PACIFIC JOURNAL OF MATHEMATICS
Vol. 80, No. 2, 1979

DOUBLE COSET AND ORBIT SPACES

D. K. HARRISON

It is our purpose to study abstractly and in general, the structure of the set of all double cosets of a group with respect to a subgroup. In our first section we allow the groups to be infinite, and focus on a ternary collineation relation. If X, Y, Z are double cosets, we say they are collinear if there exists $x \in X, y \in Y, z \in Z$ with $x \cdot y \cdot z = 1$. This relation is abstracted and forms the basis of that section. In the second section we essentially insist the groups are finite, and count the double cosets which products from two cosets can appear in (i.e., count all Z with $x \cdot y \in Z$ for $x \in X, y \in Y$). We abstract the properties that these numbers possess, and study their implications. The orbit space of conjugacy classes of a finite group can be taken as a set of double cosets (in the holomorph of the group). This set has a natural dual, and in certain instances other sets of double cosets have one also. We study this situation in the third and last section by use of a complex matrix which enjoys some of the properties of the character table of a finite group; this may be thought of as another approach (slightly different than Brauer's pseudogroups) to character tables as a thing in themselves.

We have restricted attention in all three sections to a single operation. There are applications, particularly to valuations, of two operation systems where the additive structure is that of an orbit space, but in order to keep this paper from being too long we do not include those here.

We are grateful to Kenneth A. Ross for pointing out that several harmonic analysts (see [5], [6], and [11]) have considered these same problems with certainly related solutions. We believe we have minimized overlap, except for a crucial proof that the set of double cosets does satisfy the properties we wish to generalize, a proof which is one of Jewitt's ([6]), which we include for the reader's convenience. We wish to acknowledge helpful conversations with Hom Nath Bhattarai, James W. Fernandez, and William McClung.

1. Double coset spaces. If H is a subgroup of a group G, the set of double cosets, $G//H = \{HaH \mid a \in G\}$, is a group only when H is normal in G; however, in genaral it carries some structure which is retained by the following concept. The relation Δ which we use, in many cases is, and in general can be thought of, as a

sort of collinearity. By a *Pasch geometry* (alias multigroup or hypergroup, see [3]) we mean a triple (A, Δ, e) where A is a set, e is an element in A, and Δ is a subset of $A \times A \times A$ such that:

(1) for each $a \in A$ there exists a unique $b \in A$ with $(a, b, e) \in \Delta$; denote b by $a^{\#}$,

(2) $e^{\#} = e$ and $(a^{\#})^{\#} = a$ for all $a \in A$,

(3) $(a, b, c) \in \Delta$ implies $(b, c, a) \in \Delta$, and

(4) (Pasch's axiom) (a_1, a_2, a_3), $(a_1, a_4, a_5) \in \Delta$ imply there exists an $a_6 \in A$ with $(a_6, a_4^{\#}, a_2)$, $(a_6, a_5, a_3^{\#}) \in \Delta$ (see mneumonic diagram below).

We have so labelled (4), because when A is the real projective plane and Δ is collinearity, then (4) is expressed by the following diagram:

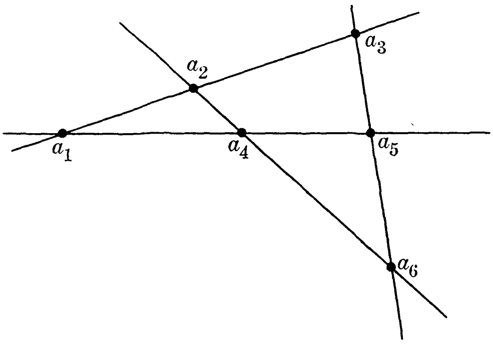

FIGURE 1

EXAMPLE 1.1 (see [4]). Let H be a subgroup of a group G. Let $G//H = \{HaH \mid a \in G\}$. Let

$$\Delta = \{(X, Y, Z) \in (G//H)^{3x} \mid \exists x \in X, y \in Y, z \in Z \text{ with } xyz = 1\} .$$

Then one easily checks $(G//H, \Delta, H)$ is a Pasch geometry.

EXAMPLE 1.2. Let F be a group of automorphisms of a group G. Let $G/F = \{\{f(a) \mid f \in F\} \mid a \in G\}$ be the set of orbits. Let

$$\Delta = \{(X, Y, Z) \in (G/F)^{3x} \mid \exists x \in X, y \in Y, z \in Z \text{ with } xyz = 1\} .$$

Then one easily checks $(G/F, \Delta, \{1\})$ is a Pasch geometry. This can be viewed as a special case of the last example, for it is isomorphic to $G \times F//F$ where $G \times F$ is the split extension of G by F with the given operation of F on G.

EXAMPLE 1.3. We say a Pasch geometry (A, Δ, e) is *sharp* if for each $a, b \in A$ there exists at most one $c \in A$ with $(a, b, c) \in \Delta$. One can show there always is at least one such c, and if $a \cdot b$ denotes $c^{\#}$, one checks a group results. Conversely, if G is a group, one gets a sharp Pasch geometry by letting $\Delta = \{(a, b, c) \in G^{3x} | abc = 1\}$.

EXAMPLE 1.4 (compare [7]). Projective spaces in which lines have exactly three points are rather transparent since they correspond exactly to groups in which every element is its own inverse; i.e., to vector spaces over Z_2. Hence in the interest of simplicity we use the following definition. By a (not necessarily Desarguean) *projective space* we mean a pair $(P, \mathscr{L})$ where P is a set and $\mathscr{L}$ is a set of subsets of P, each of which has at least *four* elements, such that:

(1) $p, q \in P, p \neq q$ imply $\exists$ unique $L \in \mathscr{L}$ (denoted by Lpq) with $\{p, q\} \subseteqq L$, and

(2) (the real Pasch axiom) p_2, p_3, p_4, p_5 distinct in P, and $p_1 \in Lp_2p_3 \cap Lp_4p_5$ imply $\exists$ $p_6 \in Lp_2p_4 \cap Lp_3p_5$.

Let $(P, \mathscr{L})$ be such. Let e be an element not in P and let $P^\# = P \cup \{e\}$. For $p_1, p_2, p_3 \in P$, we let (p_1, p_2, p_3) be in Δ if and only if they are distinct and collinear (meaning $p_3 \in Lp_1p_2$), or they are equal (meaning $p_1 = p_2 = p_3$). We also let (e, e, e) and (e, p, p), (p, e, p), (p, p, e) be in Δ for all $p \in P$. A tedius checking of special cases gives that $(P^\#, \Delta, e)$ is a Pasch geometry.

EXAMPLE 1.5. Let L be a lattice with least element e. Let

$$\Delta_L = \{(a, b, c) \in L^{3x} | a \leqq b \vee c, b \leqq a \vee c, c \leqq a \vee b\} .$$

Then we show (L, Δ_L, e) is a Pasch geometry if and only if L is modular (Proposition 1.8).

A Pasch geometry (A, Δ, e) will often simply be denoted by A, in which case we may either write Δ_A for Δ and e_A for e, or simply let context descriminate between possible ambiguities. Also, when the context is clear, we will sometimes simply write "geometry" for "Pasch geometry".

Two lemmas which are easily checked for an arbitrary Pasch geometry A are: $(a, b, c) \in \Delta$ implies $(c^\#, b^\#, a^\#) \in \Delta$, and $x, y \in A$ implies $\exists z \in A$ with $(x, y, z) \in \Delta$.

Let A, B be geometries. By a (geometry) *morphism* from A to B we mean a subset f of $A \times B$ such that:

(1) for each $a \in A$ there exists a $b \in A$ with $(a, b) \in f$,

(2) $(e, b) \in f$ implies $b = e$,

(3) $(a, b) \in f$ implies $(a^\#, b^\#) \in f$, and

(4) $(a_1, a_2, a^\#) \in \Delta_A$, $(a, b) \in f$ imply there exists $b_1, b_2 \in B$ with (a_1, b_1), $(a_2, b_2) \in f$ and $(b_1, b_2, b^\#) \in \Delta_B$.

We call a morphism f *sharp* when it is a map (i.e., when $a \in A$ implies there is at most one $b \in B$ with $(a, b) \in f$), and call it *strict* when the converse to (4) holds; i.e.,

(5) $(a_1, b_1), (a_2, b_2) \in f$, $(b_1, b_2, b^\sharp) \in \Delta_B$ imply there exists an $a \in A$ with $(a_1, a_2, a^\sharp) \in \Delta_A$ and $(a, b) \in f$.

If C is a geometry, g is a morphism from B to C, and f is a morphism from A to B, one checks $g \circ f$ is a morphism from A to C, where $g \circ f$ denotes

$$\{(a, c) \in A \times C \mid \exists b \in B \text{ with } (a, b) \in f \text{ and } (b, c) \in g\} .$$

If f and g are sharp (respectively strict), then $g \circ f$ is sharp (respectively strict). Since the identity map is a morphism (which is sharp and strict), we have the category of Pasch geometries (and the sharp and strict subcategories). One checks an isomorphism from A to B is a bijective map $f: A \rightarrow B$ with $f(e) = e$ and $(a_1, a_2, a_3) \in \Delta_A$ if and only if $(f(a_1), f(a_2), f(a_3)) \in \Delta_B$. We write $A \cong B$ only if such exists. By a *homomorphism* we mean a sharp and strict morphism. If we identify groups with sharp geometries, the category of groups is a full subcategory of the category of geometries with homomorphisms. Most of the elementary properties of the category of groups extend to this category.

By a *subgeometry* of a geometry A we mean a subset S of A such that $e \in S$ and $(s_1, s_2, a) \in \Delta$, $s_1, s_2 \in S$ imply $a \in S$. Note that if A is a group (i.e., is sharp), a subgeometry is the same as a subgroup. We call a subgeometry S of A *normal* (see [4]) if $(s, a, b) \in \Delta$, $s \in S$ imply there exists $s_1 \in S$ with $(s_1, b, a) \in \Delta$. If T is any subset of A, we denote the intersection of all subgeometries of A which contain T by $\langle T \rangle$ and call it the subgeometry generated by T. Note if S is a subgeometry of A, by letting $\Delta_S = \Delta_A \cap S^{3x}$, S is itself a Pasch geometry.

Let S be a subgeometry (*not* necessarily normal) of a geometry A. For $a, b \in S$ write $a \sim b$ if $\exists s_1, s_2 \in S$ and $x \in A$ with $(a, s_1, x^\sharp)$, $(x, b^\sharp, s_2) \in \Delta$. One checks this is an equivalence relation. For $a \in A$ let $[a]_S$ (or simply $[a]$) denote $\{b \in A \mid a \sim b\}$. Let $A//S$ denote $\{[a] \mid a \in A\}$. One checks $[e] = S$. Let

$$\Delta_{(A//S)} = \{(X, Y, Z) \in (A//S)^{3x} \mid \exists x \in X, y \in Y, z \in Z \text{ with } (x, y, z) \in \Delta_A\} .$$

PROPOSITION 1.1 (*compare* [4]). *Let S be a subgeometry of a Pasch geometry A. Then $A//S$ is a Pasch geometry. The natural map $a \mapsto [a]_S$ is a sharp morphism from A to $A//S$. It is strict (i.e., a homomorphism) if and only if S is normal.*

The proof is a routine check and is omitted.

PROPOSITION 1.2. *Let A and B be Pasch geometries. Let f be a homomorphism from A to B. Let $K_f = \{a \in A \mid f(a) = e\}$ and*

$I_f = \{f(a) \mid a \in A\}$. Then I_f is a subgeometry of B, K_f is a normal subgeometry of A, f induces an isomorphism $\bar{f}$ from $A//K_f$ onto I_f, and f can be factored as $f = i \circ \bar{f} \circ j$ where $j \colon A \to A//K_f$ and $i \colon I_f \to B$ are the natural homomorphisms.

Proof. $e \in K_f$ and if $(k_1, k_2, a) \in \Delta_A$, $k_1, k_2 \in K_f$, then $(f(k_1), f(k_2), f(a)) \in \Delta_B$ so $(e, e, f(a)) \in \Delta_B$ so $(e, f(a), e) \in \Delta_B$ so $f(a) = e^\# = e$ so $a \in K_f$. Thus K_f is a subgeometry. If $[a_1] = [a_2]$, then $(a_1, k_3, x^\#)$, $(x, a_2^\#, k_4) \in \Delta_A$ where $k_3, k_4 \in K_f$. Thus $(f(a_1), e, f(x)^\#)$, $(f(x), f(a_2)^\#, e) \in \Delta_B$ so $f(a_2)^\# = f(x)^\#$ and $(e, f(x)^\#, f(a_1)) \in \Delta_B$, so $f(a_2) = (f(a_2)^\#)^\# = (f(x)^\#)^\# = f(x)$ and $(f(x)^\#, f(a_1), e) \in \Delta_B$. Thus $f(a_1) = (f(x)^\#)^\# = f(x)$. We get $f(a_1) = f(a_2)$. Thus $[a] \mapsto f(a)$ is a well-defined map which we denote by $\bar{f}$. Let $f(a_3) = f(a_4)$. Then $(f(a_3), f(a_4^\#), e^\#) \in \Delta_B$, so since f is strict, $(a_3, a_4^\#, a^\#) \in \Delta_A$, $(a, e) \in f$ for some $a \in A$. Thus $(a^\#, e^\#) \in f$ so $a^\# \in K_f$. Also $e \in K_f$ and $(a_1, e, a_1^\#)$, $(a_1, a_2^\#, a^\#) \in \Delta_A$ so $a_1 \sim a_2$ so $[a_1] = [a_2]$. Thus $\bar{f}$ is injective. The proof is easily continued in this fashion.

PROPOSITION 1.3 (*see* [4]). *Let A be a Pasch geometry. If S is a subgeometry of A and T is a normal subgeometry of A and $S \cdot T$ denotes $\{x \in A \mid \exists s \in S, t \in T$ with $(s, t, x) \in \Delta\}$, then $S \cdot T$ is a subgeometry of A, $S \cap T$ is a normal subgeometry of S, and*

$$(S \cdot T)//T \cong S//(S \cap T) .$$

Proof. This is easily checked using among other things $s \mapsto [s]_T$ and the last proposition.

PROPOSITION 1.4. *Let S be a subgeometry (not necessarily normal) of a Pasch geometry A. Let $f \colon A \to A//S$ be the natural map. For T a subgeometry of A which contains S, $T//S$ (which is the same as $\{f(t) \mid t \in T\}$) is a subgeometry of $A//S$, and*

$$(A//S)//(T//S) \cong A//T .$$

Moreover, this gives a bijective inclusion preserving correspondence between the set of all subgeometries of A which contain S and the set of all subgeometries of $A//S$. Also normal correspond to normal in this correspondence if and only if S is normal in A.

Proof. This is a long but straightforward check which we omit.

We call a geometry A *abelian* if $(a_1, a_2, a_3) \in \Delta_A$ implies $(a_2, a_1, a_3) \in \Delta_A$.

Let A, B be geometries. We define

$$\Delta_{A\times B} = \{((a_1, b_1), (a_2, b_2), (a_3, b_3)) \in (A \times B)^{3x} \mid (a_1, a_2, a_3) \in \Delta_A, (b_1, b_2, b_3) \in \Delta_B\} ,$$

and check that $(A \times B, \Delta_{A\times B}, (e, e))$ is a geometry. For notation we let Sh (respectively St) denote the category of all Pasch geometries with sharp morphisms (respectively with strict morphisms). Thus if C is a geometry, $\mathrm{Sh}(A, C)$ denotes the set of all sharp morphisms from A to C, and $\mathrm{St}(A, C)$ denotes the set of all strict morphisms from A to C. We define $p_A \in \mathrm{Sh}(A \times B, A)$, $p_B \in \mathrm{Sh}(A \times B, B)$, $in_A \in \mathrm{St}(A, A \times B)$, $in_B \in \mathrm{St}(B, A \times B)$ by $p_A((a, b)) = a$, $p_B((a, b)) = b$, $in_A(a) = (a, e)$, $in_B(b) = (e, b)$ $\forall a \in A$, $b \in B$, and check these maps are in the sets we claim they are. It is easy (but tedious) to check the following:

PROPOSITION 1.5. *For A, B, C Pasch geometries we have a natural identification*

$$\mathrm{Sh}(C, A \times B) \longleftrightarrow \mathrm{Sh}(C, A) \times \mathrm{Sh}(C, B) \quad (h \longleftrightarrow (p_A \circ h, p_B \circ h))$$

and if in addition C is abelian, we have another natural identification

$$\mathrm{St}(A \times B, C) \longleftrightarrow \mathrm{St}(a, c) \times \mathrm{St}(B, C) \quad (h \longleftrightarrow (h \circ in_A, h \circ in_B)) .$$

Let G be a group. By a *G-geometry* we mean a Pasch geometry A together with a group homomorphism, $\alpha \mapsto f_\alpha$, of G into the group of isomorphisms of A to itself. We usually write $\alpha(a)$ for $f_\alpha(a)$. Let A and B be G-geometries. By a G-morphism from A to B we mean a morphism f from A to B such that $(a, b) \in f$ implies $(\alpha(a), \alpha(b)) \in f$ for all $\alpha \in G$. One checks these compose so we have the category of G-geometries. One checks $A \times B$ is made into a G-geometry by defining $\alpha((a, b)) = (\alpha(a), \alpha(b))$ for all $\alpha \in G$, $(a, b) \in A \times B$. By a G-subgeometry of a G-geometry A we mean a subgeometry S of A such that $\alpha(s) \in S$ for all $s \in S$ and $\alpha \in G$. Such is clearly a G-geometry in its own right. One can check that all the previous propositions hold with "geometry", "morphism," and "subgeometry" prefixed everywhere they appear by "G-".

