Group theory without groups

Pierre Cagne[1]

Last updated on August 25, 2022

These notes are supporting the colloquium given at the HoTTEST Summer School 2022. They present a synthetic version of group theory by taking advantage of two key aspects of HoTT: the built-in types of identifications and the univalence axiom.

According to popular belief, Henri Poincaré would have said to Sophus Lie:

> *Tout en mathématique est histoire de groupes.*[2]

But if we look more closely to what Poincaré considered a group back then, it is safe to assume that he meant that "all in mathematics is a tale of symmetries". If you have no preconcieved idea about goup theory and you are tying to read the seminal work of Klein, Lie and Poincaré, or the precursor ideas of Riemann and Galois, this is the picture you will see emerge: a group is a collection of symmetries *of some mathematical object* that play well together. Ordinary group theory tends to relegate the part in *emphasis* to a subordinate role. The goal of the approach presented in these notes is to make the *mathematical object* of which we are studying the symmetries the primitive notion, and not the other way around. This is by no mean a novel ideal, and this has been implemented by algebraic topologists for decades. However, I want to convey that univalent foundations allow for a formal rigorous encoding of this way of thinking, making group theory more akin to what the founders of groups were thinking of.

These notes are an invitation for the reader to dive deeper into the subject with the work-in-progress book "Symmetry" [Bez+22]. The book addresses undergraduate students with a strong curiosity for mathematics, and does not require knowledge about either ordinary group theory nor univalent type theory. People that have been following the HoTTEST Summer School 2022 are then more than well-equipped to read the book.

HoTT has built-in symmetries

In a type A, each element a comes with the type of identifications $a = a$. The elements of $a = a$ are called the *symmetries* of a in A. This is not just a game of naming convention. Take your favorite type constructed in class and explore the type of identifications from a element to itself and you'll most likely be describing a symmetry in the intuitive sense. For example, describe the elements of $2 = 2$ in the universe $\mathcal{U}$, where 2 denote the set with two elements, 0 and 1. Through the univalence axiom, you can completely describe these elements: there is refl_2 and the identification that corresponds through univalence to the equivalence swapping the two elements.

[1] Appalachian State University, pierre.cagne@gmail.com

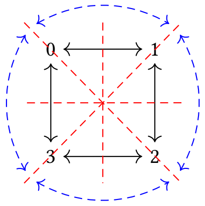
[2] Rough translation: All in mathematics is a tale of groups.

For a more geometric example, define the type of graphs to be

$$\mathrm{Graph} :\equiv \sum_{V:\mathcal{U}} (V \to V \to 2)$$

Then consider the square S, that is the graph whose first projection is the set $V :\equiv 4$ with 4 elements (0, 1, 2 and 3), and whose second projection is the function $e: 4 \to 4 \to 2$ defined by

$$e\;0\;2 :\equiv 0, \quad e\;2\;0 :\equiv 0, \quad e\;1\;3 :\equiv 0, \quad e\;3\;1 :\equiv 0, \quad e\;i\;i :\equiv 0, \quad e\;i\;j :\equiv 1 \text{ otherwise}$$



What are the symmetries of S? By definition it is a identification $\sigma : S = S$ in the type of graphs. By using the description of identification of dependent sums, σ is equivalently given by a pair of identifications $\sigma_1 : 4 = 4$ and $\sigma_2 : trp_{\sigma_1}\, e = e$. The transport involved in σ_2 is the transport in the type family $V \mapsto (V \to V \to 2)$. Now, by univalence, we know that σ_1 is equivalently an equivalence $\widetilde{\sigma_1} : V \simeq V$. By induction, prove that there is an identification $(trp_p\, f)\; i\; j = f\,(\tilde{p}^{-1}\; i)\,(\tilde{p}^{-1}\; j)$. This is proven by instantiating $p \equiv refl_V$ and recalling that $\widetilde{refl_V} \equiv \mathrm{id}_V$. In the end, the symmetry σ is equivalently given by an equivalence $\widetilde{\sigma_1} : 4 \simeq 4$ together with an identification $e\; i\; j = e\,(\widetilde{\sigma_1}\; i)\,(\widetilde{\sigma_1}\; j)$ for all $i, j : 4$. In other words, a symmetry of the square is a permutation of its vertices such that two vertices are connected by an edge if and only if their images are. These are exactly what we intend to call symmetry for such a square: they are the axis symmetries in red and the blue rotations in the drawing.

