Definition: A non-empty set G equipped with a binary operation $* : G \times G \to G$ is a **group** if...

- **Closure:**[*] $a * b \in G$ for all $a, b \in G$.
- **Associativity:** $(a * b) * c = a * (b * c)$ for all $a, b, c \in G$.
- **Identity:** There exists $e \in G$ such that $a * e = a = e * a$ for all $a \in G$.
- **Inverses:** For each $a \in G$ there exists $b \in G$ such that $a * b = e = b * a$.

If in addition, we have...

- **Commutativity:** $a * b = b * a$ for all $a, b \in G$.

then G is called an **abelian group** or sometimes a **commutative group**.

EXAMPLES:

Numbers under addition: Many of our familiar number systems form abelian groups under addition. For example, $\mathbb{Z}$ (integers), $\mathbb{Q}$ (rational numbers), $\mathbb{R}$ (real numbers), and $\mathbb{C}$ (complex numbers) are all examples of infinite abelian groups when given the operation of addition.

In each case 0 is the identity and the inverse of x would be $-x$. These are abelian groups because addition is commutative: $x + y = y + x$.

Numbers under multiplication: Our same number systems *do not* form groups under multiplication. However, if we discard elements without multiplicative inverses, we do obtain groups. For example, $\mathbb{Q}^\times = \mathbb{Q} - \{0\}$ (nonzero rationals), $\mathbb{R}^\times = \mathbb{R} - \{0\}$ (nonzero reals), and $\mathbb{C}^\times = \mathbb{C} - \{0\}$ (nonzero complex numbers) give us examples of infinite abelian groups under multiplication.

With the integers we have to toss out a lot! The only integers with *integer* multiplicative inverses are ± 1. We have $\mathbb{Z}^\times = \{1, -1\}$ is a finite abelian group (of order 2) under multiplication.

In each case 1 is the identity and the inverse of x would be $x^{-1} = \frac{1}{x}$. Again, these are abelian groups because multiplication is commutative: $xy = yx$.

Even vs. Odd: The even integers $\mathbb{E} = 2\mathbb{Z} = \{2k \mid k \in \mathbb{Z}\}$ are also an infinite abelian group. However, the odd integers are not. Notice that $3 + 5 = 8$ (odd plus odd is not odd). Thus odd integers are not closed under addition. Similar statements could be made about rational vs. irrational numbers under addition or nonzero rational vs. irrational under multiplication.

Modular Arithmetic: Let n be a positive integer. Then the equivalence classes modulo n, denoted $\mathbb{Z}_n$, form a *finite* abelian group under addition mod n. On the other hand, they do not form a group under multiplication mod n. But just like the other number systems, if we toss out elements without multiplicative inverses, we are left with a group under multiplication mod n. In particular, $\mathbb{Z}_n^\times = U(\mathbb{Z}_n) = U(n) = \{k \in \mathbb{Z}_n \mid \gcd(k, n) = 1\}$ (classes mod n whose representatives are relatively prime to the modulus n) form a finite abelian group under multiplication mod n.

Vector Spaces: Vector spaces are abelian groups under addition with the zero vector being the identity. For example, $\mathbb{R}^n$ is an abelian group under addition.

New from Old: When $R = \mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, or $\mathbb{Z}_\ell$ (for some fixed positive integer ℓ)[†], we can add $\mathbb{R}^n$ (n-tuples with entries in R), $R^{m \times n}$ ($m \times n$ matrices with entries in R), $R[x]$ (polynomials with coefficients in R). In each case we get an abelian group under addition.

If we consider $R^{n \times n}$ (square matrices), we can also multiply. If we just consider invertible matrices, $\mathrm{GL}_n(R) = \{A \in R^{n \times n} \mid \det(A)^{-1} \text{ exists }\}$ (the general linear group of $n \times n$ matrices with entries in R), we obtain a nonabelian (for $n \geq 2$) group under matrix multiplication whose identity is the identity matrix.

In particular, $\mathrm{GL}_n(\mathbb{R}) = \{A \in \mathbb{R}^{n \times n} \mid \det(A) \neq 0\}$, $\mathrm{GL}_n(\mathbb{Z}) = \{A \in \mathbb{R}^{n \times n} \mid \det(A) = \pm 1\}$, and $\mathrm{GL}_n(\mathbb{Z}_\ell) = \{A \in \mathbb{R}^{n \times n} \mid \gcd(\det(A), \ell) = 1\}$.

[*] This is already guaranteed by demanding the binary operation $*$ maps into G.

[†] More generally we just let R be any *commutative ring with* 1.

Also, for each of these R's, $\mathrm{SL}_n(R) = \{A \in R^{n \times n} \mid \det(A) = 1\}$ (the special linear group of $n \times n$ matrices with entries in R) is also a group under matrix multiplication.