Let H be a subgroup of the group G. Let A be a G-geometry. Then A is naturally an H-geometry (by restricting the operation to H). For $a, b \in A$ write $a \sim b$ if $\alpha(a) = b$ for some $\alpha \in H$. This is an equivalence relation, and we write $\langle a \rangle_H$ (or simply $\langle a \rangle$) for the unique equivalence class containing a. Let A/H denote $\{\langle a \rangle \mid a \in A\}$, and

$$\Delta_{A/H} = \{(X, Y, Z) \in (A/H)^{3x} \mid \exists x \in X, y \in Y, z \in Z \text{ with } (x, y, z) \in \Delta_A\} .$$

One checks $(A/H, \Delta_{A/H}, \langle e\rangle)$ is a Pasch geometry. For $X \in G//H$ let f_X denote

$$\{(Y, Z) \in (A/H)^{2x} \mid \exists y \in Y, z \in Z, \alpha \in X \text{ with } \alpha(y) = z\} .$$

One checks this is a morphism from A/H to itself, and if H is normal in G it gives A/H the structure of a $G//H$-geometry. We have:

PROPOSITION 1.6. *Let G be a group and A be a Pasch G-geometry. Let H be a subgroup of G. Then A/H is a Pasch geometry. If in addition H is normal, then A/H is a $G//H$-geometry. If f is the natural map from A to A/H and g is the natural morphism from A/H to A then f is a sharp morphism, g is a strict morphism and $f \circ g$ is the identity morphism of A/H.*

PROPOSITION 1.7. *Let H be a group. Let A be a Pasch H-geometry. Then there exists a natural order preserving bijection between the H-subgeometries of A and the subgeometries of A/H. This bijection is $S \mapsto \{\langle s\rangle \mid s \in S\} = S/H$. Moreover, if S is an H-subgeometry of A, then*

$$(A//S)/H \cong (A/H)//(S/H)$$

by $\langle [a]_S\rangle_H \leftrightarrow [\langle a\rangle_H]_{S/H}$.

Proof. This is a routine long check which we omit.

By the *split extension* $A \underline{\times} H$ of a Pasch H-geometry A we mean $(A \times H, \Delta, (e, 1))$ where Δ consists of all

$$((a_1, \alpha_1), (a_2, \alpha_2), (a_3, \alpha_3))$$

with

$$(a_1, \alpha_1(a_2), \alpha_1(\alpha_2(a_3))) \in \Delta_A \text{ and } (\alpha_1, \alpha_2, \alpha_3) \in \Delta_H .$$

One checks this is a Pasch geometry. If f is an H-morphism from A to an H-geometry B, we let $f \underline{\times} H$ denote

$$\{((a, \alpha), (b, \alpha)) \mid (a, b) \in f,\ \alpha \in H\} .$$

One checks this gives a functor, and allows us to extend the notion of an H-geometry to the case where H is an arbitrary Pasch geometry in a way which we now give. Let H be a Pasch geometry. By an *H-geometry* we mean a triple (B, S, f) where B is a Pasch geometry, S is a normal subgeometry of B, and f is an injective homomorphism from H into B such that $S \cap I_f = \{e\}$ and $S \cdot I_f = B$. We often denote an H-geometry (B, S, f) simply by S, in which case we write B_S for B and f_S for f. If T is another H-geometry, a *H-morphism* from S to T will mean a morphism g from B_S to B_T with $g \circ f_S = f_T$ and with $s \in S$, $(s, b) \in g$ implying $b \in T$. We denote $B//I_f$ by S/H. Proposition 1.7 can now be generalized to this situation in a natural way.

Let A be a Pasch geometry. Let $\mathscr{S}(A)$ be the set of all normal subgeometries of A. With inclusion $\mathscr{S}(A)$ is a partially ordered set, and one checks if S_i, $i \in I$, is an indexed family of normal subgeometries of A then $\langle \cup S_i \rangle$ is in $\mathscr{S}(A)$ and is a least upper bound of the S_i, $i \in I$. Hence $\mathscr{S}(A)$ is a complete lattice. If $S, T \in \mathscr{S}(A)$, the greatest lower bound, $S \wedge T$, of S and T is

$$\{a \in A \mid \exists N \in \mathscr{S}(A) \text{ with } a \in N \subseteqq S \cap T\} .$$

If A is abelian this is just the intersection; in this case one checks $\mathscr{S}(A)$ is modular so by the next result $\mathscr{S}(A)$ is an abelian Pasch geometry.

PROPOSITION 1.8. *Let L be a lattice with least element e. Let*

$$\varDelta = \{(x, y, z) \in L^{3x} \mid x \vee y = x \vee z = y \vee z\} .$$

Then $(L, \varDelta, e)$ is a Pasch geometry if and only if L is modular.

Proof. Suppose L is modular. All but Pasch is easily checked. One checks $x \leqq y \vee z$, $y \leqq w \vee u$ implies $x \leqq ((x \vee w) \wedge (z \vee u)) \vee w$. Now let $(a_1, a_2, a_3), (a_1, a_4, a_5) \in \varDelta$. Letting $a_6 = (a_4 \vee a_2) \wedge (a_5 \vee a_3)$ we have $a_6 \leqq a_4 \vee a_2$. Since $a_2 \leqq a_1 \vee a_3$ and $a_1 \leqq a_4 \vee a_5$, by letting $x = a_2$, $y = a_1$, $z = a_3$, $w = a_4$, $u = a_5$, we get $a_2 \leqq (a_2 \vee a_4) \wedge (a_3 \vee a_5) \vee a_4 = a_6 \vee a_4$. Similarly, we get $a_4 \leqq a_6 \vee a_2$. Thus $(a_6, a_4, a_2) \in \varDelta$. Similarly, we show $(a_6, a_5, a_3) \in \varDelta$.

Now conversely, suppose L is not modular. Then $\exists x \leqq z$ with $x \vee (y \wedge z) \neq (x \vee y) \wedge z$. This implies $x \neq z$ so $x < z$. It also implies $x \vee (y \wedge z) < (x \vee y) \wedge z$ (one checks). Let $b = x \vee (y \wedge z)$, $a = (x \vee y) \wedge z$, $c = y$. Then one checks $a \vee c = b \vee c = x \vee y$. Applying this same sequence of arguments to the dual of L gives $a \wedge c = b \wedge c = z \wedge y$. Thus $(a \vee c, a, c), (b \vee c, b, c) \in \varDelta$. Since $a \vee c = b \vee c$, if L were a geometry there would exist a $w \in L$ with $(w, b, a), (w, c, c) \in \varDelta$ (one checks $b^{\#}$ would have to be b and $c^{\#}$ would have to be c). This would give $w \leqq b \vee a = a$ (since $b < a$) and $w \leqq c \vee c = c$ so $w \leqq a \wedge c$. Thus $b \vee w \leqq b \vee (a \wedge c)$. But $a \leqq b \vee w$ so $a \leqq b \vee (a \wedge c)$. Thus $a \leqq b \vee (a \wedge c) = b \vee (b \wedge c) = b$ which contradicts that $b < a$. The proposition is proved.

Since a modular lattice can be reconstructed from its geometry ($a \leqq b$ if and only if $(a, b, b) \in \Delta$), we can view a modular lattice as a special kind of geometry and thus use our terminology for morphisms. For A a geometry and $a \in A$, let $\mathscr{S}(a)$ be the greatest lower bound of all $T \in \mathscr{S}(A)$ with $a \in T$. At least if one restricts attention to abelian geometries, $a \mapsto \mathscr{S}(a)$ and $S \mapsto \{(S, a) \in \mathscr{S}(A) \times A \mid a \in S\}$ are monads and comonands respectively in the appropriate categories.

The category of projective spaces is a full subcategory of the category of Pasch geometries; it can be recovered as follows. For $(P, \mathscr{L})$ a projective space with P nonempty, $(P^\sharp, \Delta, e)$ is a geometry which is not sharp and which satisfies $\mathscr{S}(a) = \{e, a\}$ for all $a \in P^\sharp$ (see Example 1.4). Conversely, let A be a Pasch geometry such that $\{e, a\}$ is a subgeometry of A for all $a \in A$, and A is not sharp. Let $A^* = A \backslash \{e\}$, and for $a, b \in A^*$, $a \neq b$ let

$$\mathrm{Lab} = \{c \in A^* \mid (a, b, c) \in \Delta\} \cup \{a, b\} ,$$

and let $\mathscr{L} = \{\mathrm{Lab} \mid a, b \in A^* \text{ with } a \neq b\}$. With some straightforward drudgery one can check that $(A^*, \mathscr{L})$ is a projective space with A^* nonempty. Also these constructions are inverses of each other.

Let G be a group (not a general geometry simply for simplicity). We call a G-homomorphism $f: A \rightarrow B$ *central* if $(f(a), b_1, b_2) \in \Delta_B$ implies $(f(a), b_2, b_1) \in \Delta_B$ for all $a \in A$.

Let S be a G-group (i.e., a sharp G-geometry). By an *S-G-geometry* we mean a pair (f_A, A) where A is a G-geometry and f_A is a strict G-morphism from S to A. One checks then f_A must be a G-homomorphism. We often denote (f_A, A) simply by A. By an S-G-morphism from an S-G-geometry A to an S-G-geometry B we mean a morphism h from A to B with $h \circ f_A = f_B$. One checks these compose so we have the category of S-G-geometries. We wish particularly to have Proposition 1.5 generalized to this context. For A and B S-G-geometries we let $\mathrm{Sh}_{S-G}(A, B)$ (respectively $\mathrm{St}_{S-G}(A, B)$) denote the set of all S-G-morphisms which are in $\mathrm{Sh}(A, B)$ (respectively $\mathrm{St}(A, B)$). By Proposition 1.5 there exists a unique sharp G-morphism f from S to $A \times B$ with $p_A \circ f = f_A$ and $p_B \circ f = f_B$ (simply $f(s) = (f_A(s), f_B(s))$). One checks (using S is a group) that f is strict, and so makes $A \times \mathrm{B}$ into an S-G-geometry. We denote f by $f_A \times f_B$. By Proposition 1.2 the image I of $f_A \times f_B$ is a G-subgeometry of $A \times B$. In general, we cannot make the G-geometry $A \times B // I$ into a S-G-geometry, but when S is abelian and both f_A and f_B are central we proceed as follows. S an abelian group implies $s \mapsto s^{-1}$ is a G-isomorphism (thus strict), so if $f_B^\sharp(s) = f_B(s^{-1})$ for all $s \in S, f_B^\sharp$ is a strict G-morphism (actually a G-homomorphism) and makes B into an S-G-geometry. We let I be the image of $f_A \times f_B^\#$ and let $A \times {}_S B$ denote the G-geometry $A \times B//I$. Using that both f_A and f_B are central, we check that I is normal in $A \times B$, and thus by Proposition 1.1 get that the natural map g: $A \times B \rightarrow A \times {}_S B$ is a strict G-morphism. Letting $1_B(s) = e \forall s \in S$ we check that 1_B is a strict G-morphism and that $f_A \times 1_B$ is strict, and use $g \circ (f_A \times 1_B)$ (i.e., $s \mapsto [(f_A(s), e)]_I$) to give $A \times {}_S B$ the structure of an S-G-geometry. The apparent lack of symmetry is only apparent, since if $s \in S$,

$$((f_A(s), e), (e, e), (f_A(s), e)^\#), ((f_A(s), e), (e, f_B(s))^\#), (f_A(s^\#), f_B^\#(s^\#)) \in \Delta$$

so

$$[(f_A(s), e)]_I = [(e, f_B(s))]_I \, .$$

PROPOSITION 1.9. *Let G be a group and S be a G-group. Let A, B, C be Pasch S-G-geometries. Then we have a natural identification*

$$\mathrm{Sh}_{S-G}(C, A \times B) \longleftrightarrow \mathrm{Sh}_{S-G}(C, A) \times \mathrm{Sh}_{S-G}(C, B)(h \longleftrightarrow (p_A \circ h, p_B \circ h))$$

and if in addition C is abelian, S is abelian, and f_A, f_B, are central, we have another natural identification

$$\mathrm{St}_{S-G}(A \times {}_S B, C) \longleftrightarrow \mathrm{St}_{S-G}(A, C) \times \mathrm{St}_{S-G}(B, C)(h \longleftrightarrow (h \circ g \circ in_A, h \circ g \circ in_B)) \, .$$

Proof. Using Proposition 1.5 this is a long routine check which we omit.

We end this section with a construction which gives examples and also gives some insight into how a single element behaves in a geometry. Let A be an arbitrary Pasch geometry (not an S-G-geometry merely for simplicity). Let T be any subset of A which is closed under $(\ )^\#$ (i.e., $t^\# \in T \forall t \in T$) with $e \notin T$. For X either A or T, we define an *X-word* to mean an n-tuple, $n \geqq 0$, of elements in X. If $\alpha = (a_1, a_2, \cdots, a_n)$, $\beta = (b_1, b_2, \cdots, b_m)$ are X-words, we let $\alpha^\#$ denote $(a_n^\#, \cdots, a_2^\#, a_1^\#)$ and let $\alpha \cdot \beta$ denote $(a_1, a_2, \cdots, a_n, b_1, b_2, \cdots, b_m)$. Since $(\alpha \cdot \beta)^\# = \beta^\# \cdot \alpha^\#$, the set of all X-words forms a monoid with involution. We let $D(X)$ denote the set of all X-words $\alpha = (x_1, x_2, \cdots, x_n)$ such that: either $n = 0$, or $n = 1$ and $x_1 = e$, or $n = 2$ and $x_2 = x_1^\#$, or $n = 3$ and $(x_1, x_2, x_3) \in \Delta_A$, or $n \geqq 4$ and $\exists a_2, \cdots, a_{n-2} \in A$ with $(x_1, x_2, a_2), (a_2^\#, x_3, a_3), \cdots, (a_{n-2}^\#, x_{n-1}, x_n) \in \Delta_A$. One easily checks the following:

(1) $(t_1, t_2, \cdots, t_n) \in D(T)$ implies $(t_2, \cdots, t_n, t_1) \in D(T)$,

(2) $\alpha \in D(T)$ implies $\alpha^\# \in D(T)$,

(3) $\alpha, \beta \in D(T)$ imply $\alpha \cdot \beta \in D(T)$,

(4) $(t_1, \cdots, t_n)$, $(s_1, \cdots, s_m) \in D(T)$ and $t_n = s_1^\#$ imply $(t_1, \cdots, t_{n-1}, s_2, \cdots, s_m) \in D(T)$,

(5) $t_1, t_2 \in T$ imply $(t_1, t_2) \in D(T)$ if and only if $t_2 = t_1^\#$, and

(6) for $t \in T$, $(t) \notin D(T)$.

We now broaden our point of view and start with a set T, a map $(\ )^\#$ from T to T, and a set $D(T)$ of T-words such that (1)-(6) above hold. We say a set J of T-words is *inversive* if $\alpha \cdot \beta^\# \in D(T)$ for all $\alpha, \beta \in J$. Such sets are inductively ordered by inclusion; we let B denote the set of all maximal inversive sets of T-words. We let

$$\Delta_B = \{(J, K, L) \in B^{3x} \mid \alpha \cdot \beta \cdot \gamma \in D(T) \text{ for all } \alpha \in J, \beta \in K, \gamma \in L\} .$$

For J an inversive set of T-words, we let $J^\#$ denote $\{\alpha^\# \mid \alpha \in J\}$ and $D(T): J$ denote the set of all T-words α such that $\alpha \cdot \beta \in D(T)$ for all $\beta \in J$. One checks $J \in B$ if and only if $D(T): J = J^\#$. With this one can check that $(B, \Delta_B, D(T))$ is a Pasch geometry. For $t \in T$ we let $f(t)$ denote $D(T): \{(t^\#)\}$. We let B^* denote $B \backslash \{e\}$ (where e is $D(T)$). One checks f is an injective map from T into B^*. In fact, one checks:

(a) for $t_1, \cdots, t_n \in T$, $(t_1, \cdots, t_n) \in D(T)$ if and only if $(f(t_1), \cdots, f(t_n)) \in D(B^*)$,

(b) for each $b \in B^*$, $\exists t_1, \cdots, t_n \in T$ with $(f(t_1), \cdots, f(t_n), b^\#) \in D(B^*)$,

(c) for $b_1, b_2, b_3 \in B^*$, $(b_1, b_2, b_3) \in \Delta_B$ if and only if for all $x_1, \cdots, x_n, y_1, \cdots, y_m, z_1, \cdots, z_r \in T$ with $(f(x_1), \cdots, f(x_n), b_1^\#)$, $(f(y_1), \cdots, f(y_m), b_2^\#)$, $(f(z_1, \cdots, f(z_r), b_3^\#))$ in $D(B^*)$, we have

$$(f(x_1), \cdots, f(x_n), f(y_1), \cdots, f(y_m), f(z_1), \cdots, f(z_r)) \in D(B^*) ,$$

and

(d) if K is any set of B^*-words such that $\alpha \cdot \beta^\# \in D(B^*)$ for all $\alpha, \beta \in K$, then $\exists b \in B$ with $\alpha \cdot (b^\#) \in D(B^*)$ for all $\alpha \in K$.

