MATH GRT: ADVANCED ALGEBRA II (GROUP THEORY)

HEESUNG YANG

Abstract. This notes cover group theory aspect of the second half of Dalhousie's algebra comprehensive exam syllabus which is not covered in Advanced Algebra II (MATH 5055). This notes will cover the following sections of Dummit & Foote: Chapter I, Chapter II, Chapter III.1, Chapter III.2, Chapter III.3, Chapter IV.5, and Chapter IV.6 (statement only – A_n is simple for any $n \geq 5$.). Some propositions and lemmas are from the past comprehensive exams; the proofs of those lemmas and propositions are also included in this note.

1. Chapter I: Introduction to Groups

Definition 1.1. A *group* is an ordered pair $(G, *)$ where G is a set, and $*$ is a binary associative operation satisfying the following axioms, for any $a, b \in G$:

- (Non-emptiness of G, or the existence of an identity) There exists $e \in G$ such that $e * a = a * e = a$ for all $a \in G$. Such e is said to be an *identity* of $(G, *)$.
- (Existence of an inverse) For any $a \in G$ there exists $z \in G$ such that $a * z = z * a = e$. z is called an *inverse* of a, and we denote $z = a^{-1}$.
- (Closure under $*$) $a * b \in G$,

Definition 1.2. If $\#G < \infty$, then G is a *finite group*.

Definition 1.3. Suppose that for any $a, b \in G$ we have $a * b = b * a$. Then G is an *abelian group*.

Proposition 1.1. *If G is a group under operation $*$, then:*

(1) the identity e of G is unique.
(2) for any $a \in G$, the inverse of a is unique.
(3) $(a^{-1})^{-1} = a$ for all $a \in G$
(4) $(a * b)^{-1} = (b^{-1}) * (a^{-1})$
(5) (Generalized associativity) For any $a_1, a_2, \ldots, a_n$, the value of $a_1 * a_2 * \cdots * a_n$ is independent of how the expression is bracketed.

Proof. Suppose that e and e' are both identities. Then we have $e' * e = e$, by letting $a = e'$ and $b = e$. Similarly, we can let $a = e$ and $b = e'$ so that $e * e' = e'$. Therefore $e = e'$, as required.

For the second part, suppose that both z and z' are inverses of a, i.e., $a * z = z' * a = e$. Hence,

$$\begin{aligned} z' &= z' * e \qquad (\because e \text{ is the identity of } G) \\ &= z' * (a * z) = (z' * a) * z \qquad (\because \text{associativity of } *) \\ &= e * z = z. \end{aligned}$$

Date: 7 December 2018.

Thus $z' = z$ as required.

Let $z = a^{-1}$, i.e., $z * a = a * z = e$. Then z^{-1} is the inverse of z, which is a. Now replace z with a^{-1}; the claim follows.

As for the fourth part, note $(b^{-1})*(a^{-1})*(a*b) = (b^{-1})*((a^{-1})*a)*b = b^{-1}*e*b = b^{-1}*b = e$, so the claim follows.

The last claim can be proved by induction on n. □

Now we shall introduce some examples of groups. Before doing so, we shall introduce a mathematical structure called *field* here, though field theory will not be explored until Chapters XIII and XIV of the textbook (see the main MATH 5055 notes for this) as we need fields to introduce some example of groups.

Definition 1.4. A *field* is a set F with operations called $+$ (addition) and $\cdot$ (multiplication) such that:

(1) $(F, +)$ is an abelian group
(2) $(F^\times, \cdot)$ is an abelian group, where $F^\times := F \setminus \{0\}$. In other words, every non-zero element in F has a unique multiplicative inverse.
(3) The distributive law $a \cdot (b + c) = (a \cdot b) + (a \cdot c)$ holds for any $a, b, c \in F$.

Definition 1.5. The *characteristic of a field* F is the smallest n such that $\underbrace{1 + 1 + \cdots + 1}_{n \text{ times}} = 0$, and we write that $\operatorname{char} F = n$. If no such n exists, then $\operatorname{char} F = 0$. If $\operatorname{char} F > 0$, then $\operatorname{char} F$ can only be a prime number.

Example. Let $\mathrm{GL}_n(F)$ be the set of n-by-n matrices with entries from F whose determinant is non-zero. $\mathrm{GL}_n(F)$ is a group under multiplication – note that the identity matrix $I_n \in \mathrm{GL}_n(F)$ since $\det(I_n) = 1_F$. Every matrix with non-zero matrix determinant has a unique inverse (i.e., for any A there exists a unique B such that $AB = BA = I_n$). Finally, since $\det(AB) = \det(A) \cdot \det(B)$, for any $A, B \in \mathrm{GL}_n(F)$, $AB \in \mathrm{GL}_n(F)$ since $\det(AB) \neq 0$ also. The matrix multiplication is not commutative, so $\mathrm{GL}_n(F)$ is a non-abelian multiplicative group.

From this point on, we shall drop the notation $*$ for the group notation. The multiplication shall denote a general group notation, unless a group notation is specified (e.g. addition, subtraction, etc).

Proposition 1.2 (Cancellation laws)**.** *The left cancellation and the right cancellation both hold in G, i.e., for any $a, b, u, v \in G$,*

(1) if $au = av$, then $u = v$;
(2) if $ub = vb$, then $u = v$.

Proof. The left cancellation follows upon multiplying a^{-1} on both sides on the left, i.e., $a^{-1}(au) = a^{-1}(av) \Leftrightarrow (a^{-1}a)u = (a^{-1}a)v$, so $u = v$. The right cancellation can be proved similarly. □

Corollary 1.1. *Let G be a group where $a, b \in G$. Then each equation $ax = b$ and $ya = b$ has a unique solution for $x, y \in G$.*

Proof. Using the left cancellation, we see that $a^{-1}(ax) = (a^{-1}a)x = x = a^{-1}b$; and since a^{-1} is unique for each a, so is x. The second equation can be solved by applying the right cancellation rule, i.e., $(ya)a^{-1} = y(aa^{-1}) = y = ba^{-1}$. □

Definition 1.6. For any $x \in G$ where G is a group, the *order of* x is the smallest integer d such that $x^d = 1$. If no such d exists, then the order of x is said to be infinite. We shall denote it by $\operatorname{ord}(x)$.

Remark. The only element in G to have order 1 is the identity element.

Example. Let p be a prime. For any additive group $(\mathbb{Z}/p\mathbb{Z}, +)$, the order of 1 is p. In fact, $\mathbb{Z}/p\mathbb{Z}$ is a field also. (In fact, in Chapter XIV.3, we will prove that any field with finitely many elements must be of prime power order.) so $\operatorname{char} \mathbb{Z}/p\mathbb{Z} = p$. $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$ are other examples of fields. In all of these cases, under addition, we have $\operatorname{ord}(1) = \infty$ in $\mathbb{Q}, \mathbb{R}$, and $\mathbb{C}$. Therefore $\operatorname{char} \mathbb{Q} = \operatorname{char} \mathbb{R} = \operatorname{char} \mathbb{C} = 0$.

