1 Vatican Square Thoughts

1.1 Index Sets

Let $\mathbb{F}$ be an ordered field and let $A \subseteq \mathbb{F}$. For each $d \in \mathbb{F}^+$ let $A_{(d)} = \{a \in A | a + d \in A\}$. If $|A| = |\mathbb{F}|$ and for each d we have either $|A_{(d)}| = |\mathbb{F}|$ or $|A_{(d)}| = 0$, then A is an *index set*.

$\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}_{\geq 0}$, $\mathbb{Q}^+$ and $\mathbb{Q}$ are all index sets using $\mathbb{F} = \mathbb{Q}$, and $\mathbb{R}_{\geq 0}$, $\mathbb{R}^+$ and $\mathbb{R}$ are all index sets using $\mathbb{F} = \mathbb{R}$. I think this covers all the types of square we've considered so far and more.

We could drop the condition that the $A_{(d)}$ are all either empty or the size of $\mathbb{F}$, I think. However, we'd then need to do something different at the distances where this did not hold in the definition of Vatican squares, similar to how in finite squares ordered pairs appear at most once at a given distance rather than exactly once. I suspect the hassle of dealing with this is not worth it.

With this definition of index set, the definition of a directed T_∞-terrace becomes:

Let A be an index set in an ordered field $\mathbb{F}$. Let G be a group of order $|A|$. For a bijection $\mathbf{a} : A \to G$ define a function $\mathbf{a}_{(d)} : A \to G \setminus \{e\}$ for each $d \in \mathbb{F}^+$ with $A_{(d)} \neq \emptyset$ by

$$\mathbf{a}_{(d)}(i) = \mathbf{a}(i)^{-1}\mathbf{a}(i + d).$$

If each $\mathbf{a}_{(d)}$ is a bijection then $\mathbf{a}$ is a directed T_∞-terrace for G.

[The no-involution clause can be left off here. That's only needed for the semi-Vatican version.]

1.2 From Finite to Countably Infinite

If in the definition of a directed T_∞-terrace, the domain of $\mathbf{a}$ is $X \subseteq A$ for some finite X and the $\mathbf{a}_{(d)}$ functions are injective instead of bijective, then $\mathbf{a}$ is a *finite partial directed T_∞-terrace*.

Let A be an index set of $\mathbb{Q}$ and let G be a group with $|G| = |A|$. Assume that $\mathbf{a}$ is a finite partial directed T_∞-terrace for some $X \subseteq A$. If I've understood things correctly, the combinatorial results we need in order for the set theory to kick in and demonstrate the existence of a directed T_∞-terrace for A are:

1. For each $a \in A \setminus X$ we can find a $\mathbf{d} \leq \mathbf{a}$ such that $\operatorname{dom} \mathbf{d} \supseteq A \cup \{a\}$.
2. For each $r \in G \setminus \operatorname{range} \mathbf{a}$ we can find $\mathbf{e} \leq \mathbf{a}$ such that $\operatorname{range} \mathbf{e} \supseteq \operatorname{range} \mathbf{a} \cup \{r\}$.

3. For each $d \in \mathbb{Q}^+$ such that $A_{(d)} \neq \emptyset$, for each $a \in A \setminus \operatorname{dom} \mathbf{a}_{(d)}$ we can find $\mathbf{g} \leq \mathbf{a}$ such that $\operatorname{dom} \mathbf{g}_{(d)} \supseteq \operatorname{dom} \mathbf{a}_{(d)} \cup \{a\}$.

4. for each $d \in \mathbb{Q}^+$ such that $A_{(d)} \neq \emptyset$, for each non-identity $r \in G \setminus \operatorname{range} \mathbf{a}_{(d)}$ we can find $\mathbf{f} \leq \mathbf{a}$ such that $\operatorname{range} \mathbf{f}_{(d)} \supseteq \operatorname{range} \mathbf{a}_{(d)} \cup \{r\}$.