Moreover, (a)-(d) characterize B in the sense that if C is any geometry and g is a map from T to C such that (a)-(d) hold with B replaced by C and f replaced by g, then there exists a unique isomorphism h from C onto B with $f = h \circ g$. We call B the *word completion* of T.

Now let A be any abelian Pasch geometry. Let t be any element in A with $t \neq e$. Either $t = t^\#$ or $t \neq t^\#$; we consider these two cases separately.

First suppose $t = t^\#$. Let $r(t)$ be the smallest odd positive integer (if such exists) with $(t, t, \cdots, t) \in D(\{t\})$ (here $r(t)$ copies of t). If no such exists let $r(t) = \infty$. Using (1)-(6) above one checks the structure of $D(\{t\})$ is determined exactly by $r(t)$. If r is any odd positive integer with $3 \leqq r$, or $r = \infty$, we let T be any set with one element, say $T = \{1\}$, let $1^{\#} = 1$, let $D(T)$ be the set of all T-words $(1, 1, \cdots, 1)$ (n copies) where $n = 0$ or n is even or $n \geqq r$, check that (1)-(6) above hold, and let $B(r)$ denote the word completion of this T. We let $b(1)$ denote the natural image of 1 in $B(r)$, and using (a)-(d) get that $r(b(1)) = r$.

Now suppose $t \neq t^{\#}$. We let $k(t)$ be the smallest positive integer k (if such exists) such that there exists an integer $m \geqq 0$ with $(t, \cdots, t, t^{\#}, \cdots, t^{\#}) \in D(\{t, t^{\#}\})$ (here $k + m$ copies of t and m copies of $t^{\#}$). If no such k exists we let $k(t) = \infty$. If $k(t) \neq \infty$ and n is any integer, we use 1.-6. to check that there exists a smallest integer $m \geqq -1$ with $(t, \cdots, t, t^{\#}, \cdots, t^{\#}) \in D(\{t, t^{\#}\})$ (here $nk + m + 1$ copies of t and $m + 1$ copies of $t^{\#}$). We denote m by $h(n)$. With (1)-(6) above we check that h is a function from Z (the integers) to Z with:

(1) $h(0) = -1$,

(2) $-1 \leqq h(n)$, $\forall n \in Z$,

(3) $h(n_1 + n_2) \leqq h(n_1) + h(n_2) + 1 \forall n_1, n_2 \in Z$,

(4) $h(n_1 + n_2) \leqq h(n_1) + h(n_2) \forall n_1, n_2 \in Z$ with $h(n_1) \neq -1$ and $h(-n_2) \neq -1$, and

(5) $h(-n) = n \cdot k + h(n) \forall n \in Z$, for $k = h(-1) - h(1)$.

We call such a *semi-subadditive integer function*. One checks that h exactly determines the structure of $D(\{t, t^{\#}\})$. Conversely, we choose any convenient set with two elements, say $T = \{1, -1\}$. We let $1^{\#} = -1$, $(-1)^{\#} = 1$. If h is a semi-subadditive integer function we let $k = h(-1) - h(1)$, and let $D(T)$ be all permutations of T-words of the form $(1, \cdots, 1, -1, \cdots, -1)$ (here p copies of 1 and q copies of -1 where $\exists$ integer n with $p - q = nk$ and $h(n) + 1 \leqq q$). For the other case, if k is to be ∞, we let $D(T)$ be all permutations of $(1, \cdots, 1, -1, \cdots, -1)$ (p copies of 1, q of -1, where $p = q$). In both instances, one checks (1)-(6) hold. We denote the resulting word completions by $B(h)$ and $B(\infty, \infty)$ respectively.

We call r, ∞, h, or (∞, ∞), whichever corresponds to t, the *type* of t (for $t \neq e$). We let 1 be the type of e and let $B(1)$ denote the trivial group 1.

2. Double coset spaces for finite subgroups.

If H is a finite subgroup of a (not necessarily finite) group G, the set $G//H$ of double cosets has some extra number theoretic properties in addition to being a Pasch geometry. By a *probability group* (alias discrete convo, or hypergroup, see [5], [6], [8]), [11], we mean a pair (A, p) where A is a set and p is a map from $A^{3\infty}$ to the nonnegative reals, $(a, b, c) \mapsto p_c(a, b)$ (which we read as "the probability that $a \cdot b$ is c") such that:

(1) for $a, b \in A$, $p_c(a, b)$ is zero for all but finitely many c in A, and $\sum_c p_c(a, b) = 1$,

(2) for $a, b, c, d \in A$,

$$\sum_x p_x(a, b)p_d(x, c) = \sum_y p_d(a, y)p_y(b, c) ,$$

(3) there exists an $e \in A$ with $p_a(e, a) = 1 = p_a(a, e)$ for all $a \in A$,

(4) for each $a \in A$, there exists a unique $a^\# \in A$ with $p_e(a, a^\#) > 0$, and

(5) for $a, b, c \in A$,

$$p_c(a, b) = p_{c^\#}(b^\#, a^\#) .$$

Note that (2) is just associativity in the probabilistic sense (using the usual rule for composite probabilities) and (5) expresses that the inverse reverses multiplication. If (A, p) is a propability group, one checks that the identity e is unique, $e^\# = e$, and $(a^\#)^\# = a$ for all $a \in A$. We often denote (A, p) simply by A. We let Δ_A denote $\{(a, b, c) \in A^{3\infty} \mid p_{c^\#}(a, b) > 0\}$ (i.e., the set of all (a, b, c) such that "$a \cdot b \cdot c$ could be e"). On easily checks:

PROPOSITION 2.1. *If A is a probability group, then (A, Δ_A, e) is a Pasch geometry.*

If A is a probability group and $a \in A$ we note $p_e(a, a^\#) > 0$ and write $h_a(p)$ (or simply h_a) for $1/p_e(a, a^\#)$. If r is a positive integer, we say A is *r-integral* if $h_a^{1/r}$ and $p_c(a, b)h_a^{1/r}h_b^{1/r}/h_c^{1/r}$ are integers for all $a, b, c \in A$ (here $(\ )^{1/r}$ denotes as usual the unique nonnegative rth root). One can show that if A is finite and r-integral and $r \neq 1$, then A is 2-integral, so $r = 1$ and $r = 2$ are the two cases that interest us. We call A *abelian* if $p_c(a, b) = p_c(b, a)$ for all $a, b, c \in A$.

EXAMPLE 2.1. (see [6]), [3]. Let H be a finite subgroup of a group G. For $X, Y, Z \in G//H$ (the set of double cosets), let

$$p_Z(X, Y) = |xHy \cap Z|/|H|$$

where $x \in X$, $y \in Y$ (it is independent of this choice). We will check this makes $G//H$ into a probability group. The next lemma shows this probability group is 1-integral

LEMMA 2.1. *Let H be a finite subgroup of a group G. For $x, y, z \in G$,*

$$|HzH|/|H| = |H|/|H \cap zHz^{-1}| = h_{(HzH)}$$

which is an integer. Also

$$|xHy \cap HzH|\cdot|zHz^{-1} \cap H|/(|xHx^{-1} \cap H|\cdot|yHy^{-1} \cap H|)$$

is an integer.

Proof. Let f map H^{2x} onto HzH by $f((h_1, h_2)) = h_1^{-1}zh_2$. Let $zHz^{-1} \cap H$ operate on H^{2x} by $h\cdot(h_1, h_2) = (hh_1, z^{-1}hzh_2)$. Each orbit has $|zHz^{-1} \cap H|$ elements, and f induces a bijection from the set of orbits. This proves the first conclusion, since $H \cap zHz^{-1}$ is a subgroup of H. Now let $T = \{(h_1, h_2) \in H^{2x} | x^{-1}h_1^{-1}zh_2y^{-1} \in H\}$. One notes $T = f^{-1}(xHy \cap HzH)$ so

$$|T| = |zHz^{-1} \cap H|\cdot|xHy \cap HzH| .$$

Let the direct product of $(xHx^{-1} \cap H)$ and $(yHy^{-1} \cap H)$ operate on T by $(g_1, g_2)(h_1, h_2) = (h_1g_1^{-1}, h_2y^{-1}g_2^{-1}y)$ for $(h_1, h_2) \in T$. Each orbit has $|xHx^{-1} \cap H|\cdot|yHy^{-1} \cap H|$ elements, and since the number of orbits is an integer, the lemma is proved.

EXAMPLE 2.2 (see [6]). Let F be a finite group of automorphisms of a group G. For $X, Y, Z \in G/F$ (the set of orbits), let

$$p_Z(X, Y) = |\{(x, y) \in X \times Y | xy = z\}|\cdot|Z|/(|X|\cdot|Y|)$$

where $z \in Z$ (it is independent of this choice). We will check this makes G/F into a 1-integral probability group.

EXAMPLE 2.3 (see [5], [6], [11]). We say a probability group A is *sharp* if for each $a, b \in A \exists c \in A$ with $p_c(a, b) = 1$ (i.e., the underlying geometry is sharp). One defines $a\cdot b = c$, checks a group results, and so checks that a sharp probability group and a group are essentially the same concept.

EXAMPLE 2.4. Let $(P, \mathscr{L})$ be a finite projective space (see last section). Let m be a real number with $m > 2$ and such that every line has exactly $m + 1$ points on it (so if $\mathscr{L}$ is not empty m is an integer). Let $P^\# = P \cup \{e\}$, where e is some element not in P, and let $p_e(e, e) = 1 = p_a(e, a) = p_a(a, e)$ for all $a \in P$. Let $p_e(a, a) = 1/(m - 1)$ and $p_a(a, a) = (m - 2)/(m - 1)$ for all $a \in P$. For $a, b \in P$ with $a \neq b$ and for $c \in L_{a,b}$ (the line through a and b) with $c \neq a$ and $c \neq b$, let $p_c(a, b) = 1/(m - 1)$. For those $a, b, c \in P^\#$ for which

$p_c(a, b)$ has not yet been defined, let $p_c(a, b)$ be zero. A long tedius straightforward checking gives that this is an abelian probability group (integral when m is an integer).

EXAMPLE 2.5 (compare [9]). Let $\hat{G} = \{\chi_1, \cdots, \chi_s\}$ be the set of all irreducible characters of a finite group G. For $\chi \cdot \theta \in \hat{G}$, χ, θ can be decomposed $\chi \cdot \theta = \Sigma g_{\chi,\theta,\psi}\psi$ (the sum over all $\psi \in \hat{G}$) where the $g_{\chi,\theta,\psi}$ are nonnegative integers. Let

$$p_\psi(\chi, \theta) = \deg(\psi) g_{\chi,\theta,\psi}/(\deg(\theta) \cdot \deg,(\chi)) ,$$

where $\deg(\Gamma) = \Gamma(1)$ for each $\Gamma \in \hat{G}$. Using some elementary properties of characters one checks this is a 2-integral abelian probability group.

We will give more examples as we progress. By a *probability map* f from a set A to a set B we mean a map, $(a, b) \mapsto f_b(a)$ (which we read as "the probability that $f(a)$ is b"), from $A \times B$ to the nonnegative reals such that for each $a \in A$, $f_b(a)$ is zero for all but finitely many $b \in B$ and $\Sigma_b f_b(a) = 1$. If g is a probability map from B to a set C, we write $g \circ f$ for the probability map from A to C where $(g \circ f)_c(a) = \sum_b g_c(b) f_b(a)$ for all $c \in C$, $a \in A$. If for each $a \in A \exists b \in B$ with $f_b(a) = 1$, we write $f(a)$ for b, and call f *sharp*. We may view each ordinary map from A to B as being a sharp probability map. By a (probability) *morphism* from a probability group A to a probability group B we mean a probability map f from A to B such that:

(1) $f_e(e) = 1$,

(2) $f_{b^\#}(a^\#) = f_b(a)$ for all $a \in A$, $b \in B$, and

(3) there exists a real constant γ such that for all $a_1, a_2 \in A$ and $b \in B$

$$\sum_a p_a(a_1, a_2) f_b(a) \leqq \gamma(\sum_c \sum_d f_c(a_1) f_d(a_2) p_b(c, d))$$

(the sums over all $a \in A$, $c \in B$, $d \in B$ respectively).

Note (3) says "the probability that $f(a_1 \cdot a_2)$ is b is bounded by γ times the probability that $f(a_1) \cdot f(a_2)$ is b". We call a morphism f *strict* if equality holds in (3), (for some γ, which must then necessarily be 1). If f is both strict and sharp, we call it a *homomorphism*. If g is a morphism from B to a probability group C, one checks that $g \circ f$ is a morphism from A to C, and $g \circ f$ is strict (respectively sharp) if both g and f are strict (respectively sharp). Hence we have the category of probability groups (and the sharp and strict subcategories). If f is a morphism from a probability group A to a probability group B, we let Δ_f denote $\{(a, b) \in A \times B \mid f_b(a) > 0\}$ and check this is a (geometry) morphism from (A, Δ_A, e)

to (B, Δ_B, e) (sharp if f is sharp and strict if f is strict). This gives a natural functor from probability groups to Pasch geometries (which preserves being strict and also being sharp). If r is a positive integer and A and B are r-integral probability groups, we say a morphism f from A to B is *r-integral* if $h_a^{1/r}f_b(a)/h_b^{1/r}$ is an integer for all $a \in A$, $b \in B$. One checks these compose and give a category (which contains the category of groups as a full subcategory).

If X is any subset of a propability group A, we write $n(X)$ for $\sum_x h_x$ (the sum over all $x \in X$; recall $h_x = 1/p_e(x, x^\#)$) and call this the *order* of X; note it is finite if and only if $|X|$ is finite. Note always $|X| \leqq n(X)$. If A is r-integral (for some positive integer r) and A is finite, then each h_x is a positive integer so $n(X)$ is an integer. By a *subgeometry* of A we mean a subset S of A such that $e \in S$, and $p_c(s_1, s_2) > 0$, $s_1, s_2 \in S$, $c \in A$ imply $c^\# \in S$ (i.e., a subgeometry of (A, Δ_A, e)). Note any such is a probability group in its own right (by restricting p to S^{3x}). By the *complex group algebra* of A, we mean the vector space $\boldsymbol{C}(A)$ over $\boldsymbol{C}$ (the complexes) which has the elements of A as a basis and has multiplication defined by linearity and $a \cdot b = \sum p_c(a, b)c$ for all $a, b \in A$. One checks $\boldsymbol{C}(A)$ is an associative algebra with identity. We define aug: $\boldsymbol{C}(A) \rightarrow \boldsymbol{C}$ and $\sigma: \boldsymbol{C}(A) \rightarrow \boldsymbol{C}(A)$ by aug $(\sum \alpha_a a) = \sum \alpha_a$ and $\sigma(\sum \alpha_a a) = \sum \bar{\alpha}_a a^\#$. Here the α_a are complex numbers, and $\bar{\alpha}_a$ is the complex conjugate of α_a. One checks aug is an algebra homomorphism and σ is a semi-linear anti-isomorphism with $\sigma(\sigma(v)) = v$ for all $v \in \boldsymbol{C}(A)$. We define an inner product on $\boldsymbol{C}(A)$ by $(\sum \alpha_a a, \sum \beta_b b) = \sum \alpha_a \bar{\beta}_a p_e(a, a^\#)$, which one checks is linear in the 1st variable, and satisfies $\overline{(v_2, v_1)} = (v_1, v_2)$, $(v_1 \cdot v_2, v_3) = (v_1, v_3 \cdot \sigma(v_2))$ for all $v_1, v_2, v_3 \in \boldsymbol{C}(A)$. Also, if $v \neq 0$, $v \in \boldsymbol{C}(A)$, then $(v, v) > 0$ (where for $\alpha \in \boldsymbol{C}$, $\alpha > 0$ means α is real and $\alpha > 0$). If $h_a = h_{a^\#}$ for all $a \in A$ (which we will see is the case if A is finite or abelian), then one checks $(v_1 \cdot v_2, v_3) = (v_2, \sigma(v_1) \cdot v_3)$ and $(\sigma(v_1), \sigma(v_2)) = (v_1, v_2)$ for all $v_1, v_2, v_3 \in \boldsymbol{C}(A)$. If r is a positive integer and A is r-integral, by the *r-integral group ring* $Z[A]$ we mean the free Z-module over Z (the integers) which has a basis in bijective correspondence with A, $w_a \leftrightarrow a$, and which has multiplication defined by linearity and

$$w_a \cdot w_b = \sum_c (p_c(a, b) h_a^{1/r} h_b^{1/r} / h_c^{1/r}) w_c$$

for all $a, b \in A$. By taking $w_a = h_a^{1/r} a \in \boldsymbol{C}(A)$, for each $a \in A$, we can take this ring as a subring of $\boldsymbol{C}(A)$. Then σ (restricted to the subring) gives an involution of $Z[A]$, the inner product (also restricted to the subring) maps to Z, and aug (restricted to $Z[A]$) also maps to Z.

The first two conclusions of the next result are from [6].

