Math 5111 (Algebra 1)

Lecture #12 of 24 $\sim$ October 19th, 2020

Groups, part 2

- Subgroups
- Generation and Presentations
- Cyclic Groups
- Group Isomorphisms and Homomorphisms

This material represents §3.1.4-3.1.7 from the course notes.

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 $sr^k = r^k s$ 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 $(a_1\ a_2\ \ldots\ a_n) = (a_1\ a_n)(a_1\ a_{n-1})\cdots(a_1\ a_2)$ 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 $A_4 = \{1, \{1\,2\,3), (1\,2\,4), (1\,3\,2), (1\,3\,4), (1\,4\,2), (1\,4\,3), (2\,3\,4), (2\,4\,3), (1\,2)(3\,4), (1\,3)(2\,4), (1\,4)(2\,3)\}$.

Generation of Groups, I

If S is a subset of a group, it need not necessarily be a subgroup. We can, however, formulate a notion of "smallest subgroup" containing S, using the same idea as what we did for fields:

Definition

If G is a group and S is a subset of G, the set $\langle S \rangle$, the subgroup generated by S, is the intersection of all subgroups of G containing S.

- This definition is well-posed since the intersection of a collection of subgroups is also a subgroup, as we showed last time.
- While this definition is useful for proving things, we would like a more concrete description of what the elements in this subgroup $\langle S \rangle$ actually are.

Generation of Groups, II

Here is a more explicit description of $\langle S \rangle$:

- If $g_1, g_2, \ldots, g_n \in S$, then since S is closed under multiplication and inverses, we see that any "word" in the g_i and their inverses (namely, any product whose terms are all among the g_i and their inverses, like $g_1 g_3^{-1} g_1 g_4$ or $g_8 g_2^{-1} g_4 g_4 g_4$) is contained in S.
- Conversely, the collection of such finite words does in fact form a subgroup, since the identity element is a finite word, the product of any two finite words is also a finite word, and the inverse of a finite word is also a finite word via the formula $(h_1 h_2 \cdots h_d)^{-1} = h_d^{-1} \cdots h_2^{-1} h_1^{-1}$.
- We will remark that if S is the empty set, then $\langle S \rangle = \{e\}$. This agrees with the explicit description of $\langle S \rangle$ as the collection of all possible words if we adopt the usual convention that an empty product is the identity element.

Generation of Groups, III

Definition

If G is a group and S is a subset of G with $G = \langle S \rangle$, we say G is generated by S.
If G is generated by a finite set, we say G is finitely generated.

A generating set is the group analogue of a spanning set for a vector space.

The point is that every element in the group G can be built up from the elements of S using only the group operations.

Generation of Groups, IV

Examples:

1. The group $(\mathbb{Z}, +)$ is generated by $\{1\}$, since the subgroup $\langle 1 \rangle$ contains all positive and negative multiples of 1, and zero, hence is the entire group.
2. From our explicit description of the dihedral group $D_{2 \cdot n} = \{e, r, r^2, \ldots, s, sr, sr^2, \ldots\}$, we can see that $D_{2 \cdot n}$ is generated by $\{r, s\}$.
3. The group $(\mathbb{Q}, +)$ is generated by the infinite set $\{1, 1/2, 1/3, 1/4, \ldots\}$ since any rational number $p/q \in \mathbb{Q}$ is equal to $p(1/q)$. In fact $(\mathbb{Q}, +)$ is not finitely generated: if S is any finite set of generators, and p is any prime not dividing any of the generators' denominators, then $1/p$ is not in the subgroup $\langle S \rangle$.

Generation of Groups, V

We would like (whenever possible) to find a small set of generators for G, since we can then describe all of the elements of G in terms of this small set of generators.

- Of course, simply knowing a list of generators of G does not say very much about the actual structure of G, because there may be numerous relations between these generators.
- For example, in $D_{2\cdot n}$, the generators r and s satisfy the relations $r^n = e$, $s^2 = e$, and $rs = sr^{-1}$.

Generation of Groups, VI

In fact, inside $D_{2\cdot n}$ the relations $r^n = e$, $s^2 = e$, and $rs = sr^{-1}$ imply all other possible relations between r and s.

- To see this, consider any group generated by elements r and s such that $r^n = e$, $s^2 = e$, and $rs = sr^{-1}$.
- Any element in this group is a finite product of terms r, s, r^{-1}, s^{-1}, and by using $r^{-1} = r^{n-1}$ and $s^{-1} = s$ each product can be rewritten to use only r and s.
- By using the third relation to move all s terms to the left of all r terms, we see any element is in fact of the form $s^a r^b$, and then we may reduce the exponents so that $a \in \{0, 1\}$ and $b \in \{0, 1, \ldots, n-1\}$ using the first two relations.
- Thus, we see that any such group must have at most $2n$ elements, but since $D_{2\cdot n}$ already has $2n$ elements, there cannot be any further "collapsing".

Presentations of Groups, I

We will be interested in searching for generators and relations that describe the structure of other groups.

Definition

If G is a group generated by S, and there is some collection of relations $R_1, R_2, \ldots, R_n, \ldots$ among the elements of S (and their inverses, and the identity e) that imply any other such relation, we call this collection of generators and relations a presentation of G, and write $G = \langle S \mid R_1, R_2, \ldots, R_n, \ldots \rangle$.

