THEORY OF GROUPS

NOTES FOR THE SENIOR SEMINAR IN ALGEBRA
HAMILTON COLLEGE, FALL 2015.

1. Abstract groups

"Abstraction is real, probably more real than nature."
- Josef Albers

1.1. The definition.

Definition 1.1. Let G be a set with a binary operation $*$. The structure $\mathbb{G} = (G, *)$ is called a ***group*** if the following axioms hold:

(1) for all $x, y, z \in G$, we have $(x * y) * z = x * (y * z)$,
(2) there exists an element $e \in G$ such that for all $x \in G$, $x * e = x = e * x$, and
(3) for all $x \in G$, there exists a w such that $x * w = e = w * x$.

We often write xy in place of $x * y$.

Theorem 1.2. *Let G be a group. If $e_1, e_2 \in G$ and for all $x \in G$, $xe_1 = x = e_1x$ and $xe_2 = x = e_2x$, then $e_1 = e_2$. In other words, G has a unique "identity" element.*

Notation 1.3. The previous theorem states that every group has a *unique* element e satisfying axiom (2) from Definition 1.1. This element will be called the ***identity*** or ***trivial*** element of the group. For groups whose binary operation is denote by $*$ or $\cdot$, the default symbol for the identity (in these notes) will be 1. However, if the binary operation is denote by $+$, the default symbol for the identity will be 0.

Theorem 1.4. *Let G be a group, and let $x \in G$. If $w_1, w_2 \in G$ with $xw_1 = 1 = w_1x$ and $xw_2 = 1 = w_2x$, then $w_1 = w_2$. In other words, every element of G has a unique "inverse."*

Notation 1.5. Theorem 1.4 states that for every element x of a group there is a *unique* element w satisfying axiom (3) from Definition 1.1 This element will be called the ***inverse*** of x. For groups whose binary operation is denote by $*$ or $\cdot$, the default notation for the inverse of x will be x^{-1}; however, if the binary operation is denote by $+$, the inverse of x will be denoted by $-x$.

Problem 1.6. Give examples of groups with the following properties by *explicitly* defining the binary operation and noting the identity and inverses:

(1) a group with 4 elements,
(2) a group with 4 elements for which multiplication is *truly different* than the previous example, and
(3) an infinite group.

1.2. **Basic arithmetic.**

Notation 1.7. Let G be a group. If $g, h \in G$, then we call gh the ***product*** of g and h. Also, for $n \in \mathbb{N}$, g^n denotes the product of g with itself n-times, and g^{-n} denotes $\left(g^{-1}\right)^n$.

Theorem 1.8. *Let G be a group. If $g \in G$ and $m, n \in \mathbb{Z}$, then*

(1) $1^n = 1$,
(2) $g^{-n} = (g^n)^{-1}$,
(3) $g^m g^n = g^{m+n}$, *and*
(4) $(g^m)^n = g^{mn}$.

Theorem 1.9. *Let G be a group. If $g, h \in G$, then $(gh)^{-1} = h^{-1}g^{-1}$.*

1.3. **Orders of elements.**

Definition 1.10. Let G be a group, and let $g \in G$. If $g^n = 1$ for some positive $n \in \mathbb{N}$, then we define the ***order*** of g, denoted $|g|$, to be the smallest such n. Otherwise, we say that g has ***infinite order*** and write $|g| = \infty$. The ***order*** of G is defined to be the cardinality of G, denoted $|G|$.

Fact 1.11 (Division Algorithm)**.** Let n be an integer and m a positive integer. There are **unique** integers q (the quotient) and r (the remainder) for which $n = qm + r$ and $0 \leq r < m$.

Theorem 1.12. *Let G be a group and $n \in \mathbb{Z}$. If $g \in G$, then $g^n = 1$ if and only if $|g|$ divides n.*

Definition 1.13. Let G be a group. If $g, h \in G$, then we say that g and h ***commute*** if $gh = hg$. More generally, $g_1, \ldots, g_r \in G$ are said to ***commute*** if $g_i g_j = g_j g_i$ for all $1 \leq i, j \leq r$.

Theorem 1.14. *If $g_1, \ldots, g_r$ are commuting elements of a group, then $|g_1 \cdots g_r|$ must divide* $\operatorname{lcm}(|g_1|, \ldots, |g_r|)$.

Problem 1.15. Determine if the conclusion of the previous theorem can be improved to read "…then $|g_1 \cdots g_r| = \operatorname{lcm}(|g_1|, \ldots, |g_r|)$."

Definition 1.16. We call a group G ***abelian*** (or ***commutative***) if $gh = hg$ for all $g, h \in G$.

Theorem 1.17. *If every nontrivial element of a group has order* 2*, then the group is abelian.*

Problem 1.18. Do you think that there is something special about the number 2 that makes the previous theorem work? If so, what might it be. If not, state a more general theorem that you believe to be true.

2. Examples

"A good stock of examples, as large as possible, is indispensable for a thorough understanding of any concept, and when I want to learn something new, I make it my first job to build one."
- Paul Halmos

2.1. **Symmetric groups.**

Definition 2.1. Let X be a set. A ***permutation*** of X is a bijection from X to X. The ***identity permutation*** is the permutation $\mathrm{id}_X : X \to X$ defined by $\mathrm{id}_X(x) = x$ for all $x \in X$.

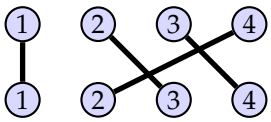
Definition 2.2. Let X be any set. The ***symmetric group*** on X, denoted $\mathrm{Sym}(X)$, is the set of all permutations of X. We denote by S_n the symmetric group on $X = \{1, 2, \ldots, n\}$.

Theorem 2.3. *If X is any set, then $\mathrm{Sym}(X)$ is a group with respect to function composition.*

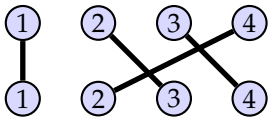
Notation 2.4 (cf. Notation 1.7)**.** If $a, b \in \mathrm{Sym}(X)$, then ab denotes the (function) composition $a \circ b$, i.e $ab(x) = a(b(x))$ for every $x \in X$.

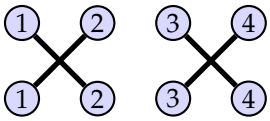
Problem 2.5 (Diagrammatic representation of S_n)**.**

(1) Which element of S_4 does the following diagram seem to represent?



(2) What is the diagram for the inverse of the previous element.
(3) Formulate a rule in this notation for finding the inverse of an element of S_4.
(4) What is the diagram for the identity.
(5) Consider $\sigma, \tau \in S_4$ whose diagrams are given below. Determine the diagrams for $\sigma\tau$ and $\tau\sigma$.

$\sigma =$ 

$\tau =$ 

(6) Formulate a rule in this notation for finding the composition of two elements.