The structure of the type of identifications

Not only are symmetries built-in in HoTT, but so is their expected behaviour. You have seen in the course that the type $a = a$ contains a specific element $refl_a$, and that you can define functions $\_^{-1} : (a = a) \to (a = a)$ and $\_ \cdot \_ : (a = a) \to (a = a) \to (a = a)$ by $=$-induction. You also have seen that you have dependent functions $lunit : \prod_{p:a=a} refl_a \cdot = p$, $runit : \prod_{p:a=a} p \cdot refl_a = p$, $linv : \prod_{p:a=a} p^{-1} \cdot p = refl_a$, $rinv : \prod_{p:a=a} p \cdot p^{-1} = refl_a$, and $ass : \prod_{p,q,r:a=a} (p \cdot q) \cdot r = p \cdot (q \cdot r)$, again defined by $=$-induction. Let me insist on the fact that these functions are obtained by $=$-induction, and thus need the full definition of the type of identifications $a = b$ for generic $a, b : A$.

Those acquainted to ordinary group theory will notice that this is very reminiscent of the usual definition of groups if we replace $refl_a$ by the neutral element and $\cdot$ by the multiplication operation. Indeed, the definition of groups in ordinary mathematics, called *abstract groups* in these notes to differentiate from the objects we will call groups later, is as follows: an *abstract group* is a set $\mathcal{G}$ together with elements

$$1 : \mathcal{G}, \quad 1/\_ : \mathcal{G} \to \mathcal{G}, \quad \_\times\_ : \mathcal{G} \to \mathcal{G} \to \mathcal{G}$$

satisfying the following axioms

$$\begin{aligned} 1 \times x &= x && \text{for all } x\colon \mathcal{G} \\ x \times 1 &= x && \text{for all } x\colon \mathcal{G} \\ (1/x) \times x &= 1 && \text{for all } x\colon \mathcal{G} \\ x \times (1/x) &= 1 && \text{for all } x\colon \mathcal{G} \\ x \times (y \times z) &= (x \times y) \times z && \text{for all } x, y, z\colon \mathcal{G} \end{aligned}$$

The main difference between an abstract group and $(a = a)$ is that the dependent functions *lunit*, *runit*, *linv*, *rinv*, and *ass* are simply statements in the case of an abstract group. This is due to the fact that their target types are propositions. So, if one require $a = a$ to be a set (in the sense of HoTT), one recover exactly the structure of an abstract group.

Connectedness

You have seen with Egbert the notion of truncation. Recall that for each type A, we can form a type $\|A\|$ which is the "universal proposition made from A". It means that $\|A\|$ is a proposition, and that there is a map $|\_|\colon A \to \|A\|$ such that mapping out of $\|A\|$ into a proposition P is fully determined by the image of $|a|$ in P for each $a\colon A$.

Deriving from it is the notion of connectedness. A type A is said to be connected when A is not empty and we have an element of the proposition $\mathrm{isConn}A :\equiv \prod_{a,a'\colon A} \|a = a'\|$. This is read as "every element is merely equal to any other". Note that this is very different from the notion of contractibility where "every element is effectively equal to any other". Connectedness is typically used as follows: given a family of propositions $P\,a$ indexed by $a\colon A$ and a specific point $a_0\colon A$ for which $P\,a_0$ can be proved true "easily"; you can invoke connectedness to show that Pa holds for all $a\colon A$. Indeed, given $a\colon A$, you are trying to provide an element in $P\,a$ from an element $w\colon \|a_0 = a\|$; but because the goal $P\,a$ is a proposition, it is enough to provide such an element when w is of the form $|p|$ for $p\colon a_0 = a$. This is easy enough as we can associate to each $p\colon a_0 = a$ the element $\mathit{trp}_p\, x_0\colon P\,a$ where x_0 is the element proving $P\,a_0$ mentioned above.

Examples of connected types include any contractible type of course, but also other typical types that you have seen during the course such as the circle. Recall that S^1 is a type containing an element $\bullet\colon S^1$ and a symmetry $\circlearrowleft\colon \bullet = \bullet$ such that for any type family $T\colon S^1 \to \mathcal{U}$, the choice of a dependent pair $(x, \ell)\colon \sum_{y\colon T\,\bullet} y =_{\circlearrowleft} y$ determines fully a dependent function $f\colon \prod_{c\colon S^1} T\,c$ such that $f\,\bullet \equiv x$ together with an identification $\mathit{ap}_f \circlearrowleft = \ell$. Informally, S^1 is the "free type with a symmetry". Because we already have a specific point $\bullet$ in S^1, proving that S^1 is connected is equivalent to providing a dependent function $\prod_{c\colon S^1} \|\bullet = c\|$. Using the property just described, it amounts to give an element $x\colon \|\bullet = \bullet\|$ and an identification $\ell\colon x =_{\circlearrowleft} x$ over $\circlearrowleft$. Take $x :\equiv |\mathit{refl}_\bullet|$, and choose for ℓ the element in $\mathit{trp}_{\circlearrowleft}\, x = x$ given by the fact that both side are element of the proposition $\|\bullet = \bullet\|$, and you are done!