PROPOSITION 2.2. *Let S be a finite subgeometry of a probability group A. Let $u_S = \sum_s (h_s/n(S))s \in \boldsymbol{C}(A)$ (the sum over all $s \in S$). Then $u_S^2 = u_S = \sigma(u_S)$ and for any $s \in S$, $h_s^\# = h_s$ and $s \cdot u_S = u_S \cdot s = u_S$. If for any $X, Y, Z \in A//S$, we let*

$$p_Z(X, Y) = \sum_s \sum_z \sum_a p_a(x, s)p_z(a, y)h_s/n(S)$$

where $x \in X, y \in Y$ (the sums over all $s \in S$, all $z \in Z$, and all $a \in A$), then this is independent of the choice of $x \in X$ and $y \in Y$ and makes $A//S$ into a probability group. $u_S \cdot \boldsymbol{C}(A) \cdot u_S$ is isomorphic to $\boldsymbol{C}(A//S)$ by $\sum \alpha_a a \leftrightarrow \sum \alpha_a [a]_S$. The natural map from A to $A//S$ is a sharp morphism. For each $Y \in A//S$, Y is finite and $n(S) \cdot h_Y = n(Y)$. If A is finite, then $n(S) \cdot n(A//S) = n(A)$.

Proof. Although the first two conclusions could be simply quoted, for the reader's convenience we outline a complete proof.

For $s, s_1, s_2 \in S \sum_a p_a(s_1, s)p_e(a, s_2^\#) = \sum_a p_e(s_1, a)p_a(s, s_2^\#)$ so $p_{s_2}(s_1, s)p_e(s_2, s_2^\#) = p_e(s_1, s_1^\#)p_{s_1^\#}(s, s_2^\#)$ so $p_{s_2}(s_1, s)h_{s_1} = p_{s_1^\#}(s, s_2^\#)h_{s_2}$ so

$$\begin{aligned} u_S \cdot s &= \sum_{s_1} \sum_{s_2} (h_{s_1}/n(S))p_{s_2}(s_1, s)s_{s_2} = \sum_{s_2} \sum_{s_1} (h_{s_2}/n(S))p_{s_1^\#}(s, s_2^\#)s_2 \\ &= \sum_{s_2} (h_{s_2}/n(S))s_2 = u_S \ . \end{aligned}$$

Also $\operatorname{aug}(u_S) = n(S)/n(S) = 1$. These two properties characterize u_S as an element in $\boldsymbol{C}(S)$, for if $v, w \in \boldsymbol{C}(S)$ with $\operatorname{aug}(v) = 1$, $\operatorname{aug}(w) = 1$, and $v \cdot s = v$, $w \cdot s = w$ for all $s \in S$, then $v \cdot \sigma(w) = v \operatorname{aug}(\sigma(w)) = v$ (since $\operatorname{aug}(\sigma(v)) = \operatorname{aug}(v) = 1$) and $w \cdot \sigma(v) = w \operatorname{aug}(\sigma(v)) = w$ so $v \cdot \sigma(w) = \sigma(\sigma(v)) \cdot \sigma(w) = \sigma(w \cdot \sigma(v)) = \sigma(w)$ and thus $v = \sigma(w)$. Applying this first with w for v we get $w = \sigma(w)$, and then applying it with a general v, we get $v = w$. Since $u_S = \sigma(u_S)$ (from letting w be u_S) we have $h_s = h_{s^\#}$ for each $s \in S$. For $s, s_1 \in S$, $\operatorname{aug}(s_1 \cdot u_S) = \operatorname{aug}(s_1) \cdot \operatorname{aug}(u_S) = 1$, and $(s_1 \cdot u_S) \cdot s = s_1 \cdot (u_S \cdot s) = s_1 \cdot u_S$ so $s_1 \cdot u_S = u_S$. Also $u_S \cdot u_S = u_S \operatorname{aug}(u_S) = u_S$.

We make $\operatorname{Hom}_C(\boldsymbol{C}(A), C)$ into a two sided $\boldsymbol{C}(A)$-module, by defining $(v_1 \cdot f \cdot v_2)(v_3)$ to be $f(v_2 \cdot v_3 \cdot v_1)$ for $v_1, v_2, v_3 \in \boldsymbol{C}(A)$ and $f \in \operatorname{Hom}_C(\boldsymbol{C}(A), C)$. Let u be u_S and let $h = u \cdot f \cdot u$ for some f in $\operatorname{Hom}_C(\boldsymbol{C}(A), C)$ with $f(x) \geqq 0$ for all $x \in A$. Then for $s_1, s_2 \in S$ and $a \in A$,

$$(s_1 \cdot h \cdot s_2)(a) = h(s_2 \cdot a \cdot s_1) = f(u \cdot s_2 \cdot a \cdot s_1 \cdot u) = f(u \cdot a \cdot u) = h(a) \ ,$$

so if we write $p_c(s_1, a, s_2)$ for $\sum_b p_c(s_1, b)p_b(a, s_2)$ we have $h(a) = \sum_c p_c(s_1, a, s_2)h(c)$. We also note that $c \in [a]_S$ if and only if $\exists s_1, s_2 \in S$ with $p_c(s_1, a, s_2) > 0$. Since S is finite this implies $[a]_S$ is finite. Note $h(c) \geqq 0$ for all $c \in A$, as is seen by expanding $h(c) = f(u \cdot c \cdot u)$ and using that f has this property. Choose $z \in [a]_S$ such that $h(z) \geqq h(c)$ for all $c \in [a]_S$. Then for $s_1, s_2 \in S$,

$$\sum_c p_c(s_1, z, s_2)(h(z) - h(c)) = h(z) - h(z) = 0$$

so for all c with $p_c(s_1, a, s_2) \neq 0$, $h(z) = h(c)$ (since all these numbers are nonnegative reals). Letting s_1 and s_2 vary over all possible elements in S, we have $h(z) = h(c)$ for all $c \in [a]_S$. Thus $f(u \cdot x \cdot u) = f(u \cdot c \cdot u)$ for all $x, c \in [a]_S$. For each $d \in A$ let f be f_d where f_d is defined by linearity and $f_d(y) = 1$ or 0 according as y is or is not d, for all $y \in A$. This gives $u \cdot x \cdot u = u \cdot c \cdot u$ for all $x, c \in [a]_S$. Thus for $X \in A//S$ we can unambiguously write $u \cdot X \cdot u$ for $u \cdot x \cdot u$ where $x \in X$. The set of all $u \cdot X \cdot u$ with $X \in A//S$ certainly generate $u \cdot \boldsymbol{C}(A) \cdot u$, and if $\sum \alpha_X u \cdot X \cdot u = 0$, taking (, d) gives $\alpha_Y = 0$ where $Y = [d]_S$. Thus this set is a basis of $u \cdot \boldsymbol{C}(A) \cdot u$. If $X, Y \in A//S$, one checks

$$u \cdot X \cdot u \cdot u \cdot Y \cdot u = \sum p_Z(X, Y) u \cdot Z \cdot u \ ,$$

where the sum is over all $Z \in A//S$. One now easily checks these $p_Z(X, Y)$ satisfy the axioms of a probability group (using the fact that $u \cdot \boldsymbol{C}(A) \cdot u$ is an associative ring closed under σ).

One checks the natural map from A to $A//S$ is a morphism with $n(S)$ for constant. Using (2) and (4) of the definition of a probability group, one checks $p_{c^\#}(a, b)h_a = p_{a^\#}(b, c)h_{c^\#}$. Let $Y \in A//S$. For $y_1 \in Y$, and $s, t \in S$, $p_a(x, s)p_t(a, y_1^\#) = 0$ unless $x \in Y$. Hence

$$\begin{aligned} p_S(Y, Y^\#)(\sum_y h_y) &= \sum_y p_S(Y, Y^\#)h_y \\ &= \sum_y \sum_s \sum_t \sum_{ap_a} (y, s)p_t(a, y_1^\#)h_s h_y/n(S) \ , \end{aligned}$$

where the first three sums are over all $y \in Y$, the next two are over all $s \in S$, $t \in S$, and the last is over all $a \in A$. This in turn is

$$\begin{aligned} &\sum_b \sum_s \sum_t \sum_a p_a(b, s)p_t(a, y_1^\#)h_s h_b/n(S) \\ &\quad = \sum_b \sum_s \sum_t \sum_a p_{b^\#}(s, a^\#)h_a p_t(a, y_1^\#)h_s/n(S) \\ &\quad = \sum_s \sum_t \sum_a h_a p_t(a, y_1^\#)h_s/n(S) \\ &\quad = \sum_s \sum_t \sum_a p_{a^\#}(y_1^\#, t^\#)h_t h_s/n(S) \\ &\quad = \sum_s \sum_t h_s h_t/n(S) = n(S)n(S)/n(S) = n(S) \ , \end{aligned}$$

where each s and t are summed through S, and each a and b are summed through A. This proves $n(S)h_Y = n(Y)$. If A is finite, summing over all Y gives the last result, and the proposition is proved.

The above proposition does not cover the obvious case in which A is sharp and S is normal but possibly infinite. For this we want the following generalization of A being finite. We say a probalility group A is of *discrete probability type* if for each $a \in A$ there is a finite set F_a of real numbers with $p_x(a, b) \in F_a$ for all $x, b \in A$. We call a subgeometry S of A *normal* if $p_s(a, b) > 0$, $s \in S$, $a, b \in A$ imply $p_t(b, a) > 0$ for some $t \in S$ (i.e., if S is normal in (A, Δ_A, e)).

PROPOSITION 2.3. *Let S be a normal subgeometry of a probability group A which is of discrete probabitity type. For $X, Y, Z \in A//S$, let $p_Z(X, Y) = \sum_z p_z(x, y)$ (the sum over all $z \in Z$), where $x \in X$, $y \in Y$. Then this is independent of the choice of $x \in X$ and $y \in Y$, and makes $A//S$ into a probability group of discrete probability type. The natural map f from A to $A//S$ is a (probability) homomorphism of A onto $A//S$. If S is finite, the notation of this and the last proposition agree. Let B be a probability group and let g be a (probability) homomorphism from A to B. Let $K_g = \{a \in A \mid g(a) = e\}$, and I_g be the image of g. Then I_g is a subgeometry of B, K_f is a normal subgeometry of A, f induces a (probability) isomorphism $\bar{f}$ from $A//K_f$ onto I_f, and f can be factored as $f = i \circ \bar{f} \circ j$ where $j\colon A \to A//K_f$ and $i\colon I_f \to B$ are the natural (probability) homomorphisms.*

Proof. Let $Y, Z \in A//S$, $a \in A$. For any $x \in A$ let $f(x) = \sum_z p_z(a, x)$ (the sum over all $z \in Z$). Extending f by linearity, we get it in $\mathrm{Hom}_C(\boldsymbol{C}(A), \boldsymbol{C})$. For $b \in A$, $s \in S$

$$f(b \cdot s) = \sum_c p_c(b, s) f(c) = \sum_c \sum_z p_c(b, s) p_z(a, c)$$
$$= \sum_z \sum_d p_d(a, b) p_z(d, s)$$

and since $p_z(d, s)$ is zero unless $d \in Z$ this is $\sum_z \sum_v p_v(a, b) p_z(v, s)$ (where v and z are summed over Z) and since $p_w(v, s)$ is zero unless $w \in Z$ this is

$$\sum_w \sum_v p_v(a, b) p_w(v, s) = \sum_v p_v(a, b) = f(b) .$$

Now choose $y_0 \in Y$ such that $f(y_0) = \max\{f(y) \mid y \in Y\}$. There are only finitely many finite sums of elements in F_a which are bounded by 1 (using A is of discrete probability type) so the above maximum exists. For $s \in S$ we now have

$$\sum_y p_y(y_0, s)(f(y_0) - f(y)) = \sum_w p_w(y_0, s)(f(y_0) - f(w))$$
$$= f(y_0) - f(y_0 \cdot s) = 0$$

so if $p_y(y_0, s) > 0$, $f(y_0) = f(y)$. Now for any $y \in Y \exists s_1, s_2 \in S$, $y_1 \in Y$ with $(y_0, s_1, y_1^\#)$, $(y_1, y^\#, s_2) \in \Delta_A$. Thus $f(y_0) = f(y_1)$ and $(s_2^\#, y, y_1^\#) \in \Delta_A$, so $\exists s_3 \in S$ with $(y, s_3, y_1^\#) \in \varDelta$ so $f(y) = f(y_1)$. Thus $f(y_0) = f(y)$. This proves the sum $\sum_z p_z(a, y)$ (over all $z \in Z$) is independent of the choice of $y \in Y$. Replacing Z by $Z^\#$and using $p_z(a, y) = p_{z^\#}(y^\#, a^\#)$ we get that if $a \in X \in A//S$, then $p_Z(X, Y)$ is well-defined. Now the rest of the proposition is easily checked.

For future use we give a slight strengthening of this last proposition. For f a strict morphism from a probability group A to a probability group B let K_f denote $\{a \in A \mid f_e(a) = 1\}$ and I_f denote $\{b \in B \mid \exists a \text{ with } f_b(a) > 0\}$. One checks K_f is a subgeometry of A and I_f is a subgeometry of B. Now assume A is finite and let j be the natural map from A to $A//K_f$, and let i be the natural map from K_f into B.

LEMMA 2.2. *Let the notation be as above. Then there exists a unique strict morphism g from $A//K_f$ to I_f with $i \circ g \circ j = f$.*

Proof. For $a_1, a_2 \in A$ write $a_1 L a_2$ (respectively $a_1 R a_2$) if $\exists s \in K_f$ with $(a_1, s, a_2^\#) \in \varDelta_A$ (respectively $(s, a_1, a_2^\#) \in \varDelta_A$). One checks these are both equivalence relations. For $b \in B$ and X an equivalence class for L choose $x_0 \in X$ with $f_b(x_0) = \max\{f_b(x) \mid x \in X\}$. For $s \in S$ one checks

$$\sum_x (f_b(x_0) - f_b(x)) p_x(x_0, s) = 0 .$$

Hence $x_0 L x$ implies $f_b(x_0) = f_b(x)$. Hence $x_1 L x_2$ implies $f_b(x_1) = f_b(x_2)$. Similarly we show $y_1 R y_2$ implies $f_b(y_1) = f_b(y_2)$. Now one checks that if $a_1, a_2 \in A$ with $[a_1] = [a_2]$ in $A//K_f$, then $\exists a_3$ with $a_1 L a_3$ and $a_3 R a_2$ so $f_b(a_1) = f_b(a_3) = f_b(a_2)$. We can define $g_b([a_1])$ to be $f_b(a_1)$, and have this is well-defined. A long straightforward check shows g is a strict morphism and proves the lemma.

Propositions 2.3 and 1.3 now immediately give:

PROPOSITION 2.4. *Let A be a probability group of discrete probability type. Let S be a subgeometry of A and T be a normal subgeometry of A. Then*

$$(S \cdot T)//T \cong S//(S \cap T) .$$

PROPOSITION 2.5 (*see* [6]). *Let S be a finite subgeometry of a probability group A. Let T be a finite subgeometry of A with $S \subseteqq T$. Then*

$$(A//S)//(T//S) \cong A//T .$$

Proof. By Proposition 2.2 $u_S \cdot C(A) \cdot u_S$ is isomorphic to $C(A//S)$

and $u_{(T//S)}\cdot C(A//S)\cdot u_{(T//S)}$ is isomorphic to $C((A//S)//(T//S))$. If φ is the first isomorphism, one checks $\varphi(u_T) = u_{(T//S)}$, so $u_T\cdot C(A)\cdot u_T = u_T\cdot u_S\cdot C(A)\cdot u_S\cdot u_T$ is isomorphic to $C((A//S)//(T//S))$. One checks the map is the natural map (the same one as in Proposition 1.4, which we now have preserves probabilities).

LEMMA 2.3. *Let B and C be subgeometries of a probability group A which is of discrete probability type. Let B' be a normal subgeometry of B and C' be a normal subgeometry of C. Then $B'\cdot(B\cap C')$ is a normal subgeometry of $B'\cdot(B\cap C)$, $C'\cdot(B'\cap C)$ is a normal subgeometry of $C'\cdot(B\cap C)$, and*

$$B'\cdot(B\cap C)//B'\cdot(B\cap C') \cong C'\cdot(B\cap C)//C'\cdot(B'\cap C)\ .$$

Proof. One checks $B\cap C$ is a subgeometry of C, so $C'\cdot(B\cap C)$ is a subgeometry of C. $(c', x, y)\in\Delta_A$, $c'\in C'$, $x, y\in C'\cdot(B\cap C)$ imply $x, y\in C$ so $\exists d'\in C'$ with $(d', y, x)\in\Delta_A$. Thus C' is a normal subgeometry of $C'\cdot(B\cap C)$ so

$$C'\cdot(B\cap C)//C' \cong B\cap C//C'\cap(B\cap C)$$

and $C'\cap(B\cap C) = C'\cap B$ is a normal subgeometry of $B\cap C$. Thus

$$C'\cdot(B\cap C)//C' \cong B\cap C//B\cap C'\ .$$

By interchanging B and C the above argument gives B' is a normal subgeometry of $B'\cdot(B\cap C)$, $B'\cap C$ is a normal subgeometry $B\cap C$ and

$$B'\cdot(B\cap C)//B' \cong B\cap C//B'\cap C\ .$$

Thus $D = (B\cap C')\cdot(B'\cap C)$ is a subgeometry of $B\cap C$. Let $(d, x, y)\in\Delta_A$, $d\in D$, $x, y\in B\cap C$. There exists $d_1\in B\cap C'$, $d_2\in B'\cap C$ with $(d_1, d_2, d)\in\Delta_A$. By an argument using Pasch's axiom one gets there is a $w\in B\cap C$ with $(d_1^\#, x, w^\#)$, $(d_2^\#, w, y)\in\Delta_A$. Thus there exist $d_3^\#\in B\cap C'$, $d_4^\#\in B'\cap C$ with $(d_3^\#, w^\#, x)$, $(d_4^\#, y, w)\in\Delta_A$ so (y, x, d_0), $(d_0^\#, d_3^\#, d_4^\#)\in\Delta_A$ so $(d_4, d_3, d_0)\in\Delta_A$. Thus $(d_5, d_0, d_3)\in\Delta_A$ where $d_5\in B'\cap C$. Thus $(d_3, d_5, d_0)\in\Delta_A$ so $d_0\in D$. This proves D is a normal subgeometry of $B\cap C$.

