Rita Vincenti

FINITE FIELDS, PROJECTIVE GEOMETRIES AND RELATED TOPICS

Morlacchi Editore U.P.

Dedicated to my students

Cover: *The Celtic Hut, the ruled variety V_2^3 of PG(4,q)*, image courtesy Maria Vittoria Barbarossa, Marco Fagiolini.

I am grateful to my son Marco for his usual careful collaboration, he interpreted and understood definitively all the figures I had only roughly hand drawn.

isbn 978-88-9392-259-3

Printed in February 2021 by “Logo srl”, Borgoricco (PD).

www.morlacchilibri.com

mail to: redazione@morlacchilibri.com

Contents

0.1 Introduction

During the second semester of 2020, we had to teach remotely online, because of Covid-19. To simplify life for both my students and myself, I manually drafted notes in Italian, so that one day before the lesson they could receive a file on which to follow my explanations. For this year I decided to organize those drafts in English in order to be printed and here they are.

Combinatorics is a teaching for the Master in Mathematics. The summarizing information is as follows:

COMBINATORICS - 6 Credits
Subtitle: Galois Fields, Galois Geometries, Algebraic-Geometric codes.
Year: I Master
Semester: II
Sector: MAT/03
Prerequisites: Algebra 1, Algebra 2, Geometria 1, Geometria 2.
Hours of lessons: 42
Language: English

The program consists of a short algebraic part and a part dedicated to finite geometric structures. It can be summmarized as follows. Galois fields: basis, algebraic extensions, norms and traces, equations. The finite geometries $PG(r, q)$, $r \geq 1$: projective incidence properties, duality. The projective plane: ternary ring, translation planes, semi-fields, quasi-fields, Lenz-Barlotti classification. Partitions and translation planes. Linear groups: Sylow-subgroups, transvections, the representation of $GL(n, q)$. Projective varieties: quadrics in $PG(r, q), r \geq 2$, rational normal curves. Grassmannians. Veronese surface. From projective systems to linear codes. Applications.
The last part was developed by my students in their seminars and it is not included in these notes.

Chapter 1

Preliminaries

Combinatorics studies finite (geometric) structures, that is, structures having a finite number of objects, and their properties. In 1872 Felix Klein in Erlangen publicly presents his program. Such a program was a revolution in the way to look at a geometry, that is, a geometry is characterized by the kind of group acting on its points, lines, planes, ... and not by their objects themselves, so that a projective, an affine or an Euclidean group defines, respectively, a projective, an affine or an Euclidean geometry, independently of the objects over which the group acts.

In 1910 Hilbert published his main Theorem. He proved that every geometry of dimension $n \geq 3$ is built over a vector space (over a field). Hence the dimension 2 (plane) is open to be generalized and to be able to represent more closely experimental situations.

Since then, mathematicians started to extend and generalize the definitions of geometric structures (as, e.g., experimental designs).
Lenz (1954) and Barlotti (1957) classified projective (graphic) planes depending on their groups of central collineations, more precisely, of incident point-line pairs (Lenz) and non-incident center-axis pairs (Barlotti), respectively. The classification consists of 7 types of planes, divided into 39 subtypes in total. It marked the passage from the so called *isotropic* structures to structures having *local properties*, that is, not transferable anywhere.

Some mathematicians were involved in rereading codes introduced in the 50s and started the foundations of the theory of codes, which began to support various new technologies related to information theory. In the 90s

the close connection between linear codes and finite geometries was showed. Since then, many studies and research about finite geometric structures can be interpreted and studied in terms of linear codes and vice versa.

1.1 Finite fields

A field $\mathcal{K}$ is an algebraic structure $(\mathcal{K}, +, \cdot)$ such that $(\mathcal{K}, +)$ and $(\mathcal{K}^*, \cdot)$ $(\mathcal{K}^* = \mathcal{K} \setminus \{0\})$ are commutative groups and the distributive laws hold. If the cardinality $|\mathcal{K}|$ is finite, we say that $\mathcal{K}$ is a *finite field*.

Let $\mathcal{Z}$ denote the ring of the integer numbers. It is well known that $\mathcal{Z}$ is a Principal Ideal Domain (PID). Denote $\mathcal{Z}_p = \mathcal{Z}/\langle p \rangle$ with p a prime number the field of the equivalence classes of $\mathcal{Z}$ *modulo* p. Let $\mathcal{K}$ be a finite field.

