Pauli Groups and Hopf-Galois Structures

Timothy Kohl

Boston University

June 5, 2025

Pauli Groups

Before digging in to the detailing of the specifics about these groups, I shall indicate what brought them to my attention.

It starts with Hopf-Galois extensions of course, and we recall some definitions.

For G a finite group, embedded as $\lambda(G) \leq B = \mathrm{Perm}(G)$, where $\mathrm{Hol}(G) = \mathrm{Norm_B}(\lambda(G))$ let

- $\mathcal{S}(G) = \{\textit{regular } N \leq \mathrm{Hol}(G) \mid N \cong G\}$
- $\mathcal{R}(G) = \{\textit{regular } N \leq B \mid N \cong G \textit{ and } \lambda(G) \leq \mathrm{Norm_B}(N)\}$
- $\mathcal{H}(G) = \{\textit{regular } N \triangleleft \mathrm{Hol}(G) \mid N \cong G\}$
- $\mathcal{Q}(G) = \bigcap_{N \in \mathcal{S}(G) \cap \mathcal{R}(G)} \{M \in \mathcal{S}(G) \cap \mathcal{R}(G) \mid N \textit{ normalizes } M\}$

Of course

$$\mathcal{R}(G) = \{regular\ N \leq B \mid N \cong G\ and\ \lambda(G) \leq \mathrm{Norm_B}(N)\}$$

is of key interest as these correspond to Hopf-Galois structures on a field extension with Galois group isomorphic to G and where the type of the Hopf algebra is $[G]$, i.e. isomorphic to the Galois group.

And $\mathcal{S}(G) \cap \mathcal{R}(G)$ consists of those such regular N which themselves normalize $\lambda(G)$, i.e. are subgroups of $\mathrm{Hol}(G)$.

The set $\mathcal{H}(G)$ consists of those regular N isomorphic to G with the same normalizer as $\lambda(G)$, i.e. $N \cong G$ and $\mathrm{Norm_B}(N) = \mathrm{Norm_B}(\lambda(G))$, whose size and properties are connected with the multiple holomorph

$$\mathrm{NHol}(G) = \mathrm{Norm_B}(\mathrm{Hol}(G))$$

where in particuler $[\mathrm{NHol}(G) : \mathrm{Hol}(G)] = |\mathcal{H}(G)|$

As such we have some basic containments

$$\mathcal{H}(G) \subseteq \mathcal{S}(G) \cap \mathcal{R}(G) \subseteq \mathcal{R}(G)$$

and even though $|\mathcal{S}(G)| = |\mathcal{R}(G)|$, these two sets are not necessarily equal, which is the reason why different methods have been explored and developed over the last 30 years to enumerate $\mathcal{R}(G)$ as it may contain N which lie outside $\mathcal{S}(G)$.

The set

$$\mathcal{Q}(G) = \bigcap_{N \in \mathcal{S}(G) \cap \mathcal{R}(G)} \{M \in \mathcal{S}(G) \cap \mathcal{R}(G) \mid N \textit{ normalizes } M\}$$

is, by its construction, a subset of $\mathcal{S}(G) \cap \mathcal{R}(G)$ whose members all mutually normalize each other.

The containments for these collections are as follows

$$\mathcal{H}(G) \subseteq \mathcal{Q}(G) \subseteq \mathcal{S}(G) \cap \mathcal{R}(G)$$

where, depending on the group G, some of these containments are strict, some are equalities.

This was explored by the presenter, and ties in with the definition of the quasi-holomorph, namely a group generated by $\mathrm{Hol}(G)$ together with the set of those elements $\pi(\mathcal{Q}(G)) \subseteq B$ which conjugate $\lambda(G)$ to the groups in $\mathcal{Q}(G)$.

Under the right conditions, $\mathrm{QHol}(G)$ is a group, and is the largest subgroup of $\mathrm{Perm}(G)$ which conjugates $\lambda(G)$ to the elements of $\mathcal{Q}(G)$.

That is, $\mathrm{QHol}(G)$ acts transitively, with $\mathrm{Hol}(G)$ being the stabilizer subgroup of $\lambda(G)$.

When $\mathcal{Q}(G)=\mathcal{H}(G)$ then $\mathrm{QHol}(G)=\mathrm{NHol}(G)$ and when $\mathcal{Q}(G)=\mathcal{S}(G)\cap\mathcal{R}(G)$, then $\mathrm{QHol}(G)$ is a group of size $|\mathcal{Q}(G)|\cdot|\,\mathrm{Hol}(G)|$.

When $\mathcal{Q}(G)$ is properly contained between $\mathcal{H}(G)$ and $\mathcal{S}(G)\cap\mathcal{R}(G)$ then it is not definitively known if $\mathrm{QHol}(G)$ is a group, although for all lower order examples known/computed, it seems to be the case.

