Math 5111 (Algebra 1)

Lecture #11 ∼ October 19th, 2020

Groups, part 1

- Examples of Groups, $D_{2\cdot n}$, S_n
- Properties of Orders
- Subgroups

This material represents §3.1.1-3.1.4 from the course notes.

Roadmap

Our goal now, and for the next three or so weeks, is to develop the basic theory of groups.

- Our focus will be on viewing groups as arising very naturally as the set of symmetries of a geometric or algebraic object, carrying the natural operation of composition.
- As such, the idea of a group action (a group acting on a set) will be the centerpiece of our discussion in this chapter.
- After this, we will focus on understanding the behavior of the group action of the automorphism group $\mathrm{Aut}(F)$ on a field F: this is the heart of Galois theory.

Groups, I

Here is the formal definition of a group:

Definition

A group is a set G *together with a binary operation* $\star$ *that satisfies the three axioms [G1]-[G3]:*

[G1] *The operation* $\star$ *is associative:* $g \star (h \cdot k) = (g \star h) \star k$ *for any elements* g, h, k *in* G.

[G2] *There is a (two-sided) identity element* e*:* $e \star g = g = g \star e$ *for any element* g *in* G.

[G3] *Every element has a (two-sided) inverse: for any* g *in* G, *there exists* g^{-1} *in* G *with* $g \star g^{-1} = e = g^{-1} \star g$.

We will establish some basic group properties before discussing examples.

Groups, II

Like with rings, certain groups will also possess additional properties, though there is only one term that we introduce now:

Definition

If a group satisfies axiom [G4], we say it is an abelian group:

[G4] *The operation $\star$ is commutative: $g \star h = h \star g$ for any elements g, h in G.*

A group that is not abelian is called non-abelian.

- Rarely, abelian groups are also called commutative groups.
- The term "abelian" is named after Neils Henrik Abel, who was a foundational figure in the study of groups; it is stylized in lowercase (rather than in uppercase as "Abelian") in honor of the depth of his contribution.

Groups, III

Some conventions regarding group notation:

- We will frequently omit the symbol for the group operation $\star$ and simply write gh for $g \star h$.
- We will also write the operation as $\cdot$ or $+$ when it represents multiplication or addition in a ring, and write 1 or 0 for the corresponding identity elements respectively.
- In an abelian group, we often write the group operation "additively" using the addition symbol $(+)$, denote the identity element as 0, and denote additive inverses with minus signs $(-)$.

Groups, IV

Because the group operation is associative, we do not need to specify the order in which the multiplications are performed when we have more than 2 terms, and can simply write expressions like ghk without needing to use parentheses to distinguish between $(gh)k$ and $g(hk)$.

- Technically, this statement requires a proof; it is straightforward though tedious to use induction on the number of terms in the product to establish that all such products are equal to the one where the order is composed left-to-right, as in $((gh)k)l$.
- If $g \in G$, for any positive integer n we define $g^0 = e$, $g^n = \underbrace{g \star g \star \cdots \star g}_{n \text{ terms}}$, and $g^{-n} = \underbrace{g^{-1} \star g^{-1} \star \cdots \star g^{-1}}_{n \text{ terms}}$.
- In an additive abelian group we would write instead $ng = \underbrace{g + g + \cdots + g}_{n \text{ terms}}$ for $n > 0$.

Groups, V

Another definition we record now:

Definition

If G is a group, the order of G, denoted as $|G|$ or $\#G$, is the cardinality of G as a set.

Groups, VI

Like with rings, we have various properties of group arithmetic:

Proposition (Basic Arithmetic in Groups)

Let G be a group. The following properties hold in G:

1. *The identity element e is unique, and $e^{-1} = e$.*
2. *G has left and right cancellation: for any g, h, k in G, either of $gh = gk$ or $hg = kg$ implies $h = k$.*
3. *Inverses are unique. Also, a one-sided inverse of g is automatically a two-sided inverse of g.*
4. *For any $g, h \in G$, $(gh)^{-1} = h^{-1}g^{-1}$, and $(g^{-1})^{-1} = g$.*
5. *For any $g \in G$ and any integers m, n, we have $g^{m+n} = g^m g^n$, $g^{mn} = (g^m)^n$, and $(g^n)^{-1} = g^{-n}$.*

These are all straightforward from the definition.

Examples of Groups, I

Examples:

1. Any ring R forms an abelian group under its addition operation $+$, as follows immediately from the ring axioms.
   - This group is known as the additive group of R.
   - Thus for example, $(\mathbb{Z}, +)$, $(\mathbb{Z}/m\mathbb{Z}, +)$, $(F[x], +)$, and $(M_{n\times n}(F), +)$ are all groups. The identity element is 0, and inverses are simply additive inverses.
2. If F is a field and V is an F-vector space, then $(V, +)$ is an abelian group, as follows immediately from the vector space axioms.

Examples of Groups, II

Examples:

3. If R is any ring with 1, then the collection of units in R, denoted $R^\times$, forms a group under multiplication $\cdot$.
   - This group is known as the multiplicative group of R.
   - Explicitly, this follows because multiplication is associative, the multiplicative identity 1 is a unit, and the product and multiplicative inverse of units are units.
   - If R is commutative, then $(R^\times, \cdot)$ is an abelian group.
4. As a special case of the above, $(\mathbb{Z}/m\mathbb{Z})^\times$, the collection of residue classes in $\mathbb{Z}/m\mathbb{Z}$ relatively prime to m, forms an abelian group under multiplication.

