Group Theory
Group Theory

Study of **symmetries** and **transformations** of mathematical objects.

Also, the study of abstract algebraic objects called ‘**groups**’.
What is group theory good for?

In theoretical computer science:

- Cryptography: Fully homomorphic encryption, obfuscation...
- Quantum algorithms
- Mulmuley’s approach to $\textbf{P}$ vs. $\textbf{NP}$
- Checksums, error-correction schemes
- Minimizing space usage of algorithms
- Derandomization
What is group theory good for?

In puzzles and games:

“15 Puzzle”

Rubik’s Cube

SET

Tangles
What is group theory good for?

In math:

There’s a quadratic formula:

\[
x = \frac{-b \pm \sqrt{b^2 - 4ac}}{2a}
\]
What is group theory good for?

In math:

There’s a cubic formula:

\[
x_1 = -\frac{b}{3a} - \frac{1}{3a} \left(\frac{1}{2} \left[ \frac{2}{2b^3 - 9abc + 27a^2d + \sqrt{(2b^3 - 9abc + 27a^2d)^2 - 4 (b^2 - 3ac)^3}} \right] \right)
\]

\[
x_2 = -\frac{b}{3a} + \frac{1}{3a} \left(\frac{1}{2} \left[ \frac{1+i\sqrt{3}}{6a} \left[ \frac{2b^3 - 9abc + 27a^2d + \sqrt{(2b^3 - 9abc + 27a^2d)^2 - 4 (b^2 - 3ac)^3}} \right] + \sqrt{3} \left[ \frac{1}{2} \left[ \frac{2b^3 - 9abc + 27a^2d - \sqrt{(2b^3 - 9abc + 27a^2d)^2 - 4 (b^2 - 3ac)^3}} \right] \right] \right) \right)
\]

\[
x_3 = -\frac{b}{3a} + \frac{1}{3a} \left(\frac{1}{2} \left[ \frac{1-i\sqrt{3}}{6a} \left[ \frac{2b^3 - 9abc + 27a^2d + \sqrt{(2b^3 - 9abc + 27a^2d)^2 - 4 (b^2 - 3ac)^3}} \right] + \sqrt{3} \left[ \frac{1}{2} \left[ \frac{2b^3 - 9abc + 27a^2d - \sqrt{(2b^3 - 9abc + 27a^2d)^2 - 4 (b^2 - 3ac)^3}} \right] \right] \right) \right)
\]
What is group theory good for?

In math:

There’s a quartic formula:

\[
\begin{align*}
\frac{1}{4} & \left( \frac{\sqrt[3]{4a^3 + 18bc - 27d^2 - \sqrt{4(4a^3 + 18bc - 27d^2)^3 + 27(8a^2b^2 - 9ab^2c + 9b^2c^2) - 72ac^2d - 36b^2cd - 8c^3 + 12ac^2d + 72c^2de + 54abcd - 3a^2d^2} - \sqrt[3]{4a^3 + 18bc - 27d^2 + \sqrt{4(4a^3 + 18bc - 27d^2)^3 + 27(8a^2b^2 - 9ab^2c + 9b^2c^2) - 72ac^2d - 36b^2cd - 8c^3 + 12ac^2d + 72c^2de + 54abcd - 3a^2d^2}}} + \frac{2}{3} b - \frac{1}{3} c \right) \\
+ & \frac{2}{3} \sqrt[3]{\frac{4a^3 + 18bc - 27d^2 - \sqrt{4(4a^3 + 18bc - 27d^2)^3 + 27(8a^2b^2 - 9ab^2c + 9b^2c^2) - 72ac^2d - 36b^2cd - 8c^3 + 12ac^2d + 72c^2de + 54abcd - 3a^2d^2} + \sqrt[3]{4a^3 + 18bc - 27d^2 + \sqrt{4(4a^3 + 18bc - 27d^2)^3 + 27(8a^2b^2 - 9ab^2c + 9b^2c^2) - 72ac^2d - 36b^2cd - 8c^3 + 12ac^2d + 72c^2de + 54abcd - 3a^2d^2}}} - \frac{2}{3} b + \frac{1}{3} c \right) \\
\end{align*}
\]

That’s just the first of four roots, actually.)
What is group theory good for?

