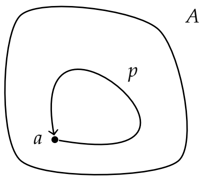
4
Groups

ch:groups

The identity type is not just any type: in the previous sections we have seen that the identity type $a =_A a$ reflects the "symmetries" of an element a in a type A.[1] Symmetries have special properties; for instance you can rotate a square by 90°, and you can rotate it by −90°, undoing the first rotation. Symmetries can also be composed, and this composition respects certain rules that holds in all examples. One way to study the concept of "symmetries", would be to isolate the common rules for all our examples, but also show, conversely, that anything satisfying these rules actually *is* an example.



With inspiration of geometric and algebraic origins, it became clear to mathematicians at the end of the 19th century that the properties of such symmetries could be codified by saying that they form an abstract *group*. In Section 2.3 we saw that the identity type was "reflexive, symmetric and transitive" – and an abstract group is just a set with such operations satisfying certain rules.

We attack the issue more concretely; instead of focusing on the abstract properties, we promote the type exhibiting the symmetries, and the axioms for an abstract group follow from the rules for identity types without needing us to worry about them. However, we *will* show that the two approaches give the same end result.

In this chapter we lay the foundations and provide some basic examples of groups.

4.0.1 *Brief overview of the chapter*

In Section 4.1 we give the formal definition of a group along with some basic examples. In Section 4.2 we spell out the details, expanding on the properties of the identity type of a group and comparing these properties with those of an abstract group. We then return in Section 4.2 to groups more generally, explaining how these map to each others through "homomorphisms" (which to us are simply pointed maps) and what this entails for the identity types: all the abstract group properties are preserved.

[1] Since the symmetries $p : a =_A a$ are paths that start and end at the point $a : A$, we also call them *loops* at a.

In most of our exposition we make the blanket assumption that the identity type in question is a set, but in Section 4.4 we briefly discuss ∞-groups where this assumption is dropped.

Classically, groups have appeared because they "act" on a set (or more general objects), that is to say, they collect some of the symmetries of the set. This is a point of view that we will return to many times and we give the basic theory in Section 4.5. This section should remind the reader very much of what happened in Chapter 3, where we did much of the same considerations for the special case of the integers. More generally, connected set bundles now reappear in the guise of "transitive G-sets", laying the groundwork for our later discussion of the set of subgroups.

Another important thing which is discussed in Section 4.5 is the type of "G-torsors", which at first glance can appear frightening. However, a G-torsor ~~correspond~~ to *a* universal set bundle and the important step is to consider the *type* of these: This idea is used in Section 4.7 to build the equivalence between our definition of a group and the abstract version taught in most algebra classes. This is followed up for homomorphisms in Section 4.8 and for G-sets in Section 4.11.

corresponds

universal??

bundle over what?

With all this in place, the structure of the type of groups is in the large in many aspects similar to the universe in the sense that many of the constructions we're used to from the universe have their analog for groups. The functions are replaced by the homomorphisms. Products stay "the same" as we will see ~~already~~ in Example 4.1.22 (and more generally, Π-types over sets). The sum of two groups is simple enough: It is the sum of the underlying types with the base points identified, as defined more precisely in Definition 4.12.1. In the usual treatment this is a somewhat more difficult subject involving "words" taken from the two groups. This reappears in our setting when we show that homomorphisms ~~out of a sum~~ correspond to pairs of homomorphisms (just as for ~~sum and functions in type~~s).

can't we say "products"?

comma

"stay the same"

from a sum to another group

sums of types
and functions
between types

[2]

4.1 *The type of groups*

sec:typegroup

Definition 4.1.1. Given a pointed type $X \equiv (A, a)$, we define its type of *loops* by $\Omega\, X$ ~~$\equiv \Omega(A, a)$~~ $:\equiv (a =_A a)$.