Definition 1.7. Let G be a group, and $S \subseteq G$ a subset of G (N.B. S need not be a group). If every element in G can be written as a (finite) product of elements of S and their inverses, then we say that the elements in S are the *generators of* G, and write $G = \langle S \rangle$. If $\#S = 1$, then G is said to be a *cyclic group*.

Definition 1.8. Let $(G, \star)$ and $(H, \circ)$ be groups, and let $\varphi : G \to H$ satisfying

$$\varphi(x \star y) = \varphi(x) \circ \varphi(y)$$

for all $x, y \in G$. Then φ is a *group homomorphism*.

Definition 1.9. If there is a bijective homomorphism φ between G and H, then G and H are said to be *isomorphic*, and φ is said to be an *isomorphism*. If G and H are isomorphic, we write $G \cong H$.

Remark. The best way to show that two groups are isomorphic is displaying an explicit isomorphism map; to show that they are not isomorphic, pick up a property that G and H don't share – for example, try to show that two groups have different number of elements of a certain order.

Proposition 1.3. *Suppose $\varphi : G \to H$ is an isomorphism. Then*

(1) $\#G = \#H$
(2) G is abelian if and only if H is abelian
(3) $\operatorname{ord}(x) = \operatorname{ord}(\varphi(x))$ for any $x \in G$.

Now we shall explore some special groups – symmetric group and dihedral group.

1.1. **Dihedral groups and the presentation of groups**

Dihedral group D_{2n} is a group consisting of reflection s and rotation r (by $2\pi/n$ radian) of the regular n-gon. In this chapter we will also talk about the presentation of groups using the dihedral groups as a median. While the group can be visualized, it is advisable to "graduate" from that perspective as soon as possible, and observe it as an abstract group in and of itself. The goal of this subsection is to show that D_{2n} is indeed generated by r and s, examine some group presentations similar to that of dihedral groups, and make a commentary on them. First, we lay down some properties of dihedral groups whose proof shall be left as an exercise.

Proposition 1.4 (Properties of a dihedral group)**.** *Let D_{2n} be the dihedral group of order $2n$; let r and s be as defined above.*

(1) $\operatorname{ord}(r) = n$*; that is,* n *is the smallest integer such that* $r^n = 1$*, and that* $1, r, \ldots, r^{n-1}$ *are all distinct.*
(2) $\operatorname{ord}(s) = 2$.
(3) $s \neq r^i$ *for any* i.
(4) $sr^i \neq sr^j$ *for any* $0 \leq i \neq j \leq n-1$*. Therefore,* D_{2n} *has exactly* $2n$ *elements, and that each element of*

$$D_{2n} = \{1, r, r^2, \ldots, r^{n-1}, s, sr, sr^2, \ldots, sr^{n-1}\}$$

can be uniquely written of the form $s^k r^m$ *where* $k \in \{0, 1\}$ *and* $m \in \{0, \ldots, n-1\}$.
(5) $rs = sr^{-1}$*. Therefore,* $r^i s = sr^{-i}$ *for all* $0 \leq i \leq n$.

We will define what relations and presentations are before proceeding to write down the presentation of D_{2n}.

Definition 1.10. *Relations in* G are any equations in a group G that the generators satisfy. If G is generated by a subset S, and there is a collection of relations from which one can deduce the relation amongst the elements of S, then such collection of relations and generators is called a *presentation of* G.

Example. The *quaternion group*, Q_8 is defined by

$$Q_8 = \{\pm 1, \pm i, \pm j, \pm k\},$$

where

(1) $(-1)^2 = 1$
(2) $i^2 = j^2 = k^2 = -1$
(3) $i \cdot j = k, j \cdot k = i, k \cdot i = j$. Therefore, $j \cdot i = -k, k \cdot j = i, i \cdot k = -j$.
(4) $(-1) \cdot a = a \cdot (-1) = -a$ and $1 \cdot a = 1 \cdot a = a$ for all $a \in Q_8$.

One can verify that one possible presentation of Q_8 is

$$Q_8 = \langle x, y : x^4 = 1, x^2 = y^2, y^{-1}xy = x^{-1} \rangle.$$

(*Hint:* Take $i = x, j = y, k = xy$, and start from there.)

Therefore, we see that D_{2n} is generated by r and s such that $s^2 = 1, r^n = 1$, and $rs = sr^{-1}$. Thus the set of generators of D_{2n} is $\{r, s\}$ and the relations are $r^n = 1, s^2 = 1, rs = sr^{-1}$. Thus the presentation of D_{2n} is

$$D_{2n} = \langle r, s : r^n = 1, s^2 = 1, rs = sr^{-1} \rangle.$$

We conclude the section with further commentaries on group presentation. While presentations with generators give one an easy way to characterize the group, such convenience comes with cautiousness when using them due to subtleties involved. For instance, two seemingly similar presentations may in fact refer to completely different groups. The presentation in and of itself does not give any hint on some important properties of a group – such as whether the group is finite or infinite. Furthermore, it also may not give any insights on whether the two elements expressed in terms of generators are in fact equal or not. Consider the following example.

Example. It is not hard to see that $\langle x_1, y_1 : x_1^2 = y_1^2 = (x_1 y_1)^2 = 1 \rangle$ is a presentation of the group of order 4 (in fact it is equal to D_4), but $\langle x_2, y_2 : x_1^3 = y_1^3 = (x_1 y_1)^3 = 1 \rangle$ is a presentation of an *infinite group*. A deceptively simple change in presentation resulted in a rather big change in this case.

Another caution is that the relations may not give any hints on where unexpected "collapsing" may occur.

Example. Consider the following presentation of G which at first sight seems awfully similar to the presentation of D_{2n}:

$$X_{2n} := \langle x, y : x^n = y^2 = 1, xy = yx^2 \rangle.$$

It seems that x behaves like the r in D_{2n}, and y like the s in D_{2n}. Since $x^n = 1$, it may seem that x has order n; thus X_{2n} has order $2n$. But in fact this is not so: since $y^2 = 1$, we have $xy^2 = x$. Now applying the commutation relation ($xy = yx^2$),

$$x = xy^2 = (xy)y = (yx^2)y = (yx)(xy) = (yx)(yx^2) = y(xy)x^2 = y(yx^2)x^2 = y^2x^4 = x^4.$$

Therefore x^4 has order at most 3. Therefore X_{2n} is a group whose order is at most 6. In fact, one can deduce that X_{2n} is precisely D_6 for any $n = 3k$; if $3 \nmid n$, then X_{2n} is just the cyclic group of order 2 since $x = 1$.

Example. Consider the group presentation

$$H = \langle x, y : x^4 = y^3 = 1, xy = y^2x^2 \rangle.$$

It may seem at first sight that $\#H = 12$, but this is in fact the trivial group (group of order 1).

