MTH320 - Abstract Algebra I

by Dara Varam

August 31st, 2020

Semi-Groups:

A semi-group is a set that upholds the following two coniditions:

$$(D,\cdot) \quad \text{where } D \text{ is a set and } \cdot \text{ is the binary operator acting on the set}$$

1. $\forall a,b \in D$ we have that $a \cdot b \in D$ (Closure)
2. $\forall a,b,c \in D, (a\cdot b)\cdot c = a\cdot(b\cdot c)$ (Associative)

What are some examples of Semi-Groups?

$$\text{Consider } (D,\cdot), \text{ where } D = \mathbb{Z} \quad \text{and } \cdot \text{ is the normal binary addition.}$$

This is a semi-group because it satisfies the closure condition (i.e. $\forall a, b \in \mathbb{Z}$, we have $a+b \in \mathbb{Z}$). Further, we have the associative condition satisfied trivially as well.

What is not a Semi-group?

$$\text{Consider } (D,\cdot) \text{ where } D \text{ is the set of odd numbers, and } \cdot \text{ is the normal binary addition.}$$

This set is not a semi-group because of the fact that if we take two odd integers, $a, b \in D$, their addition will result in an even number, which is not part of the set (Fails the closure condition).

Monoids:

$(D,\cdot)$ is a monoid if the following two conditions are satisfied:

1. $(D,\cdot)$ is a semi-group
2. $\exists e \in D$ st $e\cdot d = d\cdot e = d \quad \forall d \in D$ (Identity)

This identity can be the following under the normal circumstances we are used to, such as 1 for the set of integers under multiplication, and 0 for the set of integers under addition.

Examples of monoids: $(\mathbb{Z},+)$ is a monoid because it is a semi-group and the identity exists.

Consider $(\mathbb{Z}^+,+)$. This is not a monoid because the identity is 0 and 0 is not part of $\mathbb{Z}^+$. Similarly, if we consider $(D,+)$ where $D =$ set of even numbers, this is also not a monoid because of the simple fact that the identity, 1, is not an even number.

Groups:

$(D,\cdot)$ is a group if the following conditions are met:

1. $(D,\cdot)$ is a monoid, i.e. is also a semi-group with an identity element;
2. $\forall a \in D, \exists a^{-1} \in D$ st $a\cdot a^{-1} = e$ (Inverse)

Simple example of a group: $(\mathbb{Z}, +)$. The inverse of every element is the negation of that element. For example, if we consider the number 3, we know that the inverse is -3, since $3 + (-3)$ gives us 0, which is the identity.

On the other hand, $(\mathbb{Q}, \cdot)$ is not a group, because of the fact that the 0 in the set of rational numbers is troublesome. Every number multiplied by 0 will result in 0, so we don't satisfy the identity condition. In fact, the set $(\mathbb{Q}, \cdot)$ is only a semi-group, not even a monoid. However, if we consider the set $(\mathbb{Q}^*, \cdot)$, where $D = \mathbb{Q}$ excluding 0, then this will be a group.

Is $(\mathbb{Z}^*, \cdot)$ a group?

No. This is because of the fact that the inverse of any number under multiplication is $1/n$, and fractions are not part of the set of integers. In fact, this set is a semi-group and a monoid, but because of the lack of the inverse relationship, it cannot be a group.

Integers modulo n (Not covered until way later in the course)

Consider the notation: $(\mathbb{Z}_n, \cdot)$, where $\mathbb{Z}_n = \{0, 1, 2, \ldots n-1\}$. This is the notion of the set of integers modulo n.

Let us take a closer look at an example. Consider $(\mathbb{Z}_4, +)$ as our set.

+	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

Table 1.

As we can see from our table, the additions taken place are not those which we are used to, because we need to add w.r.t. mod n, which is 4 in our case.

Is $(\mathbb{Z}_4, +)$ a group? Yes. It is a monoid and every element has an inverse, though it may be hard to see. The inverse of 1, for example, is 3, because $1+3=4=0 \text{mod} 4$.

In fact, $(\mathbb{Z}_n, +)$ is a group for all n.

$$\text{if } a \in \mathbb{Z}_n, a^{-1} = n - a$$

$$a + n - a = n, \text{and } n \text{ modn} = 0, \text{which is the identity}, e.$$

What about for $(\mathbb{Z}_n, \times)$, where $\times$ is the normal multiplication under mod n. Consider the table for $\mathbb{Z}_5$:

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	3	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Table 2.

This is obviously not a group because of the threat the 0 poses. However, if we consider $(\mathbb{Z}_5^*, \cdot)$, where the $*$ indicates the removal of the 0, then this is a group. Some of the inverses are as follows:

$2^{-1} = 3$ since $2 \cdot 3 = 6 = 1 \text{ mod} 5$, and 1 is the identity for multiplication.

$4^{-1} = 4$ since $4 \cdot 4 = 16 = 1 \bmod 5$, etc.

September 2nd, 2020

Abelian Groups:

A group $(D, \cdot)$ is called Abelian:

$$\text{iff} \forall a, b \in D, a \cdot b = b \cdot a \qquad \text{(Commutative)}$$

Whenever you hear "Abelian group," know that it is commutative. We usually say commutative for rings though. Therefore, a group is considered Abelian if the elements commute.

Example: $(\mathbb{Z}_{10}, +) \rightarrow$ Abelian group because $\forall a, b \in \mathbb{Z}_{10}, a + b = b + a$. Remeber that $(\mathbb{Z}_n, +)$ is always a group.

Now consider $(\mathbb{Z}_6^*, \times)$. This is not a group. Which axiom fails in this case? Let's go through it. Summary of Group: Closure, associative, identity, inverse. Since we are considering $\mathbb{Z}_6^*$, we proceed by providing a counterexample:

$$\begin{aligned} &\text{Consider } (2 \times_6 3) = 0 \bmod 6, 0 \notin \mathbb{Z}_6^* \\ &\text{Since } 0 \notin \mathbb{Z}_6^*, \text{we have found the product} \\ &\text{of two elements in } \mathbb{Z}_6^* \text{that result in} \\ &\text{some value OUTSIDE of } \mathbb{Z}_6{}^* \end{aligned}$$

Therefore by counterexample, $(\mathbb{Z}_6^*, \times)$ is not a group.

Therefore, this set fails the closure axiom and cannot be a semi-group, monoid or group. Note that if a single axiom fails then we do not have to continue. There is, however, another reason why $(\mathbb{Z}_6^*, \times)$ is not a group. Conisder $(2 \cdot x) \bmod 6 = e = 1$. This element does not exist, and so the inverse axiom has also failed for the set.

Fact: $(\mathbb{Z}_n^*, \times)$ is a group iff n is prime. We cannot afford to forget this result. Remember this fact.

$(\mathbb{Z}_5^*, \times)$ is a group because 5 is a prime number. but $(\mathbb{Z}_{15}^*, \times)$ is not a group because 15 is not a prime number $(15 = 3 \cdot 5)$, and this set would fail the closure axiom because $(3 \cdot 5) \bmod 15 = 0$ and 0 is not part of $\mathbb{Z}_{15}^*$.

$(\mathbb{Z}_n^*, \times)$, where n is assumed to be prime, is an Abelian group.

What are some examples of non-Abelian groups? We will get to this later on, but we will now consider a group studied in Linear Algebra.

Consider: $(\mathbb{Z}, -)$. Check for closure, associative, identity, inverse.

Remember that e is an identity if $e \cdot a = a \cdot e = a$. Now let's consider it for this set. The trivial identity asssumed is $e = 0$.

However, let's take $a = 4 \in \mathbb{Z}$. $4 - 0 \neq 0 - 4$. So this axiom clearly fails. Therefore, this set is a group but not an Abelian group.

Food for thought: In real life, we only have addition and multiplication. Everything else is either an extension or an inverse of these two operations. For example, in $(\mathbb{Z}, +)$, which is a group, the number 5 has an inverse, -5. This is the additive inverse. Then we can see that, for example, $5 - 3 = 5 + (-3)$. This is the correct way to consider numbers in $\mathbb{Z}$. Furthermore, division should be more clearly viewed as: $\frac{3}{5} = 5 \times \frac{1}{3}$, etc.

This shows us that division and subtraction is non-Abelian.

Let's take $(D = \{A \in \mathbb{R}^{2\times 2} \mid \det(A) \neq 0\}, \times)$. This means that D is under matrix multiplication. This will be a group, but this will NOT be Abelian. Multiplication between matrices is not always commutative, as we have learned in Linear Algebra. In "Street Language," D is the set of all 2×2 invertible matrices (since $\det(A) \neq 0$), and the binary operation is the matrix multiplication.

i. Closure: The matrix multiplication of two 2×2 matrices is another 2×2 matrix

ii. Inverse: The matrices are assumed to be invertible because $\det(A) \neq 0$.

iii. Identity: The identity matrix for $\mathbb{R}^{2\times 2}$ is I_2, or

$$\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$$

iv. Associativity is clear. $\forall A, B, C \in D, (A \times B) \times C = A \times (B \times C) \in D$

The commutivity, however, fails because for $A, B \in D, A \times B \neq B \times A$. Therefore, this group is clearly not Abelian.

As a matter of fact, all invertible matrices of size $n \times n$ are groups, but they are not Abelian. This is the best example of non-Abelian groups.

Uniqueness of Identity:

Let $(D, \cdot)$ be a group. Then D has exactly one identity, e. i.e. For any group, $(D, \cdot)$, the identity is *unique*. Let's try to prove this:

Proof by contradiction: Assume $f, e \in D$, both are identities. We must show that $e = f$. Since e is an identity of D, then $e \cdot f = f$. Since f is also an identity of D, then $f \cdot e = e$. i.e.:

$$\begin{pmatrix} e \cdot f = e \\ e \cdot f = f \end{pmatrix}$$

This is clearly a contradiction unless $e = f$. Therefore, we can establish that the identity of a group is *unique*.

Uniqueness of the Inverse:

If $(D, \cdot)$ is a group, then for every $a \in D, a^{-1}$ is unique. This means that each element of D has one and only one inverse. Let's prove this.

Proof by contradiction: Assume we have an element, $a \in D$, that has two inverses, b and w. We now work to show that $b = w$ for a^{-1} to be unique.

Hence: $a \cdot b = e$ and $a \cdot w = e$. We also know that e is unique based on the previous proof.

$$\begin{aligned} a \cdot b = e = a \cdot w \Longrightarrow a \cdot b &= a \cdot w \\ a \cdot b \cdot b &= a \cdot b \cdot w \\ (a \cdot b) \cdot b &= (a \cdot b) \cdot w \\ e \cdot b &= e \cdot w \\ \text{Therefore } b &= w \end{aligned}$$

Fact: For a group, $(D,\times), a\cdot b = a\cdot c \Longrightarrow b = c$. We know that the identity for a group is unique, and the inverse is unique. Even if we have: $b\cdot a = c\cdot a \Longrightarrow b = c$ (Works from both sides). This is the cancellation.

Consider $(\mathbb{Z}_6,\times)$. Let's take $2\times 2 = 4 = 4\text{mod}6$ and $2\times 5 = 10 = 4\text{mod}6$. We can't cancel, because that would imply $2\times 2 = 2\times 5$. Cancellation is invalid.

What is the order of an element?

Assume $(D,\cdot)$ is a group. Take $a\in D$, $|a| = \text{ord}(a)$, order of a.

$\text{ord}(a) = \underline{\text{Smallest positive integer}}, n, s.t. \quad a\cdot a\cdot a\cdot a_{....}\cdot a \quad (n\,\text{times})$ gives you e. i.e. $a^n = e$. If such n does not exist, then $\text{ord}(a) = \infty$. We cannot find a positive integer, n, s.t. $a^n = e$.

Let's take $(\mathbb{Z}_6,+)$. We know that is an Abelian group. Consider 3^4. This is $(3+3+3+3)\text{mod}6$. Clearly, the exponent here is different to that we know in $\mathbb{Z}$.

Similarly, for $(\mathbb{Z}_{11}^*,\times)$, which is again, an Abelian group, $3^4 = (3\times 3\times 3\times 3)\text{mod}11$.

Let's return to $(\mathbb{Z}_6,+)$. What is $\text{ord}(1) = |1|$? We want $1^n = 0$, i.e. the smallest possible n to give us the identity, 0.

$$1+1+1+1+1+1 = 6\,\text{mod}6 = 0 = e$$

So, $|1| = 6$.

What about ord(0)? i.e. $0^n = 0$, but $0 = 0$, so the order of 0 is 1. i.e. $\text{ord}(0) = |0| = 1$.

In general, $|e| = 1\,\text{for all}\,e$. In words, this means that the order of the identity of the group is always 1.

What is $|2|$? We take the same idea to get $2^n = 0$

$$2+2+2 = 6 = \text{mod}6 = 0, \text{so}\,\text{ord}(2) = n = 3$$

Similarly, $\text{ord}(4) = 3$ because $4+4+4 = 12 = 0\text{mod}6$. This same idea follows through for all integers under $\mathbb{Z}_6$.

Now, for ord(5), we have $5+5+5+5+5+5 = 30 = 0\text{mod}6$, so $|5| = 6$. It should make sense now for all binary operations or elements in a set.

Notation:

Assume $(D,\cdot)$ is a group.

i. $a^m\cdot a^n = a^{m+n}$ (where $m,n\in\mathbb{Z}$)

ii. $a^{-n} = (a^{-1})^n$ ($n\in\mathbb{Z}^+$)

iii. $(a^n)^m = (a)^{nm}$

We can still use these properties. Let's take a few examples to solidify this;

For $(\mathbb{Z}_{10}, +)$,

$$2^5 + 2^6 = 2^{11}$$

This statement is true for all elements of $\mathbb{Z}_{10}$, under $+$.

In fact, that statement is true for any group of the form $(\mathbb{Z}_n, +)$, or even $(\mathbb{Z}, +)$ itself. Remember to always think of what planet you're in.

Now consider $(\mathbb{Z}_{10}, +)$, and 2^{-3}. This means $(2^{-1})^3$.

$$(2^{-1}) = 8, \text{since } 2 + 8 = 0 \text{mod} 10$$
$$\text{Hence we have: } 8 + 8 + 8 = 24 = 4 \text{mod} 10$$

September 7th, 2020

Order of elements in groups:

To recall, by definition, the order of an element in a group is the smallest positive integer, n, where $a^n = e$ (identity).

Result: Assume $(D, \cdot)$ is a group and $a \in D$ s.t. $\text{ord}(a) = |a| = n < \infty$ (We are assuming the order of a is finite).

$$\text{if } a^m = e \quad \text{for some } m \in \mathbb{Z}^+$$

Then: $n|m$ (i.e. n is a factor of m). In other words, m is divisible by n. How do we prove a result like this?

Proof: We can write any number as $m = kn + r$, $k \geqslant 0$ and $0 \leqslant r < n$. We need to show that n is a factor of m. To do this, remainder (r) is 0. If we show that $r = 0$, then we are done with the proof.

Hypothesis: Since $a^m = e$, we have $a^{kn+r} = e = a^{kn} \cdot a^r$ (See previous lecture notes for this fact). Now we now that $a^n = e$ (since $n = |a|$). Then we can see that: $(a^n)^k \cdot a^r = e$.

$$\begin{aligned} &\text{Since } a^n = e, \\ \text{we have:} \quad &(e)^k \cdot a^r = e \\ &e^k = e \quad \forall k \geqslant 0 \\ \text{so:} \quad &e \cdot (a^r) = e \\ &\text{therefore:} \\ &a^r = e \end{aligned}$$

We know that since $0 \leqslant r < n$ and $|a| = n$, $r \neq n$. But there has to be another value for r where if we take a^r, we get the identity. Note that: $a^0 = e \quad \forall a \in D$. Therefore, we conclude that $r = 0$.

Hence $m = kn$, i.e. the remainder, r is 0 and we have shown that $n|m$.

The more results and facts you know in Abstract Algebra, then the easier the course is going to be for you. This is why you need to remember all these facts mentioned in the notes.

Result: Last time we proved that each group has one identity and the inverse is unique. This is an extension on that.

Assume $(D,\cdot)$ is a group. Let $a \in D$. Then $|a| = |a^{-1}|$. i.e. a and its inverse have the same order. Let's first take examples to demonstrate.

Consider $(\mathbb{Z}_6,+)$. $1^{-1} = 5$ (By simple observation). Now we can see that $|1| = |5|$.

$$|1| \text{ for } (\mathbb{Z}_6,+):$$

$$(1+1+1+1+1+1)\text{mod}6 = 6\,\text{mod}6 = 0, \text{therefore } |1| = 6$$

$$|5| \text{ for } (\mathbb{Z}_6,+):$$

$$(5+5+5+5+5+5)\text{mod}6 = 30\,\text{mod}6 = 0, \text{therefore } |5| = 6$$

Proof: We have two cases. The first of which is if the order of a is infinite. The second is if the order is finite. We will show for both cases.

First case: $|a| = \infty$ (i.e. $a^n \neq e \quad \forall n \in \mathbb{Z}^+$) We now show that $|a^{-1}| = \infty$.

We will do this by contradiction. Assume $|a^{-1}| = m < \infty$. Thus: $(a^{-m}) = (a^{-1})^m = e$. Now we can proceed by the following:

$$\begin{aligned} \text{Notice that } (a^{-m}) = (a^{-1})^m = e \quad & \text{By assumption} \\ a^m \cdot (a^{-1})^m &= a^m \cdot e \\ (a \cdot a^{-1})^m &= a^m \cdot e = a^m \\ (e)^m &= a^m \end{aligned}$$

This is a contradiction since $|a| = \infty$, but the proof shows that $|a|$ is finite. Therefore $|a| = |a^{-1}|$.

Now, assume $|a| = m < \infty$. Show that $|a^{-1}| = m$. Let $k = |a^{-1}|$. We need to show that $k = m$.

$$\begin{aligned} (a \cdot a^{-1})^k = a^k \cdot (a^{-1})^k = a^k \cdot e = a^k \\ \text{But} \quad (a \cdot a^{-1})^k = e^k = e \\ \text{Therefore} \quad e = a^k \end{aligned}$$

So we can conclude that (By result 1) that $m|k$. If m is a factor of k,

$$\begin{aligned} e = (a \cdot a^{-1})^m = a^m \cdot (a^{-1})^m = e \cdot (a^{-1})^m \\ e = (a^{-1})^m \Longrightarrow k|m \end{aligned}$$

So we can establish that $m = k$ since both are factors of each other. Therefore, we can see that for any group, $(D,\cdot)$ where $a \in D$, $|a| = |a^{-1}|$.

Greatest Common Divisor:

$$\gcd(m,n)$$

Result: Assume we have a group $(D,\cdot), a \in D$ st $|a| = m < \infty$. If we know $|a| = m$, can we conlcude anything on higher powers of a?

$$|a^k| = \frac{m}{\gcd(k,m)} \quad \forall k \in \mathbb{Z}$$

The proof for this is a little technical and we will not cover it in the notes. However, we will consider the following question. How do we use this result?

Given $a \in D$ and $|a| = 12$, we can calculate any $|a^k|$. For example,

$$|a^5| = \frac{12}{\gcd(5,12)} = \frac{12}{1} = 12$$
$$|a^8| = \frac{12}{\gcd(8,12)} = \frac{12}{4} = 3$$
$$|a^9| = \frac{12}{\gcd(9,12)} = \frac{12}{3} = 4$$

What about: $|a^{-4}|$?

We know (By result 2) that $|a^{-1}| = 12$

Then: $|(a^{-1})^4| = \frac{12}{\gcd(4,12)} = \frac{12}{4} = 3$

$$|a^{-10}| = \frac{12}{\gcd(10,12)} = 6$$

We can safely conclude that given $|a|$, $|a^k| = |a^{-k}|$. This is another useful result we can use.

Subgroups:

Let $(D, \cdot)$ be a group and $H \subseteq D$. We say H is a subgroup of D if $(H, \cdot)$ (Same binary operation) is also a group. This is like in linear algebra. This is very similar to a subspace. A group is like a vector space.

For example, every vector space under addition is a group.

Keep in mind that a subgroup is still a group. The only difference is that this group lives inside a bigger group. However, do keep in mind the importance of following through with the same binary operation.

Consider $(\mathbb{Z}, +)$. This is a group. However, let's take $H \subseteq \mathbb{Z}$ where H is the set of all odd integers. This subset is not a group under the binary operation $+$. So not every subset of another set is also a subgroup.

Result: Group $(D, \cdot)$. Assume $H \subseteq D$, H is a finite subset of D. D can be any group, but H MUST be a finite subset of D.

Then: $H < D$. This notation means that H is a subgroup of D. $H < D$ iff $(H, \cdot)$ is closed. i.e. the subset has closure. We only need to check closure out of the 4 axioms, because the other three (identity, inverse, associative) are automatically correct because of D.

Proof: Assume $(H, \cdot)$ is a subgroup of D. Hence $(H, \cdot)$ is closed. This is iff relation, so the first direction is given. We need to prove the second direction.

Assume $(H, \cdot)$ is closed. We show that $H < D$ (i.e. H is a subgroup of D). We simply need to show that H is a group since it is already a subset of D.

1. $(H, \cdot)$ is closed by our hypothesis;
2. $(H, \cdot)$ is associative, and $(D, \cdot)$ is associative because it is a group;
3. We want to show for $(H, \cdot)$ that $e \in H$ and $a^{-1} \in H \quad \forall a \in H$. We do this in one step. Let us show this.

Choose $a \in H$. Start forming $a, a^2, a^3, \ldots a^n$. All of these are in H because H satisfies the closure axiom. We cannot keep this going forever because H is a finite set. At some point, you will repeat some elements.

$$a^m = a^k \quad \text{for some } m > k$$

At some point we have $a^m = a^k$ for some value of m and k. We can assume that $m > k$.

We can see that a^k has an inverse. To proceed, we do the following:

$$\begin{aligned} a^{-k} \cdot a^m = a^{-k} \cdot a^k = e \quad & \text{Binary operation } a^{-k} \text{ on both sides} \\ a^{m-k} = a^{-k} \cdot a^k & \\ a^{m-k} = e & \end{aligned}$$

Since $m > k$, by closure we can see that $a^{m-k} \in H$, and we also know that $a^{m-k} = e$, then $e \in H$. We can now see that the identity, e, is in H. Now, how do we come up with the inverse at the same time?

Firstly, we can rewrite a^{m-k} as $a \cdot a^{m-k-1}$ (Simple rule of exponents).

$$\begin{aligned} a \cdot a^{m-k-1} = e & \\ \text{we know that } a^{m-k} \in H, \text{ so:} & \\ a^{m-k-1} \in H \quad & \text{(Closure under } \cdot \text{)} \\ \text{To have an inverse means:} & \\ a \cdot (x) = e \quad & \text{where } x \text{ is the inverse} \\ \text{We see now that } a \cdot (a^{m-k-1}) = e & \\ \text{and } x = (a^{m-k-1}) & \\ \text{Therefore} \quad (a^{-1}) = (a^{m-k-1}) & \end{aligned}$$

We can now see for some $a \in H$, a^{-1} exists. Furthermore, we can see that $a^{-1} \in H$. We don't need to prove these results again, but we definitely need these results as tools to do other things. We will see this in the first homework.

September 9th, 2020

Last result from last lecture: If we have a group and we have a finite subset of this group then the subset is a subgroup iff it is closed.

Example: $(\mathbb{Z}, +)$, $E = \{\text{Set of all positive even integers, including } 0\}$. Clearly we can see that $E \subset \mathbb{Z}$. Is $(E, +)$ a subgroup of $(\mathbb{Z}, +)$? First thing to note is that E is infinite here. The set of all positive even integers is still an infinite set, as it is not "smaller" than the set of all integers. However, it is also a subset of $\mathbb{Z}$.

By observation, we can see that $(E, +)$ is closed under addition. However, we can see clearly that $(E, +)$ does not have an inverse. So the inverse axiom fails since E only contains positive integers. We don't want to think that subgroup is any different to a normal group - the only difference is that the set for a subgroup is a subset of a bigger set.

Therefore, we can conclude that if we remove "finite" from the result / hypothesis introduced in last class, then we have to treat it like normal and cannot simply count on closure. The conclusion of the hypothesis could be right or wrong (because the hypothesis depends on our subset being finite).

Now, is $(E, +)$ a subgroup? No. It is not a subgroup of $(\mathbb{Z}, +)$.

However, let $E = \{\text{Set of all even integers, including } 0\}$. This is clearly an infinite set that is a subset of $\mathbb{Z}$. Is E a subgroup? Yes! Because if we go through the 4 axioms, it satsifies all of them, even though it is not a finite set. We no longer depend on the hypothesis in this case - we go through the normal procedure of seeing if a set is a group.

Result: $(D, \cdot)$ is a group and $a \in D$, s.t. $|a| = n < \infty$. Then:

$$H = \{a, a^2, a^3, \ \ldots \ a^n (= e)\}$$

is a subgroup of $(D,\cdot)$, and the cardinality of $H, |H| = n$. [Cardinality = size of a set]

For example, if we have an element of order 5, then we can come up with a subgroup with 5 elements, and if we have an element of order 50, we can come up with a subgroup with 50 elements.

