ is an epimorphism iff $Im(\varphi) = H$.
ii) φ is a monomorphism iff $Ker(\varphi) = \{e\}$.

Proof: i) is clear from the definitions.
For ii): Note that we must have $\varphi(e) = e$ because $\varphi(e)$ is an identity of H and the identity is unique.
So if $\varphi(g) = e$ for some $g \neq e$, then φ is not injective.
Conversely, if $\varphi(g) = \varphi(h)$, then $\varphi(gh^{-1}) = \varphi(g)\varphi(h^{-1}) = \varphi(g)\varphi(h)^{-1}$ (since $\varphi(h^{-1}) = \varphi(h)^{-1}$ because inverses are unique)
$= e$, so if $gh^{-1} \neq e$, i.e., $g \neq h$, then $Ker(\varphi) \neq \{e\}$. ☒

Theorem $\varphi: G \to H$ is an isomorphism iff there is a two-sided inverse homomorphism $\varphi^{-1}: H \to G$.

Proof: Exercise. ☒

Subgroups (still § 1.2 of Hungerford)

Def'n A subset $H \subseteq G$ of a group G is called a subgroup of G if H is a group with the product from G.
Concretely, this means that H is closed under multiplication, and $e \in H$ and $g^{-1} \in H$ for all $g \in H$.
(The uniqueness of the identity means the identity for H must be the same as that for G.)
We write $H \leq G$ to mean H is a subgroup of G.

E.g.: For any $n \in \mathbb{Z}_{>0}$, $n\mathbb{Z} = \{n \cdot x : x \in \mathbb{Z}\} \subseteq \mathbb{Z}$ is a subgroup of $\mathbb{Z}$.

The trivial group $H = \{e\}$ and the whole group G are always subgroups of any group G. Other subgroups are called proper subgroups.

E.g.: Both $\{0, 3\}$ and $\{0, 2, 4\}$ are proper subgroups of $\mathbb{Z}/6\mathbb{Z} = \{0, 1, 2, 3, 4, 5\}$.

E.g.: $\mathbb{Z}/p\mathbb{Z}$ has no proper subgroups if p is a prime. (Proving this is an exercise for you.)

Theorem. If $\varphi : G \to H$ is a homomorphism, then $\varphi(K)$ is a subgroup for any subgroup $K \leq G$. In particular $\mathrm{Im}(\varphi) \leq H$ is a subgroup of H. Also $\ker(\varphi) \leq G$ is a subgroup of G.

Proof: There are straightforward checks based on the definition. Let's do the kernel claim. Suppose $g, h \in G$ satisfy $\varphi(g) = \varphi(h) = e$. Then $\varphi(gh) = \varphi(g)\varphi(h) = e \cdot e = e$, so also $gh \in \ker(\varphi)$. Similarly $g^{-1} \in \ker(\varphi)$ if $g \in \ker(\varphi)$, and $e \in \ker(\varphi)$. ☐

Note: We will see later that $\ker(\varphi) \leq G$ is a special kind of subgroup, a normal subgroup.

Theorem If H_i for $i \in I$ are subgroups $H_i \leq G$ of a group G, then their intersection $\bigcap_{i \in I} H_i$ is a subgroup.

Proof: Exercise ☐

Def'n For any set $A \subseteq G$, the subgroup generated by A, denoted $\langle A \rangle$, is $\bigcap_{i \in I} H_i$ where the H_i are all subgroups containing A.

In other words, $\langle A \rangle$ is the "smallest" subgroup of G containing A.

Theorem $\langle A \rangle = \{ x_1^{n_1} x_2^{n_2} \cdots x_k^{n_k} : x_1, \ldots x_k \in A, n_1, \ldots, n_k \in \mathbb{Z} \}$

Proof sketch: Show that this collection is a subgroup (i.e. closed under product) and every subgroup of G containing A must contain it. ☐

Corollary For a single element $x \in G$, $\langle x \rangle = \{ x^n : n \in \mathbb{Z} \}$.

Groups generated by a single element are called cyclic ...

9/4

Cyclic Groups (§1.3 of Hungerford)

Def'n A group G is called cyclic if it is generated by a single element, i.e., $G = \langle x \rangle$ for some $x \in G$.

Theorem Every cyclic group is isomorphic to $\mathbb{Z}$ (if it is infinite) or to $\mathbb{Z}/n\mathbb{Z}$ for some $n \geq 1$ (if it's finite).

Proof: Easy exercise - see the book. First step is to realize $G = \{x^n : n \in \mathbb{Z}\}$, then think about the smallest $n \geq 1$ such that $x^n = 1$ (if it exists). □

Def'n Let G be any group and $x \in G$ any element. The **order** of x is the size of the cyclic subgroup $\langle x \rangle \leq G$ generated by x, it is either in $\{1, 2, 3, 4, \ldots\}$ or ∞.

Theorem The order of x is the smallest $n \geq 1$ such that $x^n = 1$, if it is finite or ∞ otherwise.

Proof: Again a simple exercise. See the book. □

Theorem Every subgroup of a cyclic group and every homomorphic image of a cyclic group is again a cyclic group.

Proof: once again, exercise, see the book □

So cyclic groups have a very simple structure and are easily classified. We might hope that e.g. groups that are generated by two elements are classifiable, but this is far from true! E.g., S_n is generated by two elements (not obvious!) //

Cosets and Counting (Section §1.4 of Hungerford)

We extend the idea of $a \equiv b \bmod n$ for $a, b \in \mathbb{Z}$ to any groups.

