FEBRUARY 8 NOTES

1. Section 2: Groups

Definition 1.1. A **group** is a set G with a binary operation $\star$ on G such that:

(1) (associativity) $\star$ is associative, i.e. for every $x, y, z \in G$,

$$(x \star y) \star z = x \star (y \star z).$$

(2) (identity) there is an element $e \in G$ such that, for any $x \in G$,

$$x \star e = e \star x = x.$$

The element $e \in G$ is called the **identity element** or **identity of** G.

(3) (inverses) for each element $x \in G$, there is an element $y \in G$ such that

$$x \star y = y \star x = e.$$

The element y is called the **inverse** of x and is denoted by $y = x^{-1}$ or $y = -x$, depending on the context.

We denote groups by $(G, \star)$ or just by G if $\star$ is 'clear from context.'

For a general group G, $\star$ does not have to be commutative. We have a special name for the groups where $\star$ is commutative.

Definition 1.2. If $(G, \star)$ is a group and $\star$ is commutative, then G is called an **abelian** group.

Today, we will mostly focus on examples of groups. First, a reminder: let $n \in \mathbb{Z}$ be a positive integer. For $a \in \mathbb{Z}$, the notation $a \pmod{n}$ means the (positive) remainder of a when divided by n. For example: $4 \pmod 3 = 1$; $11 \pmod 4 = 3$, $-2 \pmod 3 = 1$, etc. Writing $a = b \pmod n$ means that a and b have the same remainder when divided by n.

Formally, the 'remainder' is defined as follows.

Division algorithm. Suppose n is a positive integer. Then, for any $a \in \mathbb{Z}$, there exist unique integers q, r such that $a = qn + r$ and $0 \leq r < n$. The integer q is called the **quotient** of a by n, and the integer r is called the remainder.

Proof. First, we will show that q and r exist. Let q be the largest multiple of n that is less than a, i.e. $qn \leq a < (q+1)n$. Then, defining r to be $r = a - qn$, by subtracting qn from the inequality $qn \leq a < (q+1)n$, we see that $0 \leq r < n$. Therefore, $a = qn + r$ where $0 \leq r < n$.

Next, we will show that q and r are unique. Suppose that $a = q_1 n + r_1$ and $a = q_2 n + r_2$ where $0 \leq r_1, r_2 < n$. Then, subtracting one equation from the other, we see that $(q_1 - q_2)n = r_2 - r_1$. Because $|r_2 - r_1| < n$ (because each were less than n), and $r_2 - r_1$ is a multiple of n, this implies that $r_2 - r_1 = 0$ and then $q_1 - q_2 = 0$. Therefore, $r_2 = r_1$, and $q_1 = q_2$ so q and r are unique. □

Definition 1.3. Given any integer a, the number $a \pmod n$ is the unique integer r in the Division algorithm.

Example 1.4. Let n be a positive integer and let $\mathbb{Z}_n := \{0, 1, 2, \ldots, n-1\}$. Let $+_n$ denote the binary operation $a +_n b = a + b \pmod n$. Then, $+_n$ is a binary operation on $\mathbb{Z}_n$: the elements of $\mathbb{Z}_n$ are precisely the remainders when we divide by n, and taking the sum of any two elements mod n gives another element in $\mathbb{Z}_n$.

Additionally, $(\mathbb{Z}_n, +_n)$ is a group. The binary operation is associative (this is something you probably proved in Math 300) and there is an identity element 0: for any $a \in \mathbb{Z}_n$, $a +_n 0 = 0 +_n a = a$.

Finally, each element $a \in \mathbb{Z}_n$ has an inverse. If $a = 0$, then its inverse is 0: $0 + 0 = 0$. If $a \neq 0$, then $n - a \in \mathbb{Z}_n$, and $n - a$ is the inverse of a because $a +_n (n - a) = (n - a) +_n a = 0$. Because $+_n$ is commutative, this an abelian group.

For any finite group, we can make a table describing the binary operation by listing the elements across the first row and down the first column. Then, we fill in each entry of the table with $a \star b$, where a is the first entry of that row and b is the first entry of that column. For example, if our group only had two elements a, b, we would create the table:

$\star$	a	b
a	$a \star a$	$a \star b$
b	$b \star a$	$b \star b$

Let's try with $\mathbb{Z}_2 = \{0, 1\}$ and $\mathbb{Z}_3 = \{0, 1, 2\}$. In these cases, we get:

$+_2$	0	1
0	0	1
1	1	0

and

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

Is there anything that you notice about these tables?

Another reminder from last week:

Definition 1.5. We define $M_n(\mathbb{R})$ to be the set of all $n \times n$ matrices. We define $GL_n(\mathbb{R})$ to be the set of all invertible $n \times n$ matrices.

Example 1.6. $(M_n(\mathbb{R}), +)$ is an abelian group. Addition is an associative binary operation, the identity element is the zero matrix and, given a matrix A, the inverse is $-A$.

$(GL_n(\mathbb{R}), \times)$ is a non-abelian group. Multiplication is a binary operation on $GL_n(\mathbb{R})$: given two invertible matrices $A, B \in GL_n(\mathbb{R})$, their product AB is an $n \times n$ invertible matrix. We know this from linear algebra: a matrix M is invertible if and only if $\det M \neq 0$, so $A, B \in GL_n(\mathbb{R})$ means $\det A, \det B \neq 0$. This implies that $\det(AB) = \det(A)\det(B) \neq 0$, so AB is invertible. Then, the identity element is I the $n \times n$ identity matrix, and given any $A \in GL_n(\mathbb{R})$, by definition, A^{-1} exists, so inverses exist.

Example 1.7. From the worksheet, we saw that $\cdot$ was a binary operation on $S = \{a+bi \in \mathbb{C} \mid a^2+b^2 = 1\}$. Because $\cdot$ is just multiplication, it is associative. This set also has an identity and inverses: $1 = 1+0i$ is the identity, because $1 \cdot (a + bi) = a + bi$, and given any $a + bi \in S$, because $a^2 + b^2 = 1$, we can show that $(a + bi)(a - bi) = a^2 + b^2 = 1$, so $(a + bi)^{-1} = a - bi$. Therefore, $(S, \cdot)$ is a group! As we discussed, S is actually the unit circle, so geometric objects can be groups.

Example 1.8. If X is a nonempty set, is $(\mathcal{P}(X), \cup)$ a group?

The answer is no! We already proved that $\cup$ is an associative binary operation. What would the identity element be? It must be some set $E \subset X$ such that $E \cup A = A \cup E = A$ for every set A in X. This is possible if and only if $E = \emptyset$. But, this means elements do not have inverses: the inverse of an element $A \in \mathcal{P}(X)$ must be some element B such that $A \cup B = \emptyset$. But, if $A \neq \emptyset$, it is impossible that $A \cup B = \emptyset$, so inverses cannot exist!

Example 1.9. If X is a set, is $(\mathcal{P}(X), \Delta)$ a group?

The answer is yes! On the worksheet, you showed that Δ is an associative binary operation. (Reminder: $A \Delta B = (A - B) \cup (B - A)$.) Does this have an identity? Given any $A \subset X$, we need an element $E \subset X$ such that $A\Delta E = (A-E)\cup(E-A) = A$. This is only possible if E is contained in A, and the only set contained in every other set is $E = \emptyset$. So, we must have $E = \emptyset$. Then, what is A^{-1}? It must be some set B such that $A\Delta B = (A - B) \cup (B - A) = \emptyset$. This is only possible if $B = A$, because then $A - B = B - A = \emptyset$. But, this says $A = A^{-1}$ so inverses exist and this is a group!