

Ring basics

Jonathan L.F. King
 University of Florida, Gainesville FL 32611-2082, USA
 squash@ufl.edu
 Webpage <http://squash.1gainesville.com/>
 17 November, 2017 (at 02:57)

Henceforth, the token-set is *finite*, of cardinality $N := |\Omega|$. Further, writing the symmetric group as \mathbb{S}_N shall mean that $\Omega = [1..N]$. □

Permutations

On a set Ω , a bijection $\pi: \Omega \rightarrow \Omega$ is also called a “*permutation* of Ω ”. Use *perm* to abbrev. “permutation”. A *token* is an element $x \in \Omega$. Use Id_Ω for the identity perm, $x \mapsto x$.

Composition. It will be convenient to have symbols for composition in *both* directions. We will use \triangleleft to mean \circ . Thus

1a: Both $[\beta \triangleleft \alpha](x)$ and $[\alpha \triangleright \beta](x)$ mean $\beta(\alpha(x))$.

Use $\beta^{\circ n}$ for “the n^{th} -*composition-power* of β ”. E.g

1a':
$$\beta^{\circ 3}(x) = \beta(\beta(\beta(x))),$$

and $\beta^{\circ -1}$ is the *inverse function* of β , which we will usually just write as β^{-1} . When composition is understood, we will write β^3 rather than $\beta^{\circ 3}$.

The \mathbb{S}_Ω group. The set all permutations on Ω is “the *symmetric group* on Ω ”, written \mathbb{S}_Ω .

We will view permutation-composition as going *L-to-R*; permutation $\alpha\beta$ is $\alpha \triangleright \beta$, first applying α , then β . So $[\alpha\beta](x)$ is $\beta(\alpha(x))$.

Hence triple $(\mathbb{S}_\Omega, \triangleright, Id_\Omega)$ is a group.

[Should a notational need arise to compose in the other direction, we can write $\alpha\beta$ as $\beta \triangleleft \alpha$.]

Orbits. For $\beta \in \mathbb{S}_\Omega$, “the β -*orbit* of token x ” is the set

$$\mathcal{O}_\beta(x) := \left\{ \beta^{\circ k}(x) \mid k \in \mathbb{Z} \right\},$$

together with the information that β maps $\beta^{\circ k}(x)$ to $\beta^{\circ [k+1]}(x)$. A β -orbit is either finite; a K -cycle for some posint K , or is infinite, and is a copy of the add-one function mapping $\mathbb{Z} \rightarrow \mathbb{Z}$. This last is an “ ∞ -cycle”, as “cycle” has come to mean ‘generated by a single element’, in various branches of algebra.

Cycle-structure. Consider the following shuffle, π , of an Ace-through-King suit, Ω . Our π goes from the std order [top line], to the order in the bottom line:

A	2	3	4	5	7	6	8	9	T	J	Q	K
9	T	3	Q	A	7	4	6	5	J	K	8	2

This is called “the *two-line* presentation of π ”. [If the std token-order were understood, then just the bottom line could be shown; the *one-line* presentation of π .]

The *cycle-structure* of π is a listing of all its cycles. Note that π maps $A \rightarrow 9 \rightarrow 5 \rightarrow A$; this is a 3-cycle, which I write as $\zeta(A\ 9\ 5)$. This *same cycle* could be written as $\zeta(9\ 5\ A)$ or as $\zeta(5\ A\ 9)$. Notice, however, that $\zeta(5\ 9\ A)$ is a *different* cycle; indeed, $\pi(5)$ is *not* 9.

So the *cycle-structure* of π is

1b:
$$\pi = \zeta(3)\ \zeta(7)\ \zeta(A\ 9\ 5)\ \zeta(2\ T\ J\ K)\ \zeta(4\ Q\ 8\ 6).$$

While the order in which the [pairwise disjoint] cycles are listed, does not change the permutation, it is nonetheless convenient to have a **CCN**, *canonical cycle-notation*:^{♥1}

From *L-to-R*, list all the 1-cycles, then all the 2-cycles,
 If the token-set has a natural ordering, then list each cycle with its leftmost token being its smallest taken. Finally, for each length K , list the K -cycles *L-to-R*, sorted by their leftmost [smallest] token.

So (1b) is in CCN, assuming the token-ordering is $A < 2 < 3 < \dots < 9 < T < J < Q < K$. Lastly, the [**cycle**] *signature* of a permutation, lists how many cycles of each length, occur. The signature of the π in (1b), is

1b':
$$[1^2, 3^1, 4^2] \stackrel{\text{note}}{=} [1^2, 2^0, 3^1, 4^2, 5^0 \dots],$$

since π has two 1-cycles, one 3-cycle, and two 4-cycles.

