Group Theory Notes

by Tyler Wright

github.com/Fluxanoia fluxanoia.co.uk

These notes are not necessarily correct, consistent, representative of the course as it stands today or, rigorous. Any result of the above is not the author's fault.

0 Notation

We commonly deal with the following concepts in Group Theory which I will abbreviate as follows for brevity:

Term	Notation
$\{1,2,\ldots\}$	N
$\{0, 1, 2, \ldots\}$	\mathbb{N}_0
The set of primes	ho
$(F \setminus \{0_F\}, \times)$	F^*
(invertible $n \times n$ matrices on F, \times)	$GL_n(F)$

Contents

0	Notation			1		
1	The	Funda	amentals	3		
	1.1	Binary	Operations	3		
	1.2	Group	S	3		
		1.2.1	Distinct Powers of Group Elements	3		
		1.2.2	Symmetric Groups	3		
		1.2.3	Cyclic Groups	3		
		1.2.4	Dihedral Groups	4		
		1.2.5	The Infinite Cyclic/Dihedral Group	4		
		1.2.6	Torsion Groups	4		
	1.3	<i>p</i> -grou	ps	4		
	1.4	Subset	s of Groups	5		
		1.4.1	Set Multiplication	5		
		1.4.2	Centre	5		
		1.4.3	Properties of Sets	5		
	1.5	${\rm Order}$		5		
	1.6	Isomorphisms				
	1.7	.7 Subgroups				
		1.7.1	The Product of Subgroups	7		
		1.7.2	The Subgroup Test	7		
		1.7.3	The Intersection of Subgroups	7		
	1.8	Genera	ated Subgroups	8		
	1.9	Cyclic	Groups	8		
	1.10	Cosets		9		
			A Bijection from Left to Right Cosets	9		
		1.10.2	A Equivalence Relation on Cosets	9		
		1.10.3	Index	9		
		1.10.4	Lagrange's Theorem	9		
	1.11			10		
		1.11.1	Properties of the Outer Direct Product	10		

1 The Fundamentals

1.1 Binary Operations

A binary operation on a set X is a map $X \times X \to X$.

Take a binary operation * on a set X, we say that * is associative if for all x, y, z in X:

$$x * (y * z) = (x * y) * z.$$

Furthermore, we say e in X is an identity element of * if for all x in X:

$$e * x = x * e,$$

and we say that y in X is the inverse to x if x * y and y * x are both identities of *.

1.2 Groups

A group (G, *) is a non-empty set G combined with a binary operation * such that:

- * is associative,
- G contains an identity for *,
- for each element in G, there exists some inverse in G with respect to *.

1.2.1 Distinct Powers of Group Elements

For an element x in a group G, we have that the powers of x are distinct up to the order of x.

1.2.2 Symmetric Groups

For a set X, the set of bijections $X \to X$ is a group under function composition denoted by $\operatorname{Sym}(X)$. We typically write $\operatorname{Sym}(\{1, 2, \dots, n\})$ as S_n .

1.2.3 Cyclic Groups

If we consider a regular n-gon P_n , we take rotations of $\frac{2\pi}{n}$ radians about the centre to be r and can define:

$$C_n = \{e, r, r^2, \dots, r^{n-1}\},\$$

to be the group of rotational symmetries of P_n , the cyclic group on P_n .

1.2.4 Dihedral Groups

If we consider again, a regular n-gon P_n and take:

r = a rotation of $\frac{2\pi}{n}$ radians about the centre, s = reflection in some fixed line of symmetry,

then we have that:

$$Sym(P_n) = \{e, r, r^2, \dots, r^{n-1}, s, rs, r^2s, \dots, r^{n-1}s\},\$$

called the dihedral group, denoted by D_{2n} .

1.2.5 The Infinite Cyclic/Dihedral Group

A map φ from $\mathbb{Z} \to \mathbb{Z}$ is a symmetry if for some n and m in \mathbb{Z} :

$$|\varphi(m) - \varphi(n)| = |m - n|.$$

Taking r to be the symmetry $n \mapsto n+1$, we can define the infinite cyclic group:

$$C_{\infty} = \{\dots, r^{-2}, r^{-1}, e, r, r^2, \dots\}.$$

Taking s to be the symmetry $n \mapsto -n$, we can define the infinite dihedral group:

$$D_{\infty} = \{\dots, r^{-2}, r^{-1}, e, r, r^2, \dots, r^{-2}s, r^{-1}s, s, rs, r^2s\}.$$

1.2.6 Torsion Groups

A group is a torsion group if every element has finite order and torsion-free if every non-identity element has infinite order.

1.3 p-groups

For p in \mathbb{P} , we say that a group G is a p-group if the order of each element of G is a power of p.

