Math 113, Fall 2019

Lecture 1, Thursday, 8/29/2019

CLASS ANNOUNCEMENTS:

Homework due Sept 5, in-class:
§0 : 9, 12, 16, 17, 26, 32, 34
§1 : 3, 8, 22, 25, 30, 32, 26
Readings for Tuesday: §0, 1, 2
iClickers required for the course, starting Tuesday.

Topics Today:

- Introduction
- Basics of Sets
- Functions
- Cardinalities
- Relations (if time permits)

1 Syllabus

Instructor: Paul Vojta (vojta@math.berkeley.edu)
(pronounced 'Voyta')

Lectures: T/Th 12:30-2pm, Etcheverry 3107
(https://math.berkeley.edu/ vojta/113.html)

OH: T/TH 10:30am - 12pm

Course Description: Sets and relations. The integers, congruences, and the Fundamental Theorem of Arithmetic. Groups and their factor groups. Commutative rings, ideals, and quotient fields. The theory of polynomials: Euclidean algorithm and unique factorizations. The Fundamental Theorem of Algebra. Fields and field extensions.

Textbook Sections: 0-11, 13-16, 18-23, 26, 27, 29-31, 45-47, 32, 34.

Homeworks: Due weekly on Thursdays, physical copy in class.
Comment: "I tend to follow the book rather closely, but try to give interesting exercises and examples."

2 Grading

20%	Homework	Assigned weekly	Due in class, usually on Thursdays
20%	First midterm	TBD	12:30–2:00 pm
25%	Second midterm	TBD	12:30–2:00 pm
35%	Final exam	Friday, December 20	8:00–11:00 am

3 Quoting Results: Homeworks

General rules on homework assignments are:

- For any assigned problem from the book, you may use without proof any earlier exercise in the book.
- For an assigned problem not from the book, you may use without proof any exercise in the book that occurs in or before the section containing the most recent problem from the book in the assignment prior to the problem.
- When doing a problem from a given section of the book, you may not use material from subsequent sections of the book (even if problems from those sections are also in the homework assignment). (For problems not from the book, use the principle in the previous bullet point.)

4 Brief Overview of the Course:

We'll be talking about Groups, Rings, Fields abstractly. We should already know the sets

$$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$$

and notice that we define:

$$\mathbb{N} := \{0, 1, \dots\},$$

as opposed to in Math 104.
Further, in $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$, if we only look at $+$ and $-$ (ignore $\times, /$, inequalities, limits, $\frac{d}{dx}$, $\int$) then these are **examples of groups**.

4.1 Other Examples of Groups

- $n \times m$ matrices, equipped with $+$ or $-$.
- Vector Spaces (ignoring scalar multiplication)
- $n \times n$ **invertible** matrices with matrix multiplication.
  - We say that AB^{-1} takes the role of subtraction in this group (non-commutative).
- nonzero real numbers under $\times, /$

4.2 Examples of Rings

The sets $\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$ with $+, -, \times$ are examples of **rings**. Other examples include $n \times n$ matrices. The sets $\mathbb{Q}, \mathbb{R}, \mathbb{C}$ with $+, -, \times, /$ are examples of **fields**. We can think of polynomials as rings too.

5 A Word About Abstraction:

In Math 54, we definied an **abstract vector space**, assumed to have the operation of .
To study the solutions of a rubrics cube, we can use group theory. Alternatively, the 15-puzzle of 4×4 locations and one missing square, where we slide around tiles to get a particular pattern.

Vojta gives the example that if we start with

$$\begin{bmatrix} 15 & 14 & 13 & 12 \\ 11 & 10 & 9 & 8 \\ 7 & 6 & 5 & 4 \\ 3 & 1 & 2 & \times \end{bmatrix}$$

(with exactly two with order swapped), then it turns out we **cannot** get this to pure descending order as below

$$\begin{bmatrix} 15 & 14 & 13 & 12 \\ 11 & 10 & 9 & 8 \\ 7 & 6 & 5 & 4 \\ 3 & 2 & 1 & \times \end{bmatrix}$$

We'll see why this is the case via Group Theory.

6 Introductory Material

We should already know the sets:

$$\mathbb{Z}, \mathbb{Q}, \mathbb{R}, \mathbb{C}$$

and the symbols:

$$\forall, \exists, \cup, \cap, \in, \notin, \subseteq, \subset, \supset, \supseteq$$

Vojta notes that he uses $\subsetneq$ and $\supsetneq$ for $\subset, \supset$, respectively.
We also have that

$$\bigcup_{i=1}^{n} A_i = A_1 \cup A_2 \cup \cdots \cup A_n$$

where A_i are all sets. Similarly for intersections $\cap$.
Also,

$$\bigcup_{i \in I} A_i = \{x | x \in A_i \text{ for some } i\} = \{x | \exists_{i \in I} : x \in A_i\}$$

where I and A_i are sets $\forall_{i \in I}$, we may take a union over an **indexing set** I.
So,

$$\bigcup_{i=1}^{n} A_i = \bigcup_{i \in \{1,\ldots,n\}} A_i,$$

where n can be ∞.

6.1 What if $I = \{\}$?

Looking at our above definition $\{x | \exists_{i \in I} : x \in A_i\}$, we see this condition can never be satisfied.
However, consider:

$$\bigcap_{i \in I} = \{x : x \in A_i \forall_{i \in I}\}$$

and notice this works for $I := \{\}$. This is problematic (as can be seen from a logic course), so we use that if $A_i \subseteq X \forall_i$, then

$$\bigcap_{i \in I} A_i = X \setminus \cup_{i \in I} (X \setminus A_i) \text{ if } I \neq \{\}$$

If $I = \{\}$, the answer depends on X. Usually we can tell from the context what X is.

Break time.

Vojta enters break-time, distributing a handout on sets, relations, and partitions (although we likely won't get to partitions today).

Definition: Well Defined -

- Uniquely defined (independent of any choices made)
- Is the sort of object that it is claimed to be

For example of violating the first, an empty intersection is **not** uniquely defined because it depends on the choice of X. We can make this uniquely defined by specifying X.
A qualifying example is the dimension of a vector space, where we prove that every vector space has at least one basis, and show that the dimension is unique regardless the choice of basis.

Definition: Cartesian Product -

The Cartesian product of sets A and B is:

$$A \times B := \{(a, b) : a \in A \text{ and } b \in B\},$$

and we can also write this as:

$$\prod_{i=1}^{n} A_i \text{ or } \underbrace{\prod_{i \in I} A_i}_{},$$

where this is a set of 'set of choice functions' $\phi : I \to \cup A_i$ such that $\phi(i) \in A_i \forall_i$. Note that these are ordered pairs.

Definition: Functions -

Let A, B be sets. A **function** $f : A \to B$ is a subset $\Gamma \subseteq A \times B$ with the following property:

$$\forall_{a \in A}, \exists!_{b \in B} : (a, b) \in \Gamma$$

which is essentially the vertical line test. This element is denoted as $f(a)$. Here, A is called the **domain** of f, and B is called the **codomain** of f.

We say that Γ is the **graph** of f, and $f[A] := \{f(a) : a \in A\}$ is called the **range** of f.

Example:

$$f = \{(x, \sin x) : x \in \mathbb{R}\} \subseteq \mathbb{R} \times \mathbb{R}$$
$$x \overset{f}{\mapsto} \sin x$$

is a function from $\mathbb{R}$ to $\mathbb{R}$. We write this as $f : \mathbb{R} \to \mathbb{R}$.
In this example, we say that Γ is the graph of f with range $= [-1, 1]$ (the interval).
We should also know **injective, surjective, bijective** functions.

Definition: Injective -

A one-to-one function is an injective function, and we also call this an injection. This is such that

$$f(x) \neq f(y), \forall_{x \neq y}$$

in the domain.

Definition: Surjective -

An onto function is a surjective function, and we also call this a surjection. This is such that

$$\text{range of } f = \text{codomain}$$

Definition: Bijective -

A function that is both injective and surjective is said to be **bijective**.

Definition: Inverse Functions -

If $f : A \to B$ is a bijective function, then it has an **inverse function**

$$g = f^{-1} : B \to A,$$

characterized by $f(a) = b \iff g(b) = a, \forall_{a \in A, b \in B}$, or by $f \circ g = \mathrm{id}_B$ which is the identity function $b \mapsto f(g(b))$, and $g \circ f = \mathrm{id}_A$.

7 Cardinalities:

Definition: Cardinality -

Sets A and B have the same **cardinality** if and only if there is a **bijection** from $A \to B$.

Remark: Vojta notes that in definitions, we'll usually simply state 'if' to mean 'if and only if'. However, in these notes I will make an effort for clarity sake to explicitly write 'if and only if' in this case.

Example: One can show: Let $m, n \in \mathbb{N}$. Then the sets $\{1, 2, \ldots, m\}$ and $\{1, 2, \ldots, n\}$ have the same cardinality if and only if $m = n$. (For our purposes, we define that if $m, n = 0$, then this is the empty set.)

We can make the following definition:

Definition: Finite -

A set is **finite** if it has the same cardinality as $\{1, 2, \ldots, n\}$ for some $n \in \mathbb{N}$. If so, then we say that the set is **finite**, and that the number of elements is n. (This is well-defined and agrees with common usage).

Continuing with this definition, if a set is not finite, then it is **infinite**.

Remark: Here $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ are all **infinite**. $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$ all have the same cardinality, and $\mathbb{N}, \mathbb{R}$ **do not** have the same cardinality (proved in 55 or 104).

The following definition is **different from what is given in the book**:

Definition: Relation $\mathcal{R}$ -

A **relation** on a set S is a subset $\mathcal{R}$ of $S \times S$.

Lecture ends here.

Math 113, Fall 2019
Lecture 2, Tuesday, 9/3/2019

Topics Today:

- Relations, Equivalence Relations, and Partitions
- Multiplication on the Unit Circle in $\mathbb{C}$.
- Binary Algebraic Structures (time permitting)

Readings for Thursday: up to and including page 40.

1 iClicker Question

In simplest terms, $(1+i)(2+3i)$ is:
(a) $2+5i+3i^2$
(b) $5+5i$
(c) $-1+5i$
(d) $3+4i$
(e) I don't have an iclicker yet.

And for the second question,

$$4 +_{2\pi} 5 = \boxed{9-2\pi},$$

where we omit the other answer selections.

2 Relations

Definition: Relation -

A relation $\mathcal{R}$ on a set S is a subset $\mathcal{R}$ of $S \times S$. For $x, y \in S$, we write:

$$x \mathcal{R} y$$

if the pair $(x, y) \in S$.

Of course, 'if' in a definition means 'if and only if'. As examples, for any set S, $x \mathcal{R} y$ if $x = y$ is a relation. If $S = \mathbb{R}$, then "$<$" is a relation on $\mathbb{R}$: $x \mathcal{R} y$ if $x < y$.

Let σ be a collection of sets (set of sets). Then "$\subseteq$" is a relation on σ. We say that $A \mathcal{R} B$ if $A \subseteq B$.

2.1 Same Cardinality as a Relation

For the same collection Σ "having the same cardinality" is a relation on Σ. That is,

$$A \mathcal{R} B \text{ if there is a bijection } A \to B.$$

There are certain kinds of relations that play a special role in this class, and let's start with:

Definition: Reflexive, Symmetric, Transitive -

Let $\mathcal{R}$ be a relation on set S. Then $\mathcal{R}$ is:
(1) **reflexive** if $x \mathcal{R} x$, $\forall_{x \in S}$
(2) **symmetric** if $x \mathcal{R} y \implies y \mathcal{R} x$, $\forall_{x,y \in S}$
(3) **transitive** if the **conjunction** of $x \mathcal{R} y$ and $y \mathcal{R} z$ implies $x \mathcal{R} z$, $\forall_{x,y,z \in S}$.

Example: Consider $<$ on $\mathbb{R}$. Surely this is not reflexive because no number is less than itself. Additionally, it is not symmetric; however,it is transitive. Now taking $\leq$ on $\mathbb{R}$, we have reflexivity and transitivity; however, symmetry fails.

Example: The relation 'have the same cardinality' (where $S := \Sigma$ is a collection of sets). We go back to the definition:

$$A \mathcal{R} B \text{ if there is a bijection } A \to B,$$

and to see reflexivity, for all $A \in \Sigma$, the **identity map** is a bijection $A \to A$ with:

$$\mathrm{id_A(x) = x}, \ \forall_{\mathrm{x \in A}}.$$

Now for symmetry, of course the wording implies yes; however, we need to revisit the definition. If A, B have the same cardinality, do B, A have the same cardinality? If A, B have the same cardinality, then this implies that there exists a bijection $f : A \to B$ which implies $f^{-1} : B \to A$ is also a bijection (left as an exercise), which implies that B, A have the same cardinality.
To see transitivity, if A, B have the same cardinality, and B, C have the same cardinality, then there exist the following:

$$f : A \to B, \quad g : B \to C,$$

and $g \circ f : A \to C$ is a bijection (left as an exercise). Therefore A, C have the same cardinality.

Definition: Equivalence Relation -

We say that an **equivalence relation** on a set S is a relation (on S) which satisfies (1) reflexivity, (2) symmetry, and (3) transitivity.

Example: (1) 'Have the same cardinality' is an equivalence relation (on any collection of sets).
(2) '$<$' on $\mathbb{R}$ is **not** an equivalence relation.
(3) For any set S, '$=$' is an equivalence relation.
(4) And slightly more generally, let S be a set and take $f : S \to T$ be a function, and define a relation $\sim$ (pronounced 'twiddle') on S by

$$x \sim y \text{ if } f(x) = f(y).$$

Then $\sim$ is an equivalence relation on S.

Remark: In fact, we will see fairly soon that all equivalence relations can be made to look like this. In other words, given any equivalence relation, there is a function for which the relation is given by this function.

Before we get to this, consider:

Definition: Partition -

A **partition** of a set S is a collection of nonempty subsets of S called **cells**, such that each element of S lies in **exactly one cell**.

Equivalently, cells are all nonempty, mutually disjoint ($C_1 \cap C_2 = \{\}$, $\forall_{\text{ cells } C_1 \neq C_2}$), and the union of all cells is S.

