Bachelor's project

NTNU
Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Mathematical Sciences

Torstein Vik

Power Quandles

Bachelor's project in Mathematics
Supervisor: Markus Szymik

May 2021

Kunnskap for en bedre verden

Torstein Vik

Power Quandles

Bachelor's project in Mathematics
Supervisor: Markus Szymik
May 2021

Norwegian University of Science and Technology
Faculty of Information Technology and Electrical Engineering
Department of Mathematical Sciences

NTNU
Kunnskap for en bedre verden

POWER QUANDLES

TORSTEIN VIK

Abstract. We introduce the category of power quandles, and study the forgetful functor Pq from groups to power quandles together with its left adjoint Gr. We conjecture that if two finite groups have isomorphic power quandles, then they are isomorphic as groups, and prove several partial results in this direction. Several of these new results are formally verified in the Lean theorem prover.

Contents

Date: May 18, 2021.

1. Introduction

A quandle is a set Q with a binary operation $\triangleright$ which is self-distributive, idempotent (by which we mean $a \triangleright a = a$), and bijective when we fix the first argument. Quandles can come from various sources, but importantly to us, they can come from group conjugation. That is, take a group G, use its underlying set and define $a \triangleright b = aba^{-1}$. One can verify that this satisfies the axioms.

However, the quandle of a group is a rather weak invariant, in the sense that if G and H are groups with isomorphic quandles, they are not necessarily isomorphic as groups. To see this, consider abelian groups, where we get $a \triangleright b = b$, so the operation carries no information and we are left with just a set. It is then clear that abelian groups of the same order have isomorphic quandles.

Motivated by this, we introduce a better invariant of groups that we call *power quandles*, which take the power maps $x \mapsto x^n$ for $n \in \mathbb{Z}$ into account, as well as conjugation. Power quandles form a category, and there is a forgetful functor Pq from groups to power quandles. This functor has a left adjoint Gr.

Goal. The goal of this bachelor thesis is to explore power quandles, especially the question of whether non-isomorphic groups can have isomorphic power quandles.

Results. We now list the main results of this thesis.

Theorem 1.1. *If two finite groups G, H satisfy $\operatorname{Pq} G \cong \operatorname{Pq} H$ (isomorphism of power quandles), then:*

$$\operatorname{Z} G \cong \operatorname{Z} H$$

Here $\operatorname{Z} G$ is the center of G, and the isomorphism is one of (abelian) groups.

Corollary 1.2. *If two finite abelian groups G, H satisfy $\operatorname{Pq} G \cong \operatorname{Pq} H$, then $G \cong H$.*

Theorem 1.3. ***(verified in Lean)*** *If two groups G, H satisfy $\operatorname{Pq} G \cong \operatorname{Pq} H$, then:*

$$G / \operatorname{Z} G \cong H / \operatorname{Z} H$$

The isomorphism is one of groups.

Corollary 1.4. *If two centerless groups G, H satisfy $\operatorname{Pq} G \cong \operatorname{Pq} H$, then $G \cong H$.*

Together, these two main theorems give the following additional corollaries:

Corollary 1.5. *If two finite groups G, H satisfy $\operatorname{Pq} G \cong \operatorname{Pq} H$, then G and H are both central extensions of the same groups, i.e. we have short exact sequences*

$$1 \to A \to H \to Q \to 1$$

and

$$1 \to A \to G \to Q \to 1$$

Here, we have

$$A := \operatorname{Z} G \cong \operatorname{Z} H$$

and

$$Q := G / \operatorname{Z} G \cong H / \operatorname{Z} H$$

Note that this in itself is not enough to say G and H are isomorphic. Indeed the possibilities are classified by the second group cohomology $\operatorname{H}^2(Q; A)$. We see that when A or Q is trivial, the groups are isomorphic, which corresponds to the centerless and the abelian cases.

Corollary 1.6. *Given two finite simple groups G, H, if $\operatorname{Pq} G \cong \operatorname{Pq} H$, then $G \cong H$.*

Based on these results, it is natural to conjecture the following:

Conjecture 1.1. ***Main conjecture on power quandles.*** *Given two finite groups G, H, if $\mathrm{Pq}\, G \cong \mathrm{Pq}\, H$, then $G \cong H$ as groups.*

In order to gather further evidence for this conjecture, we have pursued two separate approaches. The first approach is simply a search for counterexamples. In order to carry out such a search, we need tools allowing us to show that two power quandles are non-isomorphic. We make use of two distinct such tools.

The first tool is the abelianization functor, that takes a power quandle and yields an abelian power quandle, which is an abelian object in the category of power quandles. This carries the information about conjugacy classes in the group, and the power maps on these conjugacy classes. This is essential information about the group, often placed alongside the character table, as in GAP.

The other tool is the functor Gr from power quandles to groups, which is the left adjoint to the forgetful functor Pq taking a group to its power quandle. It essentially creates the free group of the set of elements of the power quandle Q, but quotients out by $[x \triangleright y] = [x] \triangleright [y]$ and $[x^n] = [x]^n$. Here $[g]$ is the generator of the free group coming from the element g in the power quandle Q. This means that for given G and H, we can compute $\mathrm{Gr}\, \mathrm{Pq}\, G$ and $\mathrm{Gr}\, \mathrm{Pq}\, H$ and if these two groups are not isomorphic, then $\mathrm{Pq}\, G$ and $\mathrm{Pq}\, H$ are clearly not isomorphic either. This functor is analogous to the functor taking a quandle to its enveloping group. We also have a computer program that can compute $\mathrm{Gr}\, Q$ for finite Q, although as one might expect, it is very slow for larger groups, say beyond 64 elements.

The second approach regarding the main conjecture is the investigation of a stronger conjecture:

Definition 1.7. A group G is pq-like if there exists a power quandle Q such that $G \cong \mathrm{Gr}\, Q$.

Conjecture 1.2. *Every finite group is pq-like.*

This is equivalent to Gr being essentially surjective (when we restrict the categories to finite groups and finite power quandles.) The following theorem highlights why this conjecture is stronger:

Theorem 1.8. *If G and H are finite and pq-like, and $\mathrm{Pq}\, G \cong \mathrm{Pq}\, H$, then $G \cong H$.*

These are our main results regarding pq-like groups, which can be seen as partial results towards Conjecture 1.2.

Theorem 1.9. ***(verified in Lean)*** *A group G is pq-like if and only if there exists a sub-power quandle $Q \subset \mathrm{Pq}\, G$, such that $\mathrm{Gr}\, Q \cong G$.*

Theorem 1.10. *A group is pq-like if and only if there exists a presentation of the group using, in the relations, only conjugation and powers of the generators.*

Theorem 1.11. *All Coxeter groups are pq-like.*

Note all symmetric groups are Coxeter groups.

Theorem 1.12. ***(verified in Lean)*** *Let G and H be pq-like groups and let $\phi : H \to \mathrm{Aut}(G)$ be a homomorphism. If $\phi(x)$ is in the "image" of* Gr *for all x, then $G \rtimes_\phi H$ is pq-like. This condition is always met if G is cyclic, or if ϕ is trivial.*

We believe that in most practical cases, this condition is satisfied, as there is flexibility both in which ϕ to pick, and the power quandles that G and H are pq-like with.

Theorem 1.13. *Finite abelian groups are pq-like.*

Lean Verification. Note also that during the development of the mathematical theory, we have made extensive use of the Lean theorem prover. The system is at [3], while an extensive library within the system that we also used, is at [14]. Lean is a proof assistant, which provides an interactive environment for writing strictly formal proofs, so that one can be sure the results are correct. Not everything in this paper has been formalized in Lean, but several important proofs have been. The code may be accessed at https://github.com/torstein-vik/power-quandle-lean.

SageMath Computation. For algebraic computation, we used SageMath, [11], and specifically GAP [6]. The computational code may be accessed at https://github.com/torstein-vik/power-quandle-computation.

Overview of Paper. We now give an overview of the sections. Section 2, is only about the established theory of quandles which is necessary in this paper. It contains a definition of quandles, and the adjoint pair between them and groups.

Section 3 is about defining the essentials of the theory of power quandles. It also contains the disjoint union of power quandles, which becomes useful later. It contains examples to show that the functor from groups to power quandles is neither essentially surjective, nor full.

Section 4 has a single goal, namely proving that $\mathrm{Pq}\, G \cong \mathrm{Pq}\, H$ implies $\mathrm{Z}\, G \cong \mathrm{Z}\, H$ for finite G and H.

Section 5 has an analogous goal, namely proving that $\mathrm{Pq}\, G \cong \mathrm{Pq}\, H$ implies $G/(\mathrm{Z}\, G) \cong H/(\mathrm{Z}\, H)$. Perhaps surprisingly, it has a completely different proof path. It also combines this with the main theorem of Section 4, to give a theorem displaying G and H both as central extensions of A by K, where $A \cong \mathrm{Z}\, G \cong \mathrm{Z}\, H$ and $K \cong G/(\mathrm{Z}\, G) \cong H/(\mathrm{Z}\, H)$ given that $\mathrm{Pq}\, G \cong \mathrm{Pq}\, H$. It also combines with Section 4 to give that two finite simple groups G, H with $\mathrm{Pq}\, G \cong \mathrm{Pq}\, H$ implies $G \cong H$.

Section 6 establishes the theory of abelian power quandles, which is not highly interconnected with the rest of the theory, but provides a valuable tool to exclude the possibility that $\mathrm{Pq}\, G \cong \mathrm{Pq}\, H$ when this is otherwise hard to do. We prove that in an abelian power quandle, we have $a \rhd b = b$. We also demonstrate how the abelian power quandle of a group contains information about the conjugacy classes in the group, as well as the power maps between these.

Section 7 introduces the functor Gr, which is left adjoint to Pq and is the central object of study for the remainder of the paper. We compute Gr Pq for several groups, and show that it is not the identity functor. We prove that the kernel of the counit $\epsilon : \mathrm{Gr}\, \mathrm{Pq}\, G \to G$ is in the center of $\mathrm{Gr}\, \mathrm{Pq}\, G$, meaning it is an abelian group. We also prove that $\mathrm{Gr}(Q_1 \uplus Q_2) \cong \mathrm{Gr}\, Q_1 \times \mathrm{Gr}\, Q_2$. Finally, we create a tool for determining whether a power quandle morphism is also a group homomorphism.

Section 8 introduces the property that a group may be pq-like, meaning that for G there exists Q such that $G \cong \mathrm{Gr}\, Q$. We prove that G pq-like implies $\mathrm{Gr}\, \mathrm{Pq}\, G \cong A \times G$ for some abelian group A, and use this to prove that if G and H are pq-like and finite, and $\mathrm{Pq}\, G \cong \mathrm{Pq}\, H$, then $G \cong H$. We finally provide a lot of tools for proving that groups are pq-like. This includes restricting the search-space for possible Q's to just the sub-power quandles of $\mathrm{Pq}\, G$, and that G is pq-like is equivalent to the existence of a certain presentation of G using only conjugation and powers. We also prove pq-likeness for direct products, cyclic groups, finite abelian groups, semidirect products $G \rtimes_\phi H$ (under the condition specified in Theorem 1.12 above), and Coxeter groups, including the symmetric groups.

Prerequisites. We assume familiarity with basic group theory and category theory.

Notation. C_n is the cyclic group of n elements. D_n is the dihedral group with $2n$ elements. A_n is the alternating group acting on n elements. S_n is the symmetric group acting on n elements.

Q_8 is the quaternion group. $\mathbb{Z}$ is the integers. $\mathrm{Z}\,G$ is the center of G. F_R is the free object generated by the set R, in some category specified by context.

Acknowledgements. Finally, we acknowledge those who were essential in the process of creating this bachelor thesis. First and foremost, Markus Szymik served as supervisor, and was indispensable in both the development of the mathematical ideas, and in the preparation of the paper. Also, Andreas Holmstrom provided many pointers along the way. Finally, I would like to thank my friends and family for their support.

2. Quandles

Quandles are well-established algebraic structures, which are heavily used in knot theory. They have a self-distributive operation $\triangleright$ that is in a sense idempotent and invertible. Every group induces a conjugation quandle, which are the quandles we concern ourselves with in this paper. Adjointly to the conjugation quandle, quandles induce an enveloping group. This induced group is often hard to work with, and a finite group sent through the comonad of conjugation quandle then enveloping group never yields a finite group. For a more thorough introduction to quandles, see [8] or [9] as original sources. [2] and [5] are also good sources. For a more categorical approach, see [12]. For textbooks, see [4] and [10]. This section is based on these sources.

Definition 2.1. A *quandle* is a set together with a binary operation $\triangleright$ subject to the following axioms:

$$a \triangleright (b \triangleright c) = (a \triangleright b) \triangleright (a \triangleright c)$$
$$a \triangleright a = a$$

Finally, we require that the map $b \mapsto a \triangleright b$ is bijective for all a. Indeed, it is an automorphism of the quandle structure due to the first axiom. This means:

$$a \triangleright b = a \triangleright c \Rightarrow a = c$$

and that, for all a, c there exists b such that:

$$a \triangleright b = c$$

Remark 2.2. We may use an alternate definition that circumvents the existential quantifier. This introduces a second operation $\triangleleft$ such that:

$$(a \triangleright b) \triangleleft a = b$$
$$a \triangleright (b \triangleleft a) = b$$
$$a \triangleleft a = a$$

This is indeed equivalent. However, this second operation can be a nuisance to carry around, but can be useful when an existential qualifier is undesirable. For power quandles, it does not matter as we can define $b \triangleleft a = a^{-1} \triangleright b$.

