# Notes on the Theory of Groups

by

Marcel K. Goh

## 1. PRELIMINARY NOTIONS FROM LINEAR ALGEBRA

This set of notes assumes that the reader has had some exposure to linear algebra; the most crucial notions will be outlined in this section.

### 1.1. Basic Properties of Square Matrices

We shall mainly concern ourselves with matrices of the form

$$\begin{pmatrix} a_{11} & \cdots & a_{1n} \\ \vdots & \ddots & \vdots \\ a_{n1} & \cdots & a_{nn} \end{pmatrix}$$

where $n$ is some positive integer and each entry $a_{ij} \in \mathbf{R}$. We call the set of all $n \times n$ matrices with real entries $M_n(\mathbf{R})$.

For two matrices $A$ and $B$, we may form their *sum* $A + B = (a_{ij} + b_{ij})$. (This notation means that at the $i$th row and $j$th column, the entry is the sum of $a_{ij}$ and $b_{ij}$.) Given a real number $\alpha$, we obtain the scalar product $\alpha A = (\alpha \cdot a_{ij})$ by multiplying every entry in $A$ by $\alpha$.

We can also *multiply* $n \times n$ matrices $A$ and $B$ with the following formula:

$$A \cdot B = (c_{ij}) \quad \text{where } c_{ij} = \sum_{k=1}^{n} a_{ik} \cdot b_{kj}. \tag{1}$$

Since a matrix represents a linear transformation, multiplying matrices is like composing functions. If $S$ and $T$ are the transformations represented by the matrices $B$ and $A$, respectively, then the matrix product $A \cdot B$ can be thought of as the following composition of transformations:

$$\mathbf{R}^n \quad \xrightarrow{S} \quad \mathbf{R}^n \quad \xrightarrow{T} \quad \mathbf{R}^n$$

For matrices $A$ and $B$ the commutativity of addition

$$A + B = B + A \tag{2}$$

is valid, and for three matrices $A$, $B$, and $C$, the distributive law

$$A \cdot (B + C) = A \cdot B + A \cdot C \tag{3}$$

and the associativity of multiplication

$$A \cdot (B \cdot C) = (A \cdot B) \cdot C \tag{4}$$

may be proven to hold as well. In particular, (4) is laborious to prove from the definition given in (1), but easy to derive when reasoning about matrices as transformations.

Unlike addition, multiplication is not commutative: $A \cdot B$ does not equal $B \cdot A$ in general. To prove this, we simply note that

$$\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \cdot \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} \text{ but } \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}.$$

The matrix

$$I = \begin{pmatrix} 1 & 0 & \cdots & 0 \\ 0 & 1 & \cdots & 0 \\ \vdots & \vdots & \ddots & \vdots \\ 0 & 0 & \cdots & 1 \end{pmatrix}$$

is called the *identity matrix* and has the property that $AI = IA = A$ for any matrix $A$. [When no ambiguity can arise, we often omit the $\cdot$ symbol when denoting a product.]

We say that a matrix $A$ is *invertible* if and only if there exists a matrix $B$ such that $AB = BA = I$; otherwise, it is called *singular*. Not all matrices are invertible. For example, the matrix $\mathbf{0}$, all of whose entries are 0, is not invertible in any dimension. The identity matrix is easily seen to be invertible (take $B = I$). Note that if an inverse matrix exists for a given matrix $A$, then it is unique, for if $AB = AB' = I$ and $B'A = BA = I$, then, multiplying the first identity by $B$ on the left, we arrive at $BAB = BAB'$, i.e. $B = B'$.

Since a $1 \times 1$ matrix $(a)$ contains only one real number, it is invertible if and only if $a \neq 0$. A $2 \times 2$ matrix $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right)$ is invertible if and only if $ad - bc = 0$, since for any such matrix,

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} d & -c \\ -c & a \end{pmatrix} = \begin{pmatrix} ad - bc & 0 \\ 0 & ad - bc \end{pmatrix},$$

and we can multiply both sides by $1/(ad - bc)$ to obtain the identity on the right, provided that $ad - bc$ is nonzero.

In general, there exists a function $\det : M_n(\mathbf{R}) \to \mathbf{R}$ such that a matrix $A \in M_n(\mathbf{R})$ is invertible if and only if $\det A \neq 0$. This determinant can be calculated as a sum over $n!$ terms; this formula will not be useful for our purposes.

