LINEAR CODES TO INTRODUCE VECTOR SPACES

Everyday reality is increasingly using digital communication to convey information by means of codified languages. This situation arouses the interest and excites the curiosity of young people, who are daily dealing with objects with an apparently unknown functioning, which stimulates them to discover the deepest nature of these things. The will to communicate without running the risk of being "intercepted" is becoming a common life requirement. This seemed to us a good idea to strongly support the execution of some aspects of linear algebra, and the vector spaces in particular; a field study (carried out in a third class of a senior high school specializing in classical studies in Massafra-TA) gave us the possibility to try out the introduction and use of linear codes in the "game of messages" to finally get to the concept of vector spaces.

The literature dealing with the codes and cryptography issues introduces first of all the security question as for the coding and decoding by which the receiver's and sender's keys have to be mathematically correlated, as well as the identification of a "good" code (K. Davlin, 1998). Moreover, n-dimensional spaces are also mentioned, since the difficulty to mentally create spaces with a dimension higher than three and objects of fourth dimension is actually well-known. Among the easiest games to carry out in a secondary school, one has the purpose to find out "the number the other thought of" without the possibility to "cheat", whereas the other is called "spotting of the destination"; both games are based on codified information. By performing this kind of work, it was possible to identify an algebraic structure for the words of the code which satisfies all the vector space axiomes and verifies their properties.

The experimentation which is still in progress allows us to point out some interesting results as for the discovery of some specific mathematical competences, such as the concrete use of complex algebraic structures; students are therefore stimulated to look for real situations in which algebraic structures are present.

Selected Readings

- Singh S. "Codici e segreti", Ed Rizzoli, 1999.
- Devlin K., "Il linguaggio della matematica", Ed Bollati Boringhieri, 1998.
- Berardi L., Beutelspacher A., "La storia della crittografia: l'uso dei gruppi ciclici per costruire codici", Bollettino UMI, La matematica nella società e nella cultura, serie VIII, Vol. VI-A, Aprile 2003, 105-118.
- Hill R., "A first course in coding theory", Ed Clarendon Press – Oxford, 1986.