Math 5111 (Algebra 1)

Lecture #13 of 24 $\sim$ October 19th, 2020

Cosets, Normal Subgroups, and Quotient Groups

- Cosets of Subgroups
- Lagrange's Theorem
- Normal Subgroups and Quotient Groups

This material represents §3.2.1-3.2.2 from the course notes.

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 $c \in G$.

Cosets, I

Now that we have identified the property we want to use to construct quotient groups, we examine more closely the properties of the underlying sets of elements in G:

Definition

If H is a subgroup of G and $a \in G$, the set $aH = \{ah : h \in H\}$ is called a left coset of H.
We also define the index of H in G, denoted $[G : H]$, to be the number of distinct left cosets of H in G.

- If G is an additive abelian group, we will write left cosets as $a + H$; note that this notation is consistent with our prior use of $r + I$ in rings.

Cosets, II

We also have a symmetric notion of a right coset:

Definition

If H is a subgroup of G and $a \in G$, the set $Ha = \{ha : h \in H\}$ is called a right coset of H.

- If G is abelian, then left and right cosets are the same, but when G is non-abelian, this need not be the case.
- We will see in a moment that the numbers of left cosets and right cosets are the same, so the definition of the index is independent of whether we use left or right cosets.
- If G is an additive abelian group, we will write (left) cosets as $a + H$; note that this notation is consistent with our prior use of $r + I$ in rings.

Cosets, III

Examples:

1. Let $H = \{1, (1\,3)\}$ in $G = S_3$. Find the left and right cosets of H in G and compute $[G : H]$.

Cosets, III

Examples:

1. Let $H = \{1, (1\,3)\}$ in $G = S_3$. Find the left and right cosets of H in G and compute $[G : H]$.
   - There are three left cosets of H in G: explicitly, they are $1H = (1\,3)H = \{1, (1\,3)\}$, $(1\,2)H = (1\,3\,2)H = \{(1\,2), (1\,3\,2)\}$, and $(2\,3)H = (1\,2\,3)H = \{(2\,3), (1\,2\,3)\}$.
   - Thus, here we have $[G : H] = 3$.
   - There are also three right cosets of H in G: explicitly, they are $H1 = H(1\,3) = \{1, (1\,3)\}$, $H(1\,2) = H(1\,2\,3) = \{(1\,2), (1\,2\,3)\}$, and $H(1\,3) = H(1\,3\,2) = \{(1\,3), (1\,3\,2)\}$.
   - Notice that the left and right cosets are not all equal to each other; for example, $(1\,2)H \neq H(1\,2)$.

Cosets, IV

Examples:

2. Let $H = \{e, r^2\}$ in $G = D_{2\cdot 4}$. Find the left and right cosets of H in G and compute $[G : H]$.

Cosets, IV

Examples:

2. Let $H = \{e, r^2\}$ in $G = D_{2\cdot 4}$. Find the left and right cosets of H in G and compute $[G : H]$.
   - There are four left cosets of H in G, namely $eH = r^2H = \{e, r^2\}$, $rH = r^3H = \{r, r^3\}$, $sH = sr^2H = \{s, sr^2\}$, and $srH = sr^3H = \{sr, sr^3\}$.
   - Thus, we see $[G : H] = 4$.
   - There are also four right cosets of H in G, namely $He = Hr^2 = \{e, r^2\}$, $Hr = Hr^3 = \{r, r^3\}$, $Hs = Hsr^2 = \{s, sr^2\}$, and $Hsr = Hsr^3 = \{sr, sr^3\}$.
   - Here that the left and right cosets of H are the same, even though G is not abelian.

Cosets, V

Examples:

3. Let $H = \{1, (1\,2\,3), (1\,3\,2)\}$ in $G = S_3$. Find the left and right cosets of H in G and compute $[G : H]$.

Cosets, V

Examples:

3. Let $H = \{1, (1\,2\,3), (1\,3\,2)\}$ in $G = S_3$. Find the left and right cosets of H in G and compute $[G : H]$.
   - Then there are two left cosets of H in G, namely $1H = (1\,2\,3)H = (1\,3\,2)H = \{1, (1\,2\,3), (1\,3\,2)\}$ and $(1\,2)H = (1\,3)H = (2\,3)H = \{(1\,2), (1\,3), (2\,3)\}$.
   - Thus, here we have $[G : H] = 2$.
   - In this case, the right cosets are the same as the left cosets of H: they are $H1 = H(1\,2\,3) = H(1\,3\,2) = \{1, (1\,2\,3), (1\,3\,2)\}$ and $H(1\,2) = H(1\,3) = H(2\,3) = \{(1\,2), (1\,3), (2\,3)\}$.

Cosets, VI

Examples:

4. Let $H = 2\mathbb{Z} = \{\ldots, -2, 0, 2, 4, \ldots\}$ in $G = \mathbb{Z}$. Find the left and right cosets of H in G and compute $[G : H]$.

Cosets, VI

Examples:

4. Let $H = 2\mathbb{Z} = \{\ldots, -2, 0, 2, 4, \ldots\}$ in $G = \mathbb{Z}$. Find the left and right cosets of H in G and compute $[G : H]$.
   - Here the left and right cosets are the same, since G is abelian.
   - Using additive notation, we see that the cosets are $0 + H = \{\ldots, -2, 0, 2, 4, \ldots\}$ and $1 + H = \{\ldots, -3, 1, 3, 5, \ldots\}$.
   - Perhaps unsurprisingly, the cosets are simply the residue classes $\overline{0}$ and $\overline{1}$ modulo 2, and there are $[G : H] = 2$ of them.