Translating into group theory:

1. We want a $g \in G \setminus \operatorname{range} \mathbf{a}$ such that setting $\mathbf{a}(a) = g$ does not break anything.

2. We want an $a \in A \setminus \operatorname{dom} \mathbf{a}$ such that setting $\mathbf{a}(a) = r$ does not break anything.

3. This follows from Item 1, so I'm not going to spell out what the conditions are.

4. We want an $a \in A \setminus \operatorname{dom} \mathbf{a}$ and a $g \in G \setminus \operatorname{range} \mathbf{a}$ such that $a + d \notin \operatorname{dom} \mathbf{a}$ and setting $\mathbf{a}(a) = g$ and $\mathbf{a}(a + d) = rg$ does not break anything.

What does it mean to meet these conditions?

1. For all d we need to have $g^{-1}\mathbf{a}(a+d) \notin \operatorname{range} \mathbf{a}_{(d)}$ and $\mathbf{a}(a-d)^{-1}g \notin \operatorname{range} \mathbf{a}_{(d)}$. All of these sets are finite, so these conditions can be rewritten as choosing g so as to avoid a finite set. We have infinitely many choices for g and so we can meet them.

   Also, for values of d where $a - d, a + d \in \operatorname{dom} \mathbf{a}$, we need that $\mathbf{a}(a-d)^{-1}g \neq g^{-1}\mathbf{a}(a+d)$; that is, $g\mathbf{a}(a-d)^{-1}g \neq \mathbf{a}(a+d)$. To achieve this in the draft we added the condition that G be *spreadable*: $\{xhx : x \in G\}$ is infinite for all h.

   However, in writing this, and without due reflection, I now recognise this as the problem I thought/think the old proof had/has. We potentially need to satisfy this for multiple values of d simultaneously and an intersection of infinite sets (from which we have to choose g) is not necessarily infinite. Does it fix things if we redefine spreadable to mean that $G \setminus \{xhx : x \in G\}$ is finite for all h?

   Some more reflection. The cowards' way out is simply to make the requirement we need the condition. Call a group G *cowardly* if for any finite list $((x_1, y_1), (x_2, y_2), \ldots, (x_k, y_k))$ of pairs of elements of G with $|\{x_1, x_2, \ldots, x_k, y_1, y_2, \ldots, y_k\}| = 2k$ (i.e. no repeated elements anywhere), we can find a $g \in G$ such that $x_i^{-1}g \neq g^{-1}y_i$ for $1 \leq i \leq k$.

   If G is abelian, the condition is met if given a subset $S \subseteq G$, with $G \setminus S$ finite, we can always choose a $g \in S$ such that g^2 is not in a given finite subset $T \subseteq G$. (Here $T \supseteq \{x_i y_i : 1 \leq i \leq k\}$. I don't see a way to get any value out of knowing that the x_i and y_i are distinct in general, but see below.)

   Further, if G is abelian and finitely generated then G is cowardly: any element $h \in G$ has finitely many square roots. Therefore, $\{g^2 : g \in G \setminus S\}$ is infinite as $G \setminus S$ is infinite.

   I know nothing about abelian groups that are not finitely generated, other than that they're less well-behaved than I might hope. Perhaps lots of them are also

cowardly? But consider C_2^ω: this doesn't meet the abelian group condition two paragraphs up, but it is cowardly: $x^{-1}g = g^{-1}y$ implies $x = y$, which cannot happen. So it's sneakily cowardly, and it is possible to get some traction from the distinctness of the x_i and y_i sometimes.

After a bit of trying I haven't managed to come up with an example of a non-cowardly group (somewhat serious, but far from exhaustive and mostly looking at abelian ones). Could it be that all countably infinite groups are cowardly??