Examples of Groups, III

Examples:

5. The set $GL_n(F)$ of invertible $n \times n$ matrices with entries in the field F, forms a group under multiplication.
   - This is a special case of (3), since $GL_n(F)$ is the collection of units in the ring $M_{n\times n}(F)$ of $n \times n$ matrices with entries in F.
   - When $n \geq 2$ this group is non-abelian.
   - If $F = \mathbb{F}_q$ is a finite field, we can compute the order of this group by observing that an $n \times n$ matrix is invertible precisely when its rows are linearly independent.
   - Once we have chosen the first k rows, the $(k+1)$st row has $q^n - q^k$ possible choices (it must be linearly independent from the first k rows).
   - This holds for each row, so $\#GL_n(F) = (q^n - 1)(q^n - q)(q^n - q^2)\cdots(q^n - q^{n-1})$.

Examples of Groups, IV

Examples:

6. The set $G = \{e\}$, with operation $e \cdot e = e$, is a group called the trivial group.
7. The integers do not form a group under multiplication, because 0 has no multiplicative inverse.
   - More generally, no ring (except the trivial ring) will form a group under multiplication, since 0 cannot have a multiplicative inverse in any ring where $1 \neq 0$.

Examples of Groups, V

Examples:

8. The set $V_4 = \{e, a, b, c\}$ with identity e, and other multiplications given by $a^2 = b^2 = c^2 = 1$, $ab = ba = c$, $ac = ca = b$, and $bc = cb = a$, forms a group.
   - This group is called the Klein 4-group (in German, "Viergruppe"), and is an abelian group of order 4.
   - It is straightforward (although tedious) to verify that multiplication is associative. In this group, every element is its own inverse.

Examples of Groups, VI

Examples:

9. For any positive integer n, if $\zeta_n = e^{2\pi i/n}$, then the set $G = \{1, \zeta_n, \zeta_n^2, \dots, \zeta_n^{n-1}\}$ forms a group under multiplication.
   - This group consists of the solutions to the equation $x^n - 1 = 0$ in $\mathbb{C}$, and is called the group of nth roots of unity.
   - Explicitly: associativity is inherited from $\mathbb{C}$, the identity element is 1, and $(\zeta_n^k)^{-1} = \zeta_n^{n-k}$ for any $0 \leq k \leq n-1$.
   - For example, when $n = 4$, we obtain the multiplicative group $G = \{1, i, -1, -i\}$.

Examples of Groups, VII

Examples:

10. The set $Q_8 = \{1, -1, i, -i, j, -j, k, -k\}$ forms a group under the multiplication relations $i^2 = j^2 = k^2 = -1$, $ij = -ji = k$, $ki = -ik = j$, and $jk = -kj = i$.
    - This group is called the quaternion group, and is a non-abelian group of order 8.
    - It is straightforward (although tedious) to verify that the multiplication is associative, and clearly 1 is an identity element.
    - Furthermore, 1 and -1 are their own multiplicative inverses, while the inverses of i, j, k are $-i, -j, -k$ respectively.

Examples of Groups, VIII

Examples:

11. Let S be a set and S^{-1} be the set of symbols s^{-1} for $s \in S$. We define a word to be a finite string of symbols from $S \cup S^{-1} \cup e$, and define two words to be equivalent if there is a finite sequence of cancellations from $se = s = es$, $es^{-1} = s^{-1} = s^{-1}e$, $ss^{-1} = e = s^{-1}s$ transforming one into the other. The set of equivalence classes forms a group under concatenation of strings.
    - This group is called the free group on S.
    - It is rather tedious to verify all of the technical details for this construction of free groups (it is rather like the situation for polynomial rings).
    - The idea of a free group is that it is free of any relations between the elements from the set S, and possesses the minimal features required to be a group.

Examples of Groups, IX

Examples:

11. A few more words about free groups.
    - As an example, if $S = \{a, b\}$, then some elements of the free group on S are $ababa^{-1}b$, aaa, and e.
    - As examples of equivalences, we have $aaa = aa^{-1}aaa = abbb^{-1}b^{-1}aa$ and $aa^{-1}b^{-1}bbb^{-1} = aa^{-1}b^{-1}b = aa^{-1} = e$.
    - In this group, for example, $(ababa^{-1}b)(b^{-1}ab) = ababa^{-1}bb^{-1}ab = ababa^{-1}ab = ababb$.
    - Likewise, we have $(abba^{-1})^{-1} = ab^{-1}b^{-1}a^{-1}$.
    - Free groups are quite important in topology, since they show up as fundamental groups of wedges of circles.
    - For us, free groups will show up implicitly later when we discuss generators and presentations of groups.

Examples of Groups, X

We can also construct new groups using Cartesian products.

Proposition (Cartesian Products of Groups)

If $(G, \star)$ and $(H, \circ)$ are groups, then the Cartesian product $G \times H$ is also a group, with operation performed componentwise:
$(g_1, h_1) \triangle (g_2, h_2) = (g_1 \star g_2, h_1 \circ h_2)$.
The identity element is $e_{G\times H} = (e_G, e_H)$ and inverses are given by $(g, h)^{-1} = (g^{-1}, h^{-1})$.
The group $G \times H$ has order $|G| \cdot |H|$, and is abelian if and only if both G and H are abelian.

Each of these properties is quite straightforward.