Cosets, VII

In each of the examples above, all of the cosets had the same size (which is then the same size as $eH = H$), and the left cosets partitioned G. This is true in general:

Proposition (Properties of Cosets)

Let H be a subgroup of G, and $g, h \in G$. Then the following hold:

1. *For any $a \in G$, the map $f : H \to aH$ defined by $f(g) = ag$ is a bijection between H and gH.*
2. *For any $a \in G$, the only left coset of H containing a is aH.*
3. *Any two left cosets of H in G are either disjoint or identical. Thus, the left cosets of H in G partition G.*
4. *For any $a, b \in G$, we have $aH = bH$ if and only if $a^{-1}b \in H$.*

All of these properties also hold if we replace left cosets with right cosets everywhere, and modify the statements accordingly.

Cosets, VIII

1. For any $a \in G$, the map $f : H \to aH$ defined by $f(g) = ag$ is a bijection between H and gH.

Proof:

- By definition of aH, the map f is surjective.
- On the other hand, $f(g_1) = f(g_2)$ is equivalent to $ag_1 = ag_2$, which by cancellation implies $g_1 = g_2$.
- Thus, f is also injective, so it is a bijection.

Cosets, IX

2. For any $a \in G$, the only left coset of H containing a is aH.

Proof:

- Clearly aH is a left coset of H containing a since $e \in H$, so we need to show it is the only one.
- If $a \in bH$ then by definition $a = bh$ for some $h \in H$.
- Then for any $h' \in H$, since $hh' \in H$ because H is a subgroup, we see that $ah' = b(hh') \in bH$. Thus bH contains aH.
- On the other hand, for any $bh'' \in bH$, since $b = ah^{-1}$ we can write $bh'' = a(h^{-1}h'') \in aH$ because $h^{-1}h'' \in H$ again because H is a subgroup. Thus, aH contains bH, so they are equal.

Cosets, X

3. Any two left cosets of H in G are either disjoint or identical. Thus, the left cosets of H in G partition G.

Proof:

- Suppose aH and bH are left cosets of H. If they are disjoint we are done, so suppose they have some common element g.
- But then by (2), this means $aH = gH = bH$, so $aH = bH$. The other statement is immediate since any $g \in G$ is contained in the left coset gH.

Cosets, XI

4. For any $a, b \in G$, we have $aH = bH$ if and only if $a^{-1}b \in H$.

Proof:

- If $aH = bH$ then since $b \in aH$ this means $b = ah$ for some $h \in H$: then $a^{-1}b = a^{-1}ah = h \in H$.
- Conversely, if $a^{-1}b \in H$, then $b = ah$ for some $h \in H$, and so $b \in aH$. Then by (2), this means $bH = aH$.

The corresponding arguments for right cosets in place of left cosets are essentially identical, up to changing the orders of the multiplications appropriately.

Cosets, XII

These properties seem rather simple, but we can deduce a very important consequence from them:

Theorem (Lagrange's Theorem)

If H is a subgroup of G, then $\#G = \#G \cdot [G : H]$, where if one side is infinite then both are. In particular, if G is a finite group, then the order of any subgroup H divides the order of G.

Proof:

- By our properties of cosets, each left coset of H has a bijection with H, and so all of the left cosets have the same cardinality.
- Since the left cosets form a partition of G, we may partition the $\#G$ elements into a total of $[G : H]$ left cosets each of which has size $\#H$.
- Thus, $\#G = \#G \cdot [G : H]$. The second statement follows immediately from this relation, since $[G : H]$ is an integer.

Cosets, XIII

Although its proof is seemingly easy, Lagrange's theorem is an extremely important tool in unraveling the structure of groups (particularly, finite groups) since it substantially narrows the possible orders for subgroups of G, and also orders of elements:

Corollary (Orders of Elements)

If G is a finite group of order n, then for every $g \in G$ the order of g divides n, and $g^n = e$.

Proof:

- Let $H = \langle g \rangle$ be the cyclic subgroup generated by g.
- As we have shown, the order of H is equal to the order of g, and by Lagrange's theorem we see that it divides n.
- The second statement follows immediately.

Cosets, XIV

We can use Lagrange's theorem as a tool to classify groups of very small order:

Proposition (Groups of Order ≤ 7)

Suppose G is a group. Then the following hold:

1. *If G has prime order p, then G is cyclic and isomorphic to $\mathbb{Z}/p\mathbb{Z}$. In particular, any group of order 2, 3, 5, or 7 is cyclic.*
2. *If G has order 4, then G is abelian and isomorphic either to $\mathbb{Z}/4\mathbb{Z}$ or to $V_4 \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.*
3. *If G has order 6, then G is isomorphic either to $\mathbb{Z}/6\mathbb{Z}$ or to $S_3 \cong D_{2\cdot 3}$.*

Cosets, XV

1. If G has prime order p, then G is cyclic and isomorphic to $\mathbb{Z}/p\mathbb{Z}$. In particular, any group of order 2, 3, 5, or 7 is cyclic.

Proof:

- If G is a group of prime order p, consider any nonidentity element g.
- The order of g must divide p, and it cannot be 1 because g is not the identity.
- Thus, g has order p, and then $G = \langle g \rangle$ is cyclic.

Cosets, XVI

2. If G has order 4, then G is abelian and isomorphic either to $\mathbb{Z}/4\mathbb{Z}$ or to $V_4 \cong (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

Proof:

- If $\#G = 4$ then the order of any nonidentity element must be 2 or 4. If G has an element of order 4 then it is cyclic and thus isomorphic to $\mathbb{Z}/4\mathbb{Z}$.
- Otherwise, assume that every nonidentity element has order 2. Choose any such a and b and let $H = \langle a \rangle = \{e, a\}$.
- Then there are two left cosets of H, so since $b \notin H$, they must be H and bH. Likewise, there are two right cosets of H, namely H and Hb.
- But since left or right cosets partition G, this means $bH = Hb$.
- Thus, $ba = ab$ and also $G = \{e, a, b, ab\}$.
- Then the map $\varphi : (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \to G$ given by $\varphi(x, y) = a^x b^y$ is an isomorphism.

