Mathematical Case Studies: the Geometric Algebra*

Rob Arthan

30 December 2016

Abstract

This document is one of a series of mathematical case studies in ProofPower-HOL. It gives a construction of the Geometric Algebra GA.

Reference: LEMMA1/HOL/WRK076; Current git revision: b0522be

*First posted 30 October 2006; for full changes history see: `https://github.com/RobArthan/pp-contrib`.

Contents

1 INTRODUCTION

In [2], Harrison advocates an approach to Euclidean geometry in HOL using a type constructor to model the individual Euclidean spaces $\mathbb{R}^N$, for finite N. In this document, we set up the framework for an alternative approach where one works in a fixed type that contains all of the $\mathbb{R}^n$ for all $n \in \mathbb{N}$. In fact we do more than that: we construct a system which can be viewed as the natural and in some sense final algebraic structure in the chain that begins $\mathbb{N}, Z, Q, R, C, \ldots$. This structure is known as the *geometric algebra*. To quote Macdonald [4]:

> *Geometric algebra is nothing less than a new approach to geometry. Geometric objects (points, lines, planes, [...]) are represented by members of an algebra, a* geometric algebra*, rather than by equations. Geometric operations (rotate, translate, intersect, [...]) on the objects are represented by algebraic operations in the algebra, rather than by matrix operations. Geometric algebra is* coordinate-free: *coordinates are needed only when specific objects or operations are under consideration.*

Let me now give a potted account of geometric algebra. The finite-dimensional geometric algebra $\mathsf{GA}(n)$ is paremeterised by the natural numbers n. $\mathsf{GA}(n)$ is an associative algebra over the real numbers with a two-sided unit $\mathbf{1}$. It is commutative iff. $n \leq 1$. Not all elements of $\mathsf{GA}(n)$ have multiplicative inverses, but many do and if $\mathbf{x}$ does have an inverse, it is written as $\mathbf{x}^{-1}$.

Real multiples $\lambda\mathbf{1}$ of the unit element in $\mathsf{GA}(n)$ are called *scalars* and are ordered by taking $\lambda\mathbf{1} < \mu\mathbf{1}$ iff. $\lambda < \mu$. Under this ordering, the subalgebra of scalars is isomorphic as an ordered field with the real numbers.

$\mathsf{GA}(n)$ is generated as an algebra by an n-dimensional subspace called $\mathbb{R}^n$ whose members are called *vectors*. If $\mathbf{x} \in \mathbb{R}^n$, then $\mathbf{x}^2$ is a scalar. It is easy to see that every non-zero vector has an inverse.

The *inner product* of vectors $\mathbf{x}$ and $\mathbf{y}$ is defined by $\mathbf{x}.\mathbf{y} = \frac{1}{2}(\mathbf{xy} + \mathbf{yx})$ and is a scalar. The inner product is a bilinear form, i.e., it satisfies the conditions $(\lambda\mathbf{x}).(\mu\mathbf{y}) = (\lambda\mu)(\mathbf{x}.\mathbf{y})$, $(\mathbf{x}+\mathbf{y}).\mathbf{z} = \mathbf{x}.\mathbf{z}+\mathbf{y}.\mathbf{z}$, $\mathbf{x}.(\mathbf{y}+\mathbf{z}) = \mathbf{x}.\mathbf{y}+\mathbf{x}.\mathbf{z}$. Vectors $\mathbf{x}$ and $\mathbf{y}$ are said to be *orthogonal* iff. $\mathbf{x}.\mathbf{y} = 0$. $\mathbf{x}$ and $\mathbf{y}$ are orthogonal iff. they anti-commute, i.e., iff. $\mathbf{xy} = -\mathbf{yx}$.

The *outer product* of vectors $\mathbf{x}$ and $\mathbf{y}$ is defined by $\mathbf{x} \wedge \mathbf{y} = \frac{1}{2}(\mathbf{xy} - \mathbf{yx})$, so that $\mathbf{xy} = \mathbf{x}.\mathbf{y} + \mathbf{x} \wedge \mathbf{y}$, which is a scalar iff. it is 0. Vectors $\mathbf{x}$ and $\mathbf{y}$ are said to be *collinear* iff. $\mathbf{x} \wedge \mathbf{y} = 0$. Thus, when $\mathbf{x}$ and $\mathbf{y}$ are orthogonal, $\mathbf{xy} = \mathbf{x} \wedge \mathbf{y}$, while when they are collinear, $\mathbf{xy} = \mathbf{x}.\mathbf{y}$.

In traditional vector algebra, the inner and outer products are taken as separate fundamental notions, but in the geometric algebra, the multiplication combines them into a united whole. But the multiplication does much more than this. As one example, we may think of a vector $\mathbf{x}$ as defining a notion of direction and magnitude in the line comprising all points $\lambda\mathbf{x}$ for $\lambda \in \mathbb{R}$. Now, if $\mathbf{x}$ and $\mathbf{y}$ are orthogonal vectors, one can think of the product $\mathbf{xy}$ as defining a notion of orientation and area in the plane spanned by $\mathbf{x}$ and $\mathbf{y}$. More general products $\mathbf{x}_1\mathbf{x}_2\ldots\mathbf{x}_k$ of k pairwise orthogonal vectors are called k-blades and can be thought of as providing an oriented notion of volume in the k-dimensional space spanned by the $\mathbf{x}_i$.

For another example on the power of the geometric algebra, let $\mathsf{O}(n)$ denote the set of all orthogonal mappings from the subspace $\mathbb{R}^n$ to itself (where, by definition, an orthogonal mapping is one which preserves all inner products). In linear algebra, $\mathsf{O}(n)$ is shown, with some considerable coordinate-rich work, to be given by a certain group of $n \times n$ matrices.