Definition 2.3. The *conjugation quandle* of a group $\mathrm{Conj}(G)$ is a quandle defined by the same set and the operation $a \triangleright b = aba^{-1}$ (and $b \triangleleft a = a^{-1}ba$.)

Definition 2.4. The *enveloping group* of a quandle $\mathrm{Env}(Q)$ is defined as the group:

$$\langle [x] \text{ for } x \in Q \mid \forall x, y \in Q, [x][y][x]^{-1} = [x \triangleright y] \rangle$$

This is left-adjoint to the functor taking a group to its conjugation quandle.

Remark 2.5. Quandles are not a very good tool for faithfully describing groups, because every element in the center is structurally the same. This means they do very poorly describing abelian groups. In particular, the conjugation quandle of abelian groups are isomorphic when the groups have the same order. Also, the enveloping group tends to be large and unwieldy. On the other hand, the power quandle analogue of the enveloping group is often not very much larger than the input quandle.

Example 2.6. The groups C_4 and $\mathrm{C}_2 \times \mathrm{C}_2$ have the same conjugation quandle. Both are four elements with $a \triangleright b = b$ for all a, b.

3. Power Quandles

In this section we define power quandles and their basic properties. We also show how groups are power quandles.

Definition 3.1. A *power quandle* is a quandle Q with an additional family of unary operations $\pi_n : Q \to Q$ where $n \in \mathbb{Z}$ with notation $a^n := \pi_n(a)$, subject to the following axioms:

$$a^1 = a \tag{3.1}$$

$$(a^n)^m = a^{n \cdot m} \tag{3.2}$$

$$a \rhd (b^0) = b^0 \tag{3.3}$$

$$(a \rhd b)^n = a \rhd (b^n) \tag{3.4}$$

$$(a^0) \rhd b = b \tag{3.5}$$

$$a^n \rhd (a^m \rhd b) = a^{n+m} \rhd b \tag{3.6}$$

Remark 3.2. We clearly get a category of power quandles, called **PowQdl**. Morphisms are maps that preserve $\rhd$ and powers. It is clear they then also preserve $\lhd$.

Remark 3.3. The first two equations say that the power operations π forms an action of the abelian monoid $(\mathbb{Z}, \times)$ on Q. If we define $L_a : b \mapsto a \rhd b$ then we see that this is an automorphism of the power quandle structure. Finally, noting that:

$$L_{a^n} = (L_a)^n$$

gives the last two axioms. One might also interpret the map $a \to L_a$ as being a homomorphism of power quandles, where $\mathrm{Aut}(Q)$ is interpreted as a power quandle via $f \rhd g = fgf^{-1}$ and f^n is repeated composition. The third axiom says that elements like a^0 are fixed by all the L_b automorphisms.

Remark 3.4. Quandles only include one of the possible binary operations in a group, but power quandles also capture all the unary operations possible in a group. This is because n-ary operations in a group can be defined as elements in the free group with n elements, as they are all the ways to combine n many different elements. The free group generated by one element is the infinite cyclic group, $\mathbb{Z}$, which is exactly the power maps.

Remark 3.5. If one is concerned about the operation $\lhd$ that quandles are sometimes defined using, then consider the following equations:

$$a \rhd (a^{-1} \rhd b) = a^0 \rhd b = b$$

$$a^{-1} \rhd (a \rhd b) = a^0 \rhd b = b$$

It is clear that the map $b \mapsto a^{-1} \rhd b$ is the inverse map to $b \mapsto a \rhd b$. However, $\lhd$ is defined by $b \mapsto b \lhd a$ being the inverse of that. So, since the inverse map is unique, we get that:

$$b \lhd a = a^{-1} \rhd b$$

Hence the operation $\lhd$ is completely determined by the other operations.

Remark 3.6. One might note symmetrically that $a \rhd b = b \lhd (a^{-1})$. This is because:

$$b \lhd (a^{-1}) = (a^{-1})^{-1} \rhd b = a^{(-1)\cdot(-1)} \rhd b = a^1 \rhd b = a \rhd b$$

Remark 3.7. Here we list the $\lhd$ variants of the axioms involving $\rhd$:

$$(b^0) \lhd a = b^0 \tag{3.7}$$

$$(b \lhd a)^n = (b^n) \lhd a \tag{3.8}$$

$$b \lhd (a^0) = b \tag{3.9}$$

$$(b \lhd (a^m)) \lhd (a^n) = b \lhd (a^{n+m}) \tag{3.10}$$

The proofs are all straightforward.

Theorem 3.8. ***(verified in Lean)*** *We have:*

$$a^n \rhd a^m = a^m$$

Proof. We begin with the following special case:

$$a \rhd (a^n) = a^n$$

This is easily proven by:

$$a \rhd (a^n) = (a \rhd a)^n = a^n$$

Second we prove the following special case:

$$a^{-1} \rhd a = a$$

Since conjugation by an element is bijective, it is sufficient to show:

$$a \rhd (a^{-1} \rhd a) = a \rhd a$$

The left hand side simplifies like this:

$$a \rhd (a^{-1} \rhd a) = a^{1+-1} \rhd a = a^0 \rhd a = a$$

And the right hand side simplifies axiomatically to a, which is the same. Hence $a^{-1} \rhd a = a$. Now the following is easy:

$$a^{-1} \rhd (a^n) = a^n$$

It follows analogously to the first statement:

$$a^{-1} \rhd (a^n) = (a^{-1} \rhd a)^n = a^n$$

To prove $a^n \rhd a^m = a^m$ notice first how:

$$a^{n+1} \rhd a^m = a^n \rhd (a \rhd a^m) = a^n \rhd a^m$$

$$a^{n-1} \rhd a^m = a^n \rhd (a^{-1} \rhd a^m) = a^n \rhd a^m$$

These are inductive steps, in both directions. What remains is the base case:

$$a^0 \rhd a^m = a^m$$

Which follows axiomatically. □

Example 3.9. Given a group G, we may define a power quandle $\operatorname{Pq} G$ by $a \rhd b = aba^{-1}$, and a^n as group power (that is, inductively by $a^{n+1} = a^n \cdot a$ and $a^0 = 1$ and $a^{-n} = (a^n)^{-1}$). The quandle axioms are inherited from the conjugation quandle of a group, and the power quandle axioms are mostly trivial. We showcase one:

$$(aba^{-1})^n = a(b^n)a^{-1}$$

This follows because the a's cancel in repeated multiplication. One can use a variant of induction to prove it formally.

Definition 3.10. We define Pq as the "forgetful" functor $\operatorname{Pq} : \mathbf{Grp} \to \mathbf{PowQdl}$ taking $G \mapsto \operatorname{Pq} G$, as defined above. If $f : G \to H$ is a group homomorphism then $f : \operatorname{Pq} G \to \operatorname{Pq} H$ (same map as the underlying sets are the same) is clearly a power quandle morphism.

Remark 3.11. It is clear that the categorical product of power quandles is the Cartesian product with pointwise operations. Indeed, as we will see later, Pq is a right-adjoint so group products and power quandle products are compatible. Also, we get from this that $\mathrm{Pq}\,1$ is the terminal power quandle. This is the singleton set with all operations defined the only possible way.

Remark 3.12. The initial power quandle is the empty set $\varnothing$ with operations defined the only possible way. It is clear that this is categorically initial.

Definition 3.13. (verified in Lean) Now, we define the (disjoint) *union* of power quandles $Q_1 \uplus Q_2$. It is defined as having the underlying set of the disjoint union, where we label the elements as a tuple, either $(a, 0)$ where $a \in Q_1$ or $(a, 1)$ where $a \in Q_2$. We define the operations as:

$$\begin{gathered}
(a,0)^n = (a^n, 0) \\
(a,1)^n = (a^n, 1) \\
(a,0) \triangleright (b,0) = (a \triangleright b, 0) \\
(a,1) \triangleright (b,1) = (a \triangleright b, 1) \\
(a,0) \triangleright (b,1) = (b,1) \\
(a,1) \triangleright (b,0) = (b,0) \\
b \triangleleft a = a^{-1} \triangleright b
\end{gathered}$$

To verify the axioms here the strategy is to split into all possible cases and verify them, and all of those cases are decided either by axioms for Q_1 and Q_2 or trivially as the operation $a \triangleright b = b$ always satisfies all the axioms. We will not write these down here, as there are many cases to do.

Example 3.14. This gives rise to power quandles that do not come from groups, meaning the functor Pq is not essentially surjective. A very simple example is $(\mathrm{Pq}\,\mathrm{C}_1) \uplus (\mathrm{Pq}\,\mathrm{C}_2)$. This is a power quandle of order (cardinality) 3, so if it arises from a group that group would have to be C_3, as it is the only group of order 3. This is not right, as the power structure is different. Another way to see this is to notice that a^0 can be two different values depending on whether a is from C_1 or C_2, in a sense there are two "identity" elements. For any group, a^0 is always equal to the unique element 1. Concerning the different power structures, we create the following table for π_2 in $\mathrm{Pq}\,\mathrm{C}_3$:

x	1	g	g^2
x^2	1	g^2	g

And now in $(\mathrm{Pq}\,\mathrm{C}_1) \uplus (\mathrm{Pq}\,\mathrm{C}_2)$:

x	$1 \in \mathrm{C}_1$	$1 \in \mathrm{C}_2$	$g \in \mathrm{C}_2$
x^2	$1 \in \mathrm{C}_1$	$1 \in \mathrm{C}_2$	$1 \in \mathrm{C}_2$

Example 3.15. Not all power quandle morphisms are group homomorphism when seen on the same set. This means the functor Pq is not full. An example can be found for $\mathrm{C}_2 \times \mathrm{C}_4$. The concrete map, call it f, is the one swapping $(1, 1)$ and $(1, 3)$. Note the notation may be a bit confusing, as $(1, 1)^3$ will be $(1, 3)$, it is repeated addition, not multiplication. To show this is a power quandle homomorphism, we may ignore the conjugation operation as it is inert in an abelian group. Hence the powers are sufficient (from 0 to 3 as the group has elements of order at most 4):

$$f((a,b)^0) = f(1) = 1 = f(a,b)^0$$

$$f((a,b)^1) = f(a,b) = f(a,b)^1$$
$$f((a,b)^2) = f(0,b^2) = f(0,b)^2$$

The last step here is because f does nothing to $(0,b)$. Finally:

$$f((a,b)^3) = f(a,b^3)$$

In the case that $a = 0$ this is again trivial, so we may assume $a = 1$. Now there are four cases:

$$f(1,0^3) = (1,0) = f(1,0)^3$$
$$f(1,1^3) = f(1,3) = (1,1) = (1,3)^3 = f(1,1)^3$$
$$f(1,2^3) = f(1,2) = (1,2) = (1,2)^3 = f(1,2)^3$$
$$f(1,3^3) = f(1,1) = (1,3) = (1,1)^3 = f(1,3)^3$$

Hence we see that f is a power quandle homomorphism. It has also been verified by computer, iterating all elements and powers. However, the computer has also verified it is not a group homomorphism. To see this with human eyes, pick:

$$f((1,3)\cdot(1,0)) = f(0,3) = (0,3)$$
$$f(1,3)\cdot f(1,0) = (1,1)\cdot(1,0) = (0,1)$$

We see they disagree, and hence f is not a group homomorphism. In this group, there are indeed several other such morphisms.

Remark 3.16. Even though Pq is neither full nor essentially surjective, it is still a very useful invariant. It is obviously faithful. The missing piece is what we call *essentially injective.* The definition of this is that $\mathrm{Pq}\, G \cong \mathrm{Pq}\, H$ implies $G \cong H$. We make much progress on this question. One might confuse essentially injective with conservative, but they are not the same. Essentially injective says that if there exists a power quandle isomorphism between $\mathrm{Pq}\, G$ and $\mathrm{Pq}\, H$, then there exists a group isomorphism between G and H. Conservative says that if $\mathrm{Pq}(f)$ is an isomorphism, then so is f. It is obvious that Pq is conservative, but it is not at all obvious that it is essentially injective.

Remark 3.17. A power quandle of the form $\mathrm{Pq}\, G$ comes with an element 1 such that $a^0 = 1$ for all a. There are power quandles without such an element, for example $\varnothing$ or $\mathrm{Pq}\, G \uplus \mathrm{Pq}\, H$. A closely related observation is that it is not always true that $a^0 = b^0$, as in $\mathrm{Pq}\, G \uplus \mathrm{Pq}\, H$, where $a \in G$ and $b \in H$ don't satisfy this. One might define a pointed power quandle as a power quandle with a specified element 1 such that $a^0 = 1$ for all a, but we don't use this.

4. Centers

In this section we prove that given $\operatorname{Pq} G \cong \operatorname{Pq} H$, then $\operatorname{Z} G \cong \operatorname{Z} H$, given that G and H are finite, which we assume for the rest of the section. First we need a theorem which is folklore, but which we provide an original proof for. The theorem is that for finite abelian groups, a power-preserving bijection implies isomorphism between the two groups. We will state the theorem properly when we are ready, first we need some tools.

Definition 4.1. Let G be a group. We define:

$$f_G(n) := \#\{x \in G \mid x^n = 1\}$$

That is, the number of elements in the group that become 1 when raised to the n-th power. Equivalently, it is the number of elements whose order divides n. Note we could define this in a power quandle, as $\#\{x \in G \mid x^n = x^0\}$, but we make no use of this.

