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) $h_1^{-1} H$, 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 $Z(G) := \{h \in G | \text{hg=gh} \text{ for every } g \in G\}$, 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.*

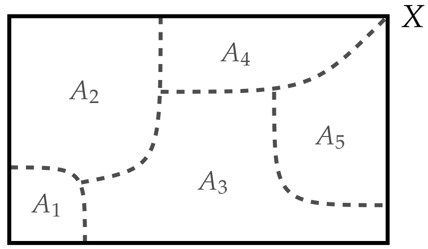
Problem 3.25. If $n \geq 1$, then $n\mathbb{Z} := \{nm | m \in \mathbb{Z}\}$ is a *subgroup* of $\mathbb{Z}$. (You don't need to prove this.) Describe the left cosets (which are the same as the right cosets) of $n\mathbb{Z}$ in $\mathbb{Z}$.

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.



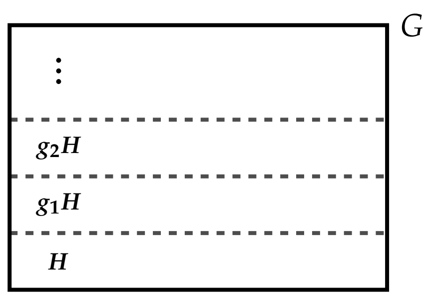
Theorem 3.29. *If H is a subgroup of G, then the set of left cosets G/H forms a partition of G.*

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 $|G : H| := |G/H| = |H\backslash G|$.

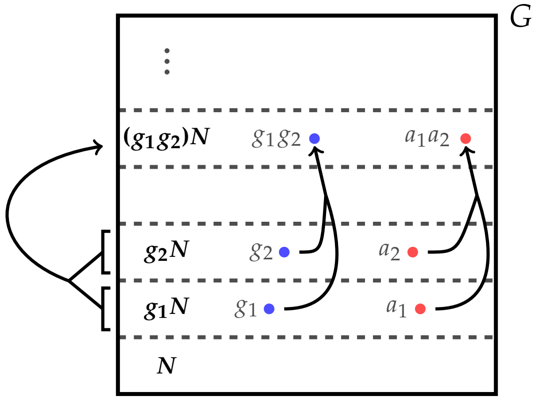
Theorem 3.37. *Every subgroup of index 2 in a group must be normal.*

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 $\mathbb{R}^+ \not\cong \mathbb{R}^\times$. 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 $\varphi(A) := \{h \in H | h = \varphi(a) \text{ for some } a \in A\}$.

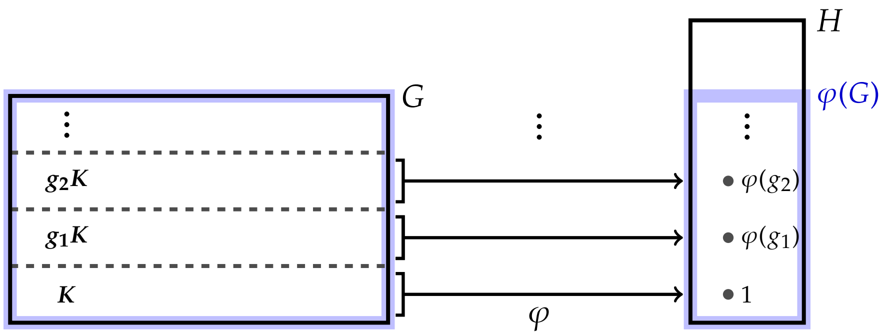
Theorem 3.75. *If $\varphi : G \to H$ is a homomorphism of groups, then the kernel of φ is a **normal** subgroup of G, and the image of any* subgroup *of G is a subgroup of H.*

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 $\mathrm{GL}_n(F)/\mathrm{SL}_n(F)$.