Example: The Cartesian product $Q_8 \times (\mathbb{Z}/5\mathbb{Z})$ is a non-abelian group of order $8 \cdot 5 = 40$.

Dihedral Groups, I

As we briefly outlined, groups arise naturally from studying symmetries of objects.

- Among the simplest objects in geometry are regular n-gons, whose associated symmetry group is called the dihedral group, and denoted $D_{2\cdot n}$.
- Many authors denote this group as D_n (emphasizing the geometric flavor of the group), but in group theory literature the notation D_{2n} (emphasizing the elements of the group) is more common. We adopt the notation $D_{2\cdot n}$ as a sort of compromise[1] between these two.

[1] In the supposed words of Henry Clay as paraphrased by Larry David and/or George R.R. Martin, "A good compromise is when both parties are dissatisfied."

Dihedral Groups, II

So: $D_{2 \cdot n}$ is the symmetry group of the regular n-gon.

- Geometrically, these symmetries are the possible ways to move an n-gon around in space (rotating or reflecting it) and then placing it back on top of itself so that all of the vertices and edges line up.
- For example, for $n = 4$ (corresponding to the symmetries of a square), one possibility is to rotate the square $\pi/2$ radians counterclockwise in the plane around its center.
- Another possibility is to reflect the square about one of its diagonals (in fact there are two such maps).

Dihedral Groups, III

If we label the vertices of the n-gon $1, 2, \ldots, n$, then we can identify all of these symmetries by their corresponding permutations of the vertices.

- For example, if we label the vertices of the square as $1, 2, 3, 4$ counterclockwise, then a counterclockwise rotation of $\pi/2$ radians would correspond to the permutation σ with $\sigma(1) = 2$, $\sigma(2) = 3$, $\sigma(3) = 4$, and $\sigma(4) = 1$.
- The collection of symmetries $D_{2\cdot n}$ of the regular n-gon is a group under composition, as follows: if g and h are both elements of $D_{2\cdot n}$, we define $g \cdot h$ to be the symmetry obtained by first applying h, and then g (i.e., by function composition).
- This operation is associative since function composition is associative, the identity element is the identity transformation, and the inverse of a symmetry g is the symmetry g^{-1} that reverses all of the rigid motions of g.

Dihedral Groups, IV

There are $2n$ elements of $D_{2 \cdot n}$:

Proposition (Order of $D_{2 \cdot n}$)

For any integer $n \geq 3$, the dihedral group $D_{2 \cdot n}$ has order $2n$.

Proof:

- The vertex labeled 1 can be moved to any of the n vertices, and then the vertex labeled 2 must go to one of the 2 vertices adjacent to it. But once we have fixed the locations of vertices 1 and 2, then all of the other vertices' locations are determined uniquely. Thus, $|D_{2 \cdot n}| \leq 2n$.
- On the other hand, we can explicitly list $2n$ distinct symmetries: there are the n possible rotations counterclockwise about the center by $2\pi k/n$ radians for $0 \leq k \leq n-1$, and there are also n possible reflections about a line through the center of the n-gon.

Dihedral Groups, V

We can give a more concrete description of the elements in $D_{2\cdot n}$ in terms of particular rotations and reflections.

- Explicitly, let r represent the counterclockwise rotation of the n-gon by $2\pi/n$ radians: as a permutation, we have $r(1) = 2$, $r(2) = 3$, ... , $r(n-1) = n$, and $r(n) = 1$.
- Then r^k represents a counterclockwise rotation by $2\pi k/n$ radians, so the elements $\{e, r, r^2, \dots, r^{n-1}\}$ are distinct, and $r^n = e$.
- Also, let s represent the reflection of the n-gon across the line through vertex 1 and the center of the n-gon.
- As a permutation, we have $s(1) = 1$, $s(2) = n$, $s(3) = n - 1$, ... , and $s(n) = 2$. It is then easy to see that s^2 is the identity element, and that $s \neq r^i$ for any i, since the only power of r that fixes vertex 1 is the identity element.

Dihedral Groups, VI

Now we claim that $D_{2 \cdot n} = \{e, r, r^2, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\}$.

- To see this, note that $\{s, sr, sr^2, \dots, sr^{n-1}\}$ are distinct, since $sr^i = sr^j$ would imply $r^{i-j} = e$ by cancellation, and they are also all distinct from the elements $\{e, r, r^2, \dots, r^{n-1}\}$ since $sr^i = r^j$ would imply $s = r^{j-i}$ by cancellation.
- To describe the multiplication of any two elements in this list, we first observe that $rs = sr^{-1}$ (so in particular, $D_{2 \cdot n}$ is always non-abelian). This relation can be visualized geometrically, since rotating and then reflecting is equivalent to reflecting and then rotating in the opposite direction.
- Alternatively, we can compute $rs(1) = r(1) = 2$ and $rs(2) = r(n) = 1$, and also $sr^{-1}(1) = s(n) = 2$ and $sr^{-1}(2) = s(1) = 2$. Then since rs and sr^{-1} agree on vertices 1 and 2, they agree on all vertices, so they are equal.
- Then by an easy induction, we see that $r^i s = sr^{-i}$ for all i.

Dihedral Groups, VII

To summarize the discussion, the dihedral group $D_{2\cdot n} = \{e, r, r^2, \dots, r^{n-1}, s, sr, sr^2, \dots, sr^{n-1}\}$, where r and s are elements satisfying the relations $r^n = s^2 = e$ and $rs = sr^{-1}$.