It is clear that when G, H are isomorphic, then $f_G = f_H$. The current goal is the converse (for finite abelian groups), i.e. to show that $f_G(n) = f_H(n)$ for all n where G, H are finite abelian groups, implies $G \cong H$. Note "finite" here is indispensable, as $f_{C_\infty} = f_{C_\infty \times C_\infty}$, as both of these are always 1, just the identity element. The strategy is to use the classification theorem for finite abelian groups. For this we need a few lemmas first, regarding how this definition interacts with cyclic groups and product groups:

Lemma 4.2. *We specify the function for the cyclic groups:*

$$f_{\mathrm{C}_k}(n) = \gcd(k, n)$$

Proof. Let g be the generator of C_k. We see that:

$$f_{\mathrm{C}_k}(n) = \#\{x \in \mathrm{C}_k \mid x^n = 1\} = \#\{0 < j \leq k \mid (g^j)^n = 1\}$$
$$= \#\{0 < j \leq k \mid j \cdot n = 0 \mod k\} = \#\{0 < j \leq k \mid k | j \cdot n\}$$

Let $j' = k / \gcd(k, n)$. Put this into the relation, and we get $n \cdot k / \gcd(k, n) = \operatorname{lcm}(k, n)$, and it is clear that $k | \operatorname{lcm}(k, n)$. In fact, $\operatorname{lcm}(k, n)$ is the smallest number which k divides and that has n as a factor. Hence, j' is the smallest value that satisfies this condition. Notice that $j = l \cdot j'$ for some l is equivalent to $k | j \cdot n$. Hence:

$$= \#\{0 < j \leq k \mid k | j \cdot n\} = \#\{l | 0 < j' \cdot l \leq k\}$$

Since $k | j'$ we may write:

$$= \#\{l | 0 < l \leq k/j'\} = k/j' = k/(k/\gcd(k, n)) = \gcd(k, n)$$

Which is what was to be shown. □

Lemma 4.3. *Now we specify the interaction of the function with group product:*

$$f_{G \times H}(n) = f_G(n) \cdot f_H(n)$$

Proof.

$$\begin{aligned} f_{G \times H}(n) &= \#\{x \in G \times H \mid x^n = 1\} \\ &= \#\{(x, y) \in G \times H \mid (x, y)^n = 1\} \\ &= \#\{x \in G, y \in H \mid x^n = 1 \wedge y^n = 1\} \\ &= \#(\{x \in G \mid x^n = 1\} \times \{y \in H \mid y^n = 1\}) \\ &= \#\{x \in G \mid x^n = 1\} \cdot \#\{y \in H \mid y^n = 1\} \\ &= f_G(n) \cdot g_H(n) \end{aligned}$$

□

Lemma 4.4. *Let G, H be finite abelian groups. Suppose $f_G(n) = f_H(n)$ for all n. Then $G \cong H$.*

Proof. We assume G, H are both non-trivial. If one of them is trivial, then $f_G(n) = f_H(n) = 1$, and they clearly both are, as if there was another element in one of them it would make this value not 1 for at least one value of n. So they are in that case both trivial, and the statement holds. Hence, going forward we may assume G, H non-trivial.

Use the classification theorem for finite abelian groups, and write $G \cong G' = \mathrm{C}_{a_0} \times \mathrm{C}_{a_1} \times \ldots \times \mathrm{C}_{a_k}$ with $a_i | a_{i+1}$ and $a_i > 1$. Do the same for H, and get data b_i with $0 \leq i \leq k'$ and $b_i | b_{i+1}$ and $b_i > 1$. Notice $f_{G'}(n) = f_{H'}(n)$. Also notice we can compute these:

$$f_{G'}(n) = \prod_i \gcd(a_i, n)$$

$$f_{H'}(n) = \prod_i \gcd(b_i, n)$$

This yields:

$$\prod_i \gcd(a_i, n) = \prod_i \gcd(b_i, n)$$

It is now sufficient to prove $a_i = b_i$ and $k = k'$ as that would yield $G' = H'$ which again yields the goal, $G \cong H$. We begin with $k = k'$. Assume not, and without loss of generality assume $k < k'$. We need to find a contradiction. Insert $n = b_0$. We get:

$$\prod_i \gcd(a_i, b_0) = \prod_i \gcd(b_i, b_0)$$

Since $b_i | b_{i+1}$ we get by transitivity that $b_0 | b_i$, yielding $\gcd(b_i, b_0) = b_0$. So we get:

$$\prod_i \gcd(a_i, b_0) = b_0^{k'}$$

However, notice also that the gcd on the left-hand side can at most be b_0, so:

$$\prod_i \gcd(a_i, b_0) \leq \prod_i b_0 = b_0^k$$

However, notice that $b_0 > 1$ and $k < k'$, so we get:

$$\prod_i \gcd(a_i, b_0) < \prod_i \gcd(b_i, b_0)$$

This is a contradiction. This gives us $k' = k$, so we write k instead of k' from now on. Now, to prove that $a_i = b_i$. We do the same, set $n = a_0$. Again, we get:

$$\prod_i \gcd(a_i, b_0) = b_0^k$$

Notice that since $\gcd(a_i, b_0) \leq b_0$, in order to reach b_0^k, every a_i must have a gcd of b_0 with b_0. So,

$$\gcd(a_i, b_0) = b_0$$

Pick $i = 0$ and get $\gcd(a_0, b_0) = b_0$. Now, repeat the analogous argument with a_0 instead of b_0. Everything is the same, so we get $\gcd(a_0, b_0) = a_0$. Combined with the earlier conclusion, we get $a_0 = b_0$. Now, cancel both these factors on both sides of the main equation, and apply a suitable induction principle for lists. The base case is that of the empty list, which are trivially equal. This is all we need to prove $G \cong H$.

□

Proposition 4.5. *Let f be a bijection between two finite abelian groups G and H, that is not necessarily a homomorphism. However, it satisfies $f(x^n) = f(x)^n$ for all x in G and integers n. Then $G \cong H$ as groups, even though f may not be an isomorphism.*

Proof. We use the previous lemma. What remains to prove is $f_G(n) = f_H(n)$ for all n. We prove this the following way:

$$\begin{aligned} f_G(n) &= \#\{x \in G \mid x^n = 1\} \\ &= \#\{x \in G \mid (f^{-1}(f(x)))^n = 1\} \\ &= \#\{x \in H \mid (f^{-1}(x))^n = 1\} \\ &= \#\{x \in H \mid f^{-1}(x^n) = 1\} \\ &= \#\{x \in H \mid x^n = 1\} \\ &= f_H(n) \end{aligned}$$

The second to last step follows because $f(x) = 1$ iff $x = 1$. This is because f is a bijection, and that $f(1) = f(x^0) = f(x)^0 = 1$. □

Definition 4.6. We define the *center* of a quandle Q, notated as $\mathrm{Z}\,Q$, as the sub-quandle defined by the following criteria:

$$\mathrm{Z}\,Q := \{x \in Q \mid \forall y, y \rhd x = x\}$$

We need to show this is closed under the quandle operation. Suppose $a, b \in \mathrm{Z}\,Q$, this means $y \rhd a = a$ and $y \rhd b = b$ for all y. Now, we see $a \rhd b \in \mathrm{Z}\,Q$ because $y \rhd (a \rhd b) = (y \rhd a) \rhd (y \rhd b) = a \rhd b$. If one is worried about $\lhd$ (whether the quandle operation is still bijective when the first argument is fixed), then note $y \rhd (a \lhd b) = (y \rhd a) \lhd (y \rhd b)$ because, taking $\lhd y$ of each side we get:

$$(y \rhd (a \lhd b)) \lhd y = a \lhd b$$

$$((y \rhd a) \lhd (y \rhd b)) \lhd y = ((y \rhd a) \lhd y) \lhd ((y \rhd b) \lhd y) = a \lhd b$$

We define the center of a power quandle Q as the center of the underlying quandle, and show that the power operations are closed. Suppose $a \in \mathrm{Z}\,Q$, i.e. $y \rhd a = a$ for all y. Then $a^n \in \mathrm{Z}\,Q$ because $y \rhd a^n = (y \rhd a)^n = a^n$.

Theorem 4.7. *The centers of groups and power quandles coincide, i.e.* $\mathrm{Pq}(\mathrm{Z}\,G) \cong \mathrm{Z}(\mathrm{Pq}\,G)$.

Proof. We need to prove that $x \in \mathrm{Z}\,G$ is equivalent to $x \in \mathrm{Z}(\mathrm{Pq}\,G)$, and the rest follows trivially. This is because $y \rhd x = x$ is clearly equivalent to $xy = yx$. □

Theorem 4.8. *Given finite groups G, H and* $\mathrm{Pq}\,G \cong \mathrm{Pq}\,H$, *then* $\mathrm{Z}\,G \cong \mathrm{Z}\,H$

Proof. Notice that $f : \mathrm{Pq}\,G \cong \mathrm{Pq}\,H$ clearly implies $f : \mathrm{Z}(\mathrm{Pq}\,G) \cong \mathrm{Z}(\mathrm{Pq}\,H)$ (not because Z is a functor, because it is not, but because the property of an element $x \in \mathrm{Z}(\mathrm{Pq}\,G)$ is clearly transferable by isomorphism giving $f(x) \in \mathrm{Z}(\mathrm{Pq}\,H)$, although one might say Z is a functor with respect to isomorphisms). Further, we use the previous theorem to give $f' : \mathrm{Pq}(\mathrm{Z}\,G) \cong \mathrm{Pq}(\mathrm{Z}\,H)$. Now notice that $\mathrm{Z}\,G$ and $\mathrm{Z}\,H$ are finite abelian groups with a bijection with the property $f(x^n) = f(x)^n$, so it follows that $\mathrm{Z}\,G \cong \mathrm{Z}\,H$ as groups. □

Corollary 4.9. *Given two finite abelian groups G, H satisfying* $\mathrm{Pq}\,G \cong \mathrm{Pq}\,H$, *then $G \cong H$, i.e. G and H are isomorphic as groups.*

Proof. This follows from $G \cong \mathrm{Z}(G)$ for finite abelian groups. □

The conclusion here is that the center is reconstructible, in the sense that power-quandle-isomorphic groups have isomorphic centers.

5. Center Quotients

In this section we prove that if $\mathrm{Pq}\,G \cong \mathrm{Pq}\,H$, then $G/\,\mathrm{Z}(G) \cong H/\,\mathrm{Z}(H)$. We also combine this with the previous section in order to relate G and H even further.

Definition 5.1. For the rest of the section, take $f : \mathrm{Pq}\,G \to \mathrm{Pq}\,H$ a power quandle isomorphism. Then we can construct a map $\overline{f} : G \to H/\,\mathrm{Z}(H)$ in the following manner: First, take $f' : G \to H$ directly from f as G and $\mathrm{Pq}\,G$ are the same set. Then, compose with the projection $H \to H/\,\mathrm{Z}(H)$.

Lemma 5.2. *If $a, b \in G$ satisfy $a \rhd x = b \rhd x$ for all x, then $a = cb$ where $c \in \mathrm{Z}\,G$.*

Proof. We clearly see that $c = ab^{-1}$ works, we just have to prove that $c \in \mathrm{Z}\,G$. We do this by noticing $c \in \mathrm{Z}\,G$ if $c \rhd y = y$ for all y, because this equation is $cyc^{-1} = y$, clearly equivalent to $cy = yc$, which is clearly equivalent to $c \in \mathrm{Z}\,G$. We get:

$$c \rhd y = (ab^{-1}) \rhd y = a \rhd (b^{-1} \rhd y)$$

Now we may use $a \rhd x = b \rhd x$ with $x = b^{-1} \rhd y$, and get:

$$= b \rhd (b^{-1} \rhd y) = b^0 \rhd y = y$$

Which is what was to be shown. □

Lemma 5.3. *We have that for all $a, b \in G$ there exists $c \in H$, such that $f(ab) = cf(a)f(b)$ with $c \in \mathrm{Z}(H)$.*

Proof. First notice that $x \rhd (y \rhd z) = x(yzy^{-1})x^{-1} = (xy)z(xy)^{-1} = (xy) \rhd z$. Using this, we see that for all x, we have $f(a) \rhd (f(b) \rhd x) = (f(a)f(b)) \rhd x$. Since f is bijective, we may write $x = f(y)$ in a unique way. We now may write $f(a \rhd (b \rhd y)) = f((ab) \rhd y)$. As f is a power quandle homomorphism, we get $f(a) \rhd (f(b) \rhd x) = f(ab) \rhd x$. Again, the left hand side may be rewritten, giving $(f(a)f(b)) \rhd x = f(ab) \rhd x$. Now we may use the previous lemma, giving us $f(ab) = cf(a)f(b)$ with $c \in \mathrm{Z}(H)$, which is what was to be obtained. □

