Some formalization ideas for VERSEIM-2025

George McNinch

2025-04-19 21:50:08 EDT (george@valhalla)

Contents

1 Warm-up problems

1.1 linear algebra results

- formalize correspondence between linear transformations $V \to W$ and matrices (where V and W are finite dimensional vector spaces over some field).
- e.g. formluate and prove statements about eigenvectors and eigenvalues of a linear endomorphism of a finite dimensional vector space V.

  Probably the ultimate target would be the Cayley-Hamilton theorem.

1.2 finite group theory

- prove that a finite p-group has a non-trivial center (and hence that a finite p-group is solvable)
- for a finite p-group G and a field k of char p>0, prove that for any finite dimensional k-vector space V and any homomorphism $\rho : G \to GL(V)$ that G fixes a non-zero vector in V.

1.3 commutative rings

- prove the Gauss Lemma and Eisenstein's criteria Gauss Lemma already has a proof in mathlib and so does Eisenstein's critera

1.4 Graph theory

- mathlib has a proof of Hall's Marriage Theorem
- prove elementary fact: sum of degrees of vertices is twice the number of edges.

2 Formalization ideas

2.1 Projective spaces and grassmannians

- mathlib has a formalization of projective spaces can we imitate this formalization to the Grassmannian? What results should be proved about it?

  Say something about Plücker embedding?

  Is there already a formalization of the *exterior powers* of a vector space? Surely...

2.2 forms over a finite field

Defined on a finite dimensional vector space V over a finite field

- reflexive forms
- quadratic forms / symmetric forms (char 2 and $p > 2$)
- alternating forms
- Hermitian forms
- Can you give a formal proof of the theorem describing the number of points of a quadric (i.e. the zero set in $\mathbb{P}(V)$ of a non-degenerate quadratic form q on the vector space V over a finite field.

2.3 Polar spaces

- such a space is a "point-line geometry". Formalize the notion of point-line geometry.
- polar spaces arise from reflexive form on a vector space on a finite field.

2.4 Fourier transforms for functions on vector spaces over a finite field

2.5 Algebraic combinatorics

- formalize proof of some results from book of R. Stanley.

  e.g. Theorem 1.1 which gives a condition for a formal power series $f \in k[\![t]\!]$ to be a *rational function.* Try to formalize this proof.

  or more generally, all the "tool-results" from the first section of Stanley's book.

2.6 error-correcting codes

- formalize some basic results about codes - see Simeon Ball's book.

2.7 quaternion algebras

- show they are simple
- describe in the form (a, b) or (in char. 2) $(a, b]$.
- give criteria on a, b for when the algebra is division.
- formalize proof of result from P. Gilles book about quadratic forms & quaternion algebras.