COUNTING WITH EXPONENTIAL OF GROUPS

AN INTRODUCTION TO RIEG THEORY

RYUYA HORA

Abstract. This note aims to introduce the notion of riegs and present categorical and combinatorial aspects of the rieg theory through a very specific example: the rieg of finite groups.

Prerequisite knowledge is limited to very basic category theory and group theory. This note is part of the author's ongoing research (or hobby?) *rieg theory* [4].

Contents

Counting problems

Later, we will give a rieg-theoretic method to answer the following undergraduate-level counting problems.

Question 0.1. *For a finite group G, let n_G denote the number of subgroups whose index (= the number of cosets) is 2. Write $n_{G\times H}$ using n_G and n_H.*

Question 0.2. *Count the number of group homomorphisms from D_6 to itself. (Hint: $D_6 \cong S_3 \times C_2$.)*

1. Definition of riegs

Since what we will consider is a ring with **e**xponentials instead of **n**egatives, we call it a *rieg*. We define riegs with numerous but familiar axioms about exponential.

Definition 1.1 (Rieg, axiomatic definition)**.** A *rieg* is a set R equipped with

- two nullary operations, $0, 1 \in R$ and
- three binary operations, $+, \times, \uparrow \colon R \times R \to R$

that satisfies the following "usual" fourteen axioms:

- $x + 0 = x$
- $(x + y) + z = x + (y + z)$

Graduate School of Mathematical Sciences, University of Tokyo. hora@ms.u-tokyo.

- $x + y = y + x$
- $x \times 1 = x$
- $(x \times y) \times z = x \times (y \times z)$
- $x \times y = y \times x$
- $x \times 0 = 0$
- $x \times (y + z) = (x \times y) + (x \times z)$
- $1 \uparrow x = 1$
- $(x \times y) \uparrow z = (x \uparrow z) \times (y \uparrow z)$
- $x \uparrow 0 = 1$
- $x \uparrow (y + z) = (x \uparrow y) \times (x \uparrow z)$
- $x \uparrow 1 = x$
- $x \uparrow (y \times z) = (x \uparrow y) \uparrow z$.

Remark 1.2. For those who know rigs (=semirings), our definition above has a much more memorable form: It is just a commutative rig (= semiring) $(R, 0, 1, +, \times)$ equipped with a rig homomorphism $R \to \mathrm{End}(R, 1, \times)$.

Example 1.3. The prototypical example is the rieg of natural numbers $\mathbb{N}$. Notice that we adopt $0^0 = 1$.

Exercise 1.4. Prove that if the underlying rig of a rieg R is a ring, then R is a singleton. (Hint: consider 0^{-1}.)

Remark 1.5. A similar algebraic structure, *Tarski high school identities*, has been studied by (finite) model theorists [2][3].

2. CCC with finite coproducts form a rieg

Proposition 2.1. *For a cartesian closed category $\mathcal{C}$ with finite coproducts, the set of isomorphism classes of $\mathcal{C}$ forms a rieg with the categorical initial object, terminal object, coproducts, products, and exponentials.*

Proof. All of the fourteen axioms are implied by the universalities. □

Exercise 2.2. Explain why this construction does not work for a symmetric monoidal closed category.

The following examples are not necessary to follow the latter sections of this note.

Example 2.3. Regarding the decategorified semiring structure, numerous studies have been conducted under the name *Burnside rig*. However, to the author's knowledge, research on its exponential structure has been very limited. Despite the exponential structure satisfying numerous equations in the definition of rieg, these have been left unused.

- The category **FinSet** forms a rieg of natural numbers.
- The category **Set** forms a rieg of cardinal arithmetic[1] The structure of this rieg is closely related to set theory, especially the (generalized) continuum hypothesis.
- The category of finite functions $[\to, \mathbf{FinSet}]$ forms a rieg of multisets of natural numbers (or Dirichlet polynomials [5]).
- More generally, for any finite category $\mathcal{C}$, its finite (co)presheaf category $[\mathcal{C}, \mathbf{FinSet}]$ forms a rieg. Examples include the category of finite graphs $[\rightrightarrows, \mathbf{FinSet}]$ and the category of rooted forests $[\omega^{\mathrm{op}}, \mathbf{FinSet}]$.
- For any (possibly infinite) group G, the category of its finite actions $[\mathbf{B}G, \mathbf{FinSet}]$ form the *Burnside rig* of the group G. Examples include the category of sets with involution $[\mathbf{B}\mathbb{Z}/2\mathbb{Z}, \mathbf{FinSet}]$ and the category of finite loops $[\mathbf{B}\mathbb{Z}, \mathbf{FinSet}]$.
- Every Heyting algebra H is a cartesian closed poset with finite coproducts, and thus a rieg.