### 1.2. The General Linear Group

Let us now restrict our attention to a certain subset of square matrices, namely those whose determinant is nonzero. This set is called the *general linear group of degree n* and is denoted $GL_n(\mathbf{R})$ when all matrix entries are real numbers. Remark that, since $(-1) + (1) = (0)$, this set is not closed under addition; scalar multiplication is also no longer a safe operation, since multiplying any matrix by 0 results in a singular matrix.

In return for these two forfeited closure properties, we get closure under matrix multiplication.

**Proposition I.** *Suppose that two matrices $A$ and $B$ are invertible. Then their product $AB$ is also invertible.*

*Proof.* Consider $B^{-1}A^{-1}$ and the product $(B^{-1}A^{-1})(AB)$. By associativity of multiplication, this becomes $B^{-1}(A^{-1}A)B = B^{-1}IB = IB^{-1}B = II = I$. Alternatively, use the fact that $\det(AB) = \det(A)\det(B)$, which is nonzero because both $\det(A)$ and $\det(B)$ are nonzero. ∎

Thus the set $GL_n(\mathbf{R})$, under the operation of matrix multiplication, has a multiplicative inverse $A^{-1}$ for every matrix $A$. It also contains an identity element $I$ and the multiplication operation is associative. These are the properties of a group.

## 2. GROUPS

### 2.1. Properties and Basic Examples

A *group* $G$ is a set on which is defined a rule of combination such that the product of two elements $g, h \in G$, denoted $g \cdot h$ or $gh$, is also in $G$. Furthermore, the following three properties must hold:

a) Multiplication must be associative: for all $g, h, k \in G$, $(gh)k = g(hk)$.

b) There exists an identity element $e \in G$ such that $ge = eg = g$ for all $g \in G$. This element is also often denoted 1.

c) For every element $g \in G$, there exists an inverse element $g^{-1}$ such that $gg^{-1} = g^{-1}g = e$.

An immediate consequence of the axioms is that the identity $e$ is unique. For if both $e$ and $e'$ are the identity of a group, then $e = ee' = e'$.

The term *order* serves a somewhat dual purpose in group theory. The order of a group $G$ is the number of elements it contains and and this value, also denoted $|G|$, need not be finite. On the other hand, we define the order of a group *element* $g$ to be the smallest $k > 0$ such that $g^k = e$. If no such $k$ exists, then $g$ is said to have infinite order.

Probably the most familiar group is the set of all integers, denoted $\mathbf{Z}$, under the operation of addition. It has 1 as its identity, inverses $-a$ for every whole number $a$, and the commutative property; likewise, any vector space $V$ is also a group under vector addition. The set of nonzero real numbers forms a group under multiplication. In these examples, the binary operation has the property that for any $g, h \in G$, the products $gh$ and $hg$ are equal. A group where this holds is called an *abelian* or *commutative* group. An example of a non-abelian group is the group $Q_8$ of quaternions with identity 1, governed by the identities $(-1)^2 = 1$ and $i^2 = j^2 = k^2 = ijk = -1$. It has the following multiplication table:

| | $1$ | $-1$ | $i$ | $-i$ | $j$ | $-j$ | $k$ | $-k$ |
|---|---|---|---|---|---|---|---|---|
| $1$ | $1$ | $-1$ | $i$ | $-i$ | $j$ | $-j$ | $k$ | $-k$ |
| $-1$ | $-1$ | $1$ | $-i$ | $i$ | $-j$ | $j$ | $-k$ | $k$ |
| $i$ | $i$ | $-i$ | $-1$ | $1$ | $k$ | $-k$ | $-j$ | $j$ |
| $-i$ | $-i$ | $i$ | $1$ | $-1$ | $-k$ | $k$ | $j$ | $-j$ |
| $j$ | $j$ | $-j$ | $-k$ | $k$ | $-1$ | $1$ | $i$ | $-i$ |
| $-j$ | $-j$ | $j$ | $k$ | $-k$ | $1$ | $-1$ | $-i$ | $i$ |
| $k$ | $k$ | $-k$ | $j$ | $-j$ | $-i$ | $i$ | $-1$ | $1$ |
| $-k$ | $-k$ | $k$ | $-j$ | $j$ | $i$ | $-i$ | $1$ | $-1$ |

The general linear group $GL_n(\mathbf{R})$ of invertible $n \times n$ matrices is another example of a non-abelian group, whenever $n > 1$.