Lemma 1 *Let $\phi : \mathcal{Z} \to \mathcal{K}$ be the mapping $n \longmapsto n \cdot 1 = 1 + 1 + ... + 1$. Then ϕ is a ring homomorphism and if $ker\,\phi = \langle m \rangle$, then $m = p$, p prime and $\mathcal{Z}_p$ is a subfield of $\mathcal{K}$.*

Proof. It is easy to prove that ϕ is a ring homomorphism. As $\mathcal{Z}$ is a PID, then $ker\,\phi = \langle m \rangle$ for some $m \in \mathcal{Z}^+$. Assume $m = 0$. Then $ker\,\phi = \langle 0 \rangle$, ϕ is a monomorphism, the field $\mathcal{K}$ contains $\mathcal{Z}/\langle 0 \rangle = \mathcal{Z}_0 \simeq \mathcal{Z}$ so that $\mathcal{K}$ is an infinite field, a contradiction. Therefore it must be $m \neq 0$. As $\mathcal{Z}/ker\,\phi \simeq \mathcal{Z}_m$ and $\mathcal{Z}_m$ is a subring of $\mathcal{K}$, then $\mathcal{Z}_m$ cannot have 0-divisors. Hence $m = p$, p a prime number, and $\mathcal{Z}_p$ is a subfield of $\mathcal{K}$. □

Definition 1 *The number p is the* characteristic *of $\mathcal{K}$, denoted $char\,\mathcal{K}$, $\mathcal{Z}_p$ is the ground subfield of $\mathcal{K}$.*

From the above follows that m is the smallest positive integer in $\mathcal{K}$ such that $m \cdot 1 = 0$.

Let $|\mathcal{K}| = q$ denote the *order* of the field $\mathcal{K}$. Assume $char\,\mathcal{K} = p$. As every field is a vector space over any of its subfield, being $\mathcal{K}$ finite, it has a finite basis, say $\{e_1, ..., e_h\}$, over $\mathcal{Z}_p$ hence $q = p^h$. The field $\mathcal{K}$ is a *Galois Field* and it is denoted $\mathcal{K} = GF(q)$.

Construction of $GF(2^2)$ Let $\mathcal{Z}_2 = \{0, 1\}$ be the field $GF(2)$. To construct the simple algebraic extension of degree 2 of $\mathcal{Z}_2$, it needs to look for a polynomial of degree 2 which is irreducible over $\mathcal{Z}_2$. The number

of the second degree polynomials $x^2 + ax + b \in \mathcal{Z}_2[x]$ equals the number $D_{n,k} = n^k = 2^2$ of the dispositions with repetition of 2 elements, two by two. They are $\{x^2,\ x^2+1,\ x^2+x,\ x^2+x+1\}$. Among them, only x^2+x+1 is irreducible. Let t be a root of it, that is, $t^2 = t + 1$. Now it is easy to construct the tables of the addition in $\mathcal{Z}_2(t) = GF(2^2) = \{0, 1, t, t+1\}$ and of the multiplication in $GF(2^2)^*$ using the rules $t^3 = 1, (t+1)^2 = t^2+1 = t$.

Let $\mathcal{N}$ denote the set of natural numbers with ordinary addition and multiplication. Let $(\mathcal{A}, +, \cdot)$ be a commutative ring.

Definition 2 *$(\mathcal{A}, +, \cdot)$ is an Euclidean ring if a mapping $\nu : \mathcal{A}^* \to \mathcal{N}$ is defined such that the following properties hold:*

$$(1)\ \ \nu(a) \leq \nu(a \cdot b),\ \nu(a) = 0 \Leftrightarrow a = 0,$$

(2) *for all $a \in \mathcal{A}$, $b \in \mathcal{A}^*$ such that $\nu(a) \leq \nu(a)$ then*

$$\exists q, r \in \mathcal{A}\, such\, that\, a = b \cdot q + r$$

with $\nu(r) \leq \nu(b)$ or $r = 0$. The mapping ν is an evaluation.

The ring $\mathcal{Z}$ is an Euclidean ring with $\nu(z) = |z|$, the *module* of every integer number z.

The ring $\mathcal{K}[x]$ of the polynomial over a field $\mathcal{K}$ is an Euclidean ring with $\nu(f(x)) = 2^{deg\, f(x)}$ for every polynomial $f(x) \in \mathcal{K}[x]$.

Let $\mathcal{A}$ be an Euclidean ring.

Definition 3 *The Great Common Divisor (f, g) of two elements $f, g \in \mathcal{A}$ is an element $d \in \mathcal{A}$ such that*
1) *d/f and d/g,*
2) *if h/f and h/g then h/d.*
By applying the Euclidean algorithm it can be proved that d is unique.