- Using these relations (and the ancillary fact that $r^i s = sr^{-i}$ for any i) we can compute the product of any two elements in $D_{2\cdot n}$.
- For example, in $D_{2\cdot 7}$, we have the following:
  $(sr^5)(r^4) = sr^9 = sr^2$,
  $(r^4)(sr^5) = sr^{-4}(r^5) = sr$, and
  $(sr^2)(sr) = s(r^2 s)r = s(sr^{-5})r = s^2 r^{-4} = r^3$.

Symmetric Groups, I

Another natural class of groups arises from “symmetries” of sets.

- To illustrate the idea, observe that the set S_3 of permutations of the set $A = \{1, 2, 3\}$ (formally, the set of bijections of S with itself) forms a group under composition.
- Note that there are a total of $3! = 6$ such bijections.
- A relatively inconvenient way to represent these maps is to write a list of the elements of the domain and codomain vertically: thus the map f with $f(1) = 2$, $f(2) = 3$, and $f(3) = 1$ would be written as $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$.
- In this notation, the 6 elements of S_3 are $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 2 & 3 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, $\begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$.

Symmetric Groups, II

- To compute the product of two elements in S_3, we can simply trace the behavior of each element of $\{1, 2, 3\}$ under the corresponding composition of functions.
- For example, if $g = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 1 & 3 \end{pmatrix}$ and $h = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 1 & 2 \end{pmatrix}$, to compute the product gh we observe that (i) h sends 1 to 3, and g sends 3 to 3, so gh sends 1 to 3, (ii) h sends 2 to 1, and g sends 1 to 2, so gh sends 2 to 2, and (iii) h sends 3 to 2, and g sends 2 to 1, so gh sends 3 to 1.
- So $gh = \begin{pmatrix} 1 & 2 & 3 \\ 3 & 2 & 1 \end{pmatrix}$. Similarly, $hg = \begin{pmatrix} 1 & 2 & 3 \\ 1 & 3 & 2 \end{pmatrix}$, so we see in particular that S_3 is non-abelian.
- It is very tedious to verify that these operations actually form a group using this explicit description (checking associativity, for example, requires 6^3 individual calculations).

Symmetric Groups, III

We can clarify matters by generalizing this idea to arbitrary sets.

Proposition (Symmetric Groups)

If A is any set, the set of bijections from A to itself forms a group under function composition. This group is the symmetric group on the set A and is denoted S_A.

Proof:

- The group operation is well-defined because the composition of two bijections is also a bijection.
- [G1] follows because function composition is associative, [G2] follows because the identity map is a bijection, and [G3] follows because the inverse of a bijection is also a bijection.

Symmetric Groups, IV

Some remarks:

- If A is a finite set of cardinality n, then $|S_A| = n!$, since bijections on a finite set are the same as injections, and there are clearly $n!$ injections from A to itself (the first element has n possible destinations, the second then has $n-1$, etc.).
- If A is infinite, then clearly $|S_A| = \infty$ (though I suppose one may need the axiom of choice for this).
- We will primarily be interested in the case where $A = \{1, 2, \dots, n\}$, in which case we will write the group as S_n, the symmetric group on n objects.

Symmetric Groups, V

We want a convenient way to describe the elements in S_n.

- We can achieve this by writing permutations in terms of cycles $(a_1\, a_2\, \dots\, a_k)$.
- Explicitly, the cycle $(a_1\, a_2\, \dots\, a_k)$ is the permutation σ with $\sigma(a_1) = a_2$, $\sigma(a_2) = a_3$, ... , $\sigma(a_{k-1}) = a_k$, and $\sigma(a_k) = a_1$, where all other elements are mapped to themselves.
- This permutation "cycles" the elements $a_1, a_2, \dots, a_k$ one step forward (whence the name).
- Thus, for example, inside S_4 the cycle $(2\,1\,4)$ is the permutation with $\sigma(2) = 1$, $\sigma(1) = 4$, $\sigma(4) = 2$, $\sigma(3) = 3$.

Symmetric Groups, VI

Definition

The length of a cycle is the number of elements it contains. A cycle of length k is called a k-cycle, and 2-cycles are often called transpositions.

Not every permutation can be written as a single cycle, but it is not hard to see that every permutation can be written as a product of disjoint cycles (i.e., cycles having no elements in common).

- For example, the permutation with $\sigma(1) = 3$, $\sigma(2) = 4$, $\sigma(3) = 1$, $\sigma(4) = 2$ can be written as the product $(1\,3)\,(2\,4)$.
- Such a representation is called the cycle decomposition of σ.

Symmetric Groups, VII

We can give a procedure for computing the cycle decomposition of an arbitrary permutation σ:

- Start with the smallest number x not contained in one of the cycles we have identified, and repeatedly apply σ until we obtain a repeated element.
- In other words, we evaluate $a_1 = x$, $a_2 = \sigma(a_1)$, $a_3 = \sigma(a_2)$, $a_4 = \sigma(a_3)$, ... until the list repeats.
- It is easy to see that the first repeated value will always be x (since $a_i = a_j$ implies $\sigma(a_{i-1}) = \sigma(a_{j-1})$ so that $a_{i-1} = a_{j-1}$ since σ is a bijection).
- Thus, we obtain a cycle $(x\, a_2\, \dots\, a_k)$ containing x.
- We repeat this process until we have identified the cycles containing every element in $\{1, 2, \dots, n\}$.