Group theory is intimately connected to the study of symmetries of an object. Let $T$ be a set and let $\mathrm{Sym}(T)$ denote the set of all bijections from $T$ to itself. This is called the *symmetric group* on $T$ as, under composition of functions, it obeys all the group axioms: It contains the identity transformation $\mathrm{Id}_T$ and every bijection $f$ has an inverse bijection $f^{-1}$. In some sense, the symmetric group is the most general group, because all other groups arise from adding restrictions to these bijections. For instance, $GL_n(\mathbf{R}) \subset \mathrm{Sym}(\mathbf{R}^n)$.

### 2.2. Permutation Groups

A bijection $\sigma$ from a set $T$ to itself is also called a *permutation*. We will focus on the case where $T$ is finite and we may simply number the elements of $T = \{1, \ldots, n\}$. Then the set of permutations of $T$ is denoted $S_n$ and called the *symmetric group on $n$ letters* or, alternatively, the *permutation group on $n$ letters*. An element $\sigma$ of this group may be explicitly presented in such a way that we see where each element is taken to by $\sigma$:

$$\sigma = \begin{pmatrix} 1 & 2 & \cdots & n \\ \sigma(1) & \sigma(2) & \cdots & \sigma(n) \end{pmatrix}$$

It is easy to see that there are $n! = n(n-1)(n-2)\cdots 1$ different permutations of $n$ letters. There are $n$ choices for $\sigma(1)$; subsequently there remain $n-1$ choices for $\sigma(2)$, $n-2$ choices for $\sigma(3)$ and so on until our hand is forced for $\sigma(n)$. So $|S_n| = n!$. Let us now consider the concrete example of the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 7 & 6 & 4 & 5 & 2 & 3 \end{pmatrix},$$

which is an element of $S_7$. Notice that the elements 1, 4, and 5 are untouched by the permutation and the remaining four items are permuted in the cycle $2 \mapsto 7$, $7 \mapsto 3$, $3 \mapsto 6$, and $6 \mapsto 2$. This suggests a more concise notation for $\sigma$, since this cycle $(2\,7\,3\,6)$ completely determines the permutation. Notation-wise, $(2\,7\,3\,6)$ denotes exactly the same cycle as $(3\,6\,2\,7)$; to avoid confusion, we usually select the one that starts with the smallest number. Not every permutation is a cycle; for example the permutation

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

cannot be represented as a single cycle. However, it contains two cycles, $(1\,4)$ and $(2\,3)$, so we can simply represent $\tau$ as $(1\,4)(2\,3)$. When two cycles permute disjoint sets of elements, the cycles commute, so $(1\,4)(2\,3) = (2\,3)(1\,4)$. Every permutation can be represented as a product of disjoint cycles. In particular, the identity permutation can be represented as $(1)$, but we will often simply denote it $e$ or $()$.

### 2.3. Subgroups

Let $G$ be a group. We call a nonempty subset $H \subset G$ a *subgroup* and write $H \leq G$ provided that

a) The set $H$ is closed under the multiplication operation of $G$.

b) Whenever $H$ contains an element $a \in G$, $H$ contains its inverse $a^{-1}$ as well.

It is immediate from these requirements that a subgroup $H$ contains the identity element. Since $H$ is nonempty, it contains an element $h$ as well as its inverse $h^{-1}$. Then from closure of multiplication we conclude that $hh^{-1} = e \in H$.

We turn our attention to $S_3$. This group is not commutative, since the elements $\sigma = (1\,2\,3)$ and $\tau = (1\,2)$ do not commute. Multiplying $\sigma\tau$ we get $(1\,3)$ whereas the product $\tau\sigma = (2\,3)$.

Note that for $k \leq n$, $S_k \leq S_n$ because we can simply fix the letters $k+1, k+2, \ldots, n$. An easy corollary, then, is that $S_n$ does not commute for $n \geq 3$. This is because $S_3 \leq S_n$ and we can simply take $\sigma$ and $\tau$ as elements of the larger group $S_n$ that do not commute.