Moreover, if $\mathcal{Q}(G)=\mathcal{H}(G)$, whence $\mathrm{QHol}(G)=\mathrm{NHol}(G)$ one has that $\mathrm{NHol}(G)$ is an extension (not necessarily split) of $\mathrm{Hol}(G)$.

But if $\mathcal{Q}(G)$ properly contains $\mathcal{H}(G)$, and $\mathrm{QHol}(G)$ is a group, then it is generally the case that it is a Zappa-Szep extension of $\mathrm{Hol}(G)$ of the form

$$\pi(\mathcal{Q}(G))\mathrm{Hol}(G)$$

where $\pi(\mathcal{Q}(G))$ is a particular set of coset representatives which forms a group, which acts *regularly* on $\mathcal{Q}(G)$.

(Recall that these coset representatives conjugate $\lambda(G)$ to each element of $\mathcal{Q}(G)$.)

And $\mathrm{Hol}(G)$ is definitely not a normal subgroup.

For many low order groups, where $\mathcal{Q}(G)$ properly contains $\mathcal{H}(G)$ the quasi-holomorph is such a Zappa-Szep product.

However, their are exceptions, and for perspective we look at a table of small order examples, and consider the first such exception.

G	$\lvert\mathcal{S}\cap\mathcal{R}\rvert$	$\lvert\mathcal{Q}\rvert$	$\lvert\mathcal{H}\rvert$	$\pi(\mathcal{Q})$
C_4	1	1	1	1
$C_2 \times C_2$	1	1	1	1
S_3	2	2	2	C_2
$C_4 \times C_2$	8	2	2	C_2
D_8	6	6	2	$S_3,\ C_6$
Q_8	2	2	2	C_2
$C_2 \times C_2 \times C_2$	8	1	1	1
C_9	3	3	1	C_3
$C_3 \times C_3$	9	1	1	1
D_{10}	2	2	2	C_2
$C_3 \rtimes C_4$	2	2	2	C_2
A_4	6	2	2	C_2
D_{12}	8	2	2	C_2
$C_6 \times C_2$	1	1	1	1
D_{14}	2	2	2	C_2
C_{16}	4	4	2	$C_4, C_2 \times C_2$
$C_4 \times C_4$	24	24	1	$C_4 \times S_3,\ (C_6 \times C_2) \rtimes C_2,\ C_3 \times D_8,\ S_4,\ C_2 \times A_4,\ C_2 \times C_2 \times S_3$
$(C_4 \times C_2) \rtimes C_2$	76	4	4	$C_2 \times C_2$
$C_4 \rtimes C_4$	72	72	8	$C_3 \times S_4,\ (C_3 \times A_4) \rtimes C_2$
$C_8 \times C_2$	10	4	4	$C_2 \times C_2$
$C_8 \rtimes C_2$	10	4	4	$C_2 \times C_2$
D_{16}	16	8	4	$C_4 \times C_2,\ D_8,\ C_2 \times C_2 \times C_2$
QD_{16}	32	16	16	$C_2 \times D_8$
Q_{16}	16	8	4	$C_4 \times C_2,\ D_8,\ C_2 \times C_2 \times C_2$
$C_4 \times C_2 \times C_2$	146	1	1	1
$C_2 \times D_8$	198	6	2	$S_3,\ C_6$
$C_2 \times Q_8$	66	2	2	C_2
$(C_4 \times C_2) \rtimes C_2$	224	224	2	QHol(G) is not a Zappa-Szép Extension of Hol(G)
$C_2 \times C_2 \times C_2 \times C_2$	106	1	1	1

$(C_4 \times C_2) \rtimes C_2$	224	224	2	QHol(G) is not a Zappa-Szép Extension of Hol(G)

This group, called the Pauli group, (whose analysis will be discussed presently), is interesting in this context in that QHol(G) is not a Zappa-Szep product, although QHol(G) is a well defined group since $\mathcal{Q}(G) = \mathcal{S}(G) \cap \mathcal{R}(G)$.

That is, QHol(G) acts transitively on $\mathcal{Q}(G)$ with Hol(G) being the stabilizer of $\lambda(G)$, but no transversal of Hol(G) in QHol(G) forms a group, which acts regularly on $\mathcal{Q}(G)$.

$(C_4 \times C_2) \rtimes C_2$	224	224	2	QHol(G) is not a Zappa-Szép Extension of Hol(G)

We note, for reference that this is, in a way, a direct analog to the difference between a split vs. non-split extension of a group.