Now geometrically, it is not hard to see that $\mathsf{O}(n)$ is generated by reflections in hyperplanes, and then in the geometric algebra it is very easy to see that, for each non-zero vector $\mathbf{y}$, the mapping $\mathbf{x} \mapsto -\mathbf{yxy}^{-1}$ maps $\mathbb{R}^n$ to itself via reflection in the hyperplane perpendicular to $\mathbf{y}$. Thus the geometric algebra instantly gives us a notation for orthogonal mappings without a coordinate or a matrix in sight. In fact, $\mathsf{GA}(n)$ has a multiplicative subgroup, $\mathsf{Pin}(n)$, which is the universal covering group of the topological group $\mathsf{O}(n)$. (As a topological space, $\mathsf{Pin}(n)$ has two connected components. The component of $\mathsf{Pin}(n)$ containing 1 is the *spinor* group $\mathsf{Spin}(n)$ beloved of physicists.)

The above discussion deals with the case of a positive definite orthogonal space $\mathbb{R}^n$. There is also much interest in semidefinite orthogonal spaces in which $\mathbf{x.x}$ can be negative and earlier drafts of this document did indeed follow the construction of [1]. However, for simplicity, it now deals with the positive definite case only[1].

Simple explicit constructions of the geometric algebras have been given by Macdonald [3], and by the author [1]. As noted in [1] the union of all of the $\mathsf{GA}(n)$ can be constructed in one step giving what I will now refer to as *the* geometric algebra, $\mathsf{GA} = \mathsf{GA}(\infty)$.

SML

```
force_delete_theory"geomalg" handle Fail _ => ();
open_theory"numbers";
new_theory"geomalg";
set_merge_pcs["basic_hol1", "'sets_alg", "'ℝ"];
```

2 THE GEOMETRIC ALGEBRA

2.1 Preliminaries

It is very convenient to have available the symmetric difference operator for sets. We follow Z in writing the symmetric difference of a and b as $a \ominus b$. This operator is provided in ProofPower as pf version 2.7.7 so some ML trickery is used here to suppress the following definitions when they are not needed.

SML

```
declare_infix(250, "⊖");
```

HOL Constant

```
$⊖ : 'a SET → 'a SET → 'a SET
────────────────────────────
∀a b• a ⊖ b = (a \ b) ∪ (b \ a)
```

The development of the theory begins with various simple facts about symmetric differences. Symmetric difference makes the lattice of sets into a commutative group. The script includes a conversion $\ominus$*_nf_conv* which gives a normal form for this group.

⊖*_group_thm*	⊖*_lemmas*	⊖*_finite_size_thm*
⊖*_comm_thm*	⊖*_finite_thm*	⊖*_infinite_thm*
⊖*_assoc_thm*	*size_*⊖*_lemma*	

[1]In fact, $\mathsf{GA}(\infty,\infty)$ is isomorphic to a subalgebra of $\mathsf{GA}(\infty)$ and we propose to work in such a subalgebra to deal with the semidefinite case. A suitable subalgebra is the one generated by the elements $f_0 = e_0, f_{(-1)} = e_{123}, f_1 = e_4, f_{(-2)} = e_{567}, f_2 = e_8, \ldots$. If one makes the $f_i, i \in \mathbb{Z}$, take the rôle of the e_i that generate $\mathsf{GA}(\infty,\infty)$ in [1], then it is routine to check that the generators obey the laws of $\mathsf{GA}(\infty,\infty)$.

The following is based on the function σ of [1] for use in specifying the multiplication in GA.

HOL Constant

$$\boldsymbol{Sign_G} : \mathbb{N}\ SET \to \mathbb{N}\ SET \to \mathbb{R}$$

$$\forall\ I\ J \bullet \quad Sign_G\ I\ J = \sim(\mathbb{NR}\ 1)\ \hat{}\ \#\{(i,\ j)\ |\ i \in I \land j \in J \land j < i\}$$

After a lemma, we have *sign_g_thm* which is lemma 1 of [1]. The proof given is a little bit more long-winded and general than the simplified version recorded in [1]. As a utility we also have the theorem that says the values taken on by σ are ± 1 and the calculations that give the values of $\mathbf{e}_i^2$ and $\mathbf{e}_i\mathbf{e}_j$.

ℝ_ℕ_*exp_mod_2_thm*	*sign_g_cases_thm*	*sign_singletons_thm*
sign_g_thm	*sign_singleton_thm*	

2.2 The Type Definition

GA in HOL will be a subtype of the type of all real-valued functions on sets of natural numbers (specifically, it will comprise the functions whose support is a finite set of finite sets). The following type abbreviation captures this.

SML

```
declare_type_abbrev("_GA", [], ⌜:ℕ SET → ℝ⌝);
```

HOL Constant

$$\boldsymbol{\_IsGARep} : \_GA \to BOOL$$

$$\forall u \bullet\ \_IsGARep\ u \Leftrightarrow Supp\ u \in Finite \land Supp\ u \subseteq Finite$$

We can now introduce the new type:

SML

```
val ga_def = new_type_defn(["GA", "ga_def"], "GA", [],
        tac_proof(([], ⌜∃u• _IsGARep u⌝),
                ∃_tac⌜(λI•ℕℝ 0)⌝
        THEN rewrite_tac[get_spec⌜_IsGARep⌝, get_spec⌜Supp⌝,
                pc_rule1"sets_ext" prove_rule[]⌜{x|F} = {}⌝,
                empty_finite_thm]));
```

2.3 Specifying the Operations on the Type

We now introduce the operations on the type GA. First of all, we define the fixity of the infix operators.

SML

```
app declare_infix[(300, "+_G"), (310, "*_G"), (310, "*_S")];
```

Now we define the operations. The following is adapted from definition 2 of [1]. The function Mon_G maps a finite set of natural numbers I to the monomial basis element $\mathbf{e}_I$ of [1]. The definition has four conjuncts: the first conjunct says that GA is an associative real algebra with a two-sided unit (cf. the check-list in [3]); the second conjunct gives the rule for multiplying monomials; the third conjunct says that the monomials $Mon_G\ I$ as I ranges over finite sets of natural numbers generate GA as a linear space, or, more precisely, it says that if V is a linear subspace of GA that contains each of these monomials, then V = GA; the final conjunct says that the monomials $Mon_G\ I$ as I ranges over finite sets of natural numbers are linearly independent, or more precisely, it says that for each J, there is a linear subspace of GA that contains $Mon_G\ I$ for all $I \neq J$, but does not contain $Mon_G\ J$.