Define a map f from $C'\cdot(B\cap C)$ to $B\cap C//D$ as follows: for $(c', b, x)\in\Delta_A$, $c'\in C'$, $b\in B\cap C$, let $f(x)$ be $[b^\#]_D$. One checks this is well-defined. One checks f is a surjective (probability) homomorphism with

$$K_f = C'\cdot(D\cap(B\cap C)) = C'\cdot(B'\cap C)\ .$$

First applying Proposition 2.3, and then interchanging B and C gives

$$C'\cdot(B \cap C)//C'\cdot(B' \cap C) \cong B \cap C//D \cong B'\cdot(B \cap C)//B'\cdot(B \cap C') .$$

The lemma is proved.

We call a probability group A *simple* if it has exactly two normal subgeometries (A and $\{e\}$). A finite probability group A will have a chain of subgeometries

$$A = A_0 \supseteqq A_1 \supseteqq \cdots \supseteqq A_n = \{e\}$$

such that A_{i+1} is a normal subgeometry of A_i, and $A_i//A_{i+1}$ is simple for $i=0, \cdots, n-1$. We call n the *length* of A and call $\{A_i//A_{i+1} | i= 0, \cdots, n-1\}$ the sequence of simple *composition factors*; using the lemma and the usual argument, one gets the length is well-defined and the sequence of composition factors is unique as an unordered sequence. The above proof is complicated by the fact that an intersection of normal subgeometries apparently need not be normal.

Let A, B be probability groups. We define

$$p_{(a_1,b_1)}((a_2, b_2), (a_3, b_3)) = p_{a_1}(a_2, a_3)p_{b_1}(b_2, b_3)$$

and check that this makes $A \times B$ into a probability group (see [6]). For notation we let Shp (respectively Stp) denote the category of all probability groups with sharp (probability) morphisms (respectively with strict probability morphisms). One checks the natural map from $A \times B$ to A (and also the one to B) is in Shp and the one from A to $A \times B$ (and also the one from B to $A \times B$) is in Stp.

PROPOSITION 2.6. *For A, B, C probability groups, we have a natural identification*

$$\mathrm{Shp}\,(C, A \times B) \longleftrightarrow \mathrm{Shp}\,(C, A) \times \mathrm{Shp}\,(C, B) \quad (h \longleftrightarrow (p_A \circ h, p_B \circ h))$$

and if in addition C is abelian, we have another natural identification

$$\mathrm{Stp}\,(A \times B, C) \longleftrightarrow \mathrm{Stp}\,(A, C) \times \mathrm{Stp}\,(B, C) \quad (h \longleftrightarrow (h \circ in_A, h \circ in_B)) .$$

Proof. The first part is easily checked. Let C be abelian. For $f \in \mathrm{Stp}\,(A, C)$, $g \in \mathrm{Stp}\,(B, C)$, define h by

$$h_c((a, b)) = \sum_{c_1} \sum_{c_2} f_{c_1}(a) g_{c_2}(b) p_c(c_1, c_2)$$

for all $c \in C$, $a \in A$, $b \in B$ (here the sums are over all $c_1, c_2 \in C$). One checks $h \in \mathrm{Stp}\,(A \times B, C)$ and $h \circ in_A = f$ and $h \circ in_B = g$. The rest of the proposition is easily checked.

Let G be a group (for simplicity; one can do what follows for G an arbitrary probability group much as was outlined in the last section). By a *G-probability group* we mean a probability group A together with a group homomorphism, $\alpha \mapsto f_\alpha$, of G into the group of (probability) isomorphisms of A to itself, such that for each $a \in A$, $\{f_\alpha(a) \mid \alpha \in G\}$ is finite. We usually write $\alpha(a)$ for $f_\alpha(a)$. Let A and B be G-probability groups. By a G-morphism from A to B we mean a morphism f from A to B such that $f_{\alpha(b)}(\alpha(a)) = f_b(a)$ for all $a \in A$, $b \in B$, $\alpha \in G$. One checks these compose so we have the category of G-probability groups. One checks $A \times B$ is made into a G-probability group by defining $\alpha((a, b)) = (\alpha(a), \alpha(b))$ for all $\alpha \in G$, $(a, b) \in A \times B$. If A is a G-probability group, we note (A, Δ_A, e) is a G-geometry. By a G-subgeometry of A we mean a subgeometry S of A such that $\alpha(s) \in S$ for all $s \in S$, $\alpha \in G$. Such is clearly a G-probability group in its own right. One can check that all the previous propositions of this section hold with "probability group", "morphism", and "subgeometry" prefixed everywhere they appear by "G-".

Let H be a subgroup of the group G. Let A be a G-probability group. Then A is naturally an H-probability group (by restricting the operation to H). In particular, $A/H = \{\langle a\rangle_H \mid a \in A\}$ is a set of finite subsets of A (here $\langle a\rangle_H = \{\alpha(a) \mid \alpha \in H\}$). For $X, Y, Z \in A/H$ let

$$p_Z(X, Y) = \sum_{x \in X} \sum_{y \in Y} p_Z(x, y) |Z| / (|X| \cdot |Y|) ,$$

where $z \in Z$.

PROPOSITION 2.7. *Let H be a subgroup of a group G. Let A be a G-probability group. Then the $p_Z(X, Y)$ defined above is well-defined and makes A/H into a probability group. For each $X \in A//H$, $h_X = n(X) = h_x|X|$, for any $x \in X$. If A is finite, then $n(A/H) = n(A)$. If H is normal (a restriction only for simplicity), then A/H is a $G//H$-probability group. Also $(A/H)/(G//H) \cong A/G$. In any case, if $|X|$ is bounded for $X \in A/H$ then the natural map from A to A/H is a sharp morphism.*

Proof. If we extend by linearity H operates on $C(A)$ by ring automorphisms. We let $C(A)^H$ denote the subring of all elements left element-wise fixed by each $\alpha \in H$. For each $X \in A/H$ let $v_X = (\sum x)/|X|$ (the sum over all $x \in X$). One checks the v_X, for $X \in A/H$, are a basis of $C(A)^H$ and $v_X \cdot v_Y = \sum_Z p_Z(X, Y) v_Z$ for all $X, Y \in A/H$. With this one easily checks the proposition. If H is normal, the operation of $G//H$ on A/H is given by $(\alpha \cdot H)(\langle x\rangle_H) = \langle \alpha(x)\rangle_H$ for all $\alpha \in G$, $x \in A$. The rest can be checked.

COMMENT 2.1. Let A be an H-probability group as in the last proposition. For $X \in A/H$, $a \in A$, let $f_a(X)$ be $1/|X|$ if $a \in X$ and be zero otherwise. Then f is a strict morphism from A/H to A. If A is 1-integral one can check A/H is also 1-integral and f is 1-integral. If g is the natural map from A to A/H, then $g \circ f$ is the identity map.

PROPOSITION 2.8. *Let H be a group. Let A be an H-probability group. Let S be a finite H-subgeometry of A. Then the natural map between $(A//S)/H$ and $(A/H)//(S/H)$ (see Proposition 1.11) is a probability isomorphism.*

Proof. Using the notation of the last proof, let φ be the isomorphism spoken of there from $C(A/H)$ to $C(A)^H$. One checks that $\varphi(u_{(s/H)}) = u_S$. Thus φ maps $u_{(S/H)} \cdot C(A/H) \cdot u_{(S/H)}$ isomorphically onto $u_S \cdot C(A)^H \cdot u_S$. One checks that $u_S \cdot C(A)^H \cdot u_S = (u_S \cdot C(A) \cdot u_S)^H$. Using that $u_S \cdot C(A) \cdot u_S$ is isomorphic to $C(A//S)$, one can combine these isomorphisms and check that the proposition is true.

Let G be a group. For A a G-probability group, one checks $A \times G$ with

$$p_{(c,\gamma)}((a, \alpha), (b, \beta)) = p_c(a, \alpha(b)) p_\gamma(\alpha, \beta)$$

is a probability group; we denote it by $A \underline{\times} G$. $A \times \{1\}$ is a normal subgeometry and $\{e\} \times G$ is a subgeometry, of $A \times G$ and if G is finite, $A \times G//\{e\} \times G \cong A/G$. If $f: A \to E$ is a G-morphism to another G-probability group E, one checks $f_{(a,\alpha)}((b, \beta)) = f_a(b)\delta_{\alpha,\beta}$ (Kronecker delta) is a morphism from $A \underline{\times} G$ to $E \underline{\times} G$. Conversely, if C is a normal subgeometry of a probability group B and D is a finite subgeometry of B with D sharp, $C \cdot D = B$, and $C \cap D = \{e\}$, then C is a D-probability group in a natural way and $B \cong C \underline{\times} D$.

For S and A G-probability groups we call a G-homomorphism $f: S \to A$ *central* if $p_x(f(s), a) = p_x(a, f(s))$ for all $s \in S$, $a, x \in A$ (note if A is abelian this is certainly the case).

We use the customary term of G-module for an abelian G-group (i.e., abelian sharp G-probability group). Let S be a G-group (so not necessarily abelian). By an *S-G-probability group* we mean a pair (f_A, A) where A is a G-probability group and f_A is a strict G-morphism from S to A. One checks then f_A must be a G-homomorphism. We often denote (f_A, A) simply by A. Let A and B be S-G-probability groups. By an S-G-morphism from A to B we mean a G-morphism g from A to B with $g \circ f_A = f_B$. We let $\mathrm{Shp}_{S\text{-}G}(A, B)$ (respectively $\mathrm{Stp}_{S\text{-}G}(A, B)$) denote the set of all S-G-morphisms which are in $\mathrm{Shp}(A, B)$ (respectively $\mathrm{Stp}(A, B)$). By Proposition 2.6, there is a unique sharp G-morphism f from S to

$A \times B$ with $p_A \circ f = f_A$ and $p_B \circ f = f_B$ (simply $f(s) = (f_A(s), f_B(s))$. One checks (using S as a group) that f is strict, and so makes $A \times B$ into an S-G-probability group. We denote f by $f_A \times f_B$. By Proposition 2.3 the image I of $f_A \times f_B$ is a G-subgeometry of $A \times B$. In general, we cannot make $A \times B//I$ into an S-G-probability group, but when S is abelian, both A and B are of finite probability type, and both f_A and f_B are central we proceed as follows. S an abelian group implies $s \rightarrow s^{-1}$ is a G-isomorphism (thus strict), so if $f_B^{\#}(s) = f_B(s^{-1})$ for all $s \in S$, $f_B^{\#}$ is a strict G-morphism (actually a G-homomorphism) and makes B into an S-G-probability group. We let I be the image of $f_A \times f_B^{\#}$, note I is a normal G-subgeometry of $A \times B$ (using Proposition 2.3 and that both f_A and f_B are central), check that $A \times B$ is of finite probability type, and let $A \boldsymbol{\times}_S B$ denote the G-probability group $A \times B//I$ (which exists by Proposition 2.3). By Proposition 2.3 the natural map $g\colon A \times B \rightarrow A \boldsymbol{\times}_S B$ is a G-homomorphism (so strict). Letting $1_B(s) = e \forall s \in S$ we check that 1_B is a strict G-morphism and that $f_A \times 1_B$ is strict, and use $g \circ (f_A \times 1_B)$ (i.e., $s \mapsto [(f_A(s), e)]_I$) to give $A \boldsymbol{\times}_S B$ the structure of an S-G-probability group. One checks $g \circ (f_A \times 1_B) = g \circ (1_A \times f_B)$.

PROPOSITION 2.9. *Let G be a group and S be a G-group. Let A, B, C, be S-G-probability groups. Then we have a natural identification*

$$\mathrm{Shp}_{S-G}(C, A \times B) \longleftrightarrow \mathrm{Shp}_{S-G}(C, A) \times \mathrm{Shp}_{S-G}(C, B) \quad (h \longleftrightarrow (p_A \circ h, p_B \circ h))$$

and if in addition C is abelian, S is abelian, A and B are of finite probability type, and f_A, f_B are central, we have another natural identification

$$\begin{gathered}\mathrm{Stp}_{S-G}(A \boldsymbol{\times}_S B, C) \longleftrightarrow \mathrm{Stp}_{S-G}(A, C) \times \mathrm{Stp}_{S-G}(B, C) \\ (h \longleftrightarrow (h \circ g \circ in_A, h \circ g \circ in_B)) \;.\end{gathered}$$

Proof. The first part is easily checked (using Proposition 2.6), so we make the assumptions for the second part. This part follows easily from three lemmas. Now f_A and f_B induce algebra homomorphisms (which we denote by the same names) $f_A\colon C(\mathrm{S}) \rightarrow C(A)$ and $f_B\colon C(S) \rightarrow C(B)$. Since f_A and f_B are central, these make both $C(A)$ and $C(B)$ into $C(S)$-algebras, and similarly $C(A \boldsymbol{\times}_S B)$ is a $C(S)$-algebra. Each of $f_A, f_B, f_A \times f_B$ is a G-homomorphism, so by Proposition 2.3 its image (which is isomorphic to a factor group of S) is a subgroup and the next lemma applies.

LEMMA 2.4. *Let T be a sharp subgeometry (i.e., a subgroup) of a Pasch geometry D. Then for $t \in T, d \in D \exists$ unique $x \in D$ with*

$(d, t, x^{\#}) \in \Delta_D$. *We denote* x *by* $d \cdot t$ ($t \cdot d$ *is defined similarly*).

Proof. Let $(d, t, x^{\#})$, $(d, t, y^{\#}) \in \Delta_D$. Then $\exists w \in D$ with $(w, t^{\#}, t)$, $(w, y^{\#}, x) \in \Delta_D$. Thus $w = e$ so $y = x$.

LEMMA 2.5. $C(A \times_S B) \cong C(A) \otimes_{C(S)} C(B)$ *as* $C(S)$*-algebras, by linearity and* $[(a, b)]_I \leftrightarrow a \otimes b$.

Proof. $C(A) \otimes_{C(S)} C(B)$ is $C(A) \otimes_C C(B)/W$, where W is the subspace spanned by all

$$(a \cdot f_A(s)) \otimes b - a \otimes (f_B(s) \cdot b), \text{ where } a \in A, b \in B, s \in S .$$

Each such term may be written (using f_A is central, S is a group, and letting c be $f_B(s) \cdot b$)

$$(f_A(s) \otimes f_B^{\#}(s) - e \otimes e) \cdot (a \otimes c), \text{ where } a \in A, c \in B, s \in S .$$

Using that I is normal one checks for $a_1, a_2 \in A$, $b_1, b_2 \in B$ that $[(a_1, b_1)]_I = [(a_2, b_2)]_I$ if and only if $\exists s \in S$ with $(f_A(s) \otimes f_B^{\#}(s)) \cdot (a_1 \otimes b_1) = (a_2 \otimes b_2)$. Thus if we extend the map $[(a_1, b_1)]_I \mapsto a_1 \otimes b_1 + W$ by linearity we get a well-defined C-homomorphism which one can check is bijective and preserves multiplication and also multiplication by elements in $C(S)$.

LEMMA 2.6. *Let* D, H *be probability groups. Then* Stp (D, H) *is in bijective correspondence with the set of all algebra homomorphisms* f *from* $C(D)$ *to* $C(H)$ *such that* $f \circ \sigma = \sigma \circ f$ *and* $f(P(D)) \subseteq P(H)$ (*where* $P(\ )$ *is the set of linear combinations with nonnegative coefficients which add to* 1).

Proof. Letting $f \in \text{Stp}(D, H)$ correspond to the linear map which takes $d \in D$ to $\sum f_h(d)h$, this is easily checked. Now the proof of Proposition 2.9 is easily concluded using usual properties of the tensor product.