2. We make a big enough to avoid any issues. Let

$$D = \max(\operatorname{dom} \mathbf{a}) - \min(\operatorname{dom} \mathbf{a})$$

and choose $a > \max(\operatorname{dom} \mathbf{a}) + D$. Set $\mathbf{a}(a) = r$. This adds at most one element to the ranges of $\mathbf{a}_{(d)}$ for $d > D$ and these were all empty prior to this assignment. It does not change the situation for $d \leq D$.

3. Nothing to see here.

4. As $\operatorname{dom} \mathbf{a}$ is finite, there are infinitely many values of a such that a and $a + d$ are not in the domain. Further, there are infinitely many values of a such that the maximum value of $\operatorname{dom} \mathbf{a}$ is smaller than a. Choose such an a.

There are finitely many g such $g \in \operatorname{range} \mathbf{a}$ and $h = gr \in \operatorname{range} \mathbf{a}$. We want to choose a $g \in G \setminus \operatorname{range} \mathbf{a}$ such that for all $b \in \operatorname{dom} \mathbf{a}$, we have

$$\mathbf{a}(b)^{-1}g \notin \operatorname{range} \mathbf{a}_{(a-b)}$$

and

$$\mathbf{a}(b)^{-1}gr = \mathbf{a}(b)^{-1}h \notin \operatorname{range} \mathbf{a}_{(a+d-b)}.$$

This is possible as $\bigcup_d \operatorname{range} \mathbf{a}_{(\mathbf{d})}$ is finite and we have infinitely many choices for g.

However, we also need to think about situations where adding g in this way adds more than one element to the range of an $\mathbf{a}_{(\ell)}$ for some ℓ: such elements cannot be equal. This we *can't* do without extra conditions. We require that $\mathbf{a}(a - \ell)^{-1}g \neq \mathbf{a}(a + d - \ell)^{-1}h$; that is, $\mathbf{a}(a - \ell + d)\mathbf{a}(a - \ell)^{-1} \neq grg^{-1}$. It might not be possible to choose g to guarantee this. (Changing our choice of a might be a route to fixing this, I have not thought that through but we have some unused leeway there.[1])

[1]First attempt (obsolete, but here in case it makes sense at some point down the line to revisit trying things in this order): There are infinitely many pairs (g, h) satisfying $g^{-1}h = r$ and we have only used finitely many pairs so far, so there are infinitely many valid choices. Choose one of them. As $\operatorname{dom} \mathbf{a}$ is finite, there are infinitely many values of a such that a and $a + d$ are not in the domain. Further, there are infinitely many values of a such that the maximum value of $\operatorname{dom} \mathbf{a}$ is smaller than a.

Given g and h we want such a value of a that, for all $b \in \operatorname{dom} \mathbf{a}$, we have

$$\mathbf{a}(b)^{-1}g \notin \operatorname{range} \mathbf{a}_{(a-b)}$$

and

$$\mathbf{a}(b)^{-1}h \notin \operatorname{range} \mathbf{a}_{(a+d-b)}$$

I don't see that we can guarantee this (although I haven't completely convinced myself that we can't). I think it'll be cleaner to fix a and look at the constraints on g and h, but as you see in the text that runs into issues too. Can those issues be avoided with this approach?

Escape Route 1: Rather than shooting for a T_∞ terrace, look for a T_D one for some fixed D. Then when choosing a, make it larger than $\max(\operatorname{dom}\mathbf{a}) + D$. This means that $\ell > D$ and we don't care if we get repeats in $\operatorname{range}\mathbf{a}_{(\ell)}$.

Escape Route 2: Insist that G is abelian. I think this will work for much the same reason as Theorem 5 of the draft paper does, but I haven't looked at the details. (Also, looking at the condition we have here, it seems like making G abelian guarantees that things can go wrong as the gs cancel entirely, which is not promising.) [Success with this track: see Theorem 1. One of the others might still be better though.]