Indeed, for $\mathrm{Hol}(G) \triangleleft \mathrm{NHol}(G)$ we have that $T(G) = \mathrm{NHol}(G)/\mathrm{Hol}(G)$ acts regularly on $\mathcal{H}(G)$, but it need not be the case that NHol(G) contain a normal complement to Hol(G).

Moreover, for group $C_5 \rtimes C_8$, $\mathrm{QHol}(G) = \mathrm{NHol}(G)$ and NHol(G) is not a split extension of Hol(G).

$(C_4 \times C_2) \rtimes C_2$	224	224	2	QHol(G) is not a Zappa-Szép Extension of Hol(G)

The other interesting fact is that here (and for many other groups) it turns out one has that

$$\mathcal{S}(G) = \mathcal{R}(G)$$

and for this G it turns out that

$$\mathcal{R}(G) = \mathcal{S}(G) \cap \mathcal{R}(G) = \mathcal{Q}(G)$$

and the number of groups in this collection is much larger than for any other group of order 16, and larger than for any group of order lower than 16.

So let's take a look at this group, called the Pauli group.

Pauli Matrices

To begin the defintion of this group we consider what are known as the Pauli matrices, (which show up in the analysis of spins of particles in quantum mechanics) which are defined as follows:

$$X = \sigma_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$Y = \sigma_2 = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$Z = \sigma_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

and they satsify a number of nice properties such as being Hermitian, involutary, traceless, and determinant=-1.

$$X = \sigma_1 = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}$$

$$Y = \sigma_2 = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

$$Z = \sigma_3 = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}$$

and the products of them satisfy the following relations

$$\begin{array}{lll} XY = iZ & YZ = iX & ZX = iY \\ YX = -iZ & ZY = -iX & XZ = -iY \end{array}$$

and, as mentioned earlier, $X^2 = Y^2 = Z^2 = I$, so that $XYZ = iI$.

The Pauli group P_1 (where, yes, the subscript does indicate a family which we'll discuss eventually) of order $4^2 = 16$ is defined as

$$\begin{aligned} P_1 &= \langle X, Y, Z \rangle \\ &= \{\pm I, \pm iI, \pm X, \pm iX, \pm Y, \pm iY, \pm Z, \pm iZ\} \end{aligned}$$

and has a number of different presentations.

One basic presentation (as indicated in the table earlier) comes from how it is given as group 13, in the **AllSmallGroups** library [1] in GAP[2], of groups of order 16, namely the semi-direct product $(C_4 \times C_2) \rtimes C_2$.

However, there is a somewhat 'better' presentation we can give, which comes from a further brief look at the matrix definition.

Consider the following table of products of matrices.

$XY = iZ$	$YZ = iX$	$ZX = iY$
$YX = -iZ$	$ZY = -iX$	$XZ = -iY$
$(iX)Y = -Z$	$(iY)Z = -X$	$(iZ)X = iY$
$Y(iX) = Z$	$Z(iY) = X$	$X(iZ) = -iY$
$X(iY) = -Z$	$Y(iZ) = -X$	$Z(iX) = -Y$
$(iY)X = Z$	$(iZ)Y = X$	$(iX)Z = Y$
$(iX)(iY) = -iZ$	$(iY)(iZ) = -iX$	$(iZ)(iX) = -iY$
$(iY)(iX) = iZ$	$(iZ)(iY) = iX$	$(iX)(iZ) = iY$

So if we let $Q = \{\pm iX, \pm iY, \pm iZ, \pm I\}$ we deduce that $Q \leq P_1$, and as $|iX| = |iY| = |iZ| = 4$ then it's clear that $Q \cong Q_2$ the quaternion group of order 8, and therefore normal in P_1.

As to the additional order 2 component, if we view Q as $\{\pm 1, \pm i, \pm j, \pm k\}$ as usual then what we end up with is that P_1 is a subgroup of $\mathrm{Hol}(Q)$, namely:

$$P_1 \cong Q \rtimes \langle c_i \rangle$$

where $c_i \in \mathrm{Aut}(Q)$ is conjugation by i and where the action of this on $i, j, k \in Q$ is

$$c_i(\pm i) = \pm i \quad c_i(\pm j) = \mp j \quad c_i(\pm k) = \mp k$$

so that $|c_i| = 2$ and with this we can determine some basic properties of this group.

We have the following facts about orders of elements:

$$|(\pm i, c_i)| = 4 \quad |(\pm j, c_i)| = 2 \quad |(\pm k, c_i)| = 2 \quad |(\pm 1, c_i)| = 2$$

and note that $Z(Q) = \{\pm 1\}$ and $Z(P_1) = \langle (i, c_i) \rangle$, which will have implications for the determination of $\mathrm{Aut}(P_1)$, and ultimately $\mathrm{Hol}(P_1)$.