Problem 2.6 (Two-line notion for S_n)**.**

(1) Which element of S_4 does the following two-line matrix seem to represent?

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

(2) What is the two-line notation for the inverse of the previous element.
(3) Formulate a rule in this notation for finding the inverse of an element of S_4.
(4) What is the two-line notation for the identity.
(5) Determine the two-line notations for σ and τ from Problem 2.5, and do the same for $\sigma\tau$ and $\tau\sigma$.
(6) Formulate a rule in this notation for finding the composition of two elements.

Problem 2.7 (Disjoint cycle notation for S_n)**.**

(1) Which element of S_4 does the following notation seem to represent?

$$(1)\,(3 \quad 4 \quad 2)$$

Note: in this notation, we will omit "cycles" of length 1 and simply write $(3 \quad 4 \quad 2)$.

(2) Using ***disjoint cycle notation***, how many different ways are there to represent the previous element?

(3) Write the inverse of the previous element in disjoint cycle notation.

(4) Formulate a rule in this notation for finding the inverse of an element of S_4.

(5) Determine disjoint cycle notation for σ and τ from Problem 2.5, and do the same for $\sigma\tau$ and $\tau\sigma$.

(6) Formulate a rule in this notation for finding the composition of two elements.

Fact 2.8. Every element of S_n can be written as a product of disjoint cycles.

Theorem 2.9. *If $n := |X|$ is finite, then* $|\mathrm{Sym}(X)| =$ *(in terms of n)*.

Definition 2.10. The list, in increasing order and with repetitions, of the lengths of the cycles in the disjoint cycle notation for an element of a symmetric group is called the ***cycle type*** of the element.

Remark 2.11. In Problem 2.7, σ has cycle type $(1, 3)$, and as we tend to omit cycles of length 1, we say that σ is a 3-cycle. The permutation τ has cycle type $(2, 2)$. The element $(3 \quad 4 \quad 2)(1 \quad 7)(6 \quad 8) \in S_{10}$ is a $(2, 2, 3)$-cycle; its cycle type is $(1, 1, 1, 2, 2, 3)$.

Problem 2.12.

(1) Find an element of S_4 of order 2.

(2) How many elements of S_4 have order 2? What are the possible cycle types of such an element?

(3) Find an element of S_4 of order 3.

(4) How many elements of S_4 have order 3? What are the possible cycle types of such an element?

(5) What are the possible cycle types for an element of S_4?

Problem 2.13. Let $\sigma \in S_n$ (with $n \in \mathbb{N}$), and fix a prime p.

(1) Suppose that the order of σ is p^k for some natural number k. Describe the possible cycle types for σ.

(2) Suppose that the cycle type of σ only involves powers of p, e.g. $(1, 1, p, p^2, p^2, p^4)$. Determine the order of σ.

(3) Suppose that the cycle type of σ is $(2, 3)$. Determine the order of σ.

Theorem 2.14. *The group S_n has* *(in terms of n)* *elements of order 2.*

Theorem 2.15. *If $\sigma \in S_n$ has cycle type $(m_1, \ldots, m_r)$, then $|\sigma| =$* *(in terms of $m_1, \ldots, m_r$)*.

Theorem 2.16. *If $\sigma \in S_n$, then $|\sigma|$ divides $|S_n|$.*

2.2. **Integers modulo n.**

Definition 2.17. Let n be a positive integer. For each $a \in \mathbb{Z}$ define the ***equivalence class of a modulo n*** to be $[a]_n := \{a + kn : k \in \mathbb{Z}\}$. Further, define $\mathbb{Z}_n := \{[a]_n : a \in \mathbb{Z}\}$.

Remark 2.18. In the previous definition, $[a]_n$ is a *set*, e.g. $[2]_7 = \{\ldots, -12, -5, 2, 9, 16, \ldots\}$. Also, note that $[a]_n = [b]_n$ if and only if $b \in [a]_n$. For example, $[2]_7 = [-12]_7$.

Fact 2.19. The following rules yield well-defined operations on $\mathbb{Z}_n$:

(1) $[a]_n +_n [b]_n := [a + b]_n$, and
(2) $[a]_n \cdot_n [b]_n := [ab]_n$.

When the context is clear, we simply use $+$ and $\cdot$ for the operations instead of $+_n$ and $\cdot_n$.

Theorem 2.20. *For every positive integer n, $(\mathbb{Z}_n, +)$ is a group.*

Definition 2.21. If G is a group and $g \in G$, we say that g ***generates*** G if every $h \in G$ is of the form $h = g^k$ for some $k \in \mathbb{Z}$. If G is generated by one of its elements, G is said to be ***cyclic***.

Theorem 2.22. *For every positive integer n, $(\mathbb{Z}_n, +)$ is cyclic.*

Problem 2.23. Make and provide evidence for (or prove) a conjecture as to which elements of $\mathbb{Z}_n$ can generate $\mathbb{Z}_n$. *[Hint: experiment! Try $\mathbb{Z}_5$, $\mathbb{Z}_6$, $\mathbb{Z}_{12}$, ...]*

Theorem 2.24. *The group $(\mathbb{Z}, +)$ is cyclic.*

Problem 2.25. Find all elements of $(\mathbb{Z}, +)$ that generate it.

Theorem 2.26. *Every cyclic group is abelian.*

2.3. **Linear groups.**

Definition 2.27. Let F be a field, and let $M_n(F)$ be the collection of $n \times n$ matrices with entries from F.

(1) The ***general linear group*** is $\mathrm{GL}_n(F) := \{A \in M_n(F) : \det A \neq 0\}$.
(2) The ***special linear group*** is $\mathrm{SL}_n(F) := \{A \in M_n(F) : \det A = 1\}$.

Theorem 2.28. *If F is a field, then $\mathrm{GL}_n(F)$ and $\mathrm{SL}_n(F)$ are both groups with respect to matrix multiplication.*

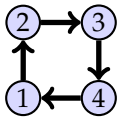
Theorem 2.29. *If F is a field and $n \geq 2$, then $\mathrm{GL}_n(F)$ is nonabelian.*

Theorem 2.30. *The group $\mathrm{SL}_2(\mathbb{R})$ has exactly one element of order 2.*

2.4. **Automorphism groups of graphs.**

Definition 2.31. A pair $\mathcal{G} = (V, E)$, where V is a set and $E \subseteq V \times V$, is called a ***directed graph*** (or ***digraph***). The elements of V are called ***vertices***, and the elements of E are called ***directed edges***.

Remark 2.32. Digraphs are usually represented by pictures. For example, consider the following picture depicting the digraph (which we will call C_4) defined by $C_4 = (V, E)$ where $V := \{1, 2, 3, 4\}$ and $E := \{(1, 2), (2, 3), (3, 4), (4, 1)\}$.



