2. Abstract groups

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

2.1. **The definition.**

Definition 2.1. Let G be a set equipped with functions $m : G \times G \to G$ and $\iota : G \to G$ as well as a distinguished element 1. The structure $\mathbb{G} = (G, m, \iota, 1)$ is called a ***group*** if the following hold for all $x, y, z \in G$; we write xy in place of $m(x, y)$ and x^{-1} in place of $\iota(x)$.

(1) $(xy)z = x(yz)$
(2) $xx^{-1} = x^{-1}x = 1$
(3) $x1 = 1x = x$

We call x^{-1} the ***inverse*** of x and 1 the ***identity*** or ***trivial*** element of $\mathbb{G}$. We often simply write G in place of $\mathbb{G}$.

Problem 2.2. Give examples of groups with the following properties by **explicitly** defining m, ι, and 1:

(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

Theorem 2.3. *Let G be a group. If $g, h \in G$, then $(gh)^{-1} = h^{-1}g^{-1}$.*

Notation 2.4. 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 $\left(g^{-1}\right)^n$.

Fact 2.5 (cf. Theorem 1.4)**.** Let G be a group. If $g \in G$ and $m, n \in \mathbb{Z}$, then

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

Definition 2.6. 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.

Fact 2.7 (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 $0 \le r < m$.

Theorem★ 2.8. *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 2.9. 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 $1 \le i, j \le r$.

Theorem★ 2.10. *If $g_1, \ldots, g_r$ are commuting elements of a group, then the product $g_1 \cdots g_r$ has order dividing* $\operatorname{lcm}(|g_1|, \ldots, |g_r|)$.

Definition 2.11. We call a group G ***abelian*** (or ***commutative***) if $gh = hg$ for all $g, h \in G$.

Theorem★ 2.12. *If every nontrivial element of a group has order* 2 *(such a group is said to be of* ***exponent*** 2*), then the group is abelian.*

2.2. Subgroups.

Definition 2.13. Let G be a group. A subset H of G is called a ***subgroup*** of G, denoted $H \leq G$, if it is *closed* under all (three) operations of G, i.e.

(1) the product of two elements of H is again in H,
(2) the inverse of each element of H is again in H, and
(3) the identity (of G) is in H.

A subgroup of G is ***proper*** if it is not equal to G. A subgroup of G is ***nontrivial*** if it has more than 1 element.

Theorem★ 2.14. *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 2.15. 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. If $G = \langle g \rangle$, we say that g ***generates*** G and that G is ***cyclic***.

Problem 2.16. Find all subgroups of S_3. Which are cyclic? Which are abelian?

Problem 2.17. Find examples of each of the following in S_4:

(1) a proper nontrivial cyclic subgroup,
(2) a proper noncyclic abelian subgroup, and
(3) a proper nonabelian subgroup.

Definition 2.18. Let $n \in \mathbb{N}$. Define $\mathbb{Z}/n\mathbb{Z}$ to be the *group* $(\{0, 1, \dots, n-1\}, +_n, -_n, 0)$ where

- $+_n$ is addition modulo n, and
- $-_n$ computes the negative an element modulo n.

When the context is clear, we usually write $+$ and $-$ instead of $+_n$ and $-_n$.

Remark 2.19. When a group is abelian, we usually use use ***additive notation*** and write $x + y$ in place of $m(x, y)$, $-x$ in place of $\iota(x)$, and 0 instead of 1. With this notation, x^n becomes nx. Also, we will often consider the integers $\mathbb{Z}$ as a *group* with operations being the usual addition $+$ and usual negation $-$. The trivial element is 0.

Theorem★ 2.20. *The groups $\mathbb{Z}/n\mathbb{Z}$ and $\mathbb{Z}$ are cyclic.*

Problem 2.21. Find all subgroups of $\mathbb{Z}/12\mathbb{Z}$ and illustrate how they are contained in each other.

Remark 2.22. It should be reasonably clear that every subgroup of an abelian group is abelian, but what happens if we replace *abelian* by *cyclic*?

Theorem★ 2.23. *(Prove or Disprove) Every subgroup of a cyclic group is cyclic.*

Theorem★ 2.24. *Let G be a group. Prove that the intersection of any collection of subgroups of G is also subgroup.*

Definition 2.25. 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 2.26. Note that every subgroup of G that contains S must also contain $\langle S \rangle$. Also, when S consists of a single element, we now have two definitions for $\langle S \rangle$, see Definition 2.15, but it is not hard to prove that they agree.