Explicitly, a "relation" is an equation in the elements of S, the inverses of the elements in S, and the identity e.

- By rearranging, we can always write any relation in the form [word] $= e$, for some word (i.e., finite product of elements) in $S \cup S^{-1}$.

Presentations of Groups, II

Examples:

1. From our analysis above, a presentation of $D_{2\cdot n}$ is $D_{2\cdot n} = \langle r, s \,|\, r^n = s^2 = e,\ rs = sr^{-1} \rangle$.
2. A presentation of $(\mathbb{Z}/m\mathbb{Z}, +)$ is $\mathbb{Z}/m\mathbb{Z} = \langle a \,|\, a^m = e \rangle$. Note that we have written the presentation multiplicatively (the generator a corresponds to the element $\overline{1} \in \mathbb{Z}/m\mathbb{Z}$, with $e = \overline{0}$).
3. A presentation of $(\mathbb{Z}, +)$ is given by $\langle a \,|\, \emptyset \rangle$. The generator a corresponds to the element $1 \in \mathbb{Z}$, which satisfies no relation.
4. A presentation of the free group on the set $\{a, b\}$ is $\langle a, b \,|\, \emptyset \rangle$: there are two generators but no relations between them.

Presentations of Groups, III

Examples:

5. A presentation of the quaternion group Q_8 is $Q_8 = \langle i, j \mid i^4 = e,\ i^2 = j^2,\ ij = ji^{-1} \rangle$.
   - It is not hard to see that i and j generate Q_8 and satisfy the three indicated relations.
   - Conversely, the relations $i^2 = j^2$ and $i^4 = e$ imply $j^4 = e$, and by similar logic as in the dihedral groups we can write every element in the form $i^a j^b$.
   - By replacing i^2 with j^2 if necessary, and using $i^4 = j^4 = e$, we can always take $a \in \{0, 1\}$ and $b \in \{0, 1, 2, 3\}$.
   - Thus, this presentation describes a group of order at most 8. Thus, it is a presentation of Q_8, as claimed.

Presentations of Groups, IV

Although presentations seem very convenient, they are quite a bit trickier than they might seem.

1. For a finite group, we can (necessarily) give a presentation with finitely many relations, although this is not so obvious to prove.
2. It is possible, for infinite groups, that there may be infinitely many independent relations among its elements, even if the group itself is finitely generated.
3. In general, if G has a presentation with a finite number of generators and relations, we say it is finitely presented.

Presentations of Groups, V

Given a presentation, it is often very difficult to tell whether two given elements (written in terms of the generators) of the group are necessarily equal.

- More precisely, the problem of deciding whether two words are equal in an arbitrary presentation is known as the word problem for groups.
- It has in fact been proven that there exists a finitely presented group G such that the word problem is undecidable in G, meaning that it is not possible to construct an algorithm that always answers the question correctly in a finite amount of time.

Presentations of Groups, VI

Worse still, it is quite difficult even to determine whether a given presentation contains any elements other than the identity (i.e., whether the presentation is merely describing the trivial group).

- For example, the presentation $\langle r, s \mid r^4 = s^2 = e,\ rs = sr^{-1} \rangle$ describes $D_{2\cdot 4}$, a group of order 8.
- On the other hand, the very similar presentation $\langle r, s \mid r^4 = s^2 = e,\ rs = sr^2 \rangle$ turns out to describe a group of order 2, since in this group one has $r = rs^2 = (rs)s = sr^2 s = (sr)rs = (sr)sr^2 = s(rs)r^2 = s(sr^2)r^2 = s^2 r^4 = e$.
- As another example, the presentation $\langle x, y \mid x^2 = y^3 = (xy)^4 \rangle$ describes a group of order 24, whereas the very similar presentation $\langle x, y \mid x^3 = y^3 = (xy)^4 \rangle$ describes an infinite group!

Presentations of Groups, VII

We will also mention that we have not given a rigorous development of presentations as abstract groups.

- Perhaps unsurprisingly, given the description in terms of words, the formal definition uses free groups.
- We will briefly mention how this works after we discuss quotient groups.

Cyclic Groups, I

The simplest nontrivial case of group generation is where $S = \{g\}$: then $\langle S \rangle = \{\ldots, g^{-2}, g^{-1}, e, g, g^2, \ldots\}$ is just the powers of g.

Definition

A group G is cyclic if it is generated by a single element: in other words, if there exists some $g \in G$ such that $G = \langle g \rangle = \{\ldots, g^{-2}, g^{-1}, e, g, g^2, \ldots\}$.

Examples:

- $\mathbb{Z}/m\mathbb{Z}$ and $\mathbb{Z}$, under addition, are both cyclic groups generated by 1.
- The group $\{1, \zeta_n, \ldots, \zeta_n^{n-1}\}$ of nth roots of unity is cyclic, generated by ζ_n.
- The subgroups $\{1, r, r^2, \ldots, r^{n-1}\}$ and $\{e, sr^k\}$ for any k are cyclic subgroups of $D_{2 \cdot n}$.

Cyclic Groups, II

Cyclic groups are abelian, as powers of g commute with each other.