1.2. **Symmetric groups**

Definition 1.11. Let Ω be a non-empty set, and let S_Ω be the set of bijections of Ω to itself. Then under the usual function composition operation, S_Ω is a group. We call this group the *symmetric group on the set* Ω. In particular, if $\Omega = \{1, 2, \ldots, n\}$, then we write $S_\Omega = S_n$, and we call S_n the *symmetric group of degree* n.

Proposition 1.5. $\#S_n = n!$.

Proof. Count how many bijections there are from $\{1, 2, \ldots, n\}$ to itself. Note that it suffices to find how many injective functions there are since $\{1, 2, \ldots, n\}$ is a finite set. □

Definition 1.12. A *cycle* is a string of integers used to represent an element in S_n which cyclically permutes these integers (and fixing the integers not in the string). The cycle $(a_1a_2 \cdots a_n)$ is the permutation sending a_i to a_{i+1} for each of $i = 1, 2, \ldots, n-1$, and a_n to a_1. The cycle $(a_1a_2 \ldots a_t)$ is a cycle of length t; such cycle is called a *t-cycle*. If two cycles share no number in common, then the two cycles are said to be *disjoint*. Each element of S_n be written as a product of disjoint cycles; such decomposition is the *cycle decomposition* of that permutation.

Proposition 1.6. *Any element in S_n can be uniquely expressed as a product of disjoint cycles, up to the order of the disjoint cycles and up to cyclical permutation of the numbers within each cycle.*

Remark. If the disjoint condition is removed, then the uniqueness property no longer holds. For example, $(123) = (13)(132)(13) = (12)(23)$ in S_3.

Proposition 1.7. *For any $n \geq 3$, S_n is non-abelian.*

Proof. Note that $(13), (12) \in S_n$, but $(13)(12) = (123)$ while $(12)(13) = (132)$. □

Remark. Any two disjoint cycles commute in S_n.

2. Chapter I.7: Group actions

One way to analyze the structure of groups is via "group actions", by examining how a group acts on a set. In the next chapter, for instance, one sees that it is possible to prove that a subset is actually a subgroup by recognizing that it is a stabilizer or a kernel of some group action.

Definition 2.1. A *group action of a group G on a set A* is a map $\cdot : G \times A \to A$ such that

(1) $g_1 \cdot (g_2 \cdot a) = (g_1 g_2) \cdot a$ for all $g_1, g_2 \in G$ and $a \in A$, and
(2) $1 \cdot a = a$ for all $a \in A$.

Proposition 2.1. *Let G be a group acting on a set A. Suppose that, for each fixed $g \in G$, we define a map $\sigma_g : A \to A$ by $\sigma_g(a) := g \cdot a$.*

(1) For each fixed $g \in G$, σ_g is a permutation of A, and
(2) the map from G to S_A (the group of permutations of A) defined by $g \mapsto \sigma_g$ is a homomorphism. This homomorphism is called the permutation representation *associated to the group action $\cdot$.*

Remark. The above proposition shows that a group action of G on a set A acts as a permutation on A while being consistent with the group operations in G.

Definition 2.2. Let G be a group acting on a set A. For any $a \in A$, the *orbit of a* is the set

$$O_a := \{b \in A : \exists g \in G \text{ such that } g \cdot a = b\} = G \cdot a.$$

3. Chapter II: Subgroups

Definition 3.1. Let G be a group. If H is a non-empty subset of G such that $xy \in H$ and $x^{-1} \in H$ for any $x, y \in H$, then H is a *subgroup of G*, and we denote $H \leq G$.

Theorem 3.1 (One-step subgroup test)**.** *A non-empty subset H is a subgroup of G if and only if $xy^{-1} \in H$ for any $x, y \in H$.*

3.1. Cyclic groups and cyclic subgroups

As defined in one of the previous chapters, a group is cyclic if every element in that group is generated by a single element. One immediate consequence of G being cyclic is that G is abelian also. Thus the cyclic condition is a stronger condition than the abelian condition.

Proposition 3.1. *Suppose that $G = \langle x \rangle$ is cyclic. If $\#G = n$ is finite, then $x^n = 1$, and $x^m \neq 1$ for any $1 \leq m \leq n-1$; therefore, each of $x, x^2, \ldots, x^{n-1}$ are distinct. If $\#G = \infty$, then no n can satisfy $x^n = 1$, and $x^a = x^b$ if and only if $a = b$ in $\mathbb{Z}$.*

Proposition 3.2. *If G is an arbitrary group with $x \in G$ such that $x^n = x^m = 1$ for two distinct n and m, then $x^d = 1$ where $d := \gcd(m, n)$. Therefore,* $\operatorname{ord}(x) \mid m$ *if $x^m = 1$.*

Proposition 3.3. *If G and H are two cyclic groups of the same order, then $G \cong H$. Particularly, if $G = \langle x \rangle$ and $H = \langle y \rangle$, then*

(1) $\varphi : G \to H$ defined by $x^k \mapsto y^k$ is a well-defined group isomorphism.
(2) $\varphi : \mathbb{Z} \to G$ defined by $k \mapsto x^k$ is a well-defined group isomorphism, provided that $\operatorname{ord}(x) = \infty$*, i.e., $\#G = \infty$.*

Proposition 3.4. *Let G be a group; let $x \in G$, and let a be a non-zero integer.*

(1) if $\operatorname{ord}(x) = \infty$*, then* $\operatorname{ord}(x^a) = \infty$ *also.*
(2) if $\operatorname{ord}(x) = n < \infty$*, then* $\operatorname{ord}(x^a) = n/\gcd(n, a)$.

Corollary 3.1. *If* $a \mid n$ *and* $\operatorname{ord}(x) = n$*, then* $\operatorname{ord}(x^a) = n/a$.

Proposition 3.5. *Suppose that* $G = \langle x \rangle$.

(1) If G *is infinite, then* $G = \langle x^a \rangle$ *if and only if* $a = \pm 1$.
(2) If $\#G = n < \infty$*, then* $G = \langle x^a \rangle$ *if and only if* $\gcd(a, n) = 1$*. Therefore, there are precisely* $\varphi(n)$ *generators of* H.

Example. For any prime p, the group of units $G_p := (\mathbb{Z}/p\mathbb{Z})^\times$ is cyclic (under multiplication). In fact, $(\mathbb{Z}/n\mathbb{Z})^\times$ is cyclic if and only if n is prime. There are precisely $\varphi(p) = p - 1$ elements in G_p, so there are $\varphi(\varphi(p)) = \varphi(p-1)$ elements that generate G_p. For instance, if $p = 7$, then we see that $G_7 = \langle 3 \rangle$. Then $3^2 = 2$, and indeed $\operatorname{ord}(2) = 6/\gcd(6, 2) = 3$. One can confirm this by noticing that $2^3 \equiv 1 \pmod 7$. Therefore 2 cannot be a generator. However, $3^5 = 243 \equiv 5 \pmod 7$, and indeed $\operatorname{ord}(5) = 6/\gcd(6, 5) = 6$. Since $5^3 \equiv -1 \pmod 7$, we know that $\operatorname{ord}(5)$ is indeed 6.

