18.312: Algebraic Combinatorics Lionel Levine

Lecture 1

Lecture date: February 1, 2011 *Notes by: Lou Odette*

1 Names, places, times:

- **Office hours** (in 2-335): *Tuesdays* 12:00-13:00 & *Wednesdays* 13:00-14:00.
- **Course info**: math.mit.edu/~levine/18.312 (levine at math dot mit dot edu)
- **Grader**: Aldo Pacchiano Camacho (pacchian at mit dot edu)
- **Grading**:
  - weekly PSET worth roughly 50 "points" throughout the term; turn in your best 30 "points" to count for *30% of final grade*,
  - midterm on **March 10** worth *20% of final grade*,
  - final on **May 5** worth *30% of final grade*, and
  - write-up of notes (1-2 lectures) worth *20% of final grade.*

2 Algebraic Combinatorics

While the term *combinatorics* frequently is used to refer to counting problems (Enumerative Combinatorics), some combinatorics is non-enumerative and in particular Algebraic Combinatorics treats the relationships between discrete structures and algebraic objects, e.g.

Discrete Structures		Algebraic Objects
graphs		groups
partially ordered sets	←--	monoids
lattices		vector spaces
matroids	--→	rings
simplicial complexes		algebras

While the connection with algebraic objects can provide more structure to the combinatorial objects, the connection can go the other way, with combinatorial objects providing concrete instances of the algebraic objects. The next section is an example of a combinatorial object helping to make an algebraic idea concrete.

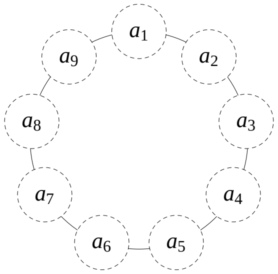
3 Fermat's "little" Theorem

Fermat's "little" theorem states that if p is a prime number, then for any $n \in \mathbb{N}$, $n^p - n$ will be evenly divisible by p. To make this concrete, consider the problem of making a necklace of p beads, choosing the beads from n distinct colors. Let $[n] \equiv \{1, 2, \ldots, n\}$, and denote the cardinality of a set S by $\#S$ (alternatively, by $|S|$).

The set of all necklaces of p beads from n colors has cardinality

$$\#\{f : [p] \to [n]\} = n^p$$

and so there are $n^p - n$ necklaces that aren't all one color (constant). Let the color of bead i be $f(i) = a_i$ and denote a necklace by a p-vector of the colors starting with the bead at 12 o'clock and proceeding clockwise. For example, the necklace $\underline{a} = (a_1, a_2, \ldots, a_9)$ can also be represented by the following picture

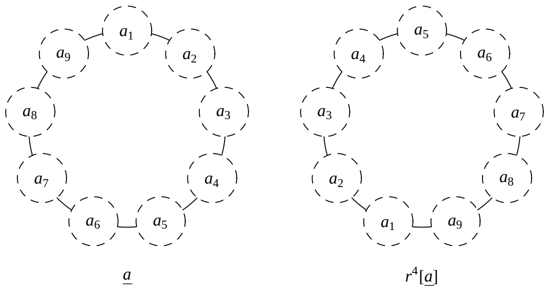


$\underline{a}$

Denote a counterclockwise rotation of the necklace by i beads by

$$r^i(a_1, a_2, \ldots . a_p) = (a_{i+1}, \ldots . a_p, a_1, \ldots, a_i)$$

so for example $r^4(a_1, a_2, \ldots . a_9) = (a_5, \ldots . a_9, a_1, \ldots, a_4)$ and the necklaces $\underline{a}$ and $r^4(\underline{a})$ are illustrated below



Proposition 1 *If $\underline{a}$ is a non-constant necklace, then the necklaces $\underline{a}, r^1(\underline{a}), \ldots, r^{p-1}(\underline{a})$ are all distinct.*

Proof:

If $r^i(\underline{a}) = r^j(\underline{a})$ then $(a_{i+1}, \ldots .a_p, a_1, \ldots, a_i) = (a_{j+1}, \ldots .a_p, a_1, \ldots, a_j)$ and so for all k, $a_{i+k} = a_{j+k} \pmod{k}$. Now let $l = j - i$, then $a_{i+k} = a_{j+k} \Rightarrow a_k = a_{k+l}$, and it follows that $a_l = a_{2l} = a_{3l} = \cdots$. However, if $i \neq j$ then $l \neq 0$ and $a_l, a_{2l}, a_{3l}, \cdots$ are all distinct $(\bmod\ p)$. Thus in this case the necklace $\underline{a}$ must be constant, so $r^i(\underline{a}) = r^j(\underline{a})$ only if $i = j$. Thus there are exactly p rotational classes on non constant necklaces, and the number of distinct non-constant necklaces is evenly divisible by p.

□

4 Review of group action.

Let G be a group and X a non-empty set, with $g, h \in G$ and $x \in X$.

Definition 2 *The* action *of G on X is a map*

$$G \times X \to X;\ (g, x) \mapsto gx$$

such that (i) $\mathbf{1}x = x$, $\forall x \in X$ and (ii) $\forall g, h \in G$, $\forall x \in X$, $g(hx) = (gh)x$.

For each $g \in G$ we also get an invertible map $\sigma(g)$ from the action of g on x

$$\sigma(g) : X \to X,\ x \mapsto gx$$

and we can check that $\sigma(g)$ is invertible

$$\sigma\left(g^{-1}\right)(\sigma(g)\, x) = g^{-1}(gx) = \left(g^{-1}g\right)x = \mathbf{1}x = x$$

and that the map $\sigma(\cdot)$ is a group homomorphism $\sigma : G \to \operatorname{Sym} X$ (i.e. $\sigma(gh) = \sigma(g)\sigma(h)$) where $\operatorname{Sym} X$ is the symmetric group of all invertible maps.

Definition 3 *Let G be a group that acts on the set X. If $x \in X$ the* orbit *of x is the set $Orb(x) = \{y \in X | y = gx,\ \text{for some}\, g \in G\}$. The* stabilizer *of x is the set $Stab(x) = \{g \in G | gx = x\}$. Notice that $Stab(x)$ is a subgroup of G*

$$g, h \in Stab(x) \Rightarrow gh(x) = g(hx) = g(x) = x \Rightarrow gh \in Stab(x)$$

Definition 4 *If $S \subset G$, then let $\langle S \rangle$ denote the subgroup generated by S, the smallest subgroup of G containing every element of S. If $G = \langle S \rangle$ then S generates G and the elements in S are called* generators.

Definition 5 *A group G is* cyclic *if there exists an element $g \in G$ such that $G = \langle g \rangle \equiv \{g^n | n \in \mathbb{N}\}$.*

Theorem 6 *The* Orbit-Stabilizer *Theorem states that $\forall x \in X$*

$$|Orb(x)| \times |Stab(x)| = |G|$$

5 A generalization of Fermat's "little" theorem.

We can generalize Fermat's "little" theorem if p is not prime as follows.

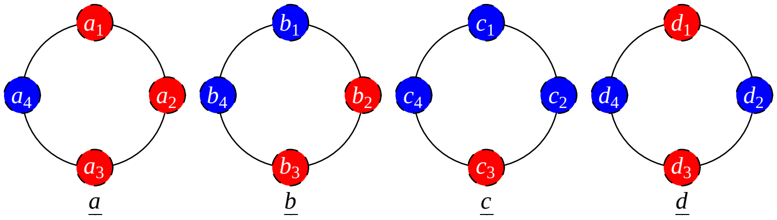
- In general, $n^k - n$ is not evenly divisible by k. For example, consider a necklace of four beads from 2 colors $(n = 2,\ k = 4)$. Clearly

  $$\frac{n^k - n}{k} = \frac{2^4 - 2}{4} = \frac{14}{4} \notin \mathbb{N}$$

  and if we count the non-constant necklaces, the fourteen necklaces are

  $$\underline{a}, r^1\left(\underline{a}\right), r^2\left(\underline{a}\right), r^3\left(\underline{a}\right), \underline{b}, r^1\left(\underline{b}\right), r^2\left(\underline{b}\right), r^3\left(\underline{b}\right), \underline{c}, r^1\left(\underline{c}\right), r^2\left(\underline{c}\right), r^3\left(\underline{c}\right), \underline{d}, r^1\left(\underline{d}\right)$$

  based on the necklaces $\underline{a}, \underline{b}, \underline{c}, \underline{d}$ shown below