- If G is cyclic with generator g of infinite order, then $g^a \neq g^b$ for any $a \neq b$ as we have previously noted, and so $G = \{\ldots, g^{-2}, g^{-1}, e, g, g^2, \ldots\}$ has infinitely many elements.
- On the other hand, if H is cyclic with generator g having finite order n, then $g^a = g^b$ if and only if $a \equiv b \pmod{n}$. Thus in fact $G = \{e, g, g^2, \ldots, g^{n-1}\}$ so that G contains n elements.
- In both cases, we see that the order of G is equal to the order of its generator g: thus, the two uses of "order", one referring to elements and the other referring to groups, are related in a very natural way.
- Also from our results on order, if g has order n then the order of g^k in H is then $n/\gcd(k, n)$, and so H is generated by any element of the form g^d for d relatively prime to n.

Cyclic Groups, III

The subgroups of cyclic groups have a particularly nice structure, in that they are all cyclic also:

Proposition (Subgroups of Cyclic Groups)

Suppose that $G = \langle g \rangle$ is a cyclic group.

1. *Every subgroup of G is cyclic.*
2. *If $|g| = \infty$, then every subgroup of G can be uniquely written as $\langle g^d \rangle$ for some nonnegative integer d. All of these subgroups are distinct.*
3. *If $|g| = n$, then every subgroup of G can be uniquely written as $\langle g^d \rangle$ for some nonnegative integer d dividing n, and this subgroup has order n/d. All of these subgroups are distinct.*
4. *Subgroups of the listed forms have $\langle g^a \rangle \subseteq \langle g^b \rangle$ if and only if a divides b.*

Cyclic Groups, IV

Proofs:

1. Every subgroup of G is cyclic.
   - Suppose $G = \langle g \rangle$ is cyclic and H is a subgroup of G.
   - If $h = g^k$ is any element of H, then $g^{|k|}$ is also in H, since it is either equal to h or to h^{-1} (and H is a subgroup).
   - Since $g^0 = e$ is always in H, we see H is completely characterized by the set $S = \{n > 0 : g^n \in H\}$.
   - If $S = \emptyset$ the result is trivial; otherwise S is nonempty, so by the well-ordering axiom S has a minimal element d.
   - Then H contains g^d hence $\langle g^d \rangle$.
   - If $h = g^a$ is any other element of H, if we divide to write $a = qd + r$, we would have $g^r = g^a(g^d)^{-q} \in H$, so by minimality of d we must have $r = 0$.
   - This means $h = g^a = (g^d)^q$ and so h is in $\langle g^d \rangle$.
   - Thus, $H \subseteq \langle g^d \rangle$ hence $H = \langle g^d \rangle$.

Cyclic Groups, IV

Proofs:

2. If $|g| = \infty$, then every subgroup of G can be uniquely written as $\langle g^d \rangle$ for some nonnegative integer d. All of these subgroups are distinct.
   - If $|g| = \infty$ then since all the powers of g are distinct, the subgroups $\langle g^a \rangle$ and $\langle g^b \rangle$ are distinct because the set of multiples of a is distinct from the set of multiples of b for any positive $a \neq b$.
   - Since every subgroup is cyclic, these are all of the subgroups.

Cyclic Groups, V

Proofs:

3. If $|g| = n$, then every subgroup of G can be uniquely written as $\langle g^d \rangle$ for some nonnegative integer d dividing n, and this subgroup has order n/d. All of these subgroups are distinct.
   - If $|g| = n$, suppose $H = \langle g^d \rangle$ where d is minimal and positive.
   - If we write $n = q'd + r'$ by the division algorithm, then $g^{r'} = g^n (g^d)^{-q'} \in H$, so by minimality of d we must have $r = 0$, meaning that d divides n.
   - Then the order of $\langle g^d \rangle$ is the same as the order of g^d, which is $n/\gcd(d, n) = n/d$.
   - All of these subgroups are then clearly distinct because their orders are distinct.
4. Subgroups of the listed forms have $\langle g^a \rangle \subseteq \langle g^b \rangle$ if and only if a divides b.
   - Immediate.

Cyclic Groups, VI

Example: List the subgroups of $\mathbb{Z}/18\mathbb{Z}$ and their orders.

Cyclic Groups, VI

Example: List the subgroups of $\mathbb{Z}/18\mathbb{Z}$ and their orders.

The subgroups are as follows:

1. $\langle 1 \rangle = \{0, 1, 2, \ldots, 17\}$, order 18.
2. $\langle 2 \rangle = \{0, 2, 4, \ldots, 16\}$, order 9.
3. $\langle 3 \rangle = \{0, 3, 6, 9, 12, 15\}$, order 6.
4. $\langle 6 \rangle = \{0, 6, 12\}$, order 3.
5. $\langle 9 \rangle = \{0, 9\}$, order 2.
6. $\langle 18 \rangle = \langle 0 \rangle = \{0\}$, order 1.

Cyclic Groups, VII

Just to keep you on your toes, I'll now throw in something very interesting (and useful) about multiplicative groups that arise from fields:

Theorem (Cyclic Groups and Fields)

If F is a finite field, then the group of units $F^\times$ is cyclic. More generally, if G is any finite subgroup of the group of units in any field (finite or not), then G is cyclic.