Lemma 5.4. *$\overline{f}$ is a group homomorphism.*

Proof. Since $\overline{f}$ is just f composed with quotienting out by $\mathrm{Z}(H)$, we get from the previous theorem:

$$\overline{f}(ab) = c\overline{f}(a)\overline{f}(b) \mod \mathrm{Z}(H)$$

Since $c \in \mathrm{Z}(H)$, we clearly get:

$$\overline{f}(ab) = \overline{f}(a)\overline{f}(b)$$

Which is what was to be shown. □

Theorem 5.5. ***(verified in Lean)***

$$G/\,\mathrm{Z}(G) \cong H/\,\mathrm{Z}(H)$$

Proof. We use the first isomorphism theorem on $\overline{f}$. We get:

$$G/\ker \overline{f} \cong \operatorname{im} \overline{f}$$

Since f was bijective, and was composed with a surjective map, it is clear that $\overline{f}$ is surjective. We may write:

$$G/\ker \overline{f} \cong H/\,\mathrm{Z}(H)$$

What remains to prove is that $\ker \overline{f} \cong \mathrm{Z}(G)$. Since they are both subgroups of G, it is sufficient to prove that for all $x \in G$, then

$$x \in \ker \overline{f} \Leftrightarrow x \in \mathrm{Z}(G)$$

Unfolding both sides, we get:

$$\overline{f}(x) = 1 \Leftrightarrow \forall y, xy = yx$$

Notice that $\overline{f}(x) = 1$ if and only if $f(x) \in \mathrm{Z}(H)$. So we need to prove:

$$\forall y \in H, f(x)y = yf(x) \Leftrightarrow \forall y \in G, xy = yx$$

We rewrite algebraically on both sides:

$$\forall y \in H, f(x) \rhd y = y \Leftrightarrow \forall y \in G, x \rhd y = y$$

Now notice that since f is a bijection, and a power quandle homomorphism, we may rewrite the left hand side as follows:

$$\begin{gathered} \forall y \in H, f(x) \rhd y = y \\ \Leftrightarrow \forall y \in G, f(x) \rhd f(y) = f(y) \\ \Leftrightarrow \forall y \in G, f(x \rhd y) = f(y) \\ \Leftrightarrow \forall y \in G, x \rhd y = y \end{gathered}$$

And this was the goal. Hence, $\ker \overline{f} \cong \mathrm{Z}(G)$, and hence:

$$G/\,\mathrm{Z}(G) \cong H/\,\mathrm{Z}(H)$$

□

Corollary 5.6. *Given two centerless groups G, H satisfying $\mathrm{Pq}\, G \cong \mathrm{Pq}\, H$, then $G \cong H$, i.e. G and H are isomorphic as groups.*

Proof. This follows from that $G \cong G/(\mathrm{Z}\, G)$, because $\mathrm{Z}\, G \cong 1$, for centerless groups. □

The conclusion here is that the center quotient is reconstructible, in the sense that power-quandle-isomorphic groups have isomorphic center quotients.

Theorem 5.7. *Given finite groups G and H with $\mathrm{Pq}\, G \cong \mathrm{Pq}\, H$, then H is isomorphic to a central extension of $\mathrm{Z}(G)$ by $G/\,\mathrm{Z}(G)$.*

Proof. Since $\mathrm{Z}(G) \cong \mathrm{Z}(H)$ and $G/\,\mathrm{Z}(G) \cong H/\,\mathrm{Z}(H)$ it is sufficient to prove H is a central extension of $\mathrm{Z}(H)$ by $H/\,\mathrm{Z}(H)$. This is trivial, as any group is an extension of a subgroup and its quotient. The extension is central because the subgroup is the center, and thus clearly a (non-proper) subgroup of the center. □

Remark 5.8. Symmetrically, G is isomorphic to a central extension of $\mathrm{Z}(H)$ by $H/\,\mathrm{Z}(H)$ by exchanging G and H.

Corollary 5.9. *The candidates for H are classified by the second group cohomology:*

$$\mathrm{H}^2(G/Z(G), Z(G))$$

Proof. It is well known that the second group cohomology $\mathrm{H}^2(G, A)$ classifies the central extensions of A by G. We know that H is a central extension of $\mathrm{Z}(G)$ by $G/\,\mathrm{Z}(G)$. □

Theorem 5.10. *Given two finite simple groups G, H with $\mathrm{Pq}\, G \cong \mathrm{Pq}\, H$, then $G \cong H$.*

Proof. All finite simple groups are either abelian or centerless. In the case that both are abelian, or both are centerless, we already know this. In the mixed case, we may assume without loss of generality that G is abelian and H is centerless. Then we get:

$$\begin{gathered} G \cong \mathrm{Z}\, G \cong \mathrm{Z}\, H \cong 1 \\ H \cong H/\,\mathrm{Z}\, H \cong G/\,\mathrm{Z}\, G \cong 1 \end{gathered}$$

The first steps are because they are abelian (resp. centerless), the second follows from $\operatorname{Pq} G \cong \operatorname{Pq} H$, and the final step is because the other group is centerless (resp. abelian). Hence we get:

$$G \cong 1 \cong H$$

as desired. However, this also tells us that the only case in which $\operatorname{Pq} G \cong \operatorname{Pq} H$ and G is abelian and H centerless, is when they are both trivial. □

6. Abelian Power Quandles

It is often a good idea to study the "abelian" or commutative part of a theory. Applying this to power quandles, we could define an abelian power quandle in many different ways. A good definition should have that $a \rhd b = b$, as abelian groups yield this. In this paper we define an abelian power quandle as an abelian group object in the category of power quandles, and as we will see it indeed follows that $a \rhd b = b$. The main advantage of defining it this way is that we automatically get an abelianization functor from power quandles to abelian power quandles, which is left-adjoint to a forgetful functor. This abelianization functor is a powerful invariant, which we can use to exclude isomorphism of power quandles. This section takes many ideas from [13], including the definition of abelian group objects in a category and the abelianization functor. See [1] as an original source for abelian group objects.

Definition 6.1. Given a category (with finite products) $\mathcal{C}$, we can form another category of *abelian group objects* in the given category, $\mathrm{Ab}(\mathcal{C})$. An abelian group object in the category $\mathcal{C}$ is an object $X \in \mathrm{Ob}(\mathcal{C})$ together with morphisms [1]:

(1) $e : \{*\} \to X$
(2) $i : X \to X$
(3) $a : X \times X \to X$

With the following notation:

(1) $0 := e()$
(2) $-x := i(x)$
(3) $x + y := a(x, y)$

Subject to the following axioms:

(1) $(a + b) + c = a + (b + c)$
(2) $0 + a = a$
(3) $a + b = b + a$
(4) $-a + a = 0$

Remark 6.2. The above definition uses elements for the axioms and notation, which only makes sense for a concrete category, but all the axioms can be defined equivalently using only composition.

Definition 6.3. *Abelian power quandles* are abelian group objects in the category of power quandles.

Theorem 6.4. ***(verified in Lean)*** *In all abelian power quandles, we have:*

$$a \rhd b = b$$

Proof. First, since addition is a power quandle morphism, we get that:

$$(a + b) \rhd (c + d) = (a \rhd c) + (b \rhd d)$$

Now, we see the following:

$$a \rhd b = (a + 0) \rhd (0 + b) = (a \rhd 0) + (0 \rhd b)$$

Now define:

$$\epsilon(x) = x \rhd 0$$

$$\alpha(x) = 0 \rhd x$$

We get

$$a \rhd b = \epsilon(a) + \alpha(b)$$

We now prove that $0^0 = 0$. First, since addition is a power quandle morphism, we get that:

$$(a+b)^n = a^n + b^n$$

Now, note that:

$$\begin{gathered} 0^0 = (0+0)^0 = 0^0 + 0^0 \\ 0^0 - 0^0 = 0^0 + 0^0 - 0^0 \\ 0 = 0^0 + 0 = 0^0 \end{gathered}$$

Now we see:

$$\begin{gathered} \epsilon(a) = a \rhd 0 = a \rhd 0^0 = 0^0 = 0 \\ \alpha(b) = 0 \rhd b = 0^0 \rhd b = b \end{gathered}$$

Hence we get:

$$a \rhd b = 0 + b = b$$

Which is what was to be proven. □

Definition 6.5. The *abelianization* functor Ω is the left adjoint of the forgetful functor from abelian objects in $\mathcal{C}$ to $\mathcal{C}$. It can be realized using the following recipe [13]:

(1) Take an object X in $\mathcal{C}$.
(2) Write it as a coequalizer of free objects F_G and F_R. This is essentially a presentation with G the set of generators and R the set of relations. The two morphisms $\mathrm{F}_R \to \mathrm{F}_G$ are the left hand side and the right hand side of the relations. This of course only works in categories where every object is isomorphic to a coequalizer of free objects.
$$\mathrm{F}_R \rightrightarrows \mathrm{F}_G \to X$$
(3) The free objects F_S must map to the free objects in $\mathrm{Ab}(\mathcal{C})$ generated by the same set. The coequalizer must also map through as it is a colimit. The arrows are induced.
(4) Obtain ΩX as the cokernel of the difference of the morphisms:
$$\Omega(\mathrm{F}_R) \to \Omega(\mathrm{F}_G) \to \Omega(X)$$

Theorem 6.6. *Every quandle has an associated set set of "orbits": the equivalence classes of the equivalence relation $x \rhd y \sim y$ (y is equivalent to y' if and only if $y' = x \rhd y$ for some x.) The abelianization functor then takes a power quandle Q to the free abelian group generated by this set of orbits, with trivial $\rhd$, and power maps induced by Q.*

Proof. Start with a power quandle Q. Pick the coequalizer:

$$\mathrm{F}_{Q \times Q \cup Q \times \mathbb{Z}} \rightrightarrows \mathrm{F}_Q \to Q$$

We now specify the morphisms. On the left part of the union, the top morphism takes (a, b) to $[a] \rhd [b]$ and the bottom takes it to $[a \rhd b]$. On the right part, the top takes (a, n) to $[a]^n$ and the bottom morphism takes it to $[a^n]$. It is clear then that the coequalizer is F_Q modulo $[a] \rhd [b] = [a \rhd b]$ and $[a]^n = [a^n]$. It is clear this is isomorphic to Q. Now, we apply Ω. The top morphism now takes (a, b) to $[a] \rhd [b] = [b]$ and the bottom takes it to $[a \rhd b]$. The power part is unchanged. Hence, $\Omega(Q)$ is the free abelian power quandle generated by the elements of Q modulo $[a \rhd b] = [b]$ and $[a^n] = [a]^n$. Hence it is Q modulo $a \rhd b = b$ and with addition, and all the axioms of abelian power quandles. □

Corollary 6.7. *The abelianization of the power quandle of a group G, i.e. $\Omega(\mathrm{Pq}\, G)$, is the free abelian (additive) group generated by the conjugacy classes of G with the additional structure of a quandle operation $\rhd$ which is always $a \rhd b = b$ (one might say we may as well just ignore it), and power operations that takes the conjugacy class $[a]$ to $[a^n]$, which is well defined because $a \rhd (b^n) = (a \rhd b)^n$ in any group. Also, we have the interaction that $(a+b)^n = a^n + b^n$, as well as all the axioms of a abelian power quandle.*

Proof. The orbits are the conjugacy classes, conjugation is hence trivial, and the power operations are as usual. □

Remark 6.8. The abelianization functor can be a very useful invariant. Consider what information $\Omega(\mathrm{Pq}\, G)$ contains. It contains all the conjugacy classes, and their power maps between each other. This is information about a group that is very important, it is often placed alongside the character table of the group, as in GAP [6].

7. The Functor Gr

Recall from Section 2 that given a group G, we may form the conjugation quandle $\operatorname{Conj}(G)$ by defining the operation $a \rhd b = aba^{-1}$ and forgetting multiplication. We also recall this functor has a left adjoint, the enveloping group $\operatorname{Env}(Q)$, which is defined as:

$$\langle [x] \text{ for } x \in Q \mid \forall x, y \in Q, [x][y][x]^{-1} = [x \rhd y] \rangle$$

Completely analogously, given a group G we may form the power quandle $\operatorname{Pq} G$, by defining $a \rhd b = aba^{-1}$ and $\pi_n(x) = x^n$, and forgetting multiplication. Now we claim that for formal reasons this has a left adjoint Gr, and that left adjoint can be defined completely analogously as:

$$\langle [x] \text{ for } x \in Q \mid \forall x, y \in Q, [x][y][x]^{-1} = [x \rhd y] \text{ and } \forall x \in Q, n \in \mathbb{Z}, [x]^n = [x^n] \rangle$$

Proof. **(verified in Lean)** We prove this using universal morphisms. We show that Gr is left adjoint to Pq. We need to show that for every group G then we have $\operatorname{Pq}(G)$ and a morphism $\epsilon_G : \operatorname{Gr}(\operatorname{Pq}(G)) \to G$ such that for every power quandle Q and every morphism $f : \operatorname{Gr}(Q) \to G$ there exists a unique morphism $g : Q \to \operatorname{Pq}(G)$ such that $\epsilon_G \circ \operatorname{Gr}(g) = f$.

Assume we are given G and Q and f. We need to construct ϵ_G and g. The first is easy, this is just the surjection that takes $[x]$ to x and maps products homomorphically.

We take g to be the morphism given by $g(x) = f([x])$, since G and $\operatorname{Pq}(G)$ have the same elements this is well-defined. We need to prove the composition $\epsilon_G \circ \operatorname{Gr}(g) = f$. We see that $\operatorname{Gr}(g) : \operatorname{Gr}(Q) \to \operatorname{Gr}(\operatorname{Pq}(G))$ is given by taking $\operatorname{Gr}(g)([x]) = [g(x)] = [f([x])]$ and $\operatorname{Gr}(g)(xy) = \operatorname{Gr}(g)(x) \operatorname{Gr}(g)(y)$. It is sufficient to show for all generators $[x]$, and then we get:

$$\epsilon_G(\operatorname{Gr}(g)([x])) = \epsilon_G([f([x])]) = f([x])$$

Which is what was to be shown. □

Remark 7.1. Gr Pq is a comonad on the category of groups. We call the counit ϵ, and note that it is surjective. This is clear to see, as $\epsilon([x]) = x$.