Theorem 3.2. *If* $G = \langle x \rangle$ *is cyclic, then any subgroup* H *of* G *is also cyclic.*

(1) If d *is the smallest integer such that* $x^d \in H$*, then* $H = \langle x^d \rangle$*. If there is no such integer, then* $H = \{1\}$.
(2) If G *is an infinite cyclic group, then* $\langle x^a \rangle = \langle x^b \rangle$ *if and only if* $a = \pm b$ *in* $\mathbb{Z}$*. Therefore, there is a bijection between* $\mathbb{N}$ *and* $X := \{\langle x^a \rangle : a \in \mathbb{N}\}$ *(just map* $a \mapsto \langle x^a \rangle$*).*
(3) If $\#G = n < \infty$*, and* $a \mid n$*, then* $\langle x^{n/a} \rangle$ *is a (cyclic) subgroup of* G*. More generally,* $\langle x^m \rangle = \langle x^{\gcd(m,n)} \rangle$*, so in this case there is a bijection between the positive divisors of* n *and* $Y := \{\langle x^a \rangle : a \mid n\}$ *(map* $a \mapsto \langle x^{n/a} \rangle$*).*

3.2. Subgroups generated by subsets of a group

Note that the cyclic case is a special case of a group generated by a single element, which in turn results in every subgroup being generated by a single element. We can generalize this notion to consider subgroups that are not necessarily generated by a single element, but many elements.

Definition 3.2. Let G be a group, and A a subset (not necessarily a subgroup) of G. Then the *subgroup generated by* A is the smallest subgroup generated by the elements in A. To put it another way, if

$$H := \bigcap_{\substack{A \subseteq Z \\ Z \leq G}} Z,$$

then H is the subgroup generated by A, and we write $H = \langle A \rangle$. If $\#A < \infty$, then we say that $\langle A \rangle$ is *finitely generated*.

Remark. Being finitely generated does *not* imply finiteness. Note that $(\mathbb{Z}, +)$ is finitely generated since $\mathbb{Z} = \langle 1 \rangle$, but $\#\mathbb{Z} = \infty$.

Example. Any symmetric group, S_n is finitely generated, since

$$S_n = \langle (12), (123 \ldots n) \rangle.$$

However, while $\operatorname{ord}((12) = 2$ and $\operatorname{ord}((123 \ldots n)) = n$, note that $\#S_n = n!$. Any dihedral group, D_{2n} is another finitely generated group, so any subgroup is also finitely generated.

At this point, one may want to verify if the H as defined above is really a subgroup.

Proposition 3.6. *Let $\mathcal{A}$ be any non-empty collection of subgroups of G. Then the intersection of all members of $\mathcal{A}$ is also a subgroup of G.*

Also, the following proposition gives ideas on how to construct an element of a group generated by elements of A. Note that we do not assume that A is not countable (i.e., A need not be countably infinite or finite).

Proposition 3.7. *Let A be a subset (which may be uncountable) of a group G. Define*

$$\overline{A} := \{a_1^{e_1} \cdots a_n^{e_n} : n \in \mathbb{N} \cup \{0\}, a_i \in A, e_i = \pm 1 \text{ for each } i\}.$$

(if $A = \emptyset$, let $\overline{A} = \{1\}$. Also, the a_i need not be distinct.) The set $\overline{A}$ is therefore the set of words of elements of A and the inverses of elements of A. Then $\overline{A}$ is a subgroup of G. Furthermore, $\overline{A} = \langle A \rangle$.

We shall finish this section by discussing a celebrated result on finitely generated abelian groups. To do so, we shall introduce the following definition first.

Definition 3.3. Write $\mathbb{Z}^r := \underbrace{\mathbb{Z} \times \mathbb{Z} \times \cdots \times \mathbb{Z}}_{r \text{ times}}$. If $r = 0$, then $\mathbb{Z}^0 = 1$. Then this group $\mathbb{Z}^r$ is called the *free abelian group of rank r*.

Theorem 3.3 (Fundamental theorem of finitely-generated abelian groups)**.** *Let G be a finitely-generated abelian group. Then*

$$G \cong \mathbb{Z}^r \oplus \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_s\mathbb{Z}$$

for some $r \geq 0$ and $n_1, \ldots, n_s \in \mathbb{N}_{>1}$ such that $n_{k+1} \mid n_k$ for all $1 \leq k \leq s-1$. Furthermore, such decomposition of G is unique. $\mathbb{Z}^r$ is sometimes called the torsion-free part of the decomposition of G, and the remaining portion the torsion portion.

Corollary 3.2 (Fundamental theorem of finite abelian groups)**.** *If G is a finite abelian group, then there exist $n_1, n_2, \ldots, n_s$ such that*

$$G \cong \mathbb{Z}/n_1\mathbb{Z} \oplus \mathbb{Z}/n_2\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/n_s\mathbb{Z},$$

where each n_i is a prime power.

Proof. Every finite abelian group is finitely generated; the claim follows upon noting that r needs to be 0. □

Corollary 3.3 (Chinese remainder theorem)**.** $\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ *if and only if* $\gcd(m, n) = 1$.

3.3. Centralizers, normalizers, stabilizers, and kernels

Definition 3.4. Let G be a group, and write $gAg^{-1} = \{gag^{-1} : a \in A\}$ where $g \in G$. Then the *normalizer of A in G* is $N_G(A) := \{g \in G : gAg^{-1} = A\}$.

If we take $A = N$, and if it happens that $N_G(N) = G$, then we have the following definition.

Definition 3.5. The element gng^{-1} is the *conjugate of $n \in N$ by $g \in G$*. The set $gNg^{-1} = \{gng^{-1} : n \in N\}$ is called the *conjugate of N by g*. The element g *normalizes* N if $gNg^{-1} = N$. If $gNg^{-1} = N$ for any $g \in G$, then N is the *normal subgroup of G*.

We introduce a special case of a normalizer.

Definition 3.6. Suppose that A is a non-empty subset of G. Then the *centralizer of* G $C_G(A)$ is the set of elements in G that commutes with every element in A.

$$C_G(A) := \{g \in G : ga = ag \text{ for all } a \in A\}.$$

If we let $A = G$, we get the following definition.

Definition 3.7. The *centre of* G $Z(G)$ is the set of elements that commute with every element in G. In other words,

$$Z(G) = \{z \in G : gz = zg \text{ for all } g \in G\}.$$

Remark. G is abelian if and only if $Z(G) = G$. In fact, showing that $Z(G) = G$ is one way to show that G is abelian.