Example: The group $(\mathbb{Z}/7\mathbb{Z})^\times$ is cyclic of order 6. Indeed, 3 is a generator, since its powers are $\{1, 3, 2, 6, 4, 5\}$.

Cyclic Groups, VIII

Our proof is nonconstructive: we will establish the existence of an element in G having order $|G|$ without explicitly finding one.

- Such an element is called a primitive root in the context of $\mathbb{Z}/m\mathbb{Z}$ or finite fields.
- In fact, no constructive algorithm is known for finding a primitive root in $\mathbb{F}_p$ that is appreciably faster than merely testing the elements 2, 3, ... until a primitive root is identified.

We start with a lemma:

Lemma

Suppose G is a finite subgroup of the group of units in a field F. If M is the maximal order among all elements in G, then the order of every element in G divides M.

Cyclic Groups, IX

Proof (of lemma):

- Let M be the maximal order of all units in G.
- Suppose g has order M, and let h be any other element of order k.
- If k does not divide M, then there is some prime q which occurs to a higher power q^f in the factorization of k than the corresponding power q^e dividing M.
- By properties of orders, the element g^{q^f} has order M/q^f, and the element h^{k/q^e} has order q^e.
- Since these two orders are relatively prime and $gh = hg$ (since these are elements in a field), we see that the element $g^{q^f} \cdot h^{k/q^e}$ has order $M \cdot q^{f-e}$.
- This is a contradiction because this element's order is larger than M. Thus, k divides M as claimed.

Cyclic Groups, IX

Proof (of theorem):

- Let M be the maximal order of all units in G.
- Then any element of order M generates a subgroup of G having M elements, so $M \leq |G|$.
- Furthermore, by the lemma, we know that all elements in G have order dividing M, so the polynomial $p(x) = x^M - 1$ has $|G|$ roots in $F[x]$.
- But by unique factorization in $F[x]$, this is impossible unless $M \geq |G|$, since a polynomial of degree M can only have at most M roots in $F[x]$.
- Hence we conclude $M = |G|$, meaning that some element has order $|G|$.
- This element is then a generator of G and so G is cyclic.

Cyclic Groups, X

Example: The unit group G of $\mathbb{F}_3[x]/(x^2+x+2)$ is cyclic of order 8.

- With some calculation, we can see that x is a generator of G.
- Explicitly, we can compute $x^2 \equiv 2x+1$ so that $x^4 \equiv 2$, and thus $x^8 \equiv 1$.
- By our results on orders, this implies that x has order 8 inside G (its order must divide 8, but it does not divide 4), so it is a generator.

Group Isomorphisms, I

We now formalize the notion of when two groups have identical structures, which captures the same idea as with rings:

Definition

Let $(G, \star)$ and $(H, \circ)$ be groups. A group isomorphism φ from G to H is a bijective function $\varphi : G \to H$ such that $\varphi(g_1 \star g_2) = \varphi(g_1) \circ \varphi(g_2)$ for all g_1 and g_2 in G.

If there is an isomorphism $\varphi : G \to H$, we say G and H are isomorphic, and write $G \cong H$.

We usually suppress the notation for the group operations and write the condition simply as $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$.

Group Isomorphisms, II

Examples:

1. If R and S are rings, any ring isomorphism $\varphi : R \to S$ yields a group isomorphism of the groups $(R, +)$ and $(S, +)$, and also (when restricted to the respective unit groups) yields a group isomorphism of $(R^\times, \cdot)$ with $(S^\times, \cdot)$.
2. For $G = \mathbb{Z}/6\mathbb{Z}$ and $H = (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/3\mathbb{Z})$, the map $\varphi : G \to H$ defined via $\varphi(n \bmod 6) = (n \bmod 2, n \bmod 3)$ is an isomorphism of groups, since we have previously shown it is a ring isomorphism.
3. For $G = (\mathbb{R}, +)$ and $H = (\mathbb{R}^+, \cdot)$, the map $\varphi : G \to H$ defined via $\varphi(x) = e^x$ is a group isomorphism from G to H.
   - The map respects the group operation since $e^{x+y} = e^x e^y$, and it is a bijection since it has an inverse map $\varphi^{-1}(x) = \ln(x)$.

Group Isomorphisms, III

Examples:

3. For $G = D_{2\cdot 3}$ and $H = S_3$, the map $\varphi : G \to H$ defined by associating a symmetry of the equilateral triangle with its associated permutation on the labeled vertices of the triangle is a group isomorphism.
   - The geometric description implies that it respects the group operations, and it is a bijection because it is injective and both groups have order 6.
   - Alternatively, of course, one could write down all the operations explicitly and just check.