In order to enumerate the regular $N \in \mathcal{R}(P_1)$ and to show that $\mathcal{R}(P_1) = \mathcal{S}(P_1)$ we need to analyze the structure of $\mathrm{Hol}(P_1)$.

To that end, we start with the determination of $\mathrm{Aut}(P_1)$.

Given that P_1 is an extension of Q, we first consider the relationship between $\mathrm{Aut}(Q)$ and $\mathrm{Aut}(P_1)$.

We let $\gamma_i = \begin{bmatrix} i \to i \\ j \to -j \\ k \to -k \end{bmatrix}$ denote conjugation by i and $\gamma_j = \begin{bmatrix} i \to -i \\ j \to j \\ k \to -k \end{bmatrix}$ denote conjugation by j, which we do in order to distinguish these automorphisms of Q, from the element 'c_i' which is embedded in the definition of P_1.

$\mathrm{Aut}(Q) = V \rtimes S \cong S_4$ where

$$V = \langle \gamma_i, \gamma_j \rangle \cong V_4$$
$$S = \langle (ij), (ik) \rangle \cong S_3$$

where $(ij) = \begin{bmatrix} i \to j \\ j \to i \\ k \to -k \end{bmatrix}$ and $(ik) = \begin{bmatrix} i \to k \\ j \to -j \\ k \to i \end{bmatrix}$ and $(jk) = \begin{bmatrix} i \to -i \\ j \to -k \\ k \to -j \end{bmatrix}$.

Moreover, V is precisely $Inn(Q)$ and $S = Out(Q)$.

Lemma

Q is a characteristic subgroup of P_1.

Proof.

For $\psi \in \mathrm{Aut}(P_1)$ suppose that $\psi(i, I) = (n, c_i)$ then $\psi(-1, I) = (nc_i(n), I)$ and since $(-1, I)$ is the unique element of order 2 in $Z(P_1)$ then we have that $nc_i(n) = -1$.

But given how c_i acts, we find that the only possibilities are $n = \pm i$.

However, both (i, c_i) and $(-i, c_i)$ lie in $Z(P_1)$ and (i, I) does not, so $\psi(i, I) = (n, c_i)$ is impossible.

And by identical arguments, one finds that $\psi(\pm j, I) \neq (n, c_i)$ and $\psi(\pm k, I) \neq (n, c_i)$. □

Since $Z(P_1) = \langle (i, c_i) \rangle = \{(\pm 1, I), (\pm i, c_i)\}$ then, as just observed, for $\psi \in \mathrm{Aut}(P_1)$ we must have $\psi(-1, I) = (-1, I)$.

Since Q is characteristic, then any $\psi \in \mathrm{Aut}(P_1)$ restricts to an automorphism of Q when applied to $Q \leq P_1$ (i.e. those ordered pairs (x, I))

And in the other direction, we can take an automorphism of Q and lift it to an automorphism of P_1.

But this requires considering the action on $(1, c_i)$ and ultimately (x, c_i).

Suppose $\phi \in Aut(Q)$ is the restriction of an automorphism $\hat{\phi} \in Aut(P_1)$, namely that

$$\hat{\phi}(x, I) = (\phi(x), I)$$

then the question is, what is $\hat{\phi}(x, c_i)$ or more fundamentally $\hat{\phi}(1, c_i)$?

Since

$$(1, c_i)(x, I)(1, c_i)^{-1} = (i, I)(x, I)(i, I)^{-1}$$

and if $\hat{\phi}(1, c_i) = (t, c_i)$ what one obtains is that

$$tc_i(x)t^{-1} = \phi(ixi^{-1}) \ \forall \ x \in Q$$

which in turn implies that

$$\phi(i)^{-1}ti \in Z(Q) = \{\pm 1\}$$

which, in the final analysis implies two possible values of 't' namely

$$t = \phi(i)(\pm i)$$

What we have then is that each $\phi \in Aut(Q)$ gives rise to two different automorphisms $\hat{\phi}_+, \hat{\phi}_- \in Aut(P_1)$ where

- $\hat{\phi}_+(x, I) = \hat{\phi}_-(x, I) = (\phi(x), I)\ \forall x \in Q$
- $\hat{\phi}_-(1, c_i) = (\phi(i)i, c_i)$
- $\hat{\phi}_+(1, c_i) = (-\phi(i)i, c_i)$

And since any $\psi \in Aut(P_2)$ restricts to an automorphism of Q then we have the following.

Proposition

$Aut(P_2) = A_+ \cup A_-$ where $A_+ = \{\hat{\phi}_+ \mid \phi \in Aut(Q)\}$ and $A_- = \{\hat{\phi}_- \mid \phi \in Aut(Q)\}$

And as far as the structure of this union, we consider $\hat{I}_+$ and $\hat{I}_-$.