Proposition 3.8. *$C_G(A)$ is a subgroup of G. Therefore, $Z(G)$ is a subgroup of G.*

Proposition 3.9. *Suppose that p is prime. Then any group of order p^2 is abelian.*

Proof. Let $\#G = p^2$ where p is a prime. It suffices to show that $G = Z(G)$. If G is cyclic (i.e. there exists an element of order p^2), then the proposition trivially follows, so assume that every non-identity element has order p. Consider $G/Z(G)$. Since $Z(G)$ is a normal subgroup of G, we have $\#Z(G) = 1, p$, or p^2. Suppose that $\#Z(G) = p$. Then $\#(G/Z(G)) = p$ also, so $G/Z(G)$ is cyclic. But this means $G/Z(G)$ is abelian, so this forces $G = Z(G)$. So once we prove that the centre of G cannot be trivial, we are done. Pick non-identity element x; then $\langle x \rangle$ has order p since $\#\langle x \rangle = \text{ord}\,(x)$. Note that $\langle x \rangle$ is normal, since both $G/\langle x \rangle$ and $\langle x \rangle$ are both abelian (the former is abelian since $\#(G/\langle x \rangle) = p$). Hence for any non-identity $g \in G$, there is $1 \leq r \leq p-1$ so that $gxg^{-1} = x^r$. Therefore $g^{p-1}xg^{-(p-1)} = x^{r^{p-1}}$. But then by Fermat's little theorem, we have $r^{p-1} \equiv 1 \pmod{p}$, so $g^{p-1}xg^{-(p-1)} = x$, or $g^{p-1}x = xg^{p-1}$. Therefore $g^{-1}x = xg^{-1}$, since the order of g is p. This implies that $x \in Z(G)$. Since the centre of G is non-trivial, $\#Z(G) = p^2 = \#G$. Therefore $G = Z(G)$ as required. □

Remark. Note that the above proof works because the order of a group happened to be prime square. One can also use the class equation to prove the same result.

Theorem 3.4 (Class equation)**.** *Let G be a finite group, and let $g_1, g_2, \ldots, g_r$ be the representatives of the distinct conjugacy classes of G not contained in $Z(G)$. Then*

$$\#G = \#Z(G) + \sum_{i=1}^{r} \frac{\#G}{\#C_G(g_i)}.$$

Remark. One can also write $|G : C_G(g_i)|$ instead of $\#G/\#C_G(g_i)$, but since G is a finite group, $|G : C_G(g_i)| = \#G/\#C_G(g_i)$. $|G : C_G(g_i)|$ is said to be the *index of $C_G(g_i)$ in G*, but this notation becomes more important when G is an infinite group. See Chapter III.1 for more information.

Proposition 3.10. *If G is a p-group (i.e., $\#G$ is a power of p), then G has a non-trivial centre.*

Proof. We shall use the class equation to solve this. If $G = Z(G)$, then the statement is true. So suppose that $G \neq Z(G)$. Then the class equation implies

$$\#G = \#Z(G) + \sum_{i=1}^{r} \frac{\#G}{\#C_G(g_i)}.$$

We may assume that $g_i \notin Z(G)$ since otherwise g_i will be "absorbed" by $Z(G)$. Therefore $C_G(g_i)$ is a proper subgroup of G; and by Lagrange, the order of $C_G(g_i)$ is a power of p; therefore $\#G/\#C_G(g_i) = p^{k_i}$ is a power of p with $k_i > 0$, hence a multiple of p. But then $\#G$ is a power of p, so $\#Z(G)$ must be a multiple of p also. This shows $\#Z(G) > 1$, so $Z(G)$ cannot be trivial. □

Proposition 3.11. *Let G be a group of order pq, where p and q are distinct primes. Then either G is abelian or G has the trivial centre.*

We shall first prove the following lemma.

Lemma 3.1. *If $G/Z(G)$ is cyclic, then G is abelian.*

Proof of Lemma 3.1. If $G/Z(G)$ is cyclic, then there exists $g \in G$ such that $\langle gZ(G)\rangle = G/Z(G)$. Thus for any $x \in G$, there exists some $a \geq 0$ so that $(gZ(G))^a = g^aZ(G) = xZ(G)$. Therefore $g^ax^{-1} \in Z(G)$. Thus there exists $z \in Z(G)$ such that $g^{-a}x = z$, so $x = g^az$. Hence any $x \in G$ can be written in the form g^az where $z \in Z(G)$ and $a \geq 0$. So if $x = g^{a_1}z_1, y = g^{a_2}z_2 \in G$, we have

$$\begin{aligned} xy &= (g^{a_1}z_1)(g^{a_2}z_2) = g^{a_1}(z_1g^{a_2})(z_2) = g^{a_1}(g^{a_2}z_1)z_2 = g^{a_1}g^{a_2}(z_2z_1) \\ &= g^{a_2}g^{a_1}z_2z_1 = g^{a_2}(z_2g^{a_1})z_1 = yx, \end{aligned}$$

so G is abelian as required. □

Proof of Proposition 3.11. Since $Z(G)$ is a subgroup of G, we see that $\#Z(G) = 1, p, q$, or pq. Suppose that $\#Z(G) = q$. Then $\#(G/Z(G)) = p$, so $G/Z(G)$ is cyclic. Then by Lemma 3.1, G is abelian. The same argument holds if we assume $\#Z(G) = p$. Thus $\#Z(G) = pq$ or 1. If $\#Z(G) = pq$, then G is abelian. Otherwise, $\#Z(G)$ must be 1. □

While one can directly verify that normalizers, centralizers, and centres are subgroup, one can also prove this by considering group actions of G as a special case of general results on group actions. This prompts us to introduce the stabilizer.

Definition 3.8. Let G be a group, and S be a set that G acts on. If $s \in S$, then the *stabilizer of s in G* is the set

$$G_s := \{g \in G : g \cdot s = s\}.$$

More specifically, the *kernel of the action of G on S* is

$$\ker_G S := \{g \in G : g \cdot s = s \text{ for all } s \in S\}.$$

Proposition 3.12. *G_S and $\ker_G S$ are subgroups of G.*

Proposition 3.13. *Suppose that A is a subset of G. Then $N_G(A), C_G(A)$, and $Z(G)$ are all subgroups of G.*

Proof. Let c be the conjugation group action on some $B \subseteq G$. In other words,

$$c : B \to gBg^{-1},$$

where $gBg^{-1} = \{gbg^{-1} : b \in B\}$. Then it is a straightforward verification to see that $N_G(A)$ is precisely the stabilizer G_s where $s = A$. Similarly, $C_G(A)$ is precisely equal to $\ker_G A$. Finally, $Z(G)$ is equal to $\ker_G G$. □

Theorem 3.5 (Orbit-stabilizer theorem)**.** *Suppose that G acts on a finite set S. Then $\#O_s \cdot \#G_s = \#G$.*

4. Chapter III.1: Quotient groups and homomorphism

Definition 4.1. The *kernel of* φ for a group homomorphism $\varphi : G \to H$ is

$$\ker \varphi = \{g \in G : \varphi(g) = 1_H\}.$$

Proposition 4.1. *Let $\varphi : G \to H$ be a group homomorphism. Then*

(1) $\varphi(1_G) = 1_H$.
(2) $\varphi(g^{-1}) = \varphi(g)^{-1}$.
(3) $\varphi(g^n) = \varphi(g)^n$.
(4) $\ker \varphi$ *is a normal subgroup of* G.
(5) $\operatorname{im} \varphi$ *is a subgroup of* H.