Def'n Let G be a group and $H \leq G$ a subgroup. For $a, b \in G$ we say a is *right congruent to b modulo H*, $a \equiv_R b \bmod H$, if $ab^{-1} \in H$, and a is *left congruent to b modulo H*, $a \equiv_L b \bmod H$, if $b^{-1}a \in H$. Right/left congruence modulo H are equivalence relations on G, and the equiv. class of $a \in G$ under right (resp. left) congruence modulo H is $Ha = \{ha : h \in H\}$ (resp. $aH = \{ah : h \in H\}$). The sets Ha for $a \in G$ (resp. aH) are called the *right cosets* (resp. *left cosets*) of the subgroup H.

Note: For abelian groups G, right/left congruence modulo any subgroup $H \leq G$ define same equiv. relation. For some nonabelian groups G and subgroups $H \leq G$, $\equiv_R^{\bmod H}$ and $\equiv_L^{\bmod H}$ coincide, and for others they are distinct.

Note: Each right (left) coset Ha (aH) has size $|Ha| = |H|$ ($|aH| = |H|$) because all the ha (ah) are distinct.

Example For $G = \mathbb{Z}$ and $H = n\mathbb{Z} \leq G$, $\equiv_L^{\bmod H}$ and $\equiv_R^{\bmod H}$ define the usual $\equiv \bmod n$ relation on the integers.

E.g. Let $G = S_3$ and $H_1 = \langle (12) \rangle = \{e, (12)\} \leq G$. The right cosets are $\{e, (12)\}$, $\{(13), (132)\}$, $\{(23), (123)\}$ while the left cosets are $\{e, (12)\}$, $\{(13), (123)\}$, $\{(23), (132)\}$ which are not the same.

E.g. Again let $G = S_3$ but now let $H = \langle (123) \rangle = \{e, (123), (132)\} \leq G$.
The right and left cosets of H are $\{e, (123), (132)\}$, $\{(12), (13), (23)\}$, they are the same (even though G is not abelian).

Proposition Let G be a group and $H \leq G$ a subgroup.
i) The right (resp. left) cosets of H partition G, i.e., every $g \in G$ belongs to exactly one right (resp. left) coset of H.
ii) If $\mathcal{R}$ is set of all distinct right cosets of H, and $\mathcal{L}$ is —"— of left cosets of H, then $Ha \mapsto a^{-1}H$ defines a bijection $\mathcal{R} \leftrightarrow \mathcal{L}$, so $|\mathcal{R}| = |\mathcal{L}|$.

Proof: i) is the same as saying right/left congruence is an equiv. relation.
ii) follow from the fact that $Ha = Hb \Leftrightarrow ab^{-1} \in H$ and $aH = bH \Leftrightarrow a^{-1}b \in H$. ∎

Def'n Let G be a group and $H \leq G$ a subgroup. The index of H in G, denoted $[G:H]$ is the cardinality of the set of distinct right (or left) cosets of H.

E.g. For $G = \mathbb{Z}$ and $H = n\mathbb{Z} \leq \mathbb{Z}$, $[G:H] = n$.
Note how $[G:H]$ is finite here even though G and H are infinite.

E.g. For any group G, if we let $H = \{e\} \leq G$ (trivial subgroup) then the right/left cosets are $\{a\}$ for $a \in G$, so if G is infinite then $[G:H]$ is infinite too.

A complete set of right (resp. left) coset representatives for $H \leq G$ is a choice of a unique $a \in G$ in each right (left) coset of H. So we pick $[G:H]$ representatives.

Theorem If $K \leq H \leq G$ are groups (w/ H a subgroup of G & K a subgroup of H), then $[G:K] = [G:H][H:K]$. If 2 of these numbers are finite, the third one is as well.

Proof: Choose a complete set of representatives a_i, $i \in [G:H]$ for the right cosets of H in G, and b_j, $j \in [H:K]$ for the right cosets of K in H. Thus $G = \bigcup_{i \in [G:H]} Ha_i$ and $H = \bigcup_{j \in [H:K]} Kb_j$ so $G = \bigcup_{i \in [G:H]} \left(\bigcup_{j \in [H:K]} Kb_j \right) a_i$, that is, $G = \bigcup_{(i,j) \in [G:H] \times [H:K]} Kb_j a_i$. So it suffices to show that all the $Kb_j a_i$ for $(i,j) \in [G:H] \times [H:K]$ are disjoint.

Suppose $Kb_j a_i = Kb_{j'} a_{i'}$, then $b_j a_i = k b_{j'} a_{i'}$ for some $k \in K$.

But since b_j, $b_{j'}$ and k are all in H, we have that $Ha_i = Hb_j a_i = HkB_{j'} a_{i'} = Ha_{i'}$. Thus $i = i'$. And then $b_j = k b_{j'}$ so $Kb_j = Kk b_{j'} = Kb_{j'}$ and thus $j = j'$. ∎

Corollary (Lagrange's Theorem)
For any $H \leq G$ we have $|G| = [G:H]\,|H|$, so $[G:H] = \frac{|G|}{|H|}$ if G is finite. In particular, for G finite the order of any $g \in G$ divides $|G|$.

Proof: Previous theorem with $K = \langle e \rangle$. Then take $H = \langle g \rangle$. ∎

E.g.: The orders of the elements in S_3 are 1 (for e), 2 (for (12), (23), (13)) and 3 (for (123) and (132)), which all divide $G = 3! = \#S_3$. Note that no element has order 6.

Exercise Show that all divisors of n are orders of elements of $\mathbb{Z}/n\mathbb{Z}$.

∎