Observe that

$$\hat{I}_+(1, c_i) = (-i \cdot i, c_i) = (1, c_i)$$
$$\hat{I}_-(1, c_i) = (ic \cdot i, c_i) = (-1, c_i)$$

so in particular the identity $I_{P_2} = \hat{I}_+ \in A_+$, and if we let $\delta = \hat{I}_-$ then $Aut(P_2) = A_+\langle\delta\rangle \cong Aut(Q) \times C_2$.

One can show also that $A_+ = \langle \gamma_i, \gamma_j, (ij)\delta, (jk)\delta \rangle \cong V \rtimes S_3$.

Our goal is to show that $\mathcal{R}(P_1) = \mathcal{S}(P_1)$, so we shall first enumerate $\mathcal{S}(P_1)$.

We have that $Hol(P_1) = P_1 \rtimes \mathrm{Aut}(P_1)$ which as a set can be written as

$$\{(q, c_i^e, \hat{\phi}_+, \delta^t) \mid q \in Q, \hat{\phi}_+ \in A^+; e, t \in \{0, 1\}\}$$

where again, $A_+ \cong Aut(Q)$.

Now, $\mathcal{S}(G)$ is usually viewed as the set of regular subgroups of the holomorph of G that are isomorphic to G, where we're viewing the holomorph as the normalizer of $\lambda(G)$.

However, we can, under the identification of the abstract semidirect product to this normalizer via

$$(g, \alpha) \leftrightarrow \rho(g) \circ \alpha$$

regularity of a subgroup of the normalizer can be interpreted as the property that, in the semi-direct product

$$N \leq G \rtimes \mathrm{Aut}(G)$$

is regular if the projection map $\pi_1 : G \rtimes \mathrm{Aut}(G) \rightarrow G$ is bijective, i.e. every element of G appears uniquely as a first coordinate of the elements of $N \leq G \rtimes \mathrm{Aut}(G)$.

Outline of the Enumeration

As the generators of any $N \in \mathcal{S}(P_1)$ are elements of $\mathrm{Hol}(P_1)$ we need to enumerate the elements of order 4 and order 2.

This is done, but the detailed tabulations are in the appendix.

Any such N has three generators, two of order 4 (which are stand-ins for 'i' and 'j' generating the copy of the Quaternion group) as well as one of order 2 acting as c_i does in P_1.

To further tame the combinatorial challenges, we filter out those elements which have fixed points under the identification

$$(g, \alpha) \leftrightarrow \rho(g) \circ \alpha$$

and with this, we consider those pairs of fixed point free generators which generate the unique (semi-regular) subgroup of N isomorphic to Q and then attach the order 2 generator.

As a (not unimportant stopover) we note the following (relatively minor in appearance) fact about $\mathrm{Hol}(P_1)$.

Proposition

$Z(\mathrm{Hol}(P_1)) = \langle(-1, c_i^0, I, \delta^0)\rangle$, which we can simply view as the element $-1 \in Q$ as naturally embedded in P_1, and in turn embedded in $\mathrm{Hol}(P_1)$.

The proof of this is straightforward, but the following observation about generators of the Quaternionic subgroup of each $N \in \mathcal{S}(P_1)$ is very important.

Proposition

If $N \in \mathcal{S}(P_1)$ *then* $-1 \in Z(N)$.

Proof.

This is a function of the enumeration of the fixed-point free elements of order 4 in $\mathrm{Hol}(P_1)$, namely that the square of each one is -1. □

As such, if we have $N \in \mathcal{S}(P_1)$ it is a subgroup of $\mathrm{Hol}(P_1)$ which contains a subgroup isomorphic to Q, as well as an element that acts like c_i.

Moreover, what this corollary says is that the 'i','j' in N must square to -1, as the squares of the imaginary units in Q lie in its center, $\langle -1 \rangle$.

All of the fixed point free elements of order 4 are potential generators.

In the interest of brevity, I will omit some of the other lower level details of the enumeration.

One interesting fact that was discovered was that all of the $N \in \mathcal{S}(P_1)$ are contained in an 'envelope', specifically.

Proposition

For each $N \in \mathcal{S}(P_1)$ *one has that* $N \leq E$ *which is the following subgroup of* $\mathrm{Hol}(P_1)$

$$E = \langle i, j, c_i, \gamma_i, \gamma_j, \delta \rangle$$

where $[\mathrm{Hol}(P_1) : E] = 6$ *and* $E \triangleleft \mathrm{Hol}(P_1)$.