Group Isomorphisms, IV

We have various properties of isomorphisms:

Proposition (Properties of Isomorphisms)

If G, H, K are any groups, the following hold:

1. *The identity map $I : G \to G$ is an isomorphism from G to G.*
2. *If $\varphi : G \to H$ is an isomorphism, then so is $\varphi^{-1} : H \to G$.*
3. *If $\varphi : G \to H$ and $\psi : H \to K$ are isomorphisms, then so is the composition $\psi\varphi : G \to K$.*
4. *If $\varphi : G \to H$ is an isomorphism and $g \in G$, then $\varphi(e_G) = e_H$ and $\varphi(g^n) = \varphi(g)^n$ for any $n \in \mathbb{Z}$. In particular, $|g| = |\varphi(g)|$.*
5. *If $\varphi : G \to H$ is an isomorphism, then $gh = hg$ if and only if $\varphi(g)\varphi(h) = \varphi(h)\varphi(g)$. In particular, G is abelian if and only if H is abelian.*
6. *If $\varphi : G \to H$ is an isomorphism and K is any subset of G, then K is a subgroup of G if and only if the set $\varphi(K) = \{\varphi(k) : k \in K\}$ is a subgroup of H.*

Group Isomorphisms, V

Proofs:

- (1)–(4), establishing that group isomorphism is an equivalence relation and that isomorphisms preserve the identity, follow the same way as for rings.
- The fact that $\varphi(g^n) = \varphi(g)^n$ follows from a trivial induction. Then $|g| = |\varphi(g)|$ follows from this and the fact that φ preserves the identity.
- Preservation of commutativity (5) is immediate from the definition.
- Finally, since isomorphisms preserve all of the properties needed to check the subgroup criterion, (6) follows easily.

Group Isomorphisms, VI

In order to show that two given groups are isomorphic, we essentially need to construct an isomorphism between them, which can often be difficult to do.

- More specifically, it has been shown that the isomorphism problem for groups (given two groups, decide whether or not they are isomorphic) is undecidable.
- Even if we are handed an isomorphism, actually verifying that it is an isomorphism can be very time-consuming.

Group Isomorphisms, VII

On the other hand, it is often easier to show that two given groups cannot be isomorphic to one another, if one of the properties of isomorphisms fails.

- For example, the group $D_{2\cdot 4}$ is not isomorphic to S_3, because the former has order 8 and the latter has order 6, and so there cannot even exist a bijection between their underlying sets of elements.
- In a similar way we can see that $D_{2\cdot 4}$ is not isomorphic to $\mathbb{Z}/8\mathbb{Z}$, because the latter is abelian and the former is not; likewise, S_3 is not isomorphic to $\mathbb{Z}/6\mathbb{Z}$.
- Also, $D_{2\cdot 4}$ is not isomorphic to Q_8, because there are 5 elements of order 2 in $D_{2\cdot 4}$ (namely, r^2 and sr^k for $0 \leq k \leq 3$) but only 1 element of order 2 in Q_8 (namely, -1).

Group Isomorphisms, VIII

A fundamental goal of group theory is to classify (up to isomorphism) all of the groups of a given order.

- By extending arguments like the ones given above, one can show, for example, that the five groups $D_{2\cdot 4}$, Q_8, $\mathbb{Z}/8\mathbb{Z}$, $(\mathbb{Z}/4\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$, and $(\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$ are nonisomorphic groups of order 8.
- It turns out that any group of order 8 must be isomorphic to one of these five, but to prove this fact only from the results we have developed so far would be very difficult.

Group Isomorphisms, IX

A first step towards such a classification is to classify cyclic groups, which turns out to be extremely easy:

Proposition (Isomorphism and Cyclic Groups)

Any two cyclic groups of the same order are isomorphic. More explicitly, any cyclic group of order n is isomorphic to $\mathbb{Z}/n\mathbb{Z}$ and any infinite cyclic group is isomorphic to $\mathbb{Z}$.

Here, we only need to show the second statement; it implies the first one because isomorphism is an equivalence relation.

Group Isomorphisms, X

Proof:

- First suppose $G = \langle g \rangle = \{e, g, g^2, \ldots, g^{n-1}\}$ is cyclic of order n, and consider the map $\varphi : \mathbb{Z}/n\mathbb{Z} \to G$ with $\varphi(\overline{a}) = g^a$.
- This map is well-defined because $g^n = e$ implies that $g^a = g^b$ whenever $a \equiv b \pmod{n}$, it is clearly surjective and hence a bijection (since both sets have the same size), and $\varphi(\overline{a} + \overline{b}) = g^{a+b} = g^a g^b = \varphi(\overline{a})\varphi(\overline{b})$.
- Thus, φ is an isomorphism.
- Now suppose $G = \langle g \rangle = \{\ldots, g^{-2}, g^{-1}, e, g, g^2, \ldots\}$ is an infinite cyclic group.
- Consider the map $\varphi : \mathbb{Z} \to G$ defined via $\varphi(a) = g^a$.
- This map is injective (since $g^a \neq e$ for any $a \neq 0$), surjective (by definition of $\langle g \rangle$), and $\varphi(a + b) = g^{a+b} = g^a g^b = \varphi(a)\varphi(b)$, so φ is an isomorphism.

Group Homomorphisms, I

Now we examine homomorphisms:

Definition

Let $(G, \star)$ and $(H, \circ)$ be groups. A group homomorphism φ from G to H is a function $\varphi : G \to H$ such that $\varphi(g_1 \star g_2) = \varphi(g_1) \circ \varphi(g_2)$ for all g_1 and g_2 in G.