The intuition here is sorting everything into piles, not including any empty piles. Recall that in homework 1, we have an example of a partition with an infinite number of cells, so a partition need not have a finite number of cells.

Theorem 2.1. Let S be a set. Then there is a natural bijection:

$$\{\text{partition of } S\} \to \text{equivalence relations on } S\}$$
$$p \mapsto x \sim y \text{ if } x, y \text{ lie in the same cell,}$$

where $p \in$ partition of S. The inverse is:

$$\text{the collection of all equivalence classes for } \sim \quad \leftarrow\!\shortmid \quad \sim$$

For proof, see the handout.

Definition: Equivalence Class -

The equivalence class of $x \in S$ is

$$\overline{x} := \{y \in S \mid y \sim x\}.$$

$x \in \overline{x}, \quad \forall_x$ (follows from reflexivity)
$\overline{x} = \overline{y} \iff x \sim y$ (follows from symmetry and transitivity)

Now, given an equivalence relation $\sim$ on a set S, let T be the set of equivalence classes and define:

$$f : S \to T$$
$$f(x) = \overline{x}$$

where $\overline{x}$ is the equivalence class containing x. Then

$$f(x) = f(y) \iff \overline{x} = \overline{y} \iff x \sim y,$$

so $\sim$ is of the type (4) in our examples above.

Example: For an important family of examples of equivalence relations, let $n \in \mathbb{Z}^+ := \{1, 2, 3, \dots\}$. For $x, y \in \mathbb{Z}$, define $x \cong_n y$ if $x - y = qn$ for some $q \in \mathbb{Z}$. This is called a **congruence modulo** n and is usually written:

$$x \cong y \pmod{n}.$$

To see reflexiity, consider that

$$x \cong x \pmod{n}$$

because $x - x = 0 \cdot n (0 \in \mathbb{Z})$. To see symmetry, consider:

$$\begin{aligned} x \cong y \pmod{n} &\implies x - y = qn, \text{ with } q \in \mathbb{Z} \\ &\implies y - x = qn, \text{ with } -q \in \mathbb{Z} \\ &\implies y \cong x \pmod{n}. \end{aligned}$$

Now to see transitivity, consider:

$$x \cong y, y \cong z \pmod{n} \implies x \cong z \pmod{n}$$

because if $x - y = q_1 n$ and $y - z = q_2 n$, then $x - z = (q_1 + q_2)n$ with $q_1 + q_2 \in \mathbb{Z}$.
Now, the equivalence classes are: $\bar{0}, \bar{1}, \dots, \overline{n-1}$ (by the 'division algorithm'). For example,

$$\overline{2} = \{\dots, 2 - 2n, 2 - n, 2, 2 + n, 2 + 2n, \dots\}$$

2.2 iClicker Question.

Which of the following is a partition of $\{1, 2, 3, 4\}$? Choices include:

$$P : \{\{1, 2, 3\}, \{2, 4\}\}$$
$$Q : \{\{1, 2\}, \{3, 4\}, \{\}\ \}$$

Neither are, because 2 is present in two cells of P and Q has an empty cell.

3 Complex Numbers

C is a vector space over $\mathbb{R}$ with the basis $\{1, i\}$. Multiply by simplifying and applying $i^2 := -1$. To divide,

$$\frac{z}{w} = zw^{-1}, \text{ where } w^{-1} = \underbrace{\frac{1}{|w|^2}}_{\mathbb{R}^+} \overline{w},$$

where $w \neq 0$. Further, we have:

$$e^{x+iy} = e^x (\cos y + i \sin y),$$

so then

$$\left|e^{x+iy}\right| = |e^x| \cdot |\cos y + i \sin y| = e^x \sqrt{\cos^2 y + \sin^2 y} = e^x.$$

Also, note that

$$\left|e^{i\theta}\right| = 1, \quad \forall_{\theta \in \mathbb{R}}.$$

Now let $U := \{z \in \mathbb{C} \mid |z| = 1\}$, where:

$$\begin{aligned} \mathbb{R} &\xrightarrow{\text{onto}} U \\ \theta &\mapsto e^{i\theta}, \end{aligned}$$

and taking $[0, 2\pi)$ gives:

$$\{x \in \mathbb{R} \mid 0 \leq x \leq 2\pi\} = [0, 2\pi) \xrightarrow{\text{bijective}} U.$$

The set U is closed under multiplication in that:

$$z, w \in U \implies |z| = |w| = 1 \implies |zw| = |z| \cdot |w| = 1 \cdot 1 = 1 \implies zw \in U.$$

However, it is easier to think of multiplication on U in terms of angles. If $z = e^{i\theta}$ and $w = e^{i\phi}$ then $zw = e^{i\theta} \cdot e^{i\phi} = e^{i(\theta+\phi)}$.

So if $\theta, \phi \in [0, 2\pi)$, then we would like to write $e^{i\theta} \cdot e^{i\phi}$ as $e^{i\psi}$ for some $\psi \in [0, 2\pi)$. Sometimes, we have: $\psi = \theta + \phi$, but not if $\theta + \phi \geq 2\pi$.

$$\theta +_{2\pi} \phi = \begin{cases} \theta + \phi, & \theta + \phi < 2\pi \\ \theta + \phi - 2\pi, & \theta + \phi \geq 2\pi. \end{cases}$$

Definition: Binary Operation -

A **binary operation** on a set S is a function from $S \times S \to S$. For each $a, b \in S$, we often use a symbol to denote the value of this function at $(a, b) \in S \times S$. For example,

$$\begin{aligned} S \times S &\longrightarrow S \\ (a, b) &\mapsto a * b \end{aligned}$$

where $(a, b) \in S \times S$ and $a * b \in S$.

Example: The binary operations $+, \times$ on $\mathbb{Z}$.

Definition: Closed under $*$, Induced Operation -

Let $*$ be a binary operation on a set S and let $H \subseteq S$. We say that H is **closed under** $*$ if

$$x * y \in H, \quad \forall_{x,y \in H}.$$

If so, then restricting $*$ (as a function $S \times S \to S$) to $H \times H$ (note $H \times H \subseteq S \times S$) gives a function $H \times H \to H$; i.e. a binary operation on H. This is called the **binary operation on H induced by $*$,** or simply the **induced operation** on H.

As an example of this, $\mathbb{Z}$ is closed under $+$ on $\mathbb{Q}$, and $+$ on $\mathbb{Z}$ is the induced operation, and etcetera. Then $+_{2\pi}$ is a binary operation on $R_{2\pi} = [0, 2\pi)$.

3.1 Last iClicker Question:

$$7 +_{2\pi} 3 = \boxed{10 - 2\pi}$$

Lecture ends here.

Math 113, Fall 2019
Lecture 3, Thursday, 9/5/2019

Topics Today:

- Isomorphisms
- Binary (Algebraic) Structures
- Structural Properties

Reading for Tuesday: up to (and including) §5
Homework due Sept 12 : §2 : 3, 6, 10, 22, 33, 36 and §3 : 2, 10, 16a, 27, 31, 33

1 Clicker Questions:

The binary operation $*$ on $\mathbb{Z}$ given by $n * m = 2n + 2m$ is:
(a) commutative but not associative
(b) associative but not commutative
(c) both
(d) neither
(e) the dog ate my clicker

The following is (are) NOT a structural property of a binary structure $\langle S, * \rangle$.
(a) $\{x * x \mid x \in S\}$ has 3 elements
(b) The function $x \mapsto 2 * x$ is injective
(c) The set $\{x * x * x \mid x \in S\}$ is all of S.
(d) All of the above
(e) Two or more of the above are NOT structural properties
The answer here is (b) because 2 would have to be an element of S for this property to be valid. As proof of (a) (and c similarly), consider:
If $f : S \to S'$ is an isomorphism, then

$$\begin{aligned} f[\{x * x \mid x \in S\}] &= \{f(x * x) \mid x \in S\} \\ &= \{f(x) *' f(x) \mid x \in S\} \quad \text{(homomorphism property)} \\ &= \{x' *' x' \mid x' \in S'\}, \end{aligned}$$

and now since f is injective,

$$\{x * x \mid x \in S\} \text{ and } \{x' *' x' = x' \in S'\}$$

have the same cardinality.

2 Binary Structures

Definition: Binary Algebraic Structure -

A **binary algebraic structure** $\langle S, * \rangle$ is a set S, equipped with a binary operation $*$ on S. We also call it a **binary structure** (for short).
Examples include:

$$\langle \mathbb{R}, + \rangle, \langle \mathbb{R}, - \rangle, \langle \mathbb{R}, \times \rangle, \langle U, \times \rangle, \langle U, / \rangle, \langle \mathbb{R}_2, +_2 \rangle, \langle \mathbb{Z}_{23}, +_{23} \rangle.$$

Definition: Isomorphism -

An **isomorphism** from a binary algebraic structure $\langle S, * \rangle$ to a binary algebraic structure $\langle S', *' \rangle$ is a bijection $\varphi : S \to S'$ such that:

$$\varphi(x * y) = \varphi(x) *' \varphi(y), \quad \forall_{x,y \in S},$$

which we call the 'homomorphism property', and $*'$ is a binary operation in S'.

If such an isomorphism exists, then we say that $\langle S, * \rangle$ and $\langle S', *' \rangle$ are **isomorphic**, and we write:

$$\langle S, * \rangle \simeq \langle S', *' \rangle,$$

(or equivalently $\langle S, * \rangle \cong \langle S', *' \rangle$).
Also, $\varphi : \langle S, * \rangle \xrightarrow{\sim} \langle S', *' \rangle$ says that φ is an isomorphism as above. Then it will be clear what $*$ and $*'$ are, so we omit them from the notation and simply say:

$$S \simeq S' (\text{ or } S \cong S'),$$

and S and S' are isomorphic, with $\varphi : S \xrightarrow{\sim} S'$.
We claim:
As with cardinalities, if Σ is a collection of binary algebraic structures, then isomorphism defines an **equivalence relation** on Σ.

Proof. The proof here is essentially the same as with cardinalities. The identity map $S \to S$ is an isomorphism $S \xrightarrow{\sim} S$. If $\varphi : S \to S'$ is an isomorphism, then so is $\varphi^{-1} : S' \to S$. If $\varphi : S \to S'$ and $\psi : S' \to S''$ are isomorphisms, then so is $\psi \circ \varphi : S \to S''$. □

As we recall, we had binary algebraic structures $\langle U, \times \rangle$ where $U := \{z \in \mathbb{C} : |Z| = 1\}$ (on the unit circle). Taking $\langle \mathbb{R}_{2\pi}, +_{2\pi} \rangle$, we have:

$$\mathbb{R}_{2\pi} = [0, 2\pi)$$
$$\theta +_{2\pi} \varphi = \begin{cases} \theta + \varphi, & \theta + \varphi < 2\pi \\ \theta + \varphi - 2\pi, & \theta + \varphi \geq 2\pi \end{cases}$$

We also had a bijection $\alpha : \mathbb{R}_{2\pi} \to U$ where $\mathbb{R}_{2\pi} \overset{\alpha}{\xrightarrow{\sim}} U$ given by:

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

We also saw:

$$\alpha(\theta +_{2\pi} \varphi) = \alpha(\theta) \cdot \alpha(\varphi), \quad \forall_{\theta, \varphi \in \mathbb{R}_{2\pi}}.$$

3 Proving $S \cong S'$:

To prove two binary structures are isomorphic:
(1) We find a candidate isomorphism $\alpha : S \to S'$.
(2) Show that α is injective

Proof. Let $\theta, \varphi \in [0, 2\pi)$. If $e^{i\theta} = e^{i\varphi}$, then we may assume $\theta \leq \varphi$. By properties of the exponential, $e^{i(\theta - \varphi)} = 1$ with $0 \leq \theta - \varphi < 2\pi$.
Then $\cos(\theta - \varphi) = 1$ and $\sin(\theta - \varphi) = 0$, with $0 \leq \theta - \varphi < 2\pi$. Hence we conclude that $\theta - \varphi = 0$, so $\theta = \varphi$. □

(3) Show that α is onto.

Proof. Given $z = x + iy \in U$, let:

$$\theta = \begin{cases} \cos^{-1} x, & y \geq 0 \\ 2\pi - \cos^{-1} x, & y < 0 \end{cases}.$$

□

Then $e^{i\theta} = z$. But z is arbitrary in U, so α is onto.
(4) Check the homomorphism property (which we did already).

Remark: Alternatively, we could have done this using degrees in place of radians.
Let $\mathbb{R}_{360} = [0, 360)$. Then:

$$a +_{360} b = \begin{cases} a + b, & a + b < 360 \\ a + b - 360, & a + b \geq 360 \end{cases}$$

and define $\beta : \mathbb{R}_{360} \to U$ with

$$\beta(a) = \cos(a^o) + i \sin(a^o).$$

We can show this is also an isomorphism.

In general, we can define $\mathbb{R}_c$ and $+_c$ for any $c > 0$ similarly and get

$$\gamma_2 : \mathbb{R}_c \xrightarrow{\sim} U$$

by

$$\gamma_2(a) := \cos\left(\frac{2\pi}{c}a\right) + i \sin\left(\frac{2\pi}{c}a\right).$$

If c is a positive integer n, then something special happens. Let $\mathbb{Z}_n := \mathbb{R}_n \cap \mathbb{Z} = \{0, 1, 2, \ldots, n-1\}$. Then $\mathbb{Z}_n \subseteq \mathbb{R}_n$ and $\mathbb{Z}_n$ is closed under $+_n$ with:

$$a +_n b = \begin{cases} a + b, & a + b < n \\ a + b - n, & a + b \geq n \end{cases}$$

So we get a binary structure $\langle \mathbb{Z}_n, +_n \rangle$ (using the induced operation).