ex:base=base

Example 4.1.2. We defined the circle S^1 in Definition 3.1.1 by declaring that it has a point • and an identification ("symmetry") ↺: $(\bullet = \bullet) \equiv \Omega\, S^1$, and we proved in Corollary 3.4.5 that $\Omega\, S^1$ is equivalent to the set $\mathbb{Z}$ (of integers), where $n \in \mathbb{Z}$ corresponds to the n-fold composition of ↺ with itself (which works for both positive and negative n). We can think of this as describing the symmetries of •: we have one "generating symmetry" ↺, and this can be applied any number of times, giving a new symmetry for each new number. Here, composition of loops corresponds to usual

[2] ((THEN SUBGROUPS TAKE CENTRAL STAGE, BUT I POSTPONE DISCUSSING THESE IN CASE THIS CHAPTER IS ALREADY OVERLY LONG AND WE WANT TO PUT THEM IN A SEPARATE CHAPTER))

addition of integers.

Hence, the circle is a very cheap packaging of the "group" of integers, the declaration of $\bullet$ and $\circlearrowleft$ not only gives the *set* Z of integers, but at the same time the addition.

Example 4.1.3. Recall the finite set $\mathbb{2} : \mathrm{fin}_2$ from Definition 2.18.1, containing two elements. According to Exercise 2.9.3, $\mathbb{2} = \mathbb{2}$ has exactly two distinct elements, $\mathrm{refl}_{\mathbb{2}}$ and twist, and doing twist twice gives you back $\mathrm{refl}_{\mathbb{2}}$. We see that this is exactly all the symmetries you'd expect to have of a two point set: You can let everything stay in place ($\mathrm{refl}_{\mathbb{2}}$), or you can swap the two elements (twist); and if you swap twice, everything is let be. The pointed type fin_2 (of "finite sets with two elements"), with $\mathbb{2}$ as the base point, is our embodiment of these symmetries,i.e., $\Omega\,\mathrm{fin}_2$.

Observe that (by the definition of S^1) there is an interesting function $\mathrm{S}^1 \to \mathrm{fin}_2$, sending $\bullet : \mathrm{S}^1$ to $\mathbb{2} : \mathrm{fin}_2$ and $\circlearrowleft$ to twist.

The examples Klein and Lie were interested in were of a type making it admissible to say that a group is the loops $\Omega(A, a) \equiv (a =_A a)$ for *some* type A and *some* element $a : A$. However, in elementary texts it is customary to restrict the notion of a group to the case when $a =_A a$ is a *set* as we will do, starting in Section 4.2. This makes some proofs easier, since if are we given two elements $g, h : a =_A a$, then the identity type $g = h$ is a proposition, i.e., g can be equal to h in at most one way. Hence questions relating to uniqueness will never be a problem.

"a group is the type of loops"

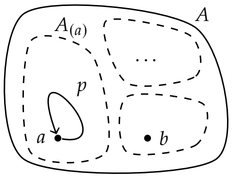
comma

See Section 5.2 for a brief summary of the early history of groups.

Remark 4.1.4. The reader may wonder about the status of the identity type $a =_A a'$ where $a, a' : A$ are different elements. One problem is of course that if $p, q : a =_A a'$, there is no obvious way of composing p and q to get another element in $a =_A a'$, and another is that $a =_A a'$ does not have a distinguished element, such as $\mathrm{refl}_a : a =_A a$.[3] Given $f : a =_A a'$ we can use transport along f to compare $a =_A a'$ with $a =_A a$ (much as affine planes can be compared with the standard plane or a finite dimensional real vector space is isomorphic to some Euclidean space), but absent the existence and choice of such an f the identity types $a =_A a'$ and $a =_A a$ are different animals. We will return to this example when we've defined torsors.

rem:whypointedconngpoid

Remark 4.1.5. As a consequence of Lemma 2.11.2, the inclusion of the component $A_{(a)} :\equiv \sum_{x:A} \|a = x\|$ into A (i.e., the first projection) induces an equivalence of identity types from $(a, !) =_{A_{(a)}} (a, !)$ to $a =_A a$, and thus from $\Omega(A_{(a)}, (a, !))$ to $\Omega(A, a)$. This means that, when considering the loop type $\Omega(A, a)$, "only the elements $x : A$ with x merely equal to a are relevant", and to avoid artificial extra components, we should consider only *connected* types A (c.f. Definition 2.14.3).