Now let A be a finite probability group. The group ring $C(A)$ is semi-simple (for if J is the radical, $J^{m+1} = 0$, $J^m \neq 0$, $v \in J^m$, then $\sigma(v) \in J^m$ so $v \cdot \sigma(v) = 0$ so $0 = (v \cdot \sigma(v), e) = (v, v)$ so $v = 0$). Thus the Wedderburn theorems give that $C(A)$ is a direct sum of complex full matrix rings. Now suppose A is abelian. Let $\hat{A}$ denote the set of all maps f from A to C such that $f(e) = 1$, and

$$\sum_{a \in A} p_a(b, c) f(a) = f(b) f(c)$$

for all $b, c \in A$. Since these correspond to the algebra homomorphisms from $C(A)$ to C, they are a basis of the algebra Map (A, C) of all maps from A to C with component-wise addition and multiplication. Hence there exist uniquely defined complex numbers $\hat{p}_\theta(\chi, \psi)$, $\theta, \chi, \psi \in \hat{A}$ with

$$\chi \cdot \psi = \sum_\theta \hat{p}_\theta(\chi, \psi)\theta \text{ , for all } \chi, \psi \in \hat{A} \text{ .}$$

We call A (in the spirit of [5], [6], [11]—they consider more than the finite case) *dualizable* if $\hat{p}_\theta(\chi, \psi)$ is a nonnegative real for all $\theta, \chi, \psi \in \hat{A}$. If this is the case, one can check then $(\hat{A}, \hat{p})$ is an abelian probability group (which is dualizable) and if $(\hat{A}, \hat{p}) = (B, q)$ then $(\hat{B}, \hat{q}) \cong (A, p)$. If G is a finite group and F is the set of inner automorphisms of G, then G/F is an abelian probability group (Example 2.2) which is dualizable with dual $\hat{G}$ (Example 2.5). If $(P, \mathscr{L})$ is a finite projective space, then $(P^\#, p)$ is an abelian probability group (Example 2.4) which is dualizable with dual coming from the projective space which has hyperspaces for points, and hyperspaces containing a subspace of codimension two for lines (i.e., the usual dual). If A is $G//H$ for G a finite group, A is dualizable ([10]). Even when A is not dualizable we have the following:

PROPOSITION 2.10. *Let A be a finite abelian probability group. Let $\chi \in \hat{A}$. Then $\chi(a^\#) = \overline{\chi(a)}$ for all $a \in A$. Define $\chi^\#$ by $\chi^\#(a) = \chi(a^\#) = \overline{\chi(a)}$ for each $a \in A$. Then $\chi^\# \in \hat{A}$ and* aug $\in \hat{A}$ *(where* aug $(a) =$ 1 *for all $a \in A$). Also $\hat{p}_{\text{aug}}(\chi, \chi^\#)$ is a positive real number. We denote its reciprocal by h_χ and we let $n(\hat{A})$ denote $\sum h_\chi$ (the sum over all $\chi \in \hat{A}$). Then $n(\hat{A}) = n(A)$, and using the Kronecker delta, we have for any $\chi, \psi \in \hat{A}$, $b, c \in A$*

$$\sum_a h_a h_\psi \chi(a)\overline{\psi(a)} = n(A)\delta_{\chi,\psi} \text{ (the sum over } a \in A\text{), and}$$

$$\sum_\chi h_\chi h_b \chi(a)\overline{\chi(b)} = n(A)\delta_{a,b} \text{ (the sum over } \chi \in \hat{A}\text{) .}$$

Proof. Let n_χ denote $\sum_a |\chi(a)|^2 h_a$, which is certainly a positive real number. Let v denote $\sum \chi(a^\#)h_a a \in C(A)$. For any $b \in A$, by direct computation (together with (2) and (4) of the definition of a probability group) $v \cdot b = v\chi(b)$, $v \neq 0$, and $v^2 = kv$ where $k = \sum \chi(a^\#)\chi(a)h_a$. $k \neq 0$ since $C(A)$ is semi-simple. Let u_χ (or u) denote $k^{-1}v$. Then $u \neq 0$, $u^2 = u$, and $u \cdot b = u\chi(b) \forall b \in A$. One checks directly that any element in $C(A)$ with these properties must be u. Now let χ^0 be defined by $\chi^0(a) = \overline{\chi(a^\#)}$ for all $a \in A$. One checks $\chi^0 \in \hat{A}$. Taking $\sigma(\ )$ of $u \cdot b = u\chi(b)$ gives $b^\# \cdot \sigma(u) = \overline{\chi(b)}\sigma(u)$, so $\sigma(u_\chi) = u_{\chi^0}$. But $0 < (u_\chi, u_\chi) = (u_\chi \cdot \sigma(u_\chi), e)$ so $u_\chi \cdot u_{\chi^0} \neq 0$. But for each $b \in A$, $u_\chi \cdot u_{\chi^0} \cdot b = u_\chi \cdot u_{\chi^0}\chi^0(b)$ and $u_\chi \cdot u_{\chi^0}$ is an idempotent, so $u_\chi \cdot u_{\chi^0} = u_{\chi^0}$. Similarly, $u_{\chi^0} \cdot u_\chi = u_\chi$. Since $u_\chi \cdot u_{\chi^0} = u_{\chi^0} \cdot u_\chi$, we have $u_{\chi^0} = u_\chi$.

Multiplying this by any $a \in A$, gives $\chi^0(a) = \chi(a)$, and thus $\chi(a^\#) = \overline{\chi(a)}$. Substituting above, we get $n_\chi = k$. One checks $\chi^\#$ and aug are in $\hat{A}$. Extending χ by linearity gives an algebra homomorphism from $C(A)$ to C. Now let $\psi \in \hat{A}$. For $a \in A$, $u_\psi \cdot a = u_\psi \psi(a)$ so $\chi(u_\psi)\chi(a) = \chi(u_\psi)\psi(a)$, so if $\chi \neq \psi$, choosing a appropriately we get $\chi(u_\psi) = 0$, while if $\chi = \psi$, $\chi(u_\chi) = \sum \chi(a^\#)h_a\chi(a)/n_\chi = 1$. Thus $\chi(u_\psi) = \delta_{\chi,\psi}$. In particular, $\chi(u_{\text{aug}}) = \delta_{\chi,\text{aug}}$. But $u_{\text{aug}} = \sum (h_a/n(A))a$ so $\sum (h_a/n(A))\chi(a) = \delta_{\chi,\text{aug}}$. Thus

$$\begin{aligned}\hat{p}_{\text{aug}}(\chi, \psi^\#) &= \sum_\theta \hat{p}_\theta(\chi, \psi^\#)\delta_{\theta,\text{aug}} = \sum_\theta \sum_a \hat{p}_\theta(\chi, \psi^\#)h_a\theta(a)/n(A) \\ &= \sum_a (h_a/n(A))\chi(a)\psi^\#(a) = \chi(\sum_a (h_a/n(A))\psi(a^\#)a) \\ &= (n_\psi/n(A))\chi(u_\psi) = (n_\psi/n(A))\delta_{\chi,\psi} .\end{aligned}$$

Since both n_ψ and $n(A)$ are positive real numbers, we have $\hat{p}_{\text{aug}}(\chi, \psi^\#)$ is nonzero if and only if $\chi = \psi$. Also $h_\chi = n(A)/n_\chi$. Plugging this in $\chi(u_\psi) = \delta_{\chi,\psi}$ gives

$$\sum_a h_a h_\psi \chi(a)\overline{\psi(a)} = n(A)\delta_{\chi,\psi} .$$

This can be written as that the product of two appropriate matrices is the identity. Hence their product in the other order is the identity, so

$$\sum_\chi h_\chi h_b \chi(a)\overline{\chi(b)} = n(A)\delta_{a,b} .$$

Letting $a = b = e$, we get $n(\hat{A}) = n(A)$.

PROPOSITION 2.11. *Let A be a finite dualizable abelian probability group. Let S be subgeometry of A. Let $S^\perp = \{\chi \in \hat{A} \mid \chi(s) = 1\ \forall s \in S\}$. Then $S^\perp$ is a subgeometry of $\hat{A}$, both $A//S$ and S are dualizable and*

$$\widehat{(A//S)} \cong S^\perp , \quad \hat{S} \cong \hat{A}//S^\perp .$$

Also $S \mapsto S^\perp$ is an order inverting bijection between the set of all subgeometries of A and set of all subgeometries of $\hat{A}$. Also $n(S^\perp) = n(A)/n(S)$ and $(S^\perp)^\perp = S$.

Proof. First one checks that the restriction to S (which we denote by φ) satisfies the rules that would make it a homomorphism if $\hat{S}$ is a probability group. In particular $\sum \hat{p}_\theta(\chi, \psi^\#)$ (the sum over all $\theta \in S^\perp$) is zero if $\varphi(\chi) \neq \varphi(\psi)$ and is nonzero otherwise for $\chi, \psi \in \hat{A}$. Hence if $(\theta, \chi, \psi) \in \Delta$ with $\theta, \chi \in S^\perp$, then $(\chi, \psi, \theta) \in \Delta$ so $\hat{p}_{\theta^\#}(\chi, \psi) > 0$ so $\varphi(\psi) = \varphi(\chi^\#)$ so $\psi \in S^\perp$. This proves $S^\perp$ is a subgeometry of $\hat{A}$.

For $\chi \in S^{\perp}$, we extend χ by linearity and note $\chi(u_S) = \sum_s (h_s/n(S))\chi(s) = 1$. Thus if $a, b \in A$ with $u_S \cdot a \cdot u_S = u_S \cdot b \cdot u_S$, then $\chi(a) = \chi(b)$. Since $u_S \cdot C(A) \cdot u_S \cong C(A//S)$, we have a well-defined map from $S^{\perp}$ to $\widehat{(A//S)}$ which is a bijection and preserves the probabilities. Since $S^{\perp}$ is a probability group, $A//S$ is dualizable. We also have $n(S^{\perp}) = n(A)/n(S)$, since from the last proposition $n\widehat{(A//S)} = n(A//S) = n(A)/n(S)$.

Now one checks that φ induces a bijection from $\hat{A}//S^{\perp}$ onto a subset I of $\hat{S}$, and this bijection preserves probabilities. Thus

$$n(I) = n(\hat{A}//S^{\perp}) = n(\hat{A})/n(S^{\perp}) = n(A)/(n(A)/n(S)) = n(S) = n(\hat{S}) .$$

Since $n(I) = n(\hat{S})$ we must have $I = \hat{S}$, so S is dualizable and $\hat{A}//S^{\perp} \cong \hat{S}$.

We now have

$$n(S) = n(\hat{A}//S^{\perp}) = n(\hat{A})/n(S^{\perp}) = n(A)/n(S^{\perp})$$

and replacing S by $S^{\perp}$ we have $n(S^{\perp}) = n(\hat{A})/n(S^{\perp\perp})$ so $n(S) = n(A)/(n(\hat{A})/n(S^{\perp\perp})) = n(S^{\perp\perp})$. Since $S \subseteqq S^{\perp\perp}$ the proposition is proved.

PROPOSITION 2.12. *Let H be a finite group and A be a finite abelian dualizable H-probability group. For $\alpha \in H$, $\chi \in \hat{A}$, define $\alpha(\chi) \in \hat{A}$ by $(\alpha(\chi))(a) = \chi(\alpha^{\#}(a))$ for all $a \in A$. This makes $\hat{A}$ into an H-probability group. Also A/H is dualizable and*

$$\widehat{(A/H)} \cong \hat{A}/H .$$

Proof. It is straightforward to check $\hat{A}$ is an. H-probability group. Every idempotent in $C(A)$ is some sum of the minimal nonzero idempotents u_χ, $\chi \in \hat{A}$ (see proof of Proposition 2.10). But $C(A/H) \cong C(A)^H$ (see proof of Proposition 2.7). Now one checks that for $\alpha \in H$, $\alpha(u_\chi) = u_{\alpha(\chi)}$, and if for $X \in \hat{A}/H$, u_X denotes $\sum u_\chi$ (the sum over all $\chi \in X$), then the u_X, $X \in \hat{A}/H$, are exactly the minimal nonzero idempotents of $C(A)^H$. For $X \in \hat{A}/H$ and $Y \in A/H$ we let $\varphi_X(Y)$ denote $\sum_y \chi_0(y)/|Y| = \sum_\chi \chi(y_0)/|X|$ for $\chi_0 \in X$, $y_0 \in Y$ (the first sum over all $y \in Y$ and the second over all $\chi \in X$). One checks $\varphi_X(Y)$ is independent of the chice of $\chi_0 \in X$, $y_0 \in Y$, and

$$u_X \cdot (\sum_y y/|Y|) = \varphi_X(Y) u_X .$$

This means $X \mapsto \varphi_X(\ )$ is a bijection from $\hat{A}/H$ onto $\widehat{(A/H)}$. But $\hat{A}/H$ is a probability group (Proposition 2.7) and one checks

$$\varphi_X(Y) \cdot \varphi_W(Y) = \sum \hat{p}_Z(X_1, X_2)\varphi_Z(Y)$$

(here X, $W \in \hat{A}/H$, $Y \in A/H$, the sum is over all $Z \in \hat{A}/H$, and $\hat{p}$ is defined as in Proposition 2.7 with A replaced by $\hat{A}$). The proposition is proved.

PROPOSITION 2.13. *Let A and B be finite abelian dualizable probability groups. For $(b, a) \mapsto f_b(a)$ a map from $B \times A$ to $\boldsymbol{C}$, let $(\chi, \theta) \mapsto \hat{f}_\chi(\theta)$ be the map from $\hat{A} \times \hat{B}$ to $\boldsymbol{C}$ defined by*

$$\hat{f}_\chi(\theta) = \sum_a \sum_b f_b(a)\theta(b)\chi(a^\sharp)h_\chi h_a/n(A) .$$

Then f is a (probability) homomorphism if and only if $\hat{f}$ is a (probability) homomorphism. Also if $g = \hat{f}$ then $\hat{g} = f$ (after identifying each of A and B with its double dual). Thus the category of finite abelian dualizable probability groups with homomorphisms is self dual.

Proof. For $a \in A$ let $f(A)$ denote $\sum_b f_b(a)b$, and then extend f to a linear map from $\boldsymbol{C}(A)$ to $\boldsymbol{C}(B)$. Extend each $\theta \in \hat{B}$ by linearity to an algebra homomorphism from $\boldsymbol{C}(B)$ to $\boldsymbol{C}$. Doing the same thing to $\hat{f}$ and each $\chi \in \hat{A}$, one checks using Proposition 2.10, that $\hat{f}(\theta) = \theta \circ f$ for each $\theta \in \hat{B}$. Thus by vector space duality $\hat{g} = f$ if $\hat{f} = g$ (after the proper identifications). If f is a homomorphism, $\hat{f}$ maps $\hat{B}$ to $\hat{A}$, so for $\theta_1, \theta_2 \in \hat{B}$, $a \in A$

$$\begin{aligned}\sum_\theta \hat{p}_\theta(\theta_1, \theta_2)\hat{f}(\theta)(a) &= \sum_\theta \hat{p}_\theta(\theta_1, \theta_2)\theta(f(a)) = \theta_1(f(a))\cdot\theta_2(f(a)) \\ &= \hat{f}(\theta_1)(a)\cdot\hat{f}(\theta_2)(a) = \sum_\chi \hat{p}_\chi(\hat{f}(\theta_1), \hat{f}(\theta_2))\chi(a) ,\end{aligned}$$

and since this is true for all a,

$$\sum_\theta \hat{p}_\theta(\theta_1, \theta_2)\hat{f}(\theta) = \sum_\chi \hat{p}_\chi(\hat{f}(\theta_1), \hat{f}(\theta_2))\chi$$

which implies $\hat{f}$ is a homomorphism. Now this same argument with f replaced by $\hat{f}$ proves the proposition.

COMMENT 2.2. The self dual category of the last proposition does not have products or coproducts so falls short of being abelian, but is exact ([2]).

COMMENT 2.3. Let A, B be finite abelian dualizable probability groups as in the last proposition. A map f from A to B determines a unique map α, $(\theta, \chi) \mapsto \alpha_\chi(\theta)$, from $\hat{B} \times \hat{A}$ to $\boldsymbol{C}$ with

$$\theta \circ f = \sum_\chi \alpha_\chi(\theta)\chi$$

for all $\theta \in \hat{B}$. One checks α is $\hat{f}$. We call f *dualizable* if for each

θ, the $\alpha_\chi(\theta)$ are nonnegative and add to 1. One can check $f \to \hat{f}$ is a bijection from the dualizable maps from A to B onto the strict morphisms from $\hat{B}$ to $\hat{A}$.

Let r and s be positive integers. We say a finite dualizable abelian probability group A is *(r, s)-integral* if A is r-integral and $\hat{A}$ is s-integral.

PROPOSITION 2.14. *Let r be a positive integer. Let A be a finite r-integral probability group. Then if $r \neq 1$, A is 2-integral. Assume further that s is a positive integer and A is a finite dualizable abelian (r, s)-integral probability group. Then if S is any subgeometry of A, $n(S)$ divides $n(A)$. Also if r and s are not both* 1, *for each $\chi \in \hat{A}$, $h_\chi^{1/s}$ divides $n(A)$ (so by duality, for each $a \in A$, $h_a^{1/r}$ divides $n(\hat{A}) = n(A)$).*

Proof. For $a, b, c \in A$,

$$m_c(a, b) = p_c(a, b)h_a^{1/r}h_b^{1/r}/h_c^{1/r}$$

is a nonnegative integer. Letting $c = e, b = a^\#$ we get (using Proposition 2.2 to show $h_a = h_{a^\#}$) h_a divides $(h_a^{1/r})^r$. If $r \geqq 2$, $(h_a^{1/r})^2(h_a^{1/r})^{r-2} = h_a$ gives that $(h_a^{1/r})^2$ divides h_a, so $(h_a^{1/r})^2 = h_a$ so $h_a^{1/r} = h_a^{1/2}$. With this one checks A is 2-integral. Now suppose A is dualizable abelian (r, s)-integral. If S is a subgeometry, $n(S)n(A//S) = n(A)$ and $n(A//S) = n(\widehat{A//S}) = n(S^\perp)$ is an integer, so $n(S)$ divides $n(A)$. Let $\chi \in \hat{A}$. The $w_a = h_a^{1/r}a$, $a \in A$, generate a subring of $C(A)$ which is finitely generated as an abelian group. Thus the same is true of the image of the extension of χ (by linearity) to this ring. Hence $h_a^{1/r}\chi(a)$ is an algebraic integer for each $a \in A$. Now assume r and s are not both 1. By Proposition 2.10,

$$\sum_a h_a\chi(a)\overline{\chi(a)} = n(A)/h_\chi\ .$$

Case 1. $r \neq 1$. Then $h_a^{1/r} = h_a^{1/2}$ so $h_a^{1/2}\chi(a)$ and $\overline{h_a^{1/2}\chi(a)}$ are both algebraic integers, so $n(A)/h_\chi$ is an algebraic integer and a rational number. Thus h_χ divides $n(A)$. But $h_\chi^{1/s}\cdot(h_\chi^{1/s})^{s-1} = h_\chi$ so $h_\chi^{1/s}$ divides h_χ.