Remark 7.2. As a way to exclude power quandle isomorphism, one may compute $\operatorname{Gr} Q_1$ and $\operatorname{Gr} Q_2$, and if they are not isomorphic as groups, then Q_1 and Q_2 can not be isomorphic as power quandles either.

Remark 7.3. We have a computer program that can compute $\operatorname{Gr} \operatorname{Pq} G$ using GAP [6] in SageMath [11]. The algorithm can be described as follows:

1. Take a suitable computer representation of a group G (we need a comprehensive list of unique elements and a way to multiply and invert elements, using indices of the elements). Say there are N elements.
2. Create an empty list of relators, that we will later append to. Concretely, this is a list of lists of elements in G, represented as indices.
3. Loop through all the elements a of the group and do the following:
   (a) Loop through all the numbers n from 0 to N, and append the relator:
   $$[a, \ldots n \text{ instances of } a \ldots, a, (a^n)^{-1}]$$
   If $a^n = a$ and $n > 1$, then break, as we have reached the order of the element.
   (b) Loop through all the elements b in the group and compute aba^{-1} and add
   $$[a, b, a^{-1}, (aba^{-1})^{-1}]$$
   to the list of relators.
4. Generate the free group of N elements.
5. Compute the free group modulo the relations, and simplify it.

(6) One now has a computer representation of the group. If this is in GAP for instance, one can use the “StructureDescription” function to compute a text representation of the group.

Note this could be adapted to any power quandle instead of just $\operatorname{Pq} G$, by using a suitable computer representation of the power quandle for generating the relations.

Example 7.4. From the SageMath program we get:

G	$\operatorname{Gr}\operatorname{Pq}(G)$
C_2	C_2
C_3	C_3
C_{10}	C_{10}
$\mathrm{C}_2 \times \mathrm{C}_2$	$\mathrm{C}_2 \times \mathrm{C}_2 \times \mathrm{C}_2$
$\mathrm{C}_3 \times \mathrm{C}_3$	$\mathrm{C}_3 \times \mathrm{C}_3 \times \mathrm{C}_3 \times \mathrm{C}_3$
$\mathrm{C}_4 \times \mathrm{C}_2$	$\mathrm{C}_4 \times \mathrm{C}_2 \times \mathrm{C}_2 \times \mathrm{C}_2$
C_2^3	C_2^7
C_2^4	C_2^{15}
S_3	S_3
S_4	$\mathrm{C}_2 \times \mathrm{S}_4$
A_4	$\mathrm{C}_2 \times \mathrm{A}_4$
A_5	$\mathrm{C}_2 \times \mathrm{A}_5$
$\mathrm{S}_3 \times \mathrm{S}_3$	$\mathrm{C}_2 \times \mathrm{S}_3 \times \mathrm{S}_3$
S_5	$\mathrm{C}_2 \times \mathrm{S}_5$
A_6	$\mathrm{C}_2 \times \mathrm{A}_6$
Q_8	$\mathrm{C}_2 \times \mathrm{Q}_8$
D_4	$\mathrm{C}_2 \times \mathrm{D}_4$
D_5	D_5
D_6	$\mathrm{C}_2 \times \mathrm{D}_6$
D_7	D_7
D_8	$\mathrm{C}_2 \times \mathrm{D}_8$
D_9	D_9
D_{10}	$\mathrm{C}_2 \times \mathrm{D}_{10}$
D_{11}	D_{11}
D_{12}	$\mathrm{C}_2 \times \mathrm{D}_{12}$
D_{13}	D_{13}
D_{14}	$\mathrm{C}_2 \times \mathrm{D}_{14}$
D_{15}	D_{15}
D_{16}	$\mathrm{C}_2 \times \mathrm{D}_{16}$
D_{17}	D_{17}
D_{18}	$\mathrm{C}_2 \times \mathrm{D}_{18}$
D_{19}	D_{19}
D_{20}	$\mathrm{C}_2 \times \mathrm{D}_{20}$

Note that we have changed some of the outputs to isomorphic groups that reflect in a better manner that the right hand side is built from the left. Also, these are perhaps not “proofs” in the traditional sense, so we follow up by proving some of the patterns.

Example 7.5. (verified in Lean)

$$\operatorname{Gr}\operatorname{Pq}\mathrm{C}_n \cong \mathrm{C}_n$$

Proof. $\operatorname{Gr}\operatorname{Pq}\mathrm{C}_n$ has presentation:

$$\langle [x], x \in \mathrm{C}_n \mid \forall xy \in \mathrm{C}_n, [x][y] = [y][x] \text{ and } [x^k] = [x]^k \rangle$$

Now note that for every $x \in \mathrm{C}_n$ we can write $x = g^k$ where g is the generator of C_n. Now the second condition gives us $[x] = [g^k] = [g]^k$, meaning every generator can be expressed using the single generator $[g]$. This means $\operatorname{Gr}\operatorname{Pq}\mathrm{C}_n$ has a single generator, and is hence isomorphic to C_l where l is the order of the generator $[g]$. Note that $[g]^n = [g^n] = [g^0] = [g]^0 = 1$. Note that this is the smallest such number, so $l = n$ and we have shown what was to be shown. □

Example 7.6. (verified in Lean)

$$\operatorname{Gr}\operatorname{Pq}(\mathrm{C}_2^2) \cong \mathrm{C}_2^3$$

Proof. $\operatorname{Gr}\operatorname{Pq}\mathrm{C}_n$ has presentation:

$$\langle [(0,0)], [(1,0)], [(0,1)], [(1,1)] \mid \forall abcd \in \mathrm{C}_2, [(a,b)][(c,d)] = [(c,d)][(a,b)] \text{ and } [(a,b)^k] = [(a,b)]^k \rangle$$

The first condition means nothing more than $\operatorname{Gr}\operatorname{Pq}\mathrm{C}_n$ being abelian. The second condition only needs to be repeated for k either 0 or 1 or 2 due to all elements having order 2. For $k = 0$ it is just $[(a,b)^0] = [(a,b)]^0$ meaning nothing more than $[(0,0)] = 1$. For $k = 1$ it is just $[(a,b)] = [(a,b)]$ containing no information. For $k = 2$ we get $[(a,b)^2] = [(a,b)]^2$ giving us $[(a,b)]^2 = [(0,0)] = 1$, meaning each element has order two. So a comprehensive list about the information we have about $\operatorname{Gr}\operatorname{Pq}\mathrm{C}_2^2$ is that:

(1) It has three generators, since the generator $[(0,0)] = 1$ and is hence trivial.
(2) Every element has order 2.
(3) It is abelian.

This uniquely determines that $\operatorname{Gr}\operatorname{Pq}(\mathrm{C}_2^2) \cong \mathrm{C}_2^3$ □

Remark 7.7. This example shows that in general, $\operatorname{Gr}\operatorname{Pq} G$ is not always isomorphic to G.

Example 7.8. For odd n,

$$\operatorname{Gr}\operatorname{Pq}\mathrm{D}_n \cong \mathrm{D}_n$$

Proof. We see that $\operatorname{Gr}\operatorname{Pq}\mathrm{D}_n$ has the following presentation:

$$\langle [x] \text{ for } x \in \mathrm{D}_n \mid \forall x, y \in \mathrm{D}_n, [x][y][x]^{-1} = [x \rhd y] \text{ and } \forall x \in Q, k \in \mathbb{Z}, [x]^k = [x^k] \rangle$$

We write:

$$\mathrm{D}_n \cong \langle a, b \mid a^n = b^2 = 1, ab = ba^{-1} \rangle$$

From this we see that every element $x \in \mathrm{D}_n$ can be written $x = a^i b^j$ where $0 \leq i < n$ and $0 \leq j < 2$. We see the following rules emerge:

$$b^j a^i = a^{(-1)^j i} b^j$$

$$(a^i b^j)(a^l b^k) = a^i a^{(-1)^j l} b^j b^k = a^{i+(-1)^j l} b^{j+k}$$

$$(a^i b^j)(a^l b^k)(a^i b^j)^{-1} = (a^{i+(-1)^j l} b^{j+k})(b^{-j} a^{-i})$$

$$= a^{i+(-1)^j l} b^k a^{-i} = a^{i+(-1)^j l + -i(-1)^k} b^k$$

Hence we get, and get only, that:

$$[a^i b^j][a^l b^k][a^i b^j]^{-1} = [a^{i+(-1)^j l + -i(-1)^k} b^k]$$

Now, doing the four cases for (j, k), we get the following:

$$[a^i][a^l][a^i]^{-1} = [a^l]$$

$$[a^i b][a^l][a^i b]^{-1} = [a^{-l}]$$

$$[a^i][a^l b][a^i]^{-1} = [a^{2i+l} b]$$

$$[a^ib][a^lb][a^ib]^{-1} = [a^{2i-l}b]$$

Note we also get power relations:

$$[a^k]^j = [a^{kj}]$$

$$[a^kb]^j = \begin{cases} [a^kb] & \text{if } j \textit{ is odd} \\ 1 & \textit{otherwise} \end{cases}$$

Now we get:

$$[a^k] = [a]^k$$

Making $[a^k]$ redundant as generators for except for $k = 1$. Next, notice:

$$[a^kb] = [a^{k/2}][b][a^{k/2}]^{-1}$$

Here $k/2$ is computed modulo n, which is possible since n is odd. Hence all $[a^kb]$ are redundant as generators except for $k = 0$, that is $[b]$. Hence we are only left with generators $[a]$ and $[b]$, subject to $[a]^n = [b]^2 = 1$ and $[b][a] = [b][a][b]^{-1}[b] = [a]^{-1}[b]$. Hence the presentation of $LR\,\mathrm{D}_n$ must be a subgroup of D_n since the presentation is subject to at least the same strictness of generation. Notice that since the counit is surjective, $\mathrm{Gr}\,\mathrm{Pq}\,\mathrm{D}_n$ must be isomorphic to D_n, which is what was to be shown. □

Example 7.9. For even n,

$$\mathrm{Gr}\,\mathrm{Pq}\,\mathrm{D}_n \cong \mathrm{C}_2 \times \mathrm{D}_n$$

Proof. We first repeat that which is the same as the previous proof for the odd case, and get:

$$[a^i][a^l][a^i]^{-1} = [a^l]$$

$$[a^ib][a^l][a^ib]^{-1} = [a^{-l}]$$

$$[a^i][a^lb][a^i]^{-1} = [a^{2i+l}b]$$

$$[a^ib][a^lb][a^ib]^{-1} = [a^{2i-l}b]$$

$$[a^k]^j = [a^{kj}]$$

$$[a^kb]^j = \begin{cases} [a^kb] & \text{if } j \textit{ is odd} \\ 1 & \textit{otherwise} \end{cases}$$

Again, $[a^k]$ is made redundant as a generator because $[a^k] = [a]^k$. Next, we again notice:

$$[a^kb] = [a^{k/2}][b][a^{k/2}]^{-1}$$

Now however, since n is even, $k/2$ only makes sense when k is even. This makes $[a^{2k}b]$ redundant as a generator. Now we need to show $[ab]$ is not redundant given just $[a^k]$ and $[a^{2k}b]$. For it to be redundant, it needs to equal either a conjugation or a power of something else. For powers, $[a^k]$ will not yield this, and as we saw $[a^{2k}b]$ has order 2. Now, suppose it is equal to some conjugation. The following two are the candidates:

$$[a^i][a^lb][a^i]^{-1} = [a^{2i+l}b]$$

$$[a^ib][a^lb][a^ib]^{-1} = [a^{2i-l}b]$$

In the first equation we see that we need l to be even, meaning $2i + l$ is also even, so it can not be 1. In the second equation both l and i need to be even, again meaning $2i - l$ is even and thus not 1. Hence $[ab]$ is a generator alongside $[a]$ and $[b]$. There are no more generators, as:

$$[a^k][ab][a^k]^{-1} = [a^{2k+1}b]$$

Now we need to find a new presentation of $\mathrm{Gr}\,\mathrm{Pq}\,G$ using these generators. We rename $g = [a]$, $h = [b]$, $k = [ab]$ We inquire the relations between all of them:

$$g^n = 1$$

$$h^2 = i^2 = 1$$

$$gh = hg^{-1}$$
$$gk = kg^{-1}$$
$$hk = g^{-2}kh$$

And converting all these to relators instead of relations:

$$g^n$$
$$h^2$$
$$k^2$$
$$(gh)^2$$
$$(gk)^2$$
$$(hk)^2g^2$$

This gives us the presentation:

$$\mathrm{Gr\,Pq\,D}_n \cong \langle g, h, k \mid g^n, h^2, k^2, (gh)^2, (gk)^2, (hk)^2g^2\rangle$$

The final step is to show this is isomorphism to $\mathrm{C}_2 \times \mathrm{D}_n$. To do so we use the canonical presentation of $\mathrm{C}_2 \times \mathrm{D}_n$:

$$\mathrm{C}_2 \times \mathrm{D}_n \cong \langle a, b, c \mid a^n, b^2, c^2, (ab)^2, caca^{-1}, cbcb^{-1}\rangle$$