In math:

There is **NO** quintic formula.
What is group theory good for?

In physics:

Predicting the existence of elementary particles before they are discovered.
What is group theory good for?

In entertainment:

Driving the plot of S06E10 of Futurama,
“The Prisoner of Benda”
So: What is group theory?
Rotate
Head-to-Toe flip
Q: How many positions can it be in?

A: Four.
Group theory is not so much about **objects** (like mattresses).

It’s about the **transformations** on objects and how they (inter)act.
\[
\begin{align*}
F(R(\text{mattress})) &= \text{H(\text{mattress})} \\
\text{H}(F(\text{mattress})) &= R(\text{mattress}) \\
R(F(H(\text{mattress})))) &= \text{Id(\text{mattress})} \\
F \circ R &= H \\
H \circ F &= R \\
R \circ F \circ H &= \text{Id} \\
R \circ \text{Id} \circ H \circ F \circ H &= H
\end{align*}
\]
The kinds of questions asked:

What is $R \circ \text{Id} \circ H \circ F \circ H$?

Do transformations $A$ and $B$ “commute”?  
I.e., does $A \circ B = B \circ A$?

What is the “order” of transformation $A$?  
I.e., how many times do you have to apply $A$ before you get to $\text{Id}$?
Definition of a **group of transformations**

Let $X$ be a set.

Let $G$ be a set of **bijections** $p : X \to X$.

We say $G$ is a **group of transformations** if:

1. If $p$ and $q$ are in $G$ then so is $p \circ q$.
   
   $G$ is "**closed**" under composition.

2. The ‘do-nothing’ bijection $\text{Id}$ is in $G$.

3. If $p$ is in $G$ then so is its inverse, $p^{-1}$.
   
   $G$ is “**closed**” under inverses.
Example: Rotations of a rectangular mattress

$X = \text{set of all physical points of the mattress}$

$G = \{ \text{Id}, \text{Rotate}, \text{Flip}, \text{Head-to-toe} \}$

Check the 3 conditions:

1. If $p$ and $q$ are in $G$ then so is $p \circ q$. ✔

2. The ‘do-nothing’ bijection $\text{Id}$ is in $G$. ✔

3. If $p$ is in $G$ then so is its inverse, $p^{-1}$. ✔
Example: Symmetries of a directed cycle

\[ X = \text{labelings of the vertices by 1, 2, 3, 4} \]

\[ |X| = 24 \]

\[ G = \text{permutations of the labels which don't change the graph} \]

\[ |G| = 4 \]

\[ G = \{ \text{Id}, \text{Rot}_90, \text{Rot}_{180}, \text{Rot}_{270} \} \]
Example: Symmetries of a directed cycle

\[ X = \text{labelings of the vertices by } 1, 2, 3, 4 \]

\[ |X| = 24 \]

\[ G = \text{permutations of the labels which don’t change the graph} \]

\[ |G| = 4 \]

\[ G = \{ \text{Id}, \text{Rot}_{90}, \text{Rot}_{180}, \text{Rot}_{270} \} \]
Example: Symmetries of a directed cycle

\[ X = \text{labelings of directed 4-cycle} \]

\[ G = \{ \text{Id}, \text{Rot}_{90}, \text{Rot}_{180}, \text{Rot}_{270} \} \]

Check the 3 conditions:

1. If \( p \) and \( q \) are in \( G \) then so is \( p \circ q \). ✔️

2. The ‘do-nothing’ bijection \( \text{Id} \) is in \( G \). ✔️

3. If \( p \) is in \( G \) then so is its inverse, \( p^{-1} \). ✔️

“Cyclic group of size 4”
Example: Symmetries of undirected $n$-cycle

$X =$ labelings of the vertices by $1, 2, \ldots, n$

$|X| = n!$

$G =$ permutations of the labels which don’t change the graph

$|G| = 2n$
Example: Symmetries of \textbf{undirected} n-cycle

\[ X = \text{labelings of the vertices by } 1, 2, \ldots, n \]

\[ |X| = n! \]

\[ G = \text{permutations of the labels which don’t change the graph} \]

\[ |G| = 2n \]

