THEORY OF GROUPS

NOTES FOR THE SENIOR SEMINAR IN ALGEBRA
HAMILTON COLLEGE, FALL 2014.

1. 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

1.1. **Symmetric groups.**

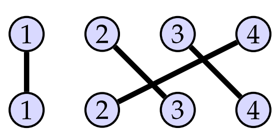
Definition 1.1. Let X be a set. A ***permutation*** of X is a bijection from X to X. The ***identity permutation*** is the permutation $\mathrm{id}_X : X \to X$ defined by $\mathrm{id}_X(x) = x$ for all $x \in X$.

Definition 1.2. 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 $X = \{1, 2, \ldots, n\}$.

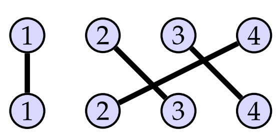
Notation 1.3. If $a, b \in \mathrm{Sym}(X)$, then ab denotes the (function) composition of a and b, i.e, $ab(x) = a(b(x))$ for every $x \in X$. Also, for $n \in \mathbb{N}$, a^n denotes the composition of a with itself n-times, and a^{-n} denotes $\left(a^{-1}\right)^n$, i.e. the composition of a^{-1} with itself n-times.

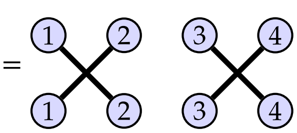
Theorem 1.4. *If $\sigma \in \mathrm{Sym}(X)$ and $m, n \in \mathbb{Z}$, then*
(1) $\sigma^{-m} = (\sigma^m)^{-1}$, and
(2) $\sigma^m \sigma^n = \sigma^{m+n}$.

Problem 1.5 (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 1.6 (Cauchy's two-line notion for S_n)**.**

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

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

Note: there is an obvious way to compress this to a one-line notation.

(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 1.5, 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 1.7 (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 1.5, and do the same for $\sigma\tau$ and $\tau\sigma$.
(6) Formulate a rule in this notation for finding the composition of two elements.

Definition 1.8. 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 1.9. In the previous problem, σ has cycle type $(1, 3)$, which is abbreviated to (3); we say that σ is a 3-cycle. The permutation τ has cycle type $(2, 2)$. The cycle type of $(3 \quad 4 \quad 2)(1 \quad 7)(6 \quad 8) \in S_{10}$ is $(2, 2, 3)$.

Problem 1.10.

(1) Find a $\sigma \in S_4$ such that σ is not the identity but σ^2 is the identity. Such an element is said to *have 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?

Definition 1.11. Let $\sigma \in \mathrm{Sym}(X)$. If $\sigma^n = \mathrm{id}_X$ for some positive $n \in \mathbb{N}$, then we define the ***order*** of σ to be the smallest such n. Otherwise, we say that σ has ***infinite order***.

Problem 1.12. 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. (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.

Notation 1.13. If X is a set, then $|X|$ denotes the cardinality of X, i.e. the "number" of elements in X. If $\sigma \in \mathrm{Sym}(X)$, then $|\sigma|$ denotes the order of σ.

Theorem 1.14. *If $n := |X|$ is finite, then $|\mathrm{Sym}(X)| =$ _(in terms of n)_.*

⋆**Theorem 1.15.** *If $n := |X|$ is finite, then $\mathrm{Sym}(X)$ has _(in terms of n)_ elements of order 2.*

⋆**Theorem 1.16.** *Assume that X is finite and $\sigma \in \mathrm{Sym}(X)$. If σ has cycle type $(m_1, \dots, m_r)$, then $|\sigma| =$ _(in terms of $m_1, \dots, m_r$)_.*

⋆**Theorem 1.17.** *If X is finite and $\sigma \in \mathrm{Sym}(X)$, then $|\sigma|$ divides $|\mathrm{Sym}(X)|$, or in words, the order of each element divides the order of the group.*

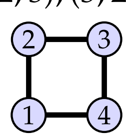
1.2. **Automorphism groups of graphs.**

Definition 1.18. A pair $\mathcal{G} = (V, E)$, where V is a set of elements called ***vertices*** and $E \subseteq V \times V$, is called a ***directed graph*** (or ***digraph***), and the elements of E are ***directed edges***. If E is symmetric, then $\mathcal{G}$ is simply called a ***graph***, and for every $(v, w) \in E$, the unordered pair $\{v, w\}$ is an ***edge***.