Another example of a subgroup is the set of $2 \times 2$ matrices that stabilise the line $y = 0$ (vectors lying on this line remain on this line after transformation). In terms of matrices, this set looks like

$$S = \left\{ \begin{pmatrix} a & c \\ 0 & d \end{pmatrix} : ad \neq 0 \right\}.$$

Showing that this set is closed is a simple matter of computing

$$\begin{pmatrix} a & c \\ 0 & d \end{pmatrix} \begin{pmatrix} a' & c' \\ 0 & d' \end{pmatrix} = \begin{pmatrix} aa' & ac' + cd' \\ 0 & dd' \end{pmatrix},$$

and observing that the determinant of this matrix is nonzero since all of $a, a', d, d'$ were assumed to be nonzero. (Closure under inversion is also easily derived.)

It is not always easy to characterise all subgroups of a given group. For the additive group of integers, however, the following proposition does so nicely.

**Proposition S.** *The subgroups of* $\mathbf{Z}$ *under addition are precisely given by* $b\mathbf{Z}$*, where* $b$ *is a fixed integer.*

*Proof.* First, we fix an integer $b$ and show that $b\mathbf{Z}$ is a subgroup. Adding two integers $bm + bn$ gives a third integer $b(m + n)$, which is also in $b\mathbf{Z}$, so the set is closed under the operation of addition; likewise $-(bm) = b(-m)$, so the set is closed under additive inverse.

Now we must show that these $b\mathbf{Z}$ are all the possible subgroups. Let $H \leq \mathbf{Z}$. It is possible that $H$ contains only the identity 0, in which case $H = 0\mathbf{Z}$. If not, let $b$ be the smallest positive integer contained in $H$. We know from closure that every multiple of $b$ is in $H$, so $b\mathbf{Z} \subset H$. Now let $h$ be any element in $H$. By the Euclidean division algorithm, we can divide $h$ by $b$ to get $h = mb + r$, where $mb$ is some multiple of $b$ and $r$ is a remainder lying in the range $0 \leq r < b$. Since $r = (-mb) + h$, we have $r \in H$. But then necessarily we have $r = 0$, since $b$ is the smallest positive integer in $H$. So $h$ is an integer multiple of $b$ and we have shown that $H \subset b\mathbf{Z}$. ∎

Finally, we introduce a specific class of subgroup. If $G$ is a group with an element $g$, the *cyclic subgroup* generated by $g$ is the set

$$\langle g \rangle = \{g^m : m \in \mathbf{Z}\}.$$

This is a subgroup because $g^m g^n = g^{m+n}$ and $(g^m)^{-1} = g^{-m}$. Note that not all powers are distinct! For example, in the group $S_3$, the cyclic subgroup generated by $\tau$ contains only the identity element and $\tau$ itself. If $g^m = e$ and $m$ is the smallest positive integer for which this holds, we say that the *order* of $g$ is $m$ and write $|g| = m$. If no such $m$ exists, then we say $g$ has infinite order.

If $G$ is a group containing an element $g$ such that $\langle g \rangle = G$, then $G$ is called a *cyclic group*.

### 2.4. Cosets and Normal Subgroups

Let $H$ be a subgroup of a group $G$. For any $g \in G$, we can form a *left coset* of $H$ by multiplying every element of $H$ by $g$ on the left:

$$gH = \{gh : h \in H\}$$

Symmetrically, we could form a *right coset* $Hg$ of $H$. Now we prove that the cosets partition the group $G$.

**Lemma P.** *Let $H$ be a subgroup of a group $G$. Then every element of $G$ is in exactly one left coset of $H$.*

*Proof.* Let $g \in G$ be given. We commence by noting that since $H$ contains the identity element $e$, the element $g$ is in at least one coset, namely $gH$. Now we show that any two cosets are either disjoint or equal. Suppose $aH$ and $bH$ are two cosets that are not disjoint. This implies that there exist $h_1, h_2 \in H$ such that $ah_1 = bh_2$. We can manipulate this identity to obtain $a^{-1}b = h_1 h_2^{-1}$. So $a^{-1}b \in H$. Then from closure properties of subgroups, the cosets must be equal, since

$$aH = a(a^{-1}bH) = (aa^{-1})bH = bH.$$

Thus $g$ is in exactly one coset of $H$. ∎

Any two cosets have the same size, namely the size of $H$, since the for any coset $aH$, the function $f : H \to aH$ given by $a \mapsto aH$ establishes a bijection. This gives us some information about $H$, since it induces a partition of $G$ into equally-sized disjoint cosets. In fact, we have just proved the following famous theorem:

**Theorem L** (*Lagrange*). *Let $H$ be a subgroup of a group $G$. Then the order of $H$ must divide the order of $G$.* ∎

Thus the value $|G|/|H|$ is an integer; it is called the *index* of $H$ in $G$ and denoted $[G : H]$. Lagrange's theorem also tells us that, for any element $g$ of a group $G$ with order $n$, the order of the cyclic subgroup $\langle g \rangle$ must divide $n$, so the order of the element $g$ divides $n$. Consequently, we know $g^n = e$ for any element $g \in G$.

