Definition 0.0.1 (Groupoid)**.** Let G be a set. We say that G together with a binary operation $*$ is a *(left) cancellative groupoid*, if

(i) $\forall g, h \in G \quad g * h \in G$

(ii) $\forall g, h, k \in G \quad (g * h = k * h) \to g = k$

Analogously $(G, *)$ is called right cancellative if we replace condition (ii) by $\forall g, h, k \in G\ (g * h = g * k) \to h = k$.

Let $\mathcal{L} = \{*\}$ be the language containing only the binary function $*$. Then an $\mathcal{L}$-structure M is a model of a cancellative groupoid, if and only if it satisfies the theory given by conditions (i)-(ii).

An example of a cancellative groupoid (without identity and which is not a group) is the positive integers $\mathbb{Z}^+$ under addition.

We now finally arrive at our main theorem. Note that in the proof of Theorem 0.0.2 it is not important weather a groupoid is left or right cancellative, but rather that it has some form of the cancellation property. In our case we choose to utilize a right cancellative groupoid.

Theorem 0.0.2. *[1] The following are equivalent in ZF:*

1. *The Axiom of Choice*

2. *Every non-empty set admits a cancellative groupoid structure*

Proof. The theorem is proven in two steps, deriving a single direction implication for each sentence.

1. **Groupoid Structure on arbitrary sets $\implies$ Axiom of Choice**

   We show that the existence of a groupoid structure on every non-empty set implies that every set can be well-ordered. By Theorem **??** this is equivalent to the Axiom of Choice.

   Let A be an arbitrary set and let α be an ordinal as described in Theorem **??** in Section **??**. This means that there exists no bijective mapping from α to any subset of A (including A itself). We then let (B, R) be a well-ordered set of type α and such that $A \cap B = \emptyset$.

   Now let C be the set $C = A \cup B$, by assumption there exists some operation $+$, such that $(C, +)$ is a cancellative groupoid. We will show that for every $x \in A$ there exists $y \in B$, such that $x + y \in B$ holds.

   Let us assume for a contradiction that the above claim does not hold. This would imply that some $a \in A$ exists for which $a + y \in A$ holds for all $y \in B$. Let $f : B \to A$ be the function defined by $f(y) = a + y$. We have that $+$ is a cancellative groupoid operation, hence f must be injective; a contradiction by Theorem **??**, since we had assumed that B is of type α.

We let $D = B \times B$ be the well-ordered set with respect to the lexicographical ordering R' of R, and define a function $g : A \to D$ by

$$g(x) = \min_{R'} \{ \langle u, v \rangle \in D \,|\, x + u = v \} .$$

The function g maps every element x of A to the least pair $\langle u, v \rangle$ in $B \times B$ satisfying $x + u = v$. From earlier in the proof we know that such a pair must exists and that g must in fact be injective. This again follows from + being cancellative, since if x_1, x_2 are two elements of A, having $f(x_1) = f(x_2)$ would imply that

$$\begin{aligned} x_1 + u = & \quad v \quad = x_2 + u \\ \iff \qquad x_1 = & \; v + u^{-1} = x_2 \end{aligned}$$

for some pair $\langle u, v \rangle \in D$. Since $\mathbf{Im}(g)$ is a subset of D it itself is a well-ordered set. As such we can define a well-order R'' on A by letting $x_i R'' x_j$ whenever $g(x_i) R' g(x_j)$.

2. **Axiom of Choice $\implies$ Groupoid Structure on arbitrary sets**

Let A be a finite set with n elements. Then we can imbue A with the structure of the cyclic group $\mathbb{Z}_n$, since every group is also a cancellative groupoid. Similarly, if A is countably infinite there exist a bijection to the set of integers $\mathbb{Z}$. Hence we can let A have the group structure $(\mathbb{Z}, +)$ of integers under addition.

Finally, since there exists a countably infinite model of a cancellative groupoid, we can apply Theorem **??**. By this there also exist models of arbitrary infinite powers.

Therefore it is possible to define a cancellative groupoid structure on every arbitrary set A. ◻