Case 2. $r = 1$. Replacing A by $\hat{A}$ in an above argument gives $h_\chi^{1/s}\chi(a)$ is an algebraic integer. Thus

$$\sum_a h_a\chi(a)h_\chi^{1/s}\overline{\chi(a)} = n(A)/(h_\chi^{1/s})^{s-1}$$

is an integer, so $(h_\chi^{1/s})^{s-1}$ divides $n(A)$, and since $s \geqq 2$, $h_\chi^{1/s}$ divides $(h_\chi^{1/s})^{s-1}$. This proves the proposition.

We end this section with a structure theorem which characterizes finite projective spaces. If $(P, \mathscr{L})$ is a finite projective space with not both P and $\mathscr{L}$ empty, and if $m > 2$ is a real number such that every line (i.e., element of $\mathscr{L}$) has exactly $m + 1$ points on it, then the probability group $P^\#$ of Example 2.4 is not sharp, and every $a \in P^\#$ is in a subgeometry of $P^\#$ which contains two or less elements (i.e., $|\langle\{a\}\rangle| \leqq 2$). $(P, \mathscr{L})$ and m are easily reconstructed from $P^\#$ so are uniquely determined by $P^\#$.

PROPOSITION 2.15. *Let A be a finite probability group such that $|\langle\{a\}\rangle| \leqq 2$ $\forall a \in A$ (where $\langle\{a\}\rangle$ denotes the subgeometry generated by a). For simplicity assume A is not sharp (i.e., not a group in which every element has order* 2 *or* 1). *Then there exists a unique (up to isomorphism) finite projective space $(P, \mathscr{L})$ with not both P and $\mathscr{L}$ empty, and there exists a unique real $m > 2$ such that every line in $\mathscr{L}$ has exactly $m + 1$ points on it and $A \cong P^\#$(where $(P, \mathscr{L})$ and m define $P^\#$ as in Example* 2.4). *In particular, A is abelian, and if it has more than two elements it is dualizable and* (1, 1)*-integral.*

Proof. If $|A| = 2$, the result is easily checked so without loss assume $|A| \geqq 3$. By the comment immediately following Proposition 1.8, $(P, \mathscr{L})$ is a finite projective space, where $P = \{a \in A \mid a \neq e\}$, where for $a, b \in P$, $a \neq b$, L_{ab} is $\{c \in A \mid p_{c^\#}(a, b) > 0$ or $c = a$ or $c = b\}$, and where $\mathscr{L} = \{L_{ab} \mid a, b \in P, a \neq b\}$. Since $\mathscr{L}$ is nonempty there is a unique m such that every line has exactly $m + 1$ points on it. Let (B, q) be the probability group associated by Example 2.4 to (P, L). Then B and A are the same sets, they have the same identity, $\Delta_B = \Delta_A$ (i.e., they have the same geometry), but it remains to prove $p_c(a, b) = q_c(a, b)$ for all $a, b, c \in B = A$. Let $\mathscr{H}$ be the set of all maximal proper subgeometries of B (or equivalently of A). For $S \in \mathscr{H}$, the sets of $A//S$ and $B//S$ are equal and $|B//S| = 2$ so $|A//S| = 2$. Hence $A//S = \{S, A\backslash S\}$ where $A\backslash S$ denotes the elements in A not in S. One can check the dual of a two element probability group $\{e, x\}$ is $x \mapsto 1$ and $x \mapsto -(h_x)^{-1}$, so the dual of $A//S$ is $\{\text{aug}, g_S\}$ where $g_S(S) = 1$ and $g_S(A\backslash S) = -(h_{A\backslash S})^{-1}$. Let k_S be the natural map from A to $A//S$. Then $f_S = g_S \circ k_S$ is in $\hat{A}$. In fact aug, and the f_S, $S \in \mathscr{H}$, are distinct, and since their number is the same as $|\hat{A}|$ (in a projective space the number of hyperspaces is the same as the number of points), they make up all of $\hat{A}$. For $a \in A$, $a \neq e$, the restriction of f_S to $\{e, a\}$ must be in the dual of $\{e, a\}$. Hence $f_S(a)$ is either 1 or $-(h_a)^{-1}$. Choosing $a \notin S$ we get $-(h_{A\backslash S})^{-1} = -(h_a)^{-1}$ so $h_{A\backslash S} = h_a$. Hence if $b \notin S$, $h_a = h_b$. Let $L \in \mathscr{L}$, $C = \{e\} \cup L$. Then L is a subgeometry of A, so all of the above holds with A replaced by C. Using that the hyperplanes of C are just the $\{e, c\}$, $c \in C$, $c \neq e$, one checks $h_a = h_b$ for all $a, b \in C$, $a \neq e$, $b \neq e$. Hence there is an h with $h_a = h$ for all $a \in A$, $a \neq e$. But by Proposition 2.2, $h_{C \backslash S} n(S) = n(C \backslash S)$; since there are $m + 1 + 1$ elements in C, this gives $h \cdot (h + 1) = mh$ so $h = m - 1$. Returning back to A, and S a hyperspace of A we have $f_S(a) = 1$ if $a \in S$ and $f_S(a) = -(m-1)^{-1}$ if $a \in A \backslash S$. This whole argument can be done with A replaced by B, and we see the dual of B is the same set of maps; i.e., $\hat{A} = \hat{B}$. For this set of maps there exist unique $\hat{p}$ with

$$f(x) \cdot g(x) = \sum \hat{p}_k(f, g) k(x)$$

for all $f, g \in \hat{A} = \hat{B}$ and all $x \in A = B$. Taking double duals the proof is completed.

3. **Formal character tables.** In [9], Brauer formalizes some properties of the character table of a finite group, and then considers tables with those properties in their own right. Here we choose a somewhat different set of properties, suggested by the last section, to make the same sort of approach.

We denote the complex conjugate of a complex number C by $\bar{C}$. We consider square matrices whose entries are complex numbers. If M is such, we write $m(M)$ for the *size* of M (i.e., the number of rows, or equivalently, the number of columns), and we denote the (i, j)-entry of M by M_{ij} for $i, j = 1, \cdots, m(M)$. The set of rows of M will be labeled $\{1, \cdots, m(M)\}$ and will be denoted by $R(M)$, and the set of columns of M will be labeled $\{1, \cdots, m(M)\}$ and will be denoted by $C(M)$.

By a *semiformal table* we mean a square complex matrix M such that there exist positive real numbers $h_1, \cdots, h_m, t_1, \cdots, t_m (m = m(M))$ with $\sum_i h_i = \sum_\alpha t_\alpha$ (call this n or $n(M)$ or the *order* of M), with $t_1 = 1$, and with:

(1) $M_{i1} = 1 \; \forall i = 1, \cdots, m$.

(1′) $M_{1\alpha} = 1 \; \forall \alpha = 1, \cdots, m$.

(2) $\sum_i M_{i\alpha} M_{i\beta} \bar{M}_{i\gamma} h_i$ is a nonnegative real number $\forall \alpha, \beta, \gamma$ and if $\alpha = 1$ it is $I_{\beta\gamma} n / t_\beta \forall \beta, \gamma$ (where I is the identity matrix of size m).

It will soon be apparent that if the h_i and t_α exist, they are unique. One can check that the transpose of a semiformal table is itself a semiformal table if and only if $\sum_\alpha M_{i\alpha} M_{j\alpha} \bar{M}_{k\alpha} t_\alpha$ is a nonnegative real $\forall i, j, k$; if this condition holds we call M a *formal table*. If M is a semiformal table, the matrix which results when the nonfirst rows (and/or the nonfirst columns) of M are permuted is certainly a semiformal table; we say it is *isomorphic* to M to express that it is essentially the same as M.

For $A = \{a_1 = e, a_2, \cdots, a_m\}$ a finite abelian probability group, let $\hat{A} = \{\chi_1 = \text{aug}, \chi_2, \cdots, \chi_m\}$ and let $M_{i\alpha} = \chi_i(a_\alpha)$ for $i, \alpha = 1, \cdots, m$. The resulting matrix M is a semiformal table by the last section (and it is a formal table if and only if A is dualizable).

PROPOSITION 3.1. *The above association is a bijection from the isomorphism classes of finite abelian probability groups onto the isomorphism classes of semiformal tables.*

Proof. Let M be a semiformal table of size m. By (2) M has an inverse, so M is nonsingular. Thus the columns of M are a basis of $C^{(m)}$, so there exist unique complex numbers $p_\gamma(\alpha, \beta)$ with

$$M_{i\alpha}M_{i\beta} = \sum_\gamma p_\gamma(\alpha, \beta)M_{i\gamma}\forall i, \alpha, \beta = 1, \cdots, m .$$

Using (2) one checks the $p_\gamma(\alpha, \beta)$ are nonnegative reals. Also, (because the columns are a basis) there exist unique complex numbers $c_{\beta\alpha}$ with

$$\bar{M}_{i\beta} = \sum_\gamma c_{\beta\gamma}M_{i\gamma}\forall i, \beta = 1, \cdots, m .$$

Taking the complex conjugate of this gives

$$\sum_\gamma \bar{c}_{\beta\gamma}c_{\gamma\alpha} = \delta_{\beta,\alpha} \text{ (Kronecker delta)} .$$

But

$$p_1(\alpha, \beta)n/t_1 = \sum_i M_{i\alpha}M_{i\beta}\bar{M}_{i1}h_i = \sum_\gamma \sum_i \bar{c}_{\beta\gamma}M_{i\alpha}\bar{M}_{i\gamma}h_i = \bar{c}_{\beta\alpha}n/t_\alpha$$

so $\bar{c}_{\beta\alpha}$ is nonnegative real. With this one can check (using $\sum \bar{c}_{\beta\gamma}c_{\gamma\alpha} = \delta_{\beta,\alpha}$) that for each β there is a unique γ with $c_{\beta\gamma} \neq 0$ (and also $c_{\beta\gamma} = 1$). With this one checks $C(M)$ with p is a finite albelian probability group, and its associated table is M. One checks that if we start with a finite abelian probability group, and perform this construction on its associated table, we get seomething isomorphic to the probability group we started with. The proposition is shown.

Now let M be a formal table. As in the above proof we have that both $C(M)$ and $R(M)$ are naturally abelian probability groups. We say M is (r, s)-integral if $C(M)$ is r-integral and $R(M)$ is s-integral. For G a finite group, D the diagonal subgroup of $G \times G$, $G\times G//D$ is a finite abelian dualizable (1, 2)-integral probability group and its associated matrix M is a formal table which we denote by $T(G)$ and call the adjusted character table of G. The matrix $h_i^{1/2}M_{i\alpha}$, $i \in R(M)$, $\alpha \in C(M)$, is the character table of G, while conversely, if N is the character table of G, $N_{i\alpha}/N_{i1}$, $i \in R(N)$, $\alpha \in C(N)$, is the adjusted character table of G.

Now let N be a formal table. By a table *morphism* from M to N we mean a map f from $C(M)$ to $C(N)$ such that $f(1) = 1$ and such that

$$\sum_{\beta} N_{if(\beta)} M_{j\beta} t_{\beta} \text{ is a nonnegative real } \forall i, j \,.$$

For $i \in R(N)$, $j \in R(M)$, we define $\hat{f}_{j\sharp}(i)$ so that $\hat{f}_{j\sharp}(i)n/h_j$ is this displayed nonnegative real.

PROPOSITION 3.2. *Let M and N be formal tables. Let f be a map from $C(M)$ to $C(N)$. Write*

$$N_{if(\beta)} = \sum_j x_j(i) M_{j\beta} \ \forall i = 1, \cdots, m(N), \beta = 1, \cdots, m(M)$$

which we can do since the rows of M are a basis. Then f is a morphism if and only if $f(1) = 1$ and all the coefficients $x_j(i)$ are nonnegative real numbers. If f is a morphism, then $x_j(i) = \hat{f}_j(i)$ for all i and j.

Proof. If f is a morphism we substitute $\hat{f}_j(i)$ for $x_j(i)$ above and then use (3′) with $\gamma = 1$. Conversely, if the $x_j(i)$ are nonnegative real numbers, we substitute in the criteria for a morphism, use (3) with $k = 1$, and get $x_{j\sharp}(i)n/h_j$. The proposition is proved.

We call a map f from $C(M)$ to $C(N)$ *a homomorphism* if for each $i \in R(N)$ there exists a $j \in R(M)$ with $N_{if(\beta)} = M_{j\beta} \forall \beta$. We denote such a j by $\hat{f}(i)$ and check if f is a homomorphism, then $\hat{f}$ is a homomorphism from N^t to M^t (where $(\ )^t$ denotes the transpose of $(\ )$). Both morphisms and homomorphisms compose and give categories. In both cases isomorphims consist of simply permuting the nonfirst rows and columns. We write $M \cong N$ if such exists from M to N.

Let M be a formal table. For S a subset of $R(M)$, $S^{\perp} = \{\alpha \in C(M) \mid M_{i\alpha} = 1 \forall i \in S\}$. For T a subset of $C(M)$, $T^{\perp} = \{i \in R(M) \mid M_{i\alpha} = 1 \forall \alpha \in T\}$. By a *submatrix* of M we mean any matrix derived at by deleting rows and columns from M. We let mat(T) denote the submatrix of M which results when first all columns not in T are deleted from M and then all but one of resulting duplicate rows are removed. Each column of mat(T) comes from some column of M; this gives a natural map from $C(\text{mat}(T))$ to $C(M)$. For S a subset of $R(M)$, the matrix derived at by deleting all rows of M not in S, and then deleting all but one of resulting duplicate columns, will be denoted mat(S). We have a natural map from $C(M)$ to $C(\text{mat}(S))$; each eolumn of M is first truncated by removing all elements not in rows of S and then appears in mat(S). By a *subtable* of M we shall mean a subgeometry of $C(M)$; if T is such this terminology tends to confuse T with $\mathrm{mat}(T)$; indeed, when no confusion can result we sometimes denote $\mathrm{mat}(T)$ simply by T. By a *factor table* of M we mean a subgeometry S of $R(M)$; when S is such we sometimes denote $\mathrm{mat}(S)$ simply by S or by $M/S^{\perp}$. Clearly the factor tables of M are exactly the subtables of M^t.

PROPOSITION 3.3. *Let M be a formal table and T be a subset of $C(M)$. Then the following are equivalent:*

(1) *$\exists$ a subset S of $R(M)$ with $S^{\perp} = T$,*

(2) *$T = (T^{\perp})^{\perp}$,*

(3) *T is a subtable of M.*

If T is a subtable of M, then T (i.e., $\mathrm{mat}(T)$) is a formal table, $T^{\perp}$ is a factor table of M, M/T (i.e., $\mathrm{mat}(T^{\perp})$) is a formal table, the natural map from $C(\mathrm{mat}(T))$ to $C(M)$ is an injective homomorphism from $\mathrm{mat}(T)$ to M, the natural map from $C(M)$ to $C(\mathrm{mat}(T^{\perp}))$ is a surjective homomorphism from M to $\mathrm{mat}(T^{\perp})$, and the image of the former map is exactly the inverse image under the latter map of the singleton consisting of the first column; also $n(\mathrm{mat}(T^{\perp}))n(\mathrm{mat}(T)) = n(M)$.

Proof. Everything is either trivially checked or follows from results in the last section, so the proof is omitted.

Note 3.1. Let T be a subtable of a formal table M. Let

$$\varphi\colon C(\mathrm{mat}(T)) \longrightarrow C(M),\ \theta\colon C(M) \longrightarrow C(\mathrm{mat}(T^{\perp}))$$

be the natural homomorphisms. For $\alpha \in C(\mathrm{mat}(T))$, $t_{\alpha} = t_{\varphi(\alpha)}$. For $\beta \in C(M)$, let $[\beta]_T = [\beta]$ be the set of all $\delta \in C(M)$ with $\theta(\beta) = \theta(\delta)$. Then $t_{\theta(\beta)} = \sum (t_{\delta}/n(\mathrm{mat}(T)))$, the sum over all $\delta \in [\beta]$. For $\beta, \gamma, \delta \in C(M)$, $q_{\theta(\delta)}(\theta(\beta), \theta(\gamma)) = \sum_{\alpha} q_{\alpha}(\beta, \gamma)$, the sum over all $\alpha \in [\delta]$. For $\beta, \gamma \in C(M)$, $\theta(\beta) = \theta(\gamma)$ if and only if $q_{\varphi(\alpha)}(\beta, \gamma^{\#}) > 0$ for some $\alpha \in C(\mathrm{mat}(T))$. By replacing M by M^t we get the corresponding statements for $\hat{\theta}\colon R(\mathrm{mat}(T^{\perp})) \to R(M)$, $\hat{\varphi}\colon R(M) \to R(\mathrm{mat}(T))$, the h's, and the p's.