+ one clockwise twist
Example: Symmetries of **undirected** n-cycle

\[ X = \text{labelings of the vertices by } 1, 2, \ldots, n \]

\[ |X| = n! \]

\[ G = \text{permutations of the labels which don’t change the graph} \]

\[ |G| = 2n \]

+ one clockwise twist
Example: Symmetries of undirected \( n \)-cycle

\[ X = \text{labelings of the vertices by } 1, 2, \ldots, n \]

\[ |X| = n! \]

\[ G = \text{permutations of the labels which don’t change the graph} \]

\[ |G| = 2n \]

\[ G = \{ \text{Id}, \ n-1 \ ‘rotations’, \ n \ ‘reflections’ \} \]

“Dihedral group of size \( 2n \)”
Example: “All permutations”

\[ X = \{1, 2, \ldots, n\} \]

\[ G = \text{all permutations of } X \]

e.g., for \( n = 4 \), a typical element of \( G \) is:

\[
\begin{pmatrix}
1 & 2 & 3 & 4 \\
\downarrow & \downarrow & \downarrow & \downarrow \\
4 & 2 & 1 & 3
\end{pmatrix}
\]

“Symmetric group, Sym(n)”
More groups of transformations

Motions of 3D space: translations + rotations
(preserve laws of Newtonian mechanics)

Translations of 2D space by an integer amount horizontally and an integer amount vertically

Rotations which preserve an old-school soccer ball.

\[ |G| = 60 \]
Group theory is not so much about **objects** (like mattresses).

It’s about the **transformations** on objects and how they (inter)act.
There is no mattress.
The laws of mattress rotation

\[ G = \{ \text{Id, R, F, H} \} \]

\[
\begin{align*}
\text{Id} \circ \text{Id} &= \text{Id} & F \circ \text{Id} &= F \\
\text{Id} \circ \text{R} &= \text{R} & F \circ \text{R} &= \text{H} \\
\text{Id} \circ \text{F} &= \text{F} & F \circ \text{F} &= \text{Id} \\
\text{Id} \circ \text{H} &= \text{H} & F \circ \text{H} &= \text{R} \\
\text{R} \circ \text{Id} &= \text{R} & H \circ \text{Id} &= H \\
\text{R} \circ \text{R} &= \text{Id} & H \circ \text{R} &= \text{F} \\
\text{R} \circ \text{F} &= \text{H} & H \circ \text{F} &= \text{R} \\
\text{R} \circ \text{H} &= \text{F} & H \circ \text{H} &= \text{Id}
\end{align*}
\]
The laws of the dihedral group of size 10

\[ G = \{ \text{Id, } r_1, r_2, r_3, r_4, f_1, f_2, f_3, f_4, f_5 \} \]
Let’s define an abstract **group**.

Let $G$ be a set.

Let $\circ$ be a “**binary operation**” on $G$;
    
    think of it as defining a “multiplication table”.

E.g., if $G = \{ a, b, c \}$ then...

    ... is a binary operation.

This means that $c \circ a = b$. 
Definition of an (abstract) group

We say $G$ is a "group under operation $\circ$" if:

1. Operation $\circ$ is associative:
   
   i.e., $a \circ (b \circ c) = (a \circ b) \circ c \quad \forall \ a, b, c \in G$

2. There exists an element $e \in G$ (called the "identity element") such that

   $a \circ e = a, \ e \circ a = a \quad \forall \ a \in G$

3. For each $a \in G$ there is an element $a^{-1} \in G$ (called the "inverse of a") such that

   $a \circ a^{-1} = e, \ a^{-1} \circ a = e$
Examples of (abstract) groups

Any group of transformations is a group.