Escape Route 3: Put some condition on the conjugacy classes of G so that we can always make the choice. That the conjugacy classes of all non-identity elements are infinite seems like a natural starting place, but also seems to be the opposite of the condition we found useful in the draft.

Escape Route 4: Limit the partial terraces we're building somehow in order to avoid future problems. This is the approach taken in the draft where some choices are ruled out in the intermediate steps between the partial terrace and the desired new element. I'm not sure how this translates (if at all) to the new approach of filling up positions at will rather than working along in a prescribed order.

Given all the above, what can we compile into a theorem with an genuine, fully-functioning proof? Theorem 1 doesn't push the limits of what is possible with these arguments, I don't think, but it's not too shabby.

Before writing it down, let's take a step that we should probably have taken long ago: replace "directed T_∞-terrace" with *vatican terrace*.

Theorem 1. *Every countably-infinite finitely-generated abelian group has a vatican terrace.*

Proof. Let $\mathbf{a}$ be a finite partial vatican terrace. To apply the set theoretic magic, we need to be able to:

1. Given $a \in A \setminus \operatorname{dom}\mathbf{a}$, find a $g \in G \setminus \operatorname{range}\mathbf{a}$ such that setting $\mathbf{a}(a) = g$ does not break anything.
2. Given $r \in G \setminus \operatorname{range}\mathbf{a}$, find an $a \in A \setminus \operatorname{dom}\mathbf{a}$ such that setting $\mathbf{a}(a) = r$ does not break anything.
3. Given $a \in A \setminus \operatorname{dom}\mathbf{a}_{(d)}$, find a $g \in G \setminus \operatorname{range}\mathbf{a}$ such that setting $\mathbf{a}(a) = g$ does not break anything and, if $a + d \notin \operatorname{dom}\mathbf{a}$, also find an $h \in G \setminus \operatorname{range}\mathbf{a}$ such that setting $\mathbf{a}(a + d) = h$ does not break anything.
4. Given a non-identity $r \in G \setminus \operatorname{range}\mathbf{a}_{(\mathbf{d})}$, find an $a \in A \setminus \operatorname{dom}\mathbf{a}$ and a $g \in G \setminus \operatorname{range}\mathbf{a}$ such that $a + d \notin \operatorname{dom}\mathbf{a}$ and setting $\mathbf{a}(a) = g$ and $\mathbf{a}(a + d) = rg$ does not break anything.

Let's consider them in turn.

To achieve Item 1, for all d we need to have $g^{-1}\mathbf{a}(a+d) \notin \operatorname{range}\mathbf{a}_{(d)}$ and $\mathbf{a}(a-d)^{-1}g \notin \operatorname{range}\mathbf{a}_{(d)}$. All of these sets are finite, so these conditions can be rewritten as choosing g so as to avoid a finite set.

Also, for values of d where $a-d, a+d \in \operatorname{dom}\mathbf{a}$, we need that $\mathbf{a}(a-d)^{-1}g \neq g^{-1}\mathbf{a}(a+d)$; that is, $g^2 \neq \mathbf{a}(a+d)\mathbf{a}(a-d)$. There are finitely many such conditions and, as G is finitely generated, there are infinitely many elements of g with distinct squares.

So we need to avoid finitely many options for g and have infinitely many to choose from; fine.

To achieve Item 2 we make a big enough to avoid any issues. Let

$$D = \max(\operatorname{dom}\mathbf{a}) - \min(\operatorname{dom}\mathbf{a})$$

and choose $a > \max(\operatorname{dom}\mathbf{a}) + D$. Set $\mathbf{a}(a) = r$. This adds at most one element to the ranges of $\mathbf{a}_{(d)}$ for $d > D$ and these were all empty prior to this assignment. It does not change the situation for $d \leq D$. [Later note: this doesn't work when A is bounded, which it can be; $\mathbb{Q} \cap (0,1)$, for example. The slightly more complicated method in the proof of Theorem 2 should patch it up though.]