PROPOSITION 3.4. *Let M and N be formal tables and let f be a homomorphism from M to N. Let $K_f = \{\alpha \in C(M) \mid f(\alpha) = 1\}$ and $I_f = \{f(\alpha) \mid \alpha \in C(M)\}$. Then K_f is a subtable of M, and I_f is a subtable of N, and if $\theta\colon M \to M/K_f$, $\varphi\colon I_f \to N$ are the natural homomorphisms, then there exists a unique isomorphism $g\colon M/K_f \to I_f$ with $\varphi \circ g \circ \theta = f$.*

Proof. This follows from Proposition 2.3.

Propositions 2.4 and 2.5 give immediately: Let T and W be subtables of a formal table M. Let $T \cdot W$ denote the set of all $\alpha \in C(M)$ such that $\exists \beta \in T, \gamma \in W$ with $q_\alpha(\beta, \gamma) > 0$. Then $T \cdot W$ aud $T \cap W$ are subtables of M and

$$(T \cdot W/W) \cong (T/(T \cap W)) .$$

If T is a subtable of a formal table M, then $L \mapsto L/T$ is a lattice preserving bijection from the set of all subtables of M which contains T onto the set of all subtables of M/T. Also if L is a subtable of M with $T \subseteqq L$, then

$$(M/T)/(L/T) \cong M/L .$$

We call a formal table *simple* if it has exactly two subtables. A formal table M will have a chain of subtables

$$M = T_0 \supseteqq T_1 \supseteqq \cdots \supseteqq T_r = \{1\}$$

such that T_i/T_{i+1} is simple for $i = 0, \cdots, r-1$. We get that the *length* r of M and the unordered sequence $\{T_i/T_{i+1} \mid i = 0, \cdots, r-1\}$ of *composition factors* of M are well-defined and unique.

We call a formal table M *projective* if $\{\alpha, 1\}$ is a subtable of $M \forall \alpha \in C(M)$. By Proposition 2.14 we know explicitly the structure of such tables (at least up to knowledge of the non-Desarguean planes), and in particular if M is such and is of size larger than 2, then M is (1, 1)-integral. If M is (1, 2)-integral (e.g., $T(G)$ for G a finite group), $n(M)$ is an integer and by Proposition 2.14 all the $h_i^{1/2}$ and t_α divide $n(M)$, and the order of any subtable divides $n(M)$. In practice this puts rather heavy restrictions on the table. For instance, if M is an (r, s)-integral formal table where r and s are not both 1, with $n(M)$ a proper prime power, then by using $n(M) = \sum h_\alpha + \sum h_\beta$ (the first sum over all $\alpha \in C(M)$ with $h_\alpha > 1$, and the second sum over all $\beta \in C(M)$ with $h_\beta = 1$), it is easy to check that M has a subtable isomorphic to $T(C_p)$, where C_p is the cyclic group of order p, and p is the prime which divides $n(M)$. Hence if $n(M) = p$, $M \cong T(C_p)$.

We now strengthen Proposition 3.4 to the "nonnormal" situation:

PROPOSITION 3.5. *Let f be a morphism from a formal table M to a formal table N. Let $K_f = \{\alpha \in C(M) \mid f(\alpha) = 1\}$, $K_{\hat f} = \{i \in R(N) \mid \hat f_1(i) = 1\}$, $I_{\hat f} = \{j \in R(M) \mid \hat f_j(i) > 0$ for some $i\}$, and I_f be the intersection of all subtables of N which contain $f(\alpha)$ for all $\alpha \in C(M)$. Then K_f is a subtable of M, I_f is a subtable of N, $K_{\hat f}$ is a factor table of N, and $I_{\hat f}$ is a factor table of M. Also $I_{\hat f}{}^\perp = K_f$ and $K_{\hat f}{}^\perp = I_f$. If $\theta: M \to M/K_f$ and $\varphi: I_f \to N$ are the natural homomorphisms, then there is a unique morphism g from M/K_f to I_f*

such that $\varphi\circ g\circ\theta = f$. *Also* $K_g = \{1\}$ *and* $I_g = I_f$. *If* f *is a homomorphism, then this all reduces to the situation and notation of Proposition* 3.4.

Proof. Let $m = m(M)$ and $C(M)$ denote the algebra $C^{(m)}$ with multiplication defined point-wise. For $i \in R(M)$ we write M_{i*} for the row $(M_{i1}, M_{i2}, \cdots, M_{im})$. We have the M_{i*} are a basis of $C(M)$ and

$$M_{i*}\cdot M_{j*} = \sum_k p_k(i, j)M_{k*}$$

for all $i, j \in R(M)$. Let $\alpha \in C(M)$. By the proof of Proposition 2.10, there exists a nonzero idempotent $u_\alpha \in C(M)$ with $u_\alpha\cdot M_{i*} = u_\alpha M_{i\alpha}$ for all i. Letting $u_\alpha = \sum r_j M_{j*}$ we have $\sum_j r_j p_k(j, i) = r_k M_{i\alpha}$ so

$$(\sum_k |r_k|)|M_{i\alpha}| \leqq \sum_k \sum_j |r_j| p_k(j, i) = \sum_j |r_j|$$

so $|M_{i\alpha}| \leqq 1$ for all $i \in R(M)$, $\alpha \in C(M)$.

Now let $\beta \in K_f$. Then from

$$1 = N_{if(\beta)} = \sum_j \hat{f}_j(i)M_{j\beta}\ ,$$

$$1 = |\sum_j \hat{f}_j(i)M_{j\beta}| \leqq \sum_j \hat{f}_j(i)|M_{j\beta}| \leqq \sum_j \hat{f}_j(i) = 1\ ,$$

we get $\hat{f}_j(i) > 0$ implies $M_{j\beta} = 1$. Thus $\beta \in I_{\hat{f}}{}^\perp$. One easily checks, $I_{\hat{f}}{}^\perp \subseteqq K_f$, so we have $I_{\hat{f}}{}^\perp = K_f$. The rest of the proposition now either is easily checked or follows from Lemma 2.2.

We say a morphism f from a formal table M to a formal table N is *2-integral* if $\hat{f}_j(i)h_i^{1/2}/h_j^{1/2}$ is an integer for all $i \in R(N)$, $j \in R(M)$. For instance, if H and G are finite groups and $\varphi: H \to G$ is a group homomorphism, then the adjusted character tables $T(H)$, $T(G)$ are (1, 2)-integral, and the natural map $f = T(\varphi): T(H) \to T(G)$ (which has the obvious effect on conjugacy classes, $\langle h\rangle \mapsto \langle\varphi(h)\rangle$) is a 2-integral morphism. One checks φ is injective if and only if $K_f = \{1\}$. With this in mind we let N be an arbitrary (1, 2)-integral formal table. By a *presubobject* of N we mean a pair (M, f) where M is a (1, 2)-integral formal table, and f is a 2-integral morphism from M to N with $K_f = \{1\}$. We call two presubobjects (M, f), (L, g) *equivalent* if there exists an isomorphism $\theta: M \to L$ with $g\circ\theta = f$. The equivalence class containing a presubobject (M, f) will be denoted $c(M, f)$ and called a *subobject* of N. It will be called *cyclic* (respectively *abelian*) if $M \cong T(G)$ for G a finite cyclic (respectively abelian) group. These can be used in defining pseudogroups (see [1]). The class of all subobjects of N is a finite partially ordered set, where we write $c(M, f) \leqq c(L, g)$ if there exists a morphism θ from M to L with $g\circ\theta = f$. There is something to prove here but it follows from:

PROPOSITION 3.6. *Let $c(M, f)$ be a subobject of a $(1, 2)$-integral formal table N. Then $n(M)$ divides $n(N)$. Also if $n(M)$ equals $n(N)$, then f is an isomorphism. There are only finitely many possibilities for $c(M, f)$.*

Proof. For $\alpha \in C(N)$, $k \in R(M)$ define

$$y_k(\alpha) = \sum_i (\hat{f}_k(i)h_i^{1/2}/h_k^{1/2})h_i^{1/2}N_{i\alpha} ,$$

$$z_k(\alpha) = (n(N)/t_\alpha)(\sum_\beta (t_\beta/n(M))h_k^{1/2}M_{k\beta})$$

where the second sum is over all β with $f(\beta) = \alpha$ (and the first sum is over all $i \in R(N)$). One checks that

$$\sum_\alpha y_k(\alpha)t_\alpha N_{j\alpha} = \sum_\alpha z_k(\alpha)t_\alpha N_{j\alpha}$$

for all j, k, and one checks this implies $y_k(\alpha) = z_k(\alpha)$. Letting $\alpha = 1, k = 1$ this gives

$$n(M)(\sum_i (\hat{f}_1(i)h_i^{1/2}/h_1^{1/2})h_i^{1/2}) = n(N) .$$

But $M_{1\beta} = 1 = N_{1f(\beta)} = \sum_j \hat{f}_j(1)M_{j\beta}$ and since the rows M_{j*} are linearly independent, we get $\hat{f}_1(1) = 1$, so $(\hat{f}_1(1)h_1^{1/2}/h_1^{1/2})h_1^{1/2} = 1$, so the above sum over all i is $\geqq 1$. Now assume this sum is equal to 1. Then we must have $\hat{f}_1(i) = 0$ for $i \neq 1$. With this one checks

$$\sum_k \hat{f}_k(i)\hat{f}_k(x)/h_k = \sum_k \sum_j \hat{f}_k(i)\hat{f}_j(x^\#)p_1(k, j) = \sum_z p_z(i, x^\#)\hat{f}_1(z) = p_1(i, x^\#)$$

so if $i \neq x$, $\hat{f}_j(i)\hat{f}_k(x) = 0$. By Proposition 3.5, $I_{\hat{f}} = R(M)$, so for each $k \in R(M)$ there exists a unique $i \in R(N)$ with $\hat{f}_k(i) > 0$. Denote i by $g(k)$. For each $i \in R(N)$, $\sum_k \hat{f}_k(i) = 1$ so $\hat{f}_k(i) > 0$ for some k, so g is surjective. Letting $x = i$ above gives

$$\sum_k \hat{f}_k(i)\hat{f}_k(i)/h_k = 1/h_i$$

or

$$\sum_k (\hat{f}_k(i)h_i^{1/2}/h_k^{1/2})^2 = 1$$

where the sum can be taken over all $k \in g^{-1}(\{1\})$. Since f is 2-integral, there exists a unique k with $\hat{f}_k(i) > 0$. We denote k by $\hat{f}(i)$. We also have g is bijective and an inverse to $\hat{f}$. f is a homomorphism so $\hat{f}$ is a homomorphism, so $\hat{f}$ is an isomorphism so f is an isomorphism.

There are certainly only a finite number of possibilities for the row orders for M since they add to a number dividing $n(N)$. The

$$m_k(i, j) = p_k(i, j)h_i^{1/2}h_j^{1/2}/h_k^{1/2}$$

are nonnegative integers limited by $\sum_k m_k(i, j)h_k^{1/2} = h_i^{1/2}h_j^{1/2}$ so there are only finitely many possibilities for them. The nonnegative integers $m_k(i) = \hat{f}_k(i)h_i^{1/2}/h_k^{1/2}$ are limited by $\sum_k m_k(i)h_k^{1/2} = h_i^{1/2}$ so there are only finitely many possibilities for them. The proposition is now proven.

When we remove integrality restrictions the above situation changes. Let M be an arbitrary formal table. For X a subset of $R(M)$ we write $n(X)$ for $\sum_x h_x$ (the sum over all $x \in X$) and $X^\#$ for $\{x^\# | x \in X\}$. This notation of course holds for M^t also. By an *admissible partition* of M we mean a pair $(\mathscr{P}, \mathscr{Q})$ where $\mathscr{P}$ is a partition of $R(M)$ and $\mathscr{Q}$ is a partition of $C(M)$ such that:

(1) $\{1\} \in \mathscr{P}$ and $\{1\} \in \mathscr{Q}$,

(2) $X^\# \in \mathscr{P}$ and $Y^\# \in \mathscr{Q}$ for all $X \in \mathscr{P}$, $Y \in \mathscr{Q}$,

(3) $\sum_{(x \in X)} (h_x/n(X))M_{xy'} = \sum_{(y \in Y)} (h_y/n(Y))M_{x'y}$ for all $y' \in Y \in \mathscr{Q}$ and all $x' \in X \in \mathscr{P}$.

We denote the number in (3) by M_{XY}, and the matrix with entries M_{XY}, $X \in \mathscr{P}$, $Y \in \mathscr{Q}$ (where $\mathscr{P} = \{X_1, \cdots, X_r\}$, $\mathscr{Q} = \{Y_1, \cdots, Y_s\}$, $X_1 = \{1\}$, $Y_1 = \{1\}$) by $M/(\mathscr{P}, \mathscr{Q})$. Letting $h_X = n(X)$, $h_Y = n(Y)$ one easily checks this is a formal table and the natural map $C(M) \to \mathscr{Q}$ is a morphism.

As an example, if G is a group of automorphisms of M, then by Propositions 2.7 and 2.12, the set $\mathscr{Q}$ of orbits of $C(M)$ by G with the set $\mathscr{P}$ of orbits of $R(M)$ by $\{\hat{\tau} | \tau \in G\}$ is a partition of M. In this case we denote $M/(\mathscr{P}, \mathscr{Q})$ by M/G.

PROPOSITION 3.7. *Let f be a morphism from a formal table M to a formal table N such that $K_f = \{1\}$. Then $n(M) \leqq n(N)$. Also $n(M) = n(N)$ if and only if there exists an admissible partition $(\mathscr{P}, \mathscr{Q})$ of M and an isomorphism φ from $M/(\mathscr{P}, \mathscr{Q})$ onto N with $\varphi \circ \theta = f$, where θ is the natural morphism from M to $M/(\mathscr{P}, \mathscr{Q})$.*

Proof. We repeat the words of the proof of Proposition 3.6 to get $n(M) \leqq n(N)$, and to assume $n(M) = n(N)$ and get there exists a surjective map g from $R(M)$ to $R(N)$ with $\hat{f}_k(i) > 0$ if and only if $g(k) = i$. Still using that proof we get

$$y_k(\alpha) = \hat{f}_k(g(k))h_{g(k)}N_{g(k)\alpha}/h_k^{1/2} ,$$

$$z_k(\alpha) = \sum_\beta (t_\beta/t_\alpha)h_k^{1/2}M_{k\beta} \text{ (over all } \beta \text{ with } f(\beta) = \alpha)$$

so letting $\alpha = 1$, $\hat{f}_k(g(k)) = h_k/h_{g(k)}$, and substituting this back,

$$t_\alpha N_{g(k)\alpha} = \sum_\beta t_\beta M_{k\beta}, \text{ the sum over all } \beta \text{ with } f(\beta) = \alpha .$$

Substituting in the equation of Proposition 3.2,

$$h_i N_{if(\beta)} = \sum_k h_k M_{k\beta}, \text{ the sum over all } k \text{ with } g(k) = i .$$

Also $f(1) = 1$, $g(1) = 1$. For $\alpha \in C(N)$, $\beta \in C(M)$, let $\hat{g}_\beta(\alpha)$ be 0 if $\alpha \neq f(\beta)$ and be $t_\beta/t_{f(\beta)}$ if $\alpha = f(\beta)$. Then

$$N_{g(k)\alpha} = \sum_\beta \hat{g}_\beta(\alpha) M_{k\beta}$$

so by Proposition 3.2, g is a morphism from N^t to M^t. Note $\hat{g}_1(\alpha) = 0$ for $\alpha \neq 1$, and $K_g = \{1\}$. By interchanging g with f, f is surjective. Let $\mathscr{P}$ and $\mathscr{Q}$ be the partitions defined on $R(M)$ and $C(M)$ by g and f respectively. The above formulas give $(\mathscr{P}, \mathscr{Q})$ is an admissible partition of M and $\varphi \circ \theta = f$, where θ is the natural morphism from M to $M/(\mathscr{P}, \mathscr{Q})$ and φ is the bijection induced by f. Clearly φ is an isomorphism. The converse is easily checked directly, so the proposition is proved.

We note by Proposition 2.6, the categories we are considering have finite products (the Kronecker product of the matrices) and zero object.

References

1. R. Brauer, *On pseudo groups*, J. Math. Soc. Japan, **20** (1968), 13-22.
2. H. B. Brinkmann und D. Puppe, *Abelsche und exacte Kategorien*, Korrespondenzen, Lect. Notes in Math., **96** (1969).
3. R. H. Bruck, *A survey of binary systems*, Springer-Verlag, 1966.
4. M. Drescher-O. Ore, *Theory of multigroups*, Amer. J. Math., **60** (1938), 705-733.
5. C. F. Dunkl, *Structure hypergroups for measure algebras*, Pacific J. Math., **47** (1973), 413-425.
6. R. I. Jewett, *Spaces with an abstract convolution of measures*, Adv. in Math., **18** (1975), 1-101.
7. W. Prenowitz, *Projective geometries as multigroups*, Amer. J. Math., **65** (1943), 235-256.
8. K. A. Ross, *Hypergroups and centers of measure algebras*, to appear.
9. R. L. Roth, *Character and conjugacy class hypergroups of a finite groups*, Annali di Mat. pura ed appl., **55** (1975), 295-311.
10. L. Scott, Jr., *A condition on Higman's parameters*, Abstract 701-20-45, Notices of Amer. Math. Soc., **20** (1973).
11. R. Spector, *Apercu de la theorie des hypergroups*, Lecture Notes in Math., #497 (1975).

Received August 31, 1977 and in revised form August 2, 1978. This work was supported in part by National Science Foundation Grant MCS 76-05934.

UNIVERSITY OF OREGON
EUGENE, OR 97403