[1] There is a size matter. One can fix a strong limit cardinal κ and consider only sets with cardinality less than κ. Then, (the isomorphism classes of) $\mathbf{Set}_{<\kappa}$ form a (small) rieg.

- The category of quasi-categories **qCat** forms a rieg. This rieg contains the rieg of categories **Cat**, posets **Poset**, and groupoids **Groupoid**. Conversely, this rieg is contained by the rieg of simplicial sets **sSet**.

Exercise 2.4. Describe the exponentials of $[\to, \mathbf{FinSet}]$, in terms of multisets.

Exercise 2.5. Prove that the category of finite discrete dynamical systems $[\mathbf{B}\mathbb{N}, \mathbf{FinSet}]$ is NOT cartesian closed[2].

3. Rieg of finite groups

Notice that all operations $0, 1, +, \times, \uparrow$ of the cartesian closed category of finite groupoids $\mathbf{Groupoid}_{\text{fin}}$ are well-defined up to equivalence. Therefore, (as a 2-categorical analogy of Proposition 2.1), the equivalence classes of finite groupoids, which are the formal sums of finite groups, form a rieg! The aim of this section is to concretely describe the rieg structure.

Definition 3.1. We definite *the rig of finite groups* $\mathcal{G}$ as follows:

- The underlying additive commutative monoid is the free commutative monoid of the set of isomorphism classes of finite groups, which is given by the finite formal sum.
$$\mathcal{G} \coloneqq \bigoplus_{[G]\colon \text{ iso.class}} \mathbb{N}$$
- The multiplication is given by the unique extension of
$$[G] \times [H] \coloneqq [G \times H].$$

Hereafter, the isomorphism class of a group G will be simply referred to as G.

Notation 3.2. The (isomorphism class of) the cyclic group $\mathbb{Z}/n\mathbb{Z}$ is denoted by C_n.

Example 3.3. Some examples of calculations include:

- $C_{12} = C_3 \times C_4$
- $D_6 = S_3 \times C_2$
- $(S_3 + C_2)^2 = {S_3}^2 + 2(S_3 \times C_2) + {C_2}^2 = {S_3}^2 + 2D_6 + {C_2}^2$

Definition 3.4 (Conjgacy classes of homomorphism)**.** Let G and H be finite groups.

- Two homomorphisms $\phi, \psi \colon G \to H$ are *conjugate* if there exists $h \in H$ such that $\phi = h\psi h^{-1}$ holds.
- The automorphism group (or the stabilizer) of a homomorphism $\phi\colon G \to H$ is the subgroup of H, defined by $\mathrm{Aut}(\phi) \coloneqq \{h \in H \mid h\phi h^{-1} = \phi\}$.

Theorem 3.5. *The rig of finite groups $\mathcal{G}$ admits the following rieg structure:*

- *For two finite groups G and H, its exponential H^G is defined by*
$$H^G \coloneqq \sum_{[\phi]:conj.class} \mathrm{Aut}(\phi)$$
- *In general, the exponential is defined by*
$$\left(\sum_j H_j\right)^{\left(\sum_i G_i\right)} \coloneqq \prod_i \sum_j \left({H_j}^{G_i}\right),$$
for any two families of finite groups $(G_i)_i$ and $(H_j)_j$.

[2]This is one of my motivations to consider the question: when is a finite presheaf category $[\mathcal{C}, \mathbf{FinSet}]$ cartesian closed? The author is also interested in the closely related question: when is a finite presheaf category a topos?

Proof. This is the rieg of equivalent classes of finite groupoids, explained at the beginning of this section. □

Example 3.6. Let's try to calculate ${D_6}^{D_6}$. In order to utilize the exponential rules, we first calculate smaller parts:

- ${C_2}^{C_2} = 2 \cdot C_2$
- ${C_2}^{S_3} = 2 \cdot C_2$
- ${S_3}^{C_2} = C_2 + S_3$
- ${S_3}^{S_3} = 1 + C_2 + S_3$

Then we obtain

$${D_6}^{D_6} = \left({S_3}^{S_3}\right)^{C_2} \cdot \left({C_2}^{S_3}\right)^{C_2} = (1 + C_2 + S_3)^{C_2} \cdot (2 \cdot C_2)^{C_2} = (1 + 3 \cdot C_2 + S_3) \cdot (4 \cdot C_2) = 4 \cdot C_2 + 12 \cdot {C_2}^2 + 4 \cdot D_6.$$

Some properties of finite groups, like being abelian, are characterized in terms of this rieg structure.

