Involute decomposition

written by Kinshuk Banik on Functor Network
original link: https://functor.network/user/3092/entry/1270

So this problem was proposed by a professor in a class yesterday. Here's my solution up for people to read, ponder, speculate, comment, critique, improve, and digress on.

Problem

Given any set X, and a bijection $f : X \to X$, there are functions $g, h : X \to X$ such that $f = h \circ g$ and $g^2 = h^2 = \mathrm{id}_X$, the identity function. ## Solution

Definitions, assumptions, and set-outs We accept the Axiom of Choice and use it freely. We define a function $f : A \to B$ as follows:

$$f := \{(a, b) \in A \times B \quad | \quad \forall a \in A,\ \exists! b \in B\}.$$

Here for each $a \in A$, the corresponding $b \in B$ is usually denoted by $f(a)$. A *restriction* of a function to a certain subset $A' \subseteq A$ of the domain A is defined as $f|_{A'} := \{(a, f(a)) \mid a \in A'\}$. In the context of this problem, all the domains and codomains we consider will be assumed to be non-empty.

Definition (Cycle). A bijection $\sigma : A \to A$ with $|A| = n$ is called a *cycle* if there is a bijection $\phi : \{1, \ldots, n\} \to A$ such that $\sigma(\phi(k)) = \phi(k+1)$ for all $k < n$ and $\sigma(\phi(n)) = \phi(1)$.

Definition (Iterated composition). For bijection $\phi : A \to A$, we define $f^0 := \mathrm{id}_A$, the identity function on A and for each $k \in \mathbb{N}$, we define $f^k := f \circ f^{k-1}$. Moreover for any $k \in \mathbb{N}$, we define $f^{-k} := f^{-1} \circ f^{-k+1}$.

Definition (Orbit). Given a function $\phi : A \to A$, and some $a \in A$, the orbit of a under ϕ is defined by $\mathrm{orb}_f(a) = \{f^k(a) \mid k \in \mathbb{Z}\}$.

Lemma 1. If a function $\phi : M \to N$ is bijective, then for any $P \subseteq M$, the restriction $\phi|_P$ is also bijective. *Proof.* First we see that $\phi|_P$ has to be injective, because $\forall x \neq y \in M,\ \phi(x) \neq \phi(y)$, hence too $\forall x \neq y \in P \subseteq M,\ \phi(x) \neq \phi(y)$. We can also see that $\phi|_P$ surjective right by its definition, since for every $\phi(p) \in \mathrm{Im}(\phi|_P)$, there is $p \in M$ such that $(p, \phi(p)) \in \phi|_P$.

Lemma 2. For any collection of bijections

$$\mathcal{C} = \{f_\lambda : A_\lambda \to B_\lambda \mid \forall \lambda \in \Lambda,\ f_\lambda \text{ is bijective}\}$$

with all A_λ pairwise disjoint and all B_λ pairwise disjoint, the union function

$$f := \bigcup_{\lambda \in \Lambda} f_\lambda : \left(\bigcup_{\lambda \in \Lambda} A_\lambda \right) \to \left(\bigcup_{\lambda \in \Lambda} B_\lambda \right)$$

is also bijective.

Proof. First we show that it is injective. Suppose $x \neq y \in A := \bigcup_{\lambda \in \Lambda} A_\lambda$. Clearly if $x \in A_\mu$ and $y \in A_\nu$ with $\mu \neq \nu$ then $B_\mu \ni f(x) \neq f(y) \in B_\nu$. If $x, y \in A_\lambda$, then since f_λ is injective, we have $f(x) \neq f(y) \in B_\lambda$. Therefore we have f being injective. Now we show that f is surjective. Consider any $y \in B := \bigcup_{\lambda \in \Lambda} B_\lambda$. Then $y \in B_\Lambda$ for some $\lambda \in \Lambda$. Now since f_λ is surjective, there is $x \in A_\Lambda \subseteq A$ such that $y = f(x)$, and hence f is surjective too, and therefore bijective.

Lemma 3. (Group theoretic) Given $S_n = \{1, 2, \ldots, n\}$ any permutation $\sigma : S_n \to S_n$ can be written as a composition of disjoint cyclic permutations. *Proof.* This proposition is well-known and we accept it without explicit proof here.

Solutions, step by step Finite set case

First we show that the proposition holds for any finite set X. So without loss of generality, we take $X := \{1, 2, \ldots, n\}$ with some $n \in \mathbb{N}$. So what we do is that we show this for all $n \in \mathbb{N}$ with any bijection $f : X \to X$. For $n = 1$, there is nothing much to be done, $X = \{1\}$ and $f = \{(1, 1)\}$. So for the decomposition, $g = h = f$ is the only choice. Suppose we have such a decomposition for any bijection of size upto $n \in \mathbb{N}$. Now consider $X = \{1, 2, \ldots, (n+1)\}$. Then if there is any cycle $\sigma_k \subset f$, with of course $k \leq n$, then σ_k being a bijection, we can write $f = \sigma_k \cup (f \setminus \sigma_k)$ as the union of two distinct bijections of size smaller than $(n+1)$ (by **Lemma 1**), which therefore can be decomposed (by induction hypothesis) into $\sigma_k = h_1 \circ g_1$ and $(f \setminus \sigma_k) = h_2 \circ g_2$, with all four functions satisfying the requirements, i.e. $f_1^2, f_2^2, g_1^2, g_2^2$ all being identities on respective sets. So now by **Lemma 2** we can have the two required functions $g, h : X \to X$ being $g = g_1 \cup g_2$ and $h = h_1 \cup h_2$. The only case left is when there is no such smaller cycle in the function. By **Lemma 3** we can see that this is only possible if f is itself a cycle. This can be broken down into two very similar but slightly different cases, namely for $(n+1)$ being even, and odd, respectively. **Case 1.** If $(n+1)$ is even, say $2m$, then we construct $g, h : X \to X$ as follows:

$$\begin{cases} g(2m) = 2m, \ g(m) = m \\ g(k) = 2m - k, \quad \forall k \neq m, 2m \end{cases} \qquad \text{and} \quad h(k) = 2m + 1 - k, \forall k \in X.$$