Definition 4.2. Let $\varphi : G \to H$ be a group homomorphism, and $K = \ker \varphi$. Then G/K is the *quotient group* where each element in G/K is a "representative" with the group operation defined for G. Namely, if a represents X, and b represents Y, then XY is represented by ab.

Proposition 4.2. *Let $\varphi : G \to H$ be a group homomorphism with $\ker \varphi = K$. If $X \in G/K$ and a represents X (i.e., $a = \varphi(X)$), then*

(1) For any $u \in X$, $X = \{uk : k \in K\}$
(2) For any $u \in X$, $X = \{ku : k \in K\}$.

Theorem 4.1. *Let G be a group, and let K be the kernel of some homomorphism from G to another group. Then the set of whose elements are the left cosets of K in G with operation defined by*

$$uK \cdot vK = (uv)K$$

forms a group G/K. If $u_1 \in uK$ and $v_1 \in vK$, then we have $u_1v_1 \in uvK$. Therefore $u_1v_1K = uvK$, so this operation is well-defined. The same claim holds for right cosets.

Remark. Therefore, it does not matter which representative we choose for each of the cosets.

In fact, we can generalize this notion for any subgroup, not just the kernel of some homomorphism. However, we shall see that the operation defined in the theorem above is not well-defined unless that subgroup is the kernel of some homomorphism. In fact, gN may not even form a subgroup of G.

Definition 4.3. Suppose $N \leq G$. Then for any g, let

$$gN := \{gn : n \in N\} \text{ and } Ng = \{ng : n \in N\}.$$

Then gN is the *left coset of N in G*, and Ng is called the *right coset of N in G*. Any element in gN is called a *representative for the coset*.

If N is the kernel, and $g_1, g \in N$, then we have $g_1N = gN$. Indeed this holds for any subgroup N also.

Proposition 4.3. *Let $N \leq G$. Then the set of left cosets of N in G form a partition of G. Furthermore, for all $u, v \in G$, $uN = vN$ if and only if $v^{-1}u \in N$. Therefore, $uN = vN$ if and only if u and v are representatives of the same coset.*

Proposition 4.4. *Let $u, v \in G$. Then the operation $uN \cdot vN = (uv)N$ is well-defined if and only if N is a normal subgroup of G, i.e., $gng^{-1} \in N$ for all $g \in G$ and $n \in \mathbb{N}$. Furthermore, if such operation is well-defined, then the set of left cosets of N in G is a group whose identity element is $1N$, and the inverse is $g^{-1}N = (gN)^{-1}$.*

At this point, we know that the induced group operation on the quotient group is well-defined if and only if the subgroup we are taking the quotient of is normal. We also know that the operation is well-defined also only when that subgroup is the kernel of some homomorphism. So the question arises: is every normal subgroup the kernel of some homomorphism? The answer is affirmative, as shown in the upcoming theorem. Before getting into that theorem, we first summarize the characterizations of normal subgroups.

Proposition 4.5. *Let N be a subgroup of G. Then the following are equivalent.*

(1) N is a normal subgroup of G.
(2) $N_G(N) = G$
(3) $gN = Ng$ for all $g \in G$.
(4) The operation $\cdot$ defined by $uN \cdot vN = (uv)N$ makes the set of left cosets into a group
(5) $gNg^{-1} \subseteq N$ for all $g \in G$.

Theorem 4.2. *A subgroup N of G is normal if and only if there exists a group homomorphism $\varphi : G \to H$ such that $\ker \varphi = N$.*

5. Chapter III.2: More on cosets

We shall present more useful results on cosets.

Definition 5.1. Let $H, K \leq G$. Then we define

$$HK := \{hk : h \in H, k \in K\}.$$

Proposition 5.1. *If H and K are finite subgroups of a group, then*

$$\#(HK) = \frac{\#H \cdot \#K}{\#(H \cap K)}.$$

Proposition 5.2. *If H and K are subgroups of G, then HK is a subgroup if and only if $HK = KH$.*

There is a neat corollary to the above proposition, but before this we need to introduce what normalization means.

Definition 5.2. If A is any subset of $N_G(K)$ (resp. $C_G(K)$), we say that A *normalizes (resp. centralizes) K*.

Corollary 5.1. *If H and K are subgroups of G, then HK is a subgroup if H (resp. K) normalizes K (resp. H). Therefore, if K is a normal subgroup of G, then HK is a subgroup for any subgroup H of G.*

6. Chapter III.2: Lagrange's theorem

An important result we are going to cover here is Lagrange's theorem. While simple and straightforward, this is a very important result in group theory.

Theorem 6.1 (Lagrange's theorem)**.** *If G is a finite group and $H \leq G$, then $\#H \,|\, \#G$. The number of left cosets of H in G is $\#G/\#H$.*

There are some quick corollaries of Lagrange's theorem.

Corollary 6.1. *If G is finite and $x \in G$, then $\operatorname{ord}(x) \mid \#G$. Therefore $x^{\#G} = 1$ for all $x \in G$.*

Corollary 6.2. *If G is a group of prime order p, then G is cyclic. In particular, $G \cong \mathbb{Z}/p\mathbb{Z}$.*

Note that Lagrange's theorem is limited to *finite* groups. Lagrange's theorem thus makes little sense if $\#G = \infty$. However, we can generalize the notion of $\#G/\#H$ with the following definition.

Definition 6.1. If G is a group (possibly infinite) and $H \leq G$, the *index of H in G* is the number of left cosets of H in G, and we denote this by $|G : H|$.

Remark. Note that the converse of Lagrange's theorem is not true. That is, even though $n \,|\, |G|$, G need not have a subgroup of order n. To see this, let A be the group of symmetries of a regular tetrahedron. One can verify that $\#A = 12$, which is divisible by 6. Suppose that $H \leq A$ is a subgroup of order 6. That means that there are two cosets, since $|A : H| = \#A/\#H = 12/6 = 2$. Therefore, $A/H \cong \mathbb{Z}/2\mathbb{Z}$. Thus A/H is abelian (in fact cyclic), so H is a normal subgroup of A. Thus the square of every element in A/H is identity, so $(gH)^2 = g^2H = 1H$. In other words, $g^2 \in H$ for any $g \in A$. Therefore if g is an element in A of order 3, then $g = (g^2)^2 \in H$, so H must contain every element in A of order 3. But this contradicts the fact that $\#H = 6$ – it's not hard to verify that there are 8 rotations of order 3 in A.

Remark. Note, however, there are some *partial converses* of Lagrange's theorem. But we shall discuss this more in depth in Chapter IV.5: Sylow theorems.

7. Chapter III.3: The four isomorphism theorems

Theorem 7.1 (First isomorphism theorem)**.** *Suppose that $\varphi : G \to H$ is a group homomorphism. Then*

$$G/\ker\varphi \cong \operatorname{im}\varphi,$$

and $\ker\varphi$ is a normal subgroup of G.