Proposition 2 *An Euclidean ring $(\mathcal{A}, +, \cdot)$ is a PID (Principal Ideal Domain).*

Proof. Let $\mathcal{I} < \mathcal{A}$ be an ideal. Denote $m \in \mathcal{I}$ an element with $\nu(m)$ minimum. That means that for all $x \in \mathcal{I}$ follows $x = m \cdot q + r$ with $\nu(r) < \nu(m)$, that is, $r = 0$. Hence $x = m \cdot q$ and $\mathcal{I} =< m >$. □

Definition 4 *A (non-constant) polynomial $f(x) \in \mathcal{K}[x]$ is reducible over $\mathcal{K}$ if $f(x) = g(x)h(x)$ with $deg\, g, deg\, h > 1$. Otherwise, it is irreducible.*

Definition 5 *The splitting field of a polynomial $f(x) \in \mathcal{K}[x]$ over $\mathcal{K}$ is the smallest field containing both $\mathcal{K}$ and all the roots of $f(x)$* (equivalently, it is the smallest field extension of $\mathcal{K}$ over which the polynomial $f(x)$ splits (decomposes) into linear factors).

Theorem 3 *Let $f(x) \in \mathcal{K}[x]$ be irreducible over $\mathcal{K}$ and of minimum degree n with respect to a root α. Then there exists a field $\mathcal{F}$ containing $\mathcal{K}$ and α, $\mathcal{F}$ is the smallest field with respect to this property and $\mathcal{F} \simeq \mathcal{K}[x]/\langle f(x)\rangle$.*

Proof. Let $\varphi : \mathcal{K}[x] \to \mathcal{K}[\alpha]$ defined by $\varphi(h(x)) = h(\alpha)$. It is a surjective ring homomorphism (the evaluation homomorphism). Let $ker\, \varphi = \{h(x)|h(\alpha) = 0\}$. As $f(x)$ is irreducible and minimum with respect to its root α, then $f(x)$ divides $h(x)$ for every $h(x) \in ker\, \varphi$ so that $ker\, \varphi = \langle f(x)\rangle$. The quotient $\mathcal{K}[x]/\langle f(x)\rangle = \{h(x)+\langle f(x)\rangle|h(x) \in \mathcal{K}[x]\}$ is a field because of $\langle f(x)\rangle$ is maximal and consists of n co-sets defined by the polynomials $h(x)$ with $deg\, h(x) < n$. Moreover, from the first theorem of homomorphism follows $\mathcal{K}[x]/\langle f(x)\rangle \cong \mathcal{K}[\alpha]$. As φ is surjective, the algebraic extension field $\mathcal{K}(\alpha)$ (i.e., the smallest field $\mathcal{F}$ containing both $\mathcal{K}$ and α) coincides with $\mathcal{K}[x]/\langle f(x)\rangle$. □

Note 1 - As $deg\, f(x) = n$, then $\mathcal{F} = \mathcal{K}(\alpha)$ has dimension n over $\mathcal{K}$ and it is the splitting field of $f(x)$ over $\mathcal{K}$. From $\mathcal{K}(\alpha) = \mathcal{K}[\alpha]$ follows that $\mathcal{K}(\alpha) = \{b_0 + b_1\alpha + ... + b_{n-1}\alpha^{n-1}|b_i \in \mathcal{K}\}$, that is, $\{1, \alpha, \alpha^2, ..., \alpha^{n-1}\}$ is a basis of $\mathcal{F}$ over $\mathcal{K}$. The addition complies the rules of the addition in a vector space, the multiplication follows the rule arising from $f(\alpha) = 0$.

If β is another root of $f(x)$, then $\mathcal{K}(\alpha) = \mathcal{K}(\beta)$ so that $\mathcal{K}(\alpha)$ contains all the roots of $f(x)$. From Definition 4 and Theorem 3 we get the following

Corollary 4 *There exists a unique splitting field of $f(x)$ over $\mathcal{K}$, up to isomorphisms.*

Proposition 5 *Let $\mathcal{K}$ be a finite field with $char\, \mathcal{K} = p$. Then $\upsilon : x \longmapsto x^p$ is an automorphism.*

