The group of inner automorphisms

An implementation & proof in Lean 4

By Roy Steffen and Clara Vossbeck

July 2024

Table of contents

Preliminary definitions and proofs

Definition 1 (Conjugation by g)

Let G be a group. For any $g \in G$, we define the *conjugation map*

$$c_g : G \to G, h \mapsto ghg^{-1}.$$

Lemma 2

For any $g \in G$, c_g is a group automorphism.

Proof.

Let $h_1, h_2, h \in G$. Then:

$$c_g(h_1 h_2) = gh_1 h_2 g^{-1} = gh_1 g^{-1} \cdot gh_2 g^{-1} = c_g(h_1) \cdot c_g(h_2)$$

An inverse map is given by $c_{g^{-1}}$:

$$\begin{aligned} c_g(c_{g^{-1}}(h)) &= c_g(g^{-1}h(g^{-1})^{-1}) \\ &= c_g(g^{-1}hg) \\ &= gg^{-1}hgg^{-1} = h \end{aligned}$$

$$c_{g^{-1}}(c_g(h)) = c_{g^{-1}}(ghg^{-1}) = g^{-1}ghg^{-1}g = h$$

$\square$

Lemma 3

The map

$$c : G \to \mathrm{Aut}(G), g \mapsto c_g$$

is well-defined and a group homomorphism.

Proof.

Well-definedness follows from Lemma 2. Let now $g_1, g_2, g, h \in G$. Then:

$$\begin{aligned}
[c(g_1 g_2)](h) &= c_{g_1 g_2}(h) \\
&= g_1 g_2 h (g_1 g_2)^{-1} \\
&= g_1 g_2 h g_2^{-1} g_1^{-1} \\
&= c_{g_1}(g_2 h g_2^{-1}) \\
&= c_{g_1}(c_{g_2}(h)) \\
&= [c_{g_1} \circ c_{g_2}](h) \\
&= [c(g_1) \circ c(g_2)](h)
\end{aligned}$$

$$\implies c(g_1 g_2) = c(g_1) \circ c(g_2)$$

$\square$

The group of inner automorphisms $\mathrm{Inn}(G)$

Finally, with these formalities behind us, we can define the group of our interest:

Definition 4 (Group of inner automorphisms)

Let G be a group. We define the *group of inner automorphisms* as $\mathrm{Inn}(G) := \mathrm{im}(c) \subset \mathrm{Aut}(G)$.

Existence of automorphisms that are not inner

Let from now on $n \in \mathbb{N}$. In this section we want to prove that the group $\mathrm{GL}_n(\mathbb{R})$ has automorphisms that are not inner. To achieve this goal, we first prove the following proposition:

Proposition 5

Let $\varphi : \mathrm{GL}_n(\mathbb{R}) \to \mathrm{GL}_n(\mathbb{R})$ be an inner automorphism and $A \in \mathrm{GL}_n(\mathbb{R})$. Then A and $\varphi(A)$ have the same characteristic polynomial.

Proof.

φ is an inner automorphism $\implies \exists B \in \mathrm{GL}_n(\mathbb{R}) : \varphi = c_B$.
Then,

$$\begin{aligned}
p_A(T) &= \det(T \cdot \mathbb{I}_n - A) \\
&= \det(BB^{-1}) \cdot \det(T \cdot \mathbb{I}_n - A) \\
&= \det(B) \cdot \det(T \cdot \mathbb{I}_n - A) \cdot \det(B^{-1}) \\
&= \det(B \cdot (T \cdot \mathbb{I}_n - A) \cdot B^{-1}) \\
&= \det(T \cdot BB^{-1} - BAB^{-1}) \\
&= \det(T \cdot \mathbb{I}_n - c_B(A)) \\
&= \det(T \cdot \mathbb{I}_n - \varphi(A)) = p_{\varphi(A)}(T)
\end{aligned}$$

□

Construction of a counterexample

Lemma 6

The map

$$\alpha : \mathrm{GL}_n(\mathbb{R}) \to \mathrm{GL}_n(\mathbb{R}), A \mapsto (A^{-1})^\intercal$$

is a group automorphism. In particular, $\alpha \circ \alpha = \mathrm{id}_{\mathrm{GL}_n(\mathbb{R})}$ *.*

Proof.

Let $A, B \in \mathrm{GL}_n(\mathbb{R})$. Then:

$$\begin{aligned} \alpha(AB) = [(AB)^{-1}]^\intercal &= (B^{-1}A^{-1})^\intercal \\ &= (A^{-1})^\intercal \cdot (B^{-1})^\intercal \\ &= \alpha(A) \cdot \alpha(B) \end{aligned}$$

Proof (Continuation).

Furthermore,

$$\begin{aligned}(\alpha \circ \alpha)(A) = \alpha(\alpha(A)) = \alpha((A^{-1})^\intercal) &= ([(A^{-1})^\intercal]^{-1})^\intercal \\ &= ([(A^{-1})^\intercal]^\intercal)^{-1} \\ &= (A^{-1})^{-1} \\ &= A = \mathrm{id}_{\mathrm{GL}_n(\mathbb{R})}(A)\end{aligned}$$

$$\implies \alpha \circ \alpha = \mathrm{id}_{\mathrm{GL}_n(\mathbb{R})} \qquad \square$$

Theorem 7

α is not an inner automorphism of $\mathrm{GL}_n(\mathbb{R})$.

Proof.

We examine $2 \cdot \mathbb{I}_n \in \mathrm{GL}_n(\mathbb{R})$. Then we have:

$$p_{2\cdot\mathbb{I}_n}(T) = \det(T \cdot \mathbb{I}_n - 2 \cdot \mathbb{I}_n) = (T - 2)^n$$

Proof (Continuation).

However,

$$\begin{aligned} p_{\alpha(2\cdot\mathbb{I}_n)}(T) &= \det(T\cdot\mathbb{I}_n - \alpha(2\cdot\mathbb{I}_n)) \\ &= \det(T\cdot\mathbb{I}_n - [(2\cdot\mathbb{I}_n)^{-1}]^\intercal) \\ &= \det(T\cdot\mathbb{I}_n - (1/2\cdot\mathbb{I}_n)^\intercal) \\ &= \det(T\cdot\mathbb{I}_n - 1/2\cdot\mathbb{I}_n) \\ &= (T-1/2)^n \end{aligned}$$

As such, we have $p_{2\cdot\mathbb{I}_n} \neq p_{\alpha(2\cdot\mathbb{I}_n)}$. Proposition 5 now tells us that therefore α cannot be an inner automorphism. □

Implementation & proof in Lean 4

Now, we are going to see how one can define and prove these statements in Lean 4!

Bibliography

- Böckle, G. (Summer semester 2023), [Exercise sheet 3, Algebra I], Heidelberg University.
- Lean Community 2024, *Mathlib 4*, accessed 14th July 2024, `https://leanprover-community.github.io/mathlib4_docs/index.html`