Also, our preference for $\Omega(A, a)$ to be a *set* indicates that we should consider only the connected types A that are *groupoids*.

[3] The type $a =_A a'$ does have an interesting *ternary* composition, mapping p, q, r to $pq^{-1}r$. A set with this kind of operation is called a *heap*, and we'll return to heaps in **??**.

def:pt-conn-groupoid

Definition 4.1.6. The type of *pointed connected groupoids* is the type

$$\mathcal{U}_*^{=1} :\equiv \sum_{A:\mathcal{U}} \sum_{a:A} \mathrm{isSet}(a =_A a) \times \prod_{x:A} \|a =_A x\|.$$

parenthesize for clarity

The meaning of the superscript "= 1" can be explained as follows: We also define

$$\mathcal{U}^{\leq 1} :\equiv \mathrm{Groupoid}$$
$$:\equiv \sum_{A:\mathcal{U}} \prod_{x,y:A} \mathrm{isSet}(x =_A y),$$

to emphasize that groupoids are 1-types; the type of connected types is denoted

$$\mathcal{U}^{>0} :\equiv \sum_{A:\mathcal{U}} \|A\| \times \prod_{x,y:A} \|x =_a y\|.$$

Similar notations with a subscript "$*$" indicate pointed types.

The following exercise reconciles the words of the above definition with the type.

xca:defgroup

Exercise 4.1.7. Show that A is indeed a groupoid for $(A, a, p, q) : \mathcal{U}_*^{=1}$.

Remark 4.1.8. We shall refer to a pointed connected groupoid (A, a, p, q) simply by the pointed type $X :\equiv (A, a)$. There is no essential ambiguity in this: Being a connected groupoid is asserted (for a pointed type) by

$$\mathrm{isSet}(a =_A a) \times \prod_{x:A} \|a =_A x\|,$$

which is a proposition (Lemma 2.10.3 and Lemma 2.10.6), and so the witness (p, q) is unique.

What does this mean?
One can see that (A,a) and (A,a,p,q)
are not even of the same type.
Why not just write (A,a,!,!)?

We also write $\mathrm{pt}_X :\equiv a$ for the *base point* of the pointed type.

We are now ready to define the *type* of groups:

insert "a"?

def:typegroup

Definition 4.1.9. A *group* is given by pointed connected groupoid $X \equiv (A, a)$ via the loop type $\Omega(A, a)$; the *type of groups*,

$$\mathrm{Group} :\equiv \mathrm{Copy}(\mathcal{U}_*^{=1}),$$

is a wrapped copy (cf. Section 2.6.5) of the type of pointed connected groupoids $\mathcal{U}_*^{=1}$. We rename the constructor $\underline{\Omega} : \mathcal{U}_*^{=1} \to \mathrm{Group}$, so a group $G \equiv \mathrm{in}_X : \mathrm{Group}$ will be referred to simply as $\underline{\Omega}\, X$. We rename the destructor $\mathrm{B} : \mathrm{Group} \to \mathcal{U}_*^{=1}$, and

the subscript + here is too tiny

$$\mathrm{B}\, G \equiv \mathrm{B}(\underline{\Omega}\, X) :\equiv X \equiv (A, a)$$

is referred to as the *classifying type of* G. The element $\mathrm{p}_G :\equiv \mathrm{pt}_{\mathrm{B}\,G} \equiv a$ will be referred to as the *base point*. Informally, we may also refer to the type $\mathrm{B}\, G_{\div} \equiv A$ itself as the classifying type of G.