Proof. That $(xy)^p = x^p y^p$ is obvious. Moreover $(x+y)^p = \sum_{k=0,...,p} \binom{p}{k} x^p y^{p-k}$, where $\binom{p}{0} = \binom{p}{p} = 1$ and $\binom{p}{k} = \frac{p!}{(p-k)!k!} = \lambda p$ for some λ. As $char\,\mathcal{K} = p$, then $\binom{p}{k} = 0$ for all $0 < k < p$. Hence $(x + y)^p = x^p + y^p$, that is, υ is a ring homomorphism.
Analogously $(x - y)^p = x^p - y^p$ holds so that from $(x - y)^p = 0$ follows $x^p - y^p = 0$, $x^p = y^p$ and also $x = y$, hence υ is injective. Assume υ is not surjective. Then $\upsilon(\mathcal{K}) < \mathcal{K}$. As $\mathcal{K}$ is finite, then $|\upsilon(\mathcal{K})| < |\mathcal{K}|$ so that there exist two elements $a \neq b$ in $\mathcal{K}$ such that $\upsilon(a) = \upsilon(b)$. As υ is injective, then it must be $a = b$, a contradiction. Therefore υ is an automorphism of $\mathcal{K}$. □

Note 2 For every mapping $\varrho : S \to S$ on a finite set S, if ϱ is injective then ϱ is also surjective (analogous proof of Proposition 5).
The mapping υ is the *Frobenius automorphism*, it fixes pointwise the ground field $\mathcal{Z}_p$ of $\mathcal{K}$ and if $|\mathcal{K}| = q = p^h$, every mapping υ^k with $k = 1, ..., h$ is a automorphism of $\mathcal{K}$. Moreover, $a^q = a^{p^h} = a$ for all $a \in \mathcal{K}$.

Exercise *Describe the full group $Aut\,\mathcal{F}$ of the automorphisms of $\mathcal{F} = GF(2^2) = \{0, 1, t, t + 1\}$.*
Note that a ring homomorphism fixes pointwise $\{0, 1\}$ so that for $\gamma \in Aut\,\mathcal{F}$ the the possibilities are $\gamma(t) = t$ and $\gamma(t) = t + 1$. In the first case $\gamma = id$, in the second case $\gamma(t + 1) = \gamma(t) + \gamma(1) = t + 1 + 1 = t$. Hence the group $Aut\,\mathcal{F} \simeq \mathcal{Z}_2$.

Let $\mathcal{K} = GF(q)$ with $q = p^h$. Define the mapping $\chi : \mathcal{K}^* \to \mathcal{K}^*$ with $x \mapsto x^2$. It is easy to prove that χ is a (multiplicative) group homomorphism. Moreover $GF(q)^*/ker\,\chi \cong im\,\chi$. From the 1st and the 3rd Homomorphism Theorem follows $|GF(q)^*|/|ker\,\chi| = |im\,\chi|$. It is $ker\,\chi = \{x \in \mathcal{K}^* | \chi(x) = x^2 = 1\}$. Two cases can occur: if $p = 2$ then $ker\,\chi = \{1\}$, if $p \neq 2$ then $ker\,\chi = \{-1, +1\}$.

If $p = 2$, then χ is a automorphism and all the elements of $GF(q)^*$ are squares. Assume $p \neq 2$. Then $\frac{|GF(q)^*|}{|ker\,\chi|} = \frac{q-1}{2} = |im\,\chi|$, hence half elements of $GF(q)^*$ are squares and half elements are non-squares.

Denote $\mathcal{Q} = im\,\chi$ and $\mathcal{N} = GF(q)^* \backslash im\,\chi$ the subset of the squares and the subset of the non-squares of $GF(q)^*$, respectively, so that $GF(q)^* = \mathcal{Q} \cup \mathcal{N}$. Clearly $\mathcal{Q}$ is a multiplicative subgroup being $\mathcal{Q} = ker\,\chi$.

Properties 1) *For every $a^2 \in \mathcal{Q}$ and $b \in \mathcal{N}$, it is $a^2 \cdot b \in \mathcal{N}$.* If $a^2 \cdot b \in \mathcal{Q}$ then $a^2 \cdot b = c^2$ and $b = c^2 \cdot (a^{-1})^2 \in \mathcal{Q}$, a contradiction.
2) *$\mathcal{N} = b \cdot \mathcal{Q}$ for a chosen and fixed element $b \in \mathcal{N}$.* Note first that $|\{b \cdot x^2 \mid x \in GF(q)^*\}| = \frac{q-1}{2} = |\mathcal{Q}| = |\mathcal{N}|$. Then the mapping $\beta : \mathcal{Q} \to \mathcal{N}$