Summer School “Giuseppe TALLINI”
Brescia, 8–13 July 2002

Planes, permutations, perspectivities

Arrigo BONISOLI
Dipartimento di Scienze Sociali, Cognitive e Quantitative
Università di Modena e Reggio Emilia
via Giglioli Valle
42100 Reggio Emilia (Italy)

Please send all remarks to the author’s e–mail address:
bonisoli.arrigo@unimore.it

version of 18 July 2002

Many discrete structures are of interest in geometry. That was already true in 1968 when Peter Dembowski chose the plural “Finite Geometries” as the title of his famous book. It is even more so today. Still, planes always deserve special attention. These lectures will attempt to explain why, at least from my own very personal point of view. Planes, permutations and perspectivities will be recurrent *notes* in the themes I want to develop, so here we go with our “Variations on three p’s”

Two little warnings before we start. First of all the audience is very composite, consequently the level of these lectures will not meet everyone’s taste. I will spend some time on material which is now considered “standard,” but I will also try to touch some results which are part of current research. So maybe the pace will increase as we go on. Secondly, I have used Dembowski’s book as a major source of information, especially for quotations, which are usually given at length in the text. Sometimes I could check the sources, sometimes I could not. I make no claim of thoroughness, nor of absolute correctness, especially when stating priorities in proving results and the like. Anyone spotting errors of any sort is kindly urged to let me know.

My acquaintanceship with the group in Brescia extends over the past two decades, since my initial meeting with Mario Marchi at an “Arbeitstagung über Geometrie” that was being organized by Helmut Karzel in Munich in February 1982. I am therefore very grateful to the organizers for their invitation and for the careful schedule arrangements which made my participation possible.

1 Are finite projective planes geometric or combinatorial objects?

Many great mathematicians worked on the foundations of geometry between the end of the nineteenth and the beginning of the twentieth century. It will be sufficient to mention David Hilbert in Europe and Oswald Veblen in North America. The italian school was also involved in the discussion on the foudations of geometry. I just mention that Fano and Veronese, two names which are frequently encountered in Finite Geometry, both wrote papers on this subject. This theme is very wide and I do not want to go into it any further and so I will simply quote the lecture *I geometri italiani e il problema dei fondamenti (1889–1899)* that Umberto Bottazzini gave at the 1999 Congress of the Unione Matematica Italiana in Naples, the printed version of which appears in the Bollettino U.M.I., La matematica nella Società e nella Cultura, Serie VIII, Vol IV-A, Agosto 2001, 281–329.

For my purposes it will be sufficient to remark that projective geometries of “dimension 2” were established in those years to be of a somewhat special kind. As a matter of fact, a projective space of dimension at least three can always be coordinatized by a non–necessarily–comutative division ring, a so called skew–field. Essentially, in these spaces the use of homogeneous coordinates is allowed in much the same way as for complex or real projective geometry, once the multiplication of scalars from the left or from the right has been agreed upon.

From the point of view of the system of axioms required to describe it, a **projective plane** is the "simplest" kind of a projective geometry. That is in fact a point–line incidence structure in which any two distinct points lie on a unique common line, any two distinct lines have a unique common point and satisfying a non–degeneracy condition assuming the existence of four points, no three of which lie on a common line.

It was Hilbert himself that exhibited a projective plane in which the coordinate structure was not a skew–field. The algebraic properties of the coordinate structure were soon connected to the validity of Desargues' theorem and so people started talking of non–desarguesian projective planes.

Projective geometry admits a finite model since finite (skew–)fields exist. This fact is important both from a conceptual point of view and from the point of view of the methods which can be employed in research. A mathematical theory admitting a finite model is non–contradictory, no matter how funny the logic you have adopted may be...! Hence we know that we are working on solid foundations. On the other hand a structure which has finitely many entities allows counting, no matter how difficult the counting may be. Increasing interest in finite structures arose during the two world wars, when the theory of designs grew from the work of F. Yates and R.C. Bose.

In modern terminology a finite projective plane is nothing but a 2–$(v, k, 1)$ design in which the parameters v and k have the form

$$v = n^2 + n + 1, \qquad\qquad k = n + 1$$

for some integer $n \geq 2$ which is called the **order** of the plane. It is a **symmetric** design, that is one in which the total number b of blocks is equal to the total number v of points and consequently the number r of blocks through any given point is equal to the number k of points on any given block.

How can we study finite projective planes? The following quotation from the **Introduction** to P. Dembowski's *Finite Geometries*, Springer, Berlin 1968, traces the beginning of the general approach based on collineation groups:

> " ... An alternative approach to the study of projective planes began with a paper by BAER 1942 in which the close relationship between Desargues' theorem and the existence of central collineations was pointed out. Baer's notion of (p, L)–transitivity, corresponding to this relationship, proved to be extremely fruitful. On the one hand, it provided a better understanding of coordinate structures (here SCHWAN 1919 was a forerunner); on the other hand it led eventually to the only coordinate–free, and hence geometrically satisfactory, classification of projective planes existing today, namely that by LENZ 1954 and BARLOTTI 1957 ... "

Non–desarguesian finite projective planes do exist as O. Veblen and J.H.M. Wedderburn showed in their paper *Non–Desarguesian and non–Pascalian geometries*, Transactions of the American Mathematical Society 8 (1907) 379–388. It is no wonder that progress in the study of finite projective planes from the point of view of collineations and coordinate structures was influenced and sometimes was a source of motivation for corresponding progress in the study of algebraic systems of various nature.

