Ring basics

Jonathan L.F. King
University of Florida, Gainesville FL 32611-2082, USA
squash@ufl.edu
Webpage http://squash.1gainesville.com/
24 July, 2016 (at *20:28*)

Permutations

On a set Ω, a bijection $\pi{:}\Omega{\to}\Omega$ 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

$$1a'\text{:} \qquad \beta^{\circ 3}(x) \;=\; \beta\Big(\beta\big(\beta(x)\big)\Big)\,,$$

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 $\mathbb{S}_\Omega$ group. The set all permutations on Ω is **"**the ***symmetric group*** on Ω**"**, written $\mathbb{S}_\Omega$.

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

$$\mathcal{O}_\beta(x) \;:=\; \Big\{ \beta^{\circ k}(x) \;\Big|\; k \in \mathbb{Z} \Big\}\,,$$

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 $\mathbb{Z}{\to}\mathbb{Z}$. This last is an **"**$\infty$-cycle**"**, as "cycle" has come to mean 'generated by a single element', in various branches of algebra.

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

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$\to$9$\to$5$\to$A; this is a 3-cycle, which I write as $(\text{A}\ 9\ 5)$. This *same cycle* could be written as $(9\ 5\ \text{A})$ or as $(5\ \text{A}\ 9)$. Notice, however, that $(5\ 9\ \text{A})$ is a *different* cycle; indeed, $\pi(5)$ is *not* 9.

So the ***cycle-structure*** of π is

$$1b\text{:} \qquad \pi \;=\; (3)\,(7)\,(\text{A}\ 9\ 5)\,(2\ \text{T}\ \text{J}\ \text{K})\,(4\ \text{Q}\ 8\ 6)\,.$$

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 $\text{A} < 2 < 3 < \ldots < 9 < \text{T} < \text{J} < \text{Q} < \text{K}$. Lastly, the [***cycle***] ***signature*** of a permutation, lists how many cycles of each length, occur. The signature of the π in (1b), is

$$1b'\text{:} \qquad \lceil 1^2,\, 3^1,\, 4^2 \rfloor \;\overset{\text{note}}{=\!=}\; \lceil 1^2,\, 2^0,\, 3^1,\, 4^2,\, 5^0 \ldots \rfloor\,,$$

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

1c: *Let* $^{\#}\text{Ev}(\beta)$ *be the number of even-length β-cycles,* $^{\#}\text{Od}(\beta)$ *counts the number of odd-length cycles, and* $^{\#}\text{All}(\beta) := {}^{\#}\text{Ev}(\beta) + {}^{\#}\text{Od}(\beta)$.

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

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

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

1c′: $$\mathrm{Sgn}(\beta) \;:=\; [\text{-}1]^{\#\mathrm{Ev}(\beta)}\,.$$

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

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

> *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 tranposition $\tau := (x\ y)$ 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,

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

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,

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

∗: *Both (†,‡) 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

$$(x_1\ x_2\ \ldots\ x_J) \quad\text{and}\quad (y_1\ y_2\ \ldots\ y_K)\,.$$

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

$$(x_1\ y_2\ \ldots\ y_J\ \ y_1\ x_2\ \ldots\ x_K)\,,$$

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

Proof continued. Observe that (‡) is (†) 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 $\tau_1\triangleright\tau_2\triangleright\cdots\triangleright\tau_M$ of transpositions. Then M is even/odd, as β is an even/odd permutation. Indeed, the sign-map is group-homomorphism,*

$$\mathrm{Sgn}:\ \big(\mathbb{S}_\Omega,\ \triangleright,\ Id_\Omega\big)\ \to\ \big(\{\pm1\},\ \cdot\ ,\ 1\big)\,,$$

i.e, $\mathrm{Sgn}(\alpha\beta)\ =\ \mathrm{Sgn}(\alpha)\cdot\mathrm{Sgn}(\beta)$. ♢

Pf. This is immediate from (2†,‡), 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

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

ISTShow, given a transposition τ, that

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

This holds when τ is an "adjacent-transposition"; of form $(i\ \ i{+}1)$: *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 $(k\ \ k{+}n)$ is a composition of oddly many, $2n-1$, adjacent-transpositions.

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

[♡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 $\beta\triangleright(y\ x)$ fixes at least one more token than did β, hence is a composition of transpositions.

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

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. ♦

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*

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

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

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

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

Proof. $N = 2H$ ♦

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

$$\dagger: \qquad {}^{\#}\mathrm{Ev}(\boldsymbol{\pi}) \ \equiv \ \mathcal{E}_1\mathcal{D}_2 \ + \ \mathcal{D}_1\mathcal{E}_2$$
$$\ddagger: \qquad \equiv \ \mathcal{E}_1 N_2 \ + \ N_1\mathcal{E}_2\,,$$

where $N_j := |\Omega_j|$. ◊

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 $\boldsymbol{\pi}$-cycle of length

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

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

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

many length-L $\boldsymbol{\pi}$-cycles. These contribute to $\mathrm{Sgn}(\boldsymbol{\pi})$ **iff** L is even *and* G is odd; i.e, when $K_1 \not\equiv K_2$. Hence (†). Evidently $\mathcal{D}_j \equiv N_j$ (Why?), giving (‡). ♦