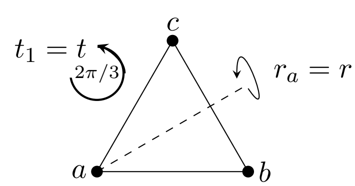
NOTES ON GROUPS, MATH 369.101

Symmetries of P_3, continued

Recall that we have a group $(D_3, \circ)$ of symmetries (each of which is a bijective function) of an equilateral triangle P_3 ($\circ$ denotes composition of functions). Since $\circ$ is an operation of a group we will write $x * y$ for $x \circ y$.

We used t_1, t_2 to write the symmetry that rotates the triangle counter-clockwise by $2\pi/3$, $4\pi/3$ respectively.

For the symmetries which reflect the triangle about the angle bisector at corner a, b or c we wrote r_a, r_b and r_c respectively. And we used e for the map that fixes every point.



Among other identities, we saw that:

$$t_1 * r_a = r_c, \quad t_2 * r_a = r_b, \quad r_a * r_b = t_1,$$
$$t_1 * t_1 = t_2, \quad t_2 * t_1 = t_1 * t_2 = e, \quad r_a * r_a = e.$$

While there are other products to consider in order to fill out the multiplication table for the group D_3, let's see that we already have enough information.

Write simply $t = t_1$ and note (from the equalities above) that $t^2 = t_2$ and $t^3 = e$.

Write simply $r = r_a$ and note that $r^2 = e$.

In addition, we have $tr = r_c$ and $t^2 r = t_2 * r_a = r_b$. And so, t_2, r_b and r_c can be written in terms of $t = t_1$ and $r = r_a$.

Also, we have that $r_a * t_1 = r_a * (r_a * r_b) = (r_a * r_a) * r_b = r_b$. But, since $r_b = t_2 * r_a = t^2 r$, this means that

$$rt = t^2 r.$$

Date: Oct. 31.

We claim that we have everything we need to make any computation in D_3. Notice that:

$$t_1 * r_a = tr = r_c;$$
$$t_1 * r_b = t(t^2 r) = r = r_a;$$
$$t_1 * r_c = t^2 r = r_b.$$

Also, if x is any of r_a, r_b, or r_c then $t_2 * x = t_1 * (t_1 * x)$ and the above three equalities tell us what to do.

Since $rt = t^2 r$, we can also convert anything (for $x = r_a, r_b$, or r_c) of the form $x * t_1$ to $(t_1)^2 * x$ and convert $x * (t_1)^2 = (t_1)^4 * x = t_1 * x$, and we know each of these elements.

Finally, $r_b * r_c = t^2(rt)r = t^4 r^2 = t$ and $r_c * r_a = tr^2 = t$. And also $r_a * r_c = rtr = t^2$, $r_b * r_a = t^2 r^2 = t^2$, and $r_c * r_b = trt^2 r = t(r^2)t = t^2$.

We have now computed every possible product of two elements (excluding those involving e). The group generated by r, t can be described by:

$$D_3 \cong \langle r, t \mid r^2 = e, t^3 = e, rt = t^2 r \rangle.$$

The right side means: everything is a (possibly multiple times) product of r and/or t and their inverses, and every equation in the group arises from the three on the right (using associativity).

(We have not carefully proved this. We will soon discuss isomorphisms of groups. Then one can define an isomorphism from $\langle r, t \mid r^2 = e, t^3 = e, rt = t^2 r \rangle$ to D_3 by setting $\varphi(r) = r_a$ and $\varphi(t) = t_1$. These two assignments, for an isomorphism, force all the others: e.g. $\varphi(rt) = r_a * t_1 = r_b$.)

Exercise: Explore the group $(D_4, \circ)$ of symmetries of a square P_4 (there are eight elements in this group, and they are each a rotation or a reflection, or the identity).

Permutations and the symmetric group S_n

Take a set, S. A **permutation** of S is a bijection (a one-to-one and onto function) $S \to S$. The set of all permutations of S is written $\mathrm{Sym}(S)$.