Item 3 follows immediately from 1.

Finally, consider Item 4. As $\operatorname{dom}\mathbf{a}$ is finite, there are infinitely many values of a such that a and $a+d$ are not in the domain. Further, there are infinitely many values of a such that the maximum value of $\operatorname{dom}\mathbf{a}$ is smaller than a. Choose such an a.

There are finitely many g such $g \in \operatorname{range}\mathbf{a}$ and $h = gr \in \operatorname{range}\mathbf{a}$. We want to choose a $g \in G \setminus \operatorname{range}\mathbf{a}$ such that for all $b \in \operatorname{dom}\mathbf{a}$, we have

$$\mathbf{a}(b)^{-1}g \notin \operatorname{range}\mathbf{a}_{(a-b)}$$

and

$$\mathbf{a}(b)^{-1}gr = \mathbf{a}(b)^{-1}h \notin \operatorname{range}\mathbf{a}_{(a+d-b)}.$$

This is possible as $\bigcup_d \operatorname{range}\mathbf{a}_{(\mathbf{d})}$ is finite and we have infinitely many choices for g.

However, we also need to think about situations where adding g in this way adds more than one element to the range of an $\mathbf{a}_{(\ell)}$ for some ℓ: such elements cannot be equal. To cover this we require that $\mathbf{a}(a-\ell)^{-1}g \neq \mathbf{a}(a+d-\ell)^{-1}h$. However, using that G is abelian, $\mathbf{a}(a-\ell)^{-1}g = \mathbf{a}(a+d-\ell)^{-1}h$ implies that $g^{-1}h = \mathbf{a}(a-\ell)^{-1}\mathbf{a}(a+d-\ell)$, contradicting $g^{-1}h = r \notin \operatorname{range}\mathbf{a}_{(d)}$.

And abracadabra, by the power of Grayskull, piff-paff-puff, we are done. □

The finitely-generated condition in the theorem can be replaced with cowardliness. The abelian condition is more baked-in. One way around the latter is to change from looking

for a vatican terrace to a directed T_D-terrace and then when meeting item (d) we can put a far enough away from the existing elements of $\operatorname{dom} \mathbf{a}$ so that it doesn't cause problems.

I'm inclined to stick with abelian groups for the main thrust of the argument and maybe talk about some of these issues in passing. Going this way leaves one big question for this section: which countably-infinite abelian groups are cowardly and which are not?

For a group G, let $G_\square = \{g^2 : g \in G\}$ (is G^2 better notation, or does that evoke $G \times G$ too strongly?). A sufficient condition for cowardliness in countably infinite abelian groups that's much broader than being finitely generated is that $G_\square$ is infinite.

Not all countably infinite abelian groups are cowardly. Consider $\mathbb{Z}_3 \times \mathbb{Z}_2^\infty$ and consider the list of pairs

$$\{(101\mathbf{0}, 201\mathbf{0}), (0\mathbf{0}, 2\mathbf{0}), (01\mathbf{0}, 21\mathbf{0})\}$$

where in yet more horrid notation I've omitted the parentheses and commas from the direct product and a bold $\mathbf{0}$ indicates 0s forever. The three pairs mean that g^2 cannot be $0\mathbf{0}$, $1\mathbf{0}$ or $2\mathbf{0}$ respectively. However these are the only square elements of the group.

Perhaps having infinitely many squares is exactly cowardliness, with the exception of the degenerate case where the group is all involutions and so the list we'd build of pairs that require distinct non-identity squares is empty? Yes, I'm increasingly confident that this is the case and will write up a proper justification at some point.

2 From Countable to Uncountable

First order of business: prove the result we want for $\mathbb{R}$. This is really just me updating the earlier proof for countably-infinite abelian groups as I work through Kaethe's version to make sure that everything lines up. Perhaps recklessly, I'm going to shoot for squareful abelian groups of order $\aleph_1$ and hope I don't run into problems, where a group is *squareful* if $|G_\square| = |G|$. (I'm not trying to see how many bad choices of naming and notation I can make in a single document, I promise.)