It is not hard to show that this algorithm always decomposes σ as a product of disjoint cycles.

Symmetric Groups, VIII

Example: Find the cycle decomposition of the permutation $\sigma \in S_6$ with $\sigma(1) = 3$, $\sigma(2) = 5$, $\sigma(3) = 4$, $\sigma(4) = 1$, $\sigma(5) = 2$, $\sigma(6) = 6$.

Symmetric Groups, VIII

Example: Find the cycle decomposition of the permutation $\sigma \in S_6$ with $\sigma(1) = 3$, $\sigma(2) = 5$, $\sigma(3) = 4$, $\sigma(4) = 1$, $\sigma(5) = 2$, $\sigma(6) = 6$.

- We start with $n = 1$: we compute $\sigma(1) = 3$, $\sigma(3) = 4$, and $\sigma(4) = 1$. This gives the cycle $(1\,3\,4)$.
- The smallest number not yet used is $n = 2$: then $\sigma(2) = 5$ and $\sigma(5) = 2$, so we obtain the cycle $(2\,5)$.
- The smallest number not yet used is $n = 6$: since $\sigma(6) = 6$ we obtain the cycle (6).
- Since we have used all 6 elements in cycles, we see that the cycle decomposition of σ is $\boxed{(1\,3\,4)(2\,5)(6)}$.

Symmetric Groups, IX

The notation for cycle decompositions is not unique.

- For example, the cycle $(1\,3\,4)$ corresponds to the same permutation as the cycle $(3\,4\,1)$, and the cycle decomposition $(1\,3\,4)(2\,5)(6)$ is the same as $(2\,5)(6)(1\,3\,4)$.
- We typically will adopt the convention of writing the cycles with the smallest element first, and ordering the cycles in increasing order of their first element.
- Under this convention, it follows by a straightforward induction argument that the cycle decomposition is unique, and that the algorithm we described earlier will compute it.
- We will also usually omit 1-cycles when we write cycle decompositions, with the convention always being that any unlisted elements are fixed (i.e., mapped to themselves).
- Thus, we would simply write $(1\,3\,4)(2\,5) \in S_6$ and omit the 1-cycle (6).

Symmetric Groups, X

We can also compute products using cycle decompositions, with the important remark that the products of cycles are read right-to-left, since they are representing compositions of functions.

- Just to reiterate: products of cycles are read *right-to-left*! This is because cycles are permutations of a set, so they are composed the way functions are.
- We can compute the cycle decomposition of a product by tracing what happens to each element $1, 2, \ldots, n$ under each of the cycles from right-to-left, and then using the cycle decomposition algorithm.

Symmetric Groups, XI

Example: If $g = (1\,3\,4)(2\,5)$ and $h = (1\,2)(3\,5)$ inside S_5, compute the cycle decomposition of gh.

Symmetric Groups, XI

Example: If $g = (1\,3\,4)(2\,5)$ and $h = (1\,2)(3\,5)$ inside S_5, compute the cycle decomposition of gh.

- Since h sends 1 to 2, and g sends 2 to 5, the composition gh sends 1 to 5.
- To compute the next element in the cycle containing 1 we need to determine where gh sends 5. Since h sends 5 to 3, and g sends 3 to 4, we see that gh sends 5 to 4.
- Continuing, we see $gh(4) = g(4) = 1$, which completes a cycle $(1\,5\,4)$.
- Also, since $gh(2) = g(1) = 3$ and $gh(3) = g(5) = 2$, we get another cycle $(2\,3)$.
- Since we have exhausted all of the elements in the set, that means the cycle decomposition of gh is $\boxed{(1\,5\,4)(2\,3)}$.

Symmetric Groups, XII

Example: The six elements in S_3 have respective cycle decompositions 1, $(1\,2)$, $(1\,3)$, $(2\,3)$, $(1\,2\,3)$, $(1\,3\,2)$.

- We can compute, for example, $(1\,2)(1\,3) = (1\,3\,2)$, by tracing what happens to each element from right to left in each of the cycles. (Explicitly, these tracings would look something like $1 \to 3 \to 3$, $3 \to 1 \to 2$, and $2 \to 2 \to 1$.)
- Similarly, $(1\,3)(1\,2) = (1\,2\,3)$, $(1\,3\,2)(1\,2) = (2\,3)$, and $(1\,2)(1\,3\,2)(1\,3) = (2\,3)$ as well.

As a final remark we observe that any two disjoint cycles commute, and so (by a trivial induction) two permutations with disjoint cycle decompositions will also commute.

Orders of Elements, I

If g is an element of G, the powers of g, namely $\{\dots, g^{-2}, g^{-1}, e, g, g^2, \dots\}$ play an important role in understanding the behavior of multiplication by g.

Definition

If g is an element of the group G, the order of g, written $|g|$, is the smallest positive integer n such that $g^n = e$, if such an n exists. If $g^n \neq e$ for any positive integer n, we say $|g| = \infty$.

If G is a finite group, then every element of G has finite order.

- Specifically, since the set of powers $\{e, g, g^2, \dots\}$ must be finite, there must exist $a < b$ with $g^a = g^b$; cancelling g^a yields $g^{b-a} = e$.

