SOME REMARKS ON TEACHING MATHS: TORSORS AND PRINCIPAL EQUIVALENCE RELATIONS

WOLFGANG BERTRAM

In our note on teaching affine spaces, the ternary map $S(a,b,c) = a - b + c$ was one of the main actors. In the present note, we discuss its analog for general groups G (written multiplicatively): to keep notation light, we abbreviate

$$(abc) := S(a,b,c) := ab^{-1}c, \tag{0.1}$$

and we call the map $G^3 \to G$, $(a,b,c) \mapsto (abc)$ the *torsor law of* G. We shall explain that *torsors are for groups what affine spaces are for vector spaces*: they are "groups with origin forgotten". The torsor law can be characterized by two identities: *para-associativity* (PA), and the *idempotent law* (IP):

(PA) $(xy(zuv)) = (x(uzy)v) = ((xyz)uv)$,
(IP) $(xxy) = y, \quad (wzz) = w$.

Indeed, checking that these laws give back a group with law $xz = (xyz)$, for fixed y, is a nice exercice for a first course in abstract algebra. As in the case of affine spaces, the approach via a ternary map has clear advantages when introducing *categorical notions*. In a second step, the same procedure leads to a (in my opinion) much nicer formulation of the notion of *(abstract) principal bundle*: one works again with a ternary product (xyz), which now is *not everywhere defined* – it is only defined if x and y belong to the same equivalence class of some equivalence relation a; the whole thing we call a *principal equivalence relation (prev)* (see [36]).

The only serious problem arising in this context is *terminology*: unfortunately, there is no universally adopted convention for fixing the name of the child – what we call here "torsor" can be found on the wikipedia page under the title *heap*. Earlier terms are *flock* and *pregroup*. As mentioned there, Boris Schein also proposed the term *groud* (which I used with Kinyon in a first version of [25]); but for various reasons this term has not been generally accepted. An equivalent term is principal homogeneous space, which is a bit clumsy and long. Thus we follow here the popularization by John Baez and use the term "torsor". One advantage is that one can easily add the prefix "semi-", or create other composed terms.

1. Torsors

Definition 1.1. *A <u>torsor</u> is a set M with a map $M^3 \to M$, $(x,y,z) \mapsto (xyz)$ satisfying (PA) and (IP). A torsor is called <u>commutative</u> if, moreover, $(xyz) = (zyx)$ for all $x,y,z \in M$. A <u>morphism of torsors</u> is a map $f : M \to M'$ between torsors commuting with structure maps: $f((xyz)) = (f(x)\,f(y)\,f(z))'$.*

Lemma 1.2. *Let G be a group with group law $(x,y) \mapsto xy$ and unit e. Then G with ternary law $G^3 \to G$, $(x,y,z) \mapsto xy^{-1}z$ is a torsor.*

Proof. Direct check – exercise! □

Lemma 1.3. *Assume M is a torsor. Then, for each element $y \in M$, the law $xz := (xyz)$ is a group law on M with unit element y.*

Proof. Exercise: from (PA) we get associativity, from (IP) that y is neutral. To prove existence of inverses, check that $u := (yxy)$ satisfies $(uyx) = y = (xyu)$. □

Theorem 1.4. *The constructions from the preceding two lemmas are inverse to each other.*

Proof. One direction is trivial: starting with a group, constructing a torsor, we end up with the same group. To prove the other direction, start with a torsor M, fix $o \in M$ and define the law $[xyz] := xy^{-1}z$ associated to the group (M, o). One has to show that $(xyz) = [xyz]$, that is, $(xyz) = ((xo(oyo))oz)$. To prove this, apply (IP) several times. □

Theorem 1.5. *The preceding constructions define equivalences of categories between groups and torsors with base point, and between "groups after forgetting their origin" and torsors. Here, commutative groups correspond to commuative torsors.*

Proof. Just note that any morphism of groups preserves also the ternary product, and conversely a torsor morphism is such that, for any $y \in M$ fixed, the map $f : (M, y) \to (M', f(y))$ is a group morphism. □

Example 1. The *empty set* is a torsor (the axioms do not require that a point exists). The theorem has to be suitably interpreted, in this case.