Theorem 2. *Assuming the Continuum Hypothesis, every squareful abelian group of order $\aleph_1$ has a vatican terrace.*

Proof. [This is the proof of Theorem 1, updated for the new situation. Pleasingly, not much needed changing. I wonder if we can write them as a single proof to cover both situations without too much difficulty?]

Let G be the group and let $\mathbf{a}$ be a countable partial vatican terrace. To apply the set theoretic magic, we need to be able to:

1. Given $a \in A \setminus \operatorname{dom} \mathbf{a}$, find a $g \in G \setminus \operatorname{range} \mathbf{a}$ such that setting $\mathbf{a}(a) = g$ does not break anything.

2. Given $r \in G \setminus \operatorname{range} \mathbf{a}$, find an $a \in A \setminus \operatorname{dom} \mathbf{a}$ such that setting $\mathbf{a}(a) = r$ does not break anything.

3. Given $a \in A \setminus \operatorname{dom} \mathbf{a}_{(d)}$, find a $g \in G \setminus \operatorname{range} \mathbf{a}$ such that setting $\mathbf{a}(a) = g$ does not break anything and, if $a + d \notin \operatorname{dom} \mathbf{a}$, also find an $h \in G \setminus \operatorname{range} \mathbf{a}$ such that setting $\mathbf{a}(a + d) = h$ does not break anything.

4. Given a non-identity $r \in G \setminus \operatorname{range} \mathbf{a}_{(\mathbf{d})}$, find an $a \in A \setminus \operatorname{dom} \mathbf{a}$ and a $g \in G \setminus \operatorname{range} \mathbf{a}$ such that $a + d \notin \operatorname{dom} \mathbf{a}$ and setting $\mathbf{a}(a) = g$ and $\mathbf{a}(a + d) = rg$ does not break anything.

Let's consider them in turn.

To achieve Item 1, for all d we need to have $g^{-1}\mathbf{a}(a + d) \notin \operatorname{range} \mathbf{a}_{(d)}$ and $\mathbf{a}(a - d)^{-1}g \notin \operatorname{range} \mathbf{a}_{(d)}$. All of these sets are countable, so these conditions can be rewritten as choosing g so as to avoid a countable set.

Also, for values of d where $a - d, a + d \in \operatorname{dom} \mathbf{a}$, we need that $\mathbf{a}(a - d)^{-1}g \neq g^{-1}\mathbf{a}(a + d)$; that is, $g^2 \neq \mathbf{a}(a + d)\mathbf{a}(a - d)$. There are countably many such conditions and, as G is squareful, there are uncountably many elements of G with distinct squares.

So we need to avoid countably many options for g and have uncountably many to choose from; fine.

To achieve Item 2 we find an a with $a \notin \operatorname{dom} \mathbf{a}$ and for all d if $a - d \in \operatorname{dom} \mathbf{a}$ then $\mathbf{a}(a - d)^{-1}r \notin \operatorname{range} \mathbf{a}_{(d)}$ and if $a + d \in \operatorname{dom} \mathbf{a}$ then $r^{-1}\mathbf{a}(a + d) \notin \operatorname{range} \mathbf{a}_{(d)}$. This gives countably many restrictions and, as $\operatorname{dom} \mathbf{a}$ is countable, we have uncountably many possibilities for a and so can find one.

Item 3 follows immediately from 1.

Finally, consider Item 4. As $\operatorname{dom} \mathbf{a}$ is countable, there are uncountably many values of a such that a and $a + d$ are not in the domain, such that for all ℓ at most one of $a - \ell$ and $a + d + \ell$ is in the domain, and such that for all ℓ at most one of $a + \ell$ and $a + d - \ell$ is in the domain. Choose such an a.