It should be clear enough that these two indeed follow the conditions as required. **Case 2.** If $(n+1)$ is odd, say $2m+1$, then the construction is as follows:

$$\begin{cases} g(2m) = 2m + 1, \ g(2m+1) = 2m \\ g(m) = m \\ g(k) = 2m - k \quad \forall k \neq m, 2m, 2m+1 \end{cases} \qquad \text{and} \qquad \begin{cases} h(2m+1) = 2m + 1 \\ h(k) = 2m + 1 - k \quad \forall k \neq 2m + 1 \end{cases}$$

Again it should be clear enough that these satisfy both requirements. And with this we have finished the induction, and therefore the proof of the proposition for the case of a finite set.

Countably infinite case

Now we show that the proposition holds for a very special countably infinite case. The more general cases will be dealt with in the final solution. So the case here is when X is of the form $X = \{\dots, x_{-1}, x_0, x_1, \dots\}$, indexed by $\mathbb{Z}$, with all x_i distinct, where for any $k \in \mathbb{Z}$, $x_k = f^k(x_0)$. This is indeed an orbit of the function where we not only consider the sequence of composing f on x_0, but also the sequence "backtracking" from x_0. The instances where anywhere in the composition sequence or the "backtracking" sequence there is a loop or cycle, will not be considered in this case and will instead be dealt with only in the final general case. So with the outset aside, the construction of the functions $g, h : X \to X$ is as follows:

$$\forall n \in \mathbb{Z}, \quad g(x_n) = x_{-1-n} \quad \text{and} \quad h(x_n) = x_{-n}.$$

This too is left to the consideration of the reader to see why this construction satisfies the requirements of the proposition.

The final solution

Given the set X and a bijection $f : X \to X$ on it, we consider the following equivalence relation first. We define $(\sim) \subseteq X \times X$ by $x \sim y$ (or alternatively $(x, y) \in (\sim)$) if and only if there is $k \in \mathbb{Z}$ such that $f^k(x) = y$. Now we consider the set of all equivalence classes (the set of all distinct orbits of f) $X/\sim$ such that, for all $C, D \in X/\sim$ with $C \neq D$, we have $C \cap D = \varnothing$, and that $\bigcup(X/\sim) = X$ (since the set $X/\sim$ is just a partition of X), and that for any $C \in X/\sim$, we have $x, y \in C \iff x \sim y$.

So now we have a closer look at each $C \in X/\sim$. Notice that $C \subseteq X$, and that it is of one of two forms. The first is when C is a finite orbit, and $C = \{x_0, \dots, x_n\}$ for some $n \in \mathbb{W}$, where $x_1 = f(x_0)$, $x_2 = f(x_1)$, and so on, with $x_0 = f(x_n)$. Notice that this also includes the case of the fixed points of f, where we do not go beyond x_0. The second is when C is countably infinite, in particular, we index it with the integers, as $C = \{\dots, x_{-2}, x_{-1}, x_0, x_1, x_2, \dots\}$. Here for any $n \in \mathbb{Z}$, $f(x_n) = x_{n+1}$. It is easy to see that since f is bijective, if we start from any "first" element, we will always have more equivalent elements (of X) by taking repeated inverses. We claim that these two are the only possibilities, namely that any such infinite $C \in X/\sim$ can always be indexed by the integers, and moreover that C cannot be uncountable. Both of these claims are easy to show, since, by choosing any $x_0 \in C$, if $x \in C$, then there is $k \in \mathbb{Z}$ such that $f^k(x_0) = x$, so we can uniquely assign the index k to that x, since f is injective. This also removes the possibility of C being uncountable because we have demonstrated a surjection $\mathbb{Z} \twoheadrightarrow C$. So therefore we have shown, rather argued, that any equivalence class $C \in X/\sim$ is countable.

Now consider the following set of restrictions of the function

$$\mathfrak{R}_f := \{f|_C \ : \ C \in X/\sim\}.$$

Each $f|_C$ is bijective, as can be easily checked by the definition of each class C. And since each distinct C is disjoint, we can see (by the way we have defined a function as a set of pairs) that

$$f = \bigcup_{C \in X/\sim} f|_C.$$

Now, to finish off the problem, notice that we have already solved it for bijections over any finite set and any countably infinite acyclic chain in the previous two cases. So using those results, we see that for each $C \in X/\sim$, there are $g_C, h_C : C \to C$ such that $h_C \circ g_C = f|_C$ and $g_C^2 = h_C^2 = \mathrm{id}_C$. So now we define the final two required functions g, h over X as

$$g = \bigcup_{C \in X/\sim} g_C \quad \text{and} \quad h = \bigcup_{C \in X/\sim} h_C.$$

Notice that these functions do really follow these properties, as can be easily checked.

Therefore, given any X, and bijection $f : X \to X$, we can decompose f into two self-inverse bijections $g, h : X \to X$, i.e. with $g^2 = h^2 = \mathrm{id}_X$ such that $f = h \circ g$.

QUOD ERAT DEMONSTRANDUM.