Namely, $E \cong P_1 \rtimes (\mathrm{Inn}(Q) \times \langle \delta \rangle) \cong P_1 \rtimes \mathrm{Inn}(P_1) \times \langle \delta \rangle$, where $P_1 \rtimes \mathrm{Inn}(P_1)$ is what is sometimes referred to as the 'inner holomorph',

So in particular, a good many of the candidate order 4 fixed-point free elements in $\mathrm{Hol}(P_1)$ are ruled out as possible generators for $N \in \mathcal{S}(P_1)$.

We already saw from the table earlier that $|\mathcal{S}(P_1)| = 224$ and these are subdivided by considering the unique subgroup isomorphic to Q they contain.

It turns out that their are 56 distinct semi-regular subgroups (isomorphic to Q) of $\mathrm{Hol}(P_1)$, and 'over' each of these are 4 different $N \in \mathcal{S}(P_1)$, keyed to 4 distinct 'c_i' that together form a regular subgroup isomorphic to P_1.

Given the enumeration of $\mathcal{S}(P_1)$ we can easily show that each is normalized by $\lambda(P_1)$ and therefore that $\mathcal{S}(P_1) = \mathcal{R}(P_1)$ since for any G, one has that $|\mathcal{R}(G)| = |\mathcal{S}(G)|$.

Still further, one shows that $\mathcal{Q}(G) = \mathcal{S}(G)$ by demonstrating that all the elements of $\mathcal{S}(G)$ normalize each other.

As such, each pair of groups in $\mathcal{Q}(P_1)$ gives rise to a bi-skew brace, and one can also show that there are 46 distinct orbits with respect to the action of $Aut(P_1)$ on $\mathcal{Q}(P_1)$.

Higher P_n

As mentioned in passing earlier, there are a whole family of Pauli groups, which are constructed by taking the *n*-fold Kronecker products of the basic matrices I, X, Y, Z, which will act on $\mathbb{C}^{2^n}$.

For example

$$P_2 = \langle I \otimes X, X \otimes X, Y \otimes X, Z \otimes X, \dots, Z \otimes X \rangle$$

which yields a matrix subgroup of $GL_4(\mathbb{C})$ of order $64 = 4 \cdot 4^2$, and one can show that this is group 266 in the **SmallGroups** library of groups of order 64, of which there are 267 isomorphism classes total.

It's not (yet) clear if this too is an extension of a quaternionic group.

And while the details (at the moment) are mostly computational, here is what has been determined:

- $|\mathcal{S}(P_2)| = 7 \cdot 31 \cdot 2^{16} = 14,221,312$ (not a typo!)
- $\mathcal{S}(P_2) = \mathcal{R}(P_2)$
- $\mathcal{Q}(P_2) = \mathcal{S}(P_2)$

And so we again have a large cohort of bi-skew brace structures.

And beyond P_2, we have

$$P_3 = \langle I \otimes I \otimes X, I \otimes I \otimes Y, I \otimes I \otimes Z, \ldots, X \otimes X \otimes X, X \otimes X \otimes Y, \ldots, Z \otimes Z \otimes Z \rangle$$

which is a subgroup of $GL_8(\mathbb{C})$ of order $4 \cdot 4^3 = 256$ which GAP recognized as group 56091 (out of 56092) in the **SmallGroups** library of groups of order 256.

No determination of $\mathcal{S}(P_3)$ has been attempted...yet!

What's also nice about these groups is that they can be 'nested' inside each other.

Proposition

Given P_n (which consistists of $2^n \times 2^n$ matrices generated by iterated tensor products of $\{I, X, Y, Z\}$) if we let

$$\hat{P}_n = \{I_2 \otimes A \mid A \in P_n\}$$

then $\hat{P}_n$ is a subgroup of P_{n+1} that is isomorphic to P_n.

The proof of this is basically a consequences of how tensor products of matrices behave, namely that

$$(I_2 \otimes A)(I_2 \otimes B) = I_2 I_2 \otimes AB = I_2 \otimes AB$$

and so, naively, we should expect some close relationships to exist between their automorphism groups, holomorphs etc. as well as some 'containments' potentially of $\mathcal{S}(P_n)$ inside $\mathcal{S}(P_{n+1})$, however this may be construed to mean.

Of course, this has not been fully explored.

YBE within P_n

We saw above that P_1 is the group of 2×2 matrices, generated by $\{X, Y, Z\}$ and that P_2 is generated by the 16 matrices in $\{I \otimes I, \ldots, Z \otimes Z\}$.

One can show that if we take the 16 elements of P_1 and compute their pair-wise Kronecker products then we get all 64 elements of P_2 establishing a type of closure, although there are 256 such Kronecker products, every one of the elements of P_2 is representable by at least one such product.