(Only need to check that composition of functions is associative.)

E.g., the ‘mattress group’ (AKA Klein 4-group)

<table>
<thead>
<tr>
<th></th>
<th>Id</th>
<th>R</th>
<th>F</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Id</td>
<td>Id</td>
<td>R</td>
<td>F</td>
<td>H</td>
</tr>
<tr>
<td>R</td>
<td>R</td>
<td>Id</td>
<td>H</td>
<td>F</td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>H</td>
<td>Id</td>
<td>R</td>
</tr>
<tr>
<td>H</td>
<td>H</td>
<td>F</td>
<td>R</td>
<td>Id</td>
</tr>
</tbody>
</table>

identity element is $\text{Id}$

$R^{-1} = R$

$F^{-1} = F$

$H^{-1} = H$
Examples of (abstract) groups

Any group of transformations is a group.

\( \mathbb{Z} \) (the integers) is a group under operation +

Check:

0. + really is a binary operation on \( \mathbb{Z} \)
1. + is associative: \( a+(b+c) = (a+b)+c \)
2. “e” is 0: \( a+0 = a, \ 0+a = a \)
3. “a\(^{-1}\)” is \( -a \): \( a+(-a) = 0, \ (-a)+a = 0 \)
Examples of (abstract) groups

Any group of transformations is a group.

\( \mathbb{Z} \) (the integers) is a group under operation +

\( \mathbb{R} \) (the reals) is a group under operation +

\( \mathbb{R}^+ \) (the positive reals) is a group under \( \times \)

\( \mathbb{R} \setminus \{0\} \) is a group under \( \times \)

\( \mathbb{Z}_n \) (the integers mod n) is a group under +
NONEXAMPLES of groups

\[ G = \{ \text{all odd integers} \}, \text{ operation } + \]

+ is not a binary operation on \( G \)!

\( \mathbb{Z} \), operation −

− is not associative!

\( \mathbb{Z} \setminus \{0\} \), operation \( \times \)

1 is the only possible identity element;
but then most elements don’t have inverses!
Abstract algebra on groups

Theorem 1:
If \((G, \circ)\) is a group, identity element is unique.

Proof:
Suppose \(f\) and \(g\) are both identity elements. Since \(g\) is identity, \(f \circ g = f\). Since \(f\) is identity, \(f \circ g = g\). Therefore \(f = g\).
Abstract algebra on groups

Theorem 2:

In any group \((G, \circ)\), inverses are unique.

Proof:

Given \(a \in G\), suppose \(b, c\) are both inverses of \(a\). Let \(e\) be the identity element.

By assumption, \(a \circ b = e\) and \(c \circ a = e\).

Now:

\[
\begin{align*}
c &= c \circ e = c \circ (a \circ b) \\
&= (c \circ a) \circ b = e \circ b = b
\end{align*}
\]
Abstract algebra on groups

Theorem 3:
For all $a$ in group $G$ we have $(a^{-1})^{-1} = a$.

Theorem 4:
For $a, b \in G$ we have $(a \circ b)^{-1} = b^{-1} \circ a^{-1}$.

Theorem 5:
In group $(G, \circ)$, it doesn’t matter how you put parentheses in an expression like

$$a_1 \circ a_2 \circ a_3 \circ \cdots \circ a_k$$

(“generalized associativity”).
Notation

In abstract groups, it’s tiring to always write $\circ$. So we often write $ab$ rather than $a \circ b$.

Sometimes write $1$ instead of $e$ for the identity.

For $n \in \mathbb{N}^+$, write $a^n$ instead of $aaa \cdots a$ (n times). Also $a^{-n}$ instead of $a^{-1}a^{-1} \cdots a^{-1}$, and $a^0$ means $1$.

