Introduction to Group Theory - Application Notes

Dom Hutchinson

May 12, 2018

How to Use One-Line Notation

Theory
One-line notation is used to denote permutations.
Then n^{th} entry shows where n is sent to.
So if σ is a permutation & $S = \{a_1, \dots, a_n\}$ is a set then σ can be denoted as $\sigma = \begin{pmatrix} \sigma(a_1) & \dots & \sigma(a_n) \end{pmatrix}$.

Process
To perform σ on S.
Create $|S|$ free spaces.
Place the first item of S in the position denoted by the first position on the one-line notation.
Repeat this $\forall\ a_i,\ i \leq |S|, i \in \mathbb{N}$.

Example
Let $S = \{1, 2, 3, 4, 5\}$ and $\sigma = \begin{pmatrix} 5 & 4 & 2 & 1 & 3 \end{pmatrix}$ in one-line notation.
Then $\underline{\sigma(S) = \{4, 3, 5, 2, 1\}}$.

How to Use Two-Line Notation

Theory
Two-line notation is used to denote permutations.
It is shown on two lines, which should we read as columns.
The top entry is the initial position & the bottom is the destination.
So σ can be denoted as $\sigma = \begin{pmatrix} a_1 & \dots & a_n \\ \sigma(a_1) & \dots & \sigma(a_n) \end{pmatrix}$.

Process
To perform σ on S.
Create $|S|$ free spaces.
Take an element from S.
Read along the top row until you find this element.
Place this element in the position denoted by the element below.
Repeat $\forall\ s \in S$.

Example
Let $S = \{1, 2, 3, 4, 5\}$ and $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 5 & 4 & 2 & 1 & 3 \end{pmatrix}$ in two-line notation.
Then $\underline{\sigma(S) = \{4, 3, 5, 2, 1\}}$.

How to Use Cycle-Decomposition Notation

Theory

Cycle-Decomposition notation is used to denote permutations.
The position an element goes to is denoted by the next element in a cycle.
The last element goes to the position denoted by the first element.
So σ can be denoted as $\sigma = \big(a_1 \quad \sigma(a_1) \quad \sigma(\sigma(a_1)) \quad \dots \quad \sigma(\dots\sigma(a_1))\big)$.
Cycles are disjoint if each element appears in only one cycle.
They are read from *right to left.*

Process

To perform σ on S.
Take the first element from S.
Starting with the rightmost cycle, read to the left until you find this element.
Place this item in the position denoted by the element on the right.
Position the rest of the items in a cycle.
Once a cycle has been completed, identify the next item in S which has not been position.
Sort this element.
Repeat this until all the elements have been sorted.

Example

Let $S = \{1, 2, 3, 4, 5\}$ and define $\sigma = (1, 5)(2, 4, 3)$ in cycle-decomposition notation.
Then $\sigma(S) = \{5, 3, 4, 2, 1\}$.

How to Prove something is a Group

Theory

A group is constituted of a set & a binary operation.
The operation must be associative.
The group must have an identity element.
Each element of the group must have an inverse element.
The group is closed under operation.

Process

To show associativity show that $(x * y) * z = x * (y * z)$.
To show an identity element show that $\exists\ e \in G\ st\ xe = x = ex\ \forall\ x \in G$.
To show an inverse show that $\forall\ x \in G\ \exists\ x^{-1} \in G\ st\ xx^{-1} = e = x^{-1}x$.
To show closure show that $\forall\ x, y \in G$ then $x * y \in G$.

Example
Show that $(2\mathbb{Z},+)$ is a group.

Let $x, y, z \in \mathbb{Z}$ then $2x, 2y, 2z \in G$.
$(2x+2y)+2z = 2(x+y)+2x = 2(x+y+z) = 2(x+y+z) = 2(x+(y+z)) = 2x+(2y+2z)$.

Set $2x+2e = 2x \implies 2e = 0 \implies e = 0$
Set $2e+2x = 2x \implies 2e = 0 \implies e = 0$.
So 0 is the identity element.

$2x+2y = 2(x+y)$ since $(x+y) \in \mathbb{Z}$ so $2x+2y \in G$.

G has all the properties of a group, therefore it is a group.