HOL Constant

$$
\begin{array}{lll}
\$\boldsymbol{+_G} : GA \to GA \to GA; & \boldsymbol{\sim_G} : GA \to GA; & \mathbf{0_G} : GA; \\
 & \$\boldsymbol{*_S} : \mathbb{R} \to GA \to GA; & \\
\$\boldsymbol{*_G} : GA \to GA \to GA; & \mathbf{1_G} : GA; & \boldsymbol{Mon_G} : \mathbb{N}\ SET \to GA
\end{array}
$$

$$
\begin{array}{lll}
(\forall u\ v\ w\ a\ b \bullet & & \\
 & & u +_G v = v +_G u \\
 & \wedge & (u +_G v) +_G w = u +_G v +_G w \\
 & \wedge & u +_G 0_G = u \wedge u +_G \sim_G u = 0_G \\
 & \wedge & \mathbb{NR}\ 1 *_S u = u \wedge a *_S (b *_S u) = (a * b) *_S u \\
 & \wedge & a *_S (u +_G v) = a *_S u +_G a *_S v \\
 & \wedge & (a + b) *_S u = a *_S u +_G b *_S u \\
 & \wedge & (u *_G v) *_G w = u *_G (v *_G w) \\
 & \wedge & u *_G (v +_G w) = u *_G v +_G u *_G w \\
 & \wedge & (v +_G w) *_G u = v *_G u +_G w *_G u \\
 & \wedge & (a *_S u) *_G v = a *_S u *_G v \\
 & \wedge & u *_G (a *_S v) = a *_S u *_G v \\
 & \wedge & 1_G *_G u = u \wedge u *_G 1_G = u \wedge 1_G = Mon_G\ \{\}) \\
\wedge\ (\forall I\ J \bullet & & I \in Finite \wedge J \in Finite \\
 & \Rightarrow & Mon_G\ I *_G Mon_G\ J = Sign_G\ I\ J *_S Mon_G(I \ominus J)) \\
\wedge\ (\forall V \bullet & & (\forall I \bullet\ I \in Finite \Rightarrow Mon_G\ I \in V) \\
 & \wedge & (\forall a\ u \bullet\ u \in V \Rightarrow a *_S u \in V) \\
 & \wedge & (\forall u\ v \bullet\ u \in V \wedge v \in V \Rightarrow u +_G v \in V) \\
 & \Rightarrow & (\forall u \bullet\ u \in V)) \\
\wedge\ (\forall J \bullet & & J \in Finite \\
 & \Rightarrow & \exists V \bullet\quad (\forall I \bullet\ \neg I = J \wedge I \in Finite \Rightarrow Mon_G\ I \in V) \\
 & & \wedge\quad (\forall a\ u \bullet\ u \in V \Rightarrow a *_S u \in V) \\
 & & \wedge\quad (\forall u\ v \bullet\ u \in V \wedge v \in V \Rightarrow u +_G v \in V) \\
 & & \wedge\quad \neg Mon_G\ J \in V)
\end{array}
$$

We now define various derived operations. The first two are binary subtraction and exponentiation with a natural number exponent:

SML

```
declare_infix(305, "-_G");
```

HOL Constant

$\$-_G : GA \to GA \to GA$

$\forall u\ v \bullet\ u -_G v = u +_G \sim_G v$

SML

```
declare_infix(320, "^_G");
```

HOL Constant

$\$\hat{}_G : GA \to \mathbb{N} \to GA$

$(\forall u \bullet\ u\ \hat{}_G\ 0 = 1_G)$
$\wedge\quad (\forall u\ m \bullet\ u\ \hat{}_G\ (m+1) = u *_G u\ \hat{}_G\ m)$

The function E_G that maps an natural number i to the element $\mathbf{e}_i$ of [1].

HOL Constant

$\boldsymbol{E_G} : \mathbb{N} \to GA$

$\forall\ m \bullet\ E_G\ m = Mon_G\ \{m\}$

The following function gives the embedding of the naturals in GA. (Since it is so widely used, we will usually use the alias Γ for this function, see below).

HOL Constant

$\mathbb{N}_G : \mathbb{N} \to GA$

$\mathbb{N}_G\ 0 = 0_G \wedge \forall\ m \bullet\ \mathbb{N}_G\ (m+1) = \mathbb{N}_G\ m +_G 1_G$

We now define aliases for the embedding of the naturals and for the ring operations on GA etc., (but not for the scalar multiplication since that does not work well with the current treatment of overloading in ProofPower-HOL).

SML

```
declare_alias("Γ", ⌜ℕ_G⌝);
declare_alias("+", ⌜$+_G⌝);
declare_alias("*", ⌜$*_G⌝);
declare_alias("~", ⌜~_G⌝);
declare_alias("-", ⌜$-_G⌝);
declare_alias("^", ⌜$^_G⌝);
```

Many of the theorems in the following block mimic ones provided in the developmet of the real numbers, up to the point where the non-commutativity of multiplication in GA begins to make a significant difference.

ga_ops_def	*ga_scale_scale_assoc_thm*	*ga_minus_eq_thm*
ga_plus_assoc_thm	*ga_scale_plus_distrib_thm*	*ga_0_times_thm*
ga_plus_comm_thm	*ga_plus_scale_distrib_thm*	*ga_0_scale_thm*
ga_plus_zero_thm	*ga_times_assoc_thm*	*ga_scale_0_thm*
ga_plus_order_thm	*ga_times_plus_distrib_thm*	*ga_minus_1_scale_thm*
ga_plus_0_thm	*ga_plus_times_distrib_thm*	*ga_ℕ_exp_clauses*
ga_0_1_thm	*ga_scale_times_assoc_thm*	*ga_minus_scale_thm*
ga_plus_minus_thm	*ga_one_times_thm*	*ga_scale_minus_thm*
ga_eq_thm	*ga_times_one_thm*	*ga_one_mon_thm*
Γ_plus_homomorphism_thm	*ga_mon_times_mon_thm*	*ga_mon_span_thm*
ga_one_scale_thm	*ga_minus_clauses*	*ga_mon_indep_thm*

2.4 Some Linear Space Notions

(Note: we use the term *linear space* for the usual notion of a vector space to avoid confusion with the privileged role of the 1-vectors in GA).

