Groups and Information

An informational reading of group theory

Hugues Genvrin

September 2026

Programme du grain

The single thread

A **group** *is an* *invariant*, *and* **information** *measures what invariance costs or preserves.*

Five short movements, read in bits:

1. **Quantifying the axioms** — the price of associativity, identity, inverses.
2. **The informational Cayley theorem** — weight of a group by symmetry.
3. **Maximal weight and bounds** — the elementary abelian group.
4. **The negentropy of cyclicity** — when "being cyclic" is free.
5. **Epistemology of the group notion** — invariance as the true origin.

Outline

Quantifying the Group Axioms

The idea: count the tables

Reverse the usual construction (set $\to$ magma $\to$ monoid $\to$ group): degrade a group by removing axioms one by one, and measure the cost of each.

A binary law is a table
On a set E of n *labelled* elements, an internal law is a map $E \times E \to E$: an $n \times n$ table valued in E. Hence

$$|\mathrm{Magma}(n)| = n^{n^2}.$$

Constraint negentropy of an axiom
For a class A and the subclass $A' \subset A$ obtained by adding one axiom,

$$N_{\text{axiom}} = \log_2 \frac{|A|}{|A'|} \geq 0 :$$

the number of **bits** needed to select the admissible tables.

The sign, corrected

- Adding an axiom **constrains**: you *pay* N_{axiom} bits (the space of tables shrinks).
- Removing an axiom **frees entropy**: more admissible tables — a loss of negentropy, not a gain.

The quantity attached to each layer is therefore the **cost of the axiom**, counted positively on reconstruction (backward chaining).

The hierarchy, quantified

Axioms stacked in order:

$$\text{magma} \xrightarrow{\text{assoc.}} \text{semigroup} \xrightarrow{\text{identity}} \text{monoid} \xrightarrow{\text{inverses}} \text{group}.$$

n	magma	semigrp	monoid	group	N_{assoc}	N_{id}	N_{inv}
2	16	8	4	2	1.00	1.00	1.00
3	19 683	113	33	3	**7.44**	1.78	3.46
4	4.29×10^9	3492	126	16	**20.23**	4.79	2.98

Total cost magma $\to$ group: **3.00** (n=2), **12.68** (n=3), **28.00** (n=4) bits.

Associativity dominates

Corollary
From $n \geq 3$, associativity is by far the most expensive axiom, and its cost grows fast with n: $1 \to 7.4 \to 20.2$ bits. At $n = 3$ it alone eliminates **99.4%** of the tables.

Why: global vs. local

- **Associativity** is a *global* constraint: it links every triple (a, b, c) — n^3 conditions. Hence its growth in n.
- **Identity** and **inverses** are *local*: one distinguished element, one partner per element.

Associativity is the informational *backbone* of algebraic structure. A group is expensive not because of its inverses, but because of associativity.

The Informational Cayley Theorem

Partition of the tables by isomorphism class

The symmetric group S_n acts on labelled group-tables by *relabelling*; two tables share an orbit iff the groups are isomorphic.

Theorem (Informational Cayley)

$$\mathrm{tables}(n) \;=\; \sum_{[G]:\,|G|=n} \frac{n!}{|\operatorname{Aut}(G)|}.$$

Each class $[G]$ *is an* S_n*-orbit with stabiliser* $\operatorname{Aut}(G)$*, hence of size* $n!/|\operatorname{Aut}(G)|$ *(orbit–stabiliser).*

At $n = 4$: two classes, $\mathbb{Z}/4$ and the Klein group V

$$\mathrm{tables}(4) = \frac{24}{|\operatorname{Aut}(\mathbb{Z}/4)|} + \frac{24}{|\operatorname{Aut}(V)|} = \frac{24}{2} + \frac{24}{6} = 12 + 4 = 16.$$

The informational weight of a group

Definition (Weight)

$$w(G) = \log_2 \frac{\mathrm{tables}(n)}{n!/|\operatorname{Aut}(G)|} = \log_2 \frac{|\operatorname{Aut}(G)| \cdot \mathrm{tables}(n)}{n!} \ \geq 0 :$$

the cost in **bits** to designate one table of G among all.