Example: $n := 5$. Then

$$\begin{array}{ccc} \gamma_5 : \mathbb{R}_5 & \xrightarrow{\quad bijection \quad} & U \\ \cup| & & \cup| \\ \gamma_5|_{\mathbb{Z}_5} : \mathbb{Z}_5 & \xrightarrow{\quad bijection \quad} & U_5 \end{array}$$

and notice:

$$\gamma_5(\mathbb{Z}_5) = \{1, e^{\frac{2\pi i}{5}}, e^{\frac{2\pi i}{5}\cdot 2}, e^{\frac{2\pi i}{5}\cdot 3}, e^{\frac{2\pi i}{5}\cdot 4}\} =: U_5$$

Then $\gamma_5|_{\mathbb{Z}_5}$ is one-to-one (because γ_5 is one-to-one), and is onto U_5 by definition of U_5. Additionally, $\gamma_5|_{\mathbb{Z}_5}$ satisfies the homomorphism property because γ_5 does.
Also, we can see that $z^5 = 1, \forall_{z \in U_5}$. Since a polynomial $z^5 - 1$ (of degree 5) has at most 5 roots and we've found 5 roots, $z^5 - 1$ has **no other roots**. Therefore,

$$U_5 = \{z \in \mathbb{C} : z^5 = 1\}.$$

If $f : A \to B$ is a function and $A' \subseteq A$, then $f|_{A'}$ is the function $A' \to B$ defined by

$$f|_{A'}(a) = f(a), \quad \forall_{a \in A'}.$$

To prove that $\langle S, * \rangle$ and $\langle S', *' \rangle$ are **not** isomorphic:
Simply find a structural property that one has that the other does not have.

Definition: Structural Property -

A **structural property** of a binary algebraic structure is a property that any two isomorphic binary structures must either both have or neither has. An example of a structural property is: having the same cardinality as some given set.

4 Structural Properties

Let $\langle S, * \rangle$ be a binary structure. We consider two common and important structural properties: commutativity and associativity.

4.1 Commutativity

We say that $*$ is commutative if

$$x * y = y * x, \quad \forall_{x,y \in S}.$$

Then $\langle S, * \rangle$ (or S) is commutative if $*$ is commutative.
For examples, $\langle \mathbb{Z}, + \rangle$ is commutative, whereas $\langle \mathbb{Z}, - \rangle$ is not.

We claim:
If $\langle S, * \rangle$ is commutative, and

$$\langle S, * \rangle \cong \langle S', *' \rangle,$$

with the isomorphism $\varphi : S \to S'$, then $\langle S', *' \rangle$ is commutative.

Proof. Let $a', b' \in S'$. Then $\exists_{a,b \in S}$ such that $\varphi(a) = a'$ and $\varphi(b) = b'$. Then

$$a' *' b' = \varphi(a) *' \varphi(b) = \varphi(a * b) = \varphi(b * a) = \varphi(b) *' \varphi(a) = b' *' a'$$

and hence this proves that commutativity is a structural property.

□

4.2 Associativity

If

$$(x * y) * z = x * (y * z), \quad \forall_{x,y,z \in S}$$

then S is associative. The rest is left as an exercise to show this is a structural property.

4.3 Example

Let A be a set and let S be the set of all functions from A to A, and let $\circ$ be the binary operation on S given by the composition of functions.
If $f, g \in S$, then $f \circ g$ takes $a \in A$ to $f(g(a))$.
This is associative because both $(f \circ g) \circ h$ and $f \circ (g \circ h)$ take

$$a \mapsto f(g(h(a))).$$

However, $\circ$ is **NOT** commutative (unless A has ≤ 2 elements). As an example of where this fails, take

$$A := \mathbb{R}_2, \quad f(x) = 2x, \quad g(x) = e^x.$$

To see this explicitly,

$$\begin{aligned} f \circ g : x \mapsto 2e^x &\implies 0 \mapsto 2 \\ g \circ f : x \mapsto e^{2x} &\implies 0 \mapsto 1 \end{aligned}$$

From earlier, an example of something that fails to be a structural property is:

$$2 \in S, \text{ or } S \subseteq \mathbb{C}.$$

Notice that $2 \notin U$ but $2 \in \mathbb{R}_{2\pi}$.

5 Clicker Question:

Which of the following following are isomorphic?

$$S_1 : \begin{bmatrix} * & a & b \\ a & a & b \\ b & b & a \end{bmatrix}, \qquad S_2 : \begin{bmatrix} * & a & b \\ a & b & a \\ b & a & b \end{bmatrix}, \qquad S_3 : \begin{bmatrix} * & a & b \\ a & a & b \\ b & a & b \end{bmatrix}$$

The correct answer is: (A) in that

$$S_1 \cong S_2.$$

Our isomorphism simply switches a and b.

Lecture ends here.

Vojta leaves us with a cliff-hanger for next time:
Is $\langle \mathbb{Z}^+, + \rangle$ isomorphic to $\langle \mathbb{N}, + \rangle$? Take $\mathbb{Z}^+ := \{1, 2, 3, \dots\}$ and $\mathbb{N} := \{0, 1, 2, \dots\}$.

Math 113, Fall 2019
Lecture 4, Tuesday, 9/10/2019

Topics Today:

- Identity elements and inverse elements, Groups
- Reading for Thurs: Up to (and including) §6

1 Clicker Questions

Which of the following is **not** a part of the definition for $\langle G, * \rangle$ to be a group? Answer: $*$ is commutative.
A group $\langle G, * \rangle$ is said to be **abelian** if (and only if): Answer: $*$ is commutative.

2 Lecture

Definition: identity element -

An **identity element** of a binary structure $\langle S, * \rangle$ is an element $e \in S$ such that $e * s = s * e = s, \forall_{s \in S}$. Hence having an identity element is a **stuctural property**.

Remark: In fact, if $\langle S, * \rangle$ has an identity element e and $\phi : S \to S'$ is an isomorphism, then $\phi(e)$ is an identity element of S'.

Proof. $\forall_{s' \in S'} \exists_{s \in S} : s' = \phi(s)$, so that

$$s' * \phi(e) = \phi(s) * \phi(e) = \phi(s * e) = \phi(s) = s',$$

and similarly $\phi(e) * s' = s'$. □

Additionally, if a binary structure has an identity element, then the identity element e is unique.

Proof. Consider:

$$e_1 = e_1 * e_2 = e_2,$$

where first equality follows from that e_2 is an identity, and the second equality follows from e_1 as the identity. □

Also, another thing: $\langle \mathbb{Z}^+, + \rangle$ is NOT isomorphic to $\langle \mathbb{N}, + \rangle$, where the latter has identity element 0, whereas the former does not have an identity element. Recall that in order to show two binary structures are isomorphic, it suffices to show that they differ in a structural property. That is, one fails the structural property whereas the other satisfies that same property.

Definition: Inverse -

Let $\langle S, * \rangle$ be a binary structure with identity element e, and let $s \in S$. Then an **inverse** of s is an element s' such that

$$s * s' = s' * s = e.$$

Example: In $\langle \mathbb{Z}, + \rangle$, 0 is the identity and n has inverse $-n$.
In $\langle \mathbb{C}, \cdot \rangle$, z has the inverse $\frac{1}{z} = \frac{\overline{z}}{|z|^2}$ if $z \neq 0$, where 0 has no inverse. And 1 is the identity element.
In $\langle \mathbb{Z}, \cdot \rangle$, only 1 and -1 have inverses.
In $\langle U, \cdot \rangle$, all elements have inverse.

2.1 Matrices

Let $n \in \mathbb{Z}^+$. Define $M_n(\mathbb{R})$ as the set of $n \times n$ matrices with entries in $\mathbb{R}$. In $\langle M_n(\mathbb{R}), \text{matrix mult} \rangle$, I_n (the identity matrix) is the identity element and a matrix M has an inverse (M^{-1}) if and only if $\det M \neq 0$.

2.2 Clicker Question

Let $\langle S, * \rangle$ be the binary structure with $S = \{e, a, b\}$ and $*$ given by:

$$\begin{bmatrix} * & e & a & b \\ e & e & a & b \\ a & a & e & e \\ b & b & e & b \end{bmatrix}$$

(so it has an identity element e). How many elements of S have inverses?
Answer: 3.

3 Groups

Definition: Group -

A group $\langle G, * \rangle$ is a binary structure $\langle G, * \rangle$ such that :
(1) $*$ is associative. That is,

$$a * (b * c) = (a * b) * c, \forall_{a,b,c \in G}.$$

(2) $\langle G, + \rangle$ has an identity element, and

$$\exists_{e \in G} : a * e = e * a = a, \forall_{a \in G}$$

(3) every element of G has an inverse.

$$\forall_{a \in G} \exists_{a' \in G} : a * a' = a' * a = e.$$

Remark: Let $\langle G, * \rangle$ be a group and let $a \in G$. Then the inverse a' of a is **unique**.

Proof. If a' and a'' are inverses of a, then associativity gives:

$$a' * (a * a'') = (a' * a) * a''$$
$$a' * e = e * a''$$
$$a' = a'',$$

□

Example:
- $\langle \mathbb{Z}, + \rangle$ is a group
- $\langle \mathbb{N}, + \rangle$ is NOT a group (only 0 has an inverse)
- $\langle \mathbb{R}, \cdot \rangle$ is NOT a group (0 has no inverse)
- $\langle \mathbb{R} \setminus \{0\}, \dot{} \rangle$ is a group
- $\langle V, + \rangle$ is a group, where V is ANY vector space.
- $\langle \{e\}, e * e = e \rangle$ is a group (this is called the 'trivial group')
- $\{\}$ is NOT a group (no inverse)

Definition: $GL_n(\mathbb{R})$ **-**

Let $n \in \mathbb{Z}^+$ and let $GL_n(\mathbb{R})$ be the set of **invertible** $n \times n$ matrices with entries in $\mathbb{R}$. Then

$$\langle GL_n(\mathbb{R}), \text{mat. mult.} \rangle$$

is a group. We check that $I_n \in GL_n(\mathbb{R})$ (the identity matrix) is the identity element. If $M \in GL_n(\mathbb{R})$ then so is M^{-1}. If $A, B \in GL_n(\mathbb{R})$, then $AB \in GL_n(\mathbb{R})$.

Definition: Abelian -

A group is **abelian** if it is commutative. It is **non-abelian** if it is not abelian.

All groups in the preceding examples are abelian, except $GL_n(\mathbb{R})$ for all $n \geq 2$.

4 Properties of Groups:

(Property 1) We can left-cancel or left-cancel. That is,

$$a * b = a * c \implies b = c.$$

Proof.

$$a * b = a * c$$
$$a^{-1} * (a * b) = a^{-1} * (a * c)$$
$$(a^{-1} * a) * b = (a^{-1} * a) * c$$
$$e * b = e * c$$
$$b = c$$

□

Caution:
Notice that

$$a * b = c * a$$

does NOT imply $b = c$ (unless the group is **abelian**). For example, take A, B nonsingular similar $n \times n$ matrices with $A + B$. Notice that $A, B, P \in GL_n(\mathbb{R})$.

(Property 2): Solve for x in equations $a * x = b \implies x = a^{-1} * b$ or $x * a = b \implies x = b * a^{-1}$.

5 Useful Facts:

(1) Notice that e is its own inverse. That is, $e^{-1} = e$ because $e^{-1} = e^{-1} * e = e$, where first equality follows from e as identity, and the second equality follows from the definition of e^{-1} as inverse.
(2)

$$(x^{-1})^{-1} = x \forall_{x \in G}$$

because

$$(x^{-1})^{-1} * x^{-1} = e = x * x^{-1}.$$

Now cancel $* x^{-1}$.
(3) $x * y = e$ implies $y = x^{-1}$ and $x = y^{-1}$ because $x * y = e = x * x^{-1}$. Cancel $x*$ similarly to get $x = y^{-1}$.
(4) As with matrices, $(x * y)^{-1} = y^{-1} * x^{-1}$ gives

$$(x * y) * (y^{-1} * x^{-1}) = x * (y * y^{-1}) * x^{-1} = x * e * x^{-1} = x * x^{-1} = e.$$

Theorem 5.1. General Associative Law
Let $\langle S, * \rangle$ be a binary structure in which $*$ is associative. Let $n \in \mathbb{Z}^+$, and let $x_1, \ldots, x_n \in S$. Then the result of $x_1 * x_2 * \cdots * x_n$ is the same regardless of how we place parenthesis to evaluate.

Proof. To prove this, we use strong induction. Taking the base cases $n = 1, 2, 3$, there is nothing to prove (regular associative law). Suppose we put parentheses in the expression in some way:
Let $E = \underbrace{(x_1 * x_2 * \cdots * x_m)} * \underbrace{(x_{m+1} * \cdots * x_n)}$ with $1 \leq m \leq n - 1$, where the parentheses in these do not matter.

Case 1: $m < n - 1$. Write $x_{m+1} * \cdots * x_n = (x_{m+1} * \cdots * x_{m-1}) * x_n$ (by the $n - m$ case; note $n - m < n$). Then

$$\begin{aligned} E &= (x_1 * \cdots * x_m) * ((x_{m+1} * \cdots * x_{n-1}) * x_n) \\ &= ((x_1 * \cdots * x_m) * (x_{m+1} * \cdots * x_{n-1})) * x_n \\ &= ((\cdots (x_1 * x_2) * \cdots) * x_{n-1}) * x_n, \end{aligned}$$

where the first equality follows from the regular associativity law, and the second equality follows from the $n - 1$ case (strong induction).

Case 2: $m = n - 1$. Then

$$E = (x_1 * \cdots * x_{n-1}) * x_n = ((\cdots (x_1 * x_2) * \cdots) * x_{n-1}) * x_n$$

by the $n - 1$ case. So they're equal to the result we get when we multiply left to right, completing our proof.

□

6 Another Example of a Group:

Let $n \in \mathbb{Z}^+$. Recall that $\equiv_n$ (stands for congruence $\mod n$) is an equivalence relation. That is, $x \equiv_n y$ means $x \equiv y \pmod n$, which shows $x - y = qn$ for some $q \in \mathbb{Z}$.

Define $+'$ on $\tilde{\mathbb{Z}}_n$ by:

$$x +' y = \overline{a + b},$$

where $a, b \in \mathbb{Z}$ are chosen so that $x = \overline{a}$ and $y = \overline{b}$.

Recall that $\overline{a} = \{m \in \mathbb{Z} \mid m \equiv a \pmod n\}$ (equivalence class of a). We choose a way to write x, y in terms of their eqiuvalence classes, we add thoses, then take the equivalence class of that. We check that the answer does NOT depend on the choice of a, b (that is, the answer is well-defined).