How do we prove this result? Since H is a finite subset, we can simply show that H is closed under $\cdot$ and hence conclude that it is a subgroup of $(D,\cdot)$ by our previous result.

$$H = \{a, a^2, a^3, ..., a^n(=e)\}$$

$$\begin{aligned}
\text{Let} \quad x, y \in H. \quad \text{Show that } x \cdot y \in H & \\
x = a^i, \quad y = a^k & \quad 1 \leqslant i, k \leqslant n \\
x \cdot y = a^i \cdot a^k = a^{i+k} & \\
\text{We need to show } a^{i+k} \in H & \\
i + k \in \mathbb{Z}, \quad i + k = cn + r & \quad \text{(By number theory)} \\
0 \leqslant r < n & \\
a^{i+k} = a^{cn+r} & \\
= a^{cn} \cdot a^r = (a^n)^c \cdot a^r & \\
(a^n)^c = e, \quad \text{so we have } e \cdot a^r & \\
\text{if } r = 0: \quad a^0 = e \in H & \\
\text{if } r \neq 0: \quad a^r \in H & \quad \text{because } 0 \leqslant r < n
\end{aligned}$$

Hence, H is closed under $\cdot$, and therefore it has to be a subgroup of $(D,\cdot)$, because it is finite. These things should stay in your mind.

What about if our set is infinite? How do we check for this? Do we need to go through all 4 axioms? Let us see.

Result: (We can use this result in general, but usually we just use it if H is infinite) Assume $(D,\cdot)$ is a group.

Then $(H,\cdot)$ is a subgroup of $(D,\cdot)$ iff $a^{-1} \cdot b \in H \quad \forall a, b \in H$. We can use this to see if a finite subgroup od $(D,\cdot)$ as mentioned above.

$$(a, b) \text{ need not be distinct.}$$

Proof: Assume $H < D$ (subgroup of D) and $a, b \in H$. Then: $a^{-1} \cdot b \in H$, because H is closed and both a^{-1} and $b \in H$ (Since H is a group). This one operation can show us everything we need to know about H being a group. This is trivial.

However, there is a second direction we need to prove.

Assume $a^{-1} \cdot b \in H \quad \forall a, b \in H$. Show that $H < D$. We saw what happens if we assume $H < D$, now let's see the other way around and prove $H < D$, while assuming $a^{-1} \cdot b \in H$. We need to show 3 out of the 4 axioms, except associativity.

1. (Identity)

$$\begin{aligned}
\text{let } a \in H, \text{and choose } b = a & \\
\text{Hence } a^{-1} \cdot b = a^{-1} \cdot a = e \in H &
\end{aligned}$$

Therefore we can see that H has an identity.

2. (Inverse)

$$\begin{aligned}
\text{Let } a \in H. \quad \text{We have to show } a^{-1} \in H & \\
a \text{ has an inverse, but we know it is in } D. & \\
\text{We want to show that it is in } H. & \\
\text{Choose } b = e \in H & \\
\text{Thus } a^{-1} \cdot b = a^{-1} \cdot e \in H & \quad \text{(By assumption)} \\
a^{-1} \cdot e = a^{-1} \in H &
\end{aligned}$$

Therefore, each arbitrary element in H has an inverse that is also in H.

3. (Associativity) This is clear because $H \subset D$.

4. (Closure)

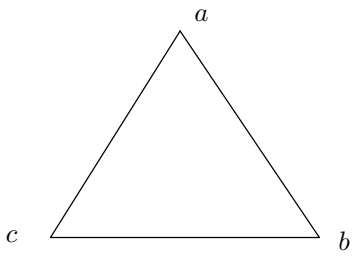
$$\begin{aligned}
\text{Let } a, b \in H. \quad \text{Show that } a \cdot b \in H & \\
\text{Remember our assumption: } a^{-1} \cdot b \in H & \\
a^{-1} \in H & \quad \text{By (2.)} \\
\text{Since } a^{-1} \in H, \text{then } (a^{-1})^{-1} \cdot b \in H & \quad \text{By our assumption}
\end{aligned}$$

This may be a little tricky to understand, but we simply need to consider our assumption and the fact that $a^{-1} \in H$ by (2.). Therefore, we can clearly see that H is closed.

So, simply put, H is a subgroup of D, and this can be used for both finite and infinite subsets.

End of proof

Symmetry group of equilateral $\triangle$*:*

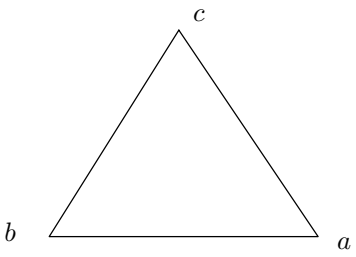


Let us consider a rotation:

$$f_1 = \text{Rotate } \triangle \text{ about center } 120° \text{ clockwise}$$

$$f_1 : \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}$$

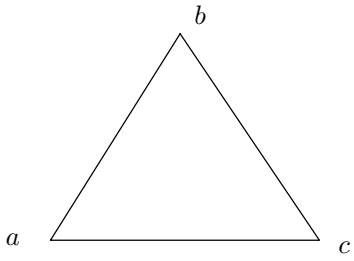
i.e.



Let's take another rotation:

$$f_2 = \text{Rotate } \triangle \quad 240^\circ \text{ clockwise}$$

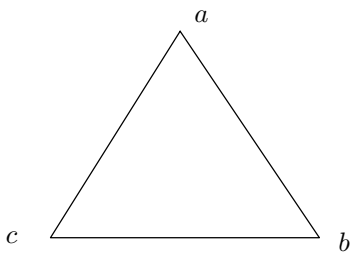
$$f_2 : \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}$$



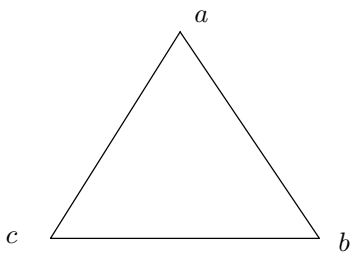
The indentity rotation:

$$f_3 = e = \text{Rotate } 360^\circ \text{ clockwise}$$

$$f_3 = e : \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}$$

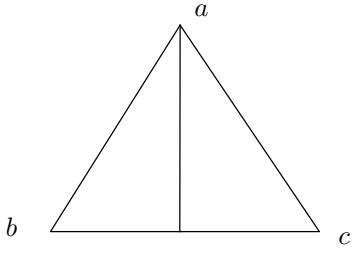


Now let us consider some reflections. Consider the following:



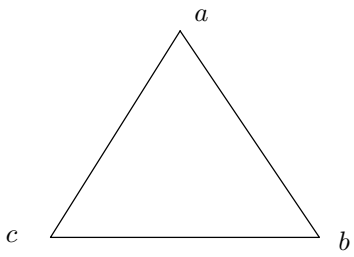
$$f_4 = \text{Reflection about vertex } a$$

$$f_4 : \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}$$

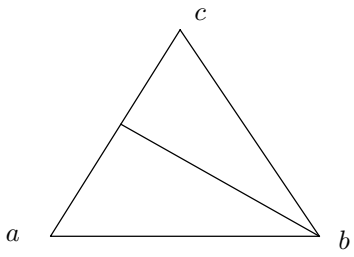


Another reflection for us to consider:

$$f_5 = \text{Reflection about } b$$

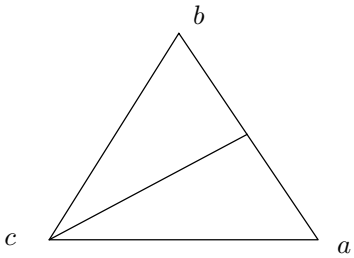


$$f_5 : \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}$$



A similar thing is done for f_6, which is a reflection about c.

$$f_6 : \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix}$$



Now let us see all the rotations:

$$\left\{ f_1 : \begin{pmatrix} a & b & c \\ b & c & a \end{pmatrix}, f_2 : \begin{pmatrix} a & b & c \\ c & a & b \end{pmatrix}, e : \begin{pmatrix} a & b & c \\ a & b & c \end{pmatrix}, f_4 : \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}, f_5 : \begin{pmatrix} a & b & c \\ c & b & a \end{pmatrix}, f_6 : \begin{pmatrix} a & b & c \\ b & a & c \end{pmatrix} \right\}$$

You view each as a function as such:

$$K : \{a, b, c\} \to \{a, b, c\}$$

For f_1:

$$K(a) = b, \quad K(b) = c, \quad K(c) = a$$

This is clearly a finite set. Our binary operation, $\cdot$, are the compositions, $\circ$. We can do the Cayley table for this finite set to see whether it is a group or not. We all this group of 6 elements the symmetry group of equilateral triangles.

Remember compositions and composite functions from Calculus 1. Let us take:

$$f_1 \circ f_5 = \begin{pmatrix} a & b & c \\ a & c & b \end{pmatrix}$$

Note that $f_1 \circ f_5 = f_1(f_5)$. This is another tricky thing to notice, but it is very doable if you look over it again. We take the first one, go to the second one, then come back to the first one and see the corresponding value.

$$f_1 \circ f_5 = f_4 \rightarrow \text{There is closure.}$$

To see everything else, then we can use the Cayley table. The symmetries of an equilateral triangle form a group. It is in fact a non-Abelian group with 6 elements. Let us see the Cayley table to cement this idea (Covered in homework 1).

$\circ$	f_1	f_2	$f_3 = e$	f_4	f_5	f_6
f_1						
f_2						
$f_3 = e$						
f_4						
f_5						
f_6						

Table 3.

September 14th, 2020

Cosets:

Take $(D, \cdot)$ as a group, $(H, \cdot)$ (same binary operator) is a subgroup of D. Let $a \in D$. Then:

$$a \cdot H = \{a \cdot h \quad s.t. \quad h \in H\}$$

This set is called the left coset of H. We can also consider the right coset, the definition is self explanatory, but traditionally we will take the left coset. $H \cdot a = \{h \cdot a \quad s.t. \quad h \in H\}$ (Right coset). If the group is not Abelian, we know for sure that $a \cdot h \neq h \cdot a$. Remember this fact to see that the left coset is different to the right coset.

Let us take $(\mathbb{Z}, +) = (D, \cdot)$. If we then take $(3\mathbb{Z}, +) = (H, \cdot)$, then we can easily check that $(3\mathbb{Z}, +)$ is a subgroup of $(\mathbb{Z}, \cdot)$. Note that $3\mathbb{Z}$ is the set of the multiples of 3.

$$3\mathbb{Z} = \{\ldots., -6, -3, 0, 3, 6, \ldots.\}$$

Select $a, b \in 3\mathbb{Z}$. Show that $a^{-1} \cdot b \in 3\mathbb{Z}$, i.e. $a^{-1} + b \in 3\mathbb{Z}$. If we use this condition, we can see that this is clearly a subgroup of $(D, \cdot)$.

Hence:

$$\begin{aligned} a = 3n \quad \text{and} \quad b = 3m \quad & \text{for some } n, m \in \mathbb{Z} \\ a^{-1} &= -3n \\ a^{-1} \cdot b &= a^{-1} + b \\ &= -3n + 3m \\ &= 3(-n + m) \end{aligned}$$

Since we know that $n, m \in \mathbb{Z}$, then we know for sure that $3(-n+m)$ is a multiple of 3, and therefore $3\mathbb{Z}$ is a subgroup of $\mathbb{Z}$ under addition.

Now, let us see the following:

$$1+3\mathbb{Z} \text{ is the left coset of } 3\mathbb{Z}$$

$$\text{In fact:} \quad 1+3\mathbb{Z} = \{\ldots., -5, -2, 1, 4, 7, 10, \ldots.\}$$

Note that $1 \notin 3\mathbb{Z}$. Will $1+3\mathbb{Z}$ be a subgroup? No. This is because the identity is not present in this set, or rather this coset. In fact, for any $(H, \cdot)$, and for any $a \in D, a \notin H$, $a \cdot H$ is NEVER a subgroup of D. This is clear because e would never be in $a \cdot H$.

Proof: Assume $e \in a \cdot H$. This means:

$$\begin{aligned} a \cdot h &= e \quad \text{for some } h \in H \\ a \cdot h \cdot h^{-1} &= e \cdot h^{-1} \\ a &= h^{-1} \end{aligned}$$

This is a contradiction, because we assumed that $a \notin H$.

$$(1+3\mathbb{Z}) \cap (3\mathbb{Z}) = \varnothing$$

Let us take $9 \in 3\mathbb{Z}$. If we take $(9+3\mathbb{Z})$, we would have a left coset of $3\mathbb{Z}$. The observation here is that if we select $a \in D$ and $a \in H$, then we would not come up with a new left coset. It would simply mean that: $a \cdot H = H$. If we want to come up with a new left coset, we should select some $a \in D$ and $a \notin H$.

Now, let us see $(2+3\mathbb{Z})$, where $2 \notin 3\mathbb{Z}$. Furthermore, $2 \notin 1+3\mathbb{Z}$.

$$(2+3\mathbb{Z}) = \{\ \ldots\ , -4, -1, 2, 5, 8,\ \ldots\ \}$$

$$(2+3\mathbb{Z}) \cap (1+3\mathbb{Z}) = \varnothing$$

That means that these two cosets of $3\mathbb{Z}$ contain nothing in common. Furthermore, we have:

$$(2+3\mathbb{Z}) \cap (3\mathbb{Z}) = \varnothing$$

We have exactly three left cosets of $3\mathbb{Z}$. These are: $0+3\mathbb{Z}, 1+3\mathbb{Z}, 2+3\mathbb{Z}$. These are the only distinct left cosets of $3\mathbb{Z}$. We can conclude that the UNION of all distinct cosets is the whole group.

$$(3\mathbb{Z}) \cup (1+3\mathbb{Z}) \cup (2+3\mathbb{Z}) = \mathbb{Z}$$

The intersection of any two cosets is $\varnothing$. Further, we can see that, for example, $4+3\mathbb{Z} = 1+3\mathbb{Z}$. As a matter of fact, this is exactly where we get the modulo n function.

$$4+3\mathbb{Z} = 1+(3+3\mathbb{Z}) = 1+3\mathbb{Z}$$

$$12+3\mathbb{Z} = 3 \cdot 4+3\mathbb{Z} = 3\mathbb{Z}$$

What can we observe from this? Assume $a \cdot H$ is a left coset. Let us select $b \in a \cdot H$.

$$b \cdot H = a \cdot H$$

Because of the fact that $b \in a \cdot H$. We can demonstrate this with an example. For example, let $b = 3 \in 3\mathbb{Z}$. Then $b+H = a+H$.

Let us take $5\mathbb{Z}$. Find all the left cosets of this subgroup. 0 through $4+5\mathbb{Z}$. These cosets have absolutely nothing in common.

By the previous examples and demonstration, we can see that $\mathbb{Z}_n$ contains numbers only from 0 to $n-1$. We can interestingly write the following:

$$\mathbb{Z}_3 = \{12, 13, 26\}$$

$$12 = 0 \text{ in } \mathbb{Z}_3$$

$$13 = 1 \text{ in } \mathbb{Z}_3$$

$$26 = 2 \text{ in } \mathbb{Z}_3$$

We don't have to deal with these bigger numbers because we know that those bigger numbers are nothing but the smaller ones in any case. This is the beauty of the concept of the left coset.

Result: $(D, \cdot)$ is a group, and $(H, \cdot)$ is a subgroup of D.

1. $a \cdot H = H$ iff $a \in H$
2. $a \cdot H = b \cdot H$ for some $a, b \in D$ iff $b^{-1} \cdot a \in H$. This is how we know that two left cosets are the same.

   Proof:

   $a, b \in D$ and $a \cdot H = b \cdot H$. Show that $b^{-1} \cdot a \in H$.

   $$\begin{aligned} a \cdot H = b \cdot H \text{ implies } a \cdot h_1 = b \cdot h_2 \quad & \text{for some } h_1, h_2 \in H \\ \text{Hence} \quad a \cdot h_1 \cdot h_2^{-1} = b \cdot h_2 \cdot h_2^{-1} = b & \\ \text{This implies} \quad b^{-1} \cdot a \cdot h_1 \cdot h_2^{-1} = b^{-1} \cdot b = e & \\ b^{-1} \cdot a = h_2 \cdot h_1^{-1} \quad & (\text{We eliminate } h_2) \\ \text{Since } H \text{ is a subgroup, then } h_2 \cdot h_1^{-1} \in H & \\ \text{then } b^{-1} \cdot a \in H & \end{aligned}$$

   Second direction: Assume $b^{-1} \cdot a \in H$. Show that $a \cdot H = b \cdot H$

   $$\begin{aligned} &\text{If we want to show that two sets are equal;} \\ &a \cdot H \subset b \cdot H \text{ and } b \cdot H \subset a \cdot H \\ &\text{Therefore } a \cdot H = b \cdot H \end{aligned}$$

   Let $x \in a \cdot H$. Show that $x \in b \cdot H$.

   $$\begin{aligned} x = a \cdot h \quad & \text{for some } h \in H \\ \text{Since } b^{-1} \cdot a \in H \Longrightarrow b^{-1} \cdot a = h_1 \quad & \text{for some } h_1 \in H \\ a = b \cdot h_1 & \\ x = a \cdot h = b \cdot h_1 \cdot h \quad & h \cdot h_1 \in H \\ \text{therefore } b \cdot h_1 \cdot h \in b \cdot H & \\ \text{hence } x \in b \cdot H & \\ \text{By symmetry, we can use the same argument} & \\ \text{to show that for some } y \in b \cdot H, y \in a \cdot H & \\ y = b \cdot h \quad & \text{for some } h \in H \\ b^{-1} \cdot a \in H \quad & \text{for some } h_1 \in H \\ b = a \cdot h_1^{-1} & \\ y = b \cdot h = a \cdot h_1^{-1} \cdot h \quad & h_1^{-1} \cdot h \in H \\ a \cdot h_1^{-1} \cdot h \in a \cdot H & \\ \text{hence } y \in a \cdot H & \end{aligned}$$

Since both are subsets of each other, then $a \cdot H = b \cdot H$.

3. Let $a \cdot H, b \cdot H$ be two left cosets. Then:

   Either $a \cdot H = b \cdot H$ or $a \cdot H \cap b \cdot H = \varnothing$. Whenever we have two left cosets, either they are the same or they do not have ANY elements in common. We observed this by the examples we saw before.

September 16th, 2020

Recall the concept of left cosets.

$$H < D \quad (H \text{ is a subgroup of } D), a \in D$$

1. $a \cdot H = \{a \cdot h \mid h \in H\}$
2. If $a \notin H$, then $a \cdot H$ is never a subgroup of D, and it is never a group either.
3. If $a, b \in D$, $a \cdot H = b \cdot H$ iff $b^{-1} \cdot a \in H$

Result:

$$a, b \in (D, \cdot) \qquad [H < D]$$

Then either:

1. $a \cdot H = b \cdot H$, or
2. $a \cdot H \cap b \cdot H = \varnothing$

Two left cosets of a subgroup are either a set or they have absolutely nothing in common (their intersection is empty)

Proof: Let $a, b \in D$. Assume that $a \cdot H \neq b \cdot H$. We will then show that $a \cdot H \cap b \cdot H = \varnothing$.

$$\begin{aligned}
&\text{We proceed by contradiction:} \\
&x \in a \cdot H \cap b \cdot H \\
&\text{ie. The intersection is NOT empty} \\
&x \text{ is in both } a \cdot H \text{ and } b \cdot H \\
x &= a \cdot h_1 \quad \text{for some } h_1 \in H \\
x &= b \cdot h_2 \quad \text{for some } h_2 \in H \\
\implies & a \cdot h_1 = b \cdot h_2 \\
\implies & b^{-1} \cdot a \cdot h_1 = b^{-1} \cdot b \cdot h_2 = h_2 \\
& b^{-1} \cdot a = h_2 \cdot h_1^{-1} \\
& h_2 \cdot h_1^{-1} \in H \\
& b^{-1} \cdot a \in H
\end{aligned}$$

The previous result showed us that $a \cdot H = b \cdot H$ iff $b^{-1} \cdot a \in H$. Therefore we can conclude that $a \cdot H = b \cdot H$. We assumed that these two are not equal. If we assumed that the intersection is not empty, then we have a contradiction. Therefore we have completed the proof.

Result: Assume $H < D, a \in D$.

$$|a \cdot H| = |H|$$

In other words, the cardinality of the left coset of H is the same as the cardinality of the set H itself. ie. if $|H| = n < \infty$, then $|a \cdot H| = n \quad \forall a \in D$

How do we show that the cardinality of two sets are equal?

Proof:

$$f: H \to a \cdot H$$

We need to show that this function is both one-to-one and onto, i.e. this function is bijective. H is our domain and $a \cdot H$ is our co-domain.

$$\begin{aligned}
f(h) &= a \cdot h \\
\text{Let } y \in a \cdot H & \quad y \text{ is in the co-domain} \\
\text{Then } y &= a \cdot h_1 \quad \text{For some } h_1 \in H \\
\text{Hence } f(h_1) &= a \cdot h_1 = y \\
\text{Therefore } f \text{ is onto} & \quad \text{(Surjective)}
\end{aligned}$$

$$\begin{aligned}
&\text{Now, to show injectivity:} \\
&\text{Assume } f(h_1) = f(h_2) \\
&\text{Show that } h_1 = h_2 \\
\Rightarrow a \cdot h_1 &= a \cdot h_2 \quad a \in D, \text{so } a^{-1} \text{ exists} \\
a^{-1} \cdot a \cdot h_1 &= a^{-1} \cdot a \cdot h_2 \\
\Longrightarrow h_1 &= h_2 \\
\text{Therefore } f \text{ is 1-1} & \quad \text{(Injective)}
\end{aligned}$$

Since we have shown that f is bijective, we conclude that the cardinality of $H =$ cardinality of $a \cdot H$.

$$|H| = |a \cdot H|$$

The method for this proof is by taking a function from H to $a \cdot H$ and showing that it is bijective. If our function is bijective, then the cardinality of the two sets are equal to one another.

Lagrange's Theorem:

$(D, \cdot)$ is a group st $|D| = n < \infty$. This is a group that is finite. Let $H < D$, and $|H| = m$. H is therefore, also finite. Then we can conclude the following:

$$m | n \ (m \text{ is a factor } n)$$

The converse:

Assume $|D| = n < \infty$ and $m | n$. We may or may not have a subgroup with m elements. Lagrange's theorem does not imply that every factor of n must have a subgroup with that factor's cardinality.

Example: If $|D| = 12 = n$, then we may or may not have a subgroup of D with $4, 6, 2$ etc. elements. But if we definitely have a subgroup with m elements, then m should be a factor of n.

But when is the converse of Largrange true? When $(D, \cdot)$ is an Abelian group. The proof of this will rely on furhter mathematics, but we can use this result anyway. In other words, we can say that if D is Abelian and $|D| = n$, we definitely have a group with m elements where $m | n$.

D is Abelian. $|D| = n < \infty$, $m|n \Longrightarrow \exists$ at least one subgroup H of D such that $|H| = m$.

Proof of Lagrange's Theorem:

Let $H = e \cdot H, a_2 \cdot H, a_3 \cdot H, \ldots a_k \cdot H$ be all distinct left cosets of H. Since they are all distinct, this means that their intersections are empty, no elements in common. The left cosets of H are also finite because we know that $|D| = n$, and thus D is a finite set.

$$D = H \cup a_2 \cdot H \cup a_2 \cdot H \cup \cdots \cup a_k \cdot H$$

$|D| = n = |H| + |a_2 \cdot H| + \cdots + |a_k \cdot H|$. Each of our $|a_i \cdot H| = m$

Therefore, $n = km$, and thus m is a factor of n. This is the end of our proof.

Result: $(D, \cdot)$ is a group and $|D| = n < \infty$. Let $a \in D$, and $|a| = m$.

Then: $m|n$. How do we show that this is true?

Proof: Let $H = a, a^2, a^3, \ldots, a^m = e$. By class-result, we know that $H < D$ and $|H| = m$. Hence, by Lagrange's theorem, we conclude that $m|n$.

Let $|D| = 14$. Assume $a \in D$, $a^2 \neq e$, $a^7 \neq e$, then $|a| = 14$.

September 21st, 2020

Quotient Groups:

Let $(D, \cdot)$ be a group and $H < D$. H is a subgroup of D. We say $H \lhd D$. This means that H is a normal subgroup of D. This is iff $\forall a \in D$, $a \cdot H = H \cdot a$. This means that every left coset is a right coset in common language.

This statement means $\forall h \in D, \exists w \in H$ s.t. $a \cdot h = w \cdot a$. h does not necessarily have to equal w. Similarly, it does not means that $a \cdot h = h \cdot a$ (although this is true if our group was Abelian).