Examples:

1. Every isomorphism is a homomorphism (of course).
2. Any ring homomorphism $\varphi : R \to S$ is automatically a group homomorphism on the underlying additive and multiplicative groups.
3. As special cases we have the projection maps $\varphi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ and $\varphi : F[x] \to F[x]/p$.

Group Homomorphisms, II

Examples:

4. The map $\varphi : (\mathbb{Z}/n\mathbb{Z}) \to D_{2 \cdot n}$ given by $\varphi(\overline{a}) = r^a$ is a group homomorphism: it is well-defined because $a \equiv b \pmod{n}$ implies $r^a = r^b$ because $r^n = e$, and also $\varphi(\overline{a} + \overline{b}) = r^{a+b} = r^a r^b = \varphi(\overline{a})\varphi(\overline{b})$. This map is injective but not surjective.
5. If G is the additive abelian group of all smooth real-valued functions, the derivative map $D : G \to G$ given by $D(f) = f'$ is a group homomorphism, since $D(f + g) = (f + g)' = f' + g' = D(f) + D(g)$.
6. Let G and H be any groups. The "trivial map" $z : G \to H$ given by $z(g) = e_H$ for every $g \in G$ is a group homomorphism.
7. If H is a subgroup of G, the inclusion map $\iota : H \to G$ given by $\iota(h) = h$ is a group homomorphism.

Group Homomorphisms, III

Many of the properties we established for isomorphisms also hold for homomorphisms (using the same proofs).

Proposition (Properties of Homomorphisms)

If G, H, K are any groups, the following hold:

1. *If $\varphi : G \to H$ and $\psi : H \to K$ are homomorphisms, then so is the composition $\psi\varphi : G \to K$.*
2. *If $\varphi : G \to H$ is a homomorphism and $g \in G$, then $\varphi(e_G) = e_H$ and $\varphi(g^n) = \varphi(g)^n$ for any $n \in \mathbb{Z}$.*

Proofs: Straightforward.

Group Homomorphisms, IV

If we do not have any structural information about the nature of the map φ, it can be difficult to verify the homomorphism condition, since it would seem that we would need to verify the condition separately for every pair of elements in G.

- However, if we have a set of generators for G, we can express all of the other elements in terms of the generators, and so it is reasonable to think that we can reduce the calculation to one involving only the generators.
- Explicitly, suppose that G is generated by the set S. If $g_1 g_2 \cdots g_n = e_G$ is any relation with the $g_i \in S \cup S^{-1}$, then applying φ to both sides yields $\varphi(g_1)\varphi(g_2)\cdots\varphi(g_n) = e_H$: this means that the images of the generators must satisfy the same relation in H.

Group Homomorphisms, V

Conversely, suppose G is generated by $S = \{s_i\}$, and $\varphi(s_i) = r_i$.

- Then every element in G can be written as a product of the elements in $S \cup S^{-1}$ so the values of $\varphi(s_i)$ determine the value of $\varphi(g)$ for every $g \in G$.
- Furthermore, if the elements r_i satisfy all of the same relations as the elements s_i, then (one can show) φ will be well-defined, and it is immediate that φ is then a group homomorphism.
- Thus, if G is generated by $S = \{s_i\}$ satisfying a collection of relations, and elements $r_i \in H$ have the property that the r_i satisfy the same relations, then there exists a (unique) homomorphism $\varphi : G \to H$ such that $\varphi(s_i) = r_i$ for each i.

To summarize: if we have a presentation of G, then to verify that $\varphi : G \to H$ is a homomorphism, all we need to do is check that φ respects all of the relations in the presentation.

Group Homomorphisms, VI

Example: Show that there is a group homomorphism $\varphi : D_{2\cdot 3} \to S_3$ with $\varphi(r) = (1\,2\,3)$ and $\varphi(s) = (1\,2)$.

Group Homomorphisms, VI

Example: Show that there is a group homomorphism $\varphi : D_{2\cdot 3} \to S_3$ with $\varphi(r) = (1\,2\,3)$ and $\varphi(s) = (1\,2)$.

- Since $D_{2\cdot 3} = \langle r, s \mid r^3 = s^2 = e,\ rs = sr^{-1} \rangle$, by the discussion above we need only verify the relations.
- We see $\varphi(r)^3 = (1\,2\,3)^3 = 1$, $\varphi(s)^2 = (1\,2)^2 = 1$, and also that $\varphi(r)\varphi(s) = (1\,2\,3)(1\,2) = (1\,3) = (1\,2)(1\,3\,2) = (1\,2)(1\,2\,3)^{-1} = \varphi(s)\varphi(r)^{-1}$.
- Since $\varphi(r)$ and $\varphi(s)$ satisfy the required relations, we conclude that there is such a homomorphism.
- In fact, since S_3 is generated by $\varphi(r)$ and $\varphi(s)$, φ is surjective, hence a bijection and thus an isomorphism.

Group Homomorphisms, VII

Example: Show that there is a group homomorphism $\varphi : V_4 \to S_4$ with $\varphi(a) = \varphi(b) = (1\,2)(3\,4)$.

Group Homomorphisms, VII

Example: Show that there is a group homomorphism $\varphi : V_4 \to S_4$ with $\varphi(a) = \varphi(b) = (1\,2)(3\,4)$.