- For general k, consider the set of k-necklaces from n colors,

  $$N_k = \left\{(a_0, a_1, \ldots, a_{k-1}) \,|a_i \in [n]\right\}.$$

  Clearly $|N_k| = n^k$, and the cyclic group C_k of order k acts on members of the set N_k by rotation. With $r^i\left(a_1, a_2, \ldots .a_p\right) = \left(a_{i+1}, \ldots .a_p, a_1, \ldots, a_i\right)$, taking the indices mod k, interpret r^i as the group element acting on the necklace $\underline{a}$. Then for the k-necklace problem $C_k = \langle r \rangle = \left\{\mathbf{1}, r, r^2, \cdots, r^{k-1}\right\}$ with $r^k = \mathbf{1}$ and $X \equiv N_k$. Thus

  $$r^i\left(r^j\left(\underline{a}\right)\right) = r^{i+j}\left(\underline{a}\right);\ r^k\left(\underline{a}\right) = \underline{a}$$

  represents two actions: rotate by j, then rotate by i.

- It is apparent then that the generators of $\underline{a}, \underline{b}, \underline{c}$ are the cyclic group $C_1 = \langle r \rangle$, while the generator of $\underline{d}$ is the cyclic group $C_2 = \left\langle r^2 \right\rangle$. The two constant necklaces have generator $C_4 = \left\langle r^4 \right\rangle$.

- The necklaces $\underline{a}, b, \underline{c}$ each have the same stabilizer, with $\text{Stab}\left(\underline{a}\right) = \left\langle r^4 \right\rangle = C_1$, while the stabilizer of the necklace $\underline{d}$ is $\text{Stab}\left(\underline{d}\right) = \left\langle r^2 \right\rangle = C_2$. The necklaces $\underline{a}, b, \underline{c}$ each have the same orbit, with $\text{Orb}\left(\underline{a}\right) = \left\{\underline{a}, r\underline{a}, r^2\underline{a}, r^3\underline{a}\right\}$, while the orbit of the necklace $\underline{d}$ is $\text{Orb}\left(\underline{d}\right) = \left\{\underline{d}, r^1\underline{d}\right\}$. An application of the Orbit-Stabilizer Theorem gives $|\text{Orb}\left(x\right)| \times |\text{Stab}\left(x\right)| = k$ for each necklace.

Definition 7 *A necklace is* primitive *if it has no stabilizer, i.e. Stab* $\left(\underline{a}\right) = C_1$.

Example 8 *Consider the case $k = pq$, where p, q are distinct primes. The goal is to count the number of* primitive *necklaces. Here $C_k = C_{pq}$ which has four subgroups, shown below with their corresponding generators*

$$\begin{tikzcd}[row sep=small] \textit{subgroup:} & C_{pq} \arrow[d, dash] & C_p \arrow[d, dash] & C_q \arrow[d, dash] & C_1 \arrow[d, dash] \\ \textit{generator:} & \left\langle r^1 \right\rangle & \langle r^q \rangle & \langle r^p \rangle & \langle r^{pq} \rangle \end{tikzcd}$$

Let the set of necklaces $E_\alpha = \{\text{necklaces } \underline{a} | Stab\,(\underline{a}) \supseteq C_\alpha\}$, with $\alpha \in \{1, p, q, pq\}$. Then the set of primitive necklaces is the set difference

$$N_k - E_p - E_q$$

and so the number of primitive necklaces is

$$|N_k| - |E_p| - |E_q| + |E_p \cap E_q|$$

but since p and q are primes, $E_p \cap E_q = E_{pq}$, the number of constant necklaces. So we have

$$\begin{aligned} |N_k| &= n^{pq} \\ |E_p| &= n^q \\ |E_q| &= n^p \\ |E_p \cap E_q| &= n \end{aligned}$$

and thus the number of primitive *necklaces is $n^{pq} - n^q - n^p + n$.*