Furthermore, if $(D, \cdot)$ is Abelian, then every subgroup of $(D, \cdot)$ is a normal subgroup.

$$H \lhd D \Longleftrightarrow a \cdot H = H \cdot a \quad \forall a \in D$$

$$H \lhd D \Longleftrightarrow a \cdot H \cdot a^{-1} = H \quad \forall a \in D$$

Result: Assume $(D, \cdot)$ is a group and $H \lhd D$. Then:

$$(D/H, *) \text{ (Quotient group), or } D \bmod H \text{, factor group}$$

$$D/H = \{a \cdot H \mid a \in D\}$$
$$D/H \text{ consists of all left cosets of } H$$
$$x \in D/H \text{, meaning } x = a \cdot H \text{ for some } a \in D$$

$$\text{Define } * \text{ on } D/H \text{ st } \forall x, y \in D/H,$$
$$x * y = (a \cdot b) \cdot H \text{, where } x = a \cdot H \text{ and } y = b \cdot H$$
$$\text{For some } a, b \in D$$

We need to show that $*$ is well defined on D/H.

$$\begin{aligned}
\text{Assume } a \cdot H = c \cdot H = x \quad & \in D/H \\
b \cdot H = d \cdot H = y \quad & \in D/H \\
x * y = a \cdot b \cdot H & \\
x * y = c \cdot d \cdot H &
\end{aligned}$$

We need to show that $a \cdot b \cdot H = c \cdot d \cdot H$
This means that $*$ does not rely
on how x or y are represented

By previous result regarding left cosets,
$a \cdot b \cdot H = c \cdot d \cdot H \iff (c \cdot d)^{-1} \cdot (a \cdot b) \in H$

Note that $(c \cdot d)^{-1} = d^{-1} \cdot c^{-1}$

$$\begin{aligned}
\text{Show that } (c \cdot d)^{-1} \cdot (a \cdot b) \in H & \\
d^{-1} \cdot c^{-1} \cdot a \cdot b \in H & \\
c^{-1} \cdot a \in H \quad & (\text{Since } a \cdot H = c \cdot H \Rightarrow c^{-1} \cdot a \in H) \\
d^{-1} \cdot h \cdot b \quad & \text{For some } h \in H \\
\text{Since } H \text{ is a normal subgroup of } D & \\
\text{Then } b \cdot H = H \cdot b & \\
\text{Hence} \quad h \cdot b = b \cdot h_1 \quad & \text{for some } h_1 \in H \\
d^{-1} \cdot h \cdot b = d^{-1} \cdot b \cdot h_1 & \\
d^{-1} \cdot b \in H \quad & (\text{Since } b \cdot H = d \cdot H \Rightarrow d^{-1} \cdot b \in H) \\
d^{-1} \cdot b \cdot h_1 = h_2 \cdot h_1 & \\
h_2 \cdot h_1 \in H \text{ Since } H < D &
\end{aligned}$$

Thus $*$ is well-defined.

Result: $(D, \cdot)$ is a group and $H \lhd D$. Then $(D/H, *)$ is a group with the identity $e' = e \cdot H = H$. e is the identity of D in this case, and e' is the identity of D/H.

Proof:

(Closure)

$$\begin{aligned}
x, y \in D/H, x = a \cdot H, y = b \cdot H \quad & \text{for some } a, b \in D \\
x * y = a \cdot b \cdot H & \\
\text{Since } (D, \cdot) \text{ is a group, } a \cdot b \in D & \\
\text{Trivially, } (a \cdot b) \cdot H \text{ is also} & \\
\text{another left coset of } H & \\
\text{Since the } \cdot \text{ of two left cosets of } H & \\
\text{result in another left coset of } H &
\end{aligned}$$

We conclude that D/H is closed under $*$

(Identity)

$$\begin{aligned} \text{Let } x \in D/H, x = a \cdot H \quad & \text{For some } a \in D \\ x * e = a \cdot H * e \cdot H \quad & e \text{ is the identity of } D \\ a \cdot e \cdot H = a \cdot H & \\ e * x = x & \end{aligned}$$

Therefore, H is the identity.

(Inverse)

$$\begin{aligned} x \in D/H, \text{show that } x^{-1} \in D/H & \\ x = a \cdot H \quad & \text{for some } a \in D \\ x^{-1} = a^{-1} \cdot H & \\ x * x^{-1} = a \cdot H * a^{-1} \cdot H & \\ (a \cdot a^{-1}) \cdot H & \\ = e \cdot H = H \quad & e \text{ is the identity of } D \\ \text{and } H \text{ is the identity of } D/H & \end{aligned}$$

(Associative)

This is clear since $(D, \cdot)$ is associative.

We are therefore done and have proven that $(D/H, *)$ is indeed a group.

Let us take an example: $(\mathbb{Z}, +)$. We know that $5\mathbb{Z} \lhd \mathbb{Z}$. Since $\mathbb{Z}$ is Abelian under addition, then $5\mathbb{Z}$ is clearly a subgroup and further a normal subgroup.

$$\frac{\mathbb{Z}}{5\mathbb{Z}} = \{5\mathbb{Z}, 1 + 5\mathbb{Z}, 2 + 5\mathbb{Z}, 3 + 5\mathbb{Z}, 4 + 5\mathbb{Z}\}$$

This group has 5 elements.

Let us take two left cosets of $\mathbb{Z}$. Let's take $4 + 5\mathbb{Z}$ and $2 + 5\mathbb{Z}$.

$$(4 + 5\mathbb{Z}) * (2 + 5\mathbb{Z}) = (6 + 5\mathbb{Z}) = 1 + 5\mathbb{Z}$$

The $*$ that we defined on our structure is simply addition mod n. Actually, studying quotient groups is the reason why we came up with the idea of $5\mathbb{Z}$, and all of modulo mathematics. The correct name of $5\mathbb{Z}$ is actually $\frac{\mathbb{Z}}{5\mathbb{Z}}$.

Result: $(D, \cdot)$ is a finite group and $|D| = n < \infty$. Further, $H < D$.

$$|D/H| \text{ is a factor of } n$$

D/H is a set of all distinct left cosets of H. This is a group if H is normal. How many distinct left cosets will we have? It has to be a factor of n, or the order of the group D.

Proof: Assume $H, a_2 \cdot H, \ldots, a_k \cdot H$ are all distinct left cosets of H, and $|H| = m$.

$$|D/H| = k, \text{we know that } |H| = |a_i \cdot H| \; \forall n \in 2 \leqslant i \leqslant k$$

$$\begin{aligned} |D| &= |H| + |a_2 \cdot H| + \cdots + |a_k \cdot H| \\ &= m + m + \cdots + m \\ n &= km \\ k &| n \end{aligned}$$

Or in other words, k is a factor of n.

Since $|D| = n, |H| = m$, $n = mk$ and $|D/H| = k$, we conclude that:

$$|D/H| = \frac{|D|}{|H|} = \frac{n}{m} = k$$

Example:

$$|D| = 30$$

$$H < D, |H| = 5$$

How many left cosets should H have by this result? We should have exactly $\frac{30}{5} = 6$ left cosets. This means that $|D/H| = 6$, or in other words the cardinality of the set D/H is 6 (comprised of 6 elements). This does not say that D/H is a group though, since that would only be the case if H is a normal subgroup.

September 23rd, 2020

Direct Sum (Product):

Definition: $(D, \cdot)$, and $(F, *)$ (Not the same binary operation). The direct sum or product is:

$$H = D \oplus F = \{(d, f) \mid d \in D, f \in F\}$$

H is the set of all ordered pairs (d, f) where $d \in D$ and $f \in F$.

Result: $(D, \cdot)$ and $(F, *)$ are groups (given). Then $(H = D \oplus F, \oplus)$ is a group with exactly $|D| \times |F|$ elements. i.e. This group has as many elements as the product of the elements in D and F, where:

$$(d_1, f_1) \oplus (d_2, f_2) = (d_1 \cdot d_2, f_1 * f_2)$$

$\forall (d_1, f_1), (d_2, f_2) \in H$. How do we prove that the new structure is a group?

Proof:

(Closure) This is clear since D, F are both closed under $\cdot$ and $*$. If we look at the definition, we can see that the structure is a group since we never get an element outside of D, F.

(Identity) $e_H = (e_D, e_F)$. Why?

$$(d, f) \oplus (e_D, e_F) = (d \cdot e_D, f * e_F) = (d, f)$$

(Inverse) $(d, f)^{-1} = (d^{-1}, f^{-1})$. Why?

$$(d, f) \oplus (d^{-1}, f^{-1}) = (d \cdot d^{-1}, f * f^{-1}) = (e_D, e_F)$$

(Associative) Since both $\cdot$ and $*$ are associative, then we can clearly see that $\oplus$ will also be associative. In other words, $(D, \cdot)$ and $(F, *)$ both satisfy the associative property.

Question: Give me an example of a non-Abelian group with 60 elements.

Solution: If we let S_3 be the symmetric group of an equilateral triangle, we know that this group is definitely non-Abelian (from HW1).

$$H = (\mathbb{Z}_{10}, +) \oplus (S_3, \circ)$$

Both $(\mathbb{Z}_{10}, +)$ and $(S_3, \circ)$ are groups, and $(\mathbb{Z}_{10}, +)$ has 10 elements and $(S_3, \circ)$ has 6 elements.

Therefore:

$$|H| = 10 \times 6 = 60 \text{ elements}$$

In S_3, we have at least two elements, called s_1 and s_2 such that $s_1 \circ s_2 \neq s_2 \circ s_1$. Now we can see the following in our new structure to determine whether H is Abelian or not.

$$(1, s_1) \oplus (2, s_2) = (3, s_1 \circ s_2)$$

but:

$$(2, s_2) \oplus (1, s_1) = (3, s_2 \circ s_1)$$

But we know that $s_1 \circ s_2 \neq s_2 \circ s_1$, so these two elements are not the same.

$$\text{ie } (1, s_1) \oplus (2, s_2) \neq (2, s_2) \oplus (1, s_1)$$

Therefore, clearly, we can see that $(H, \oplus)$ is non-Abelian. Another example would be the following:

$$H = (\mathbb{Z}_2, +) \oplus (S_3, \circ)$$

Then: $|H| = 12$.

Result: $H = (D, \cdot) \oplus (F, *)$. Then, $\forall (d, f) \in H$, what would be the order?

$$|(d, f)| = \text{lcm}\,(|d|, |f|)$$

Proof:

$$\begin{aligned} &\text{Assume } |d| = m, |f| = n \\ &|(d, f)| = k \\ \Longrightarrow &(d, f)^k = e_H = (e_D, e_F) \\ = &(d^k, f^k) = (e_D, e_F) \\ = &d^k = e_D,\ f^k = e_F \\ &m|k \text{ and } n|k \end{aligned}$$

Since $m|k$ and $n|k$ and k is the smallest positive integer s.t. $(d, f)^k = e_H$, we conclude that:

$$k = \text{lcm}\,(m, n)$$

Example: $H = (\mathbb{Z}_4, +) \oplus (\mathbb{Z}_{12}, +)$. Find $|(2,5)|$.

$$
\begin{aligned}
&= \text{lcm}\,(|2|, |5|) \\
|2| &= \frac{4}{\gcd(2,4)} = 2 \\
|5| &= \frac{12}{\gcd(5,12)} = 12 \\
&= \text{lcm}\,(2,12) = 12
\end{aligned}
$$

Therefore

$$|(2,5)| = 12$$

Recall that if we have:

$$
\begin{aligned}
|a| &= n \\
\{a, a^2, a^3 \ldots., a^n = e\}&
\end{aligned}
$$

subgroup of D with n elements,

$$
\begin{aligned}
|a| = n &\Longrightarrow \text{subgroup with } n \text{ elements} \\
\text{but } &\Longleftarrow \text{is not always true}
\end{aligned}
$$

Take $H = (\mathbb{Z}_2, +) \oplus (\mathbb{Z}_2, +)$. H is a group with 4 elements. Does H have an element of order 4? No. In fact, $|(d, f)| = 2$ when $(d, f) \neq e_H$.

Result: If we have $H = (D, \cdot) \oplus (F, *)$, choose $A < D, B < F$. Let us take:

$$K = (A, \cdot) \oplus (B, *)$$

Is this a group? Definitely. In fact, we can further see that $K < H$.

Question: $H = (D, \cdot) \oplus (F, *)$. Let $L < H$. Can we find a subgroup A of D and a subgroup B of F such that:

$$L = A \oplus B$$

No. Not always. This means we can have a subgroup in this structure that we cannot write as a direct sum of two different subgroups.

Example: Take $H = (\mathbb{Z}_2, +) \oplus (\mathbb{Z}_4, +)$. What is $|(1,1)|$?

$$|(1,1)| = \text{lcm}\,(2,4) = 4$$

We have an element of order 4. Can we construct a subgroup with 4 elements? Yes!

$$\{(1,1), (1,1)^2, (1,1)^3, (1,1)^4 = e\}$$

$$= \{(1,1), (0,2), (1,3), (0,0)\}$$

This is a subgroup with 4 elements. However, this set $\neq A \oplus B$, where $A < \mathbb{Z}_2$ and $B < \mathbb{Z}_4$.

September 26th, 2020

***Common Knowlege in Number Theory*:**

Question: If we are given a set $D = \{a | 1 \leqslant a < n \text{ and } \gcd(a, n) = 1\}$, then what is the cardinality of this set? If the gcd of two numbers is 1, then they are said to be relatively prime.

$$|D| = \varphi(n)$$

How do we calculate $\varphi(n)$?

$$\begin{aligned} n &> 1 \\ n &= p_1^{n_1} \cdot p_2^{n_2} \cdot \cdots \cdot p_k^{n_k} \\ &\text{This is the prime factorization of } n, \\ &\text{and } p_1, p_2, \ldots., p_k \text{ are distinct} \\ \varphi(n) &= (p_1 - 1)p_1^{n_1 - 1} \cdot (p_2 - 1)p_2^{n_2 - 1} \ldots. \cdot (p_k - 1)p_k^{\alpha_k - 1} \end{aligned}$$

Let us take an example. Choose $n = 74$.

$$\begin{aligned} n = 74 &= 2 \cdot 37 \\ &= 2^1 \cdot 37^1 \\ \varphi(n) &= (2-1)2^0 \cdot (37-1)37^0 \\ &= 36 \end{aligned}$$

What is the meaning of this number? This is the cardinality of D where

$$D = \{a | 1 \leqslant a < n \text{ and } \gcd(a, 74 = 1\}$$

There are exactly 36 numbers between 1 and 74 where each one of them is relatively prime to 74. We can also take another example.

$$\begin{aligned} n &= 32 \cdot 5^3 \cdot 7^4 \\ n &= 2^5 \cdot 5^3 \cdot 7^4 \quad \text{Prime factorization} \\ \varphi(n) &= 2^4 \cdot 4 \cdot 5^2 \cdot 6 \cdot 7^3 \\ \varphi(n) = |D| &\text{ where } D = \{a | 1 \leqslant a < n, \text{and } \gcd(a, n) = 1\} \end{aligned}$$

Question: Let $n > 1$. Choose $k | n$. It is possible for k to be 1. $k \neq n$. k can be 1 or any other factors of n except n.

$$M = \{a | 1 \leqslant a < n \text{ and } \gcd(a, n) = k\}$$

$$|M| = \varphi\left(\tfrac{n}{k}\right)$$

Let us take an example: $n = 32 \cdot 3^5 = 2^5 \cdot 3^5$, and $k = 6$. $k | n$.

$$\begin{aligned} M &= \{a | 1 \leqslant a < n \text{ and } \gcd(a, n) = 6\} \\ |M| &= \varphi\left(\frac{n}{k}\right) = \varphi\left(\frac{n}{6}\right) \\ \frac{n}{6} &= 2^4 \cdot 3^4 \\ \varphi\left(\frac{n}{6}\right) &= 2^3 \cdot 2 \cdot 3^3 \end{aligned}$$

What is $\varphi(\text{prime number})$? $n - 1$. This means that if we have a number, n, that is a prime number, then the prime factorization of that number, $\varphi(n) = n - 1$.

Fermat's Little Theorem:

Assume $\gcd(a, p) = 1$, where $a \in \mathbb{Z}^+$ and p is a prime number. Then:

$$p \,|a^{p-1} - 1$$

Another way of saying this is that $(a^{p-1}) \bmod p = 1$. If we take a number, a, that is relatively prime to p, and we divide by p, the remainder is going to be 1. Why is it little? Because we will get the bigger one later.

Notice that $p - 1 = \varphi(p)$

***Euler's Result*:**

$n \in \mathbb{Z}^+$ and $a \in \mathbb{Z}^+$ st $\gcd(a, n) = 1$. Then we can see that:

$$a^{\varphi(n)} (\bmod n) = 1$$

This is the same as Fermat's little theorem, but it is more general.

Result:

$$(\mathbb{Z}_n^*, \times) \text{ is a group iff } n \text{ is prime}$$

Proof:

Assume $(\mathbb{Z}_n^*, \times)$ is a group. We show that n is prime

$\Longrightarrow$

We proceed by contradiction. Assume that $n = m\,k, 1 < m, k < n$
Since m and $k \in \mathbb{Z}_n^*, m\,k = n = 0 \in \mathbb{Z}_n^*$
This is our contradiction, since $0 \notin \mathbb{Z}_n^*$
Therefore n has to be prime

Assume n is prime, show that $(\mathbb{Z}_n^*, \times)$ is a group

$\Longleftarrow$

Associative property is clear.

$e = 1$, therefore we have the identity $e \in \mathbb{Z}_n^*$

Closure:
Let $a, b \in \mathbb{Z}_n^*$. Show that $a \times b \in \mathbb{Z}_n^*$
Proceed by contradiction to see that
$a \times b = 0 \in \mathbb{Z}_n^* \Longrightarrow a = 0$ or $b = 0$
This is our contradiction since $a, b \in \mathbb{Z}_n^*$

Inverse:
Let $a \in \mathbb{Z}_n^*$, since $\gcd(a, n) = 1$,
By Fermat's Little Theorem,
$a^{n-1} (\bmod n) = 1$
$a \times a^{n-2} = 1 \in \mathbb{Z}_n$
$a^{-1} = a^{n-2} \in \mathbb{Z}_n^*$

So we have shown that if n is prime, $\mathbb{Z}_n^*$

$(\mathbb{Z}_{13}^*, \times)$ is a group, as an example

Result:

Define $n > 1$. Then $U(n) = \{a | 1 \leqslant a < n \text{ and } \gcd(a, n) = 1\}$. This is clearly a subset of $\mathbb{Z}_n^*$. ie $U(n) \subseteq \mathbb{Z}_n^*$. If our n is a prime number, then $U(n) = \mathbb{Z}_n^*$.

Result:

$$(U(n), \times) \text{ is an Abelian group}$$

Let us take an example, say $(\mathbb{Z}_{15}^*, \times)$. This is clearly not a group since we know that 15 is not prime. However, can we find a group from it:

$$U(15) = \{1, 2, 4, 6, 8, 11, 13, 14\}$$

$$|U(n)| = \varphi(n)$$

We know that $\varphi(15) = 8$, which matches the number of terms we found in $U(15)$. Therefore:

$$(U(15), \times) \text{ is a group}$$

How do we prove this result?

Closure:
$a, b \in U(n)$
since $\gcd(a, n) = 1$ and $\gcd(b, n) = 1$
$\gcd(a \times b, n) = 1$, and hence
$a \times b (\mathrm{mod}\, n) \in U(n)$

Identity:
$e = 1 \in U(n)$

Associativity is also clear

Inverse:
$a \in U(n)$
Since $\gcd(a, n) = 1$, by Euler's theorem:
$a^{\varphi(n)} (\mathrm{mod}\, n) = 1$
Hence $a \times a^{\varphi(n)-1} = 1 \in U(n)$
The inverse of $a = a^{\varphi(n)-1}$

Let us take $(U(30), \times)$, this is a group, but for the same number, $(\mathbb{Z}_{30}^*, \times)$ is not a group. Furthermore, we can see that:

$$|U(30)| = \varphi(30)$$

$30 = 2 \cdot 3 \cdot 5$
$\varphi(30) = 1 \cdot 2 \cdot 4 = 8$
Therefore $U(30)$ has 8 elements

Question: Imagine $(D,\cdot)$ is a group. We select $a\in D$ and $|a|=20$. 20 is the smallest positive integer where if we do $\cdot$ on a 20 times, we get the identity.

$$H=\{a,a^2,a^3,\ldots,a^{20}=e\}<D$$

How many elements of order 20 does H have?

Solution: $|a^k|=\frac{20}{\gcd(k,20)}=20$. This means that $\gcd(k,20)=1$, and $1\leqslant k<20$. This leads us to the conclusion: H has exactly $\varphi(20)$ elements, each of which have order 20. Furthermore, D has AT LEAST $\varphi(20)$ elements of order 20.

How many elements in H of order 5 (Since 5 is a factor of 20)?

$$|a^k|=\frac{20}{\gcd(k,20)}=5$$

$$\Longrightarrow \gcd(k,20)=4, 1\leqslant k<20$$

From the beginning of the lecture, we know that this value is $\varphi\left(\frac{20}{4}\right)=\varphi(5)=4$. Now, how many elements in H have order 10?

$$|a^k|=\frac{20}{\gcd(k,20)}=10$$

$$\gcd(k,20)=2, 1\leqslant k<20$$

$$\varphi\left(\frac{20}{2}\right)=\varphi(10) \text{ (From earlier result)}$$

Definition of a Finite Cyclic Group:

$(D,\cdot)$ is a finite group with n elements $(n<\infty)$. We say that D is a cyclic group iff D has an elmenet a where $|a|=n$. i.e. $D=\{a,a^2,a^3,\ldots,a^n=e\}$. If we have an element of order n, we can generate the whole group fom this one element. This means that each element in D is some power of a.

September 28th, 2020

Finite Cyclic Groups:

Def: We have $(D,\cdot)$, which is a finite group, and $|D|=n<\infty$. If $\exists a\in D \text{ st } |a|=n$, then we say that D is a cyclic group. In notation, we say that $D=<a>$. The order of a is n and we can write D as:

$$D=\{a,a^2,a^3,\ldots a^n=e\}$$

Do we have any examples of groups that are cyclic?

$$(\mathbb{Z}_n,+) \text{ is cyclic for all } n\geqslant 2$$

This is because of the fact that:

$$\begin{aligned}|1|&=n \text{ in } (\mathbb{Z}_n,+)\\ (\mathbb{Z}_n,+) &\text{ is generated by } 1, \text{ ie } (\mathbb{Z}_n,+)=<1>\\ &=\{1,1^2,1^3,\ldots 1^n\}\\ &=\{1,2,3,\ldots,0=e\}\end{aligned}$$

Question: Find all generators of $\mathbb{Z}_n$. What do we mean by generators? $D = <a>$, D is cyclic and is generated by a. Therefore:

$$D = \{a, a^2, a^3, \ldots . a^n\}$$

We know that 1 is a generator of $(\mathbb{Z}_n, +)$. Is that the only one? How many can we find other than 1? What is the process of thinking here? Another way of looking at this is how many elements in $\mathbb{Z}_n$ are of order n? To know all the generators, we need to know all the elements of order n.

$$(\mathbb{Z}_n, +) = <1>$$

$$\begin{aligned} \text{Assume } (\mathbb{Z}_n, +) &= <a> \\ &= <1^k>, \text{ where } a = 1^k \end{aligned}$$

$$\begin{aligned} \text{Hence } |a| &= n \\ |a| = |1^k| &= \frac{|1|}{\gcd(k, n)} = n \\ \text{In other words, } \gcd(k, n) &= 1 \\ \text{ie } |a| = n &\text{ iff } \gcd(k, n) = 1 \end{aligned}$$

Result:

$$(\mathbb{Z}_n, +) \text{ has exactly } \varphi(n) \text{ generators}$$

This means that it has exactly $\varphi(n)$ elements, each of which is of order n. To continue with this, let us take an example:

$$\text{Find all generators of } (\mathbb{Z}_{20}, +)$$

$$\begin{aligned} \text{Obviously, one of them is } 1 \\ 3 = 1^3 \text{ and } \gcd(3, 20) &= 1 \\ \gcd(7, 20) &= 1 \\ \text{etc} \ldots . \\ 1, 3, 7, 9, 11, 13, 17, 19 \end{aligned}$$

$$\begin{aligned} \text{Therfore, } (\mathbb{Z}_n, +) &= \\ <1> = <3> = \cdots &= <19> \end{aligned}$$

$$\begin{aligned} \text{How many generators do we need to have?} \\ \varphi(20) \text{ elements, and } \varphi(20) &= 8 \end{aligned}$$

Theorem about Cyclic Groups:

Assume that $(D, \cdot)$ is a cyclic group, and $|D| = n < \infty$.

1. Let $m|n$, then D has exactly $\varphi(m)$ elements, each is of order m

Proof:

Since $(D, \cdot)$ is cyclic, $\exists a \in D$
st $|a| = n$, ie $D = <a>$
$= \{a, a^2, a^3, \ldots, a^n\}$

Therefore $D = <a> = \{a, a^2, a^3, \ldots, a^n\}$

Let $m|n$, and let $b \in D$
Hence $b = a^k$ for some $1 \leqslant k < n$, and $b \neq e$

$$|b| = \frac{|a|}{\gcd(k, n)} = m$$
$$|b| = \frac{n}{\gcd(k, n)} = m$$
Therefore: $\gcd(k, n) = \frac{n}{m}$
and $1 \leqslant k < n$

$\Longrightarrow$we know that we have exactly $\varphi\left(\frac{n}{\frac{n}{m}}\right) = \varphi(m)$
elements, where $\gcd(k, n) = \frac{n}{m}$

This means that D has exactly $\varphi(m)$ elements, each is of order m.

Result from number theory:

$$n = \sum_{d|n} \varphi(d)$$

As an example, we can take $n = 15$. $15 = \varphi(1) + \varphi(3) + \varphi(5) + \varphi(15)$, and $\varphi(1) = 1$ by default

Proof:

Consider the cyclic group $(\mathbb{Z}_n, +)$
Let $d|n$
We know that $(\mathbb{Z}_n, +)$ has exactly $\varphi(d)$ elements
each of order d

Assume that $1, d_1, d_2, \ldots, d_k = n$
are all distinct factors of n
$\varphi(1) + \varphi(d_1) + \varphi(d_2) + \cdots + \varphi(n) = n$

For each divisor d of n, we have $\varphi(d)$ elements
Therefore, $\sum_{d|n} \varphi(d) = n$

As an example, let us take n=300

$$300 = \sum_{d|300} \varphi(d)$$

2. $(D, \cdot)$ is a cyclic group and $|D| = n$. If $m|n$, then there exists a unique subgroup of D with exactly m elements.