How to Prove a Group is Abelian

Theory
An operation is *commutative* is $x * y = y * x$, so order does not affect result.
A group is *abelian* if its operation is commutative.

Example
Show that $(\mathbb{Z}, *)$ where $x * y = x * y + 1$ is abelian.
$x * y = x + y + 1 = y + x + 1 = y * x$.

How to Prove a Group is a Valid Subgroup

Theory
A *subgroup* keeps the operation of its master hroup, but with a subset of its elements.
THis is denoted by $H \leq G$ where H is a subgroup of G.
It must maintain all the properties of a group.

Process
To show associativity show that $(x * y) * z = x * (y * z)$.
To show an identity element show that $\exists\ e \in G\ st\ xe = x = ex\ \forall\ x \in G$.
To show an inverse show that $\forall\ x \in G\ \exists\ x^{-1} \in G\ st\ xx^{-1} = e = x^{-1}x$.
To show closure show that $\forall\ x, y \in G$ then $x * y \in G$.

Example
Show $H = (2\mathbb{Z},+)$ is a valid subgroup of $G = (\mathbb{Z},+)$.

Let $x, y, z \in \mathbb{Z}$ then $2x, 2y, 2z \in H$.
$(2x+2y)+2z = 2(x+y)+2x = 2(x+y+z) = 2(x+y+z) = 2(x+(y+z)) = 2x+(2y+2z)$.

Set $2x+2e = 2x \implies 2e = 0 \implies e = 0$
Set $2e+2x = 2x \implies 2e = 0 \implies e = 0$.
So 0 is the identity element.

$2x+2y = 2(x+y)$ since $(x+y) \in \mathbb{Z}$ so $2x+2y \in H$.

Since $(2\mathbb{Z},+)$ has all the properties of a group, thus is a valid subgroup.

How to Prove a Group is Cyclic

Theory

The *order* of an element is the fewest number of times it needs to operated on itself to produce the identity element.

$ord(x) = n \implies x^n = e.$

The set of elements generated by an element, $x \in G$, is denoted by $\langle x \rangle = \{x^i : i \in \mathbb{Z}\} \leq G.$

If $\exists\ g \in G\ st\ \langle g \rangle = G$ such that $\langle g \rangle = G$ then G is *cycle* with g as the generator.

$\frac{\mathbb{Z}}{n\mathbb{Z}}, n \in \mathbb{N} = \{[a] : a \in \mathbb{N}; gcd(a, n) = 1\}.$

Example

Show that $U_{11} = \left(\frac{\mathbb{Z}}{11\mathbb{Z}}, \cdot\right)$ is cyclic.

$U_{11} = \{[1], [2], [3], [4], [5], [6], [7], [8], [9], [10]\}.$

$$\begin{array}{ll}
[2]^1 = [2] & [2]^6 = [20] = [9] \\
[2]^2 = [4] & [2]^7 = [18] = [7] \\
[2]^3 = [8] & [2]^8 = [14] = [3] \\
[2]^4 = [16] = [5] & [2]^9 = [6] \\
[2]^5 = [10] & [2]^{10} = [12] = [1]
\end{array}$$

[2] is a generator of U_{11}.

How to Perform Modular Arithmetic

Theory

$a \equiv b(mod\ n) \implies n|(a-b)$ & $\exists\ m \in \mathbb{Z}$ such that $mn + b = a$.

A *congurence class* of $a(mod\ n)$ is defined as

$[a]_n = \{b \in \mathbb{Z} : a \equiv b(mod\ n)\} = \{\dots, a-n, a, a+n, a+2n, \dots\}.$

Process

$[a] + [b] = [a+b].$

$[a].[b] = [ab].$

N.B. - $[a+b] = [a+b-n]$ so if $a+b \geq n$ subtract n until this is not true, do the same if $ab \geq n$.

How to Prove an Operation is Homomorphic

Theory

An opeartion, $\phi : G \to H$ where $G = (G, *)$ & $H = (H, \cdot)$, is *homomorphic* if

$\phi(x * y) = \phi(x) \cdot \phi(y)\ \forall\ x, y \in G.$

Process

Show that ϕ is a valid map, *i.e* its output is unambiguous.

Show that $\phi(x * y) = \phi(x) \cdot \phi(y)$.

