From Lie algebras to Frobenius's Theorem

Algebraic Formalisation with locales, types and relations

Richard Schmoetten

The University of Edinburgh

27th June 2023

Lie Groups and Algebras

- A Lie group is a manifold that is also a group under a smooth operation $(x, y) \mapsto xy$ with smooth inverses $x \mapsto x^{-1}$.
- A Lie algebra is anticommutative and obeys the Jacobi identity:

$$\forall x, y, z \in \mathfrak{g} : \qquad [x, [y, z]] + [y, [z, x]] + [z, [x, y]] = 0$$

```
locale lie_grp =
    c_manifold charts ∞ +
    grp_on carrier tms one +
  assumes smooth_mult: "diff_on_product_manifold charts tms"
      and smooth_inv: "diff ∞ charts invs"
```

Type Classes: Polymorphism in Isabelle/HOL

Quantification over types is not possible in HOL.

$$\cancel{\forall \alpha. \quad P(\alpha) \implies \exists a \in (\mathrm{UNIV} :: \alpha\ \mathrm{set})}$$

Type classes offer a (restricted) alternative. A class can be defined much like a locale: it is possible that no types satisfy the sort constraints.

```
class fin_dim_real_vector = real_vector +
  fixes basis
  assumes finite_Basis: "finite basis"
  and independent_Basis:
    "∄u. (∑v∈basis. u v *R v) = 0 ∧ (∃v∈basis. u v ≠ 0)"
  and span_Basis: "{∑a∈basis. r a *R a |r. True} = UNIV"
```

Transfer: Relators

Relators allow us to build transfer rules for constants from transfer relations. The most ubiquitous one is the function relator.

$$\begin{tikzcd} \alpha \arrow[r, "\cong"] \arrow[d, "f"'] & \beta \arrow[d, "g"] \\ \alpha \arrow[r, "\cong"'] & \beta \end{tikzcd}$$

- α and β *related* by $\cong : \alpha \to \beta \to \texttt{bool}$
- Say a theorem involves a function $f : \alpha \to \alpha$, and we have a candidate $g : \beta \to \beta$ with equivalent behaviour
- Isabelle can use a transfer rule

$$\forall a, b. \quad a \cong b \implies f(a) \cong g(b)$$

(Real) Division Algebras

A (associative) division algebra is an (associative) algebra that has multiplicative identity and inverses.

```
class scalar_algebra = real_div_algebra + fin_dim_real_vector
```

Example

- $\mathbb{R}$ is a division algebra over itself.
- $\mathbb{C}$ is a division algebra over $\mathbb{R}$.
- $\mathbb{H}$ is a division algebra over $\mathbb{R}$.

$\mathbb{H} = \{a + bi + cj + dk \mid a, b, c, d \in \mathbb{R}\}$

$i^2 = j^2 = k^2 = ijk = -1$

not commutative: $ij = k$ but $ji = -k$

Polynomials over Type Embeddings

The fundamental theorem of algebra states that every complex polynomial has a root. This implies every complex polynomial can be factorised.

$$p_{\mathbb{C}}(x) = c \prod_{j=0}^{\deg(p)} \Big(x - r(j)\Big)$$

```
definition "c ≃ r ≡ c = (r *ℝ 1)"
definition "p ≐ q ≡ (∀i::nat. coeff p i ≃ coeff q i)"
```

$$p_{\mathbb{R}}(x) = r \prod_{j=0}^{N_r} \Big(x - r_r(j)\Big) \prod_{k=0}^{N_i} \Big(x - r_i(k)\Big)\Big(x - \overline{r_i(k)}\Big)$$