This word is too easily confused
with the set of automorphisms
of the group G. There must
be a better word. "Motions of G"?

def:group-symmetries

Definition 4.1.10. We define the *symmetries* of a group $G \equiv \underline{\Omega}\, X$, to be the set $\mathrm{U}\, G :\equiv \Omega\, X$. In this way we have defined a map

$$\mathrm{U} : \mathrm{Group} \to \mathrm{Set}, \qquad \underline{\Omega}\, X \mapsto \Omega\, X.$$

More confusion: symmetries of the
base point or symmetries of
the group, as just above?

rem:aut

Remark 4.1.11. We are emphasizing that the essential feature of a group is the symmetries of the base point. And that is why we defined Group to be a copy of $\mathcal{U}_*^{=1}$, and not $\mathcal{U}_*^{=1}$ itself: The type most often associated to a group G is the set $\mathrm{U}\, G$, so we use a special notation for the classifying type $\mathrm{B}\, G$. However, as noted in Section 2.6.5, the constructor and destructor pair forms an equivalence $\mathrm{Group} \simeq \mathcal{U}_*^{=1}$. And $\mathcal{U}_*^{=1}$ is a subtype of $\mathcal{U}_*$, so in this sense, once you know that a pointed type X is a connected groupoid, this pointed type gives a classifying type for a group $G :\equiv \underline{\Omega}\, X$, and X carries all the information about the group G.

Recall also the example of the negated natural numbers $\mathbb{N}^-$ from Section 2.6.5: Its elements are $-n$ for $n : \mathbb{N}$ to remind us how to think about them. And the same applies to Group: Its elements are $\underline{\Omega}\, X$ for $X : \mathcal{U}_*^{=1}$ to remind us how to think about them.

rem:BG-convention

Remark 4.1.12. To define a function $f : \prod_{G:\text{Group}} T(G)$, where $T(G)$ is a type family indexed by G : Group, it suffices to consider the case $G \equiv \underline{\Omega}\, X$, where X is a pointed connected groupoid. Since $X \equiv \mathrm{B}\, G$, we shall make a convention to always use the variable name BG instead of X, and similarly, for a variable H : Group, when we use the induction principle for Group, we use the variable $BH : \mathcal{U}_*^{=1}$, etc. And whenever we introduce a variable G of type Group, we immediately and silently use the induction principle to get a variable $BG : \mathcal{U}_*^{=1}$ such that $G \equiv \underline{\Omega}\, BG$ and $BG \equiv \mathrm{B}(\underline{\Omega}\, BG) \equiv \mathrm{B}\, G$.[4]

Also note that identifications $G = H$ of groups are equivalent to identifications $BG = BH$ of pointed types.

It is not infrequent that we want to consider the symmetries $\Omega(A, a)$ of some element a in some groupoid A: ⟵ End a sentence with a period, never a colon.

def:automorphism-group

Definition 4.1.13. For a groupoid A with a specified point a, we define the *automorphism group* of $a : A$ by

$$\mathrm{Aut}_A(a) :\equiv \underline{\Omega}(A_{(a)}, (a, !)),$$

i.e., $\mathrm{Aut}_A(a)$ is the group with classifying type $\mathrm{BAut}_A(a) \equiv (A_{(a)}, (a, !))$, the connected component of A containing a, pointed at a.

m:symmetriesofnonconnectedgroupoids

Remark 4.1.14. For any $G \equiv \underline{\Omega}(A, a)$: Group, we have an identification $G = \mathrm{Aut}_A(a)$, because we have an identification of pointed types $(A_{(a)}, (a, !)) = (A, a)$, since A is connected.

In other words, for any $G \equiv \underline{\Omega}\, BG$, we have an identification $G = \mathrm{Aut}_{BG_\cdot}(\mathrm{p}_G)$, of G with the automorphism group of the base point $p_G : BG$.

Different fonts? Also, why not just write pt_BG, since we have that notation already?

sec:firstgroupexamples
excirclegroup

4.1.1 *First examples*

Example 4.1.15. The circle S^1, which we defined in Definition 3.1.1, is a connected groupoid (Lemma 3.1.5, Corollary 3.4.5) and is pointed at •. The identity type $\bullet =_{S^1} \bullet$ is equivalent to to the set of integers Z and composition corresponds to addition. This justifies our definition of the *group of integers* as

$$\mathbb{Z} :\equiv \mathrm{Aut}_{S^1}(\bullet).$$

Maybe remind the reader that this is the same as Omega underlined of S^1

It is noteworthy that along the way we gave several versions of the circle, each of which has its own merits, the version in Definition 3.5.1

$$C = (\sum_{X:\mathcal{U}} \sum_{f:X=X} \|(\mathrm{Z}, s) = (X, f)\|, (\mathrm{Z}, s))$$

being a very convenient one.

ex:groups

Example 4.1.16. Apart from the circle, there are some important groups that come almost for free: namely the symmetries in the type of sets.