- Since $V_4 = \langle a, b \,|\, a^2 = b^2 = e, ab = ba \rangle$, we need only verify the relations.
- We see $\varphi(a)^2 = \varphi(b)^2 = e$, and also $\varphi(a)\varphi(b) = (1\,2)(3\,4)(1\,2)(3\,4) = \varphi(b)\varphi(a)$.
- Since $\varphi(a)$ and $\varphi(b)$ satisfy the required relations, we conclude that there is such a homomorphism.

Group Homomorphisms, VIII

As with rings, we also have the same notions of kernel and image for group homomorphisms:

Definition

If $\varphi : G \to H$ is a group homomorphism, the kernel of φ, denoted $\ker \varphi$, is the set of elements in G mapped to e_H by φ. In other words, $\ker \varphi = \{g \in G : \varphi(g) = e_H\}$.

Definition

If $\varphi : G \to H$ is a group homomorphism, the image of φ, denoted $\operatorname{im} \varphi$, is the set of elements in H of the form $\varphi(g)$ for some $g \in G$.

Group Homomorphisms, IX

Examples:

1. The kernel of the reduction homomorphism $\varphi : \mathbb{Z} \to \mathbb{Z}/m\mathbb{Z}$ is the subgroup $m\mathbb{Z}$.
2. The kernel of the derivative map D is the collection of constant functions.
3. The kernel of the homomorphism $\varphi : V_4 \to S_4$ with $\varphi(a) = \varphi(b) = (1\,2)(3\,4)$ is $\{e, ab\}$. The image is $\{1, (1\,2)(3\,4)\}$.

Group Homomorphisms, X

We have various properties of the kernel and image:

Proposition (Kernel and Image)

Let $\varphi : G \to H$ be a group homomorphism. Then

1. *The image $\operatorname{im}\varphi$ is a subgroup of H.*
2. *The kernel $\ker\varphi$ is a subgroup of R. Also, if $g \in \ker\varphi$, then aga^{-1} is in $\ker\varphi$ for any $a \in G$.*
3. *The kernel is zero (i.e., $\ker\varphi = \{e_G\}$) if and only if φ is injective.*
4. *The map φ is an isomorphism if and only if $\ker\varphi = \{e_G\}$ and $\operatorname{im}\varphi = H$.*

Group Homomorphisms, XI

Proofs:

1. The image $\operatorname{im}\varphi$ is a subgroup of H.
   - Since $\varphi(e_G) = e_H$, the image contains e_H.
   - Also, if $h_1, h_2 \in \operatorname{im}\varphi$ so that $\varphi(g_1) = h_1$ and $\varphi(g_2) = h_2$ for some $g_1, g_2 \in R$, then $h_1 h_2^{-1} = \varphi(g_1 g_2^{-1})$ is also in $\operatorname{im}\varphi$. Thus $\operatorname{im}\varphi$ is a subgroup.
2. The kernel $\ker\varphi$ is a subgroup of R. Also, if $g \in \ker\varphi$, then aga^{-1} is in $\ker\varphi$ for any $a \in G$.
   - Since $\varphi(e_G) = e_H$, the kernel contains e_G.
   - Further, if $g_1, g_2 \in \ker\varphi$ then $\varphi(g_1 g_2^{-1}) = e_H e_H^{-1} = e_H$, so $g_1 g_2^{-1} \in \ker\varphi$. Thus $\ker\varphi$ is a subgroup.
   - Also, $\varphi(aga^{-1}) = \varphi(a)e_H\varphi(a^{-1}) = \varphi(a)\varphi(a)^{-1} = e_H$ so that $aga^{-1} \in \ker\varphi$.

Group Homomorphisms, XI

Proofs:

3. The kernel is zero (i.e., $\ker\varphi = \{e_G\}$) if and only if φ is injective.
   - If $\varphi(g_1) = \varphi(g_2)$, then $\varphi(g_1 g_2^{-1}) = \varphi(g_1)\varphi(g_2)^{-1} = e_H$, so $g_1 g_2^{-1} \in \ker\varphi$.
   - Thus, if the only element in $\ker\varphi$ is e_G, then we must have $g_1 g_2^{-1} = e_G$ so that $g_1 = g_2$.
   - Conversely, if $g \in \ker\varphi$ and φ is injective, then $\varphi(g) = e_H = \varphi(e_G)$ implies $g = e_G$, so $\ker\varphi = \{e_G\}$.
4. The map φ is an isomorphism if and only if $\ker\varphi = \{e_G\}$ and $\operatorname{im}\varphi = H$.
   - This follows from (3), since $\ker\varphi = \{e_G\}$ is equivalent to φ being injective and $\operatorname{im}\varphi = H$ is equivalent to φ being surjective.

Motivation for Cosets, I

We would now like to generalize the idea of modular arithmetic and quotients into the context of groups.

- We can give a similar sort of motivation to the development we gave with ideals of rings.
- However, some of the details will be a little bit more difficult because of the non-commutativity of the group operation.
- However, based on the situation with rings, you should be able to guess that the condition we are searching for is the same property that kernels possess.

Motivation for Cosets, II

So suppose G is a group and N is a subset of G, whose properties we intend to characterize in a moment.

