Introduction to Group Theory - Notes

Dom Hutchinson

April 17, 2018

Contents

1 Symmetries

Definition 1.01 - *Permutation*
A *permutation* of a set, G, is a bijection of the form $f : G \to G$.
N.B. - Since the composition of two bijections is also a bijection, then the composition of two permutations is a permutation.

Definition 1.02 - *Symmetries of a Polygon*
A *symmetry* of an n-sided polygon is a permutation of the vertices which preserves adjacency. So if the vertices u & v are adjacent then the permutation f is a symmetry if $f(u)$ & $f(v)$ are adjacent.

Remark 1.03 - *Symmetries*
When dealing with symmetries of a shape then they can only be rotations or reflections.

Definition 1.04 - *Identity*
The trivial symmetry, which maps an element to itself, is known as the identity.

Remark 1.05 - *Composition of Permutations*
Let R, S & T be permutations.
Then $(RS)T$ means do T, then S, then R. So

$$(RS)T = R(ST)$$

Remark 1.06 - *One-Line Notation*
Let $S = \{a_1, \dots, a_n\}$ be a set and $\sigma : S \to S$ be a permutation.
One-Line notation denotes the result of σ by

$$\begin{pmatrix}\sigma(a_1) & \dots & \sigma(a_n)\end{pmatrix}$$

So if σ maps $1 \to 2, 2 \to 3, \dots, n \to 1$ then it can be denoted by

$$\begin{pmatrix}2 & 3 & \dots & n & 1\end{pmatrix}$$

Remark 1.07 - *Two-Line Notation*
Let $S = \{a_1, \dots, a_n\}$ be a set and $\sigma : S \to S$ be a permutation.
Two-Line notation denotes the result of σ by

$$\begin{pmatrix}a_1 & \dots & a_n \\ \sigma(a_1) & \dots & \sigma(a_n)\end{pmatrix}$$

So if σ maps $1 \to 2, 2 \to 3, \dots, n \to 1$ then it can be denoted by

$$\begin{pmatrix}1 & 2 & \dots & n-1 & n \\ 2 & 3 & \dots & n & 1\end{pmatrix}$$

Remark 1.08 - *Cycle Decomposition Notation*
Let $S = \{a_1, \dots, a_n\}$ be a set and $\sigma : S \to S$ be a permutation.
Cycle Decomposition Notation denotes σ as the product of disjoint cycles.
Each element in a cycle goes the position of the element after it in the list, the last element goes to the position of the first.
() denotes no variation. The operation of σ is denoted by

$$\begin{pmatrix}a_1 & \sigma(a_1) & \sigma(\sigma(a_1)) & \dots & \sigma(\dots\sigma(a_1)\dots)\end{pmatrix}$$

2 Groups

Definition 2.01 - *Binary Operation*
A *binary operation* on a set X is a function of the form $f : X \times X \to X$.

Remark 2.02 - *Asteriks Notation*
Binary operations are general denoted by an $*$.

$$f(x, y) = x * y$$

Remark 2.03 - *Multiplicty Notation*
Multiplicity notation is used to simplify equations with a single binary operator, by not writting $*$.

$$x * y = xy$$

Remark 2.04 - *Set of Permutations*
A set of permutations have a binary operation for composition.
Let f, g, h be permutations of a set X and $x \in X$

$$f(x) \times g(x) \to h(x)$$

Definition 2.05 - *Commutativity*
A binary operation, $*$, on a set X is *commutative* if order of input doesn't affected the outcome.

$$x * y = y * x, \forall\ x, y \in X$$

Definition 2.06 - *Commute*
If $x, y \in G$ satisfy $x * y = y * x$ then it is said that x & y commute.

Defintion 2.07 - *Group*
A group is a set, G, with an associated binary operation, $*$, that

i) Is *associative*, $(x * y) * z = x * (y * z)\ \forall\ x, y, z \in G$;

ii) Has as an *identity element*, $\exists\ e \in G$ such that $x * e = x = e * x$; and,

iii) Has an inverse element $\forall\ x \in G\ \exists\ x^{-1} \in G$ st $xx^{-1} = e = x^{-1}x$.

Remark 2.08 - *Group Notation*
The group of set G and binary operation $*$ is denoted by $(G, *)$.

Definition 2.09 - *Abelian Group*
An *Abelian group*, $(G, *)$ is one where $*$ is commutative.

3 Elementary Consequences of the Definition

Proposition 3.01 - *Right Cancellation*
If $a, b, x \in G$ and $ax = bx$ then $a = b$.