The notation $t_0 =_p t_1$ applies in the context of a type family $T\colon A \to \mathcal{U}$, where $t_0\colon T\,a_0$, $t_1\colon T\,a_1$, and $p\colon a_0 = a_1$. It is the type of identifications from t_0 to t_1 over p, and it is equivalent to the type of identifications $\mathit{trp}_p t_0 = t_1$ in $T\,a_1$.

Definition of groups

We define a group to be essentially a 1-truncated pointed connected type. However, we must take some precautions. Let us first define:

$$\mathscr{U}_*^{=1} :\equiv \sum_{A:\mathscr{U}} A \times \mathrm{isConn} A \times \mathrm{isGrpd} A$$

where $\mathrm{isGrpd} A$ denotes the proposition $\prod_{x,y:A} \mathrm{isSet}(x = y)$. Notice that under the hypothesis $\mathrm{isConn} A$, then $\mathrm{isGrpd} A$ is equivalent to $\mathrm{isSet}(a = a)$ for any choice of $a\colon A$. So that the type above can be rewritten as:

$$\mathscr{U}_*^{=1} \simeq \sum_{A:\mathscr{U}} \sum_{a:A} \mathrm{isSet}(a = a) \times \prod_{x:A} \|a = x\|$$

The notation $\mathscr{U}_*^{=1}$ contains the symbol $\mathscr{U}$ to refer to types, the symbol $*$ to refer to the pointedness, and the symbol "$= 1$" to refer to both the 1-truncatedness (≤ 1) and the connectedness (> 0).

A type A for which $\mathrm{isGrpd} A$ is inhabited is said to be a groupoid, or to be 1-truncated.

The type of groups is defined as a unary sum of $\mathscr{U}_*^{=1}$. That is, the type Group is defined inductively with a unique constructor $\underline{\Omega}\colon \mathscr{U}_*^{=1} \to \mathrm{Group}$ such that $\_ \circ \underline{\Omega}\colon (\mathrm{Group} \to A) \to (\mathscr{U}_*^{=1} \to A)$ is an equivalence for all type A. It is important to understand t

In particular, there is a (propositionally unique) map $\mathrm{B}\colon \mathrm{Group} \to \mathscr{U}_*^{=1}$ in the fiber at $\mathrm{id}_{\mathscr{U}_*^{=1}}$. There is an identification $\beta\colon \mathrm{B} \circ \underline{\Omega} = \mathrm{id}_{\mathscr{U}_*^{=1}}$ by definition, and there is an identification $\underline{\Omega} \circ \mathrm{B} = \mathrm{id}_{\mathrm{Group}}$ because both $(\underline{\Omega} \circ \mathrm{B}, \overline{x \mapsto ap_{\underline{\Omega}}\, \beta_x})$ and $(\mathrm{id}_{\mathrm{Group}}, \mathit{refl}_{\underline{\Omega}})$ are in the fiber of $\_ \circ \underline{\Omega}$ at $\underline{\Omega}$. All of that is a formal intricated way to say that Group is a "black box" that is also an exact copy of $\mathscr{U}_*^{=1}$. It is important to understand that Group is not a type constructed with type formers such as $\sum$ and $\prod$, it is a posited type with the given universal property above. Each connected 1-truncated type A, pointed at an element $a\colon A$, provides a group $\underline{\Omega}(A, a)$. We call (A, a) the classifying type of the group $\underline{\Omega}(A, a)$. Conversely, every group is of this form, and given $G\colon \mathrm{Group}$, there is always an identification $\underline{\Omega}\mathrm{B}G = G$

This corresponds as a "wrapper type" in Agda:

```
data Group : 𝒰 where
  Ω : 𝒰⁼¹ → Group
```

The type Group and its elimination rule are posited in the exact same sense that $\mathbb{N}$ and its elimination rule are posited.