Proof. Suppose $x = \overline{a} = \overline{a}_1$ and $y = \overline{b} = \overline{b}_1$ (property of equivalence class). Then $a \equiv_n a_1$, so $a_1 = a + cn$ for some $c \in \mathbb{Z}$. Similarly, $b \equiv_n b_1$, so $b_1 = b + dn$ for some $d \in \mathbb{Z}$. Therefore $a_1 + b_1 = a + cn + b + dn = (a + b) + (c + d)n$, which gives

$$\begin{aligned} a_1 + b_1 &\equiv a + b \pmod n \\ \overline{a_1 + b_1} &\equiv_n \overline{a + b}. \end{aligned}$$

□

Then we conclude that $\langle \tilde{\mathbb{Z}}_n, +' \rangle$ is a well-defined binary structure. Moreover, it is also a group. We check the requirements. To see associativity, consider:

$$(\overline{a} +' \overline{b}) +' \overline{c} = \overline{a + b} +' \overline{c} = \overline{(a + b) + c} = \overline{a + (b + c)} = \overline{a} +' (\overline{b} +' \overline{c}).$$

Now $\overline{0}$ is an identity element. To see this, consider:

$$\overline{a} +' \overline{0} = \overline{a + 0} = \overline{a},$$

and $\overline{0} +' \overline{a} = \overline{a}$, similarly. Finally, $\overline{n}$ has inverse $\overline{-n}$ because

$$\overline{n} +' \overline{-n} = \overline{n + (-n)} = \overline{0},$$

and similarly for $\overline{-n} +' \overline{n}$. Its elements are $\overline{0}, \overline{1}, \overline{2}, \ldots, \overline{n - 1}$, and these are all **different**.

Proof. We use the division algorithm for $\mathbb{Z}^{-1}$ (p. 60). For all $m \in \mathbb{Z}$, $\exists!_{q,r \in \mathbb{Z}}$: $m = qn + r$, and $0 \leq r < n$. Then there is a unique $r \in \{0, 1, \ldots, n - 1\}$ such that $m \equiv r \pmod n$. That is, $\overline{m} = \overline{r}$. Vojta leaves showing that these are different as an exercise, but this really follows easily. □

Lecture ends here.

Math 113, Fall 2019
Lecture 5, Thursday, 9/12/2019

Topics Today:

- $\mathbb{Z}_n$ is a group
- Groups via tables
- Subgroups
- Subgroups of U_6
- x^n and cyclic (sub)groups

Handout on x^n.
Homework due Sept 19: §4 : 2,6,24,30,36,37 ; §5: 4,11,13,16,22,23,50 ; §6 : 2, 6, 10, 18, 22, 34, 46.
Readings: Up to top of p. 70

1 Clicker Questions

Which of the following are true?
(False) Multiplicative notation is used **only** for nonabelian groups. (True) Additive notation is used **only** for abelian groups.

How many of the following are true?
(False) $\langle \mathbb{Q}^*, \times \rangle$ is a subgroup of $\langle \mathbb{Q}, + \rangle$ (not the induced operation)
(False) $\mathbb{N}$ is a subgroup of $\mathbb{Z}$ ($\mathbb{N}$ is not a group)
(False) $\mathbb{Z}_2 := \{0, 1\}$ is a subgroup of $\mathbb{Z}_5 = \{0, 1, 2, 3, 4\}$.
(True) U is a subgroup of $\langle \mathbb{C}^*, \times \rangle$.
Where $\mathbb{C}^* := \mathbb{C} \setminus \{0\}$ and $\mathbb{Q}^* := \mathbb{Q} \setminus \{0\}$.

2 Review

Recall that last time, we took $n \in \mathbb{Z}^+$ and let $\tilde{\mathbb{Z}}_n$ to be the set of equivalence classes of $\equiv_n$ (congruence mod n) in $\mathbb{Z}$.

$$\tilde{\mathbb{Z}}_n = \{\overline{0}, \overline{1}, \ldots, \overline{n-1}\}$$

and these are each distinct.
Binary operation $+'$ on $\tilde{\mathbb{Z}}_n : \overline{a} +' \overline{b} = \overline{a+b}$ shows that $\tilde{\mathbb{Z}}_n$ is a group.
Define $\Psi : \mathbb{Z}_n \to \tilde{\mathbb{Z}}_n$ by $\Psi(a) = \overline{a}$ for all $a \in \mathbb{Z}_n := \{0, 1, \ldots, n-1\}$. This is a bijection. It is an isomorphism because for all $a, b \in \mathbb{Z}_n$, we have:

$$a +_n b = \begin{cases} a+b, & a+b < n \\ a+b-n, & a+b \geq n \end{cases}$$

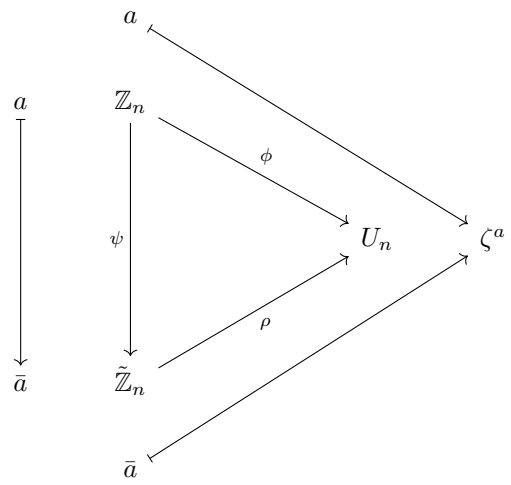
and either way, $a +_n b \equiv a + b \pmod{n}$. Therefore,

$$\overline{a +_n b} = \overline{a+b}, \forall_{a,b \in \mathbb{Z}_n}.$$

Therefore

$$\Psi(a +_n b) = \overline{a +_n b} = \overline{a+b} = \overline{a} +' \overline{b} = \Psi(a) +' \Psi(b).$$

So Ψ is an isomorphism (of binary structures). Since $\tilde{\mathbb{Z}}_n$ is a group, then we conclude that so is $\mathbb{Z}_n$. That is, definitions D_1, D_2, D_3 are structural properties.
So we have a diagram:



where $U_n = \{z \in \mathbb{C} : Z^n = 1\}$, $\zeta = e^{2\pi i/n} \in U_n$, and $U_n = \{1, \zeta, \zeta^2, \ldots, \zeta^{n-1}\}$.
ϕ is an isomorphism from Fraleigh page 18. This diagram commutes. That is, $\phi = \rho \circ \psi$.
To see this:

$$\begin{aligned} \overline{a} = \overline{b} &\implies a \equiv b \pmod{n} \\ &\quad a = b + qn \text{ with } q \in \mathbb{Z} \\ &\implies \zeta^a = \zeta^{b+qn} = \zeta^b(\zeta^n)^a = \zeta^b \cdot 1^a = \zeta^b. \end{aligned}$$

Definition: isomorphism of groups -

An **isomorphism of groups** is an isomorphism of the underlying binary structures. That is, it is a bijection that satisfies the homomorphism property.
Note that an isomorphism from G to G' takes the identity element of G to the identity element of G' (Theorem 3.14). Additionally, $\forall_x \in G$, it takes the inverse of x in G to the inverse of $\varphi(x)$ in G' (where φ is the isomorphism). This is because

$$\varphi(x)\varphi(x^{-1}) = \varphi(xx^{-1}) = \varphi(e) = e' = \varphi(x)\varphi(x)^{-1}.$$

Now cancel $\varphi(x)$ to get $\varphi(x^{-1}) = \varphi(x)^{-1}$.

Definition: Order of a group -

The **order** of a group G is the number of elements in the set G (or our convention is the order is infinity if G is infinite). We denote this $|G|$.

3 Groups via tables

If a group is small (and finite), then it is possible to give its binary operation using a table.

Example: A group of order 3. Let G be such a group, actually $\langle G, * \rangle$. Let the elements of G be e, a, b where e is the identity element. Then we know (so far) that the table looks something like:

$$\begin{bmatrix} * & e & a & b \\ e & e & a & b \\ a & a & - & - \\ b & b & - & - \end{bmatrix}.$$

Now the entries on the second row must all be different by cancellation:

$$a * a = a * b \implies a = b,$$

which is a contradiction to that we know these elements are different. Also, we must include every element of G because G is finite.

Remark: We cannot have $a * a = a$, because cancellation would imply $a = e$. Additionally, we cannot have $a * a = e$, because then the last element in row $a * \cdot$ would have to be b, where we already have a b in that last column ($e * b = b$). This makes it so the only possibility is: $\boxed{a * a = b}$.

Now we can fill in the rest of the table easily:

$$\begin{bmatrix} * & e & a & b \\ e & e & a & b \\ a & a & b & e \\ b & b & e & a \end{bmatrix}.$$

We notice that this group is also abelian.

Remark: We know this is a group because we know that groups of order 3 exist ($\mathbb{Z}_3$)

4 Clicker Question

For the table on the right, fill it out as far as you can. Then what is $c * c$?

$$\begin{bmatrix} * & e & a & b & c \\ e & e & a & b & c \\ a & a & e & - & - \\ b & b & - & e & - \\ c & c & - & - & - \end{bmatrix}$$

Voyta gives the solution brute-forcing all entries to ultimately get the final entry, namely our desired $c * c$.
Alternatively, we reason that we must have $c * c = e$ because e is present in all columns and rows except the last of each.

Remark: This example we worked with is not $\mathbb{Z}_4$, because $\mathbb{Z}_4$ is:

$$\begin{bmatrix} +_4 & 0 & 1 & 2 & 3 \\ 0 & 0 & 1 & 2 & 3 \\ 1 & 1 & 2 & 3 & 0 \\ 2 & 2 & 3 & 0 & 1 \\ 3 & 3 & 0 & 1 & 2 \end{bmatrix}$$

where the additive inverses are in different places.

Definition: Subgroups -

A **subgroup** of a group $G := \langle G, * \rangle$ is a subset H of G, such that:
(1) H is closed under $*$, and
(2) H is a group, using the induced operation.
We say that $H \subsetneq G$ is a proper subgroup if $H \neq G$ (proper subset of G). As for notation, we write:

$$H \leq G, G \geq H$$

to mean H is a subgroup of G, and

$$H < G, G > H$$

to mean H is a proper subgroup of G (that is, $H \leq G$ and $H \neq G$.)

Examples:
(1) Every group G contains itself as a subgroup (called the "improper subgroup"). That is, for all groups G, we have $G \leq G$.
(2) Every group contains the trivial subgroup $\{e\}$, where e is the identity element.
(3) $\mathbb{Z} < \mathbb{Q} < \mathbb{R} < \mathbb{C}$ (where we assume addition operation when we write these as groups).
(4) Similarly, $\{\pm 1\} < \mathbb{Q}^* < \mathbb{R}^* < \mathbb{C}^*$ (under multiplication), where $\mathbb{C}^* := \mathbb{C} \setminus \{0\}$, etc, as usual.
(5) $U_n < U < \mathbb{C}^*$, for all $n \in \mathbb{Z}^+$.
(6) The set of even integers $< \mathbb{Z}$ (is a subgroup of $\mathbb{Z}$).

Remark: The empty set $\{\}$ is NOT a subgroup of any group G, because a group must have an identity element. In particular, a group must have an element.

Then we have the following theorem:

Theorem 4.1. Let $\langle G, * \rangle$ be a group. A subset H of of G is a subgroup of G if (and only if):
(1) H is closed under $*$ (otherwise there's no induced operation)
(2) H contains the identity element of G (the identity may happen with rings but not here), and
(3) H is closed under the operation of taking inverses ($x^{-1} \in H, \forall_{x \in H}$)

Proof. See Fraleigh for proof. □

Remark: Let G be a group and $H < G$ (H is a subgroup of G). Then
(1) The identity elements of G and H are the same, and
(2) For all $x \in H$, its inverse in H equals its inverse in G.

Proof. (1) Let e_G, e_H be the identity elements of G and H, respectively. Then:

$$e_H * e_H = e_H = e_H * e_G,$$

where the final equality is from e_G as identity, and performing left-cancellation of e_H* gives $e_H = e_G$.
(2) Let $x \in H$, and let x^{-1} be its inverse in G. Let x' be its inverse in H. Then

$$x * x' = e_H = e_G = x * x^{-1},$$

where cancelling gives $x' = x^{-1}$. □

Another Useful Fact:
Let H be a sub**set** of a group G. Then $H < G$ (H is a sub**group** of G) if (and only if) :

$$H \neq \{\} \text{ and } xy^{-1} \in H, \forall_{x,y \in H}$$

Proof. For the forward $\implies$ direction,

$$H \leq G \implies H \neq \{\}$$

and

$$x, y \in H \implies x, y' \in H \implies xy^{-1} \in H$$

Now for the backwards $\impliedby$ direction, consider that $H \neq \emptyset$ implies (by setting $y := x$):

$$\exists_{x \in H} : xx^{-1} \in H \implies e \in H,$$

and

$$ex^{-1} \in H \implies x^{-1} \in H \implies H \text{ is closed under inverse.}$$

Also, $xy = x(y^{-1})^{-1} \in H$, so H is closed under $*$. Now apply the earlier theorem.

□

Example: Let $\varphi : G \to G'$ be an isomorphism, and let $H \leq G$ and recall

$$\varphi[H] = \{\varphi(x) : x \in H\}$$

Then $\varphi[H] \leq G'$.

Proof. (1) $\varphi[H] \neq \{\}$ because $H \neq \{\}$. That is, because H is nonempty, the set $\varphi[H]$ itself cannot be empty.
(2) Let $a', b' \in \varphi[H]$. Then $\exists_{a,b \in H} : \varphi(a) = a'$ and $\varphi(b) = b'$. Also, $ab^{-1} \in H$, so $\varphi(ab^{-1}) \in \varphi[H]$. Vojta leaves us with a cliffhanger, in that it remains to prove:

$$\varphi(ab^{-1}) = a'(b')^{-1}$$

□

Lecture ends here.