Orders of Elements, II

Examples:

1. The order of the identity element in any group is always 1.
2. Inside $G = \{1, i, -1, -i\}$, the element -1 has order 2 since $(-1)^2 = 1$ but $-1 \neq 1$. Similarly, both i and $-i$ have order 4.
3. Inside $(\mathbb{Z}, +)$, the order of every nonidentity element is ∞, whereas inside $(\mathbb{Z}/7\mathbb{Z}, +)$, the order of every nonidentity element is 7.
4. Inside $(\mathbb{C}^\times, \cdot)$, the order of $\zeta_6 = e^{2\pi i/6}$ is 6, while the order of 2 is ∞.
5. Inside $(\mathbb{Z}/11\mathbb{Z})^\times$, the powers of $\overline{2}$ are $\{1, 2, 4, 8, 5, 10, 9, 7, 3, 6, 1\}$. We see that $\overline{2}^{10} = 1$ but no lower power is equal to 1, so the order of $\overline{2}$ is 10 inside $\mathbb{Z}/11\mathbb{Z}$.

Orders of Elements, III

Examples:

6. Inside $GL_2(\mathbb{Q})$, the order of $A = \begin{bmatrix} 0 & 1 \\ -1 & -1 \end{bmatrix}$ is 3, since A^3 is the identity matrix, but neither A nor A^2 is. The order of $B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ is ∞, since $B^n = \begin{bmatrix} 1 & n \\ 0 & 1 \end{bmatrix}$.
7. Inside $GL_2(\mathbb{F}_7)$, the order of $B = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ is 7.
8. Every nonidentity element in the group $(\mathbb{Z}/p\mathbb{Z})^n$, the Cartesian product of n copies of $\mathbb{Z}/p\mathbb{Z}$, has order p.
9. Inside S_n, the order of any k-cycle is k.

Orders of Elements, IV

We have various properties of order:

Proposition (Properties of Order)

Suppose G is a group and $g, h \in G$. Then the following hold:

1. *If $g^n = e$ for some $n > 0$, then g has finite order and the order of g divides n.*
2. *If g has order k, then $g^a = g^b$ if and only if k divides $b - a$. If g has infinite order, then $g^a \neq g^b$ for $a \neq b$.*
3. *If g has order k, then g^n has order $k/\gcd(n, k)$. In particular, if n and k are relatively prime, then g^n also has order k.*
4. *If $g^n = e$ and $g^{n/p} \neq e$ for any prime divisor p of n, then g has order n.*
5. *If $gh = hg$, g has order n, h has order m, and m and n are relatively prime, then gh has order mn.*

Orders of Elements, V

Proofs:

1. If $g^n = e$ for some $n > 0$, then g has finite order and the order of g divides n.
   - If $g^n = e$ for some $n > 0$, then $g^k = e$ for some minimal positive integer k by the well-ordering axiom of $\mathbb{Z}$.
   - Now let k be the order of u and apply the division algorithm to write $n = qk + r$ with $0 \leq r < k$.
   - Then we have $g^r = g^n (g^k)^{-q} = e \cdot e^{-q} = e$.
   - If r were not zero, then we would have $g^r = e$ with $0 < r < k$, which contradicts the definition of order.
   - Thus $r = 0$, meaning that k divides n.

Orders of Elements, VI

Proofs:

2. If g has order k, then $g^a = g^b$ if and only if k divides $b - a$. If g has infinite order, then $g^a \neq g^b$ for $a \neq b$.
   - If $b - a = dk$ then $g^{b-a} = (g^k)^d = e^d = e$, and then multiplying by g^a yields $g^b = g^a$.
   - Conversely, if $g^a = g^b$ then $g^{b-a} = e$, and so by (1) we conclude k divides $b - a$.
   - For the second statement, if $g^a = g^b$ with $a \neq b$, then $g^{b-a} = e = g^{a-b}$ so $g^n = e$ for $n = |b - a|$; then by (1), g would have finite order.

Orders of Elements, VII

Proofs:

3. If g has order k, then g^n has order $k/\gcd(n,k)$. In particular, if n and k are relatively prime, then g^n also has order k.

   - Let $d = \gcd(n,k)$: then $(g^n)^{k/d} = (g^k)^{n/d} = e^{n/d} = e$, so the order of g^n cannot be larger than k/d.
   - Furthermore, if $e = (g^n)^a = g^{na}$, the result above implies that k divides na, so that k/d divides $(n/d)a$.
   - But since k/d and n/d are relatively prime, this implies k/d divides a, and so $a \geq k/d$.
   - Thus, the order of g^n is equal to k/d as claimed. The second statement is simply the case $d = 1$.

Orders of Elements, VIII

Proofs:

4. If $g^n = e$ and $g^{n/p} \neq e$ for any prime divisor p of n, then g has order n.

   - Suppose g has order k.
   - Then by (1), k must divide n.
   - If $k < n$, then there must be some prime p in the prime factorization of n that appears to a strictly lower power in the factorization of k: then k divides n/p.
   - But then $g^{n/p}$ would be an integral power of $g^k = e$, so that $g^{n/p} = e$, which is a contradiction. Thus, $k = n$.

Orders of Elements, IX

Proofs:

5. If $gh = hg$, g has order n, h has order m, and m and n are relatively prime, then gh has order mn.

   - If $gh = hg$ then by a trivial induction every power of g commutes with every power of h.
   - Then we can observe that $(gh)^{mn} = (g^n)^m (h^m)^m = e^m e^n = e$, so gh has some finite order $d \leq mn$.
   - Since $(gh)^d = e$, $e = e^n = (gh)^{dn} = (g^n)^d w^{dn} = w^{dn}$, so by (1), m divides dn.
   - Then since m and n are relatively prime, this implies m divides d. By a symmetric argument, n divides d.
   - Since m and n are relatively prime, this means mn divides d, and so the only possibility is $d = mn$.