We define the notion of a linear subspace of GA:

HOL Constant

$$\boldsymbol{Subspace_G} : GA\ SET\ SET$$

$$\begin{array}{lll} \forall V \bullet & V \in Subspace_G \Leftrightarrow & \\ & & 0_G \in V \\ & \wedge & (\forall a\ u \bullet\ u \in V \Rightarrow a *_S u \in V) \\ & \wedge & (\forall u\ v \bullet\ u \in V \wedge v \in V \Rightarrow u + v \in V) \end{array}$$

The linear space spanned by a subset of GA is defined as follows:

HOL Constant

$$\boldsymbol{Span_G} : GA\ SET \to GA\ SET$$

$$\forall X \bullet\quad Span_G\ X = \bigcap \{ V \mid V \in Subspace_G \wedge X \subseteq V \}$$

A set X is linearly independent iff. the spans of its proper subsets are proper subsets of its span.

HOL Constant

$$\boldsymbol{Indep_G} : GA\ SET\ SET$$

$$\forall X \bullet\ X \in Indep_G \Leftrightarrow \forall Y \bullet Y \subseteq X \wedge Span_G\ Y = Span_G\ X \Rightarrow Y = X$$

finite_friend_thm	*ga_vec_indep_thm*	*ga_span_mon_thm*
ga_mon_not_0_thm	*ga_span_subspace_thm*	*ga_span_mono_thm*
ga_mon_1_thm	*ga_⊆_span_thm*	*ga_indep_thm*
ga_mon_subgroup_thm	*ga_span_⊆_thm*	*ga_mon_indep_thm1*
ga_vec_generators_thm	*ga_trivial_subspaces_thm*	
ga_vec_relations_thm	*ga_mon_span_bc_thm*	

2.5 Some Simple Geometric Notions

In this section we define some simple geometric notions. We restrict some of these to vectors, the set of vectors being the span of the $\mathbf{e}_i$.

HOL Constant

$$\$\boldsymbol{Vector_G} : GA\ SET$$

$$Vector_G = Span_G\ \{e \mid \exists m \bullet e = E_G\ m\}$$

Vectors u and v are orthogonal, written $u \perp v$, if they anticommute:

SML

$$declare\_infix(200,\ \texttt{"}\perp\texttt{"});$$

HOL Constant

$$\$\perp : GA \to GA \to BOOL$$

$$\forall u\ v \bullet\ u \perp v \Leftrightarrow u \in Vector_G \land v \in Vector_G \land u * v = \sim v * u$$

With these definitions in hand, it is purely a matter of algebra to prove the theorem of Pythagoras, which in the geometric algebra becomes a theorem about the squares *of* the sides, not the squares *on* the sides:

$$pythagoras\_thm \vdash \forall\ u\ v{:}\ GA \bullet\ u \perp v \Rightarrow (u - v)\ \hat{}\ 2 = u\ \hat{}\ 2 + v\ \hat{}\ 2$$

References

[1] R.D. Arthan. A Minimalist Construction of the Geometric Algebra. *arXiv:math.RA/00607190 v2*, July 2006.

[2] John Harrison. A HOL Theory of Euclidean Space. In Joe Hurd and Thomas F. Melham, editors, *TPHOLs*, volume 3603 of *Lecture Notes in Computer Science*, pages 114–129. Springer, 2005.

[3] Alan Macdonald. An Elementary Construction of the Geometric Algebra, 2002. Adv. Appl. Cliff. Alg. 12, 1-6 (2002).

[4] Alan Macdonald. A Survey of Geometric Algebra and Geometric Calculus, 2006. http://faculty.luther.edu/m̃acdonald.

3 OPERATIONS ON THE REPRESENTATION TYPE

The proof of the consistency of the specification of the operations of GA in section 2.3 is made tolerable by introducing constants for the representatives of the operations on the representation type. This appendix gives the definitons of these operations.

We adopt the convention of using an initial '_' to distinguish operations on the representation type from corresponding operations on the new type.

SML

$declare\_infix(300,\ "\_+_G");$

HOL Constant

$\$\_\mathbf{+_G} : \_GA \to \_GA \to \_GA$

$\forall\ v\ w \bullet\ v\ \_+_G\ w = \lambda K \bullet\ v\ K\ +\ w\ K$

HOL Constant

$\_\mathbf{\sim_G} : \_GA \to \_GA$

$\forall\ v \bullet\ \_\sim_G\ v = \lambda K \bullet\ \sim(v\ K)$

SML

$declare\_infix(310,\ "\_*_G");$

HOL Constant

$\$\_\mathbf{*_G} : \_GA \to \_GA \to \_GA$

$$\begin{array}{l}\forall\ v\ w \bullet \\ \qquad v\ \_*_G\ w = \lambda K \bullet \\ \qquad \Sigma\ \{(I,\ J)\ |\ I \in Supp\ v \land J \in Supp\ w \land K = I \ominus J\} \\ \qquad (\lambda(I,\ J) \bullet\ Sign_G\ I\ J * v\ I * w\ J)\end{array}$$