Math 113, Fall 2019
Lecture 6, Tuesday, 9/17/2019

1 Clicker Questions:

1. Which of the following are cyclic groups:
(A) $\mathbb{Z}$, generated by 1
(B) U_n (with $n \in \mathbb{Z}^+$), generated by $\zeta = e^{2\pi i/n}$
(C) Both
(D) Neither
(E) Something Else

2. Applying the Division Algorithm to divide -53 by 10 gives:
(B) $-53 = -6 \cdot 10 + 7$
(E) My clicker fell into the toilet and this was the only button that works.

2 Review

Last time, Vojta left us with a cliffhanger. Let $\varphi : G \xrightarrow{\sim} G'$ be an isomorphism of groups and let $H \leq G$. Then

$$\varphi[G] = \{\varphi(x) : x \in H\}$$

is a subgroup of G'.

Proof. In the last lecture, we already did the case where $\varphi[H] \neq \emptyset$. Let $a', b' \in \varphi[H]$. Then $\exists_{a,b \in H}$ such that $\varphi(a) = a'$ and $\varphi(b) = b'$. Since $H \leq G$, $ab^{-1} \in H$, so $\varphi(ab^{-1}) \in \varphi[H]$.
Additionally,

$$\varphi(ab^{-1})b' = \varphi(ab^{-1})\varphi(b) = \varphi(ab^{-1}b) = \varphi(a) = a',$$

so $\varphi(ab^{-1})$ is a solution to $xb' = a'$. This implies $\varphi(ab^{-1}) = a'(b')^{-1}$, where $\varphi(ab^{-1}) \in \varphi[H]$. Hence $a'(b')^{-1} \in \varphi[H]$. Therefore we conclude that $\varphi[H]$ is a subgroup of G'.

□

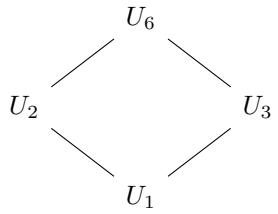
3 Extended Example:

Find all subgroups of U_6.

Solution. Recall that $U_6 := \{1, \zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5\}$, where $\zeta := e^{\frac{2\pi i}{6}}$. We already know that U_6 has the trivial subgroups $\{1\}$ and U_6. . Are there any others? Let H be a nontrivial subgroup of U_6. Then H contains an element $x \neq 1$. If $x = \zeta$, then H contains $\zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5, 1$. Then $H = U_6$.
If $x = \zeta^2$, then H contains $\zeta^2, \zeta^4, \zeta^6 = 1$, so $H \supseteq \{1, \zeta^2, \zeta^4\} = U_3$. We've found another subgroup, $U_3 < U_6$.
If $x = \zeta^3 = -1$, then H contains $\{-1, 1\} = U_2$, so we've found yet another subgroup, $U_2 < U_6$.
If $x = \zeta^4$, then H contains $\zeta^4, \zeta^4 \cdot \zeta^4 = \zeta^3$ and 1, so $H \supseteq \{1, \zeta^2, \zeta^4\} = U_3$.
If $x = \zeta^5$, then H contains $x^{-1} = \zeta$, hence as above, $H = U_6$.
If $H > U_3$, then H contains ζ or ζ^3 or ζ^5.
If H contains ζ or ζ^5, then $H = U_6$, as before.
If H contains ζ^3, then H also contains $\zeta^3 \cdot \zeta^4 = \zeta$, and so again $H = U_6$.
Therefore there are no subgroups H with $U_3 < H < U_6$.
If $H > U_2$, then H contains ζ, ζ^2, ζ^4, or ζ^5.
If it's ζ or ζ^5, then $H = U_6$. If it's ζ^2 or ζ^4, then $H \supseteq U_3$. Hence $H > U_3$.
Therefore $H = U_6$, as before.
Then in conclusion, subgroups of U_6 are:

$$\{1\} = U_1, U_2, U_3, U_6.$$

We can make the diagram:



□

4 Group (Written Multiplicatively)

Definition: x^n **-**

Let G be a group (written multiplicatively). Let $x \in G$, and let $n \in \mathbb{Z}$. Define:

$$x^n := \begin{cases} \overbrace{x \cdot x \cdots x}^{n \text{ times}}, & n \geq 0 \\ e, & n = 0 \\ (x')^{-n}, & n < 0. \end{cases}$$

It is clear from this definition that $x^1 = x$ for all $x \in G$, hence $x^{-1} = (x')^1 = x'$, so we go back to writing x^{-1} to denote the inverse.

In additive notation, we write nx instead of x^n. Then $nx + mx = (n+m)x$, and $m(nx) = (mn)x$ (notice this is not the associative law). Also nx as defined here is n times x if $G \leq \mathbb{C}$. Also, we write $(-1)x = -x$ as the additive inverse of x.

5 Cyclic Groups

Theorem 5.1. Let G be a multiplicative group, and let $a \in G$. Then:
(a) $\{a^n : n \in \mathbb{Z}\}$ is a subgroup of G; call it $\langle a \rangle$.
(b) All subgroups of G that contain a must also contain $\langle a \rangle$, and
(c) $\langle a \rangle$ is abelian (even if G isnt).

Proof. (a) $\langle a \rangle$ is nonempty. Also, if $x, y \in \langle a \rangle$, then $x = a^n$ and $y = a^m$ for some $n, m \in \mathbb{Z}$. Then $xy^{-1} = a^n(a^m)^{-1} = a^{n-m} \in \langle a \rangle$. Hence $\langle a \rangle \leq G$.
(b) If $H \leq G$ and $a \in H$, then $a^n \in H, \forall_{n \in \mathbb{Z}}$.
(c) Consider:

$$a^n a^m = a^{n+m} = a^{m+n} = a^m a^n, \forall_{m,n \in \mathbb{Z}}.$$

□

Definition: Cyclic subgroup, Cyclic generator -

The subgroup $\langle a \rangle$ is called the **cyclic subgroup** of G generated by a. A group G or subgroup H is said to be **cyclic** if there is some $a \in H$ or $a \in G$ such that $\langle a \rangle = G$ or $\langle a \rangle = H$, respectively.
If so, then we call a a **cyclic generator** of G or H, respectively.

We call it a 'cyclic' generator because later we will find that there are more generators we consider.

6 Clicker Questions:

1. Which are the cyclic generators of U_6?
Define $\zeta := e^{\frac{2\pi i}{6}}$.
(a) ζ only
(b) ζ and ζ^{-1} only
(c) $\zeta, \zeta^2, \zeta^3, \zeta^4, \zeta^5$.
(d) all elements of U_6 are cyclic generators of U_6
(e) none of the above.

2. Which subgroups of U_6 are cyclic subgroups?
(a) Only U_6 itself
(b) U_6, U_2 and U_3 only
(c) Only U_6 and U_3
(d) all of them are
(e) none of the above

7 Order of a Group

Definition: Order -

The **order** of an element $a \in G$ is the order of the cyclic subgroup that it generates. It is denoted $|a|$. So $|a| = |\langle a \rangle|$.
By convention, if $\langle a \rangle$ is infinite, then we say that a has infinite order.

Lemma 7.1. Let G be a group and let $a \in G$.
(a) If a has finite order, then $\exists_{n_1, n_2 \in \mathbb{Z}} : n_1 \neq n_2$ and $a^{n_1} = a^{n_2}$.
(b) If there exists n_1 and n_2 as in (a) above, then $\exists_{n \in \mathbb{Z}^+} : a^n = e$.

Proof. (a) If $|a| < \infty$, then $f : \mathbb{Z} \to \langle a \rangle$, defined by $f(n) = a^n$ maps an infinite set to a finite set, so f is NOT injective, as desired.
(b) Let G and a be as in the lemma, with $|a| < \infty$. Then $a^{kn} = e \forall_{k \in \mathbb{Z}}$ because

$$a^{kn} = a^{nk} = (a^n)^k = e^k = e.$$

□

Now we may ask, are there any other integers m (other than multiples of our **order** n) such that $a^m = e$?
We claim that there aren't any such m. If there is such an m, then it's between multiples of n, so:

$$kn < m < (k+1)n.$$

Then $0 < m - nk < n$, and

$$a^{m-nk} = a^m (a^n)^{-k} = a^m e^{-k} = a^m = e,$$

contradicting our choice of n. So $a^m = e \iff m$ is a multiple of $|a|$.

Lecture ends here.

Math 113, Fall 2019
Lecture 7, Thursday, 9/19/2019

Topics Today:

- Cyclic groups (continued)
- Greatest common divisor
- More!!! on Cyclic groups
- Generating sets (time permitting)

1 Clicker Questions

1. How many of the following groups are cyclic?

$$U, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$$

Answer: 1, only $\mathbb{Z}$.

2. Which of the following are NOT cyclic?

$$\mathbb{Z}_3, \text{ the trivial group}, U_7, \tilde{\mathbb{Z}}_5.$$

Answer: All of the above.

2 Theorems on Cyclic Groups

Vojta notes there are three theorems regarding cyclic groups.

Theorem 2.1. Let G be a cyclic group.

(a) If G is infinite then $G \cong \mathbb{Z}$.

(b) If G is finite, then $G \cong \mathbb{Z}_n$, where $n := |G|$.

Moreover (not in the textbook), if G is finite and is generated by an element a, then n is the smallest positive integer such that $a^n = e$, and $G = \{e, a, a^2, \ldots, a^{n-1}\}$ (without repetition).
Further, $a^j = a^k \iff j \equiv k \pmod{n}$.

Proof. Let $a \in G$ be a cyclic generator. Define $f : \mathbb{Z} \to G$ by $f(m) = a^m$. By definition of cyclic generator, this is onto.
Case 1. If f is injective, then it is bijective. Also,

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

so f has the homomorphism property and therefore defines an isomorphism between G and $\mathbb{Z}$. That is, $G \overset{f^{-1}}{\cong} \mathbb{Z}$.

Case 2. If f is NOT injective, then by the lemma from last lecture (7.1.a), there exists $n \in \mathbb{Z}^+$ with $a^n = e$.

Pick the **smallest** such n. Define $\varphi : \mathbb{Z}_n \to G$ by $\varphi(k) = a^k$. Notice this has the homomorphism property because

$$\begin{aligned}\varphi(j +_n k) &= \varphi(j + k \text{ or } j + k - n)\\ &= a^{j+k} \text{ or } a^{j+k-n}\\ &= a^j a^k \text{ or } a^j a^k \underbrace{(a^n)^{-1}}_{e}\\ &= a^j a^k \qquad \text{(in either case)}\\ &= \varphi(j)\varphi(k)\end{aligned}$$

Also, φ is injective because if $0 \le j < k < n$ and $\varphi(j) = \varphi(k)$ then $a^k = a^j$, so $a^{k-j} = e$. However, $0 < k - j < n$, and this contradicts the choice of n as the smallest such number.
Now, φ is onto because taking any $x \in \langle a \rangle = G$ equals a^m for some $m \in \mathbb{Z}$. Write $m = qn + r$ for some $q, r \in \mathbb{Z}$ and $0 \le r < n$ (via the division algorithm). Hence $r \in \mathbb{Z}_n$ (integer in the right range), and

$$a^m = a^{qn+r} = (a^n)^q a^r = e^q a^r = a^r = \varphi(r)$$

Hence x is in the image of φ, so φ is onto, one-to-one, and has the homomorphism property, so φ specifies the isomorphism $G \overset{\varphi}{\cong} \mathbb{Z}_n$.
Now we consider the two disjoint cases:
Case 1. G is infinite and $G \cong \mathbb{Z}$.
Case 2. G is finite and $G \cong \mathbb{Z}_n$.
(a) Now if G is infinite, then we fall under Case 1, so $G \cong \mathbb{Z}$.
(b) Similarly, if G is finite, then we fall under Case 2, and hence $G \cong \mathbb{Z}_n$.
The remaining parts follow from the proof of case 2.

□

Now we have our second theorem:

Theorem 2.2. A subgroup of a cyclic group is cyclic.

Proof. Let G be a cyclic group generated by a, and let $H \le G$.
Case 1. H is trivial. Then $H = \{e\} = \langle e \rangle$ is cyclic.
Case 2. H is nontrivial. Then H contains some element $x \ne e$, say $x = a^m$ for some $m \in \mathbb{Z}$. Then $m \ne 0$. If $m > 0$ then $m \in \mathbb{Z}^+$ and $a^m \in H$. On the other hand, if $m < 0$, then $-m \in \mathbb{Z}^+$ and $a^{-m} = x^{-1} \in H$. In either case, $\exists_{n \in \mathbb{Z}^+} : a^n \in H$. Pick the smallest such n.

Now we claim that $H = \langle a^n \rangle$. To see this, let $S := \{k \in \mathbb{Z} \mid a^k \in H\}$. Then $n \in S$, and also notice $jn \in S, \forall_{j \in \mathbb{Z}}$, which is because

$$a^{jn} = (a^n)^j = x^j \in H, \forall_{j \in \mathbb{Z}}.$$

Hence $S \supseteq n\mathbb{Z}$ (recall that $n\mathbb{Z} := \{nj \mid j \in \mathbb{Z}\}$).
Now suppose $S \ne n\mathbb{Z}$. Then there exists $m \in S$ with $m \notin n\mathbb{Z}$. So m is not a multiple of n.
So m is between two consecutive multiples of n:

$$jn < m < (j + 1)n.$$

Then $0 < m - jn < n$ and

$$a^{m-jn} = a^m (a^n)^{-j} = a^m x^{-j} \in H,$$

because $a^m, x \in H$. However, this contradicts the choice of n. Hence $S = n\mathbb{Z}$.
Therefore, $H \subseteq \{a^{nj} \mid j \in \mathbb{Z}\}$ because if $x \in H$, write $x = a^m$ for some $m \in \mathbb{Z}$. Then $m \in S$, so $m \in nj$, and hence

$$x \in \{a^{nj} \mid j \in \mathbb{Z}\} = \{(a^n)^j \mid j \in \mathbb{Z}\} = \langle a^n \rangle .$$

However, we also have $a^n \in G$, so that $\langle a^n \rangle \subseteq H$. Hence $H = \langle a^n \rangle$ is cyclic, completing the proof. □

If $G = \mathbb{Z}$, then we can take $a = 1$. This brings us to our corollary:

Corollary 2.2.1. The nontrivial subgroups of $\mathbb{Z}$ are exactly $n\mathbb{Z}$ for all $n \in \mathbb{Z}^+$, and these are different.