Now consider the group P_3 generated by the threefold tensor powers of $\{I, X, Y, Z\}$.

For example, this group contains $I \otimes A \otimes B$ where I is 2×2 (acting on $V = \mathbb{C}^2$) and $A \otimes B$ is an invertible linear operator acting on $V \otimes V$, whence $I \otimes (A \otimes B) \in GL(V \otimes V \otimes V)$.

Moreover, $A \otimes B$ is very naturally a member of P_2.

So if we denote $R = A \otimes B \in P_2$ (where $A, B \in P_1 = \langle X, Y, Z \rangle$) then it makes sense to contemplate whether

$$(I \otimes R)(R \otimes I)(I \otimes R) = (R \otimes I)(I \otimes R)(R \otimes I)$$

which has exactly the form of the Yang-Baxter Equation, where this equation is defined within the group P_3.

And although it's not a terribly exciting answer, there are $R \in P_2$ for which this seems to hold, namely where R is a scalar multiple of the identity matrix by elements of $\{\pm 1, \pm i\}$.

For higher dimensional examples, $R = A_1 \otimes A_2 \dots A_n \in P_n$ acts on $\mathbb{C}^2 \otimes^n \mathbb{C}^2$ where the latter can be viewed as $V \otimes V$ if $n = 2k$ which implies that $n = k$.

So for example, the next higher iteration of this would be for

$$R = A_1 \otimes A_2 \otimes A_3 \otimes A_4 \in P_4$$

for $A_i \in P_1$ where $R \in GL(V \otimes V)$ for $V = \mathbb{C}^2 \otimes \mathbb{C}^2$ where now the actions on $V \otimes V \otimes V$ would be by $I_4 \otimes R = I_2 \otimes I_2 \otimes R$ and $R \otimes I = R \otimes I_2 \otimes I_2$, both of which would be defined in P_6.

And in general the pattern continues, with $R \in P_{2k}$ and the resulting operators $I \otimes R$ and $R \otimes I$ (and corresponding YBE) being defined within P_{3k}.

This may not have any broader interest, but it's kind of neat nonetheless.

Thank You.

Appendix

Order 2 elements of $\mathrm{Hol}(P_1)$.

$([-1, I], \delta^t)$
$([\pm 1, I], \alpha)$ for
$\alpha \in \{(ij)\delta^t, (ik)\delta^t, (jk)\delta^t, \gamma_i\delta^t, \gamma_i(jk)\delta^t, \gamma_j\delta^t, \gamma_j(ik)\delta^t, \gamma_k\delta^t, \gamma_k(ij)\delta^t\}$

$([\pm 1, c_i], \alpha)$ for $\alpha \in \{\delta, (jk)\delta, \gamma_i\delta, \gamma_i(jk)\delta, \gamma_j, \gamma_k\}$

$([\pm i, I], \alpha)$ for $\alpha \in \{(jk)\delta^t, \gamma_i(jk)\delta^t, \gamma_j\delta^t, \gamma_k\delta^t\}$

$([\pm i, c_i], \alpha)$ for $\alpha \in \{I, (ij)\delta, (ik)\delta, (jk)\delta, \gamma_i, \gamma_i(jk)\delta, \gamma_j, \gamma_j(ik)\delta, \gamma_k, \gamma_k(ij)\delta\}$

$([\pm j, I], \alpha)$ for $\alpha \in \{(ik)\delta^t, \gamma_i\delta^t, \gamma_j(ik)\delta^t, \gamma_k\delta^t\}$

$([\pm j, c_i], \alpha)$ for $\alpha \in \{\delta, (ij)\delta, \gamma_i, \gamma_j, \gamma_k\delta, \gamma_k(ij)\delta\}$

$([\pm k, I], \alpha)$ for $\alpha \in \{(ij)\delta^t, \gamma_i\delta^t, \gamma_j\delta^t, \gamma_k(ij)\delta^t\}$

$([\pm k, c_i], \alpha)$ for $\alpha \in \{\delta, (ik)\delta, \gamma_i, \gamma_j\delta, \gamma_j(ik)\delta, \gamma_k\}$

Fixed Point Free elements of Order 2 in $\mathrm{Hol}(P_1)$.