Symmetry = informational richness
$w(G)$ increases with $|\operatorname{Aut}(G)|$: the more symmetric a group, the smaller its orbit, the rarer it is — the more informative.

Klein is richer than $\mathbb{Z}/4$: $w(\mathbb{Z}/4) = \log_2 \frac{16}{12} = 0.42$ bit, $\quad w(V) = \log_2 \frac{16}{4} = \mathbf{2}$ bits.

The table of weights

n	group	$\lvert\mathrm{Aut}(G)\rvert$	tables	$w(G)$ (bits)
4	$\mathbb{Z}/4$	2	12	0.42
4	$V = (\mathbb{Z}/2)^2$	6	4	**2.00**
6	$\mathbb{Z}/6$	2	360	0.42
6	S_3	6	120	2.00
8	$\mathbb{Z}/8$	4	10 080	1.13
8	$\mathbb{Z}/4 \times \mathbb{Z}/2$	8	5040	2.13
8	D_4	8	5040	2.13
8	Q_8	24	1680	3.72
8	$(\mathbb{Z}/2)^3$	168	240	**6.52**

Maximal weight always goes to the elementary abelian group $(\mathbb{Z}/2)^m$ — the most symmetric.

The case $n = 4$ explained

Where does the 6 come from?
The Klein group is the vector space $V = \mathbb{F}_2^2$. Its group automorphisms are exactly its *linear* ones:

$$\mathrm{Aut}(V) = \mathrm{GL}(2, \mathbb{F}_2), \qquad |\,\mathrm{GL}(2, \mathbb{F}_2)| = (2^2 - 1)(2^2 - 2) = 3 \cdot 2 = 6.$$

And $\mathrm{GL}(2, \mathbb{F}_2) \cong S_3$: the 6 linear maps permute the 3 nonzero vectors in every possible way.

An isolated coincidence, not a law
On $(\mathbb{Z}/2)^m$ one has $|\,\mathrm{Aut}\,| = |\,\mathrm{GL}(m, \mathbb{F}_2)| = \prod_{i=0}^{m-1}(2^m - 2^i)$:

$$m{=}1{:}\,1, \quad m{=}2{:}\,6, \quad m{=}3{:}\,168, \quad m{=}4{:}\,20\,160, \ \ldots$$

Only $m = 2$ gives $6 = |S_3|$. The right generalisation is $\mathrm{GL}(m, \mathbb{F}_2)$, *not* S_{k-1}.

Maximal Weight and Bounds

The elementary abelian group at orders 2^m

Two questions about the weight $w(G)$ at orders $n = 2^m$. The candidate for maximal weight is $E_m = (\mathbb{Z}/2)^m$:

$$\mathrm{Aut}(E_m) = \mathrm{GL}(m, \mathbb{F}_2), \qquad |\,\mathrm{GL}(m, \mathbb{F}_2)| = \prod_{i=0}^{m-1} (2^m - 2^i) \ \sim\ 2^{\,m^2}.$$

Q1 — Maximality
Is E_m always of maximal weight?

Q2 — Bounds
Is w bounded? Does its share stay significant?

Maximality: true, then false

Proposition (abelian case — sure)
Among abelian groups of order 2^m, $E_m = (\mathbb{Z}/2)^m$ has the largest Aut, hence the largest weight w. Any coarser partition $\mathbb{Z}/2^a$ $(a \geq 2)$ rigidifies the structure and shrinks $|\mathrm{Aut}|$.