   For example, if we have a group $(D, \cdot)$ and $|D| = 30$, then $\exists$ exactly one unique subgroup with 6 elements, since 6|30. The same follows for other factors of 30.

   Proof:

   We use the fact that
   every subgroup of a cyclic group is cyclic. (We will prove this later)

   Let $b \in D, |b| = m$
   Hence $< b > = \{b, b^2, b^3, \ldots., b^m = e\}$
   is a subgroup of D with m elements. We proved this in (1)

   We show that $< b >$ is unique.
   Assume D has another subgroup,
   H, st $|H| = m$
   We show that $H = < b >$.
   Using the fact that H is cyclic, ie $H = < c >, |c| = m$
   $< b >$ has exactly $\varphi(m)$ elements of order m

   We proved that D has exactly $\varphi(m)$ elements of order m
   These two statements give us the conclusion:
   Every element in D of order m must "live" inside $< b >$

   $\boldsymbol{H = < c >}$ and $|c| = m$
   $\boldsymbol{c \in < b >}$
   therefore: $< c > = < b >$

   Note that every cyclic group is Abelian. If our group is not Abelian, then it will never be cyclic.

   Proof:

   Since D is cyclic,
   $D = < a >, x, y \in D$
   $x = a^k, y = a^m$
   $x \cdot y = a^k \cdot a^m = a^{k+m}$
   $a^{k+m} = a^{m+k}$, therefore $x \cdot y = y \cdot x$

   Therefore, D is an Abelian group

October 5th, 2020

Cyclic Groups:

$(D, \cdot)$ is finite cyclic and we know that $|D| = n < \infty$.

1. D is an Abelian group

2. If $m|n$, then D has a unique subgroup with m elements

3. If $b \in D$ and $|b| = n$, then $D = \{b, b^2, \ldots, b^n = e\}$

4. D has $\varphi(n)$ elements each of order n

Def: We say that a group, $(D, \cdot)$ is an infinite cyclic group, ie $D = <a>, a \in D$ iff $\forall b \in D, \exists n \in \mathbb{Z}$ st $b = a^n$.

Result: $(D, \cdot)$ is cyclic, where it could be finite or infinite cyclic. Let $h < D$. Then $H \lhd D$ and H is cyclic.

Proof:

Since D is Abelian, it is clear that $H \lhd D$ (H is a normal subgroup of D). We now also need to prove that H is cyclic.

Since D is cyclic,
$D = <a>$ for some $a \in D$
Let $m = \min\{i | a^i \in H, i \geqslant 1\}$
Claim H is generated by a^m, ie $H = <a^m>$

Let $h \in H$. We show that $h = (a^m)\, k$ for some $k \in \mathbb{Z}$
Since $D = <a>$ and $h \in D$,
$h = a^w$ for some $w \in \mathbb{Z}$
We show that $m|w$. We are done after that
Hence $w = m\, k + r$, where $0 \leqslant r < m$
The next step is to show that $r = 0$
$h \in H, h = a^w = a^{mk+r} = a^{mk} \cdot a^r$
$a^{mk} \in H$, it has an inverse
$a^{-mk} \cdot a^w = a^{-mk} \cdot a^{mk} \cdot a^r$
$= a^r$
$a^{-mk} \cdot a^w \in H$, and therefore $a^r \in H, 0 \leqslant r < m$
Since m is the smallest positive integer st $a \in H$,
we conclude that $r = 0$. $(a^0 = e \in H)$
$\Longrightarrow h^{mk} = (a^m)^k$
$\Longrightarrow H = <a^m>$

Result: Assume $(D, \cdot)$ is an infinite cyclic group. D has exactly 2 generators. Namely, if $D = <a>$ and $D = <b>$, then $b = a^{-1}$. All other elements of D will not generate D.

$$D \text{ is infinite cyclic} \Longrightarrow \exists! a \in D \text{ st } D = <a> = <a^{-1}>$$

Why is this true for the infinite cyclic group?

Proof:

Assume $(D,\cdot) = <a>$. We show that $D = <a^{-1}>$

$$\begin{aligned}
\text{Let } b \in D, \text{hence } b = a^n \text{ for some } n \in \mathbb{Z} \\
a^n = (a^{-1})^{-n}, -n \in \mathbb{Z} \\
\Longrightarrow b = a^n \in <a^{-1}> \\
\Longrightarrow <a> = <a^{-1}> = D
\end{aligned}$$

Now, we assume $D = <b>$, where $b \neq a$ and $b \neq a^{-1}$. We will reach a contradiction, where we can see that b must equal a.

$$\begin{aligned}
\text{Since } D \text{ is infinite cyclic and } D = <a>, \\
\text{we conclude that } |a| = \infty
\end{aligned}$$

$$\begin{aligned}
\text{Since } a \in D \text{ and } D = <b>, \exists m \in \mathbb{Z} \text{ st } a = b^m \\
\text{Also, since } b \in D \text{ and } D = <a>, \exists n \in \mathbb{Z} \text{ st } b = a^n
\end{aligned}$$

$$\begin{aligned}
a = b^m \text{ and } b = a^n \Longrightarrow a = a^{nm} \\
a \cdot a^{-1} = a^{nm} \cdot a^{-1} \\
e = a^{nm-1} \\
\Longrightarrow n\,m - 1 \text{ must be } 0, \text{otherwise } |a| < \infty, \text{contradiction}
\end{aligned}$$

$$\begin{aligned}
n\,m - 1 = 0, n, m \in \mathbb{Z} \\
n = 1, m = 1 \text{ or } n = -1, m = -1
\end{aligned}$$

$$\begin{aligned}
\text{if } n = m = 1, b = a, \text{which is again, a contradiction.} \\
\text{if } n = m = -1, b^{-1} = a^{-1} \Longrightarrow b = a, \text{which is a contradiction}
\end{aligned}$$

Hence D has exactly 2 generators, and it cannot have any other generators other than one element and its inverse, as proven above through contradiction.

Example of an Infinite Cyclic Group:

$$(\mathbb{Z}, +) = <1> = <1^{-1}> = <-1>$$

This clearly shows us that 1 and -1 are the only two generators of $\mathbb{Z}$.

Let $n \in \mathbb{Z}, \exists m \in Z \text{ st } n = 1^m \Longrightarrow 1^n = m$, and thus $m = n$. Similarly, $n = (-1)^n$.

Example of an Infinite Abelian group that is NOT cyclic:

$$(\mathbb{Q}, +) \rightarrow \text{is an Abelian group that is not cyclic}$$

The same follows with $(\mathbb{R}, +)$ and $(\mathbb{C}, +)$. We could even look to **Q1 in HW2**, which is the power set of a set D. This is a finite Abelian group that is not cyclic.

How do we convince ourselves of this?

$$\begin{aligned}
(\mathbb{Q}, +) = <\frac{a}{b}> \\
\gcd(a, b) = 1
\end{aligned}$$

We can always have more rational numbers that are not generated by our "generator."

$$\begin{aligned}
\text{Let } D &= \mathbb{Z}_4 \oplus \mathbb{Z}_6 \\
D &= \{(a,b) | a \in \mathbb{Z}_4 \text{ and } b \in \mathbb{Z}_6\} \\
(a_1, b_1) \oplus (a_2, b_2) &= (a_1 +_4 a_2, b_1 +_6 b_2) \\
|(a,b)| &= \text{lcm}\,[|a|, |b|]
\end{aligned}$$

$$\begin{aligned}
D &\text{ is not cyclic, but it is Abelian} \\
(\mathbb{Z}_4, +) &\text{ is cyclic because } (\mathbb{Z}_n, +) \text{ is cyclic,} \\
(\mathbb{Z}_n, +) &= <1>
\end{aligned}$$

$$\begin{aligned}
|D| &= 6 \cdot 4 = 24 \\
D &\text{ has no elements of order } 24 \\
&\text{because lcm } (4,6) = 12
\end{aligned}$$

$$\begin{aligned}
<(1,1)> &\in \mathbb{Z}_4 \oplus \mathbb{Z}_6 \\
|(1,1)| &= \text{lcm } (|1|, |1|) \\
&= \text{lcm } (4,6) = 12
\end{aligned}$$

We will prove in the next homework that $\mathbb{Z}_n \oplus \mathbb{Z}_m$ is cyclic iff $\gcd(n,m) = 1$.

$$D = H \oplus K, |D| = |H| \times |K|$$

October 7th, 2020

Definition of a Symmetric Group (Permutation group S_n):

Let S be a finite set with n elements. This means that $S = \{1, 2, 3 \ldots, n\}$. Let $f: S \to S$ be a function such that f is bijective (both 1-1 and onto). Then:

$$S_n = \text{The set of all bijective functions from } S \text{ to } S$$

We can see that $(S_n, \circ)$ is a group. In fact, this is a non-Abelian group. How can we show this? Consider the following:

Closure: If we do the composition of two bijective functions, we will very obviously end up with another bijective function. This means that we have closure in this set.

Identity: Let $e = \text{identity map} \mid e(i) = i \quad \forall i \in S$. This means that $e: S \to S$.

Invertibility: If a function is bijective, meaning that it is both one to one and onto, that means that it is invertible. We know this result from Calculus I.

Associativity: This is clear and obvious.

$$w \in S_n \text{ means that } w: S \to S, w \text{ is a bijective function and } |S| = n$$

How do we write elements in S_n?

Let $a \in S_5$. Then:

$$a = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 3 & 1 & 5 & 2 \end{pmatrix}$$

The top line is the domain of the function, and the bottom line is the co-domain. In other words, we can see that $a(1) = 4, a(2) = 3, a(3) = 1, a(4) = 5, a(5) = 2$. This is a bijective function, as we mentioned before.

What is $|S_n|$?

$$\begin{pmatrix} 1 & 2 & 3 & .... & n \\ n \text{ possibilities} & n-1 \text{ possibilities} & n-2 \text{ possibilities} & & 1 \text{ possibility} \end{pmatrix}$$

$$|S_n| = n!$$

The symmetric / permutation group has exacty $n!$ elements. For example, $|S_4| = 4! = 24, |S_3| = 3! = 6$, and so on.

Let $a = (\ 1\ \ 4\ \ 5\ ) \in S_5$. This is a bijective function where a is a 3-cycle.

$$f: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 5 & 1 \end{pmatrix}$$

The elements cycle through to what they have been assigned. 1 goes to 4, 4 goes to 5 and 5 goes to 1, while the elements that were not mentioned in a simply map to themselves. This is obviously a bijective function. This is a short-hand notation for the functions in the symmetric groups. Let us take another example:

$$a = (\ 2\ \ 5\ \ 3\ \ 4\ ) \in S_6, \text{then } f: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 5 & 4 & 2 & 3 & 6 \end{pmatrix}. \text{ This is 4 cycles}$$

How do we find the order of a cycle? Consider $\alpha = (\ 2\ \ 3\ \ 7\ ) \in S_7$. This is again, 3-cycles. Note the following:

$$|\alpha| = 3$$

Now take the following:

$$\alpha \circ \alpha = (\ 2\ \ 3\ \ 7\ ) \circ (\ 2\ \ 3\ \ 7\ ) = (\ 2\ \ 7\ \ 3\ )$$

$$\alpha \circ \alpha \circ \alpha = (\ 2\ \ 7\ \ 3\ ) \circ (\ 2\ \ 3\ \ 7\ ) = (\ 2\ )(\ 3\ )(\ 7\ )$$

This is the identity map, because every element maps to itself.

How does this work? We go from RIGHT TO LEFT. For example, in $(\ 2\ \ 3\ \ 7\ ) \circ (\ 2\ \ 3\ \ 7\ )$, 7 maps to 2 and 2 maps to 3, therefore 7 maps to 3. 3 maps to 7 and 7 maps to 2, so 3 maps to 2. We proceed in the same manner. Always go from right to left to see what each element maps to w.r.t. the other cycles.

Fact: If we have an α that is m-cycle in S_n, then $|\alpha| = m$. Quickly, let us take an example:

$$\alpha = (\ 1\ \ 3\ \ 7\ \ 9\ \ 11\ ) \in S_{12}$$

Then clearly and quickly we can see that α is 5-cycle, and therefore $|\alpha| = 5$. This means that the minimum number of times we need to permute α with itself to get the identity function is 5 times. That's it. We cannot do it any less times. But what if we don't have the cycles?

Result: Let $f \in S_n$. Then f can be written as a composition of disjoint cycles. Let us first start with an example:

$$f: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 5 & 1 & 2 & 4 & 6 \end{pmatrix} \in S_6, f \text{ is not a cycle}$$

Then we can see the following:

$$f = (\ 1\ \ 3\ ) \circ (\ 2\ \ 5\ \ 4\ )$$

This uses the fact that the set is finite. How do we think of this as a function? Each element is a bijective function in the set of S_6. The two cycles have nothing in common. We can generalize this to be the following:

$$\alpha = (\ a_1\ \ a_2\ \ a_3\ \ \ldots\ \ a_k\ )$$

$$\beta = (\ b_1\ \ b_2\ \ b_3\ \ \ldots\ \ b_m\ )$$

We say that α, β are disjoint cycles iff $a_i \neq b_w\ \forall 1 \leqslant i \leqslant k$ and $\forall 1 \leqslant w \leqslant m$.

Let $\alpha = (\ 1\ \ 4\ \ 7\ )$ and $\beta = (\ 7\ \ 3\ \ 2\ )$. Obviously, a and β are not disjoint because there is a repeated element, 7. $|\alpha| = 3 = |\beta|$. This is a bijective function.

Example:

$$f: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 4 & 2 & 5 & 3 & 1 & 8 & 6 & 7 \end{pmatrix}$$

What can we write f as? $f = (\ 1\ \ 4\ \ 3\ \ 5\ ) \circ (\ 6\ \ 8\ \ 7\ )$. That's it. We have written the function as the composition of two disjoint cycles.

Result: α, β are two disjoint cycles. Then we can say that $\alpha \circ \beta = \beta \circ \alpha$.

First, consider s, where $s \notin \alpha$ and $s \notin \beta$. Then $\alpha \circ \beta(s) = s$, and $\beta \circ \alpha(s) = s$. The other cases are as follows: $s \in \alpha$ and $s \notin \beta$, in which case we have the following: $(\alpha \circ \beta)(s) = \alpha(\beta(s)) = \alpha(s)$. If we take $(\beta \circ \alpha)(s)$, we would get $\beta(\alpha(s)) = \alpha(s)$.

Similarly, if we have $s \notin \alpha$ and $s \in \beta$, then $(\alpha \circ \beta)(s) = \alpha(\beta(s)) = \beta(s)$ and $(\beta \circ \alpha)(s) = \beta(\alpha(s)) = \beta(s)$. This case is the same as the previous, by symmtery.

Result: Let $f \in S_n$. We know that $f = \alpha_1 \circ \alpha_2 \circ \cdots \circ \alpha_k$ of disjoint cycles (each α_i is a bijective function, but written as a cycle). Then:

$$|f| = \text{lcm}\,(|\alpha_1|, |\alpha_2|,\ \ldots, |\alpha_k|)$$

Why is this true?

Proof:

Find the smallest positive integer, m, st $f^m = f \circ f \circ f \circ \cdots \circ f = e$. This is repeated m times. We already know that: $f = \alpha_1 \circ \alpha_2 \circ \cdots \circ \alpha_k$. let $m_i = |\alpha_i|$, for $1 \leqslant i \leqslant k$ and $m = |f|$. Each $m_i | m$. We need to find an integer that is divisible by each of our m_i, and this by definition is the lcm.

$$m = \text{lcm}\,(m_1, m_2, \ldots, m_k)$$

Example:

$$f: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ 6 & 4 & 8 & 5 & 1 & 2 & 3 & 7 \end{pmatrix}$$

We want to find $|f|$. The first thing we do is write f as a composition of disjoint cycles.

$$f = (\ 1\ \ 6\ \ 2\ \ 4\ \ 5\ ) \circ (\ 3\ \ 8\ \ 7\ )$$

We have written f as the composition of two disjoint sets, and thus it is easy to find the order of f. We simply note the following: $|f| = \text{lcm}\,(|a_1|, |a_2|) = \text{lcm}\,(5, 3) = 15$. We are done.

October 12th, 2020

Definition of Even Permutations:

Let $f \in S_n$. f is called an even permutation if $f =$ composition of an even number of 2-cycles. For example, let us take:

$$(\ 1\ \ 2\ \ 3\ ) = (\ 1\ \ 3\ ) \circ (\ 1\ \ 2\ )$$

This is an even permutation, or an even function. This is true because we can take our f and write it as two 2-cycles.

Result: $f \in S_n$. Assume $f =$ composition of an even number of 2-cycles. Then if $f =$ compositions of 2-cycles, then the number of the 2-cycles is an even number. If we write f as the composition of an even number of 2-cycles, when we rewrite and try to find another composition of 2-cycles, the number of 2-cycles stays even. We can never write f as an odd number of 2-cycles, but it is definitely not unique either.

Fact: If we have some $(\ a_1\ \ a_2\ \ a_3\ \ \ldots\ \ a_m\ )$, then we can say the following (for an m-cycle):

$$(\ a_1\ \ a_2\ \ a_3\ \ \ldots\ \ a_m\ ) = (\ a_1\ \ a_m\ ) \circ (\ a_1\ \ a_{m-1}\ ) \circ (\ a_1\ \ a_{m-2}\ ) \circ \cdots \circ (\ a_1\ \ a_2\ )$$

This is a way to write an m-cycle as a composition of 2-cycles.

For example, let us take the following example:

$$\alpha = (\ 2\ \ 3\ \ 6\ \ 8\ ) \in S_8. \text{ Is } \alpha \text{ an even permutation?}$$

$$\alpha = (\ 2\ \ 8\ ) \circ (\ 2\ \ 6\ ) \circ (\ 2\ \ 3\ )$$

We have written α has the composition of 2-cycles, but the total number of 2-cycles is 3. This is an odd number, and therefore α is not an even permutation.

Note: The identity map, e, is an even permutation conventionally.

Fact: Let α be an m-cycle. If m is odd, then α is an even permutation. Moreover, if m is even, then α is an odd permutation.

Proof:

$$(\ m_1\ \ m_2\ \ m_3\ \ \ldots\ \ m_m\ ) = (\ m_1\ \ m_m\ ) \circ (\ m_1\ \ m_{m-1}\ ) \circ \cdots \circ (\ m_1\ \ m_2\ )$$

In this case, we have exactly $m - 1$ 2-cycles, and thus if m was even, we'd have an odd number of 2-cycles, and if m was odd, we'd have an even number of 2-cycles.

But what if our function is not written as a cycle? Consider the following example:

$$f: \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 5 & 1 & 3 & 2 & 6 \end{pmatrix} \in S_6$$

Then we can rewrite f as the following:

$$f = (\ 1\ \ 4\ \ 3\ ) \circ (\ 2\ \ 5\ )$$

Then we expand the 3-cycle to be the following: $(\ 1\ \ 4\ \ 3\ ) = (\ 1\ \ 3\ ) \circ (\ 1\ \ 4\ )$. And thus, f becomes the following:

$$f = (\ 1\ \ 3\ ) \circ (\ 1\ \ 4\ ) \circ (\ 2\ \ 5\ )$$

This is 3 (odd number) of 2-cycles, which means that f is not an even permutation, because we used 3 2-cycles.

Result: Let $n \geqslant 2$. A_n is a subgroup of S_n, where A_n is the set of all even permutations of S_n. How do we need to prove this? Since we know that S_n is a group, then we need to only show closure to see that A_n is a subgroup, because A_n is finite.

Proof:

Let $f_1, f_2 \in A_n$. Hence $f_1 =$ composition of an even number, n_1 of 2-cycles. Furthermore, $f_2 =$ composition of an even number, n_2, of 2-cycles. Then:

$$f_1 \circ f_2 = \text{composition of } (n_1 + n_2) \text{ of 2-cycles}$$

The addition of two even numbers is an even number, which means that $f_1 \circ f_2$ will stay in A_n. Therefore, we know that A_n is closed under the binary operation $\circ$, and therefore it is a subgroup.

Result: $|A_n| = \frac{n!}{2}$. Recall that $|S_n| = n!$, this result proves that half the permutations of S_n are even and the other half of them are odd. How do we convince ourselves of this?

Proof:

Let $|A_n| = m$. We want to show that:

$$m = \frac{n!}{2}$$

Form $(\ 1\ \ 2\ ) \circ A_n$. This is a left coset of A_n. Let us call it F. This left coset is not the same as A_n. This is because $(\ 1\ \ 2\ ) \notin A_n$. Claim that $F =$ set of all odd permutations. We only need to show that $F = (\ 1\ \ 2\ ) \circ A_n$ is the set of all odd permutations of S_n.

$$\begin{aligned} &\text{Let } f \text{ be an odd permutation} \\ &\qquad \text{Show that } f \in F \\ &\qquad f = (\ 1\ \ 2\ ) \circ k \quad \text{where } k \in S_n \\ &= (\ 1\ \ 2\ ) \circ (\ 1\ \ 2\ ) \circ f \\ &\qquad (\ 1\ \ 2\ )^2 = e \\ &= e \circ f = f \end{aligned}$$

$$\begin{aligned} k = (\ 1\ \ 2\ ) \circ f &\text{ is an even permutation} \\ \implies f = (\ 1\ \ 2\ ) \circ k, k \in A_n \\ \implies f \in F \end{aligned}$$

This means that every odd permutation lives in F.

$$S_n = F \cup A_n$$

We know that $|A_n| = m = |F|$, and so $|S_n| = m + m = 2m = n!$. Therefore:

$$m = \frac{n!}{2}$$

We have also established that A_n has exactly two left cosets. One is A_n itself, and the other is the set of all odd permutations.

Result: Let $(D, \cdot)$ be a group, and $H < D$, meaning that H is a subgroup of D. Assume that $\frac{|D|}{|H|} = 2$. In this case, $H \lhd D$. This means that H is a normal subgroup of D.

In fact, $\frac{|D|}{|H|} = [H : D]$, and is called the index of H in D. $[H : D]$ = number of all distinct left cosets of H. This is the same as the number of all distinct right cosets of H.

We need to show that if $[H : D] = 2$, then $H \lhd D$. In street language, if a set has exactly two left cosets, then it is a normal subgroup of D.

Proof: Since $\frac{|D|}{|H|} = 2$, then H has exactly two left cosets, say $a \cdot H$, and it also have 2 right cosets, say $H \cdot b$. Then we know that:

$$D = H \cup a \cdot H \quad \forall a \in D \backslash H$$

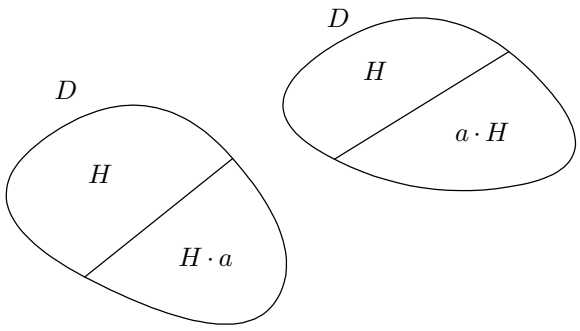
We also know that:

$$D = H \cup H \cdot a \quad \forall a \in D \backslash H$$

We need to show that $a \cdot H = H \cdot b \quad \forall a, b \in D$. If $a \in H$, then there is nothing to prove since $a \cdot H = H \cdot a$. Now let us take a outside of H, ie $a \in D \backslash H$. We show that $a \cdot H = H \cdot a$.

$$\begin{aligned} &\text{Since } D = H \cup a \cdot H \text{ and } D = H \cup H \cdot b \\ &\text{We conlcude that } a \cdot H = H \cdot a \end{aligned}$$

We can also show this graphically:



This implies that the two regions of $a \cdot H$ and $H \cdot a$ are the same, beacuse inside of D, H remains the same in both graphs.

Result: Linking this back to our previous discussion, we can conlcude that $A_n \lhd S_n$. A_n is a normal subgroup of S_n.

Proof:

$$|A_n| = \frac{n!}{2}, |S_n| = n!$$
$$[A_n : S_n] = 2 = \frac{|A_n|}{|S_n|}$$
$$\implies A_n \lhd S_n \text{ by our previous result}$$

Therefore, in addition to A_n being a subgroup of S_n, we also know now that it is indeed a normal subgroup.

Definition of the Center of a Group:

Let $(D, \cdot)$ be a group. Then the center of D, denoted by $C(D)$ or $Z(D)$ is given by the following:

$$C(D) = \{a \in D | a \cdot b = b \cdot a \quad \forall b \in D\}$$

In street language, we can see that the center of D is the set of all elements in D that commute with every element in D. There are some elements in the group that commute with all elements in D, and these elements are called the center of D.

Note that if D is an Abelian group, then the center of D is simply D itself, because every element commutes with every other element.

Take S_n with $n \geqslant 3$. Our claim here is that this group is non-Abelian. How do we prove this?