Now we need to construct an explicit isomorphism between these. We begin with defining:

$$f : \mathrm{Gr\,Pq\,D}_n \to \mathrm{C}_2 \times \mathrm{D}_n$$
$$g \mapsto a$$
$$h \mapsto b$$
$$k \mapsto abc$$

Now to verify that it is a homomorphism, we need to verify that it maps the relators to the identity:

$$f(g^n) = a^n = 1$$
$$f(h^2) = b^2 = 1$$
$$f(k^2) = (abc)^2 = abcabc = (ab)^2c^2 = 1$$
$$f((gh)^2) = (ab)^2 = 1$$
$$f((gk)^2) = (aabc)^2 = aabcaabc = (aabaab)c^2 = a^2a^{-2}b^2c^2 = 1$$
$$f((hk)^2g^2) = (babc)^2a^2 = (bba^{-1})^2c^2a^2 = a^{-2}a^2 = 1$$

Now we have verified that f is a homomorphism. We now construct its inverse:

$$f' : \mathrm{C}_2 \times \mathrm{D}_n \to \mathrm{Gr\,Pq\,D}_n$$
$$a \mapsto g$$
$$b \mapsto h$$
$$c \mapsto ghk$$

We now verify that it is a homomorphism by checking that it maps relators to the identity:

$$f'(a^n) = g^n = 1$$
$$f'(b^2) = h^2 = 1$$
$$f'(c^2) = k^2 = 1$$
$$f'((ab)^2) = (gh)^2 = 1$$
$$f'(caca^{-1}) = ghkgghkg^{-1} = ghkggg^{-2}khg^{-1} = ghkkhg^{-1} = ghhg^{-1} = gg^{-1} = 1$$
$$f'(cbcb^{-1}) = ghkhghkh = gg^{-1}hkhhkh = hkkh = hh = 1$$

So, f' too is a homomorphism. We now check that they are inverses of each other, and it is sufficient to check generators:

$$f'(f(g)) = f'(a) = g$$
$$f'(f(h)) = f'(b) = h$$
$$f'(f(k)) = f'(abc) = ghghk = (gh)^2k = k$$

And the other direction:

$$f(f'(a)) = f(g) = a$$
$$f(f'(b)) = f(h) = b$$
$$f(f'(c)) = f(ghk) = ababc = (ab)^2c = c$$

This proves f is a isomorphism between the two groups. □

Remark 7.10. Example 7.6 is a special case of Example 7.9 when $n = 2$, as $\mathrm{D}_2 \cong \mathrm{C}_2^2$

Theorem 7.11. *Let G be a finite abelian group. Then $\operatorname{Gr}\operatorname{Pq} G$ is the free abelian group generated by $[x]$ for $x \in G$ quotiented out by $[x^n] = [x]^n$.*

Proof. $\operatorname{Gr}\operatorname{Pq} G$ is the free group generated by $[x]$ for $x \in G$ quotiented out by $[x^n] = [x]^n$ and $[x \rhd y] = [x] \rhd [y]$. Since G is abelian this is equivalent to $[y] = [x] \rhd [y]$ which is equivalent to $[x][y] = [y][x]$ meaning the entire condition is equivalent to $\operatorname{Gr}\operatorname{Pq} G$ being abelian. Hence $\operatorname{Gr}\operatorname{Pq} G$ is the free abelian group generated by $[x]$ for $x \in G$ quotiented out by $[x^n] = [x]^n$. □

Example 7.12. We have $\operatorname{Gr}\operatorname{Pq}(\mathrm{C}_2^n) \cong \mathrm{C}_2^k$, where $k = 2^n - 1$.

Proof. All the non-identity elements of C_2^n are unrelated via powers. Hence each one of them is a generator in $\operatorname{Gr}\operatorname{Pq}(\mathrm{C}_2^n)$, and each has order 2. There are $k = 2^n - 1$ such non-identity elements, hence we get C_2^k. □

Lemma 7.13. ***(verified in Lean)*** *In $\operatorname{Gr}\operatorname{Pq} G$, we have:*

$$a \rhd b = [\epsilon(a)] \rhd b$$

Here ϵ is the counit of the comonad $\operatorname{Gr}\operatorname{Pq}$.

Proof. This equality can be shown as the equality of two morphisms $f, g : \operatorname{Gr}\operatorname{Pq} G \to \operatorname{Inn}(\operatorname{Gr}\operatorname{Pq} G)$. For the first:

$$f(a)(b) = a \rhd b$$

The second is the composition:

$$g = g' \circ \epsilon$$
$$g'(x)(b) = [x] \rhd b$$

We need to prove that g' is a morphism, which we save for later. Now, since Gr and Pq are adjoint, we have $\operatorname{Hom}(\operatorname{Gr}\operatorname{Pq} G, \operatorname{Inn}(\operatorname{Gr}\operatorname{Pq} G)) \cong \operatorname{Hom}_{\mathbf{PowQdl}}(\operatorname{Pq} G, \operatorname{Pq}\operatorname{Inn}(\operatorname{Gr}\operatorname{Pq} G))$, so it is sufficient to prove that f' and g' are equal after having been translated through this. This translation is realised as pre-composing with $x \mapsto [x]$. So we get that it is sufficient to prove:

$$[a] \rhd b = [\epsilon([a])] \rhd b$$

But it is trivial that $\epsilon([a]) = a$, so we are done.

Except of course, we have to show that g' is a group homomorphism. This is just proving that:

$$[xy] \rhd b = ([x][y]) \rhd b$$

We do free-group induction on b:

(1) Case 1:
That $b = 1$. In this case the equality is trivial, as both are just 1.

(2) Case 2:
That $b = [c]$. In this case we see:

$$([x][y]) \rhd [c] = [x] \rhd ([y] \rhd [c])$$

Note that $[a_1] \rhd [a_2] = [a_1 \rhd a_2]$ by the definition of $\operatorname{Gr}\operatorname{Pq} G$, so we can rewrite:

$$[xy] \rhd [c] = [xy \rhd c] = [x \rhd (y \rhd c)]$$

Also,

$$[x] \rhd ([y] \rhd [c]) = [x] \rhd [y \rhd c] = [x \rhd (y \rhd c)]$$

Hence they are equal.

(3) Case 3:
We have $b_1, b_2 \in \operatorname{Gr}\operatorname{Pq} G$ and we know that:

$$[xy] \rhd b_1 = ([x][y]) \rhd b_1$$

$$[xy] \rhd b_2 = ([x][y]) \rhd b_2$$

And we wish to show:

$$[xy] \rhd (b_1 b_2) = ([x][y]) \rhd (b_1 b_2)$$

Note that $a \rhd (bc) = abca^{-1} = aba^{-1}aca^{-1} = (a \rhd b)(a \rhd c)$. We apply this:

$$([xy] \rhd b_1)([xy] \rhd b_2) = ([x][y] \rhd b_1)([x][y] \rhd b_2)$$

Now with the inductive hypothesis this is trivial.

(4) Case 4:
We have $b' \in \operatorname{Gr}\operatorname{Pq} G$ and know that:

$$[xy] \rhd b' = ([x][y]) \rhd b'$$

And we wish to show:

$$[xy] \rhd b'^{-1} = ([x][y]) \rhd b'^{-1}$$

Since $a \rhd b^{-1} = (a \rhd b)^{-1}$, this follows trivially from the inductive hypothesis.

Those are all the cases, and we have shown that g' is a homomorphism. This concludes the proof. □

Theorem 7.14. ***(verified in Lean)*** *The kernel of the counit is in the center.*

Proof. Let a be in the kernel of the counit. Then:

$$a \rhd b = [\epsilon(a)] \rhd b = [1] \rhd b = 1 \rhd b = b$$

Hence $aba^{-1} = b$, or equivalently $ab = ba$ for all b, which is the definition of a being in the center. □

Corollary 7.15. *The kernel is abelian, and* $\operatorname{Gr}\operatorname{Pq} G$ *is a central extension of* $\ker \epsilon_G$ *by* G*.*

Example 7.16. We may ask what the kernel is for common groups. We reuse the table from Example 7.4, now with just the kernel:

G	$\operatorname{Gr}\operatorname{Pq}(G)$
C_2	1
C_3	1
C_{10}	1
$\mathrm{C}_2 \times \mathrm{C}_2$	C_2
$\mathrm{C}_3 \times \mathrm{C}_3$	$\mathrm{C}_3 \times \mathrm{C}_3$
$\mathrm{C}_4 \times \mathrm{C}_2$	$\mathrm{C}_2 \times \mathrm{C}_2$
C_2^3	C_2^4
C_2^4	C_2^{11}
S_3	1
S_4	C_2
A_4	C_2
A_5	C_2
$\mathrm{S}_3 \times \mathrm{S}_3$	C_2
S_5	C_2
A_6	C_2
Q_8	C_2
D_4	C_2
D_5	1
D_6	C_2
D_7	1
D_8	C_2
D_9	1
D_{10}	C_2
D_{11}	1
D_{12}	C_2
D_{13}	1
D_{14}	C_2
D_{15}	1
D_{16}	C_2
D_{17}	1
D_{18}	C_2
D_{19}	1
D_{20}	C_2

We see the cyclic group of order 2 appears quite a bit, but not exclusively.

Theorem 7.17. ***(verified in Lean)*** *We have:*

$$\operatorname{Gr}(Q_1 \uplus Q_2) \cong \operatorname{Gr} Q_1 \times \operatorname{Gr} Q_2$$

Proof. We construct a group homomorphism:

$$f : \operatorname{Gr}(Q_1 \uplus Q_2) \to \operatorname{Gr} Q_1 \times \operatorname{Gr} Q_2$$

By apply the adjointness of Gr to the power quandle morphism:

$$f' : Q_1 \uplus Q_2 \to \operatorname{Pq}(\operatorname{Gr} Q_1 \times \operatorname{Gr} Q_2)$$

Which is defined by:

$$f'(x) = \begin{cases} ([x], 1) & \text{if } x \in Q_1 \\ (1, [x]) & \text{if } x \in Q_2 \end{cases}$$

This is a power quandle morphism because:

$$([x], 1) \triangleright ([y], 1) = ([x \triangleright y], 1)$$
$$([x], 1)^n = ([x^n], 1)$$

And likewise symmetrically. Also,

$$([x], 1) \triangleright (1, [y]) = ([x][x]^{-1}, [y]) = (1, [y]) = f'(y) = f'(x \triangleright y)$$

Because of the definition of $\triangleright$ in the disjoint union. Now we construct a group homomorphism:

$$g : \mathrm{Gr}\, Q_1 \times \mathrm{Gr}\, Q_2 \to \mathrm{Gr}(Q_1 \uplus Q_2)$$

By $g((x, y)) = g_1(x)g_2(y)$ where:

$$g_i = \mathrm{Gr}(g_i')$$

Where $g_i' : Q_i \to Q_1 \uplus Q_2$ and is the obvious map including the power quandle into its union with the other power quandle. We need to show the product $g_1(x)g_2(y)$ is a homomorphism, which follows from $g_1(x)g_2(y) = g_2(y)g_1(x)$. A suitable induction principle lets us reduce this to $x = [q_1]$ and $y = [q_2]$ using the fact that $(ab)c = c(ab)$ follows from $bc = cb$ and $ac = ca$, which serve as the inductive hypotheses. In the base case, we get $g_1([q_1])g_2([q_2]) = g_2([q_2])g_1([q_1])$ which is equivalent to:

$$[q_1][q_2] = [q_2][q_1]$$
$$\Leftrightarrow [q_1][q_2][q_1]^{-1} = [q_2]$$
$$\Leftrightarrow [q_1] \triangleright [q_2] = [q_2]$$
$$\Leftrightarrow [q_1 \triangleright q_2] = [q_2]$$

Which follows from q_1 and q_2 coming from different power quandles. Now all that remains is showing that these two are inverses of each other. We first prove $f \circ g = id$. Since they are both homomorphisms, it is sufficient to show for generators:

$$f(g([x], [y])) = f([x][y]) = f([x])f([y]) = ([x], 1)(1, [y]) = ([x], [y])$$

And now for $g \circ f = id$:

$$g(f([x])) = g([x], 1) = [x][1] = [x]$$
$$g(f([y])) = g(1, [y]) = [1][y] = [y]$$

This proves that f is an isomorphism. □

Theorem 7.18. ***(verified in Lean)*** *Let $f : \mathrm{Pq}\, G \to \mathrm{Pq}\, H$. Then f is a group homomorphism (formally defined as there existing $f' : G \to H$ such that $\mathrm{Pq}(f') = f$) if and only if the following square commutes:*

$$\begin{tikzcd}
\mathrm{Pq}\,\mathrm{Gr}\,\mathrm{Pq}\, G \arrow[r, "\mathrm{Pq}\,\mathrm{Gr}(f)"] \arrow[d, "\mathrm{Pq}(\epsilon)"] & \mathrm{Pq}\,\mathrm{Gr}\,\mathrm{Pq}\, H \arrow[d, "\mathrm{Pq}(\epsilon)"] \\
\mathrm{Pq}\, G \arrow[r, "f"] & \mathrm{Pq}\, H
\end{tikzcd}$$