Note that BG is a pointed type for any group $G\colon \mathrm{Group}$. It has a distinguished point, denoted sh_G, and called "the shape of G". We say that G is "the group of symmetries of sh_G". An important point is that any other element $s\colon \mathrm{B}G$ is as good as a shape for G, in the sense that $\|G = \underline{\Omega}(\mathrm{B}G, s)\|$ is inhabited. Indeed, to prove such a proposition, the connectedness of BG gives an identification $p\colon \mathrm{sh}_G = s$. Then the dependent pair $(\mathit{refl}_{\mathrm{B}G}, p)$ makes an identification $\pi\colon (\mathrm{B}G, \mathrm{sh}_G) = (\mathrm{B}G, s)$ in $\mathscr{U}_*^{=1}$, which in turn produces an identification $ap_{\underline{\Omega}}\, \pi\colon \underline{\Omega}\mathrm{B}G = \underline{\Omega}(\mathrm{B}G, s)$, leading to an identification $\varpi\colon G = \underline{\Omega}(\mathrm{B}G, s)$ by composition with the canonical identification $G = \underline{\Omega}\mathrm{B}G$, whose truncation $|\varpi|$ is the element we wanted to construct. For that reason, we call any $s\colon \mathrm{B}G$ "a shape of G".

We abusively consider the pointed type BG as a bare type when needed. For example, "$s\colon \mathrm{B}G$" is inaccurate and should formally be written as $s\colon \mathrm{pr}_1 \mathrm{B}G$. We find that it clutters the text too much and we trust the reader to coerce a pointed type to its underlying type when needed.

What you have to get out of this is that any group G is defined as the group $\underline{\Omega}(A, a)$ of symmetries of a mathematical object, namely a, in a given type, namely A. The set of symmetries defined by G is the set $\mathrm{U}G :\equiv (a = a)$, and this set can be equipped with the structure of an abstract group. But, we insist that the view we propose here makes the classifying type A and its element a the primitive notion. The set UG and its structure, while important, is the derived notion here. For those of you with background in algebraic topology, it would correspond to defining any group as the group of automorphisms of a homogeneous space.

A LOT OF INTERESTING TYPES ARE 1-TRUNCATED but are not connected, hence they can not serve as a basis to generate a group. However, if given an element of such a type, we can restrict our attention to its *connected component*, which is then an element of $\mathcal{U}_*^{=1}$. Recall that in any type A, the connected component of an element $a\colon A$ is the type $A_{(a)} = \sum_{x:A} \|a = x\|$. It is a subtype of A, in the sense that the first projection $A_{(a)} \to A$ induces equivalences on all identifications types. In particular, there is an implication $\mathrm{isGrpd} A \to \mathrm{isGrpd}\big(A_{(a)}\big)$. So, for a 1-truncated type A, we can define, for each element $a\colon A$, the group

$$\mathrm{Aut}_A\, a :\equiv \underline{\Omega}(A_{(a)}, (a, |\mathit{refl}_a|))$$

In particular, if A is already connected, we use indifferently $\mathrm{Aut}_A\, a$ and $\underline{\Omega}(A, a)$.

LET US KNOW TURN TO EXAMPLES OF GROUPS.

(i) Note that $\mathrm{Set} :\equiv \sum_{X:\mathcal{U}} \mathrm{isSet} X$ is 1-truncated. For each set S, the group $\mathrm{Aut}_{\mathrm{Set}}\, S$ is called the group of permutations on elements of S. Of particular interest are the groups $\Sigma_n :\equiv \mathrm{Aut}_{\mathrm{Set}}\, \mathrm{n}$ where n is the type with n elements you defined inductively in class. The group Σ_n is called the group of permutations on n elements. In other words, Σ_n is the group of symmetries of the finite set with n elements in the type of sets. These groups, or more precisely their classifying types, have been introduced by Egbert toward the end of his lectures.

Set is 1-truncated because the type $p = q$, for $p, q\colon X = Y$ and $X, Y\colon \mathrm{Set}$, can be identified through univalence and function extensionality with $\prod_{x:X} \tilde{p}\, x = \tilde{q}\, x$. This is a dependent product of propositions (as for all $x\colon X$, $\tilde{p}\, x$ and $\tilde{q}\, x$ are elements of the set Y), hence it is a proposition itself.