(1) Recall that the set $\mathbb{1}$ = True has the single element which we can call $*$. Then $\mathrm{Aut}_{\mathbb{1}}(*)$ is a group called the *trivial group*.

[4] You see immediately the typographical reason behind this convention: The italic letters B,G get along nicely, while the roman B distances itself a bit from its italic friend G.

(2) If $n : \mathbb{N}$, then the *permutation group of n letters* is

$$\Sigma_n :\equiv \mathrm{Aut}_{\mathrm{fin}_n}(\mathbb{m}),$$

where fin_n is the groupoid of sets of cardinality n (c.f. 2.18.1). The classifying type is thus $B\Sigma_n :\equiv (\mathrm{fin}_n, \mathbb{m})$. With our convention of Remark 4.1.14 we can tolerate $\mathrm{Aut}_{\mathrm{fin}}(\mathbb{m})$, $\mathrm{Aut}_{\mathrm{Set}}(\mathbb{m})$ or even $\mathrm{Aut}_{\mathcal{U}}(\mathbb{m})$ as synonyms for the group Σ_n (where fin and Set are the subtypes of $\mathcal{U}$ of finite sets and sets).

If the reader starts worrying about size issues, that is quite legitimate; see Remark 4.1.17.

(3) More generally, if S is a set, is there a pointed connected groupoid (A, a) so that $a =_A a$ models all the "permutations" $S =_{\mathrm{Set}} S$ of S? Again, the only thing wrong with the groupoid Set of set (apart from Set being large) is that Set is not connected. ~~The~~ *group of permutations of S* is defined to be

$$\Sigma_S :\equiv \mathrm{Aut}_{\mathrm{Set}}(S),$$

with classifying type $B\Sigma_S :\equiv (\mathrm{Set}_{(S)}, S)$.

Set being unconnected is not wrong, either, in this context.

Set being large is not wrong

Here you should also assume that n is in U_0.

add a comma

rem:groupsarebig

REMARK 4.1.17. This is only for those who worry about size issues - a theme we systematically ignore in our exposition. If we start with a base universe $\mathcal{U}_0$, the groupoid of sets of cardinality n, fin_n is a Σ-type $\sum_{A:\mathcal{U}_0}\|A = \mathbb{m}\|$ over $\mathcal{U}_0$ and so without any massage will lie in a bigger universe $\mathcal{U}_1$. In order to accommodate ~~for~~ the finite permutation groups, the universe "$\mathcal{U}$" appearing as a subscript for the first Σ in the definition of groups needs to be at least as big as $\mathcal{U}_1$. If so, the type Group will not be in $\mathcal{U}_1$, but in some bigger universe $\mathcal{U}_2$, so if I choose some group G and look at *its* group of automorphisms, this will will be a group only if the universe is at least as big as $\mathcal{U}_2$. Luckily, our convention is that the universes are nested, and so at any point we'll just be somewhere big enough for our purposes, see Section 2.9. This is not to say that these questions are trivial or unimportant; they are nontrivial and important, but not what this text is about.

add a comma

ex:cyclicgroups

EXAMPLE 4.1.18. In Theorem 3.7.2 we studied the symmetries of the "m-fold set bundle" of the circle for m a positive integer, and showed that there were m different such symmetries. Moreover we showed that these symmetries were the powers f^n (for $n = 0, 1, \ldots, m-1$) of one (non-unique) symmetry f and that $f^{m+k} = f^k$ for any integer k. This very important phenomenon pops up in many situations, and is called the *cyclic group of order m*. In other words, the cyclic group of order m is the (pointed) component of the type SetBundle(S^1) of set bundles of the circle containing the m-fold set bundle. We analyzed this in Theorem 3.7.2 and found that this (pointed) component was equivalent

Hmm? I wonder about using "the" here, since there are many covering spaces of the circle of degree m. Somehow you have to say you are interested in the cyclic one.