Proof. We prove both directions separately. First we assume the diagram commutes, and prove f is a homomorphism. We need to show:

$$f(xy) = f(x)f(y)$$

Put $[x][y]$ into the top left of the diagram. We get the equation:

$$f(\epsilon([x][y])) = \epsilon(\mathrm{Pq}\,\mathrm{Gr}(f)([x][y]))$$

We simplify:

$$f(xy) = \epsilon([f(x)][f(y)]) = f(x)f(y)$$

This is exactly what we wanted. Now for the other direction, assume f is a homomorphism and we need to show the diagram commutes. It is now sufficient to prove the commutativity of the diagram:

$$\begin{tikzcd}
\operatorname{Gr}\operatorname{Pq}G \arrow[r, "\operatorname{Gr}\operatorname{Pq}(f)"] \arrow[d, "\epsilon"] & \operatorname{Gr}\operatorname{Pq}H \arrow[d, "\epsilon"] \\
G \arrow[r, "f"] & H
\end{tikzcd}$$

This follows from abstract reasons, but for a concrete proof consider that it clearly holds for $[x]$, and if it holds for x and y then it clearly holds for xy because all arrows are group homomorphisms. It clearly also holds for x^{-1} and 1 for the same reason. These are all the induction cases, so we have proved that it holds. □

Lemma 7.19. ***(verified in Lean)*** *For $x_1, \dots, x_n \in G$ we have (the following equation lives in* $\operatorname{Gr}\operatorname{Pq}G$*):*

$$[x_1][x_2]\cdots[x_n] = [x_1 \cdot x_2 \cdots x_n]$$

if and only (the following equation lives in $\operatorname{Gr}\operatorname{Pq}\operatorname{Gr}\operatorname{Pq}G$*):*

$$[[x_1]][[x_2]]\cdots[[x_n]] = [[x_1][x_2]\cdots[x_n]]$$

Proof. We begin the forward implication, assume:

$$[x_1][x_2]\cdots[x_n] = [x_1 \cdot x_2 \cdots x_n]$$

Now take $\operatorname{Gr}(\eta)$ of both sides of the equation:

$$\begin{gathered}
\operatorname{Gr}(\eta)([x_1][x_2]\cdots[x_n]) = \operatorname{Gr}(\eta)([x_1 \cdot x_2 \cdots x_n]) \\
\operatorname{Gr}(\eta)([x_1])\operatorname{Gr}(\eta)([x_2])\cdots\operatorname{Gr}(\eta)([x_n]) = \operatorname{Gr}(\eta)([x_1 \cdot x_2 \cdots x_n]) \\
[[x_1]][[x_2]]\cdots[[x_n]] = [[x_1 \cdot x_2 \cdots x_n]]
\end{gathered}$$

On the right hand side, rewrite by the assumption, and we are done. Now for the other direction. Assume:

$$[[x_1]][[x_2]]\cdots[[x_n]] = [[x_1][x_2]\cdots[x_n]]$$

Take $\operatorname{Gr}(\epsilon)$ of both sides:

$$\begin{gathered}
\operatorname{Gr}(\epsilon)([[x_1]][[x_2]]\cdots[[x_n]]) = \operatorname{Gr}(\epsilon)([[x_1][x_2]\cdots[x_n]]) \\
\operatorname{Gr}(\epsilon)([[x_1]])\operatorname{Gr}(\epsilon)([[x_2]])\cdots\operatorname{Gr}(\epsilon)([[x_n]]) = \operatorname{Gr}(\epsilon)([[x_1][x_2]\cdots[x_n]]) \\
[\epsilon[x_1]][\epsilon[x_2]]\cdots[\epsilon[x_n]] = [\epsilon([x_1][x_2]\cdots[x_n])] \\
[x_1][x_2]\cdots[x_n] = [x_1 \cdot x_2 \cdots x_n]
\end{gathered}$$

Which was the intended goal. □

Theorem 7.20. ***(verified in Lean)*** *For $x \in \operatorname{Gr}\operatorname{Pq}G$, we have that $\exists y \in G, x = [y]$ is equivalent to $[x] = \operatorname{Gr}(\eta)(x)$.*

Proof. Write $x = [x_1]\cdots[x_n]$. Note that $\exists y \in G, x = [y]$ is equivalent to $x = [x_1 \cdots x_n]$. The backward direction is obvious, the forward direction we get that $[x_1]\cdots[x_n] = [y]$, we take ϵ of both sides and get $x_1 \cdots x_n = y$, which we reinsert and get $x = [x_1 \cdots x_n]$ as required. Now, we see the left hand side of the equivalence is just $[x_1]\cdots[x_n] = [x_1 \cdots x_n]$. We know this is equivalent to $[[x_1]]\cdots[[x_n]] = [[x_1]\cdots[x_n]]$, so what remains is to show that this is equivalent to $[x] = \operatorname{Gr}(\eta)(x)$. Insert our rewriting of x to get:

$$\begin{aligned}
[[x_1]\cdots[x_n]] &= \operatorname{Gr}(\eta)([x_1]\cdots[x_n]) \\
&= \operatorname{Gr}(\eta)([x_1])\cdots\operatorname{Gr}(\eta)([x_n]) = [[x_1]]\cdots[[x_n]]
\end{aligned}$$

which is exactly the desired equation. □

Remark 7.21. Note that there is a forgetful functor taking a power quandle to its underlying quandle. This of course has a left adjoint from quandles to power quandles, which takes a quandle Q to the free power quandle but with the conjugation of Q. Of course, this commutes with Gr and the enveloping group.

8. Power Quandle-Like Groups

In this section we define power quandle-like groups, abbreviated pq-like. The point of this definition is that if G, H are pq-like (and finite), and $\operatorname{Pq} G \cong \operatorname{Pq} H$, then $G \cong H$.

Definition 8.1. A group G is *pq-like* if there exists a power quandle Q such that $\operatorname{Gr} Q \cong G$.

Remark 8.2. Every group being pq-like is equivalent to the functor Gr being essentially surjective. We are not aware of any group that is not pq-like.

Theorem 8.3. ***(verified in Lean)*** *If G is pq-like then the exact sequence:*

$$1 \to \ker \epsilon_G \to \operatorname{Gr} \operatorname{Pq} G \to G \to 1$$

Is left-split. This means $\operatorname{Gr} \operatorname{Pq} G \cong G \times \ker \epsilon_G$.

Proof. We first prove it is right-split. We rewrite as:

$$1 \to \ker \epsilon_G \to \operatorname{Gr} \operatorname{Pq} \operatorname{Gr} Q \to \operatorname{Gr} Q \to 1$$

Note that $\eta : Q \to \operatorname{Pq} \operatorname{Gr} Q$ taking $q \mapsto [q]$ is a power-quandle morphism, so $\operatorname{Gr}(\eta)$ is a group morphism. Because of category theory, $\epsilon \circ \operatorname{Gr}(\eta) = \mathrm{id}$, so the sequence is right-split. A sequence which is right-split is also left-split if the image of the left-split morphism is normal. We prove this. We need to show there exists z such that:

$$x \rhd \operatorname{Gr}(\eta)(y) = \operatorname{Gr}(\eta)(z)$$

We do this by showing:

$$x \rhd y = \operatorname{Gr}(\eta)(\epsilon(x)) \rhd y$$

We simplify by noting that $x \rhd y = [\epsilon(x)] \rhd y$ so it is sufficient to show:

$$[x] \rhd y = \operatorname{Gr}(\eta)(x) \rhd y$$

We use the same identity on the right side giving:

$$\operatorname{Gr}(\eta)(x) \rhd y = [\epsilon(\operatorname{Gr}(\eta)(x)] \rhd y = [x] \rhd y$$

Because $\epsilon \circ \operatorname{Gr}(\eta) = \mathrm{id}$. Now let $z = \epsilon(x) \rhd y$, and we see:

$$\operatorname{Gr}(\eta)(z) = \operatorname{Gr}(\eta)(\epsilon(x) \rhd y) = \operatorname{Gr}(\eta(\epsilon(x))) \rhd \operatorname{Gr}(\eta(y))$$

Making the following sufficient:

$$\operatorname{Gr}(\eta)(\epsilon(x)) \rhd y = x \rhd y$$

Which is what we just proved. □

Theorem 8.4. *If G, H are finite and pq-like, and $\operatorname{Pq} G \cong \operatorname{Pq} H$, then $G \cong H$.*

Proof. We make heavy use of the cancellation of direct products for finite groups, for which we refer to [7]. We clearly get:

$$\operatorname{Gr} \operatorname{Pq} G \cong \operatorname{Gr} \operatorname{Pq} H$$

Since both are pq-like we get:

$$G \times \ker \epsilon_G \cong H \times \ker \epsilon_H$$

We take the center of both sides of the isomorphism:

$$\mathrm{Z}(G \times \ker \epsilon_G) \cong \mathrm{Z}(H \times \ker \epsilon_H)$$

$$\mathrm{Z}(G) \times \mathrm{Z}(\ker \epsilon_G) \cong \mathrm{Z}(H) \times \mathrm{Z}(\ker \epsilon_H)$$

We also know that since G, H are finite then:

$$\mathrm{Z}(G) \cong \mathrm{Z}(H)$$

We combine these to get:

$$\mathrm{Z}(G) \times \mathrm{Z}(\ker \epsilon_G) \cong \mathrm{Z}(G) \times \mathrm{Z}(\ker \epsilon_H)$$

Now we may cancel $\mathrm{Z}(G)$ on both sides of the isomorphism:

$$\mathrm{Z}(\ker \epsilon_G) \cong \mathrm{Z}(\ker \epsilon_H)$$

Next, note that since $\ker \epsilon_G$ is abelian, the center is just itself:

$$\ker \epsilon_G \cong \ker \epsilon_H$$

Now recall we had:

$$G \times \ker \epsilon_G \cong H \times \ker \epsilon_H$$

Again we can use the isomorphism we have obtained:

$$G \times \ker \epsilon_G \cong H \times \ker \epsilon_G$$

Now we again use the cancellation of Cartesian product and obtain the desired result:

$$G \cong H$$

□

We now have a very good reason to prove groups are pq-like, so we establish some tools for this.

Proposition 8.5. *The following are always pq-like:*

1. *Any cyclic group is pq-like.*
2. *The direct product of two pq-like groups is again pq-like.*
3. *All finite abelian groups are pq-like.*

Proof. We prove them one by one, with dependencies downward:

1. For C_n, just use $\mathrm{Pq}\,\mathrm{C}_n$ and we get $\mathrm{Gr}\,\mathrm{Pq}\,\mathrm{C}_n \cong \mathrm{C}_n$, proving C_n is pq-like.
2. We wish to prove $\mathrm{Gr}\,Q_1 \times \mathrm{Gr}\,Q_2$ is pq-like. We use Theorem 7.17, so we pick $Q := Q_1 \uplus Q_2$ and get $\mathrm{Gr}\,Q \cong \mathrm{Gr}\,Q_1 \times \mathrm{Gr}\,Q_2$.
3. Any finite abelian group can inductively be written as the direct product of two finite abelian groups, or as a cyclic group. All cases are pq-like.

□

Theorem 8.6. ***(verified in Lean)*** *If G is pq-like, then (and only then) is it isomorphic to, for some S, $\mathrm{Gr}\,\mathrm{Pq}_S\,G$, where S is a subset of the elements of G that generates the entire group, and $\mathrm{Pq}_S\,G$ is the sub-power-quandle of $\mathrm{Pq}\,G$ generated by the elements of S. Note that even though S generates the entire G as a group, that does not mean it generates the entire power quandle $\mathrm{Pq}\,G$.*

Proof. Set $G \cong \mathrm{Gr}\,Q$. Pick $S \subset \mathrm{Gr}\,Q$ to be every element of the form $[q]$ for some $q \in Q$. This clearly generates $\mathrm{Gr}\,Q$ by the very definition of $\mathrm{Gr}\,Q$.

Before moving forward, we wish to prove that the power quandle generated by S is indeed just S. We see this from $[a] \triangleright [b] = [a \triangleright b]$ and $[a]^n = [a^n]$.

All that remains to prove is that $\mathrm{Gr}\,\mathrm{Pq}_S\,\mathrm{Gr}\,Q \cong \mathrm{Gr}\,Q$. We begin with constructing a group homomorphism:

$$f : \mathrm{Gr}\,\mathrm{Pq}_S\,\mathrm{Gr}\,Q \to \mathrm{Gr}\,Q$$

By adjointness of Gr and Pq, this is equivalent to a power quandle morphism:

$$\mathrm{Pq}_S\,\mathrm{Gr}\,Q \to \mathrm{Pq}\,\mathrm{Gr}\,Q$$

Here we pick the natural inclusion, as $\mathrm{Pq}_S \operatorname{Gr} Q$ is a sub-power quandle of $\mathrm{Pq} \operatorname{Gr} Q$. In the other direction, we need to provide a group homomorphism:

$$g : \operatorname{Gr} Q \to \operatorname{Gr} \mathrm{Pq}_S \operatorname{Gr} Q$$

Again, by adjointness, this is equivalent to providing a power quandle morphism:

$$Q \to \mathrm{Pq} \operatorname{Gr} \mathrm{Pq}_S \operatorname{Gr} Q$$

We send q to $[[q]]$, but for this we need to prove that $[q]$ is in $\mathrm{Pq}_S \operatorname{Gr} Q$. This follows by definition.