(ii) The group Σ_1 is also called the trivial group. Its classifying type $\mathrm{B}\Sigma_1$ is the type of those types that are merely equal to the type with one element. This is contractible, or in other words $\mathrm{B}\Sigma_1 = 1$, and Σ_1 is as well the group of symmetries of the unique element $*$ in 1. o

(iii) The group $\mathrm{Aut}_{S^1} \bullet$ is called the group of integers and is denoted $\mathbb{Z}$. In what sense exactly is it related to the brave old integers you know from your younger age? You have seen in the Agda track an overview of this relationship, namely that every element of $\mathrm{U}\mathbb{Z}$, which is $\bullet = \bullet$ by definition, is of the form $\circlearrowleft^k$ for some integer k. A proof of this fact is recalled later on in these notes, once we introduce a little more material about groups.

Construction of groups

THIS IS, IN MY OPINION, WHERE THIS APPROACH SHINES. I invite the knowledgeable reader to think about how a subgroup or a quotient group is defined in ordinary group theory: the elements of the newly constructed groups are described from the elements of the old one. It is non-obvious at all what is the mathematical object of which the newly constructed group is the group of symmetries. The approach presented here intends to correct this flaw.

ANOTHER MOTTO FOR THE THEORY PRESENTED HERE is: a group is better understood through its actions. One consequence of the identifications types in HoTT is that any function $f\colon A \to B$ provides a way to "simulate" the symmetries of a in A by symmetries of $f\,a$ in B. More precisely, you have seen that f induces a function $ap_f\colon (a = a) \to (f\,a = f\,a)$ that preserves *refl*, composition and inverses. This is exactly what we need to encode the notion of group action. For a group G: Group, define the type of G-actions in a type A as the type $\mathrm{B}G \to A$. Given such an action $f\colon \mathrm{B}G \to A$, we say that f is an action of G on $f \mathrm{sh}_G$. If H is another group, then an action f of G in $\mathrm{B}H$ together with an identification $p\colon \mathrm{sh}_H = f\,\mathrm{sh}_G$ allows to simulate symmetries of sh_G by symmetries of sh_H through the composite $p \cdot (ap_f\ \_) \cdot p^{-1}$. For this reason, the data of a map $f\colon \mathrm{B}G \to \mathrm{B}H$ together with an identification in $\mathrm{sh}_H = f\,\mathrm{sh}_G$ (also known as a *pointed map*) is called a homomorphism of groups.

ACTIONS OF A GROUP IN Set SUFFICE to understand the group completely, and we shall focus on these. Write G-Set for the type $\mathrm{B}G \to$ Set of actions of G in Set. Of importance is the following action $\mathrm{Pr}_G\colon s \mapsto (\mathrm{sh}_G = s)$. It is an action of G on the set $\mathrm{U}G$, and allows to "simulate" the symmetries of sh_G by symmetries of $\mathrm{U}G$. Those among you with background in ordinary group theory will recognize the usual action of a group on itself by multiplication, also called the principal torsor of G in geometric contexts. One crucial point of this approach is that there is an identification $p_G\colon G = \mathrm{Aut}_{G\text{-Set}}\ \mathrm{Pr}_G$. Indeed, we can generalize a bit the definition of the principal torsor to make it an action of G in G-Set as follows:

$$\mathrm{Pr}\colon \mathrm{B}G \to G\text{-Set}, \quad s \mapsto (s = \_)$$

Then the identification p_G will follow by univalence and application of $\underline{\Omega}$ as soon as we show that all fibers of $\mathrm{Pr}^{-1} X$ are contractible when X is in the connected component of Pr_G. Because being contractible is a proposition, it suffices to show that the fiber $\mathrm{Pr}^{-1}(\mathrm{Pr}_G)$ is contractible. The pair $(\mathrm{sh}_G, \mathit{refl}_{\mathrm{Pr}_G})$ is an element of this fiber; so it remains only to show that it is a center of contraction. For every $s\colon \mathrm{B}G$ together with an identification $h\colon \mathrm{Pr}_G = \mathrm{Pr}\ \ s$, we can consider the identification $(h\ \mathrm{sh}_G)\ (\mathit{refl}_{\mathrm{sh}_G})\colon s = \mathrm{sh}_G$. This provides an identification from (s, h) to $(\mathrm{sh}_G, \mathit{refl}_{\mathrm{Pr}_G})$.