Definition 1.19. An ***automorphism of a graph*** (or digraph) $\mathcal{G} = (V, E)$ is a permutation $\sigma \in \mathrm{Sym}(V)$ such that $(x, y) \in E$ if and only if $(\sigma(x), \sigma(y)) \in E$. The ***automorphism group*** of $\mathcal{G}$ is the set of all automorphisms of $\mathcal{G}$, denoted $\mathrm{Aut}(\mathcal{G})$.

Remark 1.20. If $\mathcal{G}$ is a graph with vertex set V, then $\mathrm{Aut}(\mathcal{G}) \subseteq \mathrm{Sym}(V)$. Of course, every element of $\mathrm{Aut}(\mathcal{G})$ also permutes the edges of $\mathcal{G}$, but it is possible for nontrivial elements of $\mathrm{Aut}(\mathcal{G})$ to fix every edge (but not every directed edge).

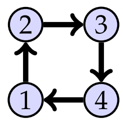
Problem 1.21. Consider the graph $\mathcal{D}_4 = (V, E)$ with vertex set $V := \{1, 2, 3, 4\}$ and (symmetric) edge relation $E := \{(1, 2), (2, 1), (2, 3), (3, 2), (3, 4), (4, 3), (4, 1), (1, 4)\}$.



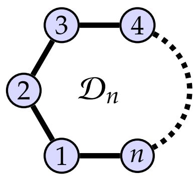
(1) Write down all elements of $\mathrm{Aut}(\mathcal{D}_4)$ in disjoint cycle notation.
(2) Determine how many elements of $\mathrm{Aut}(\mathcal{D}_4)$ have order 2.
(3) Determine how many elements of $\mathrm{Aut}(\mathcal{D}_4)$ have order 3.
(4) Determine how many elements of $\mathrm{Aut}(\mathcal{D}_4)$ have order 4.

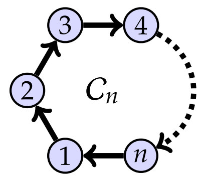
(5) True or False (and explain): there is an $a \in \mathrm{Aut}(\mathcal{D}_4)$ such that for every $b \in \mathrm{Aut}(\mathcal{D}_4)$ there exists a $k \in \mathbb{N}$ for which $b = a^k$.
(6) True or False (and explain): for every $a, b \in \mathrm{Aut}(\mathcal{D}_4)$, $ab = ba$.

Problem 1.22. Repeat the previous problem for the *directed* graph $\mathcal{C}_4 = (V, E)$ with vertex set $V := \{1, 2, 3, 4\}$ and edge relation $E := \{(1, 2), (2, 3), (3, 4), (4, 1)\}$.



Definition 1.23. Generalizing the previous two problems, we get the graphs $\mathcal{D}_n$ and $\mathcal{C}_n$ below.





(1) The automorphism group of $\mathcal{D}_n$, denoted D_n (or often D_{2n}), is the ***dihedral group of order*** $2n$.
(2) The automorphism group of $\mathcal{C}_n$, denoted C_n, is the ***cyclic group of order*** n.

Definition 1.24. Let $G \subseteq \mathrm{Sym}(X)$.

(1) We say that G ***acts transitively*** on X if for every $x, y \in X$ there is a $g \in G$ such that $g(x) = y$.
(2) We say that G ***acts freely*** on X if for every $x \in X$ and every $g \in G$ we have that $g(x) = x$ only if $g = \mathrm{id}$, i.e. the only element of G that fixes a vertex is the identity.