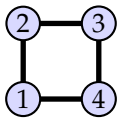
Definition 2.33. An ***automorphism of a digraph*** $\mathcal{G} = (V, E)$ is defined to be a permutation $\sigma \in \mathrm{Sym}(V)$ such that $(x, y) \in E$ if and only if $(\sigma(x), \sigma(y)) \in E$. The set of all automorphisms of $\mathcal{G}$ is denoted $\mathrm{Aut}(\mathcal{G})$.

Theorem 2.34. *If $\mathcal{G}$ is a digraph, then $\mathrm{Aut}(\mathcal{G})$ is a group.*

Problem 2.35. Consider the digraph C_4 defined in Remark 2.32.

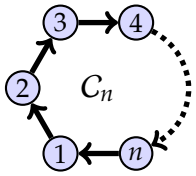
(1) Write down all elements of $\mathrm{Aut}(C_4)$ in disjoint cycle notation.
(2) Describe the various elements of $\mathrm{Aut}(C_4)$ geometrically, e.g. reflection, rotation, ...
(3) True or False (and explain): is $\mathrm{Aut}(C_4)$ cyclic?
(4) True or False (and explain): is $\mathrm{Aut}(C_4)$ is abelian?

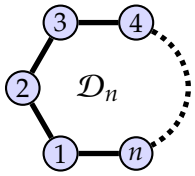
Problem 2.36. Repeat the previous problem for $\mathcal{D}_4 = (V, E)$ where $V := \{1, 2, 3, 4\}$ and $E := \{(1, 2), (2, 1), (2, 3), (3, 2), (3, 4), (4, 3), (4, 1), (1, 4)\}$. Whenever we have "both directions" of an edge, we draw it with no arrows (instead of two). Here is the picture for $\mathcal{D}_4$.



Remark 2.37. If E is symmetric (as Problem 2.36), then $\mathcal{G}$ is called a ***graph***, and we speak of ***edges*** instead of directed edges.

Definition 2.38. Generalizing the previous problems, we get the graphs $\mathcal{D}_n$ and C_n below.





(1) We denote $\mathrm{Aut}(C_n)$ by C_n.
(2) We denote $\mathrm{Aut}(\mathcal{D}_n)$ by D_n (or often D_{2n}); D_n is the ***dihedral group of order*** $2n$.

Problem 2.39. Repeat Problem 2.35 for the digraph $\mathcal{G} = (V, E)$ with $V := \{1, 2, 3, 4\}$ and $E := \{(1, 2), (2, 1), (2, 3), (3, 4), (4, 3), (1, 4)\}$.

3. Subgroups, cosets, quotients, and morphisms

"Divide each difficulty into as many parts as is feasible and necessary to resolve it."
- René Descartes

3.1. **Subgroups.**

Definition 3.1. A subset H of a group G is called a ***subgroup*** of G if for all $h_1, h_2 \in H$
(1) $h_1 h_2 \in H$,
(2) $h_1^{-1} \in H$, and
(3) $1_G \in H$.
We write $H \leq G$ to mean that H is a subgroup of G. A subgroup of G is ***proper***, denoted $H < G$, if it is not equal to G. A subgroup of G is ***nontrivial*** if it has more than 1 element.

Remark 3.2. We have seen several examples of subgroups already. For example, $\mathrm{SL}_n(F) < \mathrm{GL}_n(F)$, and $C_4 < D_4 < S_4$.

Problem 3.3. Find all subgroups of S_3. Illustrate how they are contained in each other.

Problem 3.4. Find all subgroups of $\mathbb{Z}_{12}$. Illustrate how they are contained in each other.

Problem 3.5. Find examples of each of the following in S_4:
(1) two different proper nontrivial cyclic subgroups,
(2) a proper noncyclic abelian subgroup, and
(3) two different proper nonabelian subgroups.

Theorem 3.6. *Let G be a group, and let $g \in G$. The set $\{g^k | k \in \mathbb{Z}\}$ is a subgroup of G consisting of exactly $|g|$ elements (interpreted in the obvious way when $|g| = \infty$).*

Definition 3.7. Let G be a group, and let $g \in G$. The set $\langle g \rangle := \{g^k | k \in \mathbb{Z}\}$ is called the ***(cyclic) subgroup generated by*** g.

Remark 3.8. Revisiting Definition 2.21, we see that a group G is cyclic if and only if $G = \langle g \rangle$ for some $g \in G$.

Theorem 3.9. *Every subgroup of a cyclic group is cyclic.*

Theorem 3.10. *Let G be a group. Prove that the intersection of any collection of subgroups of G is also subgroup.*

Definition 3.11. Let G be a group, and let $S \subseteq G$. The ***subgroup generated by*** S, denoted $\langle S \rangle$, is the intersection of all subgroups of G that contain S.

Remark 3.12. Note that every subgroup of G that contains S must also contain $\langle S \rangle$, so $\langle S \rangle$ is the smallest subgroup of G containing S. Also, when S consists of a single element, we now have two definitions for $\langle S \rangle$, see Definition 2.21, but they do agree.

Problem 3.13. Show that D_4 is generated by two elements.

Definition 3.14. Let G be a group. Define the ***center*** of G, denoted $Z(G)$, to be the set $Z(G) := \{h \in G | \text{hg=gh for every } g \in G\}$, and for each $g \in G$, define the ***centralizer*** of g in G to be $C_G(g) := \{h \in G | hg = gh\}$.

Theorem 3.15. *Let G be a group, and let $g \in G$. Then $C_G(g)$ and $Z(G)$ are subgroups of G, and $C_G(g)$ contains both $\langle g \rangle$ and $Z(G)$.*

Problem 3.16. Let I be the $n \times n$ identity matrix. Define S to be the subset of $\mathrm{GL}_n(F)$ consisting of the diagonal matrices where every entry on the main diagonal is the same (and nonzero), i.e. $S := \{A \in \mathrm{GL}_n(F) | A = cI \text{ for some } c \in F\}$. Show that S is subgroup and that $S \leq Z(\mathrm{GL}_n(F))$. Is there any chance that $S = Z(\mathrm{GL}_n(F))$?

Definition 3.17. The ***direct product*** of groups $(G, *_G)$ and $(H, *_H)$ is $(G \times H, *)$ where $G \times H := \{(g, h) | g \in G \text{ and } h \in H\}$ and $(g_1, h_1) * (g_2, h_2) := (g_1 *_G g_2, h_1 *_H h_2)$.

Theorem 3.18. *If G and H are groups, then $G \times H$ is a group.*

Problem 3.19. If G and H are groups, show that $\{(g, 1_H) | g \in G\}$ and $\{(1_G, h) | h \in H\}$ are subgroups of $G \times H$.

3.2. **Cosets and normal subgroups.**

Definition 3.20. Let G be a group and H a subgroup. For every $g \in G$, the set $gH := \{gh | h \in H\}$ is called a ***left coset*** of H in G, and $Hg := \{hg | h \in H\}$ is called a ***right coset*** of H in G. The collection of all left cosets of H in G will be denoted G/H; where as, $H\backslash G$ denotes the collection of all right cosets of H in G.