The identifications type $(s, h) = (\mathrm{sh}_G, \mathit{refl}_{\mathrm{Pr}_G})$ in the fiber $\mathrm{Pr}^{-1}(\mathrm{Pr}_G)$ is equivalent to $\sum_{p:s=\mathrm{sh}_G} \mathit{trp}_p\, h = \mathit{refl}_{\mathrm{Pr}_G}$. The transport occurs in the type family $s \mapsto \mathrm{Pr}_G = \mathrm{Pr}\ \ s$, hence there is an identification $\mathit{trp}_p\, h = h \cdot (ap_{\mathrm{Pr}}\ p) = h \cdot \overline{p^{-1} \cdot \_} = ((x\colon \mathrm{B}G) \mapsto (q\colon \mathrm{sh}_G = x) \mapsto p^{-1} \cdot ((h\ x)\ q))$. For any identification $k\colon \mathrm{Pr}_G = \mathrm{Pr}_G$, one shows by path induction $(k\ s)p = p \cdot ((k\ \mathrm{sh}_G)\_\ \mathit{refl}_{\mathrm{sh}_G})$ for all $p\colon \mathrm{sh}_G = s$. So symmetries k, k' of Pr_G in G-Set are equal as soon as $((k\ \mathrm{sh}_G)\ \ \mathit{refl}_{\mathrm{sh}_G} = (k'\ \mathrm{sh}_G)\ \ \mathit{refl}_{\mathrm{sh}_G}$, which allow to reduce further $\mathit{trp}_p\, h = \mathit{refl}_{\mathrm{Pr}_G}$ to the equivalent type $p^{-1} \cdot (h\ \mathrm{sh}_G)\ \ \mathit{refl}_{\mathrm{sh}_G} = \mathit{refl}_{\mathrm{sh}_G}$. In other words, the type $(s, h) = (\mathrm{sh}_G, \mathit{refl}_{\mathrm{Pr}_G})$ is a singleton type.

LET US FOCUS HERE ON THE CIRCLE S^1 and the group $\mathbb{Z}$ that it generates. As promised, I shall now prove that $\mathrm{U}\mathbb{Z}$ is indeed in bijection with the integers, and that this bijection is given by $k \mapsto \circlearrowleft^k$. Define the G-set $Z\colon S^1 \to$ Set, by setting $Z\ \bullet$ to be the set of integers and $Z \circlearrowleft$ to be $\bar{s}$ where s is the "successor" equivalence, that is the bijection $Z\ \bullet \ \to\ Z\ \bullet$ that send every integer k to $k+1$. By the induction property of S^1, this is sufficient to fully define $Z\colon S^1 \to \mathcal{U}$. The key of the proof is to construct an identification $Z = \mathrm{Pr}_{\mathbb{Z}}$. For a given $c\colon S^1$, there is an obvious function $t_c\colon \mathrm{Pr}_{\mathbb{Z}}\ c \to Z\,c$, namely $p \mapsto \mathit{trp}^Z_p\, 0$. Conversely, there is $w_c\colon Z\,c \to \mathrm{Pr}_{\mathbb{Z}}\ c$ defined by setting $w_\bullet$ to be $k \mapsto \circlearrowleft^k$ and $ap_{\underline{w}}\ \circlearrowleft$ to be the unique identification $w_\bullet =_{\circlearrowleft} w_\bullet$. We want to show that t_c and w_c are inverse equivalences. By identification induction on $p\colon \bullet = c$, we get that $w_c(t_c\ p) = p$. Indeed, $w_\bullet(t_\bullet\ \ \mathit{refl}_\bullet) = \circlearrowleft^0 = \mathit{refl}_\bullet$. Now, by the induction property of S^1, proving that $t_c \circ w_c = \mathrm{id}_{Z\,c}$ for each c amounts to providing $h\colon t_\bullet \circ w_\bullet = \mathrm{id}_{Z\ \bullet}$ and an identification $\eta\colon h =_{\circlearrowleft} h$. The element h is given pointwise by

You can check that $w_\bullet =_{\circlearrowleft} w_\bullet$ is equivalent to $w_\bullet(\_ - 1) \cdot \circlearrowleft = w_\bullet$.