There are countably many g such $g \in \operatorname{range} \mathbf{a}$ and $h = gr \in \operatorname{range} \mathbf{a}$. We want to choose a $g \in G \setminus \operatorname{range} \mathbf{a}$ that works with each $b \in \operatorname{dom} \mathbf{a}$. There are three situations depending on the position of b relative to a and $a + d$.

For all $b \in \operatorname{dom} \mathbf{a}$ with $b < a$, we require

$$\mathbf{a}(b)^{-1}g \notin \operatorname{range} \mathbf{a}_{(a-b)}$$

and

$$\mathbf{a}(b)^{-1}gr = \mathbf{a}(b)^{-1}h \notin \operatorname{range} \mathbf{a}_{(a+d-b)}.$$

For all $b \in \operatorname{dom} \mathbf{a}$ with $a < b < a + d$, we require

$$g^{-1}\mathbf{a} \notin \operatorname{range} \mathbf{a}_{(b-a)}$$

and

$$\mathbf{a}(b)^{-1}gr = \mathbf{a}(b)^{-1}h \notin \operatorname{range}\mathbf{a}_{(a+d-b)}.$$

For all $b \in \operatorname{dom}\mathbf{a}$ with $a + d < b$, we require

$$g^{-1}\mathbf{a} \notin \operatorname{range}\mathbf{a}_{(b-a)}$$

and

$$r^{-1}g^{-1}\mathbf{a}(b) = h^{-1}\mathbf{a}(b) \notin \operatorname{range}\mathbf{a}_{(b-(a+d))}.$$

These are possible as $\bigcup_d \operatorname{range}\mathbf{a}_{(\mathbf{d})}$ is countable and we have uncountably many choices for g.

However, we also need to think about situations where adding g in this way adds more than one element to the range of an $\mathbf{a}_{(\ell)}$ for some ℓ: such elements cannot be equal. Our choice of a rules out situations like $\mathbf{a}(a-\ell)^{-1}g \neq h^{-1}\mathbf{a}(a+d+\ell)$ where the existing domain elements are not to the same side of a and $a+d$ (although as it happens, I think we can handle those situations with squarefulness if we prefer)

To cover this we require that $\mathbf{a}(a-\ell)^{-1}g \neq \mathbf{a}(a+d-\ell)^{-1}h$ and $\mathbf{a}(a+\ell)^{-1}g \neq \mathbf{a}(a+d+\ell)^{-1}h$ for all ℓ in all instances where the terms in an inequality are defined. Using that G is abelian, $\mathbf{a}(a \pm \ell)^{-1}g = \mathbf{a}(a+d \pm \ell)^{-1}h$ implies that $g^{-1}h = \mathbf{a}(a \pm \ell)^{-1}\mathbf{a}(a+d \pm \ell)$, contradicting $g^{-1}h = r \notin \operatorname{range}\mathbf{a}_{(d)}$.

And abracadabra, by the power of Grayskull, piff-paff-puff, we are done. □

3 Orthogonal Orthomorphisms

Let G be a group and $\theta : G \to G$ a bijection. If $g \mapsto g^{-1}\theta(g)$ is a bijection then θ is an *orthomorphism*; if $g \mapsto g\theta(g)$ is a bijection then θ is a *complete mapping*. If θ is both an orthomorphism and a complete mapping then it is a *strong complete mapping*. Two orthomorphisms, θ, ϕ are *orthogonal* if $g \mapsto \theta(g)^{-1}\phi(g)$ is a bijection.

The study of "mutually orthogonal latin squares" is a big subset of Design Theory. In the finite case, an orthomorphism of G gives a pair of orthogonal latin squares using Cayley tables of G and a set of k mutually orthogonal orthomorphisms gives $k+1$ mutually orthogonal latin squares. There doesn't seem to have been much interest in infinite orthogonal latin squares (although there is an ILL I'm waiting on that I think will show that they've at least been defined somewhere). However, orthomorphisms for infinite groups have cropped up in a couple of places. So I propose, for now at least, we think about orthomorphisms and leave any latin square consequences to one side.