Cosets, XVI

3. If G has order 6, then G is isomorphic either to $\mathbb{Z}/6\mathbb{Z}$ or to $S_3 \cong D_{2\cdot 3}$.

Proof:

- If $\#G = 6$, then the order of any nonidentity element must be 2, 3, or 6. If G has an element of order 6 then it is cyclic and thus isomorphic to $\mathbb{Z}/6\mathbb{Z}$.
- Otherwise, assume every nonidentity element has order 2 or 3.
- By Cauchy's theorem, there exists $a \in G$ of order 3. Let $H = \{e, a, a^2\}$.
- Since $[G : H] = 2$ there is exactly one other left coset of H, say $bH = \{b, ba, ba^2\}$; these cosets are disjoint, so $b \notin H$.
- Since there is also exactly one other right coset of H, which must contain b since $b \notin H$, it is $Hb = \{b, ab, a^2b\}$.
- Since left or right cosets partition G, this means $bH = Hb$.

Cosets, XVII

Proof (continued):

- Then b^2H is also a left coset of H. It cannot equal bH since (by cancellation) this would imply $bH = H$, which is false.
- Therefore, $b^2H = H$, and so b^2 is one of e, a, a^2. If b^2 were equal to a then b would have to have order 3, but then we could write $b = b^4 = a^2$, which is impossible. Likewise, b^2 cannot equal a^2, so we must have $b^2 = e$, so b has order 2.
- Also, since $bH = Hb$, we deduce $ab \in Hb = \{b, ab, a^2b\}$, so since $ab \neq b$, we must have either $ab = ba$ or $ab = ba^2$. But if $ab = ba$, then since a has order 3 and b has order 2, ab would have order 6, contradicting our hypothesis.
- Thus, $ab = ba^2$, or equivalently, $ab = ba^{-1}$. Since $G = \langle a, b \rangle$ this means $G = \langle a, b : a^3 = b^2 = e, ab = ba^{-1} \rangle$ which is the same as the presentation for the dihedral group $D_{2\cdot 3}$.
- By our results on presentations, since G and $D_{2\cdot 3}$ both have order 6, we conclude that $G \cong D_{2\cdot 3} \cong S_3$ as claimed.

Subgroup Lattices, I

We can also use Lagrange's theorem to simplify calculations involving subgroups, toward an ultimate goal of writing down all the possible subgroups of a given group.

A convenient way to organize this information is by drawing the subgroup lattice of G: we arrange all of the subgroups of G starting with the smallest subgroups at the bottom, and then draw paths to indicate immediate containments.

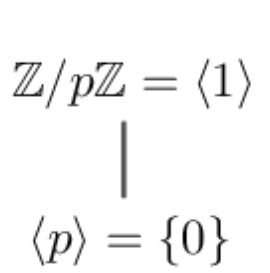
Subgroup Lattices, II

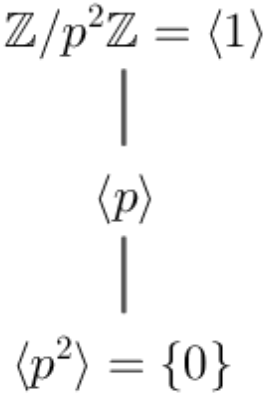
To compute an arbitrary subgroup lattice for a finite group, we may work as follows:

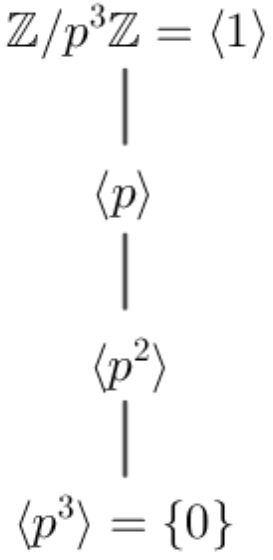
- First, write down all of the cyclic subgroups (i.e., subgroups generated by a single element).
- Next, write down all possible "joins" of two cyclic subgroups (i.e., the smallest subgroup containing both), which yield all of the subgroups generated by two elements.
- Continue the process by computing all possible joins of three cyclic subgroups (equivalently, joins of a 2-generator subgroup with a cyclic subgroup), and so on, until all subgroups have been obtained.

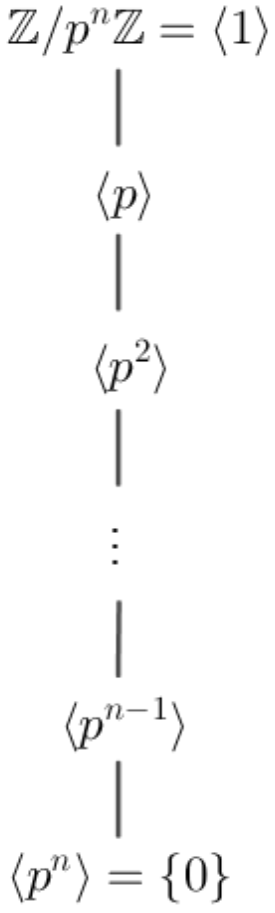
Subgroup Lattices, III

Here are the subgroup lattices of $\mathbb{Z}/p^n\mathbb{Z}$ for p a prime:



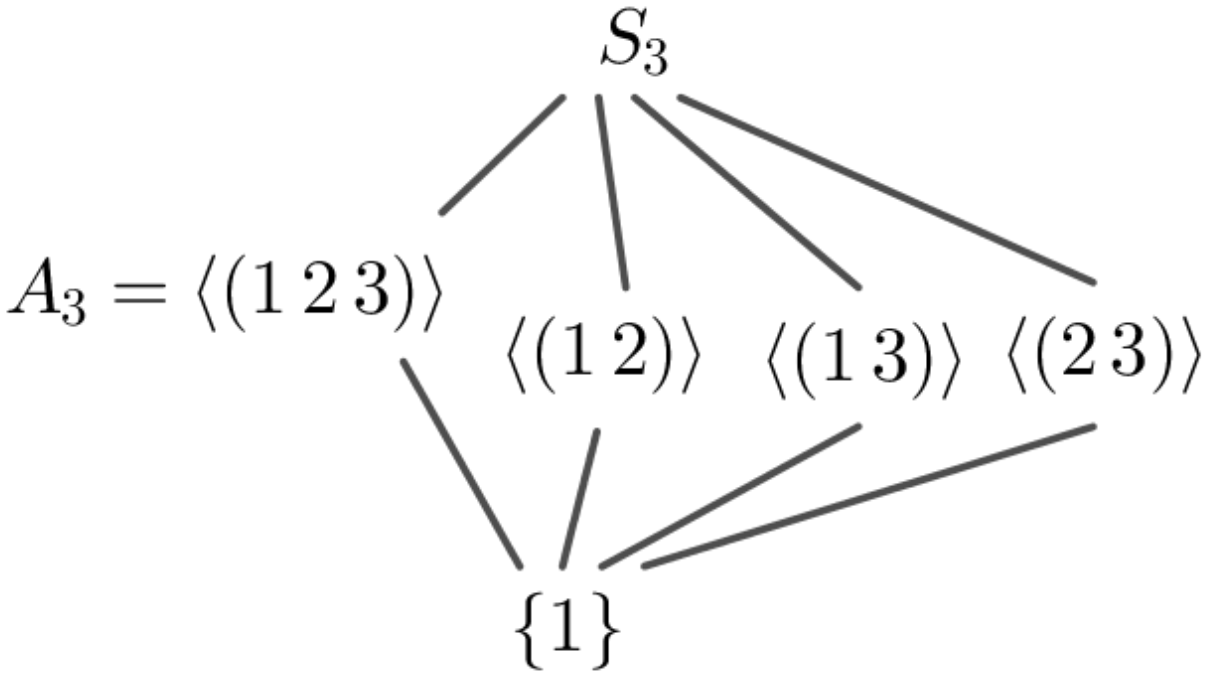






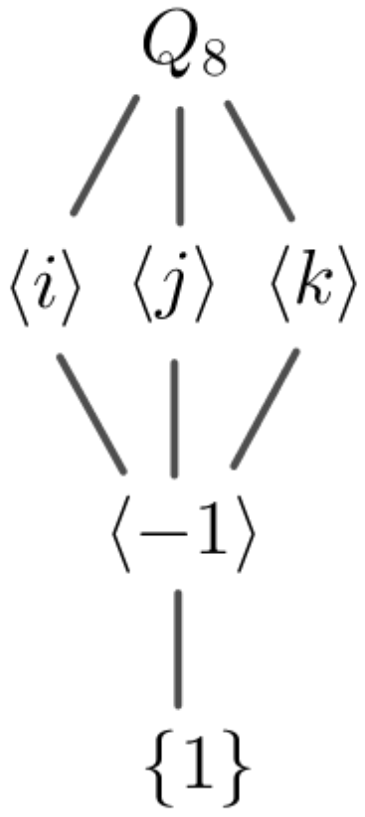
Subgroup Lattices, IV

Here is the subgroup lattice for S_3:



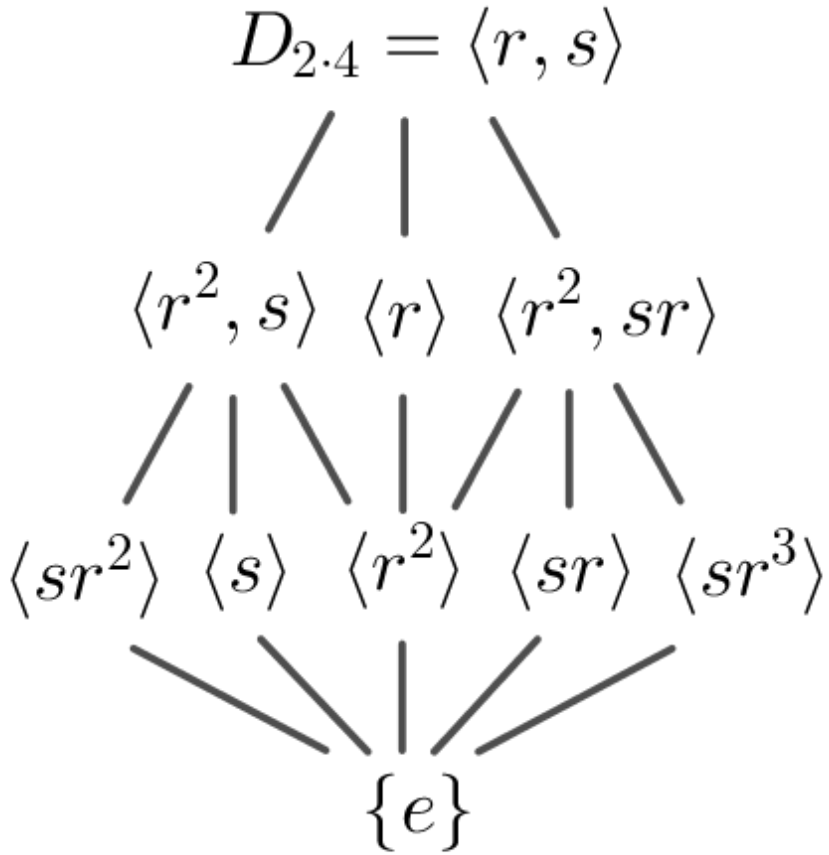
Subgroup Lattices, V

Here is the subgroup lattice for Q_8:



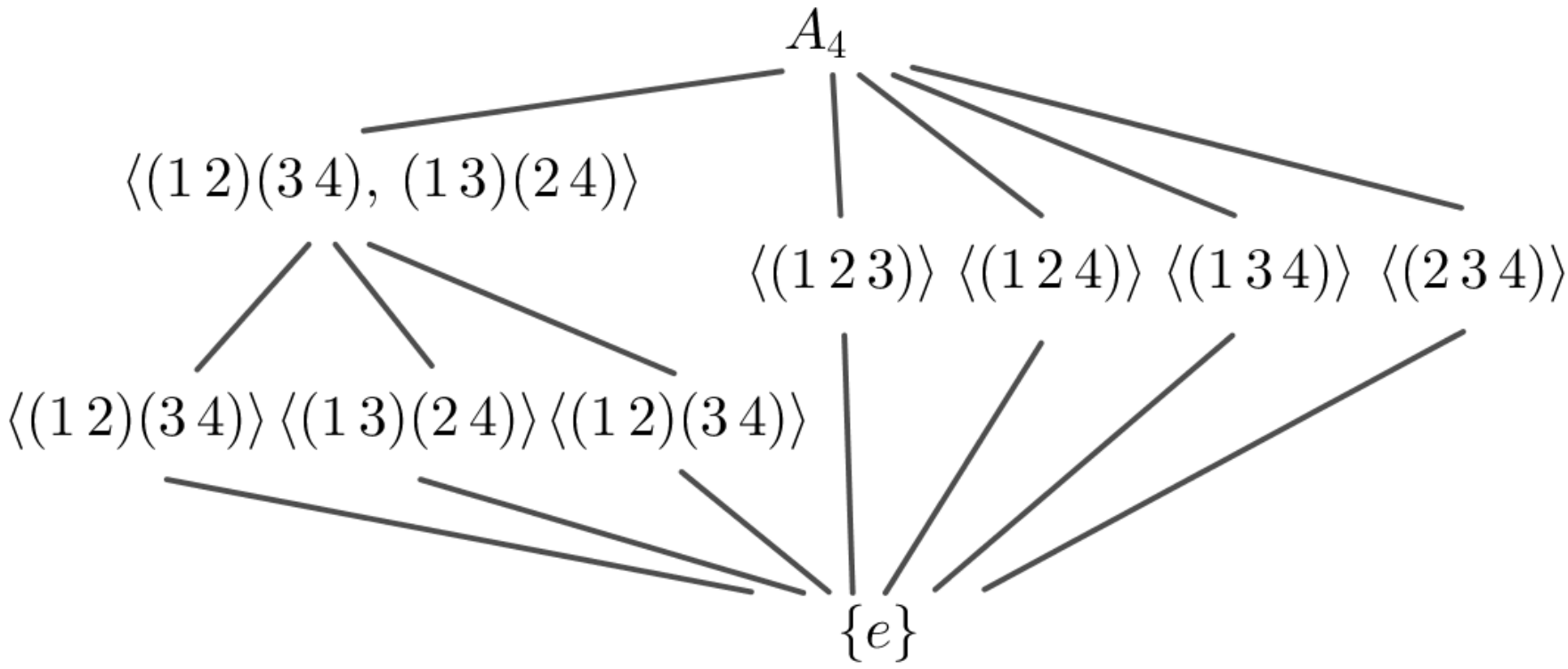
Subgroup Lattices, VI

Here is the subgroup lattice for $D_{2\cdot 4}$:



Subgroup Lattices, VII

Here is the subgroup lattice for A_4:



Notice here that A_4 has no subgroup of order 6.

Subgroup Lattices, VIII

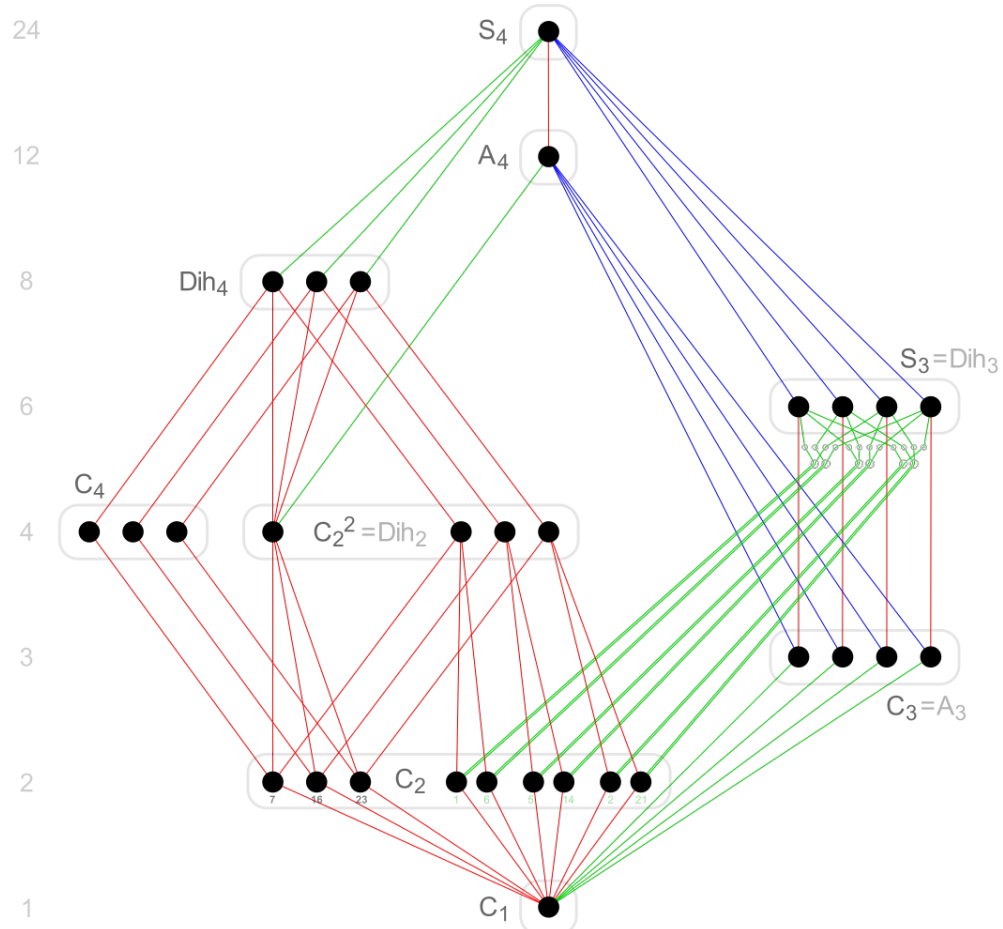
The observation on the previous slide gives a counterexample to the converse of Lagrange's theorem.