Theorem 1.25. *The group D_n acts transitively, but not freely, on the vertices of $\mathcal{D}_n$.*

$\star$**Theorem 1.26.** *The group C_n acts transitively and freely on the vertices of $\mathcal{C}_n$.*

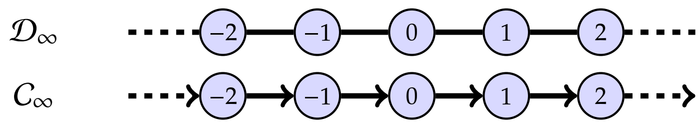
Problem 1.27. Clarify and prove the following statement: *if the automorphism group of a graph acts freely on the set of vertices, then each element of the group is determined by its action on any one individual vertex.*

Definition 1.28. If G is a (symmetric or automorphism) group and $g \in G$, we say that g ***generates*** G if for every $h \in G$ there is some $k \in \mathbb{Z}$ such that $h = g^k$. If G is generated by one of its elements, we say that the group G is ***cyclic***.

Theorem 1.29. *For every positive integer n, C_n is cyclic.*

Problem 1.30. Make and provide evidence for (or prove) a conjecture as to which elements of C_n can generate C_n.

Definition 1.31. We define the (infinite) graphs $\mathcal{D}_\infty$ and $\mathcal{C}_\infty$ as



(1) The automorphism group of $\mathcal{D}_\infty$, denoted D_∞, is the ***infinite dihedral group***.
(2) The automorphism group of $\mathcal{C}_\infty$, denoted C_∞, is the ***infinite cyclic group***.

⋆**Theorem 1.32.** *The group C_∞ is cyclic.*

Problem 1.33. Find all elements of C_∞ that generate it.

Definition 1.34. If G is a (symmetric or automorphism) group, we say that G is ***abelian*** (or ***commutative***) if $gh = hg$ for every $g, h \in G$.

⋆**Theorem 1.35.** *Every cyclic group is abelian.*

Theorem 1.36. *If $n \geq 3$ or if $n = \infty$, then D_n is not abelian.*

⋆**Theorem 1.37.** *If $n \in \mathbb{N}$ and $\mathcal{G}$ is* ____(description of a graph)____*, then* $\mathrm{Aut}(\mathcal{G}) = S_n$.

1.3. **Linear groups.**

Definition 1.38. Let F be a field, and set $M_n(F)$ to be the collection of $n \times n$ matrices with entries from F. Define
(1) the ***general linear group*** to be $\mathrm{GL}_n(F) := \{A \in M_n(F) | \det A \neq 0\}$, and
(2) the ***special linear group*** to be $\mathrm{SL}_n(F) := \{A \in M_n(F) | \det A = 1\}$.

Remark 1.39. Given any F field and any positive integer n, we have that

$$\mathrm{SL}_n(F) \subseteq \mathrm{GL}_n(F) \subseteq \mathrm{Sym}(V),$$

where V is the vector space F^n. In particular, we can talk about orders of elements as well as the properties of being transitive, free, cyclic or abelian for these groups.

Notation 1.40. If A and B are sets, $A - B$ denotes the set of elements in A but not in B. The notation $A \setminus B$ is also sometimes used.

Theorem 1.41. *The group $\mathrm{GL}_n(\mathbb{C})$ acts transitively on the set $X := \mathbb{C}^n - \{\mathbf{0}\}$.*

⋆**Theorem 1.42.** *The group $\mathrm{GL}_n(\mathbb{C})$ acts freely on the set $X := \mathbb{C}^n - \{\mathbf{0}\}$ if and only if $n =$* ____(list of numbers)____.

⋆**Theorem 1.43.** *The group $\mathrm{GL}_n(\mathbb{C})$ is abelian if and only if $n =$* ____(list of numbers)____.

⋆**Theorem 1.44.** *The group $\mathrm{SL}_2(\mathbb{C})$ has exactly one element of order 2.*