SML

$declare\_infix(310,\ "\_*_S");$

HOL Constant

$\$\_\mathbf{*_S} : \mathbb{R} \to \_GA \to \_GA$

$\forall\ c\ v \bullet\ c\ \_*_S\ v = \lambda K \bullet c * v\ K$

HOL Constant

$\_\mathbf{0_G} : \_GA$

$\_0_G = \lambda K \bullet\ \mathbb{NR}\ 0$

HOL Constant

$\_\mathbf{1_G} : \_GA$

$\_1_G = \chi\{\{\}\}$

A THEOREMS IN THE THEORY geomalg

$\ominus$**_group_thm** $\vdash \forall\ a\ b\ c$
$\bullet\ a \ominus \{\} = a$
$\wedge\ \{\} \ominus a = a$
$\wedge\ a \ominus b = b \ominus a$
$\wedge\ a \ominus b \ominus c = (a \ominus b) \ominus c$

$\ominus$**_comm_thm** $\vdash \forall\ a\ b \bullet\ a \ominus b = b \ominus a$

$\ominus$**_assoc_thm** $\vdash \forall\ a\ b\ c \bullet\ (a \ominus b) \ominus c = a \ominus b \ominus c$

$\ominus$**_lemmas** $\vdash \forall\ a\ b$
$\bullet\ a \ominus \{\} = a \wedge \{\} \ominus a = a \wedge a \ominus a = \{\} \wedge a \ominus a = \{\}$

$\ominus$**_finite_thm** $\vdash \forall\ a\ b \bullet\ a \in \mathit{Finite} \wedge b \in \mathit{Finite} \Rightarrow a \ominus b \in \mathit{Finite}$

size_$\ominus$**_lemma** $\vdash \forall\ f\ a\ b$
$\bullet\ f\ \{\} = 0$
$\wedge\ (\forall\ a\ b$
$\bullet\ a \in \mathit{Finite} \wedge b \in \mathit{Finite}$
$\Rightarrow f\ (a \cup b) + f\ (a \cap b) = f\ a + f\ b)$
$\wedge\ a \in \mathit{Finite}$
$\wedge\ b \in \mathit{Finite}$
$\Rightarrow f\ (a \ominus b) + 2 * f\ (a \cap b) = f\ a + f\ b$

$\ominus$**_finite_size_thm**
$\vdash \forall\ a\ b$
$\bullet\ a \in \mathit{Finite} \wedge b \in \mathit{Finite}$
$\Rightarrow a \ominus b \in \mathit{Finite}$
$\wedge\ \#\ (a \ominus b) + 2 * \#\ (a \cap b) = \#\ a + \#\ b$

$\ominus$**_infinite_thm**
$\vdash \forall\ a\ b \bullet\ \neg\ a \in \mathit{Finite} \wedge b \in \mathit{Finite} \Rightarrow \neg\ a \ominus b \in \mathit{Finite}$

$\mathbb{R}$_$\mathbb{N}$**_exp_mod_2_thm**
$\vdash \forall\ m \bullet\ \sim 1.\ \hat{}\ m = \sim 1.\ \hat{}\ (m\ \mathit{Mod}\ 2)$

sign_g_thm $\vdash \forall\ I\ J\ K$
$\bullet\ I \in \mathit{Finite} \wedge J \in \mathit{Finite} \wedge K \in \mathit{Finite}$
$\Rightarrow \mathit{Sign}_G\ I\ J * \mathit{Sign}_G\ (I \ominus J)\ K$
$= \mathit{Sign}_G\ I\ (J \ominus K) * \mathit{Sign}_G\ J\ K$

sign_g_cases_thm
$\vdash \forall\ I\ J \bullet\ \mathit{Sign}_G\ I\ J = 1. \vee \mathit{Sign}_G\ I\ J = \sim 1.$

sign_singleton_thm
$\vdash \forall\ i \bullet\ \mathit{Sign}_G\ \{i\}\ \{i\} = 1.$

sign_singletons_thm
$\vdash \forall\ i\ j$
$\bullet\ \neg\ i = j$
$\Rightarrow \mathit{Sign}_G\ \{i\}\ \{j\} = (\mathit{if}\ i < j\ \mathit{then}\ 1.\ \mathit{else} \sim 1.)$

app_if_thm $\vdash \forall\ p\ f\ g\ x$
$\bullet\ (\mathit{if}\ p\ \mathit{then}\ f\ \mathit{else}\ g)\ x = (\mathit{if}\ p\ \mathit{then}\ f\ x\ \mathit{else}\ g\ x)$

$+_G$**_consistent**
$\sim_G$**_consistent**
0_G**_consistent**
$*_S$**_consistent**
$*_G$**_consistent**
1_G**_consistent**
Mon_G**_consistent**
$\vdash \mathit{Consistent}$