Problem 3.21. Consider the subgroups $H := \langle (12) \rangle$ and $N := \langle (123) \rangle$ of S_3.

(1) Determine S_3/H and $H\backslash S_3$. Is $S_3/H = H\backslash S_3$? Is $|S_3/H| = |H\backslash S_3|$?
(2) Determine S_3/N and $N\backslash S_3$. Is $S_3/N = N\backslash S_3$? Is $|S_3/N| = |N\backslash S_3|$?

Definition 3.22. A subgroup N of a group G is said to be ***normal*** if $gN = Ng$ for all $g \in G$.

Theorem 3.23. *A subgroup N of a group G is normal if and only if $gng^{-1} \in N$ for all $n \in N$ and all $g \in G$.*

Theorem 3.24. *Every subgroup of an abelian group is normal.*

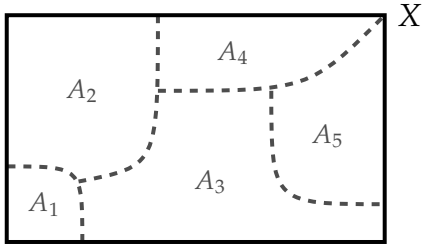
Problem 3.25. If $n \geq 1$, then $n\mathbb{Z} := \{nm | m \in \mathbb{Z}\}$ is a *subgroup* of $\mathbb{Z}$. (You don't need to prove this.) Describe the left cosets (which are the same as the right cosets) of $n\mathbb{Z}$ in $\mathbb{Z}$.

Theorem 3.26. *Let G be a group, H a subgroup, and $g, g_1, g_2 \in G$. Then*

(1) $gH = (gh)H$ for every $h \in H$, and
(2) $g_1H = g_2H$ if and only if $g_2^{-1}g_1 \in H$.

Definition 3.27. A ***partition*** of a set X is a collection P of nonempty subsets of X such that every element of X is in *exactly one* element of P.

Remark 3.28. If $X = \{a, b, c, d, e, f\}$, then $\{\{a, c\}, \{e\}, \{b, d, f\}\}$ is a partition of X, but $\{\{a, c\}, \{e\}, \{b, f\}\}$ and $\{\{a, c, d\}, \{e\}, \{b, d, f\}\}$ are not. A partition $\{A_1, A_2, A_3, A_4, A_5\}$ of a set X can be visualized as follows.



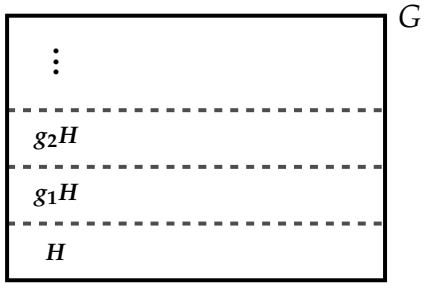
Theorem 3.29. *If H is a subgroup of G, then the set of left cosets G/H forms a partition of G.*

Remark 3.30. It is also true that the set of right cosets $H\backslash G$ forms a partition of G, though quite possibly a different one than G/H.

Fact 3.31. By definition, two sets A and B have the same cardinality ("size"), if there is a one-to-one and onto function, i.e. a bijection, from A to B.

Theorem 3.32 (Lagrange's Theorem)**.** *Let G be a group. If $H \leq G$ and A is any left or right coset of H, then $|A| = |H|$. Consequently, $|G| = |G/H| \cdot |H|$ when G is finite.*

Remark 3.33. Lagrange's Theorem tells us that the partition of a group G determined by the left cosets of a subgroup H looks as follows.



Additionally, it should be rather clear that $|G| = |H\backslash G| \cdot |H|$ and $|G/H| = |H\backslash G|$, even though it is often the case that $G/H \neq H\backslash G$.

Theorem 3.34. *The order of each element of a finite group divides the order of the group.*

Theorem 3.35. *Every group of prime order is cyclic.*

Definition 3.36. Let H a subgroup of a group G. Define the ***index*** of H in G, denoted $|G : H|$, to be $|G : H| := |G/H| = |H\backslash G|$.

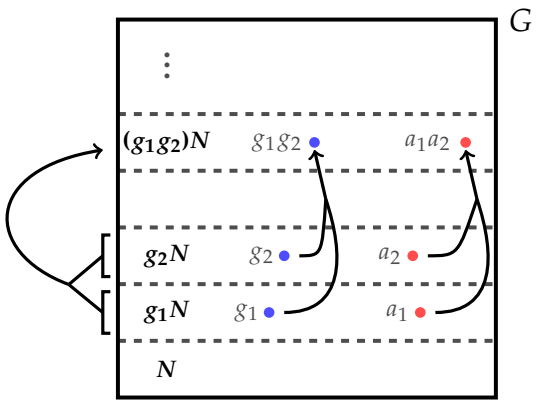
Theorem 3.37. *Every subgroup of index 2 in a group must be normal.*

3.3. **Quotient groups.**

Theorem 3.38. *Let N be a normal subgroup of G. If $g_1, g_2, a_1, a_2 \in G$ are such that $g_1N = a_1N$ and $g_2N = a_2N$, then*

(1) $(g_1g_2)N = (a_1a_2)N$, *and*
(2) $g_1^{-1}N = a_1^{-1}N$.

Remark 3.39. The previous theorem is saying that for all $a_1 \in g_1N$ and all $a_2 \in g_2N$ the product a_1a_2 always lies in the coset $(g_1g_2)N$ (see the picture below) and the inverse a_1^{-1} always lies in the coset $g_1^{-1}N$. Thus, when N is normal, this allows us to give the coset space G/N the structure of a group.



Definition 3.40 (Quotient groups)**.** Let N be a normal subgroup of G. Then the coset space G/N has the structure of a group where

(1) $(aN) \cdot (bN) = (ab)N$,
(2) $(aN)^{-1} = (a^{-1})N$, and
(3) $N = 1N$ is the identity.

Remark 3.41. If G is an group with normal subgroup N, then many properties of G transfer to the group G/N. For example, if G is abelian, then G/N is also abelian. Additionally, properties for N and G/N can sometimes be combined to deduce properties of G, but this is usually a bit more complicated.

Theorem 3.42. *If G is a cyclic group and N is a subgroup, then both N and G/N are cyclic.*

Problem 3.43. Find a group G with a normal subgroup N such that both N and G/N are cyclic but G is not even abelian.

Definition 3.44. A subgroup H of a group G is called ***central*** if $H \leq Z(G)$. Note that central subgroups are necessarily normal.

Theorem 3.45. *If N is a central subgroup of G and G/N is cyclic, then G is abelian.*

Definition 3.46. Let p be a prime. A group is a ***p-group*** if the order of every element is a power of p; that is, for every element g, there is some $k \in \mathbb{N}$ such that $|g| = p^k$.

