Lecture 9: FINITE GEOMETRIES

In this lecture we study finite geometries (X, G), i.e., geometries with a finite set of points X supplied with a (necessarily finite) transformation group. The definition of finite geometry is much too general to expect a reasonable classification theorem, and so we will try to classify certain specific classes of finite geometries (which resemble Euclidean, projective and affine geometries).

§9.1. Small finite geometries

Here we try to classify all the geometries with a "small" number of points. By classifying we mean listing (without repetitions) all the geometries with a given number of points $k := |X|$ up to equivalence. Recall that two geometries are equivalent if there is a bijection between their sets of points and an isomorphism between their transformation groups which preserves the action (for the detailed definition, see Lecture 1).

There is of course only one geometry with one point. For $|X| = 2$ there are two geometries (with $|G| = 2$ and $|G| = 1$). For $|X| = 3$ there are four: the symmetries (= isometries) of the vertices of the equilateral triangle ($G = \mathbb{S}_3$), the motions of the vertices of the equilateral triangle ($G = \mathbb{Z}_{/3}$), the symmetries of the vertices of the isosceles triangle ($G = \mathbb{Z}_{/2}$). For $|X| = 4$ there are ten: the symmetries of the regular tetrahedron, its motions, the symmetries of the square, its motions, the rotations of the square by 0 and π, the symmetries of the rhombus, and four more geometries obtained when the transformation group has a fixed point (the same one for each element).

For $|X| \geq 5$ the situation becomes too complicated to handle, for $|X| \geq 10$, even a supercomputer is powerless.

To continue our study, we need to specify some reasonable classes of finite geometries. To do that, we need some algebra.

§9.2. Finite fields

The modern logical foundation of ordinary Euclidean affine geometry is the notion of vector space over the real number field (=поле действительных чисел). To construct something similar in the finite case, we need *finite fields.*

Theorem 1. *For any $q = p^m$, where p is prime (=простое) and m is a positive integer, there exists exactly one (up to isomorphism) field $GF(q)$ of $q + 1$ elements, called a Galois field. There are no other finite fields.*

We will not prove this theorem (the proof belongs to algebra courses) and only present the simplest nontrivial example $GF(4) = \{\mathbf{0}, \mathbf{1}, \mathbf{2}, \mathbf{3}, \mathbf{4}\}$ by displaying its addition and multiplication tables:

…					
+	**0**	**1**	**2**	**3**	**4**
0	**0**	**1**	**2**	**3**	**4**
1	**1**	**2**	**3**	**4**	**0**
2	**2**	**3**	**4**	**0**	**1**
3	**3**	**4**	**0**	**1**	**2**
4	**4**	**0**	**1**	**2**	**3**

…					
·	**0**	**1**	**2**	**3**	**4**
0	**0**	**0**	**0**	**0**	**0**
1	**0**	**1**	**2**	**3**	**4**
2	**0**	**2**	**4**	**1**	**3**
3	**0**	**3**	**1**	**4**	**2**
4	**4**	**3**	**3**	**2**	**1**

In order to understand the existence of $GF(q)$, $q = p^m$, for any prime p, it is useful to construct the addition and multiplication tables for, say, $GF(3^2)$.

§9.3. Example: a Galois plane for $q = 5$

In this section we will try to construct a finite affine plane geometry starting from the Galois field $F := GF(5)$. Define the *affine plane* $AGF(5)$ corresponding to F as the set $\{(x, y) | x \in F, y \in F\}$ of pairs (coordinates of *points*). As in ordinary geometry, two points $T = (a, b)$, $S = (c, d)$ determine a *vector* $\overrightarrow{TS} = \{c - a, d - b\}$. We will define *straight lines* as in analytic geometry, i.e., by setting $A(t) = A_0 + t\overrightarrow{v}$, where A_0 is a point, $\overrightarrow{v}$ is a vector, and t runs over F. For example, if we take $A_0 = (0, 0)$ and $\overrightarrow{v} = (1, 2)$, we obtain the "straight line"

$$\{(0,0), (1,2), (2,4), (3,1), (4,3)\}.$$

In the same way, we obtain a total of $30 = q^2 + q$ straight lines, q^2 points, q points on each line, and $q + 1$ lines passing through each point. Figure 1 shows the six lines passing through the point $(0, 0)$.

The same result can be obtained by using the orbit space of an appropriate geometry. Let $\mathbb{Z} \oplus \mathbb{Z} \subset \mathbb{R}^2$ be the integer lattice (=целочисленная решетка) on the plane and let $(\mathbb{Z} \oplus \mathbb{Z}, G)$ be the geometry defined by the transformation group G, isomorphic to $\mathbb{Z} \oplus \mathbb{Z}$, acting by coordinate shifts by 5, i.e.,

$$G \ni (k, l) : (m, n) \mapsto (m + 5k, n + 5l).$$

The orbit space of this action consists of 25 "points". We identify them with the 25 points of the lattice with nonnegative coordinates less than 5. The "straight line" passing through two points of this 5 by 5 square are defined as follows: construct the Euclidean line joining these two points in $\mathbb{R}^2$, take all the integer points on this line and reduce both their coordinates mod 5, obtaining three more points in the square; together with the two given points, they constitute a " straight line".

Geometrically, you can visualize this as the covering of the torus by the plane: under this map the points of the square lattice are "wrapped around" (=накручиваются на) 25 points on the torus.