Proof:

$$\begin{pmatrix} 1 & 2 \end{pmatrix} = \alpha \text{ and } \begin{pmatrix} 1 & 3 \end{pmatrix} = \beta \in S_n \quad n \geqslant 3$$
$$\text{Let us calculate } \alpha \circ \beta$$
$$\alpha \circ \beta = \begin{pmatrix} 1 & 2 \end{pmatrix} \circ \begin{pmatrix} 1 & 3 \end{pmatrix} = \begin{pmatrix} 1 & 3 & 2 \end{pmatrix}$$
$$\text{Let us calculate } \beta \circ \alpha$$
$$\beta \circ \alpha = \begin{pmatrix} 1 & 3 \end{pmatrix} \circ \begin{pmatrix} 1 & 2 \end{pmatrix} = \begin{pmatrix} 1 & 2 & 3 \end{pmatrix}$$

Clearly these two elements are not the same and this is enough to show that S_n is non-Abelian when we have $n \geqslant 3$.

October 14th, 2020

Recall the definition of the center of a group. Note again that if a group is Abelian, the center of a group is the group itself. ie.:

$$C(D) = D$$

This means that the center of the group is mostly only interesting for non-Abelian groups. Now, we proceed with the following result:

Result: $(D, \cdot)$ is a group. Assume that $a \cdot b = b \cdot a$ for some $a, b \in D$. Then we have the following result:

$$a^{-1} \cdot b = b \cdot a^{-1}$$

This means that if a commutes with b, then the inverse of a would also commute with b.

Proof:

$$\begin{aligned}
\text{We know that } (a \cdot b)^{-1} \cdot (a \cdot b) &= e \\
b^{-1} \cdot a^{-1} \cdot (a \cdot b) &= e \\
b^{-1} \cdot a^{-1} \cdot (b \cdot a) &= e \\
(b^{-1} \cdot a^{-1} \cdot (b \cdot a)) \cdot a^{-1} &= e \cdot a^{-1} \\
= b^{-1} \cdot a^{-1} \cdot b \cdot e &= a^{-1} \\
b \cdot (b^{-1} \cdot a^{-1} \cdot b) &= b \cdot a^{-1} \\
= a^{-1} \cdot b &= b \cdot a^{-1}
\end{aligned}$$

Therefore we have shown that:

$$a^{-1} \cdot b = b \cdot a^{-1}$$

Result: Assume that $(D, \cdot)$ is a group. Then we can say that $C(D)$ is a subgroup of D.

Proof:

$$\begin{aligned}
\text{Let } a, b \in C(D) \\
\text{We want to show that } a^{-1} \cdot b \in C(D) \\
\text{Since } a \in C(D), a^{-1} \in C(D) \\
\text{This is by the previous result, proven above}
\end{aligned}$$

$$\begin{aligned}
\text{Let } h \in D \\
\text{Then } (a^{-1} \cdot h \cdot b) = a^{-1} \cdot h \cdot b &= a^{-1} \cdot h \cdot b \\
= h \cdot a^{-1} \cdot b \\
(a^{-1} \cdot b) \cdot h = h \cdot (a^{-1} \cdot b)
\end{aligned}$$

This means that since h is randomly selected in D, and since it commutes with $a^{-1} \cdot b$, then we can conclude that:

$$a^{-1} \cdot b \in C(D)$$

Result^{+}: Let $(D, \cdot)$ be a group. Then the center of $D, C(D)$ is a normal subgroup of D. This is a $+$ because we expand upon the previous result.

Proof: We already know that $C(D) < D$. Let $a \in D$. We will show that $a \cdot C(D) = C(D) \cdot a$.

$$\begin{aligned}
&\text{Since each element in } C(D) \\
&\text{commutes with each element in } D, \\
&\text{then } C(D) \cdot a = a \cdot C(D)
\end{aligned}$$

Result: Let $(D, \cdot)$ be a group. If $D/C(D)$ is a cyclic group, then we conclude that D is an Abelian group. If the left coset of the center of D is generated by one element, then the original group has to be Abelian.

Proof: Let $x, y \in D$. We want to show that $x \cdot y = y \cdot x$.

$$\begin{aligned}
&\text{Since } D/C(D) \text{ is cyclic, we know that:} \\
&\exists a \in D \text{ st } D/C(D) = <a \cdot C(D)> \\
&\text{ie } D/C(D) \text{ is generated by a left coset}
\end{aligned}$$

$$\begin{aligned}
\text{Hence } x \cdot C(D) &\in [a \cdot C(D)]^n \quad n \in \mathbb{Z} \\
\text{Because } x \cdot C(D) &\text{ is a left coset} \\
\text{and all left cosets are generated by } &a \cdot C(D)
\end{aligned}$$

$$\begin{aligned}
&= a^n \cdot C(D) \\
\text{Similarly, } y \cdot C(D) &= [a \cdot C(D)]^m \quad m \in \mathbb{Z} \\
&= a^m \cdot C(D)
\end{aligned}$$

$$\begin{aligned}
x &= a^n \cdot k_1 \quad k_1 \in C(D) \\
y &= a^m \cdot k_2 \quad k_2 \in C(D) \\
x \cdot y &= a^n \cdot k_1 \cdot a^m \cdot k_2 \\
&= a^n \cdot a^m \cdot k_1 \cdot k_2 \\
&= a^m \cdot a^n \cdot k_2 \cdot k_1 \\
&= a^m \cdot k_2 \cdot a^n \cdot k_1 \\
&= y \cdot x
\end{aligned}$$

We established that D is an Abelian group.

Result: Let $(D, \cdot)$ be a group st $|D| = q^n$ where q is a prime. Then our result is that the cardinality of the center of the group is greater or equal to q.

$$|C(D)| \geqslant q$$

This is going to be covered in more depth when we consider Congruancy groups, but for now, we can simply use it in exams and homeworks without having to know the proof.

Result: Let $(D, \cdot)$ be a group st $|D| = q^2$ for some prime number, q. Then our result is that D is Abelian.

Proof: By the previous result, $|C(D)| = q$ or q^2. Why is this true? The order of the subgroup has to be a factor of the order of D, which means that the only two possibilities for it are q and q^2 since the previous result just showed us that $|C(D)| \geqslant q$ and q is prime.

$$\begin{aligned}
&\text{If } |C(D)| = q^2, \\
&\text{the center of } D \text{ is the whole group} \\
&\text{All elements commute with each other} \\
&D \text{ is Abelian}
\end{aligned}$$

Now we assume the other case:

$$|C(D)| = q$$
$$\text{Since } C(D) \lhd D, \frac{D}{C(D)} \text{ is a group}$$
$$\text{Hence } \left|\frac{D}{C(D)}\right| = \frac{|D|}{|C(D)|} = q$$
$$\text{Thus } D/C(D) \text{ is a group with } q \text{ elements}$$
$$\text{Remember that } q \text{ is prime}$$
$$\Longrightarrow D/C(D) \text{ is cyclic}$$
$$\text{By a previous result introduced in this lecture,}$$
$$\text{if } D/C(D) \text{ is cyclic, then } D \text{ is Abelian.}$$

Therefore, in either case, if we have the cardinality of a group being equal to a prime squared, then our group is Abelian no matter what.

.....

Result for those that are interested:

$$\text{We know } S_3 = D_3$$
$$\text{Consider the symmetry group on a } \ 4-\text{gon}$$
$$D_4 \text{ is a subgroup of } S_4$$
$$|S_4| = 4! = 24, \text{ and } |D_4| = 8$$

In general, we can have the following:

$$\text{Let } D_n \text{ be the symmetric group on an } n-\text{gon}$$
$$\text{Then } |D_n| = 2n$$

Note that for an n-gon, the shape is divided so that each angle is divided equally from the center of the shape. This means that each angle is equal to: $\frac{360}{n}$ degrees.

Let us consider D_6. This means we are acting on a 6-gon. For the rotations, we have $\frac{360}{n}, \frac{360}{2n}, \ldots$. and for the reflections, we have to draw them and see. However, overall we can see that we have a total of n rotations and n reflections. In our case, D_6 has a total of 12 symmetries. Furthermore, we will never get out of this set. This is because the composition of as many reflections or rotations is still going to result in a symmetry inside the set D_n

.....

Definition of Group Homomorphism:

Let us consider the following function:

$$f\colon (D, \cdot) \to (W, *), \text{where } (D, \cdot) \text{ and } (W, *) \text{ are groups}$$

We say that f is a group homomorphism iff $f(a \cdot b) = f(a) * f(b)\ \forall a, b \in D$.

October 19th, 2020

Group Homomorphism:

Def:

$$f\colon (D, \cdot) \to (F, *)$$

is called a group-homomorphism iff $f(d_1 \cdot d_2) = f(d_1) * f(d_2)\ \forall d_1, d_2 \in D$. This is simply recalling from the last lecture.

Result:

$f\colon (D,\cdot)\to(F,*)$ is a group-homomorphism. Then we have the following results:

1. $f(e_D)=e_F$. The identity in D should map with the identity in F
2. $f(a^{-1})=[f(a)]^{-1}\quad\forall a\in D$
3. $f(a^n)=[f(a)]^n\quad\forall n\in\mathbb{Z}$

$$f(a\cdot a\cdot a\cdot a\cdot\cdots\cdot a)=f(a)*f(a)*f(a)*\cdots*f(a)$$

4. Assume $|a|=m$. Then we can say that $|f(a)|\,|m$ (the order of $f(a)$ divides the order of a). Furthermore, $|a|$ does not need to equal $|f(a)|$.

Proof(s):

1.

$$\text{We show that } f(e_D)=e_F$$

$$f(e_D)=f(e_D\cdot e_D)=\underline{f(e_D)*f(e_D)}$$
$$\text{This is since } f \text{ is group homomorphism}$$

$$f(e_D)=f(e_D)*f(e_D)$$
$$\text{Since } f \text{ is a group:}$$
$$f^{-1}(e_D)*[f(e_D)=f(e_D)*f(e_D)]$$
$$\Longrightarrow f^{-1}(e_D)*f(e_D)=f^{-1}(e_D)*f(e_D)*f(e_D)$$
$$\text{Note that } f^{-1}(e_D)*f(e_D)=e_F$$
$$\text{Therefore:}$$
$$e_F=e_F*f(e_D)$$
$$=f(e_D)$$

2.

$$\text{We show that } f(a^{-1})=[f(a)]^{-1}$$

$$e_F=f(e_D)=f(a\cdot a^{-1})=f(a)*f(a^{-1})$$
$$\Longrightarrow[f(a)]^{-1}=f(a^{-1})$$

3.

$$\text{We show that } f(a^n)=[f(a)]^n\quad\forall n\in\mathbb{Z}$$

$$\text{Assume } n\in\mathbb{Z}^+$$
$$f(a^n)=f(a\cdot a\cdot a\cdot\cdots\cdot a)$$
$$=f(a)*f(a)*f(a)*\cdots*f(a)$$
$$=[f(a)]^n$$

$$\text{Now assume } n\in\mathbb{Z}^-$$
$$f(a^n)=f((a^{-1})^{-n})=[[f(a)]^{-1}]^{-n}$$
$$=f(a^{-1})*f(a^{-1})*f(a^{-1})*\cdots*f(a^{-1})\quad -n\text{ times}$$
$$=[f(a)]^n$$

4.

$$\begin{aligned}
\text{Assume } |a| = m < \infty \text{ and } |f(a)| = n \\
\text{We show that } n|m \\
|a| = m \Longrightarrow a^m = e_D \\
e_F = f(e_D) = f(a^m) = [f(a)]^m \\
[f(a)]^m = e \\
\Longrightarrow n|m \\
n \text{ is a factor of } m
\end{aligned}$$

Def:

$$f: (D, \cdot) \to (F, *)$$

Assume that f is a group homomorphism. The Kernel of f, denoted by $\ker(f)$ is given by the following:

$$\ker(f) = \{d \in D |\ f(d) = e_F\}$$

$\ker(f)$ is the set of all elements in D that map to the identity of F, e_F.

Result:

Given that $f: (D, \cdot) \to (F, *)$ is a group homomorphism, then:

$$\ker(f) \lhd D$$

This means that the kernel of f is a normal subgroup of D. If D is Abelian, this is trivial.

Proof:

$$\begin{aligned}
\text{First we show that } \ker(f) < D \\
\text{Let } a, b \in \ker(f). \text{ We show } a^{-1} \cdot b \in \ker(f) \\
\text{In other words:} \\
f(a^{-1} \cdot b) = e_F \\
\text{This is how we show an element is in } \ker(f)
\end{aligned}$$

$$\begin{aligned}
\text{Since } a, b \in \ker(f), \\
f(a) = f(b) = e_F
\end{aligned}$$

$$\begin{aligned}
\text{We know that } f(a^{-1}) = [f(a)]^{-1} \\
\text{Since } f(a) = e_F,\ f(a^{-1}) = e_F^{-1} = e_F
\end{aligned}$$

$$\begin{aligned}
\text{Hence } f(a^{-1} \cdot b) = f(a^{-1}) * f(b) \\
= e_F * e_F = e_F \\
\Longrightarrow a^{-1} \cdot b \in \ker(f) \\
\text{Therefore } \ker(f) < D
\end{aligned}$$

$$\begin{aligned}
\text{Now we show that } \ker(f) \lhd D \\
\text{Show } \forall b \in D, b \cdot \ker(f) = \ker(f) \cdot b \\
\Longleftrightarrow \forall b \in D, b \cdot \ker(f) \cdot b^{-1} = \ker(f)
\end{aligned}$$

$$
\begin{aligned}
&\text{Let } x \in \ker(f)\\
&\text{Show that } b\cdot y\cdot b^{-1} = x \text{ for some } y \in \ker(f)\\
&\text{Let } y = b^{-1}\cdot x\cdot b\\
f(y) = f(b^{-1}\cdot x\cdot b) &= f(b^{-1}) * f(x) * f(b)\\
&= f(b^{-1}) * e_F * f(b)\\
&= f(b^{-1}) * f(b) = e_F
\end{aligned}
$$

$$
\begin{aligned}
&\text{Check if } x = b\cdot y\cdot b^{-1}\\
x &= b\cdot b^{-1}\cdot x\cdot b\cdot b^{-1}\\
&= x
\end{aligned}
$$

$$
\begin{aligned}
&\Longrightarrow \ker(f) \subseteq b\cdot\ker(f)\cdot b^{-1}\\
&\text{Choose } w \in b\cdot\ker(f)\cdot b^{-1}\\
&\text{Show that } w \in \ker(f)
\end{aligned}
$$

$$
\begin{aligned}
&\text{Since } w \in b\cdot\ker(f)\cdot b^{-1}, \exists d \in \ker(f)\\
&\text{st } w = b\cdot d\cdot b^{-1}\\
&\text{We show that } f(w) = e_F\\
f(w) = f(b\cdot d\cdot b^{-1}) &= f(b) * f(d) * f(b^{-1})\\
&= f(b) * e_F * f(b^{-1})\\
&= e_F
\end{aligned}
$$

$$
\text{Therefore } w \in \ker(f)
$$

Recall that for a function, $f\colon (D,\cdot) \to (F,*)$, our $(D,\cdot)$ is the domain, and the $(F,*)$ is the co-domain. This means that the range is a subset of F. range $\subseteq F$, and so range$(f) < F$.

October 21st, 2020

Result: Consider the following group homomorphism:

$$f\colon (D,\cdot) \to (W,*)$$

Then we can say that range$(f) < W$. The range of f is a subgroup of W.

Proof:

$$
\begin{aligned}
&\text{Let } a, b \in \text{range}(f)\\
&\text{Show } a^{-1} * b \in \text{range}(f)
\end{aligned}
$$

$$
\begin{aligned}
&\text{Since } a, b \in \text{range}(f), \exists x, y \in D \text{ st } f(x) = a \text{ and } f(y) = b\\
&\text{Hence } f(x^{-1}) = [f(x)]^{-1} = a^{-1}\\
&\text{Thus } f(x^{-1}\cdot y) = f(x^{-1}) * f(y) = a^{-1} * b\\
&\Longrightarrow a^{-1} * b \in \text{range}(f)
\end{aligned}
$$

Isomorphism:

$$f\colon (D,\cdot) \to (W,*)$$

is a group homomorphism. We say that f is a group isomorphism iff f is a bijective function. This means that f is both one-to-one and onto.

If two groups form an isomorphism, this means that they share the same structure. If prof. Badawi comes into class next week and his name is Mike, the only thing that has changed is his name. Everything else is the same - he still teaches us Abstract Algebra, etc.

If D and W are isomorphic, if D has 1,000,000 elements, then W has 1,000,000 elements, and so on. However, the names of the elements are different. It is their structure that stays the same.

Result [Big]:

Assume we have $f: (D, \cdot) \to (W, *)$ is a group homomorphism. Then:

$$D/\ker(f) \approx \text{range}(f)$$

$\approx$ means that they are isomorphic to one another. We are saying that the group $D/\ker(f)$ is isomorphic to range(f).

Proof:

We need to construct a map, K, where $K: D/\ker(f) \to \text{range}(f)$ st K is a group homomorphism, is one-to-one and onto. If we can construct such a mapping, then we are done.

$$\begin{aligned} f: (D, \cdot) &\to (W, *) \\ K: (D/\ker(f), \cdot') &\to \text{range}(f) \\ K(a \cdot \ker(f)) &= f(a) \qquad \forall a \cdot \ker(f) \in D/\ker(f), a \in D \\ f(a) \in W &, \text{and } f(a) \in \text{range}(f) \end{aligned}$$

$$\begin{aligned} &\text{Consider the following:} \\ &K(a \cdot \ker(f) \cdot' b \cdot \ker(f)) \\ =&K(a \cdot b \cdot \ker(f)) = f(a \cdot b) \\ =&f(a) * f(b) = K(a \cdot \ker(f)) * K(b \cdot \ker(f)) \\ \implies &K \text{ is a group homomorphism} \end{aligned}$$

$$\text{We show that } K \text{ is } 1-1 \text{ and onto}$$

$$\begin{aligned} &\text{Onto:} \\ &\text{Let } y \in \text{range}(f). \text{ Hence } \exists x \in D \text{ st} \\ &f(x) = y \\ &\text{Thus } K(x \cdot \ker(f)) = f(x) = y \\ &\text{Therefore we have shown that} \\ &\text{for all elements in the range,} \\ &\text{we have some element in } D \\ &\text{that maps to it} \end{aligned}$$

$$\begin{aligned} &1-1: \\ &\text{Assume } K(a \cdot \ker(f)) = K(b \cdot \ker(f)) \\ &\text{Show that } a \cdot \ker(f) = b \cdot \ker(f) \\ &\text{We have:} \\ &K(a \cdot \ker(f)) = K(b \cdot \ker(f)) \\ &K(a \cdot \ker(f)) = f(a) \end{aligned}$$

$$K(b \cdot \ker(f)) = f(b)$$
$$\text{ie } f(a) = f(b)$$

Take this right operation:
$$f(a) * f(b^{-1}) = f(b) * f(b^{-1})$$
$$f(a) * [f(b)]^{-1} = e_W \in \text{range}(f)$$
$$f(a) * f(b^{-1}) = e_W$$
$$f(a \cdot b^{-1}) = e_W$$
since f is group homomorphism
$$\implies a \cdot b^{-1} \in \ker(f)$$
$$\implies a \cdot \ker(f) = b \cdot \ker(f)$$

Therefore, K is $1-1$

Question: Assume that $f: (D, \cdot) \to (W, *)$ is a group homomorphism. Also, assume that $|D| = n < \infty$, and $|\text{range}(f)| = m < \infty$. Prove that $m|n$. Remember that $\text{range}(f) < W$. We want to prove that the cardinality of the range is a factor of the cardinality of D.

Proof: We know that $D/\ker(f) \approx \text{range}(f)$. Since they are isomorphic:

$$|D/\ker(f)| = |\text{range}(f)|$$

Then we can easily see the following:

$$\frac{|D|}{|\ker(f)|} = |\text{range}(f)| \implies |D| = |\text{range}(f)| \times |\ker(f)|$$
$$\text{in other words:}$$
$$n = |\ker(f)| \times m$$

Therefore, we have shown that m is a factor of n, or the cardinality of the range is a factor of the cardinality of D.

Question: $f: (\mathbb{Z}_{10}, +) \to (\mathbb{Z}_{21}, +)$ is a group homomorphism. For each $a \in \mathbb{Z}_{10}$, find its image, or $f(a)$. We want to find the image of every element in $\mathbb{Z}_{10}$.

Proof: We know that $|\text{range}(f)|$ is a factor of $|\mathbb{Z}_{10}| = 10$. This is by the result we just proved. Also, we know that the range of f has to be a subgroup of $(\mathbb{Z}_{21}, +)$. So $|\text{range}(f)| \,|\, |\mathbb{Z}_{21}| = 21$.

$$\implies \text{What is the number that is}$$
$$\text{the factor of 21 and 10?}$$
$$= 1$$

Therefore, we conclude that $|\text{range}(f)| = 1$. The subgroup that contains only one element is the subgroup that contains only the identity. So we have the following:

$$f: (\mathbb{Z}_{10}, +) \to (\mathbb{Z}_{21}, +)$$

is a group homomorphism, and $f(a) = 0 \forall a \in \mathbb{Z}_{10}$. This is called the trivial group homomorphism. Every element in the domain maps to the identity of the co-domain.

Question: $f: (\mathbb{Z}_{14}, +) \to (\mathbb{Z}_{35}, +)$ is a non-trivial group homomorphism. Find $\text{range}(f)$ and $\ker(f)$. This means that there exists at least one element in the domain that maps to an element in $\mathbb{Z}_{35}$ that is NOT 0.

Proof: Firstly, we need to observe that $|\text{range}(f)| = 7$ because it has to be a factor of 35 and 14, so it is either 1 or 7. However, we know that it is a non-trivial group homomorphism, so it must be 7.

$$\begin{aligned}
\text{range}(f) &< (\mathbb{Z}_{35}, +) \\
(\mathbb{Z}_{35}, +), \exists! \text{ subgroup of } \mathbb{Z}_{35} &\text{ with 7 elements} \\
\mathbb{Z}_{35} &= <1> \\
|5| = |1^5| &= \frac{35}{\gcd(5, 35)} = 7
\end{aligned}$$

$$\begin{aligned}
\text{Therefore range}(f) &= <5> \\
&= \{0, 5, 10, 15, 20, 25, 30\}
\end{aligned}$$

Now, to find the kernel:

$$\begin{aligned}
\frac{|D|}{|\ker(f)|} &= |\text{range}(f)| \\
\text{because } D/\ker(f) &\approx \text{range}(f)
\end{aligned}$$

$$\begin{aligned}
\frac{14}{|\ker(f)|} &= 7 \\
|\ker(f)| &= 2 \\
\text{How many subgroups with 2 elements do we have in } \mathbb{Z}_{14}&? \\
1 &
\end{aligned}$$

$$\implies \ker(f) = \{0, 7\}$$

October 26th, 2020

Let us take a linear differential equation:

$$y'' = 3y' + 7y = \sin(t)\, e^t$$

Take a mapping of the following form:

$$f: \text{all cont. diff. functions} \longrightarrow K$$

K is indeed a vector space, and it is therefore an Abelian group. Now consider the following:

$$f(h(t)) = h'' + 3h' + 7h \quad \forall h \in K$$

f is a group homomorphism. This is because it satisfies all the requirements for group homomorphism, which means that we can see that $f(h_1 + h_2) = f(h_1) + f(h_2)$. This is clear.

Since f is a group homomorphism, we porve that:

$$K/\ker(f) \approx \text{range}(f) \qquad \text{(They are isomorphic)}$$

Recall that isomorphic means that they have the safe group structure. We know that $K/\ker(f)$ is a group because K is Abelian and $\ker(f)$ is always a normal subgroup to K.

Also recall that $\ker(f) = \{\text{set of all elements in } K \text{ that map to } e = 0\}$. If we want to find what $\ker(f)$ is, we need to see the definition of our function, f. We need to find all $h \in K$ st $f(h) = e = 0$.

By our function, we have $\sin(t)\, e^t$, which is in the range of f. Recall this from the Wednesday lecture:

$$K_1 \colon K/\ker(f) \longrightarrow \text{range}(f) \text{ st:}$$

$$\begin{aligned}
K_1(f_1 + \ker(f)) &= f(f_1) \\
\Longrightarrow &\exists! \text{ left coset, say } f_1 + \ker(f) \text{ st} \\
K_1(f_1 + \ker(f)) &= f(f_1) \longrightarrow \sin(t)\, e^t \\
&\text{each element in the left coset will} \\
&\text{map to the same function, for } f_1,\, f_2,\, f_3,\, \ldots. \\
&\text{we want } f(f_1) = \sin(t)\, e^t \\
f(h) &= h'' + 3h' + 7h \\
K_1(f_1 + \ker(f)) &= f(f_1) = \sin(t) \times e^t \\
&\text{each element in } f_1 + \ker(f) \text{ will map} \\
&\text{to } \sin(t)\, e^t \\
&\text{To find } f_1,\, f_1'' + 3f_1' + 7f_1 = \sin(t)\, e^t \\
&\text{in DE, this is our } y_p \,(y \text{ particular})
\end{aligned}$$

In general, whenever we write $D \approx L$, this means that each element in D corresponds to exactly one element in L. It means that we have a function, $f \colon D \longrightarrow L$ st f is group homomorphism, and f is 1-1 and onto.