Remark 3.47. Note that D_4 is a 2-group, and by Lagrange's Theorem, every group of prime-power order must be a p-group. Can you think of an infinite p-group?

Theorem 3.48. *Let p be a prime, and let N be a normal subgroup of G. If N and G/N are p-groups, then G is also a p-group.*

Remark 3.49. Let G be a finite group. We know, by Theorem 3.34, that the order of every element of G divides $|G|$. Now, suppose that some prime p divides $|G|$; does this imply that G has an element of order p? The next few theorems start to explore this question.

Theorem 3.50. *Let G be a finite cyclic group. If p is a prime dividing $|G|$, then G has an element of order p.*

Definition 3.51. Let $n \in \mathbb{N}$. A group G is said to be ***n-divisible*** if for every $g \in G$ there is some $x \in G$ such that $g = x^n$, i.e. the function $G \to G : x \mapsto x^n$ is surjective. In additive notation, the condition $g = x^n$ becomes $g = nx$, justifying the name n-divisible.

Theorem 3.52. *Let G be a finite abelian group, and let p be a prime. If G has no elements of order p, then G is p-divisible.*

Theorem 3.53. *Let G be a finite group and p be a prime. If N is a central subgroup of G and G/N has an element of order p, then G has an element of order p.* [Hint: either N has an element of order p or it does not. In the latter case, try to use the previous theorem.]

Theorem 3.54. *Let G be a finite abelian group. If p is a prime dividing $|G|$, then G has an element of order p.* [Hint: this theorem is hard. Solving it will bring much honor and glory! Towards a contradiction, assume that the theorem is false. Consider using the following technique of exploring a "minimal counterexample." Let $\mathcal{A}$ be the set of all counterexamples to the theorem. By the Well-ordering Principle, $\mathcal{A}$ contains a group G for which $|G|$ is minimal, i.e. G is a counterexample to the theorem, but every group of smaller order than G satisfies the theorem. Now, to find a contradiction, show that G must have a proper nontrivial subgroup N, and then study N and G/N.]

Remark 3.55. The previous three theorems raise many questions. Is it true that *every* finite group without elements of order p is p-divisible? What about infinite groups? Is it necessary that N be central in the statement of Theorem 3.53? If p is a prime dividing the order of an *arbitrary* finite group, must the group have an element of order p?

Problem 3.56. Generalize Theorem 3.54 in some way.

3.4. **Morphisms.**

Definition 3.57. Let G and H be groups. A function $\varphi : G \to H$ is called a ***homomorphism*** if $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$ for all $g_1, g_2 \in G$. A *bijective* homomorphism from G to H is called an ***isomorphism***, and in this case, G and H are said to be ***isomorphic***, denoted $G \cong H$. An isomorphism from G to G is called an ***automorphism*** of G.

Remark 3.58. In the equation $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$, the product g_1g_2 is computed according to the definition of multiplication **in G**; where as, the product $\varphi(g_1)\varphi(g_2)$ is computed according to the definition of multiplication **in H**.

Theorem 3.59. *If $\varphi : G \to H$ is a homomorphism of groups, then for all $g \in G$, $\varphi(g^{-1}) = \varphi(g)^{-1}$ and $\varphi(1_G) = 1_H$.*

Theorem 3.60. *A group G is abelian if and only if the inversion map $G \to G : x \mapsto x^{-1}$ is an automorphism.*

Remark 3.61. Recall that any bijection f from a set X to a set Y has an inverse defined by $f^{-1} \circ f = \mathrm{id}_X$ and $f \circ f^{-1} = \mathrm{id}_Y$.

Theorem 3.62. *The inverse of an isomorphism between two groups is also an isomorphism.*

Remark 3.63. A homomorphism from G to H translates the group operations of G to those of H, and this transfers various properties of G to H. This is especially true when $G \cong H$ as, in this case, G and H are for all intents and purposes the same group, except that the elements have different names.

Theorem 3.64. *Let $\varphi : G \to H$ be a* surjective *homomorphism of groups.*

(1) If G is cyclic, then H is cyclic.
(2) If G is abelian, then H is abelian.

Remark 3.65. If $\varphi : G \to H$ is an isomorphism of groups, the previous two theorems can be combined to see that G is cyclic if and only if H is cyclic and that G is abelian if and only if H is abelian.

Theorem 3.66. *Let $\varphi : G \to H$ be a homomorphism of groups. If $g \in G$ has finite order, then $|\varphi(g)|$ divides $|g|$, and if, additionally, φ is injective, then $|\varphi(g)| = |g|$.*

Theorem 3.67. *Every two infinite cyclic groups are isomorphic, and two finite cyclic groups are isomorphic if and only if they have the same cardinality.*

Problem 3.68. Show that $\mathbb{Z}$ contains (many) *proper* subgroups that are isomorphic $\mathbb{Z}$.

Definition 3.69. The ***quaternion group*** is the *group* $Q_8 := \left\{\{\pm 1, \pm i, \pm j, \pm k\}, \cdot, ^{-1}, 1\right\}$ where

- $(-1)(-1) = 1$,
- $g(-1) = (-1)g = -g$ for all $g \in Q_8$,
- $i^2 = j^2 = k^2 = -1$, and
- $ij = k$.

Note that these axioms imply that 1 is the identity and that $g^{-1} = -g$ for all $g \in Q_8 - \{\pm 1\}$.

Problem 3.70. Show that Q_8 is a nonabelian group of order 8 that is *not* isomorphic to D_4.

Notation 3.71. There are two groups attached to every field F: the elements of F under addition, denoted F^+, and the *nonzero* elements of F under multiplication, denoted $F^\times$.

Problem 3.72. Show that $\mathbb{R}^+ \ncong \mathbb{R}^\times$. However, if H is the *subgroup* of $\mathbb{R}^\times$ consisting of the *positive* real numbers, show that $\mathbb{R}^+ \cong H$.

Problem 3.73. Let F be any field. Find two subgroups of $\mathrm{GL}_2(F)$ isomorphic to F^+ and $F^\times$. *[Hint: you can restrict your attention to upper triangular matrices.]*

Definition 3.74. Let G and H be groups, and let $\varphi : G \to H$ be a homomorphism. Define the ***kernel*** of φ to be $\ker\varphi := \{g \in G | \varphi(g) = 1\}$. For any subset $A \subseteq G$, define the ***image of*** A to be $\varphi(A) := \{h \in H | h = \varphi(a) \text{ for some } a \in A\}$.