Proof. Suppose $k \in \ker\varphi$. Then for any $g \in G$, we have $\varphi(gkg^{-1}) = \varphi(g)\varphi(k)\varphi(g^{-1}) = \varphi(g)1\varphi(g^{-1}) = \varphi(g)\varphi(g^{-1}) = \varphi(gg^{-1}) = \varphi(1) = 1$, so $\ker\varphi$ is a normal subgroup. Also, $\operatorname{im}\varphi$ is a subgroup of H. $\operatorname{im}\varphi$ is non-empty since $1_H = \varphi(1_G)$. Also, for any $h_1, h_2 \in \operatorname{im}\varphi$ there exist g_1 and g_2 so that $\varphi(g_1) = h_1$ and $\varphi(g_2) = h_2$. Thus $h_1h_2^{-1} = \varphi(g_1)\varphi(g_2)^{-1} = \varphi(g_1)\varphi(g_2^{-1}) = \varphi(g_1g_2^{-1})$, so $h_1h_2^{-1} \in \operatorname{im}\varphi$ as required.

Let $\overline{\varphi} : G/\ker\varphi \to H$ be the map induced by φ. Suppose that $g_2 \in g_1 \ker\varphi$. Then $g_2g_1^{-1} \in \ker\varphi$. Thus $\overline{\varphi}(g_2\ker\varphi) = \varphi(g_2)$ and $\overline{\varphi}(g_1\ker\varphi) = \varphi(g_1)$; but $\varphi(g_2g_1^{-1}) = \varphi(g_2)\varphi(g_1)^{-1} = 1_H$,

so $\varphi(g_2) = \varphi(g_1)$. Thus $\overline{\varphi}$ is well-defined. Therefore if $\overline{\varphi}(g_1 \ker\varphi) = 1_H$, then $g_1 \in \ker\varphi$. Thus $\ker\overline{\varphi} = \{1 \ker\varphi\}$. φ is homomorphism since for any $g_1 \ker\varphi, g_2 \ker\varphi \in G/\ker\varphi$,

$$\overline{\varphi}(g_1 \ker\varphi \cdot g_2 \ker\varphi) = \overline{\varphi}((g_1 g_2)\ker\varphi) = \varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2) = \overline{\varphi}(g_1 \ker\varphi)\overline{\varphi}(g_2 \ker\varphi).$$

Finally, $\overline{\varphi}$ is surjective: for any $h \in \operatorname{im}\varphi$ there exists $g \in G$ such that $\varphi(g) = h$, so $\overline{\varphi}(g \ker\varphi) = \varphi(g) = h$. Therefore $\overline{\varphi}$ is an isomorphism from $G/\ker\varphi$ to $\operatorname{im}\varphi$ as needed. □

Corollary 7.1. *If $\varphi : G \to H$ is a group homomorphism, then φ is injective if and only if $\ker\varphi$ is trivial. Further, $|G : \ker\varphi| = |\varphi(G)|$.*

Theorem 7.2 (Second isomorphism theorem)**.** *Suppose that G is a group, and that $A, B \leq G$ such that $A \leq N_G(B)$. Then*

(1) AB is a subgroup of G.
(2) B is a normal subgroup of AB.
(3) $A \cap B$ is a normal subgroup of A.
(4) $AB/B \cong A/(A \cap B)$.

Proof. A and B are both subgroups of G, so AB is also a subgroup of G. Since $A \leq N_G(B)$ and $B \leq N_G(B)$, indeed $AB \leq N_G(B)$. Thus B is a normal subgroup of AB.

Now let $\varphi : A \to AB/B$ defined by $\varphi(a) = aB$. Since AB/B is well-defined (as B is a normal subgroup of AB), the group operation in AB/B i well-defined also. Then $\varphi(a_1a_2) = (a_1a_2)B = (a_1B)(a_2B) = \varphi(a_1)\varphi(a_2)$. Since $abB = aB$ for any $a \in A$ and $b \in B$, it follows that φ is surjective. Finally, if $\varphi(a) = 1B$, then $a \in B$. Thus $a \in A \cap B$, so $\ker\varphi = A \cap B$. Therefore $A \cap B$ is normal in A and $A/(A \cap B) \cong AB/B$ by the first isomorphism theorem. □

Theorem 7.3 (Third isomorphism theorem)**.** *Let G be a group, and let H and K be normal subgroups of G with $H \leq K$. Then K/H is a normal subgroup of G/H, and*

$$(G/H)/(K/H) \cong G/K.$$

Proof. We shall assume that K/H is a normal subgroup of G/H and prove this later. Let $\varphi : G/H \to G/K$ defined by $\varphi(gH) = gK$. First, verify that φ is well-defined. If $g_1H = g_2H$, then there is $h \in H$ such that $g_1 = g_2h$. Thus $g_1 = g_2h$ in K also. Therefore $g_1K = g_2K$, or $\varphi(g_1H) = \varphi(g_2H)$. So φ is surjective also, as $\varphi(gH) = gK$ for any arbitrary $g \in G$. Finally, if $\varphi(gH) = 1K$, then $\varphi(gH) = gK = 1K$. Therefore $g \in K$, so $gH \in K/H$ also. Hence $\ker\varphi = K/H$. $(G/H)/(K/H) \cong G/K$ by the first isomorphism theorem.

Now it remains to show that K/H is a normal subgroup of G/H. Let $kH \in K/H$ (i.e., $k \in K$). Then for any $g \in G$, $gkg^{-1} \in K$, so $gkg^{-1}H \in K/H$ also. Thus K/H is normal in G/H as required. □

Theorem 7.4 (Fourth isomorphism theorem)**.** *Let G be a group, and let N be a normal subgroup of G. Then there is a one-to-one correspondence between the set of subgroups of G containing N (say A) and the set of subgroups of the form $\overline{A} := A/N$ of $\overline{G} := G/N$. Therefore, every subgroup of G/N is of the form A/N where A is a subgroup of G containing N. Also, this bijection satisfies the following properties:*

(1) $A \leq B$ if and only if $\overline{A} \leq \overline{B}$,
(2) if $A \leq B$ then $\#(B/A) = \#(\overline{B}/\overline{A})$,
(3) $\overline{\langle A, B\rangle} = \langle \overline{A}, \overline{B}\rangle$,

(4) $\overline{A \cap B} = \overline{A} \cap \overline{B}$*, and*
(5) A *is a normal subgroup of* G *if and only if* $\overline{A}$ *is normal in* $\overline{G}$*.*

8. Chapter IV.5: Sylow theorems

Definition 8.1. Let G be a group, and p a prime.