Let $\#Ev(\beta)$ be the number of even-length β -cycles, $\#Od(\beta)$ counts the number of odd-length cycles, and $\#All(\beta) := \#Ev(\beta) + \#Od(\beta)$.

For (1b), then, $\#All(\pi) = 5$ and $\#Ev(\pi) = 2$.

^{♥1}E.g, write cycle $\zeta(9\ 8\ 5)$ as $\zeta(5\ 9\ 8)$, putting its smallest token, 5, leftmost. List three-cycle $\zeta(5\ 9\ 8)$ somewhere left of four-cycle $\zeta(1\ 28\ 14\ 7)$. Finally, for two three-cycles, list $\zeta(3\ 15\ 6)$ before $\zeta(5\ 9\ 8)$, since $3 < 5$.

Sign of a permutation. Given a permutation, β , of a finite set, define its **sign** as

$$1c': \quad \text{Sgn}(\beta) := [-1]^{\#\text{Ev}(\beta)}.$$

Permutation β is called **even** ($\text{Sgn}(\beta) = +1$), or **odd** ($\text{Sgn}(\beta) = -1$), depending on whether $\#\text{Ev}(\beta)$ is even or odd.

A **transposition** is a permutation comprised of a single two-cycle; its signature is $[1^{[N-2]}, 2^1]$.

Every permutation on a [finite] Ω is a composition^{♥2} of transpositions.

For the next result, consider distinct tokens x,y , in a common L -cycle, π . Pair x,y is “ **$J:K$ -separated**” if the smallest posints j,k such that $\pi^j(x) = y$ and $\pi^k(y) = x$ are $j=J$ and $k=K$. (Necessarily, $J+K = L$.)

2: Cleave lemma. Consider perms β, γ and transposition $\tau := \langle x y \rangle$ such that $\tau \triangleright \beta = \gamma$.

Suppose tokens x and y lie in different β -cycles, of lengths J and K , respectively. Then γ has these two coalesced into a single cycle of length $J+K$, and they are $J:K$ -separated in this γ -cycle. Consequently,

$$\#\text{All}(\gamma) = \#\text{All}(\beta) - 1.$$

$$\dagger: \quad \#\text{Ev}(\gamma) = \#\text{Ev}(\beta) + \begin{cases} +1 & \text{if } J, K \text{ both odd} \\ -1 & \text{otherwise} \end{cases}.$$

Instead, if x,y lie $J:K$ -separated in the same β -cycle, then this cycle splits into two γ -cycles, of lengths J and K . Further,

$$\#\text{All}(\gamma) = \#\text{All}(\beta) + 1.$$

$$\ddagger: \quad \#\text{Ev}(\gamma) = \#\text{Ev}(\beta) + \begin{cases} -1 & \text{if } J, K \text{ both odd} \\ +1 & \text{otherwise} \end{cases}.$$

*: Both (\dagger, \ddagger) hold if, instead, τ follows β , i.e., $\gamma = \beta \triangleright \tau$. ♦

Pf of (2†). Rename x,y to x_1, y_1 , and write the relevant β -cycles as

^{♥2}If perm β fixes every token then β is the empty composition. Else there is a token x such that $y := \beta(x) \neq x$; so composition $\beta \triangleright \langle y x \rangle$ fixes at least one more token than did β , hence is a composition of transpositions.

$$\langle x_1 x_2 \dots x_J \rangle \quad \text{and} \quad \langle y_1 y_2 \dots y_K \rangle.$$

Then $\gamma := \tau \triangleright \beta$ has coalesced these into γ -cycle

$$\langle x_1 y_2 \dots y_J y_1 x_2 \dots x_K \rangle,$$

in which pair x_1, y_1 is indeed $J:K$ -separated. ♦

Proof continued. Observe that (\ddagger) is (\dagger) backwards, noting that $\tau^{-1} = \tau$ and thus $\tau \triangleright \gamma = \beta$.