Example 2. If A and B are two sets, then the set $\mathrm{Bij}(A, B)$ of bijections $A \to B$ with law $(fgh) := fg^{-1}h$, becomes a torsor. Of course, it may be emtpy.

Lemma 1.6. *The torsor axioms (PA) ∧ (IP) are equivalent to (Ch) ∧ (IP):*

(Ch) left Chasles relation: $(xy(yuv)) = (xuv)$, and
right Chasles relation: $((xyz)zv) = (xyv)$;
(IP) idempotency: $(xxy) = y = (yxx)$.

Proof. (IP) ∧ (Ch) implies (PA): $(xy(uvw)) = ((xyu)u(uvw)) = ((xyu)vw)$, and conversly (IP) ∧ (PA) implies (Ch) by taking $y = z$. □

Definition 1.7. *In a torsor M we define maps $L_{x,y}, R_{z,y}$ and $M_{x,z} : M \to M$ by*

$$L_{x,y}(z) := R_{z,y}(x) := M_{x,z}(y) := (xyz),$$

called left, right and middle translations.

Using this notation, we rewrite (PA), (IP) and (Ch) in terms of left translations:

(PA') $L_{xy} \circ L_{zu} = L_{x,L_{u,z}(y)} = L_{L_{xyz},u}$,
(IP') $L_{x,x} = \mathrm{id}_M$, $L_{w,z}(z) = w$,
(Ch') $L_{x,y} \circ L_{y,u} = L_{x,u}$ and $L_{x,y} = L_{L_{x,y}(z),z}$.

Theorem 1.8. *Torsors are equivalent to principal homogeneous spaces:*

(1) Let M be a torsor. Then the set $L(M) = \{L_{x,y} \mid x, y \in M\}$ of all left translations is a group acting simply transitively on M.

(2) Conversely, a simply transitive group action $G \times M \to M$ gives back a torsor structure on M, via $(xyz) = \lambda_{x,y}(z)$, where $\lambda_{x,y} \in G$ is the unique element such that $\lambda_{x,y}(y) = x$.

Proof. (1) From (IP') and (PA') we see that $L(M)$ is a group. Fixing an origin $e \in M$, this is the usual group of left translations on the group (M, e), and one proves as usual that it acts simply transitively.

(2) Since $\lambda_{x,y} \circ \lambda_{y,u}$ sends u to x, we get the first relation of (Ch'), and since $\lambda_{x,y}$ sends z to $\lambda_{x,y}(z)$, we get the second one. (IP) is obvious, hence, by Lemma 1.6, we get a torsor. □

Moreover, $L(M)$ acts by *torsor automorphisms* on M: this follows from

$$(xy(uvw)) = ((xyu)vw) = ((xyu)(yx(xyv))w) = ((xyu)(xyv)(xyw)).$$

2. Semitorsors

By definition, a *semitorsor* is a set M with a tenary map satisfying just (PA), but not necessarily (IP). They are for torsors what semigroups are for groups: fixing the middle element y, the law $xz := (xyz)$ is a associative. However, it is in general not possible to recover the ternary law from this product, nor is there an analog of Lemma 1.6. The main example one should have in mind is an analog of the one given above: if A and B are two sets, then the set M of all *binary relations between A and B*, with law coming from *relational composition* and *reverse relations* via $(RST) := R \circ S^{-1} \circ T$, is a semitorsor, but not a torsor. See [25] for more on this.

3. Principal equivalence relations (prev's)

A *principal equivalence relation* (abbreviated: prev) is an equivalence relation on a set M that "acts" on M (from the left, or from the right), as follows:

Definition 3.1. *An* equivalence relation on M *is a subset $a \subset M^2$ such that:*

(1) $\forall x, y \in M$: $(x, y) \in a \Leftrightarrow (y, x) \in a$
(2) $\forall x, y, z \in M$: $(x, y) \in a, (y, z) \in a \Rightarrow (x, z) \in a$
(3) $\forall x \in M$: $(x, x) \in a$.