- Let us say that two elements $a, b \in G$ are "congruent modulo N" if $a^{-1}b \in N$.
- Note that this is just the multiplicative version of the statement $b - a \in I$ we used for ideals, but written in the order $(-a) + b$ instead.
- We would like "congruence modulo N" to be an equivalence relation, which requires
  1. $a \equiv a \pmod{N}$
  2. $a \equiv b \pmod{I}$ implies $b \equiv a \pmod{N}$
  3. $a \equiv b \pmod{N}$, $b \equiv c \pmod{N}$ imply $a \equiv c \pmod{N}$.

Motivation for Cosets, III

We require

1. $a \equiv a \pmod{N}$
2. $a \equiv b \pmod{I}$ implies $b \equiv a \pmod{N}$
3. $a \equiv b \pmod{N}$, $b \equiv c \pmod{N}$ imply $a \equiv c \pmod{N}$.

- (1) says $a^{-1}a = e_G \in N$.
- (2) says if $a^{-1}b \in N$ then $b^{-1}a \in N$. Since $b^{-1}a = (a^{-1}b)^{-1}$, this is the same as saying that N is closed under inverses.
- (3) says if $a^{-1}b \in N$ and $b^{-1}c \in N$, then $a^{-1}c \in N$. Since $a^{-1}c = (a^{-1}b)(b^{-1}c)$, this is the same as saying that N is closed under multiplication.
- Thus, all of these conditions together are equivalent to saying that N is a subgroup of G, which seems quite reasonable.

Motivation for Cosets, IV

We would also like congruences to respect the group operation: if $a \equiv c \pmod{N}$ and $b \equiv d \pmod{N}$ then $ab \equiv cd \pmod{N}$.

- The hypotheses are equivalent to saying that there exist $n_1, n_2 \in N$ such that $a^{-1}c = n_1$ and $b^{-1}d = n_2$, which is to say, $c = an_1$ and $d = bn_2$.
- Then the desired condition is that $(ab)^{-1}(cd) = b^{-1}a^{-1}an_1bn_2 = b^{-1}n_1bn_2$ is in N, for any $a, b \in G$ and $n_1, n_2 \in N$.
- This condition is a bit unwieldy, but if we set $n_2 = e_G$ and $b^{-1} = c$, then it reduces to the statement that $cn_1c^{-1} \in N$ for any $c \in G$ and any $n_1 \in N$.
- On the other hand, if $cnc^{-1} \in N$ for every $c \in G$ and $n \in N$, then if we write $b^{-1}n_1b = n_3 \in N$ (by hypothesis) then the element $b^{-1}n_1bn_2 = n_3n_2$ is then also in N, since N is a subgroup.

Motivation for Cosets, V

To summarize, the hypothesis that N is a subgroup and $cnc^{-1} \in N$ for every $c \in G$ and $n \in N$ is equivalent to saying that congruences are an equivalence relation respecting the group operation.

- With this condition in hand, we can define residue classes.
- Specifically, the residue class $\overline{a}$ is the collection of all b such that $a \equiv b \pmod{N}$: explicitly, $\overline{a} = \{b \in G : a^{-1}b \in N\} = \{an : n \in N\}$.
- Finally, we can define the group operation on residue classes via $\overline{a} \cdot \overline{b} = \overline{ab}$, and observe that this operation is well defined because congruence respects the group operation.
- Explicitly, if $\overline{a} = \overline{c}$ and $\overline{b} = \overline{d}$, then $\overline{ab} = \overline{cd}$, because $a \equiv c \pmod{N}$ and $b \equiv d \pmod{N}$ imply that $ab \equiv cd \pmod{N}$ per the above discussion.

Motivation for Cosets, VI

With these assumptions, the collection of residue classes $\overline{a} = aN = \{an : n \in N\}$ will then have a well-defined group operation given by $\overline{a} \cdot \overline{b} = \overline{ab}$.

- We will also note that the statement that $cnc^{-1} \in N$ for every $c \in G$ and $n \in N$ is equivalent to the statement that for every $c \in G$, the set $cNc^{-1} = \{cnc^{-1} : n \in N\}$ is equal to N itself.
- One direction is clear, since if $cNc^{-1} = N$ for every $c \in G$, then certainly $cnc^{-1} \in N$ for every $c \in G$ and $n \in N$.
- On the other hand, if $cnc^{-1} \in N$ for every $c \in G$ and $n \in N$, then $cNc^{-1} \subseteq N$ for all c. In particular, plugging in c^{-1} for c yields $c^{-1}Nc \subseteq N$, which is equivalent to $N \subseteq cNc^{-1}$: thus we must have $cNc^{-1} = N$ for all $c \in G$.

Motivation for Cosets, VII

Next time, we will examine more closely the properties of the sets aH for $a \in G$ and H a subgroup of G: these sets are called left cosets of H.

We will then go through the details of quotient groups and analyze the properties of normal subgroups, the subgroups for which $cNc^{-1} = N$ for all $c \in G$.

Summary

We discussed generators and presentations of groups.

We discussed the structure of cyclic groups.

We discussed group isomorphisms and homomorphisms.

We introduced the motivation behind the definition of cosets.

Next lecture: Cosets, normal subgroups, and quotients.