$$
\begin{array}{l}
(\lambda\ ({+_G}',\ {\sim_G}',\ {\mathit{0}_G}',\ {*_S}',\ {*_G}',\ {\mathit{1}_G}',\ {\mathit{Mon}_G}') \\
\quad \bullet\ (\forall\ u\ v\ w\ a\ b \\
\qquad \bullet\ {+_G}'\ u\ v = {+_G}'\ v\ u \\
\qquad\quad \land\ {+_G}'\ ({+_G}'\ u\ v)\ w = {+_G}'\ u\ ({+_G}'\ v\ w) \\
\qquad\quad \land\ {+_G}'\ u\ {\mathit{0}_G}' = u \\
\qquad\quad \land\ {+_G}'\ u\ ({\sim_G}'\ u) = {\mathit{0}_G}' \\
\qquad\quad \land\ {*_S}'\ \mathit{1.}\ u = u \\
\qquad\quad \land\ {*_S}'\ a\ ({*_S}'\ b\ u) = {*_S}'\ (a * b)\ u \\
\qquad\quad \land\ {*_S}'\ a\ ({+_G}'\ u\ v) \\
\qquad\qquad = {+_G}'\ ({*_S}'\ a\ u)\ ({*_S}'\ a\ v) \\
\qquad\quad \land\ {*_S}'\ (a + b)\ u \\
\qquad\qquad = {+_G}'\ ({*_S}'\ a\ u)\ ({*_S}'\ b\ u) \\
\qquad\quad \land\ {*_G}'\ ({*_G}'\ u\ v)\ w = {*_G}'\ u\ ({*_G}'\ v\ w) \\
\qquad\quad \land\ {*_G}'\ u\ ({+_G}'\ v\ w) \\
\qquad\qquad = {+_G}'\ ({*_G}'\ u\ v)\ ({*_G}'\ u\ w) \\
\qquad\quad \land\ {*_G}'\ ({+_G}'\ v\ w)\ u \\
\qquad\qquad = {+_G}'\ ({*_G}'\ v\ u)\ ({*_G}'\ w\ u) \\
\qquad\quad \land\ {*_G}'\ ({*_S}'\ a\ u)\ v = {*_S}'\ a\ ({*_G}'\ u\ v) \\
\qquad\quad \land\ {*_G}'\ u\ ({*_S}'\ a\ v) = {*_S}'\ a\ ({*_G}'\ u\ v) \\
\qquad\quad \land\ {*_G}'\ {\mathit{1}_G}'\ u = u \\
\qquad\quad \land\ {*_G}'\ u\ {\mathit{1}_G}' = u \\
\qquad\quad \land\ {\mathit{1}_G}' = {\mathit{Mon}_G}'\ \{\}) \\
\qquad \land\ (\forall\ I\ J \\
\qquad \bullet\ I \in \mathit{Finite} \land J \in \mathit{Finite} \\
\qquad\quad \Rightarrow {*_G}'\ ({\mathit{Mon}_G}'\ I)\ ({\mathit{Mon}_G}'\ J) \\
\qquad\qquad = {*_S}'\ (\mathit{Sign}_G\ I\ J)\ ({\mathit{Mon}_G}'\ (I \ominus J))) \\
\qquad \land\ (\forall\ V \\
\qquad \bullet\ (\forall\ I \bullet\ I \in \mathit{Finite} \Rightarrow {\mathit{Mon}_G}'\ I \in V) \\
\qquad\qquad \land\ (\forall\ a\ u \bullet\ u \in V \Rightarrow {*_S}'\ a\ u \in V) \\
\qquad\qquad \land\ (\forall\ u\ v \bullet\ u \in V \land v \in V \Rightarrow {+_G}'\ u\ v \in V) \\
\qquad\quad \Rightarrow (\forall\ u \bullet\ u \in V)) \\
\qquad \land\ (\forall\ J \\
\qquad \bullet\ J \in \mathit{Finite} \\
\qquad\quad \Rightarrow (\exists\ V \\
\qquad\quad \bullet\ (\forall\ I \\
\qquad\qquad \bullet\ \neg\ I = J \land I \in \mathit{Finite} \\
\qquad\qquad\quad \Rightarrow {\mathit{Mon}_G}'\ I \in V) \\
\qquad\qquad \land\ (\forall\ a\ u \bullet\ u \in V \Rightarrow {*_S}'\ a\ u \in V) \\
\qquad\qquad \land\ (\forall\ u\ v \\
\qquad\qquad \bullet\ u \in V \land v \in V \Rightarrow {+_G}'\ u\ v \in V) \\
\qquad\qquad \land\ \neg\ {\mathit{Mon}_G}'\ J \in V)))
\end{array}
$$

ga_ops_def $\vdash (\forall\ u\ v\ w\ a\ b$

$$
\begin{array}{l}
\bullet\ u + v = v + u \\
\quad \land\ (u + v) + w = u + v + w \\
\quad \land\ u + \mathit{0}_G = u \\
\quad \land\ u + \sim u = \mathit{0}_G \\
\quad \land\ \mathit{1.}\ *_S\ u = u \\
\quad \land\ a *_S b *_S u = (a * b) *_S u \\
\quad \land\ a *_S (u + v) = a *_S u + a *_S v \\
\quad \land\ (a + b) *_S u = a *_S u + b *_S u \\
\quad \land\ (u * v) * w = u * v * w
\end{array}
$$

$\land\ u * (v + w) = u * v + u * w$
$\land\ (v + w) * u = v * u + w * u$
$\land\ (a *_S u) * v = a *_S u * v$
$\land\ u * a *_S v = a *_S u * v$
$\land\ 1_G * u = u$
$\land\ u * 1_G = u$
$\land\ 1_G = Mon_G\ \{\})$
$\land\ (\forall\ I\ J$
$\bullet\ I \in Finite \land J \in Finite$
$\Rightarrow Mon_G\ I * Mon_G\ J$
$= Sign_G\ I\ J *_S Mon_G\ (I \ominus J))$
$\land\ (\forall\ V$
$\bullet\ (\forall\ I \bullet\ I \in Finite \Rightarrow Mon_G\ I \in V)$
$\land\ (\forall\ a\ u \bullet\ u \in V \Rightarrow a *_S u \in V)$
$\land\ (\forall\ u\ v \bullet\ u \in V \land v \in V \Rightarrow u + v \in V)$
$\Rightarrow (\forall\ u \bullet\ u \in V))$
$\land\ (\forall\ J$
$\bullet\ J \in Finite$
$\Rightarrow (\exists\ V$
$\bullet\ (\forall\ I \bullet\ \neg\ I = J \land I \in Finite \Rightarrow Mon_G\ I \in V)$
$\land\ (\forall\ a\ u \bullet\ u \in V \Rightarrow a *_S u \in V)$
$\land\ (\forall\ u\ v \bullet\ u \in V \land v \in V \Rightarrow u + v \in V)$
$\land\ \neg\ Mon_G\ J \in V))$