Now all that remains is to prove that these two morphisms compose to the identity in both directions. Since they are group homomorphisms it is sufficient to prove it for the generators, i.e. $[q]$ for all q. We begin with:

$$f(g([q])) = f([[q]]) = [q]$$

Now let $[q] \in \operatorname{Gr} \mathrm{Pq}_S \operatorname{Gr} Q$. Since $q \in \mathrm{Pq}_S \operatorname{Gr} Q$ we have $q = [q']$. This gives us:

$$g(f([[q']])) = g([q']) = [[q']]$$

Hence all compositions are the identity. □

Remark 8.7. For a finite group G, this would allow us to iterate over all possible S to determine whether G is pq-like deterministically. For a computer program it would be more efficient to loop over all possible sub-power-quandles of $\mathrm{Pq}\, G$, where the elements would generate G as a group, as to not have so much redundancy. A good first guess is any minimal generating set, as the goal should be seen as the smallest possible power quandle that still generates the group.

Remark 8.8. Recall Theorem 7.20, that $x = [y]$ if and only if $[x] = \operatorname{Gr}(\eta)(x)$ in $\operatorname{Gr} \mathrm{Pq}\, G$. This is not the same as $\operatorname{Gr} Q$, but we can use it as inspiration to find candidate sub-power quandles of $\mathrm{Pq}\, G$. Recall the desired sub-power quandle of $\mathrm{Pq}\, G$ is the one consisting of $[q]$ for some $q \in Q$, where $G \cong \operatorname{Gr} Q$. Hence, this sub-power quandle is just the equalizer $\mathrm{Eq}(\eta, \mathrm{Pq} \operatorname{Gr}(\eta))$ in the category of power quandles. This is the sub-power quandle of $\mathrm{Pq}\, G$ such that $[x] = \mathrm{Pq} \operatorname{Gr}(\eta)(x)$. Of course, one does not know $\operatorname{Gr}(\eta)$, but here one can guess candidate homomorphisms $G \to \operatorname{Gr} \mathrm{Pq}\, G$. Of course, if $\operatorname{Gr} \mathrm{Pq}\, G \cong G \times A$ (and if not, then it is definitely not pq-like), then there is at least one morphism for each homomorphism $G \to A$. The zero homomorphism would not be a bad guess.

Theorem 8.9. ***(verified in Lean)*** *Let G and H be pq-like groups and let $\phi : H \to \operatorname{Aut}(G)$ be a homomorphism. Since G, H are pq-like, let Q_1 and Q_2 be power quandles such that we have isomorphisms $G \cong \operatorname{Gr} Q_1$ and $H \cong \operatorname{Gr} Q_2$. Use these isomorphisms to obtain $\phi' : \operatorname{Gr} Q_2 \to \operatorname{Aut}(\operatorname{Gr} Q_1)$. If for all $x \in Q_2$ and $y \in Q_1$ there exists $z \in Q_1$ such that $\phi'([x])([y]) = [z]$, then $G \rtimes_\phi H$ is pq-like. This condition is automatically met if the automorphism $\phi'(x)$ is in the image of* Gr. *It is always met if G is cyclic, or if ϕ is trivial.*

Proof. We first create a subset of $\operatorname{Gr} Q_1 \rtimes_\phi \operatorname{Gr} Q_2$, as all the elements $([a], 1)$ and $(1, [b])$. Then we create a sub-power-quandle generated by these elements, and call it Q. This is the power quandle with which the group is pq-like, so we need to prove $\operatorname{Gr} Q_1 \rtimes_\phi \operatorname{Gr} Q_2 \cong \operatorname{Gr} Q$. We begin with the inverse morphism, which using adjointness comes from the power quandle morphism:

$$Q \to \mathrm{Pq}(\operatorname{Gr} Q_1 \rtimes_\phi \operatorname{Gr} Q_2)$$

This is just the inclusion morphism. Call the adjoint morphism h. The other direction is more complicated. Here we use a property of semidirect products in that given two morphisms $f : \operatorname{Gr} Q_1 \to \operatorname{Gr} Q$ and $g : \operatorname{Gr} Q_2 \to \operatorname{Gr} Q$, then one can construct a homomorphism $fg : \operatorname{Gr} Q_1 \rtimes_\phi \operatorname{Gr} Q_2 \to \operatorname{Gr} Q$ given that:

$$f(a)g(b)f(a)^{-1} = g(\phi(a)(b))$$

We set f to be the morphism sending $[a]$ to $([a], 1)$ and g sends $[b]$ to $(1, [b])$. Now we need to prove the property:

$$f(a)g(b)f(a)^{-1} = g(\phi(a)(b))$$

We prove this inductively:

(1) For the case of multiplication in a, given:

$$\forall b, f(a_1)g(b)f(a_1)^{-1} = g(\phi(a_1)(b))$$
$$\forall b, f(a_2)g(b)f(a_2)^{-1} = g(\phi(a_2)(b))$$

Prove that:

$$f(a_1a_2)g(b)f(a_1a_2)^{-1} = g(\phi(a_1a_2)(b))$$

We simplify first:

$$f(a_1)f(a_2)g(b)f(a_2)^{-1}f(a_1)^{-1} = g(\phi(a_1)(\phi(a_2)(b)))$$

Now we use the second inductive hypothesis (with b set to b) to get:

$$f(a_1)g(\phi(a_2)(b))f(a_1)^{-1} = g(\phi(a_1)(\phi(a_2)(b)))$$

Now we use the first inductive hypothesis (with b set to $\phi(a_2)(b)$), to finish the goal.

(2) For the case of multiplication in b, given:

$$f(a)g(b_1)f(a)^{-1} = g(\phi(a)(b_1))$$
$$f(a)g(b_2)f(a)^{-1} = g(\phi(a)(b_2))$$

Then prove:

$$f(a)g(b_1b_2)f(a)^{-1} = g(\phi(a)(b_1b_2))$$

This is clear, because both sides are homomorphisms in b (for the left hand side, note that $abca^{-1} = aba^{-1}aca^{-1}$).

(3) For the case of $a = 1$, and for the case of $b = 1$, those are trivial.

(4) For the case of inversions, those are not necessary in $\operatorname{Gr} Q'$, as every element $[a]$ can be inverted as $[a^{-1}]$ and a multiplication can be inverted as $(ab)^{-1} = b^{-1}a^{-1}$.

(5) Finally, the case of $[a]$ and $[b]$:

$$f([a])g([b])f([a])^{-1} = g(\phi([a])([b]))$$

Note that we took as a hypothesis that $\phi([a])([b]) = [c]$ for some c, so we use this, as well as the definitions of f and g to get:

$$([a], 1)(1, [b])([a], 1)^{-1} = (1, [c])$$

Now we again use the definition of c to get the following goal:

$$([a], 1)(1, [b])([a], 1)^{-1} = (1, \phi([a])([b])])$$

Which follows by definition in a semidirect product.

Now we have morphisms in both directions, we just need to show that both compositions are id. It is sufficient to test using the generators of the groups, as they are group homomorphisms. We show:

$$h(fg(([x], [y]))) = h(f([x])g([y])) = h(f([x]))h(g([y])) = h(([x], 1))h((1, [y]))$$
$$= ([x], 1)(1, [y]) = ([x], [y])$$
$$fg(h([x], 1)) = fg([x], 1) = f([x])g(1) = ([x], 1)$$
$$fg(h(1, [y])) = fg(1, [y]) = f(1)g([y]) = (1, [y])$$

Those are all the cases, and we have proven that a semidirect product with the stated property, is pq-like. □

Remark 8.10. Since a group can be pq-like by many different power quandles, and many different variants of ϕ can yield the same semidirect product, there is much flexibility in terms of finding a situation which satisfies the condition. Hence we believe a broad class of semidirect products satisfy this.

Lemma 8.11. ***(verified in Lean)*** *Let F_S^{pq} be the free power quandle generated by the set S. This is just all possible combinations of power and conjugation of the generators, modulo the power quandle axioms. Then:*

$$\mathrm{Gr}(\mathrm{F}_S^{pq}) \cong \mathrm{F}_S$$

It follows that free groups are pq-like.

Proof. This follows from free power quandle (and free groups) being left adjoint to the forgetful functors to **Set**. Since the underlying set of $\mathrm{Pq}\,G$ is the same as G, the forgetful functors commute. Hence the left adjoints must commute, and we get the desired isomorphism. □

Theorem 8.12. *The group G being pq-like is equivalent to there existing some presentation of G using only conjugations and powers in the relations.*

Proof. We begin with the forward direction. Assume $G \cong \mathrm{Gr}\,Q$, now display Q as a coequalizer of free power quandles:

$$\mathrm{F}_R^{pq} \rightrightarrows \mathrm{F}_G^{pq} \to Q$$

This is always possible using $G = Q$ and R every relation that holds in Q. Sometimes, a more lean presentation can be found as well. Now, take Gr of this coequalizer. As Gr is a left adjoint, this is still a coequalizer in groups:

$$\mathrm{Gr}(\mathrm{F}_R^{pq}) \rightrightarrows \mathrm{Gr}(\mathrm{F}_G^{pq}) \to \mathrm{Gr}(Q)$$

Now we simplify a bit:

$$\mathrm{F}_R \rightrightarrows \mathrm{F}_G \to G$$

A coequalizer of free groups is precisely a presentation, where the two arrows are the left- and right-hand side of the relations. Note that these arrows come from free power quandles, which is equivalent to them being expressed using only powers and conjugation. For the other direction, just reverse everything: The presentation of G is a coequalizer, the two arrows of which are in the image of Gr, and then Q is the coequalizer of the free power quandles with those arrows. □

Example 8.13. The group:

$$\langle x, y, z \mid x^3 = y^6 = z^6 = 1, xyx^{-1} = y^{-1}, xzx^{-1} = z, yzy^{-1} = z\rangle$$

is clearly pq-like, because it only uses powers and conjugation. Also, the same group can be written

$$\langle x, y, z \mid x^3 = y^6 = z^6 = 1, yxy = x, xz = zx, yz = zy\rangle$$

And this is still pq-like because this presentation can be rewritten to something that only uses conjugation and powers.

Remark 8.14. This also demonstrates why finite abelian groups are pq-like: they can be presented using only relations of the form $a^n = 1$ and $aba^{-1} = b$.

Theorem 8.15. *All Coxeter groups are pq-like. Since the symmetric groups are Coxeter, this implies the symmetric groups are pq-like. Recall a Coxeter group is a group with presentation:*

$$\langle r_1, r_2, \dots, r_n \mid (r_i r_j)^{m_{ij}}\rangle$$

Where $m_{ii} = 1$ and $m_{ij} \geq 2$ for $i \neq j$.

Proof. All Coxeter groups have presentation:

$$\langle r_1, r_2, \ldots, r_n \mid (r_i r_j)^{m_{ij}} \rangle$$

Where $m_{ii} = 1$ and $m_{ij} \geq 2$ for $i \neq j$. This means every generator r_i has order two. The other relations are of the form:

$$r_i r_j r_i \ldots r_j = 1$$

This can be rewritten:

$$r_i r_j \ldots r_i \ldots r_j^{-1} r_i^{-1} = r_j$$

Hence they are conjugations, and when $i = j$ they are powers. □

References

[1] Jonathan Mock Beck, *Triples, algebras and cohomology*, Repr. Theory Appl. Categ. **2003** (2003), no. 2, 1–59 (English).

[2] Egbert Brieskorn, *Automorphic sets and braids and singularities*, Braids (Santa Cruz, CA, 1986), Contemp. Math., vol. 78, Amer. Math. Soc., Providence, RI, 1988, pp. 45–115.

[3] Leonardo Mendonça de Moura, Soonho Kong, Jeremy Avigad, Floris van Doorn, and Jakob von Raumer, *The lean theorem prover (system description)*, Automated Deduction - CADE-25 - 25th International Conference on Automated Deduction, Berlin, Germany, August 1-7, 2015, Proceedings, 2015, pp. 378–388.

[4] Mohamed Elhamdadi and Sam Nelson, *Quandles: an introduction to the algebra of knots*, Student mathematical library, no. volume 74, American Mathematical Society, Providence, Rhode Island, 2015.

[5] Roger Fenn and Colin Rourke, *Racks and links in codimension two*, Journal of Knot Theory and Its Ramifications **01** (1992), no. 04, 343–406.

[6] The GAP Group, *GAP – Groups, Algorithms, and Programming, Version 4.11.1*, 2021.

[7] Ronald Hirshon, *On cancellation in groups*, The American Mathematical Monthly **76** (1969), no. 9, 1037–1039.

[8] David Joyce, *A classifying invariant of knots, the knot quandle*, Journal of Pure and Applied Algebra **23** (1982), no. 1, 37 – 65.

[9] Sergeĭ Vladimirovich Matveev, *Distributive groupoids in knot theory*, Mathematics of the USSR-Sbornik **47** (1984), no. 1, 73–83.

[10] Takefumi Nosaka, *Quandles and Topological Pairs*, SpringerBriefs in Mathematics, Springer Singapore, Singapore, 2017.

[11] William Arthur Stein et al., *Sage Mathematics Software (Version 9.0)*, The Sage Development Team, 2020, `http://www.sagemath.org`.

[12] Markus Szymik, *Permutations, power operations, and the center of the category of racks*, Comm. Algebra **46** (2018), 230–240.

[13] Markus Szymik, *Alexander-Beck modules detect the unknot*, Fundam. Math. **246** (2019), no. 1, 89–108 (English).

[14] The mathlib community, *The Lean mathematical library*, Proceedings of the 9th ACM SIGPLAN International Conference on Certified Programs and Proofs, CPP 2020, New Orleans, LA, USA, January 20-21, 2020, 2020, pp. 367–381.

NTNU

Kunnskap for en bedre verden