Orders of Elements, X

We will warn that this last item fails essentially completely in non-abelian groups.

- For example, in S_5, the element $(1\,2)$ has order 2, the element $(1\,3\,4)$ has order 3, but the product $(1\,2)(1\,3\,4) = (1\,3\,4\,2)$ has order 4.
- Also in S_5, $(1\,2)(3\,4)$ has order 2 and $(1\,3\,5)$ has order 3, but the product $(1\,2)(3\,4)(1\,3\,5) = (1\,4\,3\,5\,2)$ has order 5.
- For a third example, in the matrix group $GL_2(\mathbb{R})$, the matrices $g = \begin{bmatrix} 1 & 0 \\ 1 & -1 \end{bmatrix}$ and $h = \begin{bmatrix} 1 & 1 \\ 0 & -1 \end{bmatrix}$ both have order 2, but the product matrix $gh = \begin{bmatrix} 1 & 1 \\ 1 & 2 \end{bmatrix}$ has infinite order.

Orders of Elements, X

We will be able to say more about orders of elements in particular groups later, once we discuss cosets. For now we record a few basic observations about element orders in dihedral and symmetric groups:

- In the dihedral group $D_{2 \cdot n}$, since $r^n = e$ but $r^k \neq e$ for $0 < k < n$, we see that $|r| = n$.
- Then by our results above on orders, the order of r^k is $n / \gcd(k, n)$.
- Also, since $(sr^k)^2 = s(r^k s) r^k = s(sr^{-k}) r^k = s^2 = e$, we see that $\left|sr^k\right| = 2$ for any k.

Orders of Elements, XI

We noted earlier that in S_n, the order of any n-cycle $\sigma = (a_1\, a_2\, \dots\, a_n)$ is n.

- In particular, we can see that every nonidentity element in S_3 has order 2 or 3.
- Furthermore, in S_n, if a lies in a k-cycle for the permutation τ, then $\tau^n(a) = a$ only when k divides n, since $\sigma^k(a_1) = a_k$.
- Thus, the order of τ is the least common multiple of the lengths of the cycles in its cycle decomposition.
- For example, the powers of $\tau = (1\,3\,5)(2\,6) \in S_6$ are $\tau^2 = (1\,5\,3)$, $\tau^3 = (2\,6)$, $\tau^4 = (1\,3\,5)$, $\tau^5 = (1\,5\,3)(2\,6)$, and $\tau^6 = 1$, so τ indeed has order 6.

Orders of Elements, XII

As we have seen (in the examples of S_3 and $(\mathbb{Z}/p\mathbb{Z})^n$), even when the order of G is composite it is possible that all its nonidentity elements have prime order.

We can therefore only expect a general existence result for elements of prime order:

Theorem (Cauchy's Theorem)

Suppose G is a group and p is a prime dividing $|G|$. Then there exists an element of G of order p.

Orders of Elements, XIII

Proof:

- Consider the set S of ordered p-tuples of elements $(g_1, g_2, \ldots, g_p)$ in G such that $g_1 g_2 \cdots g_p = e$.
- Since $g_p = (g_{p-1} \cdots g_2 g_1)^{-1}$, there are exactly $|G|^{p-1}$ such p-tuples, so the cardinality of S is divisible by p.
- Also observe that if $(g_1, g_2, \ldots, g_p) \in S$ then any cyclic permutation, such as $(g_2, \ldots, g_p, g_1)$, is also in S. If not all the elements in the tuple are equal, then there are p distinct cyclic permutations of this tuple in S, while if all elements are equal there is only 1, namely $(g, g, \ldots, g)$.
- Thus, since $\#S$ is divisible by p, and the number of tuples of the first type is divisible by p, the number of tuples of the second type must be divisible by p.
- In particular, there must be at least one tuple $(g, g, \ldots, g)$ with $g \neq e$: then $g^p = e$ so g is an element of order p.

Subgroups, I

Like with subrings, subfields, and vector subspaces, we have a natural notion of subgroup:

Definition

If G is a group, we say a subset S of G is a subgroup if it also possesses the structure of a group, under the same operations as G.

Associativity is automatically inherited, so we only need to check nonemptiness and closure under the group operation and inverses:

Proposition (Subgroup Criterion)

A subset S of G is a subgroup if and only if S contains the identity of G and is closed under the group operation of G and inverses. Equivalently, S is a subgroup if and only if $e_G \in S$ and for any $g, h \in S$, the element $gh^{-1} \in S$.

Subgroups, II

Proof:

- By definition, S must be closed under the group operation.
- By [G2] in S, there must be an identity element e_S in S with the property that $ge_S = g$ for every $g \in S$.
- However, by the cancellation law in G, since $ge_S = g = ge_G$, we see that $e_S = e_G$, so S must contain the identity of G.
- Likewise, in order for [G3] to hold in S, we require that for every $g \in S$, it must have an inverse g_S^{-1}. Since $gg_S^{-1} = e_S = e_G = gg_G^{-1}$ by cancellation in G we must have $g_S^{-1} = g_G^{-1}$, which is to say, the inverse of g must be in S.
- Conversely, if S contains the identity of G and is closed under the group operation and inverses, then it is also a group.