the identification $trp^{Z}_{\circlearrowleft^k}\,0 = (trp^{Z}_{\circlearrowleft})^k 0 = s^k\,0 = k$. Now notice that the type of h is a proposition, as $Z\,\bullet$ is a set, hence η is provided for free. In the end, we do have that $w_\bullet : k \mapsto \circlearrowleft^k$ is an equivalence (with inverse $t_\bullet$) from the set of integers to $\mathrm{U}\mathbb{Z}$. But notice that we actually did more. As announced, we have constructed an identification $\overline{w}\colon Z = \mathrm{Pr}_{\mathbb{Z}}$. So in particular, we have an identification $\mathrm{Aut}\,\mathbb{Z}\text{-Set}Z = \mathbb{Z}$, by applying $\mathrm{Aut}\,\mathbb{Z}\text{-Set}$ to $\overline{w}$ and composing with the identification ${p_{\mathbb{Z}}}^{-1}\colon \mathrm{Aut}\,\mathbb{Z}\text{-Set}\,\mathrm{Pr}_{\mathbb{Z}} = \mathbb{Z}$. This provides an alternative description of the circle: S^1 is equivalent to $\mathbb{Z}-\mathrm{Set}_{(Z)}$ and under this equivalence $\bullet$ is identified with the $\mathbb{Z}$-set Z. We can simplify further by noticing that $\mathbb{Z}\text{-Set} \equiv (S^1 \to \mathrm{Set})$ is equivalent, by the universal property of the circle and univalence, to $\sum_{X:\mathrm{Set}} X \simeq X$. In the end, writing $\mathsf{Z} :\equiv Z\,\bullet$ for the set of integers, it provides an equivalence of type

$$S^1 \simeq \sum_{X:\mathcal{U}} \sum_{\varphi:X\to X} \|(\mathsf{Z}, s) = (X, \varphi)\|$$

The identifications type $(\mathsf{Z}, s) = (X, \varphi)$ takes place in the type $\sum_{X:\mathcal{U}} X \to X$. In particular, $\|(\mathsf{Z}, s) = (X, \varphi)\|$ implies that X is a set and φ an equivalence, so that the right hand-side in the displayed equality is equivalently written as $\sum_{X:\mathrm{Set}} \sum_{\varphi:X\simeq X} \|(\mathsf{Z}, s) = (X, \varphi)\|$.

For those of you with knowledge about ordinary group theory, you might know see why the theory exposed here is indeed group theory and not some new kind of theory with a vague analogy with group theory. We defined groups and groups homomorphisms, and you can check that there is a (univalent) category of groups, denoted $\mathcal{G}roup$ in the following. We can as well define a (univalent) category $\mathcal{A}bs\mathcal{G}roup$ whose objects are the abstract groups and their morphisms the homomorphisms of such defined in ordinary group theory. This is not the focus of these notes, so I'll skip over the proper definitions here. The interested reader can check [Bez+22] for the rigorous details. However, the function U from groups to abstract groups that associates to G: Group the set $\mathrm{sh}_G = \mathrm{sh}_G$ with its structure of abstract group, can be extended into a functor from $\mathcal{G}roup$ to $\mathcal{A}bs\mathcal{G}roup$. This functor can be shown to be an equivalence of categories, using crucially the identification $p_G\colon G = \mathrm{Aut}\,G\text{-Set}\,\mathrm{Pr}_G$ we constructed earlier.

Each G-set X produces a 1-truncated type, namely the total space $\widetilde{X} :\equiv \sum_{s:\mathrm{B}G} X\,s$. If you think of the G-set X as associating to each shape $s\colon \mathrm{B}G$ a set $X\,s$ of possible *structures* on s, then $\widetilde{X}$ is the type of *X-structured shapes*, whose elements are the choice of a shape s together with a structure on s drawn from $X\,s$. From this point of view, the symmetries of a X-structure shape of the form (sh_G, x) ought to be symmetries of sh_G that *respect* the structure x in some sense. To go back to the example of the square graph S of earlier, consider the type $\mathrm{Graph}_{\mathrm{Set}}$ of graphs whose type of vertices is a set. Then define the family of sets $V\colon \mathrm{Graph}_{\mathrm{Set}} \to \mathrm{Set}$ associating to each such graph its set of vertices. We can simply restrict V to get a $\left(\mathrm{Graph}_{\mathrm{Set}}\right)_{(S)}$-set, abusively still denoted V. Here, a shape is a graph merely equal to S, and a structure on such an graph is a choice of one of its vertices. A V-structured graph of the form (S, v) is then a pointed graph whose underlying plain graph is S. The type of symmetries of (S, v) in $\tilde{V}$ can be calculated to be equivalent to the type of those symmetries of S in $\mathrm{Graph}_{\mathrm{Set}}$ preserving the selected vertex.