$([-1, I], \delta)$

$([\pm 1, c_i], \alpha)$ for $\alpha \in \{\delta, (jk)\delta, \gamma_i\delta, \gamma_i(jk)\delta, \gamma_j, \gamma_k\}$

$([\pm i, I], \alpha)$ for $\alpha \in \{\gamma_j\delta^t, \gamma_k\delta^t\}$

$([\pm i, c_i], \alpha)$ for $\alpha \in \{I, (ij)\delta, (ik)\delta, (jk)\delta, \gamma_i, \gamma_i(jk)\delta, \gamma_j, \gamma_j(ik)\delta, \gamma_k, \gamma_k(ij)\delta\}$

$([\pm j, I], \alpha)$ for $\alpha \in \{\gamma_i\delta^t, \gamma_k\delta^t\}$

$([\pm j, c_i], \alpha)$ for $\alpha \in \{\delta, (ij)\delta, \gamma_i, \gamma_j, \gamma_k\delta, \gamma_k(ij)\delta\}$

$([\pm k, I], \alpha)$ for $\alpha \in \{\gamma_i\delta^t, \gamma_j\delta^t\}$

$([\pm k, c_i], \alpha)$ for $\alpha \in \{\delta, (ik)\delta, \gamma_i, \gamma_j\delta, \gamma_j(ik)\delta, \gamma_k\}$

Order 4 elements in $\mathrm{Hol}(P_1)$.

$([\pm 1, I], \alpha)$ for $\alpha \in \{\gamma_i(ij)\delta^t, \gamma_i(ik)\delta^t, \gamma_j(ij)\delta^t, \gamma_j(jk)\delta^t, \gamma_k(jk)\delta^t\}$

$([\pm 1, c_i], \alpha)$ for $\alpha \in \{I, (jk), \gamma_i, \gamma_i(jk), \gamma_j\delta, \gamma_j(jk)\delta^t, \gamma_k\delta, \gamma_k(jk)\delta^t\}$

$([\pm i, I], \alpha)$ for $\alpha \in \{I, \delta, \gamma_i\delta^t, \gamma_j(jk)\delta^t, \gamma_k(jk)\delta^t\}$

$([\pm i, c_i], \alpha)$ for

$$\alpha \in \{\delta, (ij), (ik), (jk), \gamma_i\delta, \gamma_i(ij)\delta^t, \gamma_i(ik)\delta^t, \gamma_i(jk), \gamma_j\delta, \gamma_j(ij)\delta^t, \\ \gamma_j(ik), \gamma_j(jk)\delta^t, \gamma_k\delta, \gamma_k(ij), \gamma_k(ik)\delta^t, \gamma_k\delta^t\}$$

$([\pm j, I], \alpha)$ for $\alpha \in \{\delta^t, \gamma_i(ik)\delta^t, \gamma_j\delta^t, \gamma_k(ik)\delta^t\}$

$([\pm j, c_j], \alpha)$ for $\alpha \in \{I, (ij), \gamma_i\delta, \gamma_i(ij)\delta^t, \gamma_j\delta, \gamma_j(ij)\delta^t, \gamma_k, \gamma_k(ij)\}$

$([\pm k, I], \alpha)$ for $\alpha \in \{\delta^t, \gamma_i(ij)\delta^t, \gamma_j(ij)\delta^t, \gamma_k\delta^t\}$

$([\pm k, c_i], \alpha)$ for $\alpha \in \{I, (ik), \gamma_i\delta, \gamma_i(ik)\delta^t, \gamma_j, \gamma_j(ik), \gamma_k\delta, \gamma_k(ik)\delta^t\}$

Fixed Point Free elements of Order 4 in $\mathrm{Hol}(P_1)$.

$([\pm 1, c_i], \alpha)$ for $\alpha \in \{I, (jk), \gamma_i, \gamma_i(jk), \gamma_j\delta, \gamma_k\delta\}$

$([\pm i, I], \alpha)$ for $\alpha \in \{I, \delta, \gamma_i\delta^t\}$

$([\pm i, c_i], \alpha)$ for $\alpha \in \{\delta, (ij), (ik), (jk), \gamma_i\delta, \gamma_i(jk), \gamma_j\delta, \gamma_j(ik), \gamma_k\delta, \gamma_k(ij)\}$

$([\pm j, I], \alpha)$ for $\alpha \in \{\delta^t, \gamma_j\delta^t\}$

$([\pm j, c_j], \alpha)$ for $\alpha \in \{I, (ij), \gamma_i\delta, \gamma_j\delta, \gamma_k, \gamma_k(ij)\}$

$([\pm k, I], \alpha)$ for $\alpha \in \{\delta^t, \gamma_k\delta^t\}$

$([\pm k, c_i], \alpha)$ for $\alpha \in \{I, (ik), \gamma_i\delta, \gamma_j, \gamma_j(ik), \gamma_k\delta\}$

Hans Ulrich Besche, Bettina Eick, and E. A. O'Brien.
A millennium project: constructing small groups.
Internat. J. Algebra Comput., 12(5):623–644, 2002.

The GAP Group.
GAP – Groups, Algorithms, and Programming, Version 4.9.3, 2018.