Example
Let $\phi : \mathbb{R} \times \mathbb{R} \to \mathbb{R}$ such that $\phi(x, y) = x + y$.
Show that ϕ is homomorphic.

Let $x_1, x_2, y_1, y_2 \in \mathbb{R}$.

$$\begin{aligned} \phi((x_1, y_1) + (x_2, y_2)) &= \phi((x_1 + x_2, y_1 + y_2)) \\ &= x_1 + x_2 + y_1 + y_2 \\ &= (x_1 + y_1) + (x_2 + y_2) \\ &= \underline{\phi(x_1, y_1) + \phi(x_2, y_2)}. \end{aligned}$$

How to Prove an Operation is Isomorphic

Theory
An opeartion, $\phi : G \to H$ where $G = (G, *)$ & $H = (H, \cdot)$, is *isomorphic* if
$\phi(x * y) = \phi(x) \cdot \phi(y)\ \forall\ x, y \in G$ and $\underline{\phi \text{ is bijective}}$.

Process
Show that ϕ is a valid map, *i.e* its output is unambiguous.
Show that ϕ is homomorphic, *i.e.* $\phi(x * y) = \phi(x) \cdot \phi(y)$.
Show that ϕ is injective, *i.e.* If $\phi(x) = \phi(y) \implies x = y$.
Show that ϕ is surjective, *i.e.* $\forall\ x \in G\ \exists\ y \in H\ st\ \phi(x) = y$.
Thus ϕ is bijective & homomorphic, thus an *isomorphism.*

Example
Let $G = (G, +)$ & $H = (H, \times)$.
Define $\phi : G \to H$ as $\phi(x) = e^x$. Show that ϕ is an isomorphism.

$\phi(x + y) = e^{x+y} = e^x e^y = \phi(x)\phi(y)$.
ϕ is homomorphic.

Let $x, y \in G$ such that $\phi(x) = \phi(y)$.
$\implies e^x = e^y$
$\implies ln(e^x) = ln(e^y)$
$\implies x = y$.
ϕ is injective.

Let $y = e^x$.
$\implies x = ln(y)$
$\implies f(x) = f(ln(y))$
$\implies e^x = e^{ln(y)} = y$.
ϕ is surjective.

Since ϕ is injective & surjective it is bijective.
Since ϕ is homomorphic & bijective then it is an isomorphism.

How to Prove Lagrange's Theorem

Theory
Lagrange's Theorem states that
If G is a finite group & $H \leq G$ then $|H|$ divides $|G|$.
Cosets are the set formed by operating on all elements of a subgroup with a single element of the main group.
There are two types of cosets, left & right.
$xH = \{xh : h \in H\}$ &$Hx = \{hx : h \in H\}$.

Proof
Let $g \in G$.
Then $g = ge = gH$.
So $G = \bigcup_{g \in G} gH$

Then $|G| = \sum_{g \in G} |gH| = \#$ cosets $\times |H|$.
Hence $|H|$ divides $|G|$.

How to Apply Fermat's Little Theorem & the Fermat-Euler Theorem

Theory
Fermat's Little Theorem states that
If p is prime, $a \in \mathbb{Z}$ & $p \not| a$ then $a^{p-1} \equiv 1 (mod\ p)$.
Euler's Phi Function, $\phi\mathbb{N} \to \mathbb{N}$, is the number of natural numbers which are less than & co-prime to a given number.
$\phi(n) = |\{a \in \mathbb{N} : a \leq m, gcd(a,m) = 1\}|$.
The *Fermat-Euler Theorem* states
If $m > 0$ &$a \in \mathbb{Z}$ with $gcd(a,m) = 1 \implies a^{\phi(m)} \equiv 1(mod\ m)$.

Example
Find $2^300(mod\ 17)$.