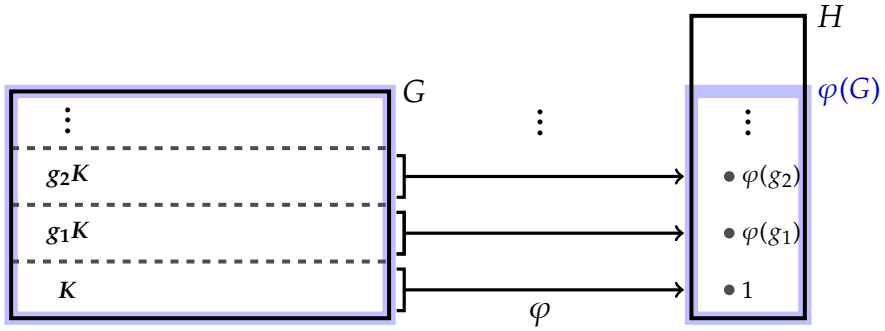
Theorem 3.75. *If $\varphi : G \to H$ is a homomorphism of groups, then the kernel of φ is a* ***normal*** *subgroup of G, and the image of any* subgroup *of G is a subgroup of H.*

Remark 3.76. The previous theorem states that kernels of homomorphisms are normal subgroups, but the converse is also true: every normal subgroup is the kernel of some homomorphism. Indeed, if $N \trianglelefteq G$, then the map $\varphi : G \to G/N : g \mapsto gN$ is a (surjective) homomorphism with kernel equal to N.

Theorem 3.77. *A homomorphism of groups is injective if and only if the kernel is trivial.*

Theorem 3.78 (First Isomorphism Theorem)**.** *If $\varphi : G \to H$ is a surjective homomorphism of groups, then $G/\ker\varphi \cong H$.* [Hint: Use φ to define a related function from $G/\ker\varphi$ to H.]

Remark 3.79. If $\varphi : G \to H$ is a homomorphism of groups, then $\varphi : G \to \varphi(G)$ is a *surjective* homomorphism, so $G/\ker\varphi \cong \varphi(G)$. In words, "$G$ modulo the kernel is isomorphic to the image." Setting $K := \ker\varphi$, the picture is roughly as follows.



Problem 3.80. Let F be any field. Show that $\mathrm{SL}_n(F)$ is normal in $\mathrm{GL}_n(F)$ by showing that $\mathrm{SL}_n(F)$ is the kernel of a homomorphism from $\mathrm{GL}_n(F)$ to another group. Use this homomorphism to describe the quotient group $\mathrm{GL}_n(F)/\mathrm{SL}_n(F)$.

4. Group actions

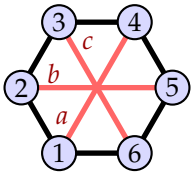
"Groups, as men, will be known by their actions."
- Guillermo Moreno

4.1. **The definition.**

Definition 4.1. An ***action*** of a group G on a set X is a function from $\alpha : G \times X \to X$ such that the following hold for all $g, h \in G$ and all $x \in X$; we write $g \cdot x$ in place of $\alpha(g, x)$.

(1) $g \cdot (h \cdot x) = (gh) \cdot x$, and
(2) $1 \cdot x = x$.

Problem 4.2. Recall that D_6 is the automorphism group of the regular hexagon $\mathcal{D}_6$. Let V be the set of vertices of $\mathcal{D}_6$, let E the set of edges of $\mathcal{D}_6$, and let $X = \{a, b, c\}$ be the set of (three) diagonal edges shown below.

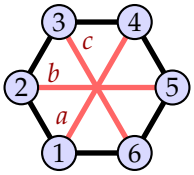


(1) Show that D_6 acts on V via the rule $\sigma \cdot v = \sigma(v)$ for all $\sigma \in D_6$ and all $v \in V$.
(2) Show that D_6 acts on E via the rule $\sigma \cdot (v_1, v_2) = (\sigma(v_1), \sigma(v_1))$ for all $\sigma \in D_6$ and all $(v_1, v_2) \in E$.
(3) Show that D_6 acts on X via the rule $\sigma \cdot (v_1, v_2) = (\sigma(v_1), \sigma(v_1))$ for all $\sigma \in D_6$ and all $(v_1, v_2) \in X$.

Definition 4.3. Let G act on X.

(1) The action is ***transitive*** if for every $x, y \in X$ there is a $g \in G$ such that $g \cdot x = y$.
(2) For $g \in G$ and $x \in X$, we say that g ***fixes*** x if $g \cdot x = x$.
(3) For $x \in X$, the ***stabilizer of*** x, denoted G_x, is set of all $g \in G$ that fix x.

Problem 4.4. Let $G = D_6$, and consider the action of G on $X = \{a, b, c\}$ defined by the rule $\sigma \cdot (v_1, v_2) = (\sigma(v_1), \sigma(v_1))$.



(1) Is the action transitive?
(2) Determine the G_a.
(3) Find a numerical relationship between $|G|$, $|X|$, and $|G_a|$.
(4) Determine $G_{a,b}$ where $G_{a,b}$ is the set of elements of G that fix both a and b.
(5) Are there elements of G that fix *every* element of X? If so, find them all.

Theorem 4.5. *An action of a group G on X is transitive if there exists some $x \in X$ such that for all $y \in X$ there is a $g \in G$ for which $g \cdot x = y$.*

Definition 4.6. Let G act on X.

(1) The ***kernel*** of the action is the subset of G that fixes every $x \in X$.
(2) The action is said to be ***faithful*** if the kernel is trivial.

Theorem 4.7. *If G acts on X and $x \in X$, then G_x is a subgroup of G, and the kernel of the action is a normal subgroup.*

Theorem 4.8. *Let G act on X. For every $g \in G$, define $\sigma_g : X \to X$ by $\sigma_g(x) = g \cdot x$. Then σ_g is a bijection, i.e. $\sigma_g \in \mathrm{Sym}(X)$.* [Hint: make use of the fact that g has an inverse.]

Theorem 4.9. *Let G act on X, and define $\sigma : G \to \mathrm{Sym}(X)$ by $\sigma(g) = \sigma_g$ where σ_g is defined as in the previous theorem. Then σ is a homomorphism.* [Hint: in order to show that $\sigma_{gh} = \sigma_g \circ \sigma_h$, show that $\sigma_{gh}(x) = \sigma_g(\sigma_h(x))$ for all $x \in X$.]

Definition 4.10. In the previous theorem, the function $\sigma : G \to \mathrm{Sym}(X)$ is called the ***associated permutation representation*** of the action of G on X.

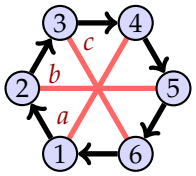
Remark 4.11. Observe that the kernel of an action corresponds with the kernel of the associated permutation representation, so an action is faithful if and only if the associated permutation representation is injective.

Problem 4.12. As in Problem 4.4, consider the action of D_6 the 3 diagonals of $\mathcal{D}_6$.

(1) What is the kernel of the action? Is the action faithful?
(2) What is the image of the associated permutation representation?

Note: the kernel is a subgroup of D_6; the image of the representation is a subgroup of $\mathrm{Sym}(a, b, c)$.