Proof. Take $G := \mathbb{Z}$ and $a = 1$, and let H be a nontrivial subgroup of $\mathbb{Z}$. Then $H = \langle n \rangle = n\mathbb{Z}$ (where n is the smallest positive element of H). Also, for all $n \in \mathbb{Z}^+$, notice $n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ via our theorem. So we ave a one-to-one correspondence:

$$\mathbb{N} \cong \text{set of subgroups of } \mathbb{Z},$$

via the mapping $n \mapsto n\mathbb{Z}$. Note that 0 corresponds to the trivial subgroup. □

3 (Greatest Common) Divisors:

Definition: Divide -

Let $a, b \in \mathbb{Z}$ (we allow $a = 0$ or $b = 0$ or both). We say that a **divides** b and write

$$a \mid b,$$

if $aq = b$ for some $q \in \mathbb{Z}$. If so, then we also say that b is a "multiple" of a, or that a is a divisor of b.

Remark: Suppose $a \neq 0$. Then $a \mid b \iff \frac{b}{a} \in \mathbb{Z}$. If $a = 0$, then $0 \mid b \iff b = 0$.

Definition: Greatest common divisor (gcd) -

Let $r, s \in \mathbb{Z}$ (where one or both may be zero). Then the set

$$H := \{nr + ms \mid n, m \in \mathbb{Z}\}$$

is a **subgroup** of G, so it equals $d\mathbb{Z}$ for some **unique** $d \in \mathbb{N}$.
Then d is called the **greatest common divisor** of r and s, and we write:

$$d = \gcd(r, s).$$

Remark: Notice $r = 1 \cdot r + 0 \cdot s \in H$, so $d \mid r$. Similarly, $d \mid s$, so d is a **common divisor** of r and s. Since $d \in H$, there exist $m, n \in \mathbb{Z}$ such that $d = mr + ns$. So if $e \mid r$ and $e \mid s$, then $e \mid mr$ and $e \mid ns$, and hence $e \mid (mr + ns)$. Therefore, $e \mid d$, so $e \leq d$ (unless of course $d = 0$). So every common divisor is less than or equal to d, unless $= s = 0$.
Also, if $r \neq 0$ or $s \neq 0$, then $\gcd(r, s)$ is the smallest positive element of H. As for $r = s = 0$, then $\gcd(r, s) = \gcd(0, 0) := 0$.

4 Clicker Questions Again!!!

3. Let $H = 6\mathbb{Z} \cap 10\mathbb{Z}$. Then :
(A) H is not a subgroup of $\mathbb{Z}$
(B) H is a subgroup of $\mathbb{Z}$, but not a cyclic subgroup.
(C) $H = 2\mathbb{Z}$
(D) $H = 30\mathbb{Z}$
(E) None of the above.

4. Let $H = 6\mathbb{Z} \cup 10\mathbb{Z}$. Then :
(A) H is not a subgroup of $\mathbb{Z}$
(B) H is a subgroup of $\mathbb{Z}$, but not a cyclic subgroup.
(C) $H = 2\mathbb{Z}$
(D) $H = 30\mathbb{Z}$
(E) None of the above.

5 Subgroups of the Cyclic Groups

Example: Let $G = U_{10} = \langle \zeta \rangle$, where $\zeta = e^{\frac{2\pi i}{10}}$. We may ask what is $\left\langle \zeta^4 \right\rangle$? Let $b := \zeta^4$.
Drawing out a pentagram on the unit circle, we have that $\langle b \rangle$ has 5 elements (so we write $|b| = 5$). In fact, $\langle b \rangle = U_5 = \left\langle \zeta^2 \right\rangle$, where $\zeta^2 = e^{\frac{2\pi i}{5}}$.

5.1 Generalizing

Now in general, let G be a finite cyclic group of order n, generated by a, and let $s \in \mathbb{Z}$. What can we say about the cyclic subgroup $\langle b \rangle$, where $b := a^s$?
Let's revisit the proof of the earlier theorem, in that all subgroups of cyclic groups are cyclic. Let $H = \langle b \rangle$. We may ask, for which $m \in \mathbb{Z}$ is $a^m \in H$?
We notice:

$$\begin{aligned} a^m \in H &\iff a^m = b^j \text{ for some } j \in \mathbb{Z} \\ &\iff a^m = a^{sj} \\ &\iff m \equiv js \pmod{n} \\ &\iff m = in + js \text{ for some } i, j \in \mathbb{Z} \\ &\iff m \in \{in + js \mid i, j \in \mathbb{Z}\}, \end{aligned}$$

which is a subgroup of $\mathbb{Z}$ from earlier proof. The smallest positive such $m := \gcd(n, s)$, and H contains

$$a^d, a^{2d}, \ldots, a^{\frac{n}{d}d} = a^n = 1,$$

where all of these but the last are not equal to 1. So $H \supseteq \left\langle a^d \right\rangle$, and a^b has order $\frac{n}{d}$. To be continued.

Lecture ends here.

Math 113, Fall 2019
Lecture 8, Tuesday, 9/24/2019

Topics Today:

- Finish cyclic groups
- Generating sets
- Cayley digraphs (not really)

Assigned readings: §8 and 9.

We open with two clicker questions on Cayley digraphs.

1 Review from last lecture

Let G be a cyclic group generated by a, and let $n := |G|, s \in \mathbb{Z}, b := a^s$, and let $H = \langle b \rangle$. Then

$$\{k \in \mathbb{Z} \mid a^k \in H\} = \{in + js \mid i, j \in \mathbb{Z}\}$$

This is a nontrivial subgroup of $\mathbb{Z}$, equal to $d\mathbb{Z}$, where d is its smallest positive element. Then

$$d := \gcd(s, n),$$

and H contains $\{a^d, a^{2d}, \ldots, a^{\frac{n}{d}d} = 1\}$, so $H \supseteq \langle a^d \rangle$, which has $\frac{n}{d}$ elements. Now from an earlier proof (of Theorem 6.6), $H = \langle a^d \rangle$, and $|H| = \frac{n}{d}$. So we've shown part of the following theorem:

Theorem 1.1. Let G, a, and n be as above. Let $b \in G$, and pick $s \in \mathbb{Z}$ such that $b = a^s$.
Let $d := \gcd(s, n)$. Then $|B| = \frac{n}{d}$ and $\langle b \rangle = \langle a^d \rangle$. Also, for all $t \in \mathbb{Z}$,

$$\langle a^s \rangle = \langle a^t \rangle \iff \gcd(s, n) = \gcd(t, n)$$

Proof. We've computed $|b| = \frac{n}{d}$, and showed $\langle b \rangle = \langle a \rangle$. Also, $\gcd(s, n) = \gcd(t, n) \implies \langle a^s \rangle = \langle a^t \rangle$, since both equal $\langle a^d \rangle$, where $d = \gcd(s, n) = \gcd(t, n)$.
Conversely, if $\langle a^s \rangle = \langle a^t \rangle$, then $\gcd(s, n) = \frac{n}{|\langle a^s \rangle|} = \frac{n}{|\langle a^t \rangle|} = \gcd(t, n)$. □

As a corollary, we have the additional homework problem (on HW4).

Example: We showed that the subgroups of U_6 are U_1, U_2, U_3, and U_6, and $1, 2, 3, 6$ are the positive divisors of 6.
As another corollary, the cyclic generators of G are

$$\{a^s \mid \gcd(s, n) = 1\} = \{b \in G \mid \langle b \rangle = G\}.$$

2 Generating Sets

Recall that for all $a \in G$, we have:

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

We also said (or Vojta notes perhaps the book said) that $\langle a \rangle$ is the smallest subgroup of G containing a.
Let's look in more detail. Suppose we have a nonempty collection of subgroups of a group G, and let

$$K := \bigcap_{i \in I} H_i.$$

Then K is a subgroup of G.

Proof. Notice $e \in H_i$ for all i, so $e \in \cap H_i = K$. In particular, $K \neq \{\}$. Let x, y be arbitrary elements of K. Then $x, y \in H_i, \forall_i$. Therefore, $xy^{-1} \in H_i, \forall_i$, which implies $xy^{-1} \in K$, and hence $K \leq G$. □

Further, consider that $\langle a \rangle$ is the **intersection of all subgroups** of G containing a.

Proof. Let $\{H_i\}_{i \in I}$ be all subgroups of G containing a. This is a nonempty collection because it contains G. Let $K := \cap_{i \in I} H_i$. Then $\langle a \rangle \subseteq K$ because all of the H_i contain a. Hence they all contain $\langle a \rangle$. Also, $K \subseteq \langle a \rangle$ because $\langle a \rangle$ is one of the H_i. □

Vojta notes that we now have two characterizations of cyclic groups. That is, $\langle a \rangle$ is
(1) $\{a^n \mid n \in \mathbb{Z}\}$, and
(2) The intersection of all subgroups containing a.
Vojta gives the analogy that the first is the '3d printing method' , building it up piece by piece, whereas the second is the 'sculpture method', chipping away piece by piece.
Now, instead of a single element a, consider a subset of G.

3 Generating Sets

We now consider generating sets as opposed to the cyclic group generated by a single cyclic generator. We emphasize here that we take a generic subset (in fact, it's most interesting when our subset is NOT a subgroup).
Let G be a group, and let $S \subseteq G$ be a sub**set**. Let $\{H_i\}_{i \in I}$ be the set of all subgroups of G containing S.
Again, G itself is one of these subgroups, so $I \neq \{\}$.
Then we can let $K := \cap_{i \in I} H_i$. This is a subgroup of G, and it contains S. In fact, it si the smallest subgroup of G containing S. That is,

$$K \subseteq H_i, \forall_i,$$

and $K \in \{H_i\}_{i \in I}$.

Definition: Subgroup generated by a set -

$K := \cap_{i \in I} H_i$ as above is the **subgroup** of G **generated by** S, and is denoted $\langle S \rangle$.

Remark: If $S = \{a_1, \ldots, a_n\}$, then we also write:

$$\langle a_1, \ldots, a_n \rangle = \langle S \rangle .$$

and if $S = \{a_1, a_2, \ldots\}$, we write:

$$\langle a_1, a_2, \ldots \rangle = \langle S \rangle .$$

On the other hand, if we take the 3d-printing method, we have:

$$\langle S \rangle = \{s_1^{n_1}, \ldots, s_m^{n_m} \mid m \in \mathbb{N}, s_1, \ldots, s_m \in S, n_1, \ldots, n_m \in \mathbb{Z}\}$$

The right hand side (rhs) is a subgroup of G, because take $m = 0$ and $e \in rhs$. Then rhs is closed under the group operation (concatenate the formulas). Also, the rhs is closed under the inverse, namely

$$\left((s_1^{n_1} \cdots s_m^{n_m})^{-1} = s_m^{-n_m} \cdots s_1^{-n_1}\right) .$$

Also, the rhs contains S, because $\forall_{s \in S}$, take $m = n_1 = 1$ and $s_1 = s$. Also, all H_i contain the rhs (the H_i contains S and are closed under taking integer powers and taking products). Then we get the desired equality.

Examples:

- Let G be any group. Then $S = \{\}$ implies $\langle S \rangle = \{e\}$.
- $G = \mathbb{R}$ (or $\mathbb{Q}$ or $\mathbb{C}$) and $S = \{1\}$ imply $\langle S \rangle = \langle 1 \rangle = \mathbb{Z}$.
- $G = \mathbb{R}$ (or $\mathbb{C}$), and $S = \left\{\frac{1}{1}, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \ldots\right\}$. These imply that $\langle S \rangle = \mathbb{Q}$.

Definition: Generating set -

A **generating set** for a group G is a subset S of G such that $\langle S \rangle = G$. If so, then we also say that S **generates** G.

Often we'll use the word "generator" to mean an element of some **specific** generating set (otherwise it has no meaning, because always $G = \langle G \rangle$).

4 Cayley Digraphs

Vojta notes that he will hold us responsible for Cayley digraphs as discussed in the text, except the examples 7.10 and 7.12. All others are fair game.

5 Clicker Questions

3. For which of these pairs G, S is $G \neq \langle S \rangle$?
(a) $G := \mathbb{Z}, S = \{-1\}$
(b) $G = \mathbb{R}, S = (0, 1) \cup \mathbb{Z}$
(c) $G = \mathbb{C}^*, S = \mathbb{R}^* \cup U$
(d) None of the above (all S above generate the given G)
(e) $G \neq \langle S \rangle$ for more than one of the above three.

Lecture ends here.

Math 113, Fall 2019
Lecture 9, Thursday, 9/26/2019

1 Clicker Questions

1. Consider the following statements:

- α - The symmetric group S_{10} has 10 elements
- β - The symmetric group S_3 is cyclic
- γ - S_n is not cyclic for any n

Which of these are true?

It turns out, all cyclic groups are abelian, so none of the above is true.

2. Let G be a be a **finite** group.
Cayley's theorem constructs an isomorphism of G with a subgroup H of S_G.
We have $H = S_G$ if and only if:
(a) G is trivial
(b) $|G| \leq 2$
(c) $0 = 1$ (never)
(d) $G \cong S_n$ (for some $n \in \mathbb{N}$)
(e) None of the above
Vojta says this boils down to counting, and $|S_n| = n!$, so this is true precisely for $n = 1, 2$.

2 Permutation Groups

Theorem 2.1. Let A be a set. Then S_A (the set of permutations of A) is a group under composition of functions.