Proposition 3.02 - *Left Cancellation*
If $a, b, x \in G$ and $x =>$ then $a = xba = b$.

Proposition 3.03 - *Uniqueness of Identity*
If $a, x, e \in G$ with e as the identity of G then

$$ax = a => e = x$$

Proposition 3.04 - *Uniqueness of Inverses*
If $x, y, e \in G$ with e as the identity of G then

$$xy = e => x = y^{-1} \ \& \ y = x^{-1}$$

Proposition 3.05 - *Inverse of Inverse*
Let $x \in G$ then

$$(x^{-1})^{-1} = x$$

Proposition 3.06 - *Composite Inverses*
Let $x, y \in G$ then

$$(xy)^{-1} = y^{-1}x^{-1}$$

Definition 3.07 - *Caley Table*
Let e, x, y be all the elements of G then the result of all compositions can be displayed in a *Caley Table.*

	e	x	y
e	e	x	y
x	x	xx	yx
y	y	xy	yy

The operation of the column is done first, then the operation of the row.
N.B. - All values in any given column or row are unique, so all elements of G appear exactly once.

Definition 3.08 - *Powers of Elements*
If $n > 0$ then x^n means $x * \cdots * x$ n times.

$$x^{-n} = (x^n)^{-1} = (x^{-1})^n, \quad x^0 = e$$

Definition 3.09 - *Composition of Powers*
For $m, n \in \mathbb{Z}$

$$x^m x^n = x^{m+n}$$

4 Dihedral Groups

Definition 4.01 - *Order*
The *order* of a group G is the number of elements in G.
N.B. - Order of G is denoted by $|G|$.

Definition 4.02 - *Dihedral Groups*
The *dihedral group* D_{2n} is the group of symmetries of a regular n-sided polygon, with $n \geq 3$.
N.B. - $|D_{2n}| = 2n$.

Proposition 4.03 - *Elements of Dihedral Group*
Let a describe a rotation by $\frac{2\pi}{n}$ and b a reflection then

$$D_{2n} = \{e, a, a^2, \dots, a^{n-1}, b, ab, \dots, a^{n-1}b\}$$

N.B. - $a^n = e = b^2, \quad a^{-1} = a^{n-1}, b = b^{-1}$.

Proposition 4.04 - *Reflections & Rotations*
Let a denote a rotation and b denoted a reflection then

$$ab = ba^{-1}$$

5 Subgroups

Definition 5.01 - *Subgroup*
A *subgroup* of a group G is a group formed of a subset of G with the same associated operation.
N.B. - H being a subgroup of G is denoted by $H \leq G$.

Definition 5.02 - *Non-Trivial Subgroup*
A subgroup H of G is non-trivial if $H \neq \{e\}$.

Definition 5.03 - *Proper Subgroup*
A subgroup H of G is a *proper subgroup* if $H \neq G$.

Theorem 5.04 - *Subgroup*
A subset H of a group G is a subgroup iff

i) It is closed under the binary operation $x, y \in H => xy \in H$;

ii) It has an identity element $\exists\ e \in H$ st $xe = x\ \forall\ x \in H$; and,

iii) All elements have an inverse $\forall\ x \in H\ \exists\ x^{-1} \in H$ st $xx^{-1} = e$.

Proposition 5.05 - *Pairs of Subgroups*
Let G, H & K be groups with $H \leq G$ & $K \leq G$ then $H \cap K \leq G$.

6 Order of Elements

Definition 6.01 - *Order of an Element*
Let $x \in G$ such that $x^n = e$, then the *order* of x is the smallest such n.

$$ord(x) = n$$

N.B. - If there is no such n then $ord(x) = \infty$.

Proposition 6.02 - *Uniqueness of Powers*
Let $x \in G$ with $ord(x) = \infty$ then

$$x^i \neq x^j\ \forall\ i \neq j$$

Theorem 6.03 - *Order Elements in a Finite Group*
Every element of a finite group has finite order.

Theorem 6.04 - *Properties of Order of an Element*
Let $x \in G$ such that $ord(x) = n < \infty$ then if

i) $x^i = e \iff n|i$;

ii) $x^i = x^j \iff i \equiv j(mod\ n)$;

iii) $x^{-1} = x^{n-1}$; and,

iv) The powers of x less than n are all distinct.

Proposition 6.05 - *Order of Powers of Elements*
Let $x \in G, i \in \mathbb{Z}$.

i) If $ord(x) = \infty$ then $ord(x^i) = \infty$ if $i \neq 0$; and,

ii) If $ord(x) = n < \infty$ then $ord(x^i) = \dfrac{n}{gcd(n, i)}$.