We now know that a subgroup $H$ can partition a group $G$ in two ways, namely into left cosets of the form $aH$ or into right cosets of the form $Ha$. Remark that in general, the left cosets *do not equal* the right cosets.

### 2.5. Isomorphisms and Homomorphisms

Consider the group $G_1 = \{\pm 1, \pm i\}$ under complex multiplication alongside the group $G_2 = \langle \rho \rangle \leq S_4$, where $\rho$ is the permutation that takes $1 \mapsto 2$, $2 \mapsto 3$, $3 \mapsto 4$, and $4 \mapsto 1$. The groups have the following multiplication tables:

$G_1$:

| | $1$ | $i$ | $-1$ | $-i$ |
|---|---|---|---|---|
| $1$ | $1$ | $i$ | $-1$ | $-i$ |
| $i$ | $i$ | $-1$ | $-i$ | $1$ |
| $-1$ | $-1$ | $-i$ | $1$ | $i$ |
| $-i$ | $-i$ | $1$ | $i$ | $-1$ |

$G_2$:

| | $e$ | $\rho$ | $\rho^2$ | $\rho^3$ |
|---|---|---|---|---|
| $e$ | $e$ | $\rho$ | $\rho^2$ | $\rho^3$ |
| $\rho$ | $\rho$ | $\rho^2$ | $\rho^3$ | $e$ |
| $\rho^2$ | $\rho^2$ | $\rho^3$ | $e$ | $\rho$ |
| $\rho^3$ | $\rho^3$ | $e$ | $\rho$ | $\rho^2$ |

It doesn't take long to realise that these two multiplication tables are the same, up to relabeling $1 \equiv e$, $i \equiv \rho$, $-1 \equiv \rho^2$, and $-i \equiv \rho^3$. This is an example of the concept of isomorphisms between groups.

Formally, an *isomorphism* is a bijection $f : G \to G'$ from a group to another such that

$$f(x \cdot y) = f(x) \cdot f(y).$$

The multiplication on the left-hand side is taking place in $G$ while the right-hand multiplication takes place in $G'$. In the above example, the function $f : G_1 \to G_2$ that takes $i^k \mapsto \rho^k$ for $k = 0, 1, 2, 3$ gives an explicit isomorphism. If there exists an isomorphism between two groups, we say that they are *isomorphic*.

Any two cyclic groups of order $n$ are isomorphic. We will not formally prove this, but it is clear that if $G_1$ and $G_2$ are cyclic groups of the same order generated by $g_1$ and $g_2$ respectively, then the function $f : G_1 \to G_2$ given by $f({g_1}^k) = {g_2}^k$ for any integer $k$ will be a well-defined isomorphism.

As a perhaps surprising example, the group of real numbers under addition and the group of positive real numbers under multiplication are isomorphic to one another. The function $f(x) = e^x$ is a bijection from $\mathbf{R}$ to $\mathbf{R}^+$ and $e^{x+y} = e^x e^y$ for real numbers $x$ and $y$.

If two groups $G_1$ and $G_2$ are isomorphic, then

a) The groups have the same order, i.e. $|G_1| = |G_2|$.

b) Either $G_1$ and $G_2$ are both abelian or they are both non-abelian.

c) Both groups have the same number of elements of every order.

These properties are useful in showing that two groups are not isomorphic. For example, $S_3$ has no element of order 6, so it is not isomorphic to the cyclic group of order 6, which has two such elements: 1 and 5.

An isomorphism from a set to itself is called an *automorphism*. Given a group $G$, we can construct a set $\mathrm{Aut}(G)$ of all automorphisms of $G$ and in fact, it is easily verifiable that $\mathrm{Aut}(G)$ is a group under function composition.