Proof. Composition is a well defined operation on S_A. Let $f, g \in S_A$. Then $f \circ g$ is a function from A to A, and it is bijective because it's a composition of bijections. Hence $f \circ g \in S_A$.
We check the three requirements (axioms). Associativity is proved already for composition of functions. The identity function $\mathrm{id}_A : A \to A$ is bijective, so it's in S_A. Also,

$$\mathrm{id}_A \circ f = f \circ \mathrm{id}_A = f, \forall_{f \in S_A}.$$

Finally, to check the existence of the inverse element, consider that for all $f \in S_A$, because f is a bijection, it has a (unique) inverse function $f^{-1} A \to A$ characterized by

$$f \circ f^{-1} = f^{-1} \circ f = \mathrm{id}_A,$$

so f^{-1} is an inverse **element** of f in S_A, the set of permutations (bijections). □

Vojta reminds us that we've seen this in a Clicker question, but:

Definition: Permutation group $S_{\{1,2,\ldots,n\}}$ -

For all $n \in \mathbb{N}$, S_n is the permutation group $S_{\{1,2,\ldots,n\}}$.

Notice that $|S_n| = n!$ for all $n \in \mathbb{N}$ because choosing $\sigma \in S_n$ involves n choices for $\sigma(1)$, $n-1$ choices for $\sigma(2)$, and so on until 2 choices for $\sigma(n-1)$, and 1 choice for $\sigma(n)$, where these can be in any order.

Example: One such example is to consider permutations (shuffling orders) of a deck of cards: S_{52}. So S_{52} is the set of possible rearrangements of a 52-card deck.

Example: A simpler example is S_3, which we can write as:

$$S_3 = \{\rho_0, \rho_1, \rho_2, \sigma_1, \sigma_2, \sigma_3\},$$

where $\sigma_1 := \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$ and $\rho_1 := \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$. Vojta reminds that there's a full group table on page 79 of our text.
From this table, we see that $\rho_i = \rho_1^i, \forall_{i=0,1,2}$ and $\mu_1 = \mu_1\rho_{i-1}$ (where $\mu = \sigma$). Hence $S_3 = \langle \rho_1, \mu_1 \rangle$.
Permutations tell us something about all finite groups due to the following theorem:

Theorem 2.2. If the sets A and B have the same cardinality, then $S_A \cong S_B$.

Proof. Because they have the same cardinality, that means there exists some bijection $f : A \to B$. The idea for the rest of the proof is to use f to relabel the elements of A.
Define $\varphi : S_a \to S_B$ by $\varphi(\sigma) = f \circ \sigma \circ f^{-1}$. This maps B to B

$$B \xrightarrow{f^{-1}} A \xrightarrow{\sigma} A \xrightarrow{f} B, \qquad B \xrightarrow{f \circ \sigma \circ f^{-1}} B$$

and it is bijective because it's a composition of bijections. Similarly, define $\phi : S_B \to S_A$ by $\psi(\tau) = f^{-1} \circ \tau \circ f$ for all $\tau \in S_B$. Then

$$\psi \circ \varphi : S_A \to S_A = \mathrm{id}_{S_A},$$

because

$$\begin{aligned} \psi(\varphi(\sigma)) &= f^{-1} \circ (f \circ \sigma \circ f^{-1}) \circ f \\ &= \cancel{f^{-1} \circ f} \circ \sigma \circ \cancel{f^{-1} \circ f} \\ &= \sigma \\ &= \mathrm{id}_{S_A}(\sigma), \forall_{\sigma \in S_A}. \end{aligned}$$

Similarly, $\varphi \circ \psi = \mathrm{id}_{S_B}$. Therefore, φ is bijective, because it has an inverse, namely ψ.
Now to exhibit the homomorphism property, consider:

$$\begin{aligned} \varphi(\sigma_1) \circ \varphi(\sigma_2) &= f \circ \sigma^1 \circ f^{-1} \circ f \circ \sigma_2 \circ f^{-1} \\ &= f \circ \sigma_1 \circ \sigma_2 \circ f^{-1} \\ &= \varphi(\sigma_1 \circ \sigma_2), \forall_{\sigma_1, \sigma_2 \in S_A}. \end{aligned}$$

Then $\varphi : S_A \xrightarrow{\sim} S_B$, as required.

□

Definition: Dihedral group D_n -

For an integer $n \geq 3$, the **dihedral group** D_n is the group of symmetries (rigid motions) of a regular n-gon.
Moreover,

$$|D_n| = 2n$$

Notice that D_n has a subgroup $\cong \mathbb{Z}_n$, namely the rotations in the plane of the polygon. Moreover,

$$\underbrace{\mathbb{Z}_n}_{|\mathbb{Z}_n|=n} < \underbrace{D_n}_{|D_n|=2n} \leq \underbrace{S_n}_{|S_n|=n!},$$

where for all $n \geq 4$, the right 'inequality' is strict (it is a proper subgroup), and the left inequality is strict for all $n \leq 2$.

Theorem 2.3. (Cayley's Theorem) Every group G is isomorphic to a subgroup of S_A for some set A.

In fact, we'll show it's true with $A = G$. Keep in mind the following example:

$+_3$	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

Proof. In fact, we'll show it's true with $A = G$. We'll construct an isomorphism $\varphi : G \to H$ for some $H \leq S_G$.
To do this, define

$$\lambda_x : G \to G$$
$$\lambda_x(g) = xg, \forall_{g \in G}.$$

Note $\lambda_x = S_G$ because every element of G occurs exactly once in each row of the group table. Hence λ_x is bijective. Therefore we have $\varphi : G \to S_G$ is well defined.
Now φ is injective because all of the rows in the group are different (actually, $\lambda_x = \lambda_y \implies \lambda_x(e) = \lambda_y(e) \implies x = y$ because $\lambda_x(e) = xe = x$ and $\lambda_y = y$ similarly).
Now for the homomorphism property, consider:

$$\begin{aligned}\varphi(x) \circ \varphi(y) &= \lambda_x \circ \lambda_y \\ &= (g \mapsto \lambda_x(\lambda_y(g)) = x(yg) = (xy)g = \lambda_{xy}(g)) \\ &= \varphi(xy).\end{aligned}$$

Then by Lemma 8.15, φ is a group isomorphism (isomorphism of groups) with a subgroup of S_G. □

3 Clicker Questions

3. Let $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 5 & 6 & 3 & 1 & 4 & 2 \end{pmatrix} \in S_6$.
Then all of the orbits of σ are:
$\{1, 4, 5\}, \{2, 6\}, \{3\}$.

4. How many of the following are true, for the same σ as before?

$$\sigma = (1, 5, 4)(2, 6)(3)$$
$$\sigma = (1, 5, 4)(2, 6)$$
$$\sigma = (1, 5, 4)(6, 2)$$
$$\sigma = (1, 4, 5)(2, 6) \text{ this is false}$$
$$\sigma = (5, 4, 1)(2, 6)$$

All but the fourth one are true.

4 Orbits and Cycles

Given a set A and permutation $\sigma \in S_A$, we define a relation on A by $a \sim b$ if

$$\sigma^n(a) = b,$$

for some $n \in \mathbb{Z}$. This is an equivalence relation, where:

$$\text{reflexivity} : \sigma^p(a) = a, \forall_{a \in A}$$
$$\text{symmetry} : \sigma^n(a) = b \implies \sigma^{-n}(b) = a$$
$$\text{transitivity} : \sigma^n(a) = b, \sigma^m(b) = c \implies \sigma^{n+m}(a) = c.$$

Now because this is an equivalence relation, the cells of the corresponding partition are called "orbits" of σ.

Definition: Cycle -

We introduce **cycle notation**:

$$\sigma := (a_1, a_2, \ldots, a_n), \text{ with } a_1, \ldots, a_n \in A \text{ mutually distinct}$$

which means

$$\sigma(a_i) = a_{i+1}, \quad \forall_{i=1,\ldots,n-1},$$
$$\sigma(a_n) = a_1,$$

and

$$\sigma(a) = a, \quad \forall_{a \notin \{a_1, \ldots, a_n\}}.$$

If σ is of this form, then we say it's a **cycle**.

Definition: Disjoint Cycles -

The cycles σ and τ are **disjoint** if

$$\{a \in A : \sigma(a) : \sigma(a) \neq a\} \cap \{a \in A : \tau(a) \neq a\} = \{\}$$

Vojta notes that the identity element is always a cycle (even in $S_\emptyset$ by definition).

Lecture ends here.

Math 113, Fall 2019
Lecture 10, Thursday, 10/1/2019

1 Clicker Questions

1. Write

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 1 & 6 & 2 & 4 & 7 & 3 \end{pmatrix} \in S_7$$

as a product of disjoint cycles.
Answer: One product is $(4, 2, 1, 5)(6, 7, 3)$ and another is $(1, 5, 4, 2)(3, 6, 7)$.

2. Which of the following are odd permutations?

$$\alpha = (1, 2)(2, 3)(3, 4) \in S_4$$
$$\beta = (1, 2, 3, 4, 5, 6, 7, 8, 9, 10) \in S_{10}$$
$$\gamma = (1, 2, 3)(2, 4)(1, 3, 5) \in S_6.$$

Answer: All of them are odd permutations. We can write

$$\beta = (1, 2)(2, 3)(3, 4)(4, 5)(5, 6)(6, 7)(7, 8)(8, 9)(9, 10).$$

2 Even and Odd Permutations

Theorem 2.1. Every permutation of a finite set can be written as a product of disjoint cycles.
In addition, this is **unique** up to:
(1) Writing the cycles in a different order (disjoint cycles commute), and
(2) choosing a (possibly) different starting point for each cycle.

One particular kind of cycle is:

Definition: Transposition -

A **transposition** is a cycle of length 2.
(This is only defined for some (a, b) where $a, b \in A$ and $a \neq b$.)

Vojta notes that these have the following central role:

Proposition 2.1.1. Every permutation of a finite set can be written as a product of transpositions.

Notice that we leave out the word 'disjoint' here because that would be false.

Proof. Use Thm 9.8 and the identity

$$(a_1, a_2, \ldots, a_n) = (a_1, a_2)(a_2, a_3) \cdots (a_{n-1}, a_n).$$

□

Then we have the following theorem:

Theorem 2.2. No permutation in (any finite set which would then be isomorphic to) S_n can be expressed both as a product of an even number of transpositions and as a product of an odd number of transpositions.

We'll sketch the book's second proof (as the first proof uses linear algebra's concept of the determinant, where many linear algebra texts rely on this theorem to develop the theory of determinants). The book shows that if $\sigma \in S_n$ is a permutation and $\tau \in S_n$ is a transposition, then:

$$(\#\text{ of orbits of } \sigma\tau) = (\#\text{ of orbits of } \sigma) \pm 1.$$

This rules out the possibility that the odd and even possibilities are concurrent. Vojta gives that the book thereafter is a bit sketchy, so we add a few more points.
We show that if σ is a product of m transpositions, then

$$m \equiv n - (\#\text{ of orbits of } \sigma) \pmod 2$$

To prove this, we use induction on m. Base case is $m = 0$ with $m = 0$ implies that σ is the identity, which implies that it has n orbits, with both sides of the congruence simply equals 0. Then the inductive step is easy.
Then, suppose σ is a product of m transpositions and is also a product of m' transpositions. Then notice

$$m = \underbrace{n - (\#\text{ orbits of } \sigma)}_{} \equiv m' \pmod 2,$$

where the underbraced portion depends only on σ. So $m \cong m' \pmod 2$.
This then allows us to define even and odd permutations, where any permutation is either one or the other (and not both).

Definition: Alternating Group -

The set $A_n = \{\sigma \in S_n \mid \sigma \text{ is even}\}$ is a subgroup of S_n, called the **alternating group**.

Vojta comments that the inverse of an even permutation is also even. Let's look at some examples.

2.1 Examples

Example:
Recall:

$$S_3 = \{\underbrace{\rho_0 = (1), \rho_1 = (1,2,3), \rho_2 = (1,3,2)}_{A_3,\text{ even}}, \underbrace{\mu_1 = (2,3), \mu_2 = (1,3), \mu_3 = (1,2)}_{\text{odd}}\}$$

If $n = 0$ or 1 then S_n is trivial, and so is A_n. Hence $|S_n| = |A_n| = 1$.
If $n \geq 2$, then $\sigma \mapsto \sigma \circ (1,2)$ maps $A_n \to S_n \setminus A_n$, and this is bijective. Hence

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

Example: Recall at the beginning of the semester, we brought up the 15-puzzle. We teased that the solution of the 15-puzzle cannot be found if any two adjacent squares are interchanged.

3 More Clicker Questions

3. Let G be a finite cyclic group (order n) generated by element a, and let $b = a^s$. Then the **index** of the cyclic subgroup $\langle b \rangle$ of G is?

Answer: The index of $\langle b \rangle$ is

$$\frac{n}{\frac{n}{\gcd(s,n)}} = \gcd(s,n)$$

because the order of $\langle b \rangle$ is $\frac{n}{\gcd(s,n)}$. In Vojta's words, recall from before that

$$\langle b \rangle = \left\langle a^{\gcd(s,n)} \right\rangle$$

has $\frac{n}{\gcd(s,n)}$ elements, so as above, we have $\gcd(s,n)$.

4. How many of the following statements are true?

(T) A subgroup of a group is a left coset of itself; true by taking the identity $eH = H$
(F) Every finite group G contains an element of every order that divides the order of G; false via S_3, because if this were true, every group would be cyclic (order 6, but has no element of order 6, otherwise it would be cyclic)
(T) Every group of prime order is abelian; true because such groups are cyclic and hence abelian
(T) A_n is of index 2 is $S_n, \forall_{n>1}$.

4 Cosets and Lagrange's Theorem

Definition: Cosets -

Let H be a subgroup of a group G. Then a **left coset** of H in G is a sub**set** of G of the form

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

for some $a \in G$.

In additive notation, this is

$$a + H = \{a + h : h \in H\}.$$

4.1 Facts about cosets

(Fact 1) $|aH| = |H|$ because $h \mapsto ah$ is a bijection $H \to aH$.

(Fact 2) $a \in aH, \forall_{a \in G}$. In particular, $aH \neq \emptyset, \forall_{a \in G}$, and $\cup_{a \in G} aH = G$.

(Fact 3) $b \in aH \implies bH = aH$.

Proof. Notice $b \in aH \implies b = ah$, for some $h \in H$. Then $bH = (ah)H = a(hH) = aH$. Recall that for every subset S of G and all $a \in G$, we defined $aS = \{as : s \in S\}$ as before. Then for all $a, b \in G, S \subseteq G$, we have

$$(ab)S = a(bS),$$

where $\{(ab)s : s \in S\} = \{a(bs) : s \in S\}$.
Finally, $hH = H, \forall_{h \in G}$, which Vojta leaves as an exercise. □

(Fact 4) If $aH \cap bH \neq \emptyset$, then $aH = bH$.