Result: $f \colon (D, \cdot) \longrightarrow (W, *)$ is a group homomorphism. f is 1-1iff $\ker(f) = e_D$. This is true for any group homomorphism.

Proof:

$$\begin{aligned}
&\Longrightarrow \\
&\text{Assume } f \text{ is } 1-1 \\
&\text{Show } \ker(f) = \{e_D\} \\
&\text{We know that } e_D \in \ker(f) \text{ since } f(e_D) = f(e_W) \\
&\text{since } f \text{ is } 1-1 \text{ and } f(e_D) = f(e_W), \\
&\text{we conclude that } \ker(f) = \{e_D\}
\end{aligned}$$

$$\begin{aligned}
&\Longleftarrow \\
&\text{Assume } \ker(f) = \{e_D\} \\
&\text{Show that } f \text{ is } 1-1 \\
&\text{Assume } f(a) = f(b), \text{prove that } a = b \\
&f(b) \in W \\
&[f(a) = f(b)] * [f(b)]^{-1} \\
&f(a) * [f(b)]^{-1} = f(b) * [f(b)]^{-1} \\
&\Rightarrow f(a) * f(b)^{-1} = e_W \\
&f(a \cdot b^{-1}) = e_W \\
&\Longrightarrow a \cdot b^{-1} \in \ker(f) \\
&\text{Since } a \cdot b^{-1} \in \ker(f) \text{and } \ker(f) = \{e_D\}, \text{we conclude:} \\
&a \cdot b^{-1} = e_D \\
&a \cdot b^{-1} \cdot b = e_D \cdot b \\
&a = b
\end{aligned}$$

Result: Let D be a finite cyclic group with $n < \infty$ elements. Then $D \approx (\mathbb{Z}_n, +)$. This means that every cyclic and thus Abelian group is isomorphic to $(\mathbb{Z}_n, +)$.

Proof: We build the following function:

$$f: D \longrightarrow (\mathbb{Z}_n, +)$$

st f is a group homomorphism. Then we show that f is 1-1 and onto.

Since D is cyclic with n elements, $\exists a \in D$ st $|a| = n$ and $D = <a>$. We know that $(\mathbb{Z}_n, +)$ is cyclic and $|1| = n$, with $(\mathbb{Z}_n, +) = <1>$.

$$\begin{aligned}
f: D &\longrightarrow (\mathbb{Z}_n, +) \\
f(a^k) = 1^k = k &\quad \forall 1 \leqslant k \leqslant n \\
f(a \cdot a \cdot a \cdot \cdots \cdot a) &= (1 + 1 + 1 + \cdots + 1) \\
\text{Let } x, y \in D. \text{ Show that } f(x \cdot y) &= f(x) + f(y) \\
x, y \in D, x = a^{m_1}, y &= a^{m_2} \\
f(x \cdot y) &= f(a^{m_1} \cdot a^{m_2}) \\
&= 1^{m_1 + m_2} = 1^{m_1} + 1^{m_2} \\
&= m_1 + m_2 \\
&= f(x) + f(y) \\
\text{Since } |D| = |\mathbb{Z}_n| = n, &\text{ we show that } f \text{ is } 1 - 1 \\
&\text{and hence it will be onto.} \\
&\text{We know that } \ker(f) = \{e_D\} \\
f(x) = 0 \Longrightarrow f(a^m) &= 1^m = 0 \\
&\Longrightarrow m = n \\
&\text{Therefore } f(a^m) = 0 \\
f(a^n) = 0 &\text{ and thus } f(e_D) = 0 \\
&\text{We map the generator to the generator.}
\end{aligned}$$

October 28th, 2020

Result: Let $(D, \cdot)$ be an infinite cyclic group. Then $D \approx (\mathbb{Z}, +)$. This means that every infinite cyclic group is isomorphic to $\mathbb{Z}$ under addition.

Proof:

Since D is cyclic, $D = <a>$ for some $a \in D$. We also know that $\mathbb{Z} = <1>$. So we proceed as follows: we build the following function mapping.

$$f: D \longrightarrow \mathbb{Z}$$

st $f(a^m) = 1^m \quad \forall m \in \mathbb{Z}$. f is a group homomorphism. Why?

$$\begin{aligned}
f(a^{m_1} \cdot a^{m_2}) = f\left(a^{m_1 + m_2}\right) &= 1^{m_1 + m_2} \\
&= 1^{m_1} + 1^{m_2} \\
&= m_1 + m_2 \\
&= f(a^{m_1}) + f(a^{m_2})
\end{aligned}$$

$$\begin{aligned}
&\text{We show that } f \text{ is onto:} \\
&\text{Let } K \in \mathbb{Z}. \text{ Then } K = 1^K \\
&\text{Hencec } b = a^K \in D
\end{aligned}$$

$$f(b) = f(a^K) = 1^K$$
We show that f is $1-1$
We do this by showing $\ker(f) = \{e_D\}$.
Assume $f(b) = 0$ for some $b \in D$
Show $b = e_D$. We are done if we do this.
Since $b \in <a> = D$, $b = a^m$ for some $m \in \mathbb{Z}$
$$\implies f(b) = f(a^m) = 1^m = 0$$
$$\implies m = 0. \text{ Why?}$$
$$|1| = \infty$$

Question: Imagine we have the following group: $D = \mathbb{Z}_4 \oplus \mathbb{Z}_{11}$. Is D a cyclic group? We did not write the operation because we assume that it is addition. Construct all the subgroups of D.

Solution: We know $(\mathbb{Z}_4, +)$ and $(\mathbb{Z}_{11}, +)$ are both cyclic groups. Since $\gcd(4, 11) = 1$, by a previous HW probelm, we conclude that D is cyclic.

Let H be a subgroup of D. $|D| = 44$. The possibilities for $|H| = 1, 2, 4, 11, 22, 44$. We will go through each of the following:

$$|H| = 1 \longrightarrow H = \{(0,0)\}$$
$$|H| = 2 \longrightarrow H = \{(0,0), (2,0)\} < D$$
If we have cyclic, then the subgroup is unique.
$$|H| = 4 \longrightarrow H = \{(0,0), (1,0), (2,0), (3,0)\}$$
This is exactly how we proceed with the rest.
$$|H| = 11 \longrightarrow H = \{0\} \oplus \mathbb{Z}_{11}$$
....

Fact: $D = F \oplus W$, assuming that D is cyclic. If $H < D$, then we have the following:

$$H = H_1 \oplus H_2, \text{where } H_1 < F \text{ and } H_2 < W$$

The proof is technical, but it is simple. We don't need to do the proof, we can just take it as a given.

Let us have an example where this is not true.

$$D = \mathbb{Z}_4 \oplus \mathbb{Z}_6$$

Give me all the subgroups with 2 elements.

We know that D is not cyclic
since $\gcd(4, 6) \neq 1$
We can come up with many subgroups with 2 elements
$$\{0, 2\} \oplus \{0\} \longrightarrow |H| = 2$$
$$\{0\} \oplus \{0, 3\} \longrightarrow |H| = 2$$
$$|(2,3)|, H = <(2,3)>$$
$$= \{(2,3), (0,0)\}$$
But we cannot write this as $F \oplus K$

A subgroup of D does not necessarily have to be a subgroup of both F and K.

Take the following: $(D,\cdot)$, and fix some $a\in D$. Now consider the following function mapping:

$$f\colon D\longrightarrow D \qquad \text{where } f(d)=a\cdot d\cdot a^{-1}$$

$\Longrightarrow$This is an automorphism map from D to D
f is an isomorphism. This means that there is:
1. group homomorphism, 2. $1-1$ and 3. onto.

$f\colon D\longrightarrow D$, and fix $a\in D$
$f(d)=a\cdot d\cdot a^{-1}$

Let $d_1,d_2\in D$. Show $f(d_1\cdot d_2)=f(d_1)\cdot f(d_2)$
$f(d_1\cdot d_2)=a\cdot(d_1\cdot d_2)\cdot a^{-1}$
$=a\cdot d_1\cdot a^{-1}\cdot a\cdot d_2\cdot a^{-1}$
$=f(d_1)\cdot f(d_2)$

Show that f is onto
Let $x\in D$. Find some $y\in D$ st $f(y)=x$
Let $y=a^{-1}\cdot x\cdot a\in D$
$f(y)=f(a^{-1}\cdot x\cdot a)=a\cdot a^{-1}\cdot x\cdot a\cdot a^{-1}$
$=x$

$f\colon D\longrightarrow D$, $f(d)=a\cdot d\cdot a^{-1}$
Show that f is $1-1$
Assume $f(d_1)=f(d_2)$
Show that $d_1=d_2$
$a\cdot d_1\cdot a^{-1}=a\cdot d_2\cdot a^{-1}$
$a^{-1}\cdot[a\cdot d_1\cdot a^{-1}=a\cdot d_2\cdot a^{-1}]\cdot a$
$\Longrightarrow d_1=d_2$

Def.: Let $a\in D$. Then $C(a)=\{x\in D\,|\,x\cdot a=a\cdot x\}$. Recall that the center of a group, $C(D)$, is defined by the following:

$$C(D)=\{y\,|\,y\cdot z=z\cdot y \quad \forall z\in D\}$$

Result: Let $a\in D$. Then $C(a)<D$.

Proof: Let $x,y\in C(a)$. Then we need to show that $x^{-1}\cdot y\in C(a)$.

$x,y\in C(a)$. Show $x^{-1}\cdot y\in C(a)$
$\Longrightarrow a\cdot(x^{-1}\cdot y)=(x^{-1}\cdot y)\cdot a$
Since $x\in C(a)$, $y\in C(a)$,
$x\cdot a=a\cdot x$ and $y\cdot a=a\cdot y$
We also know from the notes that $a\cdot x^{-1}=x^{-1}\cdot a$
Hence clearly $a\cdot(x^{-1}\cdot y)=(x^{-1}\cdot y)\cdot a$

Let us take the following example. Let D be a group with $|D|=12$, and some $a\in D$. Then $C(a)$ contains at least 2 elements.

Since $C(a)<D$, $|C(a)|\,|\,12$ By Lagrange
$|C(a)|=2,3,4,6$ or 12

Def.: Let $a \in D$. The conjugate of a, denoted by $\text{conj}(a) = \{b \in D \mid b = w \cdot a \cdot w^{-1} \text{ for some } w \in D\}$. When we write $b = w \cdot a \cdot w^{-1}$, we say that a and b are conjugate. Of course, this is for some $w \in D$.

If a is conjugate to b, then b is also conjugate to b. We can see the following:

$$\begin{aligned} b &= w \cdot a \cdot w^{-1} \\ &\text{Solve for } a: \\ w^{-1} \cdot b \cdot w &= a \end{aligned}$$

It does not matter how we write this.

Result: $(D, \cdot)$ is a group. We define $\sim$ on D st $a \sim b$ iff a is conjugate to b. Then we say that $\sim$ is an equivalence relation.

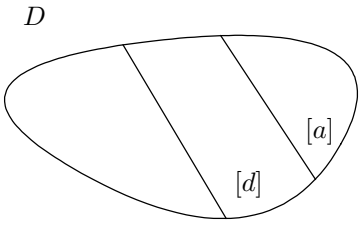
Proof:

$$\begin{aligned} &\text{Reflexive: Show } a \sim a \\ &\text{Since } a = e \cdot a \cdot e^{-1}, (e \text{ identity in } D) \\ &\text{Then } a \sim a \end{aligned}$$

$$\begin{aligned} &\text{Symmetric: Assume } a \sim b. \text{ Show } b \sim a \\ &a = d \cdot b \cdot d^{-1} \text{ for some } d \in D \\ &\text{Hence } d^{-1} \cdot a \cdot d = b \\ &\text{Thus } b \sim a \end{aligned}$$

$$\begin{aligned} &\text{Transitive: Assume } a \sim b, b \sim c. \text{ Show } a \sim c \\ &a \sim b \Longrightarrow a = w \cdot b \cdot w^{-1} \text{ for some } w \in D \quad (1) \\ &b \sim c \Longrightarrow c = d \cdot b \cdot d^{-1} \text{ for some } d \in D \quad (2) \\ &\Longrightarrow b = d^{-1} \cdot c \cdot d. \text{ Substitute } b \text{ into } (1) \\ &a = w \cdot d^{-1} \cdot c \cdot d \cdot w^{-1} \\ &\text{Let } y = w \cdot d^{-1}, y^{-1} = d \cdot w^{-1} \\ &\Longrightarrow a = y \cdot c \cdot y^{-1} \\ &\text{Therefore } a \sim c \end{aligned}$$

We have shown that $\sim$ is an equivalence relation on D. It is interesting to note that the equivalence relation is just a generalization of an equal, $=$.



$[a] = \{b \in D \mid b \sim a\}$
Choose $d \notin [a]$

Fact: If $\sim$ is an equivalence relation on D, then the intersection of every two distinct equivalence classes are empty sets, and the union of all equivalence classes is D itself. This is exactly the same way left cosets behave.

Result: Let $a \in D$. Recall that $\text{conj}(a) = \{w \cdot a \cdot w^{-1} | w \in D\}$. Then $|\text{conj}(a)| = \frac{|D|}{|C(a)|}$. This number tells you exactly how many elements are conjugates to a. Be careful with the fact that we are considering the center of a, not the center of the group D.

$\frac{|D|}{|C(a)|}$ is the number of left cosets of $C(a)$. In other words, we are saying that the number of elements that are conjugates to a is the same as the number of left cosets of $C(a)$.

November 4th, 2020

Proof: Let $L =$ set of all distinct left cosets of $C(a)$, say $L = \{C(a), a_1 \cdot C(a), \ldots., a_n \cdot C(a)\}$. We define the following function:

$$f: L = \{C(a), a_1 \cdot C(a), \ldots., a_n \cdot C(a)\} \longrightarrow \text{conj}(a)$$

$$f(a_i \cdot C(a)) = a_i \cdot a \cdot a_i^{-1} \in \text{conj}(a)$$

We need to show that f is $1-1$ and onto.

$$f: L \longrightarrow \text{conj}(a)$$
$$f(a_i \cdot C(a)) = a_i \cdot a \cdot a_i^{-1}$$

Let $b \in \text{conj}(a)$, hence $b = w \cdot a \cdot w^{-1}$ for some $w \in D$

Hence $f(w \cdot C(a)) = w \cdot a \cdot a^{-1} = b$

Therefore f is onto.

Let $a_i \cdot C(a) \in L$. Choose $b \in a_i \cdot C(a)$

We will show that $f(b \cdot C(a)) = f(a_i \cdot C(a))$

$= a_i \cdot a \cdot a_i^{-1} = b \cdot a \cdot b^{-1}$

All elements in the left coset are assigned to one and only one element in $\text{conj}(a)$.

Let $b \in a_i \cdot C(a). b = a_i \cdot d$ for some $d \in C(a)$

$$b \cdot a \cdot b^{-1} = (a_i \cdot d) \cdot a \cdot (a_i \cdot d)^{-1}$$
$$= a_i \cdot d \cdot a \cdot d^{-1} \cdot a_i^{-1}$$

Since $d \in C(a)$, then:

$$a_i \cdot a \cdot d \cdot d^{-1} \cdot a_i^{-1}$$
$$= a_i \cdot a \cdot a_i^{-1}$$

Assume $f(b \cdot C(a)) = f(d \cdot C(a))$

Show that $b \cdot C(a) = d \cdot C(a)$

$$f(b \cdot C(a)) \Longrightarrow b \cdot a \cdot b^{-1}$$
$$f(d \cdot C(a)) \Longrightarrow d \cdot a \cdot d^{-1}$$

To get $b \cdot a \cdot b^{-1} = d \cdot a \cdot d^{-1}$

we show $b \cdot d^{-1} \in C(a)$

$$b^{-1} \cdot b \cdot a \cdot b^{-1} \cdot d = b^{-1} \cdot d \cdot a \cdot d^{-1} \cdot d$$
$$a \cdot b^{-1} \cdot d = b^{-1} \cdot d \cdot a$$
$$\Longrightarrow b^{-1} \cdot d \in C(a) \text{ Since it commutes with } a$$

Thus f is $1-1$

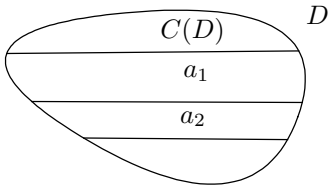
Result: $|D| = p^n \Longrightarrow |C(D)| \geqslant p$, for some prime number p. This is an extension of a previously shown result where we said that if $|D| = p^2$ for some p prime, then D is an Abelian group.

Proof:

Let $a \in D$. $|\text{conj}(a)|$ is a factor of $|D| = n$. Why is this true? Because $|\text{conj}(a)| = \frac{|D|}{|C(a)|}$.

Observation: Let $a \in C(D)$. Then $\text{conj}(a) = \{w \cdot a \cdot w^{-1} | w \in D\} = \{a\}$. Since a is already in the center, it commutes with every element of D. Therefore we have that the conjugate of a is itself.

Recall the equivalence relation, $\sim$. If $a \in C(D), \text{then conj}(a) = [a] = \{a\}$. Let us take a look at D:



Let $\text{conj}(a), \text{conj}(a_1), \text{conj}(a_2), \ldots, \text{conj}(a_i)$ be the set of all distinct equivalent classes of $\sim$, where $a_1, a_2, \ldots, a_i \notin C(D)$.

if $b \notin C(D)$, then $\text{conj}(b) \cap C(D) = \varnothing$. Now let us take some $b_1 \notin \text{conj}(b) \cup C(D) \Longrightarrow \text{conj}(b_1) \cap \text{conj}(b) = \varnothing$ and $\text{conj}(b_1) \cap C(D) = \varnothing$.

This means: Let $\text{conj}(b_1), \text{conj}(b_2), \ldots, \text{conj}(b_k)$ be all distinct conjugate classes st $b_1, b_2, \ldots, b_k \notin C(D)$. Then:

$$D = C(D) \cup \text{conj}(b_1) \cup \text{conj}(b_2) \cup \cdots \cup \text{conj}(b_k)$$

$$\begin{aligned} \Longrightarrow |D| &= |C(D)| + |\text{conj}(b_1)| + \cdots + |\text{conj}(b_k)| \\ &\Longrightarrow \text{From the hypothesis, } |D| = p^n \\ p^n &= |C(D)| + |\text{conj}(b_1)| + \cdots + |\text{conj}(b_k)| \\ &\Longrightarrow |C(D)| \geqslant p \end{aligned}$$

Since $b_1, b_2, ..., b_k \notin C(D)$, then $|\text{conj}(b_i)| = p^{n_i}$ for every $1 \leqslant i \leqslant k$. We have:

$$\begin{aligned} p^n &= |C(D)| + |\text{conj}(b_1)| + \cdots + |\text{conj}(b_k)| \\ p^n &= |C(D)| + p^{n_1} + p^{n_2} + \cdots + p^{n_i} \\ &\Longrightarrow p \,|\, |C(D)| \\ &\text{and thus } |C(D)| \geqslant p \end{aligned}$$

Def.: Consider the following:

$$f_1 = (\ 1\ \ 2\ \ 3\ ) \circ (\ 4\ \ 5\ )$$

$$f_2 = (\ 3\ \ 5\ \ 7\ ) \circ (\ 2\ \ 4\ )$$

By staring we know that both f_1 and f_2 are of order 6 and they are the same type. They are compositions of a 3-cycle and a 2-cycle.

Result: We say that two compositions, or in our case f_1 and f_2 are conjugate to each other in S_n iff they have the same type.

November 9th, 2020

(Most of the lecture was a discussion of the exam with a small introduction to simple groups.)

.....

We will first go to the second question of the exam:

Question: $|D| = 65$, $H \lhd D$ and $|H| = 13$. Show that D is a cyclic group.

Proof: Let $x \notin H$. If we show that $|x| = 65$, we are done. Assume there is no elements in D that have order 65. Hence if $x \in D$, then $|x| = 1, 5$ or 13.

$$\begin{aligned}
&\text{We first claim } |x| = 5\\
&x \cdot H \in D/H\\
&\text{Since } |D/H| = 5, |x \cdot H| \text{ is a factor of } 5\\
&\text{But since } x \notin H, |x \cdot H| = 5\\
\Longrightarrow &\text{Let } m = |x|, x^m = e \in D\\
(x \cdot H)^m = H \in D/H \Longrightarrow &\ 5 \text{ is a factor of } m\\
&\text{Therefore } m = 5 \text{ or } 65
\end{aligned}$$

How many subgroups of order 5 does D have? How many elements of order 5 does D have?

$$\begin{aligned}
\Longrightarrow &\text{no. of elements of order 5 outside of } H:\\
&H = 65 - 13 = 52 \text{ elements of order 5}\\
&\text{Now, how many subgroups do we have of order 5?}\\
&\text{If } K \text{ is a subgroup with 5 elements, then}\\
&K \text{ has 4 elements of order 5}
\end{aligned}$$

$$\Longrightarrow \frac{52}{4} = 13 \text{ subgroups of order 5}$$

$$\begin{aligned}
&\text{Choose } a \in D \text{ st } |a| = 5, \text{and choose } h \in H \text{ st } |h| = 13\\
&\text{Now let } y = a \cdot h \in H \text{ and } y \notin H\\
&a \cdot h = y \in H \Longrightarrow a = y \cdot h^{-1} \in H, \text{contradiction}\\
&\text{therefore } y \notin H\\
\Longrightarrow &|y| = 5
\end{aligned}$$

$$\begin{aligned}
H_1 = <a \cdot h> \longrightarrow &\text{ subgroup of order 5}\\
\text{Consider } H_2 = <a \cdot h_2> &\text{ subgroups of order 5}
\end{aligned}$$

So we can construct $H_1, H_2, ..., H_{12}$, each with exactly 5 elements. We construct them as $<a \cdot h_1>$, $....$, $<a \cdot h_{12}>$. Also, we have $<a> = H_{13}$.

D has 13 subgroups, call them $F_1, F_2, ..., F_{13}$, where $F_1 = <a_1>$, with $|a_1| = 5$ and so on for all. We constructed $H_i = <a_1 \cdot h_i>$, and we know that $H_{13} = <a_1>$, because we are doing $\cdot$ with e.

Proof was not completed and left here after some complications.

.....

Def.: Let $(D,\cdot)$ be a group. We say that $(D,\cdot)$ is simple iff $\{e\} \lhd D$. This means that D has no non-trivial normal subgroups.

Observation: D is a finite Abelian group. Then D is simple iff $|D| = p$ for some p prime. The concept of simple groups become more interesting if our group is not Abelian.

November 11th, 2020

.....

Question 2 of the exam needs a special case of Sylow's theorem, which was not introduced to us before. Therefore it is removed. However, the case is mentioned below now.

.....

Fact: Assume that q_1, q_2 are two distinct prime numbers and $q_1 < q_2$. Assume we also have a group, $(D,\cdot)$, st $|D| = q_1 \times q_2$. If q_1 is not a factor of $(q_2 - 1)$, then D is a cyclic group.

Result: Let $(D,\cdot)$ be a group and $H \lhd D, K \lhd D$ st $H \cdot K = D$, or in other words $|H| \times |K| = |D|$ and $H \cap K = \{e\}$. Then we have the following: $D \approx H \oplus K \approx D/K \oplus D/H$.

Proof: To prove that this isomorphism is true, we show group homomorphism first and then show that it is 1-1 and onto. We take the following function mapping:

$$f: (D,\cdot) \longrightarrow D/H \oplus D/K$$

$$\begin{aligned} f(d) &= (d\cdot H, d\cdot K), \text{assuming } D \text{ is finite} \\ &\text{We show that } f \text{ is group homomorphism.} \\ f(d_1\cdot d_2) &= (d_1\cdot d_2\cdot H, d_1\cdot d_2\cdot K) \\ &= (d_1\cdot H, d_1\cdot K)\oplus(d_2\cdot H, d_2\cdot K) \\ &= f(d_1)\oplus f(d_2) \end{aligned}$$

What is $|D/H \oplus D/K|$? It is $|D/H| \times |D/K| = |D|$. If we show equality between $|D/H \oplus D/K|$ and $|D|$, it would suffice to show that f is 1-1 [***Fact:*** $f: S \longrightarrow L, |S| = |L|$, then f is 1-1 iff f is onto].

We have that $|D/H \oplus D/K| = \frac{|D|}{|H|} \times \frac{|D|}{|K|} = \frac{|D| \times |D|}{|H| \times |K|}$. Since $H \cdot K = D$ and $H \cap K = \{e\}$, we conclude that $|D/H \oplus D/K| = |D|$.

