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 $x \in X$.

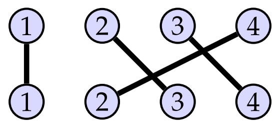
Definition 2.2. Let X be any set. The ***symmetric group*** on X, denoted $\mathrm{Sym}(X)$, is the set of all permutations of X. We denote by S_n the symmetric group on $X = \{1, 2, \ldots, n\}$.

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

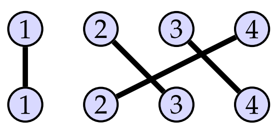
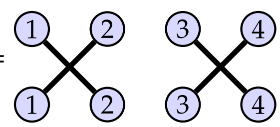
Notation 2.4 (cf. Notation 1.7)**.** If $a, b \in \mathrm{Sym}(X)$, then ab denotes the (function) composition $a \circ b$, i.e $ab(x) = a(b(x))$ for every $x \in X$.

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 $k \in \mathbb{Z}$; in this case we write $G = \langle g \rangle$. 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.*

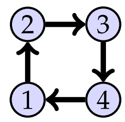
Theorem 2.29. *If F is a field and $n \geq 2$, then $\mathrm{GL}_n(F)$ is nonabelian.*

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 $E := \{(1, 2), (2, 3), (3, 4), (4, 1)\}$.



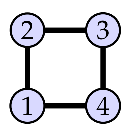
Definition 2.33. An ***automorphism of a digraph*** $\mathcal{G} = (V, E)$ is defined to be a permutation $\sigma \in \mathrm{Sym}(V)$ such that $(x, y) \in E$ if and only if $(\sigma(x), \sigma(y)) \in E$. The set of all automorphisms of $\mathcal{G}$ is denoted $\mathrm{Aut}(\mathcal{G})$.

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.

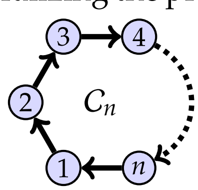
(1) Write down all elements of $\mathrm{Aut}(C_4)$ in disjoint cycle notation.
(2) Describe the various elements of $\mathrm{Aut}(C_4)$ geometrically, e.g. reflection, rotation, . . .
(3) True or False (and explain): is $\mathrm{Aut}(C_4)$ cyclic?
(4) True or False (and explain): is $\mathrm{Aut}(C_4)$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

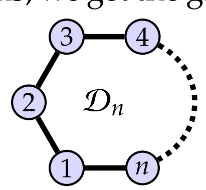
Problem 2.36. Repeat the previous problem for $\mathcal{D}_4 = (V, E)$ where $V := \{1, 2, 3, 4\}$ and $E := \{(1, 2), (2, 1), (2, 3), (3, 2), (3, 4), (4, 3), (4, 1), (1, 4)\}$. Whenever we have "both directions" of an edge, we draw it with no arrows (instead of two). Here is the picture for $\mathcal{D}_4$.



Remark 2.37. If E is symmetric (as Problem 2.39), 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 $E := \{(1, 2), (2, 1), (2, 3), (3, 4), (4, 3), (1, 4)\}$.