- To be more explicit: Lagrange's theorem tells us that if G is a finite group, then the only possible orders of a subgroup are divisors of n.
- The point of the example is that for any given divisor of n, there need not actually be a subgroup having that order.

We will discuss a partial converse to Lagrange's theorem (namely, Sylow's theorems) next week.

Subgroup Lattices, IX

Subgroup lattices are usually a bit more complicated:



[Diagram credit: Tilman Piesk, via wikimedia commons]

Normal Subgroups and Quotient Groups, I

We now continue with our discussion of quotient groups.

As we have already explained, in order to have well-defined operations on the collection of left cosets of H, we must impose an additional condition on H:

Definition

If K is a subgroup of G and $g \in G$, we define the conjugate of K by g gKg^{-1} as $gKg^{-1} = \{gkg^{-1} : k \in K\}$. We say $g \in G$ normalizes K if $gKg^{-1} = K$, and we N is a normal subgroup of G, written $N \trianglelefteq G$, if all $g \in G$ normalize N.

Every subgroup of an abelian group is normal, trivially.

Normal Subgroups and Quotient Groups, II

When G is non-abelian, it is tedious to try to verify that $gKg^{-1} = K$ for every $g \in G$.

- We can reduce the amount of calculation by observing that if $g, h \in G$ both normalize K, then $(gh)K(gh)^{-1} = g(hKh^{-1})g = gKg^{-1} = K$ so that gh also normalizes K, and also by multiplying by g^{-1} on the left and g on the right, $gKg^{-1} = K$ implies $K = g^{-1}Kg$ so that g^{-1} normalizes K.
- Thus, since the identity clearly normalizes K, we see that the collection of elements normalizing K is a subgroup of G. This subgroup is called the normalizer of K in G, and is denoted $N_G(K)$.
- Hence, to show K is normal, we need only verify that it is normalized by a set of generators for G.

Normal Subgroups and Quotient Groups, III

Examples:

1. If $H = \{e, r^2\}$ in $G = D_{2\cdot 4}$, then H is normal in G because $rHr^{-1} = \{e, r^2\} = H$ and $sHs^{-1} = \{e, sr^2s\} = \{e, r^2\} = H$.
2. If $H = \{e, s\}$ in $G = D_{2\cdot 4}$, then H is not normal in G because $rHr^{-1} = \{e, rsr^{-1}\} = \{e, sr^2\} \neq H$.
3. If $H = \{1, (1\,2\,3), (1\,3\,2)\}$ in $G = S_3$, then H is normal in G because $(1\,2\,3)H(1\,2\,3)^{-1} = H$ since H contains $(1\,2\,3)$, and also $(1\,2)H(1\,2)^{-1} = \{1, (1\,3\,2), (1\,2\,3)\} = H$.
4. If $H = \{1, (1\,3)\}$ in $G = S_3$, then H is not normal in G because $(1\,2)H(1\,2)^{-1} = \{1, (2\,3)\} \neq H$.
5. If $H = \{1, i, -1, -i\}$ in $G = Q_8$, then H is normal in G because $iHi^{-1} = H$ since $i \in H$, and also $jHj^{-}1 = \{1, -i, -1, i\} = H$ by explicit calculation.

Normal Subgroups and Quotient Groups, IV

Now we can construct quotient groups. When $N \trianglelefteq G$, we will also write the left coset aN as $\overline{a}$.

Theorem (Quotient Groups)

Let N be a normal subgroup of G.
Then the collection of left cosets of N in G forms a group (the quotient group of G by N, denoted G/N) under the operation $(aN) \cdot (bN) = (ab)N$, or, in residue class notation, $\overline{a} \cdot \overline{b} = \overline{ab}$.
In particular, the identity element is $\overline{e} = eN$ and inverses are given by $(gN)^{-1} = g^{-1}N$.
Furthermore, we have $\#(G/N) = [G : N]$, and also if G is abelian then so is G/N.

Normal Subgroups and Quotient Groups, V

Proof:

- First we must show that the operation is well-defined: that is, if we choose different elements $c \in aN$ and $d \in bN$, then the coset of cd is the same as that of ab.
- To see this, if $c \in aN$ then $c = an_1$ for some $n_1 \in N$, and similarly $d = bn_2$ for some $n_2 \in N$.
- Because $xN = yN$ if and only if $x^{-1}y \in N$, we see that $(ab)N = (cd)N$ is equivalent to $(ab)^{-1}(an_1bn_2) \in N$.
- We see that $(ab)^{-1}(an_1bn_2) = b^{-1}a^{-1}an_1bn_2 = (b^{-1}n_1b)n_2$, and then since $b^{-1}n_1b \in N$ because b^{-1} normalizes N, we conclude that $(ab)^{-1}(an_1bn_2) \in N$.
- Therefore, $(ab)N = (cd)N$, and so the operation is well-defined.