The notion of subgroups of a given group emerges. A subgroup of

G is defined to be a G-set X together with a choice of element of $X\,\mathrm{sh}_G$, with the side propositional condition that $\widetilde{X}$ is connected (we say that X is transitive). In other words, a subgroup of G is an element of the type

$$\mathrm{Sub}_G :\equiv \sum_{X:G\text{-Set}} (X\,\mathrm{sh}_G) \times (\mathrm{isConn}\ \widetilde{X})$$

Thinking again in terms of structures, a subset of G is the choice of a notion of structure on shapes, together with such a structure on the shape sh_G. The intuitive meaning of the side condition $\mathrm{isConn}\ \widetilde{X}$ is that all structures (in the sense of X) on a given shape $s\colon \mathrm{B}G$ are essentially "equivalent". In the example of the previous paragraph, $V\colon \mathrm{Graph}_{\mathrm{Set}(S)}$-Set satisfies $\mathrm{isConn}\ \tilde{V}$ as, the vertices of S are indistinguishable if we erase their names 0, 1, 2, and 3. Going back to the general case, There is a map, that associates to each subgroup of G an actual group together with a homomorphism to G:

$$\mathrm{Sub}_G \to \sum_{H:\mathrm{Group}} \sum_{f:\mathrm{B}H\to\mathrm{B}G} \mathrm{sh}_G = f\,\mathrm{sh}_H, \quad (X, x) \to (\mathrm{Aut}_{\widetilde{X}}(\mathrm{sh}_G, x), \mathrm{pr}_1, \mathit{refl}_{\mathrm{sh}_G})$$

Notice that this map would still make sense for a definition of Sub_G without the side condition of connectedness. But the advantage of requiring the connectedness of $\widetilde{X}$ is that the map has propositional fibers. In other words, no two different elements of Sub_G will yield the same group H over G. This recover the notion of subgroup found in ordinary group theory: if $f\colon \mathrm{B}H \to \mathrm{B}G$ is such that ap_f is injective, then the fiber at (H, f, p) is non empty (and so contractible) because the type family f^{-1} is then a G-set, whose total space is connected (it is $\mathrm{B}H$), so we can form the subgroup given by f^{-1} and the element (sh_H, p) of the set $f^{-1}\ \mathrm{sh}_G$; this subgroup is sent to an element equal to (H, f, p) by the previous map. While abstract group theory introduces the notion of subgroup through algebraic axioms (in the form of a subset stable under the different operations), our approach introduces the notion directly as "the group of symmetries of something", this something being the selected X-structure on the shape sh_G.

A TRANSITIVE G-SET X DETERMINES SEVERAL SUBGROUPS. Indeed, a priori, different elements of the set $X\,\mathrm{sh}_G$ yield different subgroups. Given a symmetry $g\colon \mathrm{U}G$ of sh_G and $x\colon X\,\mathrm{sh}_G$, the subgroup $(X, \mathit{trp}^X_g\ x)$ is called the *conjugate* of (X, x) by g. The type Sub_G of subgroups of G can be proven to be a set, and when the proposition $\prod_{g:\mathrm{U}G}(X, \mathit{trp}^X_g\ x) = (X, x)$ holds, the subgroup (X, x) is said to be *normal*. It is then only natural to consider the group $\mathrm{Aut}_{G\text{-Set}}\,X$, that is the group of symmetries of the G-set X itself. This group recover the notion of *quotient group* in ordinary group theory. Here, the synthetic approach offers a very nice point of view: in ordinary group theory, it is very not obvious how the quotient group is the group of symmetries of a mathematical object; the synthetic approach on the contrary gives directly the mathematical object of which the quotient group is the group of symmetries, namely the G-set X. Thinking of X as defining a notion of structure on the shape in $\mathrm{B}G$, the quotient group is the set of "G-equivariant permutations of X-structure on sh_G".

I am intentionally cutting corners here about normal subgroups. The reader should refer to Chapter 5 of [Bez+22] for a complete treatment of the subject.

ONE CAN EVEN CONSIDER THE SAME GROUP $\mathrm{Aut}_{G\text{-Set}}\,X$ when the given subgroup (X, x) is not normal. This is a perfectly fine group, implementing the symmetries of perfectly well-defined mathematical object (the G-set X). The equivalent construction in abstract group theory is far from trivial. It is only accessible as the quotient of the *normalizer* of H in G by the subgroup H (where H is the abstract subgroup corresponding to the concrete subgroup (X, x)). This construction is sometimes called the Weyl group of H in G. The mathematical object of which this Weyl group is the group of symmetries is not obvious at all in abstract group theory. In our synthetic version, this mathematical object is readily available! I invite you to explore further how this view on group theory can be fruitful in many ways by consulting [Bez+22]. Although the book is still far from a final version, the first 4 chapters are in good enough shape to be read by the student of this Summer School.

References

[Bez+22] Marc Bezem et al. *Symmetry*. https://github.com/UniMath/SymmetryBook. Commit: 982015d. Aug. 18, 2022.