We may obtain a generalisation of an isomorphism by relaxing the requirement that the function be bijective. Any map $f : G_1 \to G_2$ between groups that satisfies $f(x \cdot y) = f(x) \cdot f(y)$ for all $x, y \in G_1$ is called a *homomorphism*, and an isomorphism is simply a bijective homomorphism. It follows from the definition that any homomorphism maps the identity of the first group to the identity of the second, and that inverses are mapped to inverses. The simplest example of a homomorphism is the trivial homomorphism that maps every element of $G_1$ to the identity of $G_2$. Another homomorphism that is not an isomorphism is the map from $\mathbf{Z}$ to $S_2$ that takes all even integers to the identity and all odd integers to the permutation that switches 1 and 2.

Let $f : G \to G'$. The *kernel* of $f$, denoted $\ker(f)$, is a the set of all elements in the $G$ that map to the identity $e'$ of the target group $G'$. The *image* of $f$, denoted $\mathrm{Im}(f)$, is the set of all elements in $G'$ that equal $f(g)$ for some $g \in G$. Then the homomorphism $f$ is an isomorphism if and only if $\ker(f) = \{e\}$ and $\mathrm{Im}(f) = G'$. It is an easy exercise to verify that $\ker(f)$ and $\mathrm{Im}(f)$ are subgroups of $G$ and $G'$ respectively. In fact, the kernel of a homomorphism is a normal subgroup.

### ?.?. Group Actions on Sets

Let $G$ be a group and $S$ a set of elements. We say that $G$ *acts on* $S$ if there exists a map from $G \times S \to S$ (whose pairs $(g, s)$ are written $g(s)$) such that, for all $s \in S$, $e(s) = s$ and $(gh)(s) = g\big(h(s)\big)$ for every $g, h \in G$. For any element $s \in S$, the *orbit* is set of elements in $S$ to which $s$ may be taken by $G$:

$$O_s = \{g(s) \in S : g \in G\}$$

If there exists an $s$ such that $O_s = S$, then we say that $G$ acts *transitively* on $S$. In fact, because the orbits of a group action partition the set $S$ into equivalence classes, transitivity of a group action implies there is only one orbit, and for any $s, s' \in S$, there exists some $g \in G$ such that $g(s) = s'$.

The *stabiliser* of $s$ is the set of all elements in $G$ that leave $s$ fixed:

$$G_s = \{g \in G : g(s) = s\}$$

Consider a model example of a transitive action. Let $G$ be a group with a subgroup $H \leq G$; let $S$ be the set $\{aH : a \in G\}$ of left cosets of $H$. The group $G$ acts on $S$ by taking a coset $aH$ to $gaH$. This action is transitive: For any $a, a'$, there exists some $g$ such that $g(a) = a'$, so we can take any $aH$ to $a'H$ via $g$ as well. The closure property of subgroups gives us $G_H = H$, and the stabiliser of an arbitrary coset $aH$ is the set $\{g \in G : gaH = aH\}$. We find that this is exactly the conjugate subgroup $aHa^{-1}$. More generally, if $G$ acts transitively on a set $S$ and $g(s) = s'$, then $G_{s'} = gG_s g^{-1} \subset G$.

### ?.?. The Sylow Theorems

Suppose that a group $G$ acts on itself by conjugation:

$$s \mapsto gsg^{-1}.$$

Then the orbit of an element $s$ is its conjugacy class and its stabiliser is the set $\{g \in G : gsg^{-1}\}$, also called the centraliser. Let $\overline{H}$ denote the set of all subgroups of $G$. Then $G$ also acts on $\overline{H}$ by conjugation: $g(H) = gHg^{-1}$. In this action, the stabiliser of a subgroup $H$ is the set

$$G_H = \{g \in G : gHg^{-1} = H\}.$$

Note that this is not the centraliser of $H$; elements may not be taken to themselves pointwise, so long as the sets $gHg^{-1}$ and $H$ are equal. This subset of $G$ is called the *normaliser* of $H$ and is itself a subgroup, denoted $N(H)$.

## REFERENCES

The contents of this document are heavily based on the following three sets of lectures: Math 122 given by Benedict Gross at Harvard University, Fall 2003; MATH 235 given by Dani Wise at McGill University, Fall 2018; and MATH 456 given by Mikaël Pichot at McGill University, Fall 2019.