Normal Subgroups and Quotient Groups, VI

Proof (continued):

- The three group axioms [G1]-[G3] then follow from the corresponding properties in G.
- For [G1] we have $(\overline{a} \cdot \overline{b}) \cdot \overline{c} = \overline{ab} \cdot \overline{c} = \overline{(ab)c} = \overline{a(bc)} = \overline{a} \cdot \overline{bc} = \overline{a} \cdot (\overline{b} \cdot \overline{c})$.
- For [G2], the multiplicative identity is $\overline{e}$, since $\overline{a} \cdot \overline{e} = \overline{ae} = \overline{a} = \overline{ea} = \overline{e} \cdot \overline{a}$.
- For [G3], we have $\overline{a} \cdot \overline{a^{-1}} = \overline{aa^{-1}} = \overline{e} = \overline{a^{-1}a} = \overline{a^{-1}} \cdot \overline{a}$, so $\overline{a}^{-1} = \overline{a^{-1}}$.
- For the last statements, by definition $\#(G : N)$ is the number of left cosets of N in G, which is $[G : N]$. Finally, if G is abelian then $\overline{a} \cdot \overline{b} = \overline{ab} = \overline{ba} = \overline{b} \cdot \overline{a}$ so G/N is also abelian.

Normal Subgroups and Quotient Groups, VII

Here are some equivalent properties for normality:

Proposition (Normality Conditions)

If N is a subgroup of G, the following are equivalent:

1. *N is a normal subgroup of G: $gNg^{-1} = N$ for all $g \in G$.*
2. *The collection of left cosets of G forms a group under the operation $(aN)(bN) = abN$.*
3. *$gNg^{-1} \subseteq N$ for every $g \in G$.*
4. *$gN = Ng$ for every $g \in G$.*
5. *Every left coset of G is also a right coset of G, and vice versa.*

Condition (3) is usually the easiest to check, and to show (3) it is only necessary to verify that $g_i n_j g_i^{-1} \in N$ for a set of generators g_i of G and a set of generators n_j of N.

Normal Subgroups and Quotient Groups, VIII

Proof:

- In our motivation for the definition of normality, we showed that (2) implies (1) and that (3) implies (1).
- Our theorem on quotient groups shows (1) implies (2), and (1) clearly implies (3). So (1), (2), (3) are equivalent.
- (3) $\implies$ (4): If $gN = Ng$ then for any $n \in N$ there exists $n' \in N$ with $gn = n'g$. Thus $gng^{-1} = n' \in N$ for every $g \in G$ and $n \in N$, which is (3).
- (4) $\implies$ (1): If $gNg^{-1} = N$, multiplying every element in both sets on the right by g shows $gN = Ng$, which gives (4).
- (4) $\implies$ (5): If $gN = Ng$ for all $g \in G$, then every left coset is a right coset, so (4) implies (5).
- (5) $\implies$ (4): If every left coset is a right coset, then since gN is the unique left coset containing g and Ng is the unique right coset containing g, we must have $gN = Ng$ for every g, giving (4).

Normal Subgroups and Quotient Groups, IX

Example: For $G = S_3$ and $N = \langle (1\,2\,3) \rangle$, identify the elements of G/N and determine the structure of G/N.

Normal Subgroups and Quotient Groups, IX

Example: For $G = S_3$ and $N = \langle (1\,2\,3) \rangle$, identify the elements of G/N and determine the structure of G/N.

- Since $[G : N] = |G| / |N| = 2$ there are 2 left cosets of G, so G/N is a group of order 2. Thus G/N will be isomorphic to $\mathbb{Z}/2\mathbb{Z}$.
- We can compute the elements of G/N explicitly as $1N = \{1, (1\,2\,3), (1\,3\,2)\}$ and $(1\,2)N = \{(1\,2), (2\,3), (1\,3)\}$.
- By the definition of the quotient group structure, we can then compute $[1N][1N] = 1$, $[1N][(1\,2)N] = (1\,2)N = [(1\,2)N][1N]$, and $[(1\,2)N][(1\,2)N] = (1\,2)^2 N = 1N$.
- Indeed, the structure of G/N is precisely that of $\mathbb{Z}/2\mathbb{Z}$.

Normal Subgroups and Quotient Groups, X

Example: For $G = Q_8$ and $N = \langle -1 \rangle$, identify the elements of G/N and determine the structure of G/N.

Normal Subgroups and Quotient Groups, X

Example: For $G = Q_8$ and $N = \langle -1 \rangle$, identify the elements of G/N and determine the structure of G/N.

- Since $[G : N] = |G| / |N| = 4$ there are 4 left cosets of G, so G/N is a group of order 4.
- The elements of G/N are $1N = \{1, -1\}$, $iN = \{i, -i\}$, $jN = \{j, -j\}$, and $kN = \{k, -k\}$. The identity element is $1N$.
- By the definition of the quotient group structure, we can then compute, for example, $(iN)(jN) = ijN = kN$, and $(jN)(iN) = jiN = -kN = kN$.
- Also, we have $(iN)^2 = i^2N = -1N = 1N$, and likewise $(jN)^2 = 1N$ and $(kN)^2 = 1N$, so each nonidentity element of the group has order 2.
- From our characterization of the groups of order 4, this tells us that G/N is isomorphic to the Klein 4-group V_4.

Normal Subgroups and Quotient Groups, XI

Example: For $G = \mathbb{Z}/12\mathbb{Z}$ and $N = \langle 6 \rangle$, identify the elements of G/N and determine the structure of G/N.