7 Cyclic Groups & Cyclic Subgroups

Definition 7.01 - *Generating Cyclic Groups*
Let G be a group and $x \in G$.
We define a *cyclic group* generated by x

$$\langle x \rangle = \{x^i : i \in \mathbb{Z}\} \leq G$$

.
Theorem 7.02 - *Cyclic Subgroup*
Let $x \in G$ then $\langle x \rangle$ is a subgroup of G.

Definition 7.03 - *Cyclic Group*
A group G is cyclic if $G = \langle x \rangle$ for some $x \in G$.
N.B. - Here x is called the *generator* of G.

Theorem 7.04 - *Abelian Cyclic Groups*
Every cyclic group is abelian.

Theorem 7.05 - *Finding Cyclic Groups*
Let G be a group with $|G| = n < \infty$.
G is cyclic iff $\exists\ x \in G$ such that $ord(x) = n$.

Theorem 7.06 - *Subgroups of Cyclic Groups*
Every subgroup of a cyclic group is also a cyclic group.

8 Groups from Modular Arithmetic

Definition 8.01 - *Congurence Class*
Let $n \in \mathbb{N}$ then $a \equiv b(mod\ n)$ means $n|a - b$.
There are n *congurence classes* $[0], [1], \dots, [n-1]$ where every integer is in exactly one of these classes.

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

Definition 8.02 - *Congurence groups*
Let $n \in \mathbb{N}$ then we denoted a congurence group of n by

$$\frac{\mathbb{Z}}{n\mathbb{Z}} = [0], [1], \dots, [n-2], [n-1]$$

N.B - Addition and multiplication are valid binary operations for congurence groups.

Definition 8.03 - *Properties of Congurence Groups*
Let $[a], [b] \in \frac{\mathbb{Z}}{n\mathbb{Z}}$ for some $n \in \mathbb{N}$ then

$$[a] + [b] = [a+b], \quad [a].[b] = [a.b]$$

Theorem 8.04 - *Abelian Congurence Groups*
Let $n \in \mathbb{N}$ then $\frac{\mathbb{Z}}{n\mathbb{Z}}$ is an abelian group.

Theorem 8.05 - *Cyclic Abelian Congurence Groups*
The group $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, +\right) = \langle [1] \rangle$, so it is a cyclic group.
The group $\left(\frac{\mathbb{Z}}{n\mathbb{Z}}, \cdot\right)$ is never a group for $n > 1$ as $[0][x] = [0] \neq [1] = e$.

Theorem 8.06 - *Multiplicative Inverse of Congurence Groups*
$[a] \in \frac{\mathbb{Z}}{n\mathbb{Z}}$ has a multiplicative inverse if, and only if, $gcd(a, n) = 1$.

Definition 8.07 - *Subset of $\frac{\mathbb{Z}}{n\mathbb{Z}}$ with multiplicative inverses*
U_n is the subset of $\frac{\mathbb{Z}}{n\mathbb{Z}}$ such that

$$U_n = \left\{[a] \in \frac{\mathbb{Z}}{n\mathbb{Z}}; gcd(a, n) = 1\right\}$$

N.B. - $(U_n, \cdot)$ is an abelian group.

9 Isomorphic Groups

Definition 9.01 - *Isomorphism*
Let $(G, *)$ and $(H, \cdot)$ be groups.
An *isomorphism* from G to H is a bijective function $\phi : G \to H$ such that

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

N.B. - Since ϕ is bijective then there exists an inverse such that $\phi^{-1} : H \to G$.

Definition 9.02 - *Isomorphic*
Let G and H be groups.
G and H are said to be *isomorphic* if there exists an isomorphism $\phi : G \to H$. This is denoted by $G \cong H$.

Proposition 9.03 - *Transitive property of Isomorphisms*
Let G, H and I be groups.
If $G \cong H$ and $H \cong I$, then $G \cong I$.
If $G \cong H$ and H is *abelian*, then G is albelian.
If $G \cong H$ and H is *cyclic*, then H is cyclic.

Proposition 9.04 - *Indentity element and Isomorphisms*
Let $\phi : G \to H$ be an isomorphism, e_G & e_H be the identity elements of these groups and $x \in G$. Then

i) $\phi(e_G) = e_H$;

ii) $\phi(x^{-1}) = \phi(x)^{-1}$;

iii) $\phi(x^i) = \phi(x)^i, \quad \forall\ i \in \mathbb{Z}$; and,

iv) $ord_G(x) = ord_H(\phi(x))$.

