Proseminar on computer-assisted mathematics

Session 10 - The fundamental theorem of algebra

Theorem 1. *Any nonconstant polynomial with complex coefficients has a complex root.*

We will prove this theorem by reformulating it in terms of eigenvectors of linear operators. Let

$$f(z) = z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0$$

have degree $n \geq 1$, with $a_j \in \mathbf{C}$. By induction on n, the matrix

$$A = \begin{pmatrix} 0 & 0 & 0 & \cdots & 0 & -a_0 \\ 1 & 0 & 0 & \cdots & 0 & -a_1 \\ 0 & 1 & 0 & \cdots & 0 & -a_2 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ 0 & 0 & 0 & \cdots & 0 & -a_{n-2} \\ 0 & 0 & 0 & \cdots & 1 & -a_{n-1} \end{pmatrix}$$

satisfies $\det(\lambda I_n - A) = f(\lambda)$. Therefore Theorem 1 is a consequence of

Theorem 2. *For each $n \geq 1$, every $n \times n$ square matrix over $\mathbf{C}$ has an eigenvector. Equivalently, for each $n \geq 1$, every linear operator on an n-dimensional complex vector space has an eigenvector.*

Florent Schaffhauser
Heidelberg University, Summer semester 2023

The fundamental theorem of algebra

A non-constant polynomial with complex coefficients has a complex root.

A proof of this using concepts from linear algebra can be found here:

https://kconrad.math.uconn.edu/blurbs/fundthmalg/fundthmalglinear.pdf

The goal of this project is to formalize fragments from the above paper and prove them (this can be split between several teams).

Lemma 3

Let F be a Field.

Let V be a finite-dimensional F-module.

Let $d := \dim V$ and $m \geq 1$ be an integer.

Assume that

$m \nmid d \Rightarrow \forall A : V \to V$ linear, $\exists \lambda \in F, \exists v \in V \setminus \{0\}, Av = \lambda v$

Then :

$(*)\begin{cases} \forall A_1, A_2 : V \to V \text{ linear}, \\ (A_1 A_2 = A_2 A_1) \Rightarrow \exists \lambda_1, \lambda_2 \in F, \exists v \in V \setminus \{0\}, \\ \qquad A_1 v = \lambda_1 v \text{ and } A_2 v = \lambda_2 v. \end{cases}$

Task 1

(F : Type) [hF : Field F]

(V : Type) [hV : module F V]

(m : ℤ) (hm : m > 0)

(H : $m \nmid d \to (A : V \to V) \wedge (A \text{ linear}) \to \exists (\lambda : F), \exists (v : V), (v \neq 0) \wedge (Av = \lambda v)$.)

$\underbrace{\qquad\qquad}$

We define a function sending F, V, m, hm and H to a proof of the statement (*)

Remarks on the proof of Lemma 3

You will need to use mathlib for the definition of a field and a vector space. | Task 2

The proof is by strong induction on d. | Task 3

If things go well, you might be able to prove the following Corollary (using mathlib again for the Intermediate Value Theorem). | Task 4

Corollary 4. *For every real vector space V whose dimension is odd, any pair of commuting linear operators on V has a common eigenvector.*

Proof. In Lemma 3, use $F = \mathbf{R}$ and $m = 2$. Any linear operator on an odd-dimensional real vector space has an eigenvector since the characteristic polynomial has odd degree and therefore has a real root, which is a real eigenvalue. Any real eigenvalue leads to a real eigenvector. $\square$

Proof of the main theorem

Write $d = 2^k n$ where $\overbrace{2 \nmid n}^{\iff n \text{ is odd}}$.

Then the result is proved by strong induction on k.

The $\overbrace{k = 0 \text{ case}}^{\iff d \text{ is odd}}$ is already interesting and should be treated as a separate lemma.

Task 4

---> can you formalise its statement?

---> can you prove it?

Note that this uses Corollary 4!