So far, we have that f is group homomorphism, and $|D/H \oplus D/K| = |D|$. To show that f is bijective, we only need to show that f is 1-1.

$$\begin{aligned} f: (D,\cdot) &\longrightarrow D/H \oplus D/K, \\ \text{with } f(d) &= (d\cdot H, d\cdot K) \\ \text{To conclude } f \text{ is } 1-1&, \text{we show} \\ \ker(f) &= \{e\} \end{aligned}$$

$$\begin{aligned} \text{Assume } f(b) &= (e\cdot H, e\cdot K) \text{ for some } b \in D \\ \text{Show that } b &= e \end{aligned}$$

$$\begin{aligned} f(b) &= (b\cdot H, b\cdot K) = (e\cdot H, e\cdot K) \\ &\Longrightarrow b\cdot H = e\cdot H, b\cdot K = e\cdot K \\ &b \in H \text{ and } b \in K \\ &\Longrightarrow b \in H \cap K \\ &\text{and } b = e \text{ since we assumed } H \cap K = \{e\} \end{aligned}$$

We have proven that $D \approx D/K \oplus D/H$. Now we have to show that $D \approx H \oplus K$. Let us define the following mapping:

$$L: D \longrightarrow H \oplus K$$

$$\begin{aligned}
\text{Let } d \in D. \text{ Since } D = H \cdot K, \text{ then} \\
\exists h \in H \text{ and } k \in K \text{ st } d = h \cdot k \\
L(d) = L(h \cdot k) = (h, k). \\
\text{Show that } L \text{ is well defined.}
\end{aligned}$$

$$\begin{aligned}
\text{Assume } d = h_1 \cdot k_1 = h_2 \cdot k_2 \\
\text{Show that } h_1 = h_2 \text{ and } k_1 = k_2 \\
h_1 \cdot k_2 = h_2 \cdot k_2 \Longrightarrow \\
h_2^{-1} \cdot h_1 \cdot k_1 = k_2 \\
\Longrightarrow h_2^{-1} \cdot h_1 = k_2 \cdot k_1^{-1} \\
h_2^{-1} \cdot h_1 \in H \text{ and } k_2 \cdot k_1^{-1} \in K \\
k_2 \cdot k_1^{-1} \in H \cap K, h_2^{-1} \cdot h_1 \in H \cap K \\
k_2 \cdot k_1^{-1} = e \text{ and thus } k_1 = k_2 \\
\text{similar argument to show } h_1 = h_2 \\
\text{Therefore } L \text{ is well defined}
\end{aligned}$$

$$\begin{aligned}
L: D \longrightarrow H \oplus K, L(d) = (h, k) \\
\text{where } d = h \cdot k, \text{ both unique.} \\
|D| = |H \oplus K| = |H| \times |K| \\
\text{To show } L \text{ is bijective, we have to show} \\
L \text{ is } 1-1, \text{ by concluding } \ker(L) = \{e\}
\end{aligned}$$

$$\begin{aligned}
L(d) = (h, k) = (e, e) \\
\Longrightarrow h = e, k = e \\
\ker(L) = \{e\} \text{ and thus } L \text{ is } 1-1
\end{aligned}$$

$$\begin{aligned}
\text{To show } L \text{ is group homomorphism,} \\
\text{we play the same game as usual.}
\end{aligned}$$

Let us take an example, say $|D| = 35$, with $H \lhd D$ and $K \lhd D$. $|H| = 7$ and $|K| = 5$. Prove that D is a cyclic group.

$$\begin{aligned}
|H \cdot K| = \frac{|H| \cdot |K|}{|H \cap K|} = \frac{7 \times 5}{1} = 35 \\
\text{since } H \cap K = \{e\} \\
H \approx \mathbb{Z}_7 \text{ and } K \approx \mathbb{Z}_5 \\
\text{Since } H \lhd D \text{ and } K \lhd D, H \cdot K = D \\
\text{with } H \cap K = \{e\}, D \approx H \oplus K \\
D \approx \mathbb{Z}_7 \oplus \mathbb{Z}_5 \\
\approx \mathbb{Z}_{35}
\end{aligned}$$

Therefore we have shown that, through the isomorphism of D to $\mathbb{Z}_n$, that D is a cyclic group given its specifications and assumptions in the question.

Recall that if H and K are subgroups of D, then:

$$|H \cdot K| = \frac{|H| \times |K|}{|H \cap K|}$$

Also recall the special case of Sylow's theorem. We will now proceed with some examples as practice.

Question: $(D, \cdot)$ is a group with $|D| = 39$. Assume D has normal subgroups, H, K with the following properties: $|H| = 3$ and $|K| = 13$. Prove that D is cyclic.

Solution: We use the following facts. $|D| = 39$, $H \lhd D$ and $K \lhd D$, with $|H| = 3$ and $|K| = 13$.

$$|H \cdot K| = \frac{|H| \times |K|}{|H \cap K|} = \frac{3 \times 13}{1} = 39$$
$$|H \cap K| = 1 \text{ since } H \cap K = \{e\}$$
$$\gcd(13, 3) = 1$$

$$\text{Since } |H \cdot K| = 39, H \cdot K = D$$
$$\text{Therefore } D \approx H \oplus K$$
$$\text{Since } |H| = 3, \longrightarrow H \approx \mathbb{Z}_3$$
$$\text{and } K \approx \mathbb{Z}_{13}$$
$$D \approx \mathbb{Z}_3 \oplus \mathbb{Z}_{13}$$
$$\text{because } \gcd(3, 13) = 1, D \text{ is cyclic and}$$
$$D \approx \mathbb{Z}_{39} \text{ under addition}$$

Result: *Cauchy's Theorem*: Let $|D| = n$ and $q|n$, where q is prime. Then D has an element of order q. This result also means that D has a subgroup with q elements.

Remember that if D is Abelian and we have a subgroup with m elements, then we must have an element of order m.

Proof: Assume $|D| = q$. Then $D \approx \mathbb{Z}_q$ and we are done because each non-identity element will have order q by Lagrange's theorem.

This is how we proceed with induction for groups:

Assume result is true
for every group of order $m, m < n$

Consider $C(D)$, center of D
We have two cases. Firstly:
1.
Assume $q \mid |C(D)|$
Remember that the center, $C(D)$, is Abelian
since $q \mid |C(D)|$, we conclude that $C(D)$
has a subgroup with q elements, say H
Hence $H \approx \mathbb{Z}_q$, and thus H has an element
of order q, and since $H < D \Longrightarrow D$ has an element
of order q. Therefore we are done.

2.
Assume q is not a factor of $|C(D)|$

$$\text{Recall if } a \in D, |\text{conj}(a)| = \frac{|D|}{|C(a)|}$$
$$\text{Recall: if } |D| = n, \text{ then:}$$
$$|D| = |C(D)| + |\text{conj}(a_1)| + |\text{conj}(a_2)| + \cdots + |\text{conj}(a_k)|$$
$$\text{for some } a_1, a_2, \ldots, a_k \notin C(a)$$
$$\implies \text{By staring, we can see that:}$$
$$\exists a_i, 1 \leqslant i \leqslant k \text{ st } q \text{ is not a factor of } |\text{conj}(a_i)|$$
$$|\text{conj}(a_i)| = \frac{|D|}{|C(a_i)|}$$
$$\implies |\text{conj}(a_i)| \times |C(a_i)| = |D|$$
$$\implies q \text{ is not a factor of } |\text{conj}(a_i)| \implies q \mid |C(a_i)|$$
$$\text{We know that } C(a_i) \neq D \text{ because } a_i \notin D$$
$$C(a_i) < D \text{ and } |C(a_i)| < n$$

$$\text{we have that:}$$
$$q \mid |C(a_i)| \text{ and } |C(a_i)| < n$$
$$\implies \text{by hypothesis, } C(a_i) \text{ will have an element of order } q$$
$$\implies D \text{ has an element of order } q$$

Recall from the HW that if $H < D$ and $[H : D] = 2 = \frac{|D|}{|H|}$ (number of all left cosets of H), then we have that $H \lhd D$. We will use it in the following result.

Fact: $H < D$ and $[H : D] = q$, where q is the smallest prime factor of $|D|$. We conclude that H is a normal subgroup of D, $H \lhd D$. This is obviously a general case of the HW proof.

Application of Theorem: Take an Abelian group, D. $|D| = p^3$, where p prime. Porve that $D \approx \mathbb{Z}_{p^3}$, $D \approx \mathbb{Z}_p \oplus \mathbb{Z}_{p^2}$, or $D \approx \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p$.

To help, if we have $K_1 \oplus K_2 \oplus \cdots \oplus K_n = \{(a_1, a_2, \ldots, a_n) \mid a_1 \in K_1, a_2 \in K_2, \ldots, a_n \in K_n\}$. As an example of this, we will also see the order: For $K_1 \oplus K_2 \oplus K_3$, $|(a_1, a_2, a_3)| = \text{lcm}\,(|a_1|, |a_2|, |a_3|)$. Common mistake for the lcm of three numbers:

$$\text{lcm}\,(4, 6, 5) \neq \frac{4\,5\,6}{\text{gcd}\,(4, 6, 5)}$$

We have to take two steps: First we calculate the lcm of any two of the numbers, and then take that and find the lcm with whatever number remains.

$$\begin{aligned} &\text{lcm}\,(4, 5, 6) \\ =&\text{lcm}\,(4, 5) = \frac{4\,5}{\text{gcd}\,(4, 5)} = 20 \\ \implies &\text{lcm}\,(20, 6) = \frac{20\,6}{\text{gcd}\,(20, 6)} \\ =&60 \end{aligned}$$

November 18th, 2020

Recall that if we have a group with $|D| = q_1 \times q_2$ and we have that q_1 is NOT a factor of $(q_2 - 1)$, then we conclude that D is a cyclic group.

Also recall the following result: let $(D, \cdot)$ be a group and $H \lhd D$, $K \lhd D$ st $H \cdot K = D$, or in other words $|H| \times |K| = |D|$ and $H \cap K = \{e\}$. Then we have the following: $D \approx H \oplus K \approx D/K \oplus D/H$.

Finally, recall that if $H < D$ and $K < D$, then:

$$|H \cdot K| = \frac{|H| \times |K|}{|H \cap K|}$$

***Result**: Caley's Theorem:* Let D be a finite group st $|D| = n$. There exists a subgroup, L, of S_n, st $D \approx L$. All finite groups are nothing but a subgroup of S_n in terms of the structure of the group itself.

Proof: We will build the following function mapping:

$$F: D \longrightarrow S_n$$

$$\forall d \in D, F(d) = \begin{pmatrix} e & d_2 & d_3 & .... & d_n \\ d \cdot e & d \cdot d_2 & d \cdot d_3 & .... & d \cdot d_n \end{pmatrix}$$

This map is definitely bijective by staring

Remember that the domain of F is D

the co-domain of F is S_n

We will show that F is group-homomorphism:

Let $x, y \in D$

$$F(x \cdot y) = \begin{pmatrix} e & d_2 & d_3 & .... & d_n \\ x \cdot y \cdot e & x \cdot y \cdot d_2 & x \cdot y \cdot d_3 & .... & x \cdot y \cdot d_n \end{pmatrix}$$

We need to show that $F(x \cdot y) = F(x) \circ F(y)$

$$\implies F(x) \circ \begin{pmatrix} e & d_2 & d_3 & .... & d_n \\ y \cdot e & y \cdot d_2 & y \cdot d_3 & .... & y \cdot d_n \end{pmatrix}$$

$$= \begin{pmatrix} e & d_2 & d_3 & .... & d_n \\ x \cdot y \cdot e & x \cdot y \cdot d_2 & x \cdot y \cdot d_3 & .... & x \cdot y \cdot d_n \end{pmatrix}$$

Therefore $F(x \cdot y) = F(x) \circ F(y)$

We show that $\ker(F) = \{e\}$

Let $w \in \ker(F)$

$$F(w) = \begin{pmatrix} e & d_2 & d_3 & .... & d_n \\ w \cdot e & w \cdot d_2 & w \cdot d_3 & .... & w \cdot d_n \end{pmatrix}$$

$$= \begin{pmatrix} e & d_2 & d_3 & .... & d_n \\ e & d_2 & d_3 & .... & d_n \end{pmatrix}$$

$$\implies w \cdot e = e$$

$$\implies w = e$$

$$\ker(F) = \{e\}$$

By 1st isomorphism theorem,

$$\frac{D}{\ker(F)} \approx \text{range}(F)$$

$$\frac{D}{\{e\}} = D$$

$$D \approx \text{range}(F) < S_n$$

The original theorem was that our group, D, is isomorphic to a subgroup of S_n. This is exactly what we show here since range(F) is a subgroup of the co-domain, S_n. In other words, let $L = \text{range}(F)$. Then we have that $L < S_n$ and $D \approx L$.

Recall the definition: $(D, \cdot)$ is simple iff $\{e\}$ is the only normal subgroup of D.

Result: Take A_n, with $n \geqslant 5$.We know that $A_n \lhd S_n$ and $|A_n| = \frac{n!}{2}$. The theorem says that A_n is a simple group for every $n \geqslant 5$.

Recall that $(\mathbb{Z}_n^*, \times)$ is a group iff n is a prime number.

Fact: $(\mathbb{Z}_q^*, \times)$, where q is prime, is a cyclic group. For example, we can see the fact in the following: Let us take $(\mathbb{Z}_{11}^*, \times) = <a>, |a| = 10$.

Def.: Let us consider $n \geqslant 2$. Then:

$$U(n) = \{a \in \mathbb{Z}_n^* \,|\, \gcd(a, n) = 1\}$$

For example, if we have $n = 7$,

$$U(7) = \{a \in \mathbb{Z}_7^* | \gcd(a, 7) = 1\}$$

$$\begin{aligned} U(7) &= \{1, 2, 3, 4, 5, 6\} = \mathbb{Z}_7^* \\ U(10) &= \{1, 3, 7, 9\} \neq \mathbb{Z}_{10}^* \\ |U(10)| &= 4 = \varphi(10) \end{aligned}$$

$$\text{Observe that for } n \geqslant 2, |U(n)| = \varphi(n)$$

Recall the following result from earlier in the semester: $(U(n), \times)$ is an Abelian group with exactly $\varphi(n)$ elements.

Result: We have that $U(n) \approx \mathbb{Z}_{q_1 - 1} \oplus \mathbb{Z}_{q_1^{\alpha_1 - 1}} \oplus \cdots \oplus \mathbb{Z}_{q_k - 1} \oplus \mathbb{Z}_{q_k^{\alpha_k - 1}}$. This comes from how we generate $\varphi(n)$.

Consider the following example:

$$\begin{aligned} n &= 7^3 \cdot 5^2 \\ \varphi(n) &= 6 \cdot 7^2 \cdot 4 \cdot 5 \\ U(n) &\approx \mathbb{Z}_6 \oplus \mathbb{Z}_{49} \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_5 \\ &\text{We can simplify this further} \\ &\text{For example, } \mathbb{Z}_4 \oplus \mathbb{Z}_5 \approx \mathbb{Z}_{20} \\ \Longrightarrow U(n) &\approx \mathbb{Z}_{294} \oplus \mathbb{Z}_{20} \end{aligned}$$

The proof of this relies on Sylow's theorem, so we will just take it as a fact rather than going through the entire proof.

Note: Using the prime factorization, we can write $\varphi(n)$ as one of the two:

$$\begin{aligned} \varphi(n) &= (q_1 - 1) q_1^{\alpha_1 - 1} \cdot \cdots \cdot (q_k - 1) q_k^{a_k - 1} \\ \varphi(n) &= (q_1^{\alpha_1} - q_1^{\alpha_1 - 1})(q_2^{\alpha_2} - q_2^{\alpha_2 - 1}) \cdot \cdots \cdot (q_k^{\alpha_k} - q_k^{\alpha_k - 1}) \end{aligned}$$

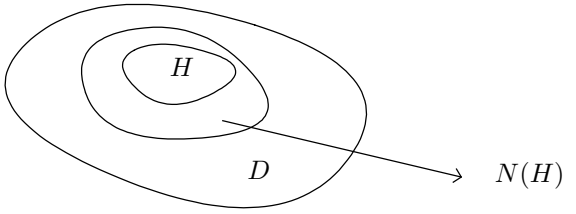
November 23rd, 2020

Def.: We have $H < D$. This could be either a normal subgroup or any other type of subgroup. What does $N(H)$ mean?

$$N(H) = \{x \in D \,|\, x \cdot H = H \cdot x\}$$

This is called the normalization of H in D. In street language, it is the set of all elements in D where the left cosets of H are the same as the right cosets of H.

If we have that $H \lhd D$, then $N(H) = D$. This is trivial, but the concept of the normalization is interesting when H is NOT normal in D. Further, it is interesting if our group, D, is not Abelian.



By default, H will be a normal subgroup of $N(H)$. $N(H)$ is the largest subgroup of D st $H \lhd N(H)$.

Result: $N(H) < D$, and clearly $H \lhd N(H)$

Proof:

$$\begin{aligned}
&\text{Let } x, y \in N(H)\\
&\text{Show that } x^{-1} \cdot y \in N(H)\\
&\text{Since } x, y \in N(H), \text{we know:}\\
&x \cdot H = H \cdot x \text{ and } y \cdot H = H \cdot y
\end{aligned}$$

$$\begin{aligned}
&\text{We show that}\\
&x^{-1} \cdot y \cdot H = H \cdot x^{-1} \cdot y\\
&\text{Since } y \cdot H = H \cdot y \Longrightarrow y \cdot H \cdot y^{-1} = H\\
&x \cdot H = H \cdot x \Longrightarrow x \cdot H \cdot x^{-1} = H
\end{aligned}$$

$$\begin{aligned}
&\text{Since } y \cdot H \cdot y^{-1} = H \text{ and } x \cdot H \cdot x^{-1} = H,\\
&\text{we conclude that:}\\
&x^{-1} \cdot y \cdot H \cdot y^{-1} \cdot x = H\\
&\Longrightarrow x^{-1} \cdot y \cdot H = H \cdot x^{-1} \cdot y
\end{aligned}$$

Therefore, we have shown that $x^{-1} \cdot y \in N(H)$ and thus $N(H)$ is a subgroup of D.

Question: $H < D$, with $|D| = 100$. Given that $|N(H)| > 50$, prove $H \lhd D$.

If we prove that $N(H) = D \Longrightarrow H \lhd D$. Therefore this is the roadmap that we will take to prove this question.

Solution:

$$\begin{aligned}
&\text{Since } N(H) < D, |N(H)| \,|\, |D|\\
&|N(H)| > 50 \text{ by the question}\\
&\text{Therefore } |N(H)| = 100 \,|\, |D| = 100
\end{aligned}$$

$$\text{Since } |N(H)| = |D|, H \lhd D$$

Recall the definition of a simple group: $\{e\} \lhd D$. The identity is the only normal subgroup of D. Also that A_n, with $n \geqslant 5$ is simple.

Consider the following example:

$$\alpha = (\ 1\ \ 2\ \ 3\ \ 4\ \ 5\ ) \in A_5$$
$$|\alpha| = 5$$
Let us take some H
$$H = \{\alpha, \alpha^2, \alpha^3, \alpha^4, e\}$$

We have the following three statements:

1. H is never a normal subgroup of A_5 (True)
2. $\forall a \in A_5, a \cdot H \neq H \cdot a$ (False)
3. For some $a \in A_5, a \cdot H \neq H \cdot a$ (True)

If we were told that D is simple, is it possible that D has non-trivial subgroups? Yes, it is possible. However, if we asked can D have non-trivial NORMAL subgroups, then it is not possible.

Take the following statement:

$$(\mathbb{Z}_2, +) < (\mathbb{Z}_4, +)$$

Is this statement correct or wrong? This is clearly wrong, because when we are in $\mathbb{Z}_2$, we are taking the addition modulo 2, whereas it is addition modulo 4 in $\mathbb{Z}_4$. They are two different binary operations and even though $\mathbb{Z}_2$ is a subset of $\mathbb{Z}_4$, the fact is that it cannot be a group because of the difference in the binary operation.

However, $(\mathbb{Z}_4, +)$ has a subgroup that is isomorphic to $(\mathbb{Z}_2, +)$. How is this true? We have that $\mathbb{Z}_4$ has a subgroup with 2 elements, and this is clearly a cyclic subgroup. Using a previous result, we know that every cyclic subgroup is isomorphic to some $\mathbb{Z}_n$ under addition.

November 25th, 2020

Result: Given the following:

$$U(n) = \{a \in \mathbb{Z}_n \,|\, \gcd(a, n) = 1\}, \text{with } |U(n)| = \varphi(n)$$

$$\text{Aut}(\mathbb{Z}_n) = \{f : (\mathbb{Z}_n, +) \longrightarrow (\mathbb{Z}_n, +) |\ f \text{ is group-isomorphic}\}$$

Then we have that $(\text{Aut}(\mathbb{Z}_n), \circ) \approx (U(n), \times)$. Note that $\text{Aut}(\mathbb{Z}_n)$ is the set of all group isomorphisms from $(\mathbb{Z}_n, +)$ onto $(\mathbb{Z}_n, +)$. We show that $(\text{Aut}(\mathbb{Z}_n), \circ)$ is isomorphic to $U(n)$.

What can we get out of this result? $(\text{Aut}(\mathbb{Z}_p), \circ) \approx (\mathbb{Z}_p^*, \times)$. Note that $U(p) = \mathbb{Z}_p^*$ where p is a prime number. This means that for all p prime, $(\text{Aut}(\mathbb{Z}_p), \circ)$ is always a cyclic group.

For example, let us take $\text{Aut}(\mathbb{Z}_{12})$. This is going to be isomorphic to $(U(12), \times)$. This means that the structure of the two groups are the same.

How many group isomorphisms are there from $(\mathbb{Z}_{12}, +)$ to $(\mathbb{Z}_{12}, +)$? The answer is $|\text{Aut}(\mathbb{Z}_{12})| = |U(12)| = \varphi(12) = 4$.

Proof:

Let $a \in U(n)$
$F_a : (\mathbb{Z}_n, +) \longrightarrow (\mathbb{Z}_n, +)$ st
$F_a(x) = a\,x \pmod n$

a is fixed.
Our claim is that F_a is a group-isomorphism
from $(\mathbb{Z}_n, +)$ to $(\mathbb{Z}_n, +)$

$\longrightarrow$We show that F_a is a group-homomorphism
Let $x, y \in \mathbb{Z}_n$
$F(x+y) = a(x+y) = a\,x + a\,y$
$= F_a(x) + F_a(y)$

$\longrightarrow$Show that F_a is onto
Let $b \in \mathbb{Z}_n$. Show that $\exists w \in \mathbb{Z}_n$ st
$F_a(w) = b$
Remember that $F_a(x) = a\,x (\text{mod}\, n)$
$\longrightarrow w = a^{-1} \cdot b \in \mathbb{Z}_n$
$F_a(a^{-1} \cdot b) = a \cdot (a^{-1} \cdot b) = b$

$\longrightarrow$Show that F_a is $1-1$
We show that $\ker(F_a) = \{0\}$
Let $x \in \ker(F_a)$. We show that $x = 0$
$x \in \ker(F_a) \Longrightarrow F_a(x) = 0 = a\,x$
$\Longrightarrow a\,x = 0 \Longrightarrow a^{-1} \cdot a \cdot x = a^{-1} \cdot 0 \Longrightarrow x = 0$

We have shown that F_a is a group-isomorphism, for some $a \in U(n)$. We emphasize the fact that $F_a \in \text{Aut}(\mathbb{Z}_n)$. This means that each function in $\text{Aut}(\mathbb{Z}_n)$ is a group-isomorphism.

Sub-Result: Let $K \in \text{Aut}(\mathbb{Z}_n)$. then $K = F_a$ for some $a \in U(n)$. We use the same function mapping for F_a.

Proof:

Given $K: (\mathbb{Z}_n, +) \longrightarrow (\mathbb{Z}_n, +)$
st K is a group-isomoprhism
Show that $\exists a \in U(n)$ st $K(b) = a\,b (\text{mod}\, n)$
$\forall b \in \mathbb{Z}_n$
$\Longrightarrow K = F_a$

Let $a \in K(1)$
Show that $K(x) = a\,x (\text{mod}\, n)\, \forall x \in \mathbb{Z}_n$
$K(0) = a \cdot 0 = 0$
$K(1) = a \cdot 1 = a$

$\longrightarrow$Assume $K(x) = a\,x$ for some $x \in \mathbb{Z}_n$
$\longrightarrow$Show that $K(x+1) = a(x+1)$
$= K(x) + K(1)$ because K is group-homomorphism
$= a\,x + a = a(x+1)$

What we learned: If $K \in \text{Aut}(\mathbb{Z}_n)$, then $\exists a \in U(a)$ st $K(x) = a\,x (\text{mod}\, n)\, \forall x \in \mathbb{Z}_n \longrightarrow$ where $a = K(1)$.

Question: Find all elements of $\mathrm{Aut}(\mathbb{Z}_{12})$:

Solution:

$$U(12) = \{1, 5, 7, 11\}$$
$$F_1 \colon (\mathbb{Z}_{12}, +) \longrightarrow (\mathbb{Z}_{12}, +)$$
$$F_1(x) = 1 \cdot x (\mathrm{mod}\, 12)\ \forall x \in \mathbb{Z}_{12}$$

$$F_5 \colon (\mathbb{Z}_{12}, +) \longrightarrow (\mathbb{Z}_{12}, +)$$
$$F_2(x) = 5 \cdot x (\mathrm{mod}\, 12)\ \forall x \in \mathbb{Z}_{12}$$

and so on.

Now we can prove the original result; that $(\mathrm{Aut}(\mathbb{Z}_n), \circ) \approx (U(n), \times)$.