Proposition 9.05 - *Order of Isomorphic Groups*
Let G & H be isomorphic then $|G| = |H|$.

Proposition 9.06 - *Order of Elements of Isomorphic Groups*
Let G & H be isomorphic and $n \in \mathbb{N}$.
Then G and H have the same number of elements of order n.

10 Direct Product

Definition 10.01 - *Direct Product*
Let G & H be groups with the same binary operator.
The *direct product*, $G \times H$, is the cartesian product of the sets of G and H with the binary operator

$$(x, y)(x', y') = (xx', yy'), \quad x, x' \in G \; y, y' \in H$$

Proposition 10.02 - *Direct Product as a group*
The direct product of two groups is itself a group.

Proposition 10.03 - *Properties of Direct Product*
Let G and H be groups with the same binary operator.

i) $G \times H$ is *infinite* iff both G and H are infinite;

ii) $G \times H$ is *abelian* iff both G and H are abelian; and,

iii) If $G \times H$ is *cyclic*, then G and H are cyclic.

Proposition 10.04 - *Order of Elements of Direct Product*
Let $g \in G, h \in H$ with $ord_G(g) = m \in \mathbb{N}$ and $ord_H(h) = n \in \mathbb{N}$ then for $(g, h) \in G \times H$

$$ord_{G \times H}(g, h) = lcm(m, n)$$

Theorem 10.05 - *Cycle Direct Products*
Let G & H be finite cyclic groups.
Then $G \times H$ is a cyclic group iff $gcd(|G|, |H|) = 1$.

Definition 10.06 - *Klein 4-Group*
A *Klein 4-Group* is a group of order 4 such that every element, except the identity, has order 2.

Proposition 10.07 -
Let $m, n \in \mathbb{N}$ such that $gcd(m, n) = 1$. Then

$$U_{mn} \cong U_m \times U_n$$

11 Lagrange's Theorem

Theorem 11.01 - *Lagrange's Theorem*
Let G be a finite group, and $H \leq G$, then $|H|$ divides $|G|$.

Definition 11.02 - *Co-Sets*
Let G be a group, $H \leq G$ and $x \in G$.
The *left co-set* is defined as $xH = \{xh \in G : h \in H\} \subseteq G$.
The *right co-set* is defined as $Hx = \{hx \in G : h \in H\} \subseteq G$.

Theorem 11.03 - *Order of Co-set*
There exists a bijection, $\phi : H \to xH$, where $\phi(h) = xh$ so

$$|H| = |xH|$$

Theorem 11.04 - *Relationship between Co-sets*
Let $x, y \in G$ and $H \leq G$ then either

$$xH = yH \text{ or } xH \cap yh = \emptyset$$

Theorem 11.05 - *Cosets of Abelian Groups*
Let G be an abelian group and $H \leq G$ then $xH = Hx$.

Definition 11.06 - *Index*
Let $H \leq G$.
Then *index*, $|G : H|$, is the number of left co-sets, xH, in G.

12 Some Consequences and Applications of Lagrange's Theorem

Propostion 12.01 - *Lagrange for Order of Elements*
Let G be a finite group with $|G| = n$.
Then $\forall\ x \in G,\ ord(x)|n$ meaning $x^n = e$.

Theorem 12.02 - *Fermat's Little Theorem*
Let $p \in \mathbb{N}$ and $a \in \mathbb{Z}$ such that $p \not| a$. Then

$$a^{p-1} \equiv 1(mod\ p)$$

Definition 12.03 - *Euler's Phi Function*
Euler's phi function is the function, $\phi : \mathbb{N} \to \mathbb{N}$, where

$$\phi(m) = |\{a \in \mathbb{Z} : 0 \leq a \leq m; gcd(a, m) = 1\}|$$

Theorem 12.04 - *Fermat-Euler Theorem*
Let $m > 0$ and $a \in \mathbb{Z}$ with $gcd(a, m) = 1$. Then

$$a^{\phi(m)} \equiv 1(mod\ m)$$

Theorem 12.05 - *Properties of Prime-Ordered Groups*
Let $p \in \mathbb{N}$ be prime and G be a group such that $|G| = p$. Then

i) G is cyclic;

ii) $\forall\ x \in G\backslash\{e\}, ord(x) = p$ and $G = \langle x \rangle$; and,

iii) G only has two subgroups, both trivial, $\{e\}$ and G itself.