§9.4. Example: a Galois plane for $q = 2^2$

We now start our construction with $F = GF(2^2)$. Define the *affine plane* $AGF(4)$ corresponding to F as the set $\{(x, y) | x \in F, y \in F\}$ of pairs (coordinates of *points*). Using the same approach as in §9.3 (including the "vector definition" of straight line), we obtain, for example, the "straight line"

$$\{(0,0),(1,1),(2,2),(3,3)\}.$$

Now consider the line passing through $(0, 0)$ along the vector $\{1, 2\}$; it consists of the points

$$\{(0,0),(1,2),(2,0),(3,2)\}.$$

But there is another line passing through the two points $(0, 0)$, $(2, 0)$, namely the "horizontal line"

$$\{(0,0),(1,0),(2,0),(3,0)\}.$$

Thus in our geometry the fundamental fact that "through two points there passes one and only one straight line" does not hold in the affine geometry with straight lines defined as above!

Nevertheless, a reasonable affine geometry can be constructed on the set of points P by defining straight lines in a different way. In particular, the "straight line" that passes through the points $(0, 0)$, $(1, 2)$ must contain two more points ($(2, 3)$ and $(3, 1)$) and is unique. In this geometry there are $16 = q^2$ points, $q^2 + q$ straight lines, q points on each line, and $q + 1$ lines pass through each point. The five lines passing through the point $(0, 0)$ are shown in Figure 2.

The details of this construction, which works for $q = p^m$, where p is any prime and m any positive integer, are left as an exercise. The result is called a *Galois plane* and is denoted by $AGF(q)$

The set $AGF(q)$ is indeed a geometry $(AGF(q), \Gamma)$ if for the transformation group Γ we take the set of all bijections of $AFG(q)$ that map lines into lines.

§9.5. Finite projective planes

Let G_q be a Galois plane for some $q = p^m$. Two lines are called *parallel* if they coincide or have no common points. Parallelism is an equivalence relation, and so all lines are partitioned into equivalence classes of parallel lines. There are $q+1$ such classes (why?). To G_q let us add $q + 1$ points (called *points at infinity*) and agree that they all lie on one straight line (the *line at infinity*). The set thus obtained is called a *finite projective plane* and is denoted by $P\mathbb{G}_q$; it has $q^2 + q + 1$ points, $q^2 + q + 1$ straight lines, $q + 1$ points on each line, $q + 1$ lines passing through each point, and any two distinct lines of $P\mathbb{G}_q$ have exactly one common point. For $q = 4$ this construction is shown in Figure 3.

§9.6. Axioms for finite affine planes

A more traditional approach to finite geometries is the axiomatic approach. A finite affine plane is a nonempty finite set of elements P (called *points*) with a family L of subsets (called it lines) that satisfy the following axioms:

Aff.1. *There exists exactly one line passing through any pair of distinct points.*

Aff.2. *There exists exactly one line parallel to a given line and passing through a given point.*

Aff.3. *There exists a generic triangle (three points not belonging to one and the same line).*

The definition of parallelism given above is appropriate for plane geometry, not for space. Indeed, under this definition skew lines (=скрещивающиеся прямые) in space would be "parallel". Here the second axiom ensures that the dimension of the set of points is less than or equal to 2. The third axiom ensures that its dimension is greater than or equal to 2. Thus the dimension of the set of points is two, this set can be regarded as a "plane". The construction of the two simplest affine planes (with 4 and 9 points) is an easy exercise.

Theorem 2. *For every $q = p^m$, where p is prime and m is a positive integer, there exists a set of q^2 points P with a family of q^2+q subsets L that satisfies the axioms* Aff.1–Aff.3. *If Γ_q is the group of bijections of P that map lines (i.e., elements of L) into lines, then (P, Γ_q) is a geometry, called a Galois plane of order q.*

The proof of this theorem is a series of problems for the exercise class.

§9.7. Axioms for finite projective planes

A finite projective plane is a nonempty finite set of elements P (called *points*) with a family L of subsets (called it lines) that satisfy the following axioms:

Proj.1. *There exists exactly one line passing through a pair of distinct points.*

Proj.2. *There exists exactly one point contained in a pair of distinct lines.*

Proj.3. *There exists a generic quadrangle (=четырехугольник общего вида), i.e., four points that determine six distinct lines (by the first axiom).*

The simplest finite projective plane (called the *Fano plane*) consists of 7 points (see Figure 4).

Theorem 3. *For every $q = p^m$, where p is prime and m is a positive integer, there exists a set of q^2+q+1 points P with a family of q^2+q+1 subsets L that satisfies the axioms* Proj.1–Proj.3. *If Γ_q is the group of bijections of P that map lines (i.e., elements of L) into lines, then $(P, \Gamma_q$ is a geometry, called the finite projective plane of order q.*

This theorem is proved by introducing "homogeneous coordinates" as in the classical case, but using the Galois group instead of $\mathbb{R}$; see the problems for the exercise class.

Remarks (1) One can pass from the Galois plane to the projective plane by adding $q+1$ "points at infinity" (corresponding to each class of parallel lines) and one new line (the line of all points at infinity). Conversely, one can pass from the projective plane to the Galois plane by removing one line (with all its points). Unfortunately, the result is not well defined (=не является корреткно определенным): it may depend on the choice of the line!

(2) There is no uniqueness theorem for projective planes of order q. For example, there is are several non-isomorphic projective planes of order 9, and several non-isomorphic Galois planes of order 9 as well!

(3) The classification problem for finite projective planes is one of the hardest and most famous unsolved problems of elementary mathematics.

FIGURE 1. Five lines in $AGF(4)$

FIGURE 2. Six lines in $AGF(5)$

FIGURE 3. Projectivization of $AGF(4)$

FIGURE 4. The Fano plane