(Note: a symmetry of a polygon P – or any other shape – is an element of $\mathrm{Sym}(P)$.)

Mostly we will discuss the situation when S is finite. In this case we can simply name the elements of S with numbers $\{1, 2, \ldots, n\}$ for some integer $n > 0$. In this case, that $S = \{1, 2, \ldots, n\}$, we use the notation S_n for $\mathrm{Sym}(S)$.

Proposition 1. *For any set S, Sym(S) with the operation of function composition is a group. In particular S_n is a group.*

Proof. First, we check that the composition of two permutations is a permutation. In other words, if φ and ψ are in $\mathrm{Sym}(S)$ then we need that $\varphi \circ \psi : S \to S$ is one-to-one and onto. We will leave out this routine check.

Composition of functions is always associative, so the operation is associative.

Recall that two functions f, g are equal if they have the same domain and target (codomain) and if $f(x) = g(x)$ for all x in the domain.

Let $e : S \to S$ be the function defined by $e(s) = s$ for all $s \in S$. Then e is one-to-one and onto and so in $\mathrm{Sym}(S)$. Moreover, for any $\varphi \in \mathrm{Sym}(S)$

$$\varphi(e(s)) = \varphi(s) \qquad \text{and} \qquad e(\varphi(s)) = \varphi(s)$$

for all $s \in S$. This means $\varphi \circ e = \varphi = e \circ \varphi$. So $e : S \to S$ is the identity under composition.

For $\varphi \in \mathrm{Sym}(S)$, define $\varphi^{-1} : S \to S$ by $\varphi^{-1}(s) = r$, for $s \in S$, if $s = \varphi(r)$. This indeed defines an element of $\mathrm{Sym}(S)$ because for every $s \in S$, there is a unique $r \in S$ with $s = \varphi(r)$, since φ is one-to-one and onto.

Then we have $\varphi \circ \varphi^{-1} = \varphi^{-1} \circ \varphi = e$ as these functions agree on every $s \in S$. □

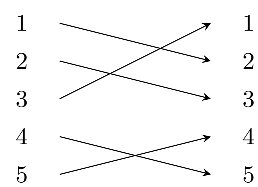
We will often use σ and τ for permutations in S_n, and remember that $\sigma(i)$, for $i \in \{1, 2, \ldots, n\}$, is the number to which i is sent by σ.

We will also drop the composition notation $\circ$ and instead just write $\sigma\tau$ to mean $\sigma \circ \tau$. Note that this means τ is applied first, then σ.

Notation: For $\sigma \in S_n$, write

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & \ldots & n \\ \sigma(1) & \sigma(2) & \sigma(3) & \ldots & \sigma(n) \end{pmatrix}.$$

For example, $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix}$ is in S_5. Represented as a function we can write:



Exercises:

(1) Find $\sigma\tau$ if

$$\tau = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 2 & 3 & 1 & 5 & 4 \end{pmatrix} \qquad \text{and} \qquad \sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 \\ 4 & 2 & 3 & 1 & 5 \end{pmatrix}.$$

(2) Let $\sigma \in S_3$ be as below. Check that $\sigma^3 = e$.

$$\sigma = \begin{pmatrix} 1 & 2 & 3 \\ 2 & 3 & 1 \end{pmatrix}.$$

Definition 1. If $\sigma \in S_n$ and there are numbers $a_1, a_2, \ldots, a_k \in \{1, 2, \ldots, n\}$, no two of which are the same, so that $\sigma(a_i) = a_{i+1}$ for $1 \le i \le k-1$ and $\sigma(a_k) = a_1$, then $(a_1, a_2, \ldots, a_k)$ is called a **cycle of length** k.

Exercise: Find all the cycles of the permutation

$$\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 & 11 & 12 \\ 8 & 2 & 10 & 11 & 5 & 9 & 4 & 6 & 1 & 3 & 12 & 7 \end{pmatrix}$$