Then $a^j a^k = a^{j+k}$ holds for all $j, k \in \mathbb{Z}$. 
Algebra practice

Problem: In the mattress group \( \{1, R, F, H\} \), simplify the element \( R^2 (H^3 R^{-1})^{-1} \)

One (slightly roundabout) solution:

\[
H^3 = H H^2 = H 1 = H, \text{ so we reach } R^2 (H R^{-1})^{-1}.
\]
\[
(H R^{-1})^{-1} = (R^{-1})^{-1} H^{-1} = R H, \text{ so we get } R^2 R H.
\]
But \( R^2 = 1 \), so we get \( 1 R H = R H = F \).

Moral: the usual rules of multiplication, except...
Commutativity?

In a group we do NOT NECESSARILY have

$$a \circ b = b \circ a$$

Actually, in the mattress group we do have this for all elements. E.g., $RF = FR (=H)$.

Definition:

“$a,b \in G$ commute” means $ab = ba$.

“$G$ is commutative” means all pairs commute.
In group theory, “commutative groups” are usually called **abelian** groups.

Niels Henrik *Abel* (1802–1829)
Norwegian
Died at 26 of tuberculosis 😞
Age 22: proved there is no quintic formula.
Evariste Galois (1811–1832)
French
Died at 20 in a duel 😞
One of the main inventors of group theory.
Some abelian groups:

“Mattress group”  
(Symms of a **directed** cycle)  
(\(\mathbb{R}, +\))  
(“Klein 4-group”)  

Some nonabelian groups:

Symms of an **undirected** cycle ("dihedral group")  
Motions of 3D space  
Sym(n)  
("symmetric group on n elements")
Another fun group: Quaternion group

\[ Q_8 = \{ 1, -1, i, -i, j, -j, k, -k \} \]

Multiplication defined by:

- \((-1)^2 = 1,\) \((-1)a = a(-1) = -a\)
- \(i^2 = j^2 = k^2 = -1\)
- \(ij = k,\) \(ji = -k\)
- \(jk = i,\) \(kj = -i\)
- \(ki = j,\) \(ik = -j\)

Exercise: valid def. of a (nonabelian) group.
Application to computer graphics

“Quaternions”: expressions like
\[ 3.2 + 1.4i - .5j + 1.1k \]
which generalize complex numbers \((\mathbb{C})\).

Suppose we store points \((x,y,z)\) in 3D space as quaternions \(xi + yj + zk\).

To rotate point \(p\) an angle of \(\theta\) around an axis defined by unit vector \((u,v,w)\), let
\[ q = \cos(\theta/2) + \sin(\theta/2)u i + \sin(\theta/2)v j + \sin(\theta/2)w k. \]
Then the rotated point is \(qpq^{-1}\).
Isomorphism

Here’s a group: \( V = \{ 00, 01, 10, 11 \} \)
\( \oplus \) (bitwise XOR) is the operation

There’s something familiar about this group...

<table>
<thead>
<tr>
<th>( V )</th>
<th>( \oplus )</th>
<th>00</th>
<th>01</th>
<th>10</th>
<th>11</th>
</tr>
</thead>
<tbody>
<tr>
<td>00</td>
<td>00</td>
<td>01</td>
<td>10</td>
<td>11</td>
<td></td>
</tr>
<tr>
<td>01</td>
<td>01</td>
<td>00</td>
<td>11</td>
<td>10</td>
<td></td>
</tr>
<tr>
<td>10</td>
<td>10</td>
<td>11</td>
<td>00</td>
<td>01</td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>11</td>
<td>10</td>
<td>01</td>
<td>00</td>
<td></td>
</tr>
</tbody>
</table>

| same after renaming: | 00\(\leftrightarrow\)Id | 01\(\leftrightarrow\)R | 10\(\leftrightarrow\)F | 11\(\leftrightarrow\)H |