1.4 Subsets of Groups

1.4.1 Set Multiplication

For X, Y subsets of a group (G, *), we define:

$$X * Y = \{x * y : x \in X, y \in Y\},\$$

the product set of X and Y (which is a subset of G). We have that * is an associative binary operation on $\mathcal{P}(G)$. Additionally, we define:

$$X^{-1} = \{x^{-1} : x \in X\}.$$

However, these definitions do not define a group on $\mathcal{P}(G)$ as an inverse does not necessarily exist for each element, despite the existence of an identity $\{e_G\}$.

1.4.2 Centre

For a group G, the centre of G is the set of elements that commute with all elements of G, denoted by Z(G):

$$Z(G) = \{ z \in G : gz = zg, \forall g \in G \}.$$

We have that Z(G) is a subgroup.

1.4.3 Properties of Sets

For a group (G, *) with $X \subseteq G$, we have some defined properties:

- X is symmetric if for each x in X, x^{-1} is also in X,
- X is closed under * if for all x, y in X, x * y is in X.

1.5 Order

For a group G = (X, *), G has order |X|. The order of an element x of X is defined as follows:

$$|x| = \infty$$
 if $x^n \neq e_G$ for any n in \mathbb{N} , $|x| = \min\{n \in \mathbb{N} \mid x^n = e_G\}$ otherwise.

Taking x in X, if x has finite order, then:

- 1. $x^n = e_G$ if and only if |x| divides n,
- 2. $x^n = x^m$ if and only if |x| divides m n,

and if x has infinite order:

3. $x^n = x^m$ if and only if n = m.

Proof. For (1), we take n = q|x| + r for some q in \mathbb{Z} , r in $\{0, 1, \ldots, |x| - 1\}$. Thus:

$$x^{n} = x^{q|x|}x^{r},$$

$$= e_{G}^{q}x^{r},$$

$$= x^{r},$$

and we can see that $x^r = e_G$ if and only if r = 0 as r < |x| and |x| is minimal. Thus, $x^n = e_G$ if and only if r = 0 which occurs if and only if |x| divides n.

For (2) and (3), we take x to have any order and consider:

$$x^n = x^m,$$
$$x^{m-n} = e_G.$$

Thus, if $|x| < \infty$ then |x| divides m - n by (1) and if $|x| = \infty$ then m - n = 0 by the definition of order.

1.6 Isomorphisms

For (G, *), (H, \circ) groups, an isomorphism $\varphi : G \to H$ is a bijection such that $\varphi(x * y) = \varphi(x) \circ \varphi(y)$ for all x, y in G. If such a map exists, we say G is isomorphic to H, denoted by $G \cong H$.

For G, H, and K groups, $\varphi: G \to H$ and $\psi: H \to K$ isomorphisms, we have that:

- φ^{-1} is an isomorphism,
- $(\psi \circ \varphi)$ is an isomorphism,

which means \cong is an equivalence relation on any set of groups.

1.7 Subgroups

A subset X of a group (G, *) is a subgroup if and only if (X, *) (with * restricted to X, for which X must be closed under *) is a group, denoted by $X \leq G$ (or if $X \neq G, X < G$).

Alternatively, we have that X is a subgroup if and only if:

- e_G is in X,
- X is closed under *,
- X is symmetric under *.

1.7.1 The Product of Subgroups

For $H, K \leq G, HK$ is a subgroup of G if and only if HK = KH.

Proof. By the alternate definition of a subgroup above, we know that for a subgroup X of G, X contains e_G , and X is closed and symmetric under *.

Suppose $HK \leq G$, thus:

$$HK = (HK)^{-1}$$
$$= K^{-1}H^{-1}$$
$$= KH$$

Now, suppose HK = KH:

- $e_G = e_G e_G$ is in HK,
- (HK)(HK) = H(KH)K = H(HK)K = (HH)(KK) = HK,
- $(HK)^{-1} = K^{-1}H^{-1} = KH = HK$,

so HK is a subgroup.

1.7.2 The Subgroup Test

For X a subset of a group G, X is a subgroup if and only if $X \neq \emptyset$ and $x^{-1}y$ is in X for each x, y in X.

Proof. Suppose $X \leq G$, then e_G is in X so $X \neq \emptyset$. For x, y in X, x^{-1} is also in X by the inverse rule of subgroups, so $x^{-1}y$ is also in X by the closure of subgroups.

Suppose $X \neq \emptyset$ and for each x, y in $X, x^{-1}y$ is also in X. Taking x, y in X, we have that $x^{-1}x = e_G$ is also in X. Also, $x^{-1}e_G = x^{-1}$ is in X. Finally, $xy = (x^{-1})^{-1}y$. \square

1.7.3 The Intersection of Subgroups

We have that for a group G with A a set of subgroups of G:

$$\bigcap_{a \in \mathcal{A}} a,$$

is a subgroup of G.

Proof. We will use the subgroup test. We set X to be the intersection of the subgroups in A, X must be non-empty as each subgroup must contain e_G . Taking x, y in X, for each a in A, we know that x and y are in a. As a is a subgroup, x^{-1} and thus $x^{-1}y$ are in a. As a is arbitrary, $x^{-1}y$ must be in X.