Subgroups, III

Proof (second statement):

- For the second statement, if S is a subgroup then $e_G \in S$ and for any $g, h \in S$ we must have $h^{-1} \in S$ and then $gh^{-1} \in S$.
- Conversely, if $e_G \in S$ and $gh^{-1} \in S$ for any $g, h \in S$, setting $g = e_G$ implies that $h^{-1} \in S$ so S is closed under inverses.
- Then for any $k \in S$, setting $h = k^{-1}$ and using the fact that $(k^{-1})^{-1} = k$ implies that $gh^{-1} = gk \in S$ so S is closed under the group operation, hence is a subgroup.

Subgroups, IV

As for subfields and subrings, intersections of subgroups yield subgroups:

Corollary (Intersection of Subgroups)

The intersection of an arbitrary collection of subgroups of G is also a subgroup of G.

Proof:

- Let $S = \bigcap_{i \in I} G_i$ where the G_i are subgroups of G. Then by the subgroup criterion, $e_G \in G_i$ for all $i \in I$, so S contains e_G.
- Furthermore, for any $g, h \in S$ we have $g, h \in G_i$ for all i. Thus, $gh^{-1} \in G_i$ for all i by the subgroup criterion, so $gh^{-1} \in S$ so S is a subgroup.

Subgroups, V

Examples:

1. For any group G, the sets $\{e\}$ and G are always subgroups of G. The subgroup $\{e\}$ is called the trivial subgroup.
2. The set $(\mathbb{Q}^+, \cdot)$ of positive rational numbers under multiplication is a subgroup of $(\mathbb{C}, \cdot)$ since it satisfies the subgroup criterion.
3. The set $(\mathbb{Z}_{\geq 0}, +)$ of nonnegative integers under addition is not a subgroup of $(\mathbb{Z}, +)$ since it is not closed under inverses.
4. The set of odd integers together with 0, under addition, is not a subgroup of $(\mathbb{Z}, +)$ since it is not closed under addition.
5. The set $(SL_n(F), \cdot)$ of matrices with coefficients in F having determinant 1 is a subgroup of $(GL_n(F), \cdot)$.
   - Explicitly, $\det(I_n) = 1$, and if $\det(A) = \det(B) = 1$, then $\det(AB) = \det(A^{-1}) = 1$ by determinant properties.

Subgroups, VI

We have an important general subgroup:

Definition

If G is a group, the center $Z(G)$ is the subgroup consisting of all of elements G that commute with every other element of G. Explicitly, $Z(G) = \{a \in G : ag = ga \text{ for all } g \in G\}$.

The center $Z(G)$ is a subgroup of G.

- It contains the identity, and if $a, b \in Z(G)$ and $g \in G$, then $(ab)g = a(bg) = a(gb) = (ag)b = (ga)b = g(ab)$ so that $ab \in Z(G)$, and also $ga^{-1} = a^{-1}(ag)a^{-1} = a^{-1}(ga)a^{-1} = a^{-1}g$ so that $a^{-1} \in Z(G)$.

The group G is abelian if and only if $Z(G) = G$.

Subgroups, VII

Examples:

1. The center of the dihedral group $D_{2\cdot 4}$ is $\{e, r^2\}$ since both of these elements commute with all the other elements of the group (powers of r all commute with one another, and also $(r^2)(sr^k) = (r^2s)r^k = (sr^2)r^k = (sr^k)(r^2)$), but no other elements do (since $sr^k = r^ks$ implies $sr^k = sr^{-k}$ so that $r^{2k} = e$, and also $r(sr^k) = sr^{k-1}$ while $(sr^k)r = sr^{k+1}$).
2. The center of the symmetric group S_3 is $\{1\}$, since one may verify that none of the 2-cycles commutes with any of the 3-cycles.

Subgroups, VIII

We also have an important subgroup of S_n:

Definition

For a positive integer n, we define the subgroup A_n of S_n to be all the elements in S_n that can be written as the product of an even number of transpositions (not necessarily disjoint transpositions). This subgroup is called the alternating group on n objects.

We can see that A_n is a subgroup of S_n:

- The identity is the empty product of 0 transpositions.
- A_n is closed under multiplication since the product of two even numbers of transpositions is clearly also of that form.
- A_n is closed under inverses since the inverse of a transposition is itself, so the inverse of a product of an even number of transpositions is also the product of an even number of transpositions.

Subgroups, IX

It is not hard to see that every permutation in S_n is a product of some number of transpositions.

- Explicitly, since for any n-cycle we can write $(a_1\, a_2\, \dots\, a_n) = (a_1\, a_n)(a_1\, a_{n-1}) \cdots (a_1\, a_2)$ as a product of $n-1$ transpositions.
- Thus, A_n contains every cycle of odd length, along with the product of any two cycles of even length. Thus, by taking products of such elements, we see that A_n contains every permutation whose cycle decomposition contains an even number of cycles of even length.
- We will prove later that these are all of the permutations in A_n, and that there are precisely $n!/2$ such elements.
- For example, we have $A_3 = \{1, (1\,2\,3), (1\,3\,2)\}$, and also $A_4 = \{1, \{1\,2\,3), (1\,2\,4), (1\,3\,2), (1\,3\,4), (1\,4\,2), (1\,4\,3), (2\,3\,4), (2\,4\,3), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$.

Summary

We introduced groups and their basic properties.

We discussed basic examples of groups, including the dihedral groups $D_{2\cdot n}$ and the symmetric groups S_n.

We discussed properties of orders.

We discussed subgroups.

Next lecture: More groups.