Given such a, we define the left domain D_a^L *and the* right domain $D_a^R \subset M^3$ *by*

$$D_a^L := a \times M = \{(x, y, z) \in M^3 \mid (x, y) \in a\}, \qquad D_a^R := M \times a.$$

Recall that, given a, there is a *quotient space* M/a and a canonical projection $M \to B := M/a$, sending x to its *equivalence class* $[x] = [x]_a$.

Definition 3.2. *A* (left, resp. right) principal equivalence relation on M *is an equivalence relation a on M together with partially defined ternary product maps,*

$$M^3 \supset D_a^L \to M, \quad (x, y, z) \mapsto (xyz),$$
$$M^3 \supset D_a^R \to M, \quad (x, y, z) \mapsto (xyz),$$

respectively, such that the following holds:

(1) if $(x, y) \in a$ and $(u, v) \in a$, then also $(u, (xyv)) \in a$ (resp.: $(u, (vyx)) \in a$),
(2) the para-associative law (PA) is satisfied,
(3) the idempotent law (IP) is satisfied.

Condition (1) guarantess that, if all terms on the right hand side of (PA) are defined, then so are all terms on the left hand side, and hence it makes sense in (2) to require that equality holds. The following lemma is proved like Lemma 1.6 above:

Lemma 3.3. *A (left) prev on M can, equivalently, be defined by requiring that (1) and (Ch) and (IP) hold. Similarly for right prev's.*

Definition 3.4. *In a left prev, we define* left translations *for $(x, y) \in a$ by*

$$L_{x,y} : M \to M, \quad x \mapsto L_{x,y}(z) := (xyz).$$

Similarly, right translations *are defined in right prev's.*

Lemma 3.5. *In terms of left translations, a left prev can be characterized as follows:*

(1) each equivalence class $[u]_a$ is preserved under left translations $L_{x,y}$,
(2) $L_{x,y} \circ L_{z,u} = L_{x,L_{u,z}(y)} = L_{L_{xyz},u}$,
(3) $L_{x,x} = \mathrm{id}_M$ and $L_{x,y}(y) = x$.

Proof. This is just a rewriting (see (PA') and (IP') above). □

Theorem 3.6. *If a is a left prev on M, then the set of left translations*

$$G := L(M, a) := \{L_{x,y} \mid (x, y) \in a\}$$

is a group that preserves equivalence classes of a and acts simply transitively on each fiber. In other words, $(M, G, M/a)$ is an abstract (left) principal bundle (where "abstract" means that no topological conditions are imposed). Conversely, given an abstract (left) principal bundle (M, G, B), the equivalence relation given by the projection $M \to B$ and the law

$$(xyz) := \lambda_{x,y}(z),$$

where $g := \lambda_{x,y} \in G$ is the unique element such that $g.y = x$, defines a left prev.

Proof. The arguments from the proof of Theorem 1.8 apply, *mutatis mutandis*. □

Remark on morphisms. *Morphisms of prev's* are defined in the obvious way (maps preserving equivalence relation and ternary product). The definition of morphisms of principal bundles is less pleasant; but I hope the reader will see that the correct definition is equivalent to the one of prev-morphism. Thus, finally, we get an *equivalence of categories between prev's and principal bundles.*

4. Assocoids

The postfix "-oid" signalizes that an algebraic structure need not be defined everywhere. In [36], I define an *associoid* to be a set with partially defined ternary product satisfying (PA) and (IP). Besides left or right prevs, the most important examples come from groupoids: considering the not everywhere defined ternary map $(gh) = gf^{-1}h$ on a groupoid, we get what Anders Kock calls a pregroupoid. For instance, the set of *local bijections* $f : A \supset U \to U' \subset B$ between A and B with product $(fgh) = fg^{-1}h$ defined if these three maps are composable, is a pregroupoid. This may be a topic for another note.

E-mail address: wolfgang.bertram(Klammeraffe)univ-lorraine.fr