(1) If $\#G = p^a$ for some $a \geq 0$, then G is a *p-group*. If a subgroup of G satisfies this property, then that subgroup is a *p-subgroup*.
(2) If $\#G = p^a m$ where $\gcd(p, m) = 1$, then a subgroup of order p^a is said to be a *Sylow p-subgroup* or a *p-Sylow subgroup* of G.
(3) The set of Sylow p-subgroups of G will be denoted by $\mathrm{Syl}_p(G)$, and $n_p(G)$ shall denote the number of p-Sylow subrgroups of G.

Lemma 8.1. *If P is a Sylow p-subgroup, then $Q \cap N_G(P) = Q \cap P$ where Q is any p-subgroup of G.*

Theorem 8.1 (Sylow's first theorem)**.** *Let G be a group of order $p^a m$ where $p \nmid m$. Then there exists a Sylow p-subgroup, i.e., $\mathrm{Syl}_p(G) \neq \emptyset$.*

Theorem 8.2 (Sylow's second theorem)**.** *Let G be a group of order $p^a m$ where $p \nmid m$. If P is a Sylow p-subgroup of G and Q is any p-subgroup of G, then there exists $g \in G$ such that $Q \leq gPg^{-1}$. Therefore, any two Sylow p-subgroups are conjugate of each other in G.*

Theorem 8.3 (Sylow's third theorem)**.** *Let G be a group of order $p^a m$ where $p \nmid m$. $n_p \equiv 1 \pmod{p}$. Furthermore, n_p is the index of the normalizer $N_G(P)$ for any Sylow p-subgroup ($n_p = [G : N_G(P)]$). Hence, $n_p \mid m$.*

Corollary 8.1 (Cauchy's theorem)**.** *If G is a finite group, and $p \mid \#G$, then there exists an element of order p in G. Therefore, G has a subgroup of order p.*

Corollary 8.2. *Any two Sylow p-subgroups (for the identical prime p) are isomorphic.*

Corollary 8.3. *The following are equivalent, for any P a Sylow p-subgroup of G.*

(1) $n_p = 1$
(2) P *is normal in* G
(3) for any σ*, an automorphism of* G*,* $\sigma(P) = P$*.*
(4) All subgroups generated by elements of p-power order are p-groups. In other words, if $X = \{x \in G : \mathrm{ord}\,(x) = p^a \text{ for some } a \geq 1\}$, then $\langle X \rangle$ is a p-group.

Proof. ((1) $\Rightarrow$ (2)) Suppose that $n_p = 1$, so let P be the unique Sylow p-subgroup. So if $q \in P$ (i.e., the order of q is some power of p) then for any $g \in G$, gqg^{-1} also has order p^k for some k. But since P is the unique Sylow p-subgroup, $gqg^{-1} \in P$ also. Thus $gPg^{-1} = P$ as required.

((2) $\Rightarrow$ (1)) Suppose that P is normal in G. Now, suppose that there is another Sylow p-subgroup Q. So Sylow's second theorem there exists $g \in G$ such that $Q \leq gPg^{-1}$. But since Q is another Sylow P-subgroup, and since $gPg^{-1} = P$, it follows that $Q = P$. Hence $n_p = 1$ as desired.

The remaining implications are left as exercises. □

8.1. **Using Sylow theorems to prove that a group of certain order is not simple**

Previously the notion of "normal subgroup" was introduced. Clearly, the trivial subgroup $\{1\}$ and the entire group G itself are normal in G. Some groups, however, have only those as normal subgroups.

Definition 8.2. A group G is a *simple group* if G has no proper normal subgroups. In other words, G only has $\{1\}$ and G as its only normal subgroups.

Example. Any trivial group is (trivially) simple. Any alternating group A_n is non-abelian and simple for all $n \geq 5$. See Chapter IV.6 of Dummit & Foote for the proof of this theorem. Note that A_4 is not simple since $n_2(A_4) = 1$. A_3 is simple and abelian.

We conclude the notes with an example where you can use Sylow theorems to prove that a group of certain order can never be a simple group.

Example. We shall prove that any group of order $6545 = 5 \cdot 7 \cdot 11 \cdot 17$ is not simple. By the third Sylow theorem, $n_p \equiv 1 \pmod{p}$, and $n_p \,|\, p_1p_2p_3$ where p_i is the remaining three prime factors of 6545 except for p, so

$$n_5 \in \{1, 11\}, n_7 \in \{1, 85\}, n_{11} \in \{1, 595\}, n_{17} \in \{1, 35\}.$$

If this group *were* simple, we would have $n_5 = 11, n_7 = 85, n_{11} = 595, n_{17} = 35$. By the second Sylow theorem, any two Sylow p-subgroups of the same p is conjugate of each other, so there are at least $(5-1) \cdot 11 = 44$ elements of order 5, $(7-1) \cdot 85 = 510$ elements of order 7, $(11-1)595 = 5950$ elements of order 11, and $(17-1)35 = 560$ elements of order 17. Thus this group has at least $44 + 510 + 5950 + 560 + 1$ elements, but this is already greater than 6545. Therefore at least one of n_5, n_7, n_{11}, n_{17} must be 1. Therefore there is at least one non-trivial normal subgroup, so this group cannot be simple.

Example. If G is a group of order 60 that has more than one Sylow 5-subgroup, then G is simple. For the sake of contradiction, suppose that $n_5 > 1$ and $\#G = 60$, but that G is not simple. Since $n_5 \equiv 1 \pmod{5}$ and $n_5 \,|\, 12$, n_5 can only be 1 or 6. But since $n_5 > 1$, there are six Sylow 5-subgroups. If $P \in \mathrm{Syl}_5(G)$, then $\#N_G(P) = 10$ since $n_5 = |G : N_G(P)| = 6$.

Suppose that H is a nontrivial normal subgroup of G. If $\#H$ is a multiple of 5, then H must contain a Sylow 5-subgroup of G. In fact, since H is normal, it must contain all six Sylow 5-subgroups. Therefore $\#H \geq 1 + 6 \cdot 4 = 25$, so this forces $\#H = 30$. Therefore $\#H$ has a normal subgroup isomorphic to $\mathbb{Z}/15\mathbb{Z}$ (see p143 of Section IV.5), which is a contradiction.

If $\#H = 6$ or 12, then H has a normal Sylow subgroup, which is also normal in G. If needed, replaced H by this normal Sylow subgroup. Therefore we may assume that $\#H = 2, 3$, or 4. If $\overline{G} = G/H$, then $\#\overline{G} = 30, 20$, or 15. In any of those cases, $\overline{G}$ has a normal subgroup $\overline{P} = P/H$ of order 5. So if H_1 is the complete pre-image of $\overline{P}$ in G, then not only is H_1 a proper normal subgroup of G, but $5 \,|\, \#H_1$. However we just proved that no non-trivial normal subgroup of G can have order divisible by 5. Thus G is simple as required. One corollary to this is that A_5 is simple, since both $\langle(12345)\rangle$ and $\langle(13245)\rangle$ are distinct Sylow 5-subgroups of A_5.

Department of Mathematics and Statistics, Dalhousie University, 6316 Coburg Rd, Halifax, NS, Canada B3H 4R2

E-mail address: hsyang@dal.ca