Proposition (global case — only $m \leq 3$)
E_m has maximal weight among *all* groups of order 2^m only for $m \leq 3$. For $m \geq 4$ some non-abelian 2-groups (extraspecial and relatives) have $|\mathrm{Aut}|$ exceeding $|\mathrm{GL}(m, \mathbb{F}_2)|$.

m	max-weight group	$\|\mathrm{Aut}\|$	w (bits)
1	$\mathbb{Z}/2$ (only)	1	0
2	$(\mathbb{Z}/2)^2$	6	2.00
3	$(\mathbb{Z}/2)^3$	168	6.52
≥ 4	not always $(\mathbb{Z}/2)^m$	—	—

Bounds: w diverges, its share vanishes

Theorem (Unboundedness)

$$w(E_m) \;\geq\; \log_2 |\operatorname{GL}(m,\mathbb{F}_2)| - (m-1) \;\sim\; m^2 \xrightarrow[m\to\infty]{} +\infty.$$

Theorem (The normalised fraction $\to 0$)

$$\frac{w(E_m)}{\log_2 \mathrm{tables}(2^m)} \;\sim\; \frac{m^2}{2^m\, m} = \frac{m}{2^m} \xrightarrow[m\to\infty]{} 0,$$

since $\log_2(2^m!) \sim 2^m m$ *(Stirling) grows exponentially while* $\log_2|\operatorname{GL}(m,\mathbb{F}_2)| \sim m^2$ *grows only polynomially.*

m	$\log_2(2^m!)$	$w(E_m)$	fraction
2	4.6	1.58	0.44
3	15.3	5.39	0.41
4	44.3	11.30	0.27
5	117.7	19.25	0.17
6	296.0	29.23	0.10

Absolutely heavier, relatively lighter

The two statements do not contradict each other.

- E_m becomes **absolutely heavier**: more and more bits to designate one of its tables ($w \sim m^2$).
- E_m becomes **relatively lighter**: this weight is a vanishing share of the total information ($\sim m/2^m$), because the number of tables explodes far faster.

The rarity of the elementary abelian group is real — but drowned in a combinatorics that grows factorially.

The Negentropy of Cyclicity

The cost of “being cyclic”

Let $\mathrm{gnu}(n)$ be the number of groups of order n up to isomorphism (OEIS `A000001`). Since $\mathbb{Z}/n\mathbb{Z}$ is the *unique* cyclic group of order n:

Definition (Cyclicity negentropy)

$$N_{\text{cyc}}(n) = \log_2 \frac{\mathrm{gnu}(n)}{1} = \log_2 \mathrm{gnu}(n) \ \geq 0.$$

It measures the information needed to *select* the cyclic structure among all group structures of order n. It is zero exactly when there is nothing to select.

Labelled tables of $\mathbb{Z}/n\mathbb{Z}$

$\dfrac{n!}{|\operatorname{Aut}(\mathbb{Z}/n\mathbb{Z})|} = \dfrac{n!}{\varphi(n)}$, since $\mathbb{Z}/n\mathbb{Z}$ has $\varphi(n)$ generators. Its *table* cost $\log_2\big(n!/\varphi(n)\big)$ oscillates with Euler's φ.

Nullity $\iff$ cyclic number

Theorem (Annulment)
For every $n \geq 1$,

$$N_{cyc}(n) = 0 \iff \mathrm{gnu}(n) = 1 \iff \gcd\bigl(n, \varphi(n)\bigr) = 1.$$

The integers with $\gcd(n, \varphi(n)) = 1$ are the **cyclic numbers** *(OEIS A003277); the equivalence with $\mathrm{gnu}(n) = 1$ is a classical theorem of T. Szele.*

All primes — and more
Every prime p has $N_{\mathrm{cyc}}(p) = 0$ (Lagrange). But the converse is false: some composites also vanish — $15, 33, 35, 51, 65, 69, \ldots$ So N_{cyc} detects *uniqueness of structure*, not primality.