Problem 2.26.1. Let S be the set of all ***transpositions***, i.e. 2-cycles, in S_4.

(1) Show that $S_4 = \langle S \rangle$, i.e. that S_4 is generated by the transpositions.
(2) Do you need *all* of the transpositions? That is, can you find a proper subset of S that still generates S_4?
(3) Is it possible for S_4 to be generated by two elements (that are not necessarily transpositions)?

Theorem★ 2.27. *If g and h are commuting elements of a group and $\langle g \rangle \cap \langle h \rangle = \{1\}$, then the product gh has order* $\mathrm{lcm}(|g|, |h|)$.

Definition 2.28. 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★ 2.29. *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 $Z(G)$.*

2.3. **Cosets and normal subgroups.**

Definition 2.30. 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 2.31. 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 2.32. A subgroup N of a group G is said to be ***normal*** if $gN = Ng$ for all $g \in G$.

Theorem 2.33. *Every subgroup of an abelian group is normal.*

Problem 2.34. If n is any natural number larger than 1, then $n\mathbb{Z} := \{nm|m \in \mathbb{Z}\}$ is a *subgroup* of $\mathbb{Z}$. Describe the left cosets (which are the same as the right cosets) of $n\mathbb{Z}$ in $\mathbb{Z}$.

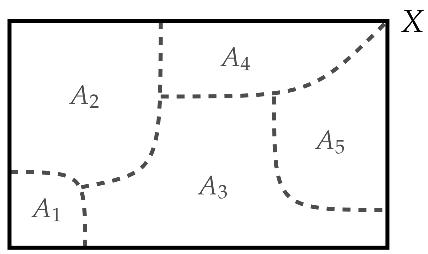
Theorem★ 2.35. *Let G be a group, H a subgroup, and $g, g_1, g_2 \in G$. Then*

(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 2.36. 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 2.37. 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★ 2.38. *If H is a subgroup of G, then the set of left cosets G/H forms a partition of G.*

Remark 2.39. 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.

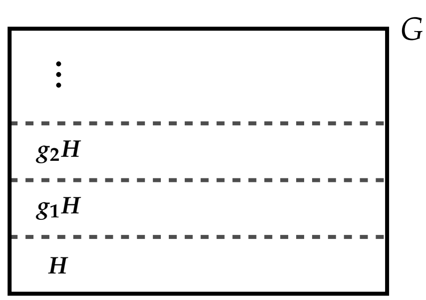
Fact 2.40. By definition, two sets A and B have the same cardinality, i.e. "size", if there is a bijection between A and B.

Theorem★ 2.41 (Lagrange's Theorem)**.** *Let G be a finite group and H a subgroup. Then every left coset of H in G has the same cardinality, and consequently, $|G| = |G/H| \cdot |H|$.*

Theorem★ 2.42. *The order of each element of a finite group divides the order of the group.*

Theorem★ 2.43. *Every group of prime order is cyclic.*

Remark 2.44. 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 Lagrange's Theorem also holds for right cosets. Thus, all left *and* right cosets of H in G have the same cardinality and $|G/H| = |H\backslash G|$.

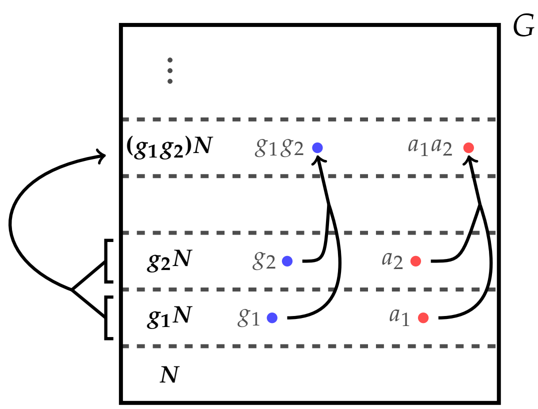
Definition 2.45. Let H a subgroup of a group G. Define the ***index*** of H in G, denoted $|G : H|$, to be $|G : H| := |G/H| = |H\backslash G|$.

Theorem★ 2.46. *Every subgroup of index* 2 *in a group must be normal.*

Theorem 2.47. *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 2.48. 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 2.49 (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 2.50. 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★ 2.51. *If G is a cyclic group and N is a subgroup, then both N and G/N are cyclic.*

Problem 2.52. 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 2.53. A subgroup H of a group G is called ***central*** if $H \leq Z(G)$. Note that central subgroups are necessarily normal.