Proposition 12.06 - *Relationship between Prime-Ordered Subgroups*
Let $p \in \mathbb{N}$ be prime and $H, I \leq G$ such that $|H| = p = |I|$, then either

$$P = Q \text{ or } P \cap Q = \{e\}$$

Proposition 12.07 - *Relationship between Relatively-Prime-Ordered Subgroups*
Let $m, n \in \mathbb{N}$, with $gcd(m, n) = 1$ and $H, I \leq G$ such that $|H| = m, |I| = n$, then

$$H \cap I = \{e\}$$

Theorem 12.08 - *Odd Primed-Ordered Groups*
Let $p \in \mathbb{N}$ be an odd-prime. Then

i) Every group of order $2p$ is either *cyclic* or *isomorphic* to D_{2p}; and,

ii) Every group of order p^2 is either *cyclic* or *isomorphic* to $(\frac{\mathbb{Z}}{p\mathbb{Z}}) \times (\frac{\mathbb{Z}}{p\mathbb{Z}})$.

13 Symmetric Groups

Definition 13.01 - *Symmetric Group*
Let X be a set.
The *symmetric group* on X is the group, $S(X)$, of all permutations of X under composition.
N.B. - S_n is the group of all permutations of $\{1, \dots, n\}$.

Proposition 13.02 - *Order of Symmetric Group*

$$|S_n| = n!$$

Definition 13.03 - *k-cycle*
A *k-cycle* in S_n, where $k \leq n$, is a permutation where

$$\sigma(x_i) = x_{i+1}, \quad \sigma(x_k) = x_1$$

N.B. - denoted by $\sigma = (x_1\ x_2\ \dots\ x_k)$.

Theorem 13.04 - *Order of a k-cycle*
Let σ be a k-cycle then $ord_{S_n}(\sigma) = k$.

Definition 13.05 - *Transposition*
A *transposition* is a permutation that swaps two-elements and leaves all other elements unchanged.
N.B. - $\sigma(x_m) = x_n,\ \sigma(x_n) = x_m$ is denoted by $\sigma = (x_m, x_n)$. This can be extended for any number of elements.

Definition 13.06 - *Disjoint Cycles*
Disjoint cycles are cycles of S_n that have no elements share a common position.

Theorem 13.07 - *Order of Products of Disjoint Cycles*
Let f be the product of disjoint cycles of length $k_1, k_2, \dots, k_n$ then

$$ord(f) = lcm(k_1, k_2, \dots, k_n)$$

14 Transpositions and Alternating Groups

Definition 14.01 - *Transposition*
A *transposition* is a 2-cycle.
i.e. - A permutation where only two elements are swapped.

Theorem 14.02 - *Permutations as Transpositions*
Any permutation, $\sigma \in S_n$, is the product of a series of transpositions.
N.B. - The identity transposition, id_{S_n}, is the product of zero transpositions.

Proposition 14.03 - *K-Cycles as Transpositions*
Let $k > 1$.
Then a k-cycle is a product of $k - 1$ transpositions.
N.B. - $(1, 2, \dots, k) = (1, 2)(2, 3) \dots (k - 1, k)$.

Definition 14.04 - *Even & Odd Permutations*
Let $\sigma \in S_n$.
We say σ is *even* if it is the product of an even number of transpositions.

We say σ is *odd* if it is the product of an odd number of transpositions.
N.B. - The identity is even.

Theorem 14.05 - *Exclusivity of Even & Odd Permutations*
Every $\sigma \in S_n$ is either even or odd, never both.

Proposition 14.06 - *Composition of Even & Odd Permutations*
Let $\sigma, \tau \in S_n$.
If σ & τ are both *even* then, $\sigma\tau$ is *even*.
If σ is *even* & τ is *odd* then, $\sigma\tau$ is *odd*.
If σ is *odd* & τ is *even* then, $\sigma\tau$ is *odd*.
If σ & τ are both *odd* then, $\sigma\tau$ is *even*.

Proposition 14.07 - *Even & Oddness of K-Cycles*
Let $\sigma \in S_n$.
If $\sigma = \tau_1\tau_2 \dots \tau_k$, where τ_i is a k_i-cycle.
Then σ is *even* if the number of odd τ_i is even.
σ is *odd* if the number of odd τ_i is odd.

Proposition 14.08 - *Even Permutations*
The set of even permutations in S_n is a subgroup of S_n.

Definition 14.09 - *Alternating Group*
The subgroup of even permutations in S_n is called the *Alternating Group*, A_n.

Theorem 14.10 - *Order of an Alternating Group*
Let $n > 1$.
Then $|A_n| = \frac{n!}{2} = \frac{1}{2}|S_n|$.