Proof:

Define the following function mapping:

$$L \colon U(n) \longrightarrow \mathrm{Aut}(\mathbb{Z}_n)$$

$$L(a) = F_a\ \forall a \in U(n)$$
Recall the definition of F_a:
$$F_a \colon (\mathbb{Z}_n, +) \longrightarrow (\mathbb{Z}_n, +) \text{ st}$$
$$F_a(x) = a\, x (\mathrm{mod}\, n)\ \forall x \in \mathbb{Z}_n$$

Show that L is a group-homomorphism
$$L(a \times b) = L(a) \circ L(b)$$
$$F_{a \times b} = F_a \circ F_b$$
$$F_{a \times b}(x) = a\, b\, x \quad \forall x \in \mathbb{Z}_n$$
$$F_a(x) = a\, x \quad \forall x \in \mathbb{Z}_n$$
$$F_b(x) = b\, x \quad \forall x \in \mathbb{Z}_n$$
$$F_a \circ F_b(x) = F_a(b\, x) = a\, b\, x = F_{a \times b}(x)$$

L is clearly onto because of our sub-result
Choose $K \in \mathrm{Aut}(\mathbb{Z}_n), K = F_a$ for some $a \in U(n)$
$\Longrightarrow L$ is onto

We show that L is $1 - 1$
By showing $\ker(L) = \{1\}$
Let $b \in \ker(L) \Longrightarrow L(b) = F_b(x) = e$
$\Longrightarrow F_b(x) = b\, x = x \forall x \in \mathbb{Z}_n$
Note that $b \in U(n)$
$\Longrightarrow F_b(b) = b^2 = b \Longrightarrow b^{-1} \cdot b^2 = b^{-1} \cdot b$
$\Longrightarrow b = 1$
$\Longrightarrow \ker(L) = \{1\}$

Result: $(U(n), \times)$ is cyclic iff $= 2, 4, \text{or } 2\, p^m$ for some prime, p, and $m \geqslant 1$. Proof will be covered in the next lecture.

Let us take an example first:

$$\begin{aligned} &\text{Consider } U(50) \\ &50 = 2 \times 5^2 \\ &\text{By our result, } U(50) \text{ is cyclic} \end{aligned}$$

$$\begin{aligned} &\text{Consider } U(100) \\ &100 = 2^2 \times 5^2 \\ &\text{By our result, } U(100) \text{ is not cyclic} \end{aligned}$$

If we consider $U(100)$, we know by this result that we cannot have an element of order $\varphi(100)$, because $|U(100)| = \varphi(100)$. Since $\varphi(100) = 40$ and the order of a subgroup or an element must divide $\varphi(100)$, this means that each subgroup of $U(100)$ will have at most order 20.

November 30th, 2020

Consider $U(n)$. Of course, we know that $U(n)$ is Abelian group under multiplication modulo n. We have the following cases and subcases:

1. $n = 2^m$ for $m \geqslant 1$
   a) $m = 1, U(n) = \{1\}$
   b) $m = 2, U(n) = \{1, 3\} = <3> \approx \mathbb{Z}_2$
   c) $m \geqslant 3, U(n) = U(2^m) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{m-2}}$
      $m = 7 \longrightarrow U(2^7) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_{2^5} \approx \mathbb{Z}_2 \oplus \mathbb{Z}_{32}$
      $m = 3 \longrightarrow U(8) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2$
2. $n = p^m, m \geqslant 1, p$ prime, $p \neq 2$
   $\xrightarrow{\text{know}} U(p^m) \approx \mathbb{Z}_{p-1} \oplus \mathbb{Z}_{p^{m-1}}$, from previous idea introduced in lecture. Note that $p = 2$ is exceptional because $\varphi(2^m) = 2^{m-1}$ but we have that $U(2^m) \not\approx \mathbb{Z}_{2^{m-1}}$. In fact, as noted above, $U(2^m) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{m-2}}$.
   For what values of m is $U(2^m)$ cyclic?
   $m = 1 \longrightarrow U(2) = \{1\} \longrightarrow$ cyclic.
   $m = 2 \longrightarrow U(4) \approx \mathbb{Z}_2$
   $m \geqslant 3 \longrightarrow U(2^m) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_{2^{m-2}}$, not cyclic.
   Therefore we can see that $U(2^m)$ is cyclic iff $m = 1, 2$.
   $U(p^m) \approx \mathbb{Z}_{p-1} \oplus \mathbb{Z}_{p^{m-1}} \iff$ cyclic because we have that gcd $(p-1, p^{n-1}) = 1$. Therefore we conlcude that $U(n)$ is cyclic for $n = p^m$, p prime and $m \geqslant 1$. In fact, if we have $m = 1$, we get $U(p) = (\mathbb{Z}_p^*, \cdot) \approx (\mathbb{Z}_{p-1}, +)$

Question:

$$\begin{aligned} &\text{Take } U(2^{10}), a \in U(2^{10}) \text{ st} \\ &|a| = n \text{ is a maximum} \end{aligned}$$

Find the value of n. What is the approach we take to solve a question like this?

Solution:

$$\begin{aligned} &U(2^{10}) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_{2^8} = D \\ &\text{max. order of an element is } D \\ &\text{Recall } |(a, b)| = \text{lcm}\,(|a|, |b|) = 2^8 \\ &\text{because } \mathbb{Z}_n \text{ is cyclic in general} \end{aligned}$$

Remember that $|U(2^{10})| = \varphi(2^{10}) = 2^9$.

Question:

$$\begin{aligned} &\text{Take } U(3^{12}), a \in U(3^{12}) \text{ st} \\ &|a| = n \text{ is a maximum} \end{aligned}$$

Solution:

$$\begin{aligned} &\text{We know that } U(3^{12}) \text{ is cyclic} \\ &|U(3^{12})| = 2 \cdot 3^{11} \\ &\text{Hence } n = 2 \cdot 3^{11} \text{ because the group is cyclic} \\ &\text{and thus if } n \text{ is maximum, it must be } 2 \cdot 3^{11} \end{aligned}$$

Let us take $n = 2\,p^m, m \geqslant 1, p$ prime and $p \neq 2$. Then we have that $\varphi(n) = (p-1)p^{m-1}$ and:

$$U(2p^m) \approx \mathbb{Z}_{p-1} \oplus \mathbb{Z}_{p^{m-1}} \text{ is cyclic}$$

Further, we have that $U(2p^m) \approx (p^m) \approx \mathbb{Z}_{p-1} \oplus \mathbb{Z}_{p^{m-1}}$ because isomorphism is a transitive operation. The number of elements in $U(2p^m)$ is the same as the number of elements in $U(p^m)$.

So far, we know that $U(n)$ is cyclic if $n = 2, 4, p^m$ or $2p^m$. p is prime and $m \geqslant 1$. Are ther any other values for n? No. This is all we have.

Consider $n = p_1^{\alpha_1} p_2^{\alpha_2}$, where p_1 and p_2 are two distinct odd primes.

$$\begin{aligned} \varphi(n) &= (p_1 - 1)p_1^{\alpha_1 - 1} \times (p_2 - 1)p_2^{\alpha_2 - 1} \\ U(n) &\approx \mathbb{Z}_{p_1-1} \oplus \mathbb{Z}_{p_1^{\alpha_1-1}} \oplus \mathbb{Z}_{p_2-1} \oplus \mathbb{Z}_{p_2^{\alpha_2-1}} \\ &\mathbb{Z}_{p_1-1} \oplus \mathbb{Z}_{p_1^{\alpha_1-1}} \text{ is cyclic, even order} \\ &\mathbb{Z}_{p_2-1} \oplus \mathbb{Z}_{p_2^{\alpha_2-1}} \text{ is cyclic, even order} \end{aligned}$$

$$\begin{aligned} &\text{The direct sum of both is even order} \\ &\text{in fact,} \\ &U(n) \approx \mathbb{Z}_{p_1^{\alpha_1} - p_1} \oplus \mathbb{Z}_{p_2^{\alpha_2} - p_2} \\ &\longrightarrow \text{This is not cyclic} \end{aligned}$$

Fact: Take the following:

$$\begin{aligned} n &= p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \cdots \cdot p_k^{\alpha_k} \\ U(n) &\approx U(p_1^{\alpha_1}) \oplus U(p_2^{\alpha_2}) \oplus \cdots \oplus U(p_k^{\alpha_k}) \end{aligned}$$

We always have even, and the gcd between any two cannot be 1. This means that we cannot have cyclic if this were the case.

Result: $U(n)$ is cyclic iff $n = 2, n = 4, n = p^m, n = 2p^m, p$ is prime, $p \neq 2$ and $m \geqslant 1$.

For example, if we take $U(4 \cdot 3^5)$, it is isomoprhic to $U(4) \oplus U(3^5) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{3^4}$. The $\mathbb{Z}_2 \oplus \mathbb{Z}_{3^4}$ poses an issue because it is not of even order and therefore we know that $U(4 \cdot 3^5)$ is not cyclic. It cannot be generated by one element.

Classifcation of Finite Abelian Groups (up to isomorphism):

This whole concept relies on the following result previously introduced in the lecture.

Recall: $H \lhd D, K \lhd D, D = H \cdot K$ and $H \cap K = \{e\}$. This implies $D \approx H \oplus K$.

HW Question:

$$|D| = p^2. \text{ Prove that } D \approx \mathbb{Z}_{p^2} \text{ or } D \approx \mathbb{Z}_p \oplus \mathbb{Z}_p$$

Solution:

$$\begin{aligned}
&D \text{ is Abelian. Since } p \mid |D| \\
\Longrightarrow &D \text{ has an element of order } p, \\
&\text{say } a \\
\Longrightarrow &H = <a> \\
&\text{Choose } b \notin H. \text{ Hence } |b| = p \text{ or } p^2
\end{aligned}$$

$$\begin{aligned}
&\text{If } |b| = p^2 \Longrightarrow D \text{ is cyclic} \\
\Longrightarrow &D \approx \mathbb{Z}_{p^2}
\end{aligned}$$

$$\begin{aligned}
&\text{Assume } |b| = p \\
&\text{Let } K = <b> \\
&K \text{ is a subgroup of } D \text{ with } p \text{ elements} \\
&H \cap K = \{e\} \\
&H \cdot K = D \text{ and thus } D \approx H \oplus K \\
\Longrightarrow &D \approx \mathbb{Z}_p \oplus \mathbb{Z}_p
\end{aligned}$$

Question: Upto isomorphic, classify all Abelian groups with p^3 elements.

Solution:

$$\begin{aligned}
&\text{Assume } D \text{ is not cyclic.} \\
&\text{Let } H < D \text{ with } p^2 \text{ elements} \\
&\text{Hence } H \lhd D \text{ because } p^2 | p^3
\end{aligned}$$

$$\begin{aligned}
&\text{There exists } a \notin H \text{ st } |a| = p \\
&\text{Assume we were able to prove this} \\
&K = <a> \text{ with } p \text{ elements, } K \lhd D \text{ since } D \text{ Abelian} \\
&K \cap H = \{e\} \text{ because } K \text{ cannot be inside } H \\
&\text{since } K = <a> \\
&K \cap H = \{e\} \longrightarrow H \cdot K = D
\end{aligned}$$

$$\begin{aligned}
&D \approx H \oplus K \\
&D \approx \mathbb{Z}_p \oplus \mathbb{Z}_{p^2} \text{ or } D \approx \mathbb{Z}_p \oplus \mathbb{Z}_p \oplus \mathbb{Z}_p \\
&\text{If } D \text{ was cyclic, } D \approx \mathbb{Z}_{p^3}
\end{aligned}$$

D has to have one of these three structures, but it is important to note that the three different groups are not isomorphic to one another. They have completely different structures.

Invariant Factors of Finite Abelian Groups:

We first need to agree that $\mathbb{Z}_{mn} \approx \mathbb{Z}_n \oplus \mathbb{Z}_m$ iff $\gcd(m,n) = 1$.

Proof:

(Sketch) Since $m \mid n\,m$ and $n \mid n\,m$, there is a normal subgroup of $\mathbb{Z}_{mn}$, say H,with n elements, and a normal subgroup F of $\mathbb{Z}_{mn}$ with m elements.

Since $\gcd(m,n) = 1$, $H \cap F = \{e\}$. Hence $H \cdot F = \mathbb{Z}_{mn}$, and by a class result, we know that $\mathbb{Z}_{mn} \approx H \oplus F$. Since H and F are both cyclic and every cyclic group is isomorphic to some $\mathbb{Z}_n$, we can conclude that:

$$\begin{aligned} H \approx \mathbb{Z}_n, F \approx \mathbb{Z}_m \\ \implies \mathbb{Z}_{mn} \approx \mathbb{Z}_n \oplus \mathbb{Z}_m \end{aligned}$$

For example, $\mathbb{Z}_{11 \cdot 17} \approx \mathbb{Z}_{17} \oplus \mathbb{Z}_{11}$. We will need this result to move forward with invariant factors.

Result:

$$D = \mathbb{Z}_{k_1} \oplus \mathbb{Z}_{k_2} \oplus \cdots \oplus \mathbb{Z}_{k_n} \approx \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_w}$$

such that the following property holds true: $m_1 | m_2 | m_3 | \ldots . | m_w$. In other words, m_1 is a factor of m_2, which is a factor of m_3, all the way to m_w. They are continuous factors of one another until the end. Furthermore, $m_1, m_2, \ldots m_w$ are all unique. This means thas each m_i is completely distinct.

Question:

Consider the following group:

$$D = \mathbb{Z}_{15} \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_{10}$$

Find the invariant factors of D.

Solution:

$$\begin{aligned} D \approx \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_w} \\ \text{st each } m_i \text{ is a factor of the next } m_{i+1} \end{aligned}$$

$$\begin{aligned} D \approx \mathbb{Z}_3 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_9 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_5 \\ D \approx \mathbb{Z}_{15} \oplus \mathbb{Z}_{90}, \text{ and thus:} \\ m_1 = 15, m_2 = 90 \\ \text{These two are clearly unique by our result} \end{aligned}$$

We can write $D \approx \mathbb{Z}_3 \oplus \mathbb{Z}_5 \circ \oplus \mathbb{Z}_{90}$. However, although this is true in terms of isomorphism, there is only one way of writing D in terms of its invariant factors. In this, clearly 3 is not a factor of 5.

Question:

$$D = \mathbb{Z}_8 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{12}$$

Find the invariant factors of D.

Solution:

$$D \approx \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \cdots \oplus \mathbb{Z}_{m_w}$$
$$\text{st } m_1 | m_2 | \ldots . | m_w$$

$$\text{We can see that } D \approx \mathbb{Z}_8 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_{12}$$
$$\text{We combine the } \mathbb{Z}_8 \text{ and } \mathbb{Z}_3 \text{ since gcd } (8,3) = 1$$
$$D \approx \mathbb{Z}_2 \oplus \mathbb{Z}_{12} \oplus \mathbb{Z}_{24}$$
$$m_1 = 2, m_2 = 12, m_3 = 24$$

There is no algorithm to this. We simply have to try and see what we can get. Notice that in the above example, we know that the last term, m_w, is given by: $\text{lcm}\,(8,6,12) = 24$. So we need to try to see how we can play with the isomorphism to get all the m_i to be a factor of 24.

Question:

$$D \approx \mathbb{Z}_{17} \oplus \mathbb{Z}_{19} \oplus \mathbb{Z}_{29}$$

Solution:

In this example, we clearly know that since the gcd between the three numbers is 1, then:

$$D \approx \mathbb{Z}_{17 \times 19 \times 29}, \text{with } m_1 = 17 \times 19 \times 29$$

We are done. We only have one invariant factor in this case.

Question:

$$D \approx \mathbb{Z}_4 \oplus \mathbb{Z}_{16} \oplus \mathbb{Z}_{32}$$

In this case, we know that each of them are clearly factors of the one that follows, and thus $m_1 = 4$, $m_2 = 16$ and $m_3 = 32$.

Classification of Finite Abelian Groups:

Question:

Upto isomorphism, classify all Abelian groups with 81 elements. Note that $(81 = 3^4)$. This means that we want to list all possible non-isomorphic groups in terms of direct sums of $\mathbb{Z}_n$.

So if we have one particular Abelian group that has 81 elements, let us call it D, then D is isomoprhic to one and only one of these structures in the list.

Let us make a table to see this example. Note that all of these structures are NOT isomorphic to each other.

Partitions of 4	**structures with 81 elements**
1+1+1+1	$\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3$
2+2	$\mathbb{Z}_9 \oplus \mathbb{Z}_9$
1+3	$\mathbb{Z}_3 \oplus \mathbb{Z}_{27}$
1+1+2	$\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_9$
4	$\mathbb{Z}_{81}$ (cyclic)

Table 4.

Fact: $D \approx F$ iff the invariant factors of D equal the invariant factors of F. If we use this result, we can get the structures essentially for free.

Question:

Imagine we were told that D has 81 elements and D has an element of order 27. Upto isomorphic, find all possible groups that D is isomorphic to.

Solution:

We simply go to the table we just created and look at it to see in each of the 5 options, an element of order 27 could exist.

There are the following:

$$D \approx \mathbb{Z}_3 \oplus \mathbb{Z}_{27}$$
$$D \approx \mathbb{Z}_{81}$$

These are the only two possibilities. No matter what we do, these are the only two possibilities for the structure of D. Note that (Reminder) D is Abelian.

Question:

Imagine D has 81 elements and it has an element of order 27, and D is not cyclic. What are the possible structures of D upto isomorphism?

Solution:

To add on to the previous question, we know that the group $\mathbb{Z}_{81}$ is cyclic, because it contains the same number of elements as D. This new piece of information shows us that the only possible group structure for D is: $\mathbb{Z}_3 \oplus \mathbb{Z}_{27}$.

Question:

Upto isomorphism, classify all finite Abelian groups with 36 elements.

Solution:

We first start with the prime factorization of 36.

$$36 = 3^2 \cdot 2^2$$

Note that $D \approx H \oplus K$, where $|H| = 9$ and $|K| = 4$, with $H \cap K = \{e\}$.

We will proceed by doing two tables:

Partitions of 2	$\mathbf{3^2 = \lvert H \rvert}$	$\mathbf{2^2 = \lvert K \rvert}$
2	$\mathbb{Z}_9$	$\mathbb{Z}_4$
1+1	$\mathbb{Z}_3 \oplus \mathbb{Z}_3$	$\mathbb{Z}_2 \oplus \mathbb{Z}_2$

Table 5.

Here are all our choices for the possible structures for D:

$$\mathbb{Z}_9 \oplus \mathbb{Z}_4 \quad (1)$$
$$\mathbb{Z}_9 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2 \quad (2)$$
$$\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_4 \quad (3)$$
$$\mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_3 \quad (4)$$

We can rewrite these 4 in terms of their invariant factors:

$$\mathbb{Z}_{36} \quad (1)$$
$$\mathbb{Z}_2 \oplus \mathbb{Z}_{18} \quad (2)$$
$$\mathbb{Z}_3 \oplus \mathbb{Z}_{12} \quad (3)$$
$$\mathbb{Z}_6 \oplus \mathbb{Z}_6 \quad (4)$$

None of them are isomorphic to each other because their invariant factors are not the same at all.

As a quick example, if we said our group has an element of order 18, then clearly the possible structures are either (1) or (2). If we instead said that our group is not cyclic, then the only possibility would be (3), since the rest are all cyclic groups.

December 9th, 2020

Let us look back and remember some facts:

1. $|U(n)| = \varphi(n)$
2. $(U, \cdot)$ is a cyclic group iff $n = 2, 4, p^m, 2p^m$ where p is an odd prime number with $m \geqslant 1$
3. $$n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \dots \cdot p_k^{\alpha_k}$$
$$U(n) \approx U(p_1^{\alpha_1}) \oplus U\left(p_2^{\alpha_2}\right) \oplus \dots \oplus U(p_k^{\alpha_k})$$
4. $U(2^m) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_{m-2}$, with $m \geqslant 3$
5. Finally, $U(p^m) \approx \mathbb{Z}_{p-1} \oplus \mathbb{Z}_{p^{m-1}}$

Let us take an example. Consider $n = 2^6 \times 5^3 \times 7^2$. Then we know that:

$$U(n) \approx U(2^6) \oplus U(5^3) \oplus U(7^2)$$

$$U(n) \approx \mathbb{Z}_2 \oplus \mathbb{Z}_{2^4} \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{5^2} \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_7$$

Now, what do we need to do to find the invariant factors?

$$U(n) \approx \mathbb{Z}_{m_1} \oplus \mathbb{Z}_{m_2} \oplus \dots \oplus \mathbb{Z}_{w_k}$$
$$\text{We can find } w_k = \operatorname{lcm}(2, 2^4, 4, 5^2, 6, 7)$$
$$w_k = 2^4 \cdot 5^2 \cdot 3 \cdot 7$$

Alternatively, we can use the formula:
$$\operatorname{lcm}(a, b) = \frac{a \times b}{\gcd(a, b)}$$
$$\text{let } a = p_1^{\alpha_1} \cdot \dots \cdot p_k^{\alpha_k}$$
$$\text{and let } b = q_1^{\beta_1} \cdot \dots \cdot q_m^{\beta_m}$$
We can find the common primes between a and b
$$\text{call them } f_1, f_2, \dots, f_l$$
$$\gcd(a, b) = f_1^{\min(\alpha_1, \beta_1)} \cdot \dots \cdot f_l^{\min(\alpha_l, \beta_l)}$$
$$\operatorname{lcm}(a, b) = f_1^{\max(\alpha_1, \beta_1)} \cdot \dots \cdot f_l^{\max(\alpha_l, \beta_l)}$$
we also add all missing primes to this.

Consider the following example to make this clear:

$$a = 3^2 \cdot 5^3 \cdot 7^2 \cdot 2^{10}$$
$$b = 2^3 \cdot 7^2 \cdot 3$$

$$\gcd(a,b) = 2^3 \cdot 7^2 \cdot 3$$
$$\operatorname{lcm}(a,b) = 2^{10} \cdot 3^2 \cdot 7^2 \cdot 5^3$$

Question:

$$n = 2^5 \cdot 3^2 \cdot 7^2$$

Write $U(n)$ is terms of its invariant factors

Solution:

$$\begin{aligned} U(n) &\approx U(2^5) \oplus U(3^2) \oplus U(7^2) \\ &\approx \mathbb{Z}_2 \oplus \mathbb{Z}_{2^3=8} \oplus \mathbb{Z}_3 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_7 \end{aligned}$$

But these are not invariant factors.

$$m_w = 7 \cdot 6 \cdot 8$$

We have $\mathbb{Z}_{7\cdot 6\cdot 8}$ as our last term

$$\mathbb{Z}_2 \oplus \mathbb{Z}_6 \oplus \mathbb{Z}_{7\cdot 6\cdot 8}$$

Another example:

$$\text{Consider } U(2^5 \cdot 3 \cdot 5^2)$$
$$\begin{aligned} U(n) &\approx U(2^5) \oplus U(3) \oplus U(5^2) \\ &\approx \mathbb{Z}_2 \oplus \mathbb{Z}_8 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_5 \\ m_w &= \operatorname{lcm}(2,8,2,4,5) = 5 \cdot 8 \\ &\approx \mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_4 \oplus \mathbb{Z}_{5\cdot 8} \end{aligned}$$

Therefore:

$$m_1 = 2, m_2 = 2, m_3 = 4, m_4 = 40$$

Question:

Classify all finite Abelian groups upto isomorphism of order $2^3 \cdot 3^2 \cdot 5^3$.

Solution:

We will proceed by making the table for the partitions

Partition of 3	**Partition of 2**	**order 2^3**	**order 3^2**	**order 5^3**
0+3	0+2	$\mathbb{Z}_8$	$\mathbb{Z}_9$	$\mathbb{Z}_{125}$
1+2	1+1	$\mathbb{Z}_2 \oplus \mathbb{Z}_4$	$\mathbb{Z}_3 \oplus \mathbb{Z}_3$	$\mathbb{Z}_5 \oplus \mathbb{Z}_{25}$
1+1+1		$\mathbb{Z}_2 \oplus \mathbb{Z}_2 \oplus \mathbb{Z}_2$		$\mathbb{Z}_5 \oplus \mathbb{Z}_5 \oplus \mathbb{Z}_5$

Table 6.

Counting the number of choices, we will have exactly $2 \times 3 \times 3$ non-isomorphic groups of our order. This means there is a total of 18 structures for our group of order $2^3 \cdot 3^2 \cdot 5^3$

Introduction to Rings:

We have $(R, +, \cdot)$, a set R with two binary operations, $+$ and $\cdot$. It needs to satisfy the following conditions:

1. $(R, +)$ is an Abelian group
2. $(R, \cdot)$ is a semi-group (Recall that this means it has closure and is associative)
3. $\forall a, b, c \in R$, we want $a \cdot (b + c) = a \cdot b + a \cdot c$. This is the distributive property, both from the right and the left. i.e. $(b + c) \cdot a = b \cdot a + c \cdot a$

A ring is any structure that satisfies these three properties. Our set does not need to be Abelian under $\cdot$, but it definitely needs to be Abelian under $+$.

If $(R^*, \cdot)$, where $R^* = R - \text{additive identity of } R$, is Abelian, we say that R is a field. A field is a ring, but in the second condition, we remove the additive identity and see whether we have an Abelian group rather than a semi-group.

Let us see some examples of rings:

$$(\mathbb{Z}, +, \times) \text{ is a ring}$$

This is because $\mathbb{Z}$ under addition is an Abelian group and $\mathbb{Z}$ under multiplication is a semi-group. In fact, this is a commutative ring. This is because $\mathbb{Z}$ under multiplication is the same regardless of order. $a \times b = b \times a$.

$$(\mathbb{R}^{2\times 2}, +, \cdot) \text{ is also a ring}$$

This, however, is not a commutative ring, because the order of multiplication matters in the context of 2×2 matrices.

The set of all continuous functions under addition and composition (semi-group, but non-commucative) is also a ring.