Functions and Symmetries: If X is some set, the collection of all invertible functions from X to itself, denoted $S(X) = \{f : X \to X \mid f \text{ is one-to-one and onto } \}$ (permutations on X) is a nonabelian (when $|X| > 2$) group under function composition. In particular, $S_n = S(\{1, 2, \dots, n\})$ is *permutations on n items* (aka the *symmetric group*). Permutation groups play a large role in group theory.

If we limit ourselves to permutations that preserve some kind of structure, we get groups of *symmetries*. For example, given a regular n-gon X, $D_n = \{f : \mathbb{R}^2 \to \mathbb{R}^2 \mid f \text{ is an isometry sending } X \text{ to itself } \}$[‡] (the *dihedral group* of order $2n$) is all symmetries of the regular n-gon X. Thus D_3 is symmetrices of an equilateral triangle, D_4 is symmetrices of a square, etc.

Quaternions: There is a way to "Cayley-Dickson double" the complex numbers to a generalized number system called the *quaternions*, $\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$. This system has an addition and multiplication similar to the complex numbers except multiplication is not commutative. Within this system we have $Q = \{\pm 1, \pm i, \pm j, \pm k\}$ (the *quaternion group* of order 8). This is a nonabelian group under multiplication where -1 flips signs, $i^2 = j^2 = k^2 = -1$ (so i, j, k act like $\sqrt{-1}$) and finally, $ij = k$, $jk = i$, and $ki = j$ whereas $ji = -k$, $kj = -i$, and $ik = -j$. In other words, multiplying i's, j's, and k's works just like the cross product that you may have seen in multivariable calculus or physics.

Notation:

- Most of the time our operations are called "addition" or "multiplication". Typically, an additive identity is called "0" and a multiplicative identity is called "1". But there are exceptions – the symmetric group's identity is called (1) and the identity of $\mathrm{GL}_n(\mathbb{R})$ is I_n (the identity matrix). For a general abstract group, we often use "e" to denote the identity.

- When working in an abstract group, we use multiplicative notation by default. We usually write ab for the product of a and b (this is "juxtaposition" notation) instead of $a * b$ or $a \cdot b$ or $a \times b$. Since additive notation will trick you into using the commutative law (without noticing), we don't use "+" expect for abelian groups. *Note:* When using additive notation, we also use subtraction as shorthand for: $a - b = a + (-b)$ (a plus the additive inverse of b).

- Exponents? Let G be a group with identity e. Also, let $a, b \in G$ and $m, n \in \mathbb{Z}$.

  Multiplicative Notation: $a^0 = e$, $a^1 = a$, $a^2 = aa$, $a^3 = aaa$. In general, if $n > 0$, then $a^n = \underbrace{aa \cdots a}_{n-\text{times}}$. For negative exponents, a^{-1} is a's inverse. $a^{-2} = a^{-1}a^{-1}$ and $a^{-3} = a^{-1}a^{-1}a^{-1}$. In general, if $n > 0$, then $a^{-n} = \underbrace{a^{-1}a^{-1} \cdots a^{-1}}_{n-\text{times}}$. A few laws of exponents: $a^m a^n = a^{m+n}$ and $(a^m)^n = a^{mn}$.

  Careful! In general, $(ab)^n \neq a^n b^n$ (unless a and b commute). However, we do have $(ab)^{-1} = b^{-1}a^{-1}$.

  Additive Notation: Additive exponents are written in front of the element. Sometimes we call these "multiples" instead of exponents. $0a = e$ (the identity). $1a = a$, $2a = a + a$, and $3a = a + a + a$. In general, if $n > 0$, then $na = \underbrace{a + a + \cdots + a}_{n-\text{times}}$. For negative exponents, $(-1)a = -a$ (that is a's inverse). $-2a = (-a) + (-a)$ and $-3a = (-a) + (-a) + (-a)$. In general, if $n > 0$, then $(-n)a = \underbrace{(-a) + (-a) + \cdots + (-a)}_{n-\text{times}}$. A few laws of exponents: $ma + na = (m+n)a$ and $n(ma) = (nm)a$. Since we *only* use + when the operation is **commutative**, we also have: $n(a + b) = na + nb$. Keep in mind that this works because we are assuming that a and b commute. For example: $(-1)(a + b) = (-1)a + (-1)b$. Notice that the left hand side is $-(a + b)$ which is the inverse of $a + b$. On the other hand, the right hand side is $(-a) + (-b)$ this is the inverse of a plus the inverse of b. If + wasn't commutative we would still have $-(a + b) = (-b) + (-a)$.

[‡] An isometry is a distance and angle preserving invertible function.