ga_plus_assoc_thm
$\vdash \forall\ u\ v\ w \bullet\ (u + v) + w = u + v + w$

***ga_plus_assoc_thm*1**
$\vdash \forall\ u\ v\ w \bullet\ u + v + w = (u + v) + w$

ga_plus_comm_thm
$\vdash \forall\ u\ v \bullet\ u + v = v + u$

ga_plus_zero_thm
$\vdash \forall\ u \bullet\ u + 0_G = u$

ga_plus_order_thm
$\vdash \forall\ x\ y\ z$
$\bullet\ y + x = x + y$
$\land\ (x + y) + z = x + y + z$
$\land\ y + x + z = x + y + z$

ga_plus_0_thm
$\vdash \forall\ x \bullet\ x + \Gamma\ 0 = x \land \Gamma\ 0 + x = x$

ga_0_1_thm $\vdash 0_G = \Gamma\ 0 \land 1_G = \Gamma\ 1$

ga_plus_minus_thm
$\vdash \forall\ x \bullet\ x + \sim x = \Gamma\ 0 \land \sim x + x = \Gamma\ 0$

ga_eq_thm $\vdash \forall\ x\ y \bullet\ x = y \Leftrightarrow x + \sim y = \Gamma\ 0$

Γ_plus_homomorphism_thm
$\vdash \forall\ m\ n \bullet\ \Gamma\ (m + n) = \Gamma\ m + \Gamma\ n$

ga_one_scale_thm
$\vdash \forall\ u \bullet\ 1. *_S u = u$

ga_scale_scale_assoc_thm
$\vdash \forall\ a\ b\ u \bullet\ a *_S b *_S u = (a * b) *_S u$

ga_scale_plus_distrib_thm
$\vdash \forall\ a\ u\ v \bullet\ a *_S (u + v) = a *_S u + a *_S v$

ga_plus_scale_distrib_thm

$\vdash \forall\ a\ b\ u\bullet\ (a\ +\ b)\ *_S\ u\ =\ a\ *_S\ u\ +\ b\ *_S\ u$

ga_times_assoc_thm

$\vdash \forall\ u\ v\ w\bullet\ (u\ *\ v)\ *\ w\ =\ u\ *\ v\ *\ w$

ga_times_plus_distrib_thm

$\vdash \forall\ u\ v\ w\bullet\ u\ *\ (v\ +\ w)\ =\ u\ *\ v\ +\ u\ *\ w$

ga_plus_times_distrib_thm

$\vdash \forall\ v\ w\ u\bullet\ (v\ +\ w)\ *\ u\ =\ v\ *\ u\ +\ w\ *\ u$

ga_scale_times_assoc_thm

$\vdash \forall\ a\ u\ v\bullet\ (a\ *_S\ u)\ *\ v\ =\ a\ *_S\ u\ *\ v$

ga_times_scale_assoc_thm

$\vdash \forall\ u\ a\ v\bullet\ u\ *\ a\ *_S\ v\ =\ a\ *_S\ u\ *\ v$

ga_one_times_thm

$\vdash \forall\ u\bullet\ \mathit{\Gamma}\ \mathit{1}\ *\ u\ =\ u$

ga_times_one_thm

$\vdash \forall\ u\bullet\ u\ *\ \mathit{\Gamma}\ \mathit{1}\ =\ u$

ga_one_mon_thm

$\vdash \mathit{\Gamma}\ \mathit{1}\ =\ \mathit{Mon}_G\ \{\}$

ga_minus_clauses

$$\begin{aligned}
&\vdash \forall\ x\ y\\
&\quad \bullet \sim (\sim x)\ =\ x\\
&\qquad \wedge\ x\ +\ \sim x\ =\ \mathit{\Gamma}\ \mathit{0}\\
&\qquad \wedge\ \sim x\ +\ x\ =\ \mathit{\Gamma}\ \mathit{0}\\
&\qquad \wedge\ \sim (x\ +\ y)\ =\ \sim x\ +\ \sim y\\
&\qquad \wedge\ \sim (\mathit{\Gamma}\ \mathit{0})\ =\ \mathit{\Gamma}\ \mathit{0}
\end{aligned}$$

ga_minus_eq_thm

$\vdash \forall\ x\ y\bullet\ \sim x\ =\ \sim y \Leftrightarrow x\ =\ y$

ga_0_times_thm

$\vdash \forall\ u\bullet\ \mathit{\Gamma}\ \mathit{0}\ *\ u\ =\ \mathit{\Gamma}\ \mathit{0}$

ga_0_scale_thm

$\vdash \forall\ u\bullet\ \mathit{0.}\ *_S\ u\ =\ \mathit{\Gamma}\ \mathit{0}$

ga_scale_0_thm

$\vdash \forall\ a\bullet\ a\ *_S\ \mathit{\Gamma}\ \mathit{0}\ =\ \mathit{\Gamma}\ \mathit{0}$

ga_minus_1_scale_thm

$\vdash \forall\ u\bullet\ \sim \mathit{1.}\ *_S\ u\ =\ \sim u$

ga_ℕ_exp_clauses

$\vdash \forall\ u\bullet\ u\ \hat{}\ \mathit{0}\ =\ \mathit{\Gamma}\ \mathit{1}\ \wedge\ u\ \hat{}\ \mathit{1}\ =\ u\ \wedge\ u\ \hat{}\ \mathit{2}\ =\ u\ *\ u$

ga_minus_scale_thm

$\vdash \forall\ u\bullet\ \sim u\ =\ \sim \mathit{1.}\ *_S\ u$

ga_scale_minus_thm

$\vdash \forall\ u\bullet\ \sim \mathit{1.}\ *_S\ u\ =\ \sim u$

ga_mon_span_thm

$$\begin{aligned}
&\vdash \forall\ V\\
&\quad \bullet\ (\forall\ I\bullet\ I\ \in\ \mathit{Finite} \Rightarrow \mathit{Mon}_G\ I\ \in\ V)\\
&\qquad\quad \wedge\ (\forall\ a\ u\bullet\ u\ \in\ V\ \Rightarrow\ a\ *_S\ u\ \in\ V)\\
&\qquad\quad \wedge\ (\forall\ u\ v\bullet\ u\ \in\ V\ \wedge\ v\ \in\ V\ \Rightarrow\ u\ +\ v\ \in\ V)\\
&\qquad \Rightarrow\ (\forall\ u\bullet\ u\ \in\ V)
\end{aligned}$$