$gcd(2,17) = 1$ & $\phi(17) = 16$.
So by the *Fermat-Euler Theorem* $2^{16} \equiv 1(mod\ 17)$.

$$\begin{array}{rrcl} & 300 & = & 18 \times 16 + 12 \\ \implies & 2^{300} & = & (2^{16})^{18} 2^{12} \\ \implies & 2^{300} & \equiv & 2^{12}(mod\ 17) \\ \\ & 12 & = & 3 \times 4 \\ & 2^4 & = & 16 \equiv (-1)(mod\ 17) \\ \implies & 2^{12} & \equiv & (2^4)^3(mod\ 17) \\ & & \equiv & (-1)^3(mod\ 17) \\ & & \equiv & -1(mod\ 17) \\ \implies & 2^{300} & \equiv & \underline{16(mod\ 17)} \end{array}$$

How to Simplify Transpositions

Theory
A transposition is a switch of 2 elements.
Read them from *right to left*.

Process
Take the first element of S.
Start on the right & follow the path of this element.
Write down where it ends up.
Now repeat with this position you just found.
When you cycle back to the first element find the next element in S which has not been placed.

Example
Simplify $(1,2)(2,4)(1,5)(3,5)(1,2)(2,4)$.

$$\begin{aligned}&1 \to 2 \to 4\\&4 \to 2 \to 1 \to 5\\&5 \to 3\\&3 \to 5 \to 1 \to 2\\&2 \to 4 \to 2 \to 1\\&\underline{(1,4,5,3,2)}\end{aligned}$$

How to Prove a Group is Normal

Theory
$N \leq G$ is a *normal subgroup* if
$gng^{-1} \in \mathbb{N} \ \forall \ g \in G, n \in N$.
This is then denoted as $N \trianglelefteq G$.
This means $gN = Ng \ \forall \ g \in G$.

Process
Show that $gN = Ng \ \forall \ g \in G$.

Example
Prove $\langle a \rangle$ is a normal subgroup of D_{2n}.

$\langle a \rangle = \{a, a^2, \dots, a^{n-1}, e$.

Let $a^i \in \langle a \rangle$.
$a^i b = ba^{-i} = ba^{n-i}$.
$(n-i) \in [0, n)$ so $b\langle a \rangle = \langle a \rangle b$.

$a^j a^i = a^{i+j} = a^j a^i$.
So $a^i \langle a \rangle = \langle a \rangle a^i \ \forall \ i \in \mathbb{N}$.

$e\langle a \rangle = \langle a \rangle = \langle a \rangle e$.

So $x\langle a \rangle = \langle a \rangle x \ \forall x \in D_{2n}$.
$\underline{\langle a \rangle \text{ is a normal subgroup.}}$

How to Prove The Homomorphism Theorem

Theory
The Homomorphism Theorem states that
if G, H be groups and $\varphi : G \to H$ is a homomorphism then $Ker(\varphi) \trianglelefteq G, Im(\phi) \leq H$ & $G/ker(\varphi) \cong Im(\varphi)$.

Process
Show the function is well defined.
Show the function is a homomorphism.
Show the function is injective, $f(x) = f(y) \implies x = y$.
Show the function is surjective, $\forall\ y \in H\ \exists\ x \in G\ st\ f(x) = y$.
Thus the function is bijective and thus an isomorphism.

Proof
Define $\alpha : G/Ker(\varphi) \to Im(\varphi)$ such that

$$\alpha([g]) = \varphi(g)$$

WTS α is well defined.

$$\begin{aligned} \text{Take } [x] = [y] \implies x &= yn \in yN \\ \implies \varphi(x) &= \varphi(yn) \\ &= \varphi(y)\varphi(n) \\ &= \varphi(y)e_H \\ &= \varphi(y) \end{aligned}$$

WTS α is a homomorphism

$$\begin{aligned} \alpha([x][y]) &= \alpha([xy]) \\ &= \varphi(xy) \\ &= \varphi(x)\varphi(y) \\ &= \alpha([x])\alpha([y]) \end{aligned}$$

WTS α is a bijective, and thus an isomorphism

$$\begin{aligned} &\text{Let } [x] \in Ker(\alpha) \\ &\implies \varphi(x) &&= e_H \\ &\implies x \in Ker(\varphi) \\ &\implies [x] &&= [e] \in G/Ker(\varphi) \\ &\text{So } \ \alpha \text{ is injective.} \\ &\text{Let } \varphi(g) \in Im(\varphi) \\ &\implies \varphi(g) &&= \alpha([g]) \in Im(\alpha) \end{aligned}$$

So α is surjective and thus is bijective and an isomorphism.