1.8 Generated Subgroups

For a group G with $X \subseteq G$ non-empty, we define the subgroup generated by X as:

$$\langle X \rangle = \bigcap_{A \le G: X \subseteq A} A,$$

the intersection of all the subgroups containing X. This can also be called the smallest subgroup containing X.

Alternatively, we have that:

$$\langle X \rangle = \Gamma(X) = \{x_1 x_2 \cdots x_n : x_i \in X \cup X^{-1}, m \in \mathbb{N}\}.$$

Proof. We can see that $\Gamma(X) \subseteq \langle X \rangle$ as $\langle X \rangle$ contains X and is a subgroup so it contains all the finite products of elements of $X \cup X^{-1}$ by closure and existence of inverses.

If we can show that $\Gamma(X)$ is a subgroup, then that would mean $\langle X \rangle \subseteq \Gamma(X)$ as $\Gamma(X)$ contains X so would have been included in the intersection used to generate $\langle X \rangle$. We know that $\Gamma(X)$ is non-empty as X is non-empty and taking x, y in $\Gamma(X)$, for some n, m in \mathbb{N} , we have that:

$$x = x_1 x_2 \cdots x_n,$$

$$y = y_1 y_2 \cdots y_m,$$

by the definition of $\Gamma(X)$. For each x_i with i in [n], we know that x_i^{-1} is in $\Gamma(X)$ as $X^{-1} \subset \Gamma(X)$ so:

$$x^{-1}y = (x_1x_2 \cdots x_n)^{-1}y$$

= $x_n^{-1}x_{n-1}^{-1} \cdots x_1^{-1}y_1y_2 \cdots y_m$,

is in $\Gamma(X)$ by its definition. Thus, $\Gamma(X)$ is a subgroup as required.

1.9 Cyclic Groups

A group G is cyclic if it is generated by a single element. Elements in G that generate G are called generators. Supposing G is cyclic:

- For x a generator of G, $G = \{x^n : n \in \mathbb{Z}\},$
- \bullet G is abelian,
- $G \cong C_{|G|}$,
- For X < G, X is cyclic.

1.10 Cosets

For a group G with $H \leq G$ and x in G, the subset xH is a left coset of H in G and similarly, Hx is a right coset. We have some properties of left cosets:

- For h in H, hH = H = Hh,
- For g in $G \setminus H$ we cannot say gH = Hg in general,
- G is the union of all the left cosets,
- For x, y in G, xH = yH if and only if x is in yH,
- For x, y in G, either xH = yH or $xH \cap yH = \emptyset$,
- For all x in G, |xH| = |H|.

1.10.1 A Bijection from Left to Right Cosets

For a group G with $H \leq G$, the map $xH \mapsto Hx^{-1}$ is a bijection from the set of left cosets to the set of right cosets.

1.10.2 A Equivalence Relation on Cosets

We can define an equivalence relation \sim on a group G with $H \leq G$ by setting:

$$x \sim y \iff y \in xH$$
,

where xH is the equivalence class containing x.

1.10.3 Index

For a group G with $H \leq G$, the number of distinct left cosets of H in G is called the index of H in G, denoted by [G:H] (the choice of left cosets here is arbitrary due to the bijection between the coset types).

1.10.4 Lagrange's Theorem

For a finite group G with $H \leq G$, |G| = [G:H]|H|.

This means, for any subgroup $H \leq G$, its index and order divide the order of G. Thus, for G a finite group:

- For x in G, |x| divides |G|,
- If G has prime order, G is cyclic and every non-identity element is a generator,
- For p in \mathbb{P} with $P, Q \leq G$ and |P| = |Q| = p, $P \cap Q = \emptyset$ or P = Q.

1.11 Outer Direct Product

For G_1, \ldots, G_n groups, we set:

$$G_1 \times \cdots \times G_n = \{(a_1, \dots, a_n) : a_i \in G_i, i \in [n]\},$$

and define a binary operation on $G = G_1 \times \cdots \times G_n$ by:

$$(a_1,\ldots,a_n)(b_1,\ldots,b_n)=(a_1b_1,\ldots,a_nb_n).$$

G is a group under this operation.

1.11.1 Properties of the Outer Direct Product

For G_1, \ldots, G_n groups, with $G = \prod_{i \in [n]} G_i$:

- $|G| = \prod_{i \in [n]} |G_i|$,
- $Z(G) = \prod_{i \in [n]} Z(G_i),$
- If G is cyclic, G_i is cyclic for each i in [n],
- For all σ in S_n , $G \cong \prod_{i \in [n]} G_{\sigma(i)}$,
- For the integers $1 \le n_1 < n_1 < \dots < n_r < n$,

$$G \cong (G_1 \times \cdots \times G_{n_1}) \times (G_{n_1+1} \times \cdots \times G_{n_2}) \times \cdots \times (G_{n_r+1} \times \cdots \times G_n),$$

• For H_1, \ldots, H_n groups with $G_i \cong H_i$ for each i in [n] $G \cong \prod_{i \in [n]} H_i$.