Problem 4.13. Let $G = C_6$. As with D_6, we have an action of G on $X = \{a, b, c\}$ defined by $\sigma \cdot (v_1, v_2) = (\sigma(v_1), \sigma(v_1))$.



(1) Is the action transitive?
(2) Determine the G_a.
(3) Find a numerical relationship between $|G|$, $|X|$, and $|G_a|$.
(4) What is the kernel of the action. Is the action faithful?
(5) What is the image of the associated permutation representation?

4.2. **Action by left multiplication.**

Theorem 4.14 (Action by left multiplication)**.** *Let G be a group, and let H be a subgroup. Then the rule $g \cdot aH = (ga)H$ defines an action of G on the coset space G/H.*

Problem 4.15. Let G be a group, and let H be a subgroup. Consider the action of G on G/H by left multiplication (as in the previous theorem).

(1) Is the action transitive?
(2) Show that the stabilizer of the coset aH is aHa^{-1}.
(3) Show that the kernel of the action is $\bigcap_{a\in G} aHa^{-1}$. (Note that, in particular, this shows that the kernel is a normal subgroup of G contained in H.)
(4) Give an example of a group G and a proper nontrivial subgroup H for which this action is **not** faithful.

Definition 4.16. A group is ***simple*** if it has *no* proper nontrivial normal subgroups.

Remark 4.17. Whenever a group G has a proper nontrivial normal subgroup N, we can break G into two "simpler" pieces: N and G/N. The simple groups are the groups that can not be broken down this way; they may be thought of as the building blocks of all groups.

Theorem 4.18. *If G is an infinite group with a proper subgroup H of finite index, then G is **not** simple.* [Hint: argue by contradiction, and consider the action of G on G/H by left multiplication. This gives rise to the associated representation $\sigma : G \to \mathrm{Sym}(G/H)$. Now, if G is simple, what do you know about the kernel of the action? What does the First Isomorphism Theorem, i.e. Theorem 3.78 and Remark 3.79, tell you?]

Theorem 4.19. *Let G be a finite group with a proper subgroup H, and let $n = |G : H|$. If $|G|$ does not divide $n!$, then G is **not** simple.* [Hint: same hint as the previous problem.]

4.3. **Action by conjugation.**

Notation 4.20. Let G be a group. For $g \in G$, the function $\gamma_g : G \to G$ defined by $\gamma_g(h) = ghg^{-1}$ is called ***conjugation by*** g.

Theorem 4.21. *If G is a group and $g \in G$, then γ_g is an automorphism of G. In particular,*
(1) if $h \in G$, then $|h| = |ghg^{-1}|$, and
(2) if H is a subgroup of G, then gHg^{-1} is a subgroup of G with $H \cong gHg^{-1}$.

Theorem 4.22. *Let $\sigma, \tau \in S_n$. If the disjoint cycle decomposition of σ is*

$$\begin{pmatrix} a_1 & a_2 & \cdots & a_{k_1} \end{pmatrix} \begin{pmatrix} b_1 & b_2 & \cdots & b_{k_2} \end{pmatrix} \cdots,$$

then the disjoint cycle decomposition of $\tau\sigma\tau^{-1}$ is

$$\begin{pmatrix} \tau(a_1) & \tau(a_2) & \cdots & \tau(a_{k_1}) \end{pmatrix} \begin{pmatrix} \tau(b_1) & \tau(b_2) & \cdots & \tau(b_{k_2}) \end{pmatrix} \cdots.$$

In particular, σ and $\tau\sigma\tau^{-1}$ have the same cycle type. [Hint: let $\psi = \tau\sigma\tau^{-1}$, and note that the theorem simply states that for all $x, y \in \{1, \ldots, n\}$ if $\sigma(x) = y$, then $\psi(\tau(x)) = \tau(y)$.]

Theorem 4.23 (Action by conjugation)**.** *Let G be a group. Then*
(1) the rule $g \cdot a = gag^{-1}$ defines an action of G on G, and
(2) the rule $g \cdot H = gHg^{-1}$ defines an action of G on the set of all subgroups of G.

Definition 4.24. Let H be a subgroup of a group G. The set $N_G(H) := \{g \in G |\ gHg^{-1} = H\}$ is called the ***normalizer*** of H in G.

Remark 4.25. Note that we have some overlapping terminology. When G acts on itself by conjugation (as in the first part of the previous theorem), the stabilizer of an element a of G is $C_G(a)$. When G acts on its subgroups by conjugation (as in the second part of the previous theorem), the stabilizer of a subgroup H is $N_G(H)$.

Theorem 4.26. *If H is a subgroup of a group G, then H is a normal subgroup of $N_G(H)$.*

Definition 4.27. If A and B are subsets of a group G, we define $AB := \{ab | a \in A, b \in B\}$.

Theorem 4.28. *If H is a subgroup of a group G and K is a subgroup of $N_G(H)$, then KH is a subgroup of $N_G(H)$.*

Definition 4.29. Let G be a group acting on a set X. If $x \in X$, then the subset of X defined by $Gx := \{g \cdot x | g \in G\}$ is called the ***orbit of x under G***.

Theorem 4.30. *If G is a group acting on a set X, then the set of orbits forms a partition of X.*

Definition 4.31. When G acts on itself (or on its subgroups) by conjugation, the orbits are called ***conjugacy classes*** (or ***conjugacy classes of subgroups***) and two elements in the same conjugacy class are said to be ***conjugate***.

Problem 4.32. Determine the conjugacy classes of S_3. Determine the conjugacy classes of subgroups of S_3.

Theorem 4.33. *Two elements of S_n are conjugate if and only if they have the same cycle type.*

Theorem 4.34. *If $n \geq 3$, then $Z(S_n) = \{1\}$.*

Problem 4.35. Determine the conjugacy classes of D_4.

4.4. **The Orbit-stabilizer Theorem.**

Remark 4.36. Suppose that G acts on X. Observe that, for any orbit $\mathcal{O}$, the action of G on X restricts to an action of G on $\mathcal{O}$, and this latter action is now transitive. In this way, many questions about group actions can be reduced to questions about transitive group actions.

Theorem 4.37 (Orbit-stabilizer Theorem)**.** *Let G be a group acting on a set X. Then for every $x \in X$, $|Gx| = |G : G_x|$.* [Hint: construct a bijection from G/G_x to Gx.]

Notation 4.38. For a group G acting on a set X, we define $\mathrm{Fix}(G)$ to be the set of all $x \in X$ such that x fixed by *every* element of G, i.e. $\mathrm{Fix}(G)$ is the set of fixed points of G. The elements of $\mathrm{Fix}(G)$ represent the orbits of G of size 1.