Finally, $(*)$ follows by noting that when $\gamma = \tau \triangleright \beta$, then $\gamma^{-1} = \beta^{-1} \triangleright \tau$. ♦

2a: Transposition Parity theorem. Consider a β written as a composition $\tau_1 \triangleright \tau_2 \triangleright \dots \triangleright \tau_M$ of transpositions. Then M is even/odd, as β is an even/odd permutation. Indeed, the sign-map is group-homomorphism,

$$\text{Sgn}: (\mathbb{S}_\Omega, \triangleright, \text{Id}_\Omega) \rightarrow (\{\pm 1\}, \cdot, 1),$$

i.e., $\text{Sgn}(\alpha\beta) = \text{Sgn}(\alpha) \cdot \text{Sgn}(\beta)$. ♦

Pf. This is immediate from $(2\dagger, \ddagger)$, the Cleave lemma. Here are two other proofs, which proceed by ordering the token-set, viewing Ω as $[1..N]$.

Define the **inversion number** $f(\beta)$ to be the cardinality of

$$\{(i, j) \mid i, j \in \Omega \text{ with } i < j, \text{ yet } \beta(i) > \beta(j)\}.$$

ISTShow, given a transposition τ , that

$$f(\beta \triangleright \tau) = f(\beta) + \text{Odd}.$$

This holds when τ is an “adjacent-transposition”; of form $\langle i \ i+1 \rangle$: If $(i, i+1)$ was an inversion, then $f(\beta\tau)$ equals $f(\beta) - 1$; else $f(\beta) + 1$. Finally, observe that an arbitrary transposition $\langle k \ k+n \rangle$ is a composition of oddly many, $2n - 1$, adjacent-transpositions.

For a third proof, from perm β create an $N \times N$ matrix $\hat{\beta}$, whose (i, j) entry is 1, if $j = \beta(i)$, and is 0 otherwise. [Such is called a **permutation matrix**.] Then $\text{Sgn}(\beta)$ equals the determinant $\text{Det}(\hat{\beta})$. Multiplicativity $\text{Sgn}(\alpha\beta) = \text{Sgn}(\alpha) \cdot \text{Sgn}(\beta)$ follows from multiplicativity of the determinant. ♦

2b: Minimum-transposition lemma. Each $\beta \in \mathbb{S}_N$ can be written as a product of $[N - \#\text{All}(\beta)]$ many transpositions, but no fewer. \diamond

Proof. Repeated apply (2†). Pick distinct x, y in a cycle, then compose with $(x\ y)$, to split the cycle. Continue, until you have N -many 1-cycles. \blacklozenge

Permutation-Sign examples. Here are a few sample computations.

3: Multiplication-sign. On group $(\mathbb{Z}_N, +, 0)$, an $\mathbf{r} \in \mathbb{Z}_N$ engenders permutation

$$\alpha_{\mathbf{r}}(x) := x + \mathbf{r}. \quad [\text{Addition mod-}N]$$

The cycle-structure of $\alpha_{\mathbf{r}}$ is M many K -cycles, where

$$*: \quad K := \text{Gcd}(\mathbf{r}, N) \quad \text{and} \quad M := N/K.$$

When N is even, then $\text{Sgn}(\alpha_{\mathbf{r}}) = 1$ IFF \mathbf{r} is a “doubling-residue”, i.e., $\exists y \in \mathbb{Z}_N$ with $2y = \mathbf{r}$. \diamond

Proof. $N = 2H$ \blacklozenge

4: Cartesian-sign Lemma. For $j = 1, 2$, consider permutation β_j on token-set Ω_j , with $\mathcal{E}_j := \#\text{Ev}(\beta_j)$ and $\mathcal{D}_j := \#\text{Od}(\beta_j)$. Letting \equiv mean \equiv_2 , then, cartesian product permutation $\pi := \beta_1 \times \beta_2$ has that

$$\begin{aligned} \dagger: \quad \#\text{Ev}(\pi) &\equiv \mathcal{E}_1 \mathcal{D}_2 + \mathcal{D}_1 \mathcal{E}_2 \\ \ddagger: \quad &\equiv \mathcal{E}_1 N_2 + N_1 \mathcal{E}_2, \end{aligned}$$

where $N_j := |\Omega_j|$. \diamond

Pf. Consider token $x_j \in \Lambda_j$, where Λ_j is a β_j -cycle of length K_j . Then (x_1, x_2) generates a π -cycle of length

$$L := \text{Lcm}(K_1, K_2).$$

So, cartesian product $\Lambda_1 \times \Lambda_2$ splits up into

$$G := \text{Gcd}(K_1, K_2)$$

many length- L π -cycles. These contribute to $\text{Sgn}(\pi)$ iff L is even and G is odd; i.e., when $K_1 \neq K_2$. Hence (†). Evidently $\mathcal{D}_j \equiv N_j$ (Why?), giving (‡). \blacklozenge