ga_mon_indep_thm

$$\begin{aligned}
&\vdash \forall\ J\\
&\quad \bullet\ J\ \in\ \mathit{Finite}\\
&\qquad \Rightarrow\ (\exists\ V\\
&\qquad \bullet\ (\forall\ I\bullet\ \neg\ I\ =\ J\ \wedge\ I\ \in\ \mathit{Finite}\ \Rightarrow\ \mathit{Mon}_G\ I\ \in\ V)
\end{aligned}$$

$\land\ (\forall\ a\ u \bullet\ u \in V \Rightarrow a *_S u \in V)$
$\land\ (\forall\ u\ v \bullet\ u \in V \land v \in V \Rightarrow u + v \in V)$
$\land\ \neg\ Mon_G\ J \in V)$

ga_mon_times_mon_thm

$\vdash \forall\ I\ J$
$\bullet\ I \in Finite \land J \in Finite$
$\Rightarrow Mon_G\ I * Mon_G\ J$
$= Sign_G\ I\ J *_S Mon_G\ (I \ominus J)$

finite_friend_thm

$\vdash \forall\ b \bullet\ b \in Finite \Rightarrow (\exists\ a \bullet\ a \in Finite \land \neg\ a = b)$

ga_mon_not_0_thm

$\vdash \forall\ I \bullet\ I \in Finite \Rightarrow \neg\ Mon_G\ I = \Gamma\ 0$

ga_mon_1_thm $\vdash Mon_G\ \{\} = \Gamma\ 1$

ga_mon_subgroup_thm

$\vdash \forall\ X$
$\bullet\ (\forall\ i \bullet\ E_G\ i \in X)$
$\land\ (\forall\ u \bullet\ u \in X \Rightarrow \sim 1. *_S u \in X)$
$\land\ (\forall\ u\ v \bullet\ u \in X \land v \in X \Rightarrow u * v \in X)$
$\Rightarrow (\forall\ I \bullet\ I \in Finite \Rightarrow Mon_G\ I \in X)$

ga_vec_generators_thm

$\vdash \forall\ A$
$\bullet\ (\forall\ i \bullet\ E_G\ i \in A)$
$\land\ (\forall\ u\ a \bullet\ u \in A \Rightarrow a *_S u \in A)$
$\land\ (\forall\ u\ v \bullet\ u \in A \land v \in A \Rightarrow u + v \in A)$
$\land\ (\forall\ u\ v \bullet\ u \in A \land v \in A \Rightarrow u * v \in A)$
$\Rightarrow (\forall\ u \bullet\ u \in A)$

ga_vec_relations_thm

$\vdash \forall\ i\ j$
$\bullet\ E_G\ i * E_G\ i = \Gamma\ 1$
$\land\ (\neg\ i = j \Rightarrow E_G\ i * E_G\ j = \sim (E_G\ j * E_G\ i))$

ga_vec_indep_thm

$\vdash \forall\ j$
$\bullet\ \exists\ V$
$\bullet\ (\forall\ i \bullet\ \neg\ i = j \Rightarrow E_G\ i \in V)$
$\land\ (\forall\ a\ u \bullet\ u \in V \Rightarrow a *_S u \in V)$
$\land\ (\forall\ u\ v \bullet\ u \in V \land v \in V \Rightarrow u + v \in V)$
$\land\ \neg\ E_G\ j \in V$

ga_span_subspace_thm

$\vdash \forall\ X \bullet\ Span_G\ X \in Subspace_G$

ga_⊆_span_thm

$\vdash \forall\ X \bullet\ X \subseteq Span_G\ X$

ga_span_⊆_thm

$\vdash \forall\ V \bullet\ V \in Subspace_G \land X \subseteq V \Rightarrow Span_G\ X \subseteq V$

ga_trivial_subspaces_thm

$\vdash Universe \in Subspace_G \land \{\Gamma\ 0\} \in Subspace_G$

ga_mon_span_bc_thm

$\vdash \forall\ V\ u$
$\bullet\ (\forall\ I \bullet\ I \in Finite \Rightarrow Mon_G\ I \in V)$
$\land\ (\forall\ a\ u \bullet\ u \in V \Rightarrow a *_S u \in V)$
$\land\ (\forall\ u\ v \bullet\ u \in V \land v \in V \Rightarrow u + v \in V)$
$\Rightarrow u \in V$

ga_span_mon_thm

$\vdash \mathit{Span}_G\ \{u | \exists\ I \bullet\ I \in \mathit{Finite} \land u = \mathit{Mon}_G\ I\} = \mathit{Universe}$

ga_span_mono_thm

$\vdash \forall\ X\ \ Y \bullet\ X \subseteq Y \Rightarrow \mathit{Span}_G\ X \subseteq \mathit{Span}_G\ Y$

ga_indep_thm $\vdash \forall\ X$

$\bullet\ X \in \mathit{Indep}_G \Leftrightarrow (\forall\ x \bullet\ x \in X \Rightarrow \neg\ x \in \mathit{Span}_G\ (X \setminus \{x\}))$

***ga_mon_indep_thm*1**

$\vdash \{u | \exists\ I \bullet\ I \in \mathit{Finite} \land u = \mathit{Mon}_G\ I\} \in \mathit{Indep}_G$

pythagoras_thm

$\vdash \forall\ u\ v \bullet\ u \perp v \Rightarrow (u - v)\ \hat{}\ \mathit{2} = u\ \hat{}\ \mathit{2} + v\ \hat{}\ \mathit{2}$

INDEX