Theorem 4.39. *Let G be a finite group acting on a finite set X. Let $\mathcal{O}_1, \ldots, \mathcal{O}_n$ be the orbits of G not contained in* $\mathrm{Fix}(G)$*, if any, and let $x_1, \ldots x_n \in X$ be such that $x_i \in \mathcal{O}_i$. Then*

$$|X| = |\mathrm{Fix}(G)| + \sum_{i=1}^{n} |G : G_{x_i}|.$$

[Hint: recall that the orbits of G partition X.]

Theorem 4.40. *Let P be a group of order p^k for some prime p. If P acts on a finite set X, then $|\mathrm{Fix}(P)| \equiv |X|$ modulo p.*

Theorem 4.41. *If P is a group of order p^k for some prime p, then $Z(P)$ is nontrivial.* [Hint: let P act on itself by conjugation. What is $\mathrm{Fix}(P)$ with respect to this action?]

Theorem 4.42. *If P is group of order p^2 for some prime p, then P is abelian.*

Problem 4.43 (The Class Equation)**.** Let G be a finite group. Let $C_1, \ldots, C_n$ be the conjugacy classes of G not contained in $Z(G)$, if any, and let $x_1, \ldots x_n \in G$ be such that $x_i \in C_i$. Explain how Theorem 4.39 can be used to quickly deduce that

$$|G| = |Z(G)| + \sum_{i=1}^{n} |G : C_G(x_i)|.$$

Theorem 4.44. *Let G be a finite group. If p is a prime dividing $|G|$, then p divides $|C_G(g)|$ for some nontrivial $g \in G$.* [Hint: class equation.]

Theorem 4.45 (Cauchy's Theorem)**.** *Let G be a finite group. If p is a prime dividing $|G|$, then G has an element of order p.* [Hint: consider a minimal counterexample, and first show that it must have a nontrivial center.]

Theorem 4.46. *Let p be a prime. If G is a finite group, then G is a p-group (see Definition 3.46) if an only if $|G| = p^k$ for some $k \in \mathbb{N}$.*

Problem 4.47. We should always be asking if we can generalize things. Make at least two conjectures related to generalizing (or not being able to generalize) Cauchy's Theorem.

5. Sylow's Theorem

"For a group theorist, Sylow's Theorem is such a basic tool, and so fundamental, that it is used almost without thinking, like breathing."
- Geoff Robinson

5.1. **The definition.**

Definition 5.1. Let p be a prime. A subgroup P of G is called a ***Sylow p-subgroup*** if P is a p-group and P is not properly contained in another p-subgroup of G, i.e. P is a maximal p-subgroup of G. Let $\mathrm{Syl}_p(G)$ be the set of Sylow p-subgroups of G.

Remark 5.2. If G is a finite group of order $p^k m$ with p prime and p not dividing m, then a Sylow p-subgroup of G has order at most p^k, by Theorem 4.46.

Problem 5.3. Find a Sylow 5-subgroup of S_5.

Problem 5.4. Find a Sylow 2-subgroup of S_4. *[Hint: the maximum possible cardinality is* 8*. Do you know of a group with* 8 *elements that acts on a set of size* 4*?]*

5.2. **Sylow's Theorem.**

Theorem 5.5. *Let p be a prime. If $P \in \mathrm{Syl}_p(G)$, then $gPg^{-1} \in \mathrm{Syl}_p(G)$ for all $g \in G$, so G acts on $\mathrm{Syl}_p(G)$ by conjugation.*

Theorem 5.6. *Let p be a prime. If P is a p-subgroup of a group G and Q is a p-subgroup of $N_G(P)$, then QP is a p-subgroup of $N_G(P)$.* [Hint: first show that QP/P is a p-group.]

Theorem 5.7. *Let p be a prime, and let P be a Sylow p-subgroup of a group G. If P is normal in G, then P is the only Sylow p-subgroup of G, and consequently, P is always the unique Sylow p-subgroup of $N_G(P)$.*

Theorem 5.8 (Sylow's Theorem - part 1)**.** *If G is a finite group and p is a prime dividing $|G|$, then any two Sylow p-subgroups of G are conjugate, and further, $|\mathrm{Syl}_p(G)| \equiv 1$ modulo p.*
[Hint: let $\mathcal{O}$ be an orbit of G acting on $\mathrm{Syl}_p(G)$ by conjugation. The goal is to show $\mathcal{O} = \mathrm{Syl}_p(G)$ and $|\mathcal{O}| \equiv 1 \bmod p$. Choose $P \in \mathcal{O}$, and towards a contradiction, assume that $Q \in \mathrm{Syl}_p(G)$ with $Q \notin \mathcal{O}$. Now, the key is to consider how P and Q act on $\mathcal{O}$ (by conjugation).

(1) Show that the only subgroup in $\mathcal{O}$ that P fixes, i.e. normalizes, is P itself. Conclude that $|\mathcal{O}| \equiv 1$ modulo p.
(2) Show that Q fixes nothing in $\mathcal{O}$. Conclude from this that $|\mathcal{O}| \equiv 0$ modulo p.

The previous theorem and Theorem 4.40 are very relevant.]

Theorem 5.9 (Sylow's Theorem - part 2)**.** *If G is a finite group and $|G| = mp^k$ with p prime and p not dividing m, then $|P| = p^k$ for every $P \in \mathrm{Syl}_p(G)$.*
[Hint: use part 1 of Sylow's Theorem and the Orbit-Stabilizer Theorem to show $|N_G(P)| =$

$m'p^k$ for some m'. Now, towards a contradiction, assume that $|P| = p^\ell$ with $\ell < k$, and consider the quotient group $N_G(P)/P$. Show that $N_G(P)/P$ must have an element of order p and use this find a contradiction.]

5.3. **Applications of Sylow's Theorem.**

Remark 5.10. Since all Sylow p-subgroups of a finite group are conjugate, a finite group has a normal Sylow p-subgroup if and only if it has a unique one. Thus, the condition "$|\mathrm{Syl}_p(G)| \equiv 1$ modulo p" can be helpful in determining if a group has a normal Sylow subgroup or not. And one should always remember that $|\mathrm{Syl}_p(G)| = |G : N_G(P)|$ by the Orbit-Stabilizer Theorem, so in particular, $|\mathrm{Syl}_p(G)|$ is always coprime to p.

Theorem 5.11. *If G is a group of order mp^k with p prime and $m < p$, then G has a normal Sylow p-subgroup.*

Theorem 5.12. *If G is a group of order pqr where p, q, and r are prime with $p < q < r$, then some Sylow subgroup of G is normal.* [Hint: the following counting technique often works well when the largest prime divisors of $|G|$ only occur to the first power (make sure you see when you use this). The rough idea is that if no Sylow subgroup of G is normal, then G will have too many Sylow subgroups and, in turn, too many elements. Assume the theorem is false. First count the number of Sylow r-subgroups, and use this to count the number of elements of G of order r. Now estimate (it will be hard to precisely count) the number of Sylow q-subgroups, and use this to estimate the number of elements of G of order q. Finally, compare the sum of these with the order of G.]

The End