Proposition 3.7. *For a finite group A,*

- *if A is abelian, then we have $A^G = \#\mathrm{Hom}(G, A) \cdot A$.*
- *conversely, if A^G is a sum of A for any G, then A is abelian.*

Proof. The former statement is immediate from the definition. If A^G is a sum of A for any G, then A^A is a sum of A. Especially, we have $\mathrm{Aut}(\mathrm{id}_A) = A$ and A is abelian. □

Now we can answer the first problem, Question 0.1!

Answer 3.8 (to Question 0.1)**.** Since ${C_2}^G = (n_G + 1) \cdot C_2$, we have

$$(n_{G\times H} + 1) \cdot C_2 = {C_2}^{G\times H} = \left({C_2}^G\right)^H = (n_G + 1) \cdot {C_2}^H = (n_G + 1) \cdot (n_H + 1) \cdot C_2.$$

This proves $n_{G\times H} = n_G \cdot n_H + n_G + n_H$.

Remark 3.9. For a limit cardinal κ, one can consider a rieg of larger groups, in which we can similarly consider representations of product groups, like ${\mathbb{C}\mathbf{Vect}_{\text{f.d.iso.}}}^{G\times H} = \left(\sum_{k=0}^{\infty} \mathrm{GL}_k(\mathbb{C})\right)^{G\times H}$.

4. Groupoid cardinality

In order to utilize riegs for counting something, the basic rieg theoretic method is to consider a **rig** homomorphism from a given rieg to the rig of numbers, like $\mathbb{N}, \mathbb{Z}, \mathbb{Q}$.

For the rieg of finite groups $\mathcal{G}$, the notion of *groupoid cardinality*, introduced in [1], is useful. We can utilize it to obtain rational numbers from elements of $\mathcal{G}$.

Definition 4.1. For $x = \sum_i G_i \in \mathcal{G}$, its *groupoid cardinality* $|x| \in \mathbb{Q}$ is defined by

$$|x| \coloneqq \sum_i \frac{1}{\#G_i}.$$

Proposition 4.2. *The groupoid cardinality $|-|\colon \mathcal{G} \to \mathbb{Q}$ preserves sum and products. Furthermore, for finite groups G and H, we have*

$$\left|G^H\right| = \frac{\#\mathrm{Hom}(H, G)}{\#G}.$$

Proof. For sums and products, the proof is easy. Regarding exponentials, one can use the orbit-stabilizer theorem for the conjugate action of G on $\mathrm{Hom}(H, G)$. □

Exercise 4.3. Check that Proposition 4.2 is compatible with Proposition 3.7.

Let us finish this introductory note by giving the answer to Question 0.2!

Answer 4.4 (to Question 0.2)**.** In Example 3.6, we obtained ${D_6}^{D_6} = 4 \cdot C_2 + 12 \cdot {C_2}^2 + 4 \cdot D_6$. By taking the groupoid cardinality, we obtain

$$\frac{\#\mathrm{Hom}(D_6, D_6)}{12} = \frac{4}{2} + \frac{12}{4} + \frac{4}{12}.$$

This proves that $\mathrm{Hom}(D_6, D_6) = 64$.

5. Other aspects of riegs

The author would like to claim that this is just one of many aspects of rieg theory. The other aspects would include enumerative combinatorics (regarding higher homotopy), elementary number theory with exponentials, p-adic arithmetics (with the profinite completion of the rieg $\mathbb{N}$), universal algebra, rig theory, finitely cocomplete locally cartesian closed category (including topoi), type theory with sum type, lattice theory (especially, a generalization of Heyting algebra), and combinatorial game theory.

If you are interested in some of them, please let me know!

References

[1] John C Baez and James Dolan. "From finite sets to Feynman diagrams". *Mathematics unlimited—2001 and beyond* (2001), pp. 29–50.

[2] Stanley Burris and Simon Lee. "Tarski's high school identities". *The American Mathematical Monthly* 100.3 (1993), pp. 231–236.

[3] Stanley N Burris and Karen A Yeats. "The saga of the high school identities". *Algebra Universalis* 52 (2005), pp. 325–342.

[4] Ryuya Hora. "Notes on Rieg theory (in progress)" ().

[5] David I Spivak and David Jaz Myers. "Dirichlet Polynomials form a Topos". *arXiv preprint arXiv:2003.04827* (2020).