Why should we think about them at all? Because we've pretty much already constructed a bunch of them.

Let A be an index set in an ordered field $\mathbb{F}$. Let G be a group of order $|A|$. For a bijection $\mathbf{a} : A \to G \setminus \{e\}$ define a function $\mathbf{a}_{(d)} : A \to G \setminus \{e\}$ for each $d \in \mathbb{F}^+$

with $A_{(d)} \neq \emptyset$ by

$$\mathbf{a}_{(d)}(i) = \mathbf{a}(i)^{-1}\mathbf{a}(i+d).$$

If each $\mathbf{a}_{(d)}$ is a bijection then $\mathbf{a}$ is a directed R_∞-terrace for G.

Spot the difference. It's that we've taken the identity out of the range of $\mathbf{a}$. That we had the identity in the range was never an important point in the constructions, so for all groups for which we have constructed a directed T_∞-terrace we also have a directed R_∞-terrace.

Theorem 3. *Let G be a group of infinite order κ. If G has a directed R_∞-terrace then G has a set of κ mutually orthogonal orthomorphisms.*

Proof. Let $\mathbf{a}$ be a directed R_∞-terrace for G over some index set A. For each d such that $A_d \neq \emptyset$ (of which there are κ) define $\theta_d(e) = e$ and $\theta_d(\mathbf{a}(a)) = \mathbf{a}(a+d)$. This gives us the orthogonal orthomorphisms we're looking for:

First, they are orthomorphisms: given $g \in G \setminus \{e\}$ with $\mathbf{a}(a) = g$ we get

$$g^{-1}\theta_d(g) = \mathbf{a}(a)^{-1}\mathbf{a}(a+d) = \mathbf{a}_{(d)}(a)$$

which, when we also consider that $\theta_d(e) = e$, gives us a bijection on G.

Second, they are orthogonal: again taking $g \in G \setminus \{e\}$ with $\mathbf{a}(a) = g$, if $d_2 > d_1$ we get:

$$\theta_{d_1}^{-1}(g)\theta_{d_2}(g) = \mathbf{a}(a+d_1)^{-1}\mathbf{a}(a+d_2) = \mathbf{a}_{(d_2-d_1)}(a+d_1).$$

If $d_1 < d_2$ we get:

$$\theta_{d_1}^{-1}(g)\theta_{d_2}(g) = \mathbf{a}(a+d_1)^{-1}\mathbf{a}(a+d_2) = \mathbf{a}_{(d_1-d_2)}(a+d_2)^{-1}.$$

Also $\theta_{d_1}(e)^{-1}\theta_{d_2}(e) = e$ in each case, giving bijections on G. □

If we have a directed R_D-terrace, with the obvious definition, then the same argument gives $|\{d \leq D : A_d \neq \emptyset\}|$ mutually orthogonal orthomorphisms for G.

It's known that every infinite group has an orthomorphism [2] and that every countably infinite group has a strong complete mapping [1]. I haven't found anything about orthogonal orthomorphisms in infinite groups.

Question: can we set up posets of partial orthogonal orthomorphisms analogously to our partial terraces ones that lead to more families of groups having them than we can get via directed R_∞-terraces? What about strong complete mappings? In the latter case I think that the argument in [1] might extend to uncountable groups without much effort.

Even without doing any more work than we already have, we have infinite sets of mutually orthogonal orthomorphisms for squareful abelian groups of order $\aleph_0$ or $\aleph_1$.

References

[1] A. B. Evans, The existence of strong complete mappings, *Electronic J. Combin.* **19** (2012), #P34.

[2] P. T. Bateman, A remark on infinite groups, *Amer. Math. Monthly* **57** (1950), 623–624.