Proof. Pick $c \in aH \cap bH$. Then $aH = cH = bH$, by fact (3) above. □

Then facts (2) and (4) together imply the following theorem:

Theorem 4.1. Let H be a subgroup of a group G. Then the left cosets of H form a partition of G.

Vojta notes that the book presents this in a different way, constructing the corresponding equivalence relation. That is, $aH = bH \iff b^{-1}a \in H$.
We'll look at some examples.

Example: Let $H = \langle \mu_3 \rangle = \{\rho_0, \mu_3\} \in S_3$, where $\mu_3 = (1, 2)$.
Its left cosets are

$$\begin{aligned} \rho_0 H &= H = \{\rho_0, \mu_3\} \\ \rho_1 H &= \{\rho_1\rho_0, \rho_1, \mu_3\} = \{\rho_1, \mu_1\} \\ \rho_2 H &= \{\rho_2\rho_0, \rho_2\mu_3\} = \{\rho_2, \mu_2\}, \end{aligned}$$

via the table on page 79.
Then its right cosets are $\{\rho_0, \mu_3\}, \{\rho_1, \mu_1\}$, and $\{\rho_2, \mu_2\}$.
Notice that $H\rho_1 \neq \rho_1 H$.

Definition: $(G : H)$**, left coset -**

If $H < G$, then $(G : H)$ is the number (or cardinality) of left cosets of H in G.

On our homework, we prove that this is the same as the cardinality of **right** cosets of H in G.
This brings us to an important theorem, where we deviate a little from the book:

Theorem 4.2. (**Lagrange's Theorem**) Let G be a finite group and let H be a subgroup of G. Then

$$|G| = (G : H)|H|.$$

In particular, $|H|$ divides $|G|$.

Proof.

$$\begin{aligned} G &= \sum_{\text{cosets } aH} |aH| \\ &= \text{sum of } |H| \text{ added } (G:H) \text{ times} \\ &= (G:H)|H| \end{aligned}$$

□

4.2 Corollaries of Lagrange's Theorem

Corollary 4.2.1. If G is finite, then

$$(G:H) = \frac{|G|}{|H|}.$$

Corollary 4.2.2. Every group of prime order is cyclic.

Corollary 4.2.3. If G is a finite group with order n, then $a^n = e$, for all $a \in G$.

Proof. Let $m = |a|$. Then $m = |\langle a \rangle|$ divides n, so $a^n = (a^m)^{n/m} = e^{n/m} = e$. □

Now a fact:

S_3 is the smallest non-abelian group.

Proof. If $|G| = n < 6$, then

$$|G| = 2, 3, 5$$

imply n is prime, so G is cyclic, and hence abelian. Then if $|G| = 4$ (had an element of order 4), then it's cyclic and hence abelian. Otherwise, all $a \in G$ have order 1 or 2. Then this implies that $a^2 = e, \forall_{a \in G}$, which implies $a = a^{-1}, \forall_{a \in G}$, and hence

$$ab = (ab)^{-1} = b^{-1}a^{-1} = ba, \forall_{a,b \in G},$$

which is close to exercise 4.36 in the text. □

5 Introduction: Products of Groups

The groups we've developed so far are:

- cyclic
- permutation
- dihedral
- numbers: $(\mathbb{Q}, \mathbb{R}, \mathbb{C}, \mathbb{Q}^*, \ldots, U)$
- matrices
- Klein V

We can use groups we know about as building blocks to create other groups.

Recall that if $S_1, \ldots, S_n$ are sets, then their product

$$\prod_{i=1}^{n} S_i = S_1 \times \cdots \times S_n$$

is defined to be the set of all ordered n-tuplies $(s_1, \ldots, s_n)$, such that $s_i \in S_i$, for all i. A canonical example is $\mathbb{R}^n = \mathbb{R} \times \cdots \times \mathbb{R}$ (n times).

Then we can make the following definition:

Definition: Group product -

Let $G_1, \ldots, G_n$ be groups. Then their **product**

$$\prod_{i=1}^{n} G_i = G_1 \times \cdots \times G_n$$

is the set $\prod_{i=1}^{n} G_i$, with group operation defined component-wise.

So if $n = 2$, then $(a_1, a_2)(b_1, b_2) = (a_1 b_1, a_2 b_2)$, and $(a_1, a_2)^{-1} = (a_1^{-1}, a_2^{-1})$, the identity element is (e_1, e_2) where e_i is the identity of G_i, for all i.

Remark: If all G_i are abelian, then so are their products.

This is easy to see, and we may refer to their product as their **direct sum**:

$$\bigoplus_{i=1}^{n} G_i = G_1 \oplus G_2 \oplus \cdots \oplus G_n.$$

Lecture ends here.

Math 113, Fall 2019
Lecture 11, Thursday, 10/3/2019

1 Clicker Questions

1. Which of the groups

$$G_1 = \mathbb{Z}_6 \times \mathbb{Z}_{20} \cong \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_4 \times \mathbb{Z}_5$$
$$G_2 = \mathbb{Z}_{15} \times \mathbb{Z}_8 \cong \mathbb{Z}_5 \times \mathbb{Z}_3 \times \mathbb{Z}_8$$
$$G_3 = \mathbb{Z}_{12} \times \mathbb{Z}_{12} \cong \mathbb{Z}_4 \times \mathbb{Z}_3 \times \mathbb{Z}_2 \times \mathbb{Z}_5$$

Answer: $G_3 \cong G_1 \ncong G_2$.

2. Let $G := \mathbb{Z}_3 \times \mathbb{Z}_9 \times \mathbb{Z}_9 \times \mathbb{Z}_{27}$. Let m be the number of elements of G of order ≤ 3.
Choose the following correct answer:
(A) $m \leq 3$
(B) $3 < m \leq 27$
(C) $27 < m \leq 81$
(D) $81 < m < |G|$
(E) $m \geq |G|$
Answer: Notice $|G| = 3^8$ (which is an odd order), so no elements are of order 2. Then $a \in G$ has order ≤ 3 if and only if its order divides 3.

2 Review

Last time we defined the (finite) product of groups

$$G_1 \times \cdots \times G_n = \prod_{i=1}^{n} G_i.$$

Also, if $G_1, \ldots, G_n$ are abelian, then so is their product. In this case, we may also call $\prod G_i$ the "direct sum", and write it as

$$G_1 \oplus \cdots \oplus G_n \quad \text{or} \quad \bigoplus_{i=1}^{n} G_i.$$

A word of caution: One can also define an infinite product $\prod_{i \in I} G_i$ with $|I| = \infty$. However, in this case, if all G_i are abelian, the direct sum is different.

3 Examples of Products:

(0) The additive group of a product of vector spaces.
(1) The Klein V group is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ (other isomorphisms are possible)

$$e \leftrightarrow (0,0)$$
$$a \leftrightarrow (0,1)$$
$$b \leftrightarrow (1,0)$$
$$c \leftrightarrow (1,1)$$

(2) How about $\mathbb{Z}_2 \times \mathbb{Z}_3$? What is the order of $(1,1)$? We note that the order of this must divide the order of the group, which is 6. The fact that $(1,1), 2(1,1), 3(1,1)$ are all not $(0,0)$ shows that the order is not 1,2,3 respectively. Hence it must have order 6.
This is a special case of the following theorem:

Theorem 3.1. Let $(a_1, \ldots, a_n) \in G_1 \times \cdots \times G_n$. If a_i is of finite order r_i in G_i, then for all i, the order of $(a_1, \ldots, a_n)$ is equal to the least common multiples of each of their orders. That is,

$$\text{order}(a_1, \ldots, a_n) = \text{lcm}(r_1, \ldots, r_n).$$

Proof. The proof in the text is the same as we've done in the previous example. □

Corollary 3.1.1. Let $m_1, \ldots, m_n \in \mathbb{Z}^+$. Then the largest order of an element of $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n}$ is $\text{lcm}(m_1, \ldots, m_n)$, and it occurs with the element $(1, 1, 1, \ldots, 1)$, where 1 means 0 if $m_i = 1$).

Proof. Let $(a_1, \ldots, a_n) \in \prod \mathbb{Z}_{m_i}$, and let $r_i := |a_i|$. Then $r_i | m_i \forall_i$, so

$$|(a_1, \ldots, a_n)| = \text{lcm}(r_1, \ldots, r_n) \mid \text{lcm}(m_1, \ldots, m_n),$$

so it's less than or equal to $(\leq)$.
If $a_1 = 1$ for all i, then $r_i = m_i, \forall_i$, and we have equality. □

Corollary 3.1.2. Let $m, n \in \mathbb{Z}^+$. Then $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic if and only if $\gcd(m, n) = 1$.
If so, then $\mathbb{Z}_m \times \mathbb{Z}_n \cong \mathbb{Z}_{mn}$, and $\mathbb{Z}_m \times \mathbb{Z}_n$ is generated by $(1, 1)$.

Proof. Notice $\gcd(m, n) = 1$ implies that $\text{lcm}(m, n) = \frac{m}{\gcd(m,n)} = mn$, which then implies that $\mathbb{Z}_m \times \mathbb{Z}_n$ is cyclic, generated by $(1, 1)$.

On the other hand, $\gcd(m, n) \neq 1$ implies $\gcd(m, n) > 1$, which then implies $\text{lcm}(m, n) < mn$, and so $\mathbb{Z}_m \times \mathbb{Z}_n$ has no element of order mn. Hence $\mathbb{Z}_m \times \mathbb{Z}_n$ is NOT cyclic. □

4 Facts about Products

4.1

$G_1 \times G_2 \cong G_2 \times G_1$, and

$$(G_1 \times G_2) \times G_3 \cong G_1 \times (G_2 \times G_3) \cong G_1 \times G_2 \times G_3.$$

Similarly, products of higher numbers of groups also commute and associate (up to isomorphism).

5 Finitely Generated Abelian Groups

Definition: Finitely generated -

A group is **finitely generated** if it can be generated by a finite subset.

Example: Any finite group G with $G = \langle G \rangle$, the group $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{mn}$, and

$$\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n} \times \mathbb{Z} \times \cdots \times \mathbb{Z}, (m_1, \ldots, m_n \in \mathbb{Z}^+).$$

Theorem 5.1. (Fundamental Theorem of Finitely Generated Abelian Groups.)

Let G be a finitely generated abelian group. Then

$$G \cong \mathbb{Z}_{p_1^{r_1}} \times \cdot \times \mathbb{Z}_{p_n^{r_n}} \times \mathbb{Z} \times \cdots \times \mathbb{Z},$$

where $n \in \mathbb{N}$, where primes $p_1, \ldots, p_n$ may be repeated, and $r_1, \ldots, r_n \in \mathbb{Z}^+$. Moreover, these factors are unique, up to reordering them.

We won't prove this result. The converse states that all groups of the form

$$\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_n} \times \mathbb{Z} \times \cdots \times \mathbb{Z}$$

are finitely generated abelian groups. Additionally, we can make this representation unique by requiring that

$$p_1 \leq p_2 \leq \cdots \leq p_n,$$

and $r_i \geq r_{i+1}$ whenever $p_i = p_{i+1}$.
However, the isomorphism need not be unique. For example, recall that $V \cong \mathbb{Z}_2 \times \mathbb{Z}_2$ in many ways.

5.1 Examples

(1) $\mathbb{Z}_4 \times \mathbb{Z}_{12} \cong \mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_5$.
(2) Find (up to isomorphism) all groups of order $96 = 2^5 \cdot 3$.

Solution. For $p = 3$, we can only have one $p_i = 3$, and its exponent must be 1: $p_n = 3, r_n = 1$.
For $p = 2$, we have $p_1 \cdots p_{n-1} = 2$ (where $n > 1$) and $R_1 + \cdots + r_{n-1} = 5$.
How many ways are there to write 5 as $r_1 + \cdots + r_{n-1}$ with integers $r_1 \geq r_2 \geq \cdots \geq r_{n-1} > 0$? We find 7 possibilities:

$$\begin{aligned}
r_1 = 5 &\implies n = 2, 5 = 5 \\
r_1 = 4 &\implies n = 3, 5 = 4 + 1 \\
r_1 = 3 &\implies 5 = 3 + 2 = 3 + 1 + 1 \\
r_1 = 2 &\implies 5 = 2 + 2 + 1 = 2 + 1 + 1 + 1 \\
r_1 = 1 &\implies 5 = 1 + 1 + 1 + 1 + 1.
\end{aligned}$$

□

(3) Find all abelian groups of order 10.

Solution. This is much easier: it's just $\mathbb{Z}_2 \times \mathbb{Z}_5$, because $10 = 2 \times 5$. This is the same for all products of distinct primes (Them 11.17). □

6 Clicker Question

3. Which of the following **must be** homomorphisms?
(A) $\varphi : H \to G$ given by $\varphi(x) = x, \forall_{x \in H}$, where $H \leq G$, for all G, H.
(B) $\varphi : G \to G$ given by $\varphi(x) = x^{-1}, \forall_G$.
(C) $\psi \circ \varphi : G \to G''$, where $\varphi : G \to G'$ and $\psi : G' \to G$" are homomorphisms, for all $G, G', G", \varphi, \psi$.
Answer: (A) and (C) are true.

4. How many of the following are true:
(1) A_n is a normal subgroup of S_n (for all $n \in \mathbb{N}$) (true)
(2) For all groups G, G', there exists a homomorphism from G to G' (true, just take the trivial homomorphism)
(3) A homomorphism is one-to-one if and only if its kernel is the trivial subgroup (true)
(4) The image of a group of 6 elements under a homomorphism may have 12 elements (false)
(5) It is not possible to have a nontrivial homomorphism from some finite group to some infinite group (false; an example would be $U_3 \to \mathbb{C}^*$.)

Lecture ends here.

Math 113, Fall 2019

Lecture 12, Tuesday, 10/8/2019

Absent, out of state. Midterm exam in-class next Tuesday.