<table>
<thead>
<tr>
<th>The mattress</th>
<th>( \circ )</th>
<th>Id</th>
<th>R</th>
<th>F</th>
<th>H</th>
</tr>
</thead>
<tbody>
<tr>
<td>Id</td>
<td>Id</td>
<td>R</td>
<td>F</td>
<td>H</td>
<td></td>
</tr>
<tr>
<td>R</td>
<td>R</td>
<td>Id</td>
<td>H</td>
<td>F</td>
<td></td>
</tr>
<tr>
<td>F</td>
<td>F</td>
<td>H</td>
<td>Id</td>
<td>R</td>
<td></td>
</tr>
<tr>
<td>H</td>
<td>H</td>
<td>F</td>
<td>R</td>
<td>Id</td>
<td></td>
</tr>
</tbody>
</table>
Isomorphism

Groups \((G, \circ)\) and \((H, \bullet)\) are “\textbf{isomorphic}” if there is a way to \textit{rename} elements so that they have the \textit{same} multiplication table.

Fundamentally, they’re the “same” abstract group.
Isomorphism and orders

Obviously, if G and H are isomorphic we must have $|G| = |H|$.

$|G|$ is called the order of G.

E.g.: Let $C_4$ be the group of transformations preserving the directed 4-cycle.

$|C_4| = 4$

Q: Is $C_4$ isomorphic to the mattress group $V$?
Isomorphism and orders

Q:  Is $C_4$ isomorphic to the mattress group $V$?

A:  No!

$a^2 = 1$ for every element $a \in V$.

But in $C_4$, $\text{Rot}_{90}^2 = \text{Rot}_{270}^2 \neq \text{Rot}_{180}^2 = \text{Id}^2$

Motivates studying powers of elements.
Order of a group element

Let $G$ be a finite group. Let $a \in G$.
Look at $1, a, a^2, a^3, \ldots$ till you get some repeat.
Say $a^k = a^j$ for some $k > j$.
Multiply this equation by $a^{-j}$ to get $a^{k-j} = 1$.
So the first repeat is always $1$.

Definition: The order of $a$, denoted $|a|$, is the smallest $m \geq 1$ such that $a^m = 1$.
Note that $a, a^2, a^3, \ldots, a^{m-1}, a^m=1$ all distinct.
Examples:

In mattress group (order 4),
\[ |\text{Id}| = 1, \quad |R| = |F| = |H| = 2. \]

In directed-4-cycle group (order 4),
\[ |\text{Id}| = 1, \quad |\text{Rot}_{180}| = 2, \quad |\text{Rot}_{90}| = |\text{Rot}_{270}| = 4. \]

In dihedral group of order 10
(symmetries of undirected 5-cycle)
\[ |\text{Id}| = 1, \quad |\text{any rotation}| = 5, \quad |\text{any reflection}| = 2. \]
Order Theorem:

\[ |a| \text{ always divides evenly into } |G|. \]

Claim: also of length \( m \).

Because \( xa^j = xa^k \Rightarrow a^j = a^k \).
Order Theorem:
|a| always divides evenly into |G|.

Impossible.
Multiply on right by $a^{-1}$. 
Order Theorem:

$|a|$ always divides evenly into $|G|$.

$G$ partitioned into cycles of size $m$. 
Order Theorem:
\[ |a| \text{ always divides evenly into } |G|. \]

Corollary: If \(|G| = n\), then \(a^n = 1\) for all \(a \in G\).

Proof: Let \(|a| = m\). Write \(n = mk\).
Then \(a^n = (a^m)^k = 1^k = 1.\)
A Group Theory Application
Check Digits

Say you have important strings of digits:

credit card numbers
EFT routing numbers
UPC numbers
money serial numbers
book ISBNs

People screw up when transcribing them.
Check Digits

Most common human screwups:

- single digit wrong (e.g., 6→8): 60-90%
- omitting/adding digit: 10-20%
- transposition (e.g., 35→53): 10-20%
- other screwups: ≤ 5%

Instead of making them $n$ random digits, make them $n$ random digits + a ‘check digit’.
Check Digits