A worked table

n	prime?	$\mathrm{gnu}(n)$	$N_{\mathrm{cyc}}(n)$	
5	yes	1	0	prime $\Rightarrow$ null
7	yes	1	0	
8	no	5	**2.322**	very composite
12	no	5	2.322	
15	no	1	**0**	composite yet cyclic, $\gcd(15, 8)=1$
16	no	14	3.807	
24	no	15	3.907	
35	no	1	**0**	$\gcd(35, 24)=1$

The authentic rebound

$N_{\mathrm{cyc}}(n) = \log_2 \mathrm{gnu}(n)$ falls back to zero precisely at the cyclic numbers — a rebound "to the floor", at primes and their coprime-with-φ cousins. (Beware a false rebound: never mix labelled counts $n!/\varphi(n)$ with up-to-iso counts $\mathrm{gnu}(n)$.)

Epistemology of the Group Notion

The origin: invariance

Definition (Origin — invariance under transformation)
The notion of group arises from **bijective, structure-preserving** transformations under composition. Such a collection is *closed* (composing two preservations preserves), contains the *identity* (trivial preservation) and *inverses* (a preserving bijection undoes itself) — it is a group.

Finite cyclicity is only a special case
We do *not* restrict to finite cyclic transformations ($\exists n,\ f^n = \mathrm{id}$). The fundamental groups are massively non-cyclic and infinite: $SO(3)$, $(\mathbb{Z}, +)$, $(\mathbb{R}, +)$, the Lie groups of physics. $\mathbb{Z}/n$ is the *minimal* case (one transformation, iterated), not the root.

By Klein's theorem, $\mathrm{Sym}(A)$ is exactly the set of semantic-equilibrium transformations ($N = 0$): the group *is* the invariant, read as structure.

The scale of structures — definitions, not axioms

$$\text{magma} \subset \text{semigroup} \subset \text{monoid} \subset \text{group} \subset \text{cyclic group}.$$

Each rung adds a property, with a **measurable informational cost** (associativity being by far the dearest).

A distinction to keep

- **Definitions**: the structures (magma, monoid, group. . .) — conventions naming objects that satisfy properties.
- **Axioms**: the imposed properties (associativity, identity, inverses).

The heuristic direction (invariant $\to$ magma, or the reverse) does not change this status. The heuristic direction is not the logical direction.

Transport by morphism

Lemma (The image of a group is a group)
Let $(G, \cdot)$ be a group, $(H, +)$ a magma, $f : G \to H$ a morphism. Then $\operatorname{im} f = f(G)$ *is a group. If f is surjective, then all of $(H, +)$ is a group.*

Everything happens in $\operatorname{im} f$: $f(e)$ is the identity there, and $f(a^{-1}) = -f(a)$.

Why the image — and not all of H
Counterexample: $G = \{e\}$, $H = (\mathbb{N}, +)$, $f(e) = 0$. The image $\{0\}$ is a group, but $(\mathbb{N}, +)$ is not (2 has no inverse). The morphism does not *make* H a group — it exhibits a subgroup.

Cyclicity transported: if $G = \langle a \rangle$ then $f(a^k) = k\, f(a)$; e.g. $f : (\mathbb{Z}, +) \to (\mathbb{Z}/n, +)$ is surjective and carries the structure onto all of $\mathbb{Z}/n$.

Groups in nature: revealed, not created

The morphism reveals, it does not fabricate
A morphism from a group makes a group structure *appear* in its image — but that structure **pre-exists**: it is *transported* from G, not created by f. The morphism is a revealer, not a generator.

Why so many groups in nature
Ubiquity does not follow from transport (which already assumes a group upstream) but from a deeper fact: **physical laws have symmetries**. Invariance under space/time translation, rotation, gauge transformation — each is a collection of invertible, law-preserving transformations, hence a group. *Noether* ties each continuous symmetry to a conserved quantity: the deep source.

One thread, five readings

A group is an invariant.

its origin is invariance (Klein);
the scale magma $\to$ group has a cost in bits (axioms);
a group's weight measures its rarity (Cayley);
the elementary abelian group is absolutely heaviest, relatively lightest;
"being cyclic" is free exactly at the cyclic numbers;
morphisms reveal the structure, symmetries (Noether) ground it.

Thank you

Groups and Information

Hugues Genvrin — Programme du grain