Normal Subgroups and Quotient Groups, XI

Example: For $G = \mathbb{Z}/12\mathbb{Z}$ and $N = \langle 6 \rangle$, identify the elements of G/N and determine the structure of G/N.

- Since $[G : N] = |G| / |N| = 6$ there are 6 left cosets of G, so G/N is a group of order 6.
- The elements of G/N are $0 + N = \{0, 6\}$, $1 + N = \{1, 7\}$, $2 + N = \{2, 8\}$, $3 + N = \{3, 9\}$, $4 + N = \{4, 10\}$, and $5 + N = \{5, 11\}$.
- We can see that $k(1 + N) = k + N$ for any integer k, and so G/N is a cyclic group (of order 6) generated by $1 + N$.
- Remark: More generally, if $G = \langle g \rangle$ is cyclic and generated by the element g, it is not hard to see that G/N is cyclic and generated by $\overline{g} = gN$.

Normal Subgroups and Quotient Groups, XII

Example: For $G = D_{2 \cdot 6}$ and $N = \langle r^3 \rangle$, identify the elements of G/N and determine the structure of G/N.

Normal Subgroups and Quotient Groups, XII

Example: For $G = D_{2\cdot 6}$ and $N = \langle r^3 \rangle$, identify the elements of G/N and determine the structure of G/N.

- Since $[G : N] = |G| / |N| = 6$ there are 6 left cosets of G, so G/N is a group of order 6.
- The elements of G/N are $eN = \{e, r^3\}$, $rN = \{r, r^4\}$, $r^2N = \{r^2, r^5\}$, $sN = \{s, sr^3\}$, $srN = \{sr, sr^4\}$, and $sr^2N = \{sr, sr^2\}$.
- Note that $(rN)^3 = r^3N = eN$ and $(r^2N)^3 = r^6N = eN$ so both rN and r^2N have order 3. In a similar way we can see that sN, srN, and sr^2N each have order 2.
- From our characterization of the groups of order 6, this tells us that G/N is isomorphic to $D_{2\cdot 3} \cong S_3$. (In fact, an explicit isomorphism with $D_{2\cdot 3}$ can be obtained simply by reading off the corresponding label from the cosets as labeled above!)

Normal Subgroups and Quotient Groups, XIII

One of the primary reasons that quotient groups are of interest is that it is often possible to "piece together" information about N and G/N to yield information about G.

- For example, we will use an argument of this type later to prove that if p is prime, then every group of order p^2 is abelian, and isomorphic to one of $\mathbb{Z}/p^2\mathbb{Z}$ or $(\mathbb{Z}/p\mathbb{Z}) \times (\mathbb{Z}/p\mathbb{Z})$.

Normal Subgroups and Quotient Groups, XIV

However, even if the isomorphism types of N and G/N are known, then this information does not uniquely determine the structure of G.

- For example, we have seen that both Q_8 and $D_{2\cdot 4}$ have normal subgroups N of order 2 (isomorphic to $\mathbb{Z}/2\mathbb{Z}$), such that the quotient group by N is isomorphic to the Klein 4-group; nonetheless, Q_8 and $D_{2\cdot 4}$ are not isomorphic.
- In general, the problem of describing all groups G having a normal subgroup N isomorphic to a specific group A and with G/N isomorphic to another specific group B is called the extension problem for groups.

Normal Subgroups and Quotient Groups, XV

Of course, when G is large it can be difficult to understand the structure of G/N in a useful way. We mention two interesting examples, however:

1. Every element of the quotient group $\mathbb{Q}/\mathbb{Z}$ has finite order, although element orders in this group can be arbitrarily large. Explicitly, if p/q is in lowest terms then the coset $\overline{p/q}$ has order q, since $q \cdot \overline{p/q} = \overline{p} = \overline{0}$ but no smaller multiple of p/q will yield an integer.
2. If p is a prime and G is the group of p-power roots of unity in $\mathbb{C}$ (i.e., the union of the p^nth roots of unity for all $n \geq 1$) and N represents the group of pth roots of unity, then G/N is isomorphic to G itself. Explicitly, one may verify that the map given by $\varphi(\zeta N) = \zeta^p$ is well-defined and yields an isomorphism of G/N with G.

Normal Subgroups and Quotient Groups, XVI

A common proof technique for establishing structural results about finite groups is to use induction on $|G|$, and piece information together from normal subgroups and quotient groups.

A major obstruction to this type of argument occurs if G possesses no nontrivial proper normal subgroups:

Definition

A group G is simple if $|G| > 1$ and the only normal subgroups of G are $\{e\}$ and G.

- The cyclic groups $\mathbb{Z}/p\mathbb{Z}$ for p prime are simple, and in fact it is not hard to see that they are the only abelian simple groups.
- Another family of simple groups is given by the alternating groups A_n for $n \geq 5$. (This is not as easy to prove!)

Normal Subgroups and Quotient Groups, XVII

A major goal of finite group theory is to classify the finite simple groups, since they provide a partial analogue to the prime numbers in that they are the "building blocks" for the construction of groups from smaller groups.

- The classification of finite simple groups was completed (up to some minor components) in the 1980s, and established that there are 18 infinite families of finite simple groups, along with 26 "sporadic" simple groups not belonging to any of these families, such that every finite simple group is isomorphic to one of these listed groups.
- In total, the classification is estimated to run over 10000 pages, spanning several hundred papers by dozens of individual authors.

Summary

We introduced cosets and established some of their properties.

We proved Lagrange's theorem and deduced some of its consequences.

We discussed subgroup lattices.

We discussed normal subgroups and quotient groups.

Next lecture: The isomorphism theorems, group actions.