Desired id#: 1360429947

1098765432

dot-prod mod 11: 1×10+3×9+6×8+0×7+4×6+2×5+9×4+9×3+8×2 = 4

check digit: top it off to get 0 mod 11

Pros: You can detect any single-digit or transposition error.
Check Digits


Desired id#: 1 3 6 0 4 2 9 9 4 7

\[
\begin{array}{cccccccccc}
10 & 9 & 8 & 7 & 6 & 5 & 4 & 3 & 2 \\
\end{array}
\]

dot-prod mod 11: \(1 \times 10 + 3 \times 9 + 6 \times 8 + 0 \times 7 + 4 \times 6 + 2 \times 5 + 9 \times 4 + 9 \times 3 + 8 \times 2 = 4\)

check digit: top it off to get 0 mod 11

Cons: Um, check digit should be 10? “Write X”!
Doesn’t scale if you want longer id#’s.
Verhoeff Check Digit Method

Encode digits by elements of dihedral group of order 10.

Let \( \sigma \) be the permutation

\[
\begin{pmatrix}
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
1 & 5 & 7 & 6 & 2 & 8 & 3 & 0 & 9 & 4
\end{pmatrix}
\]

Given a desired id\# \( a_0 \, a_1 \, a_2 \cdots a_{n-1} \),
choose unique check digit \( a_n \) satisfying group equation

\[
\text{enc}(\sigma^0(a_0)) \circ \text{enc}(\sigma^1(a_1)) \circ \text{enc}(\sigma^2(a_2)) \circ \cdots \circ \text{enc}(\sigma^n(a_n)) = e
\]

Pros: Detects single-digit & transposition errors.
Uses just digits 0, 1, 2, ..., 9.
Scales to any length of id\#. 
Verhoeff Check Digit Method

Encode digits by elements of dihedral group of order 10.

Let $\sigma$ be the permutation

\[
\begin{pmatrix}
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
1 & 5 & 7 & 6 & 2 & 8 & 3 & 0 & 9 & 4 \\
\end{pmatrix}
\]

Given a desired id# $a_0 a_1 a_2 \cdots a_{n-1}$,
choose unique check digit $a_n$ satisfying group equation

\[
\text{enc}(\sigma^0(a_0)) \circ \text{enc}(\sigma^1(a_1)) \circ \text{enc}(\sigma^2(a_2)) \circ \cdots \circ \text{enc}(\sigma^2(a_n)) = e
\]

Cons: Can’t really be done by a human.
Verhoeff Check Digit Method

Encode digits by elements of dihedral group of order 10.

Let \( \sigma \) be the permutation

\[
\begin{array}{ccccccccccc}
0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 \\
\downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow & \downarrow \\
1 & 5 & 7 & 6 & 2 & 8 & 3 & 0 & 9 & 4 \\
\end{array}
\]

Given a desired id\# \( a_0 \ a_1 \ a_2 \ \cdots \ a_{n-1} \),
choose unique check digit \( a_n \) satisfying group equation

\[
\text{enc}(\sigma^0(a_0)) \circ \text{enc}(\sigma^1(a_1)) \circ \text{enc}(\sigma^2(a_2)) \circ \cdots \circ \text{enc}(\sigma^2(a_n)) = e
\]

Is this really a con?
What human manually checksums credit cards?
We have computers, you know.
Verhoeff Check Digit Method

Nevertheless, it’s like the Dvorak keyboard of check digit methods. 😞

German federal bank started using it for Deutsche Marks (with some letters?) in 1990.

Then they went and got the euro (which uses a different scheme).
The 10 is a good denomination for mathematicians.

Leonhard Euler on the back of the old 10 Swiss franc note.
The 10 is a good denomination for mathematicians.

I do not know how this works.

Cahit Arf and an equation in the group $\mathbb{Z}_2$ starring on the back of a Turkish 10 lira.
Study Guide

Definitions:
- Groups
- Commutative/abelian
- Isomorphism
- Order

Groups:
- Klein 4-, cyclic, dihedral,
- symmetric, quaternions

Doing:
- Checking for groupness
- Computations in groups

Theorem/proof:
- Order Theorem