Theorem★ 2.54. *If N is a central subgroup of G and G/N is cyclic, then G is abelian.*

Definition 2.55. 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 2.56. 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★ 2.57. *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 as well.*

Remark 2.58. Let G be a finite group. We know, by Theorem 2.42, 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.

Definition 2.59. 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★ 2.60. *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★ 2.61. *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★ 2.62. *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. First prove it assuming G is cyclic. Now, assume that the theorem is false, and consider a counterexample to the theorem for which $|G|$ is as small as possible. To find a contradiction, show that G must have a proper nontrivial subgroup N, and then study N and G/N.]

Remark 2.63. 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 2.61? If p is a prime dividing the order of an *arbitrary* finite group, must the group have an element of order p?

Problem 2.63.1. Generalize Theorem 2.62 in some way.

2.4. **Morphisms.**

Definition 2.64. Let G and H be groups. A function $\varphi : G \to H$ is called a ***homomorphism*** if for all $g_1, g_2 \in G$, (1) $\varphi(g_1 g_2) = \varphi(g_1)\varphi(g_2)$, (2) $\varphi(g_1^{-1}) = \varphi(g_1)^{-1}$, and (3) $\varphi(1) = 1$. 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 2.65. 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**. Similar statements holds for the equations $\varphi(g_1^{-1}) = \varphi(g_1)^{-1}$ and $\varphi(1) = 1$.

Theorem★ 2.65.1. *A function $\varphi : G \to H$ between two groups is a homomorphism if and only if $\varphi(g_1g_2) = \varphi(g_1)\varphi(g_2)$ for all $g_1, g_2 \in G$.*

Theorem★ 2.66. *A group G is abelian if and only if the inversion map $G \to G : x \mapsto x^{-1}$ is an automorphism.*

Remark 2.67. 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 2.68. *The inverse of an isomorphism between two groups is also an isomorphism.*

Remark 2.69. 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★ 2.70. *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 2.71. 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★ 2.72. *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 an isomorphism, then $|\varphi(g)| = |g|$.*

Theorem★ 2.73. *Every two infinite cyclic groups are isomorphic, and two finite cyclic groups are isomorphic if and only if they have the same cardinality.*

Problem 2.74. Show that $\mathbb{Z}$ contains (many) *proper* subgroups that are isomorphic $\mathbb{Z}$.

Notation 2.75. 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 2.76. 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 2.77. 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 2.78. 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 2.79. Show that Q_8 is a nonabelian group of order 8 that is *not* isomorphic to D_4.

Definition 2.80. Let G and H be groups, and let $\varphi : G \to H$ be a homomorphism. Define the ***kernel*** of φ to be $\ker\varphi := \{g \in G | \varphi(g) = 1\}$, and the ***image*** of φ to be $\varphi(G) := \{h \in H | h = \varphi(g) \text{ for some } g \in G\}$.

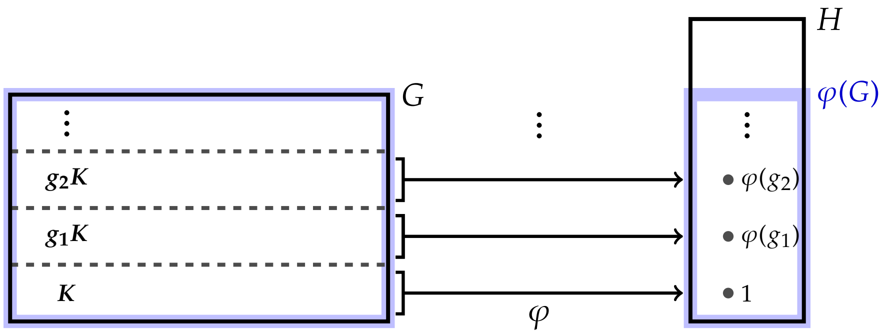
Theorem★ 2.81. *If $\varphi : G \to H$ is a homomorphism of groups, then the kernel of φ is a* ***normal*** *subgroup of G, and the image of φ is a subgroup of H.*

Remark 2.82. 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★ 2.83. *A homomorphism of groups is injective if and only if the kernel is trivial.*

Theorem 2.84 (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 2.85. 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 2.86. 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 $\mathrm{GL}_n(F)/\mathrm{SL}_n(F)$.