What is the existence spectrum for 2–$(v, k, 1)$ designs? This very basic combinatorial question becomes even more intriguing for finite projective planes. What are the orders of finite projective planes, that is what are the possible values of n? A finite field of order n exists if and only if n is a prime power, hence the orders of finite *desarguesian* planes are precisely the prime powers. Designs with the strangest values for k and v exist, so there is no *a priori* reason prohibiting the existence of a finite projective plane whose order is not a prime power. The fact is that every finite projective plane constructed thus far has prime power order, while no proof is available of the assertion that this MUST be the case. The best piece of information that we have in this direction is still the result by R.H. Bruck, H.J. Ryser, *The non–existence of certain finite projective planes*, Canadian Journal of Mathematics 1 (1949) 88–93.

Proposition 1.1 *Assume n is congruent to 1 or 2 $\bmod 4$. If there exists a finite projective plane of order n then n can be expressed as a sum of two integral squares.*

As the title of the original paper stresses, this theorem excludes the existence of a projective plane of order 6, 14, 21 and infinitely many other values of n. Unfortunately it says nothing about $n = 10$, 12, 15 and infinitely many others. The case $n = 10$ is a very instructive story: anyone wishing to know the details is encouraged to read the extremely well written report by C.W.H. Lam, *The search for a finite projective plane of order* 10, American Mathematical Monthly 98 (1991) no. 4, 305–318.

Geometric or combinatorial? I do not know what the ultimate answer is or will be. The Bruck–Ryser theorem itself addresses a question which is probably combinatorial in nature, but looking at the proof one actually realizes that it is a theorem on quadratic forms, and so here comes geometry again. The results that I am going to present will probably suggest that finite projective planes are BOTH geometric AND combinatorial entities, a point of view that I am certainly willing to subscribe.

I shall usually denote by π a finite projective plane of order n. Unlike Dembowski I grew up with the idea that points of π should be denoted by latin capitals such as P, Q, R, whereas lines of π should be denoted by small latin letters such as a, b, c, ℓ. I will stick to this convention whenever possible.

An **arc** in π is a set of points no three of which are collinear. An **oval** in π, which I will usually denote by Ω, is an arc admitting a unique tangent line at any one of its points. The combinatorics of ovals in finite projective planes is assumed (see the textbook by D.R. Hughes, F.C. Piper, *Projective Planes*, Springer, Berlin 1971), in particular an arc is an oval if and only if it has cardinality $n+1$, or, as people more frequently say, it is an $(n+1)$–arc.

In case n is even, I usually denote by Ω' the union of an oval Ω with its nucleus. That is an $(n+2)$–arc, a so called **hyperoval** and, conversely, each point of a hyperoval is the nucleus of the oval which remains after the deletion of the point.

If n is odd, then the points not on the oval Ω are of two kinds: those which lie on precisely two tangents are called **external** points, while those which lie on no tangent are called **internal** points. There are $(n+1)n/2$ external points and $(n-1)n/2$ internal points.

A **subplane** of a projective plane π consists of some points and some lines of π forming themselves a projective plane with respect to the incidence induced by that of π. The following result was proved in R.H. Bruck, *Difference sets in a finite group*, Transactions of the American Mathematical Society 78 (1955) 464–481.

Proposition 1.2 *If a finite projective plane of order n has a proper subplane of order m then $n = m^2$ or $n \geq m^2 + m$.*

A subplane of order m of a projective plane of order m^2 is called a **Baer subplane**. It has the remarkable property that every point of the plane is incident with some line of the subplane and every line of the plane is incident with some point of the subplane. Combinatorics shows that a line in the Baer subplane meets the Baer subplane in $m+1$ points, while a line not in the Baer subplane meets the Baer subplane in precisely one point. A similar statement holds for the number of lines in the Baer subplane through a given point: this number is $m+1$ if the point lies in the Baer subplane, 1 if not.

An example of a subplane can be obtained in a desarguesian plane $PG(2,F)$ by taking points and lines whose coordinates lie in some subfield K of F. Such a subplane is usually called a *subfield subplane* (another frequent terminology is *subplane in canonical position*). In the finite case we have $F = GF(p^e)$ and $K = GF(p^d)$ for some divisor d of e and so the subfield subplane will be a Baer subplane if and only if $e = 2d$.

2 A review of permutation groups and sets

Some textbooks dealing specifically with permutation groups:

- H. Wielandt, *Finite permutation groups*, Academic Press, New York 1964.
- D.S. Passman, *Permutation groups*, Benjamin, New York 1968.
- N.L. Biggs, A.T. White, *Permutation Groups and Combinatorial Structures*, Cambridge Univ. Press, Cambridge 1979.
- J.D. Dixon, B. Mortimer, *Permutation Groups*, Springer, Berlin 1996.

Some textbooks on group theory with sections devoted to permutation groups:

- M. Hall, *The Theory of Groups*, Macmillan, New York 1959.
- B. Huppert, *Endliche Gruppen I*, Springer, Berlin 1967.
- J.S. Rose, *A course on group theory*, Cambridge Univ. Press, Cambridge 1978.

In Italian:

- A. Machì, *Introduzione alla teoria dei gruppi*, Feltrinelli.
- G. Zappa, *Fondamenti di teoria dei Gruppi*, Cremonese, Roma I 1965, II 1970.

If X is a finite set of cardinality n we shall denote by $\mathrm{Sym}(X)$ or $\mathrm{Sym}(n)$ or S_n the full symmetric group of degree n, that is the group of all permutations on X. We shall denote by $\mathrm{Alt}(X)$ or $\mathrm{Alt}(n)$ or A_n the alternating group of degree n, that is the group of all **even** permutations on X. Note that n here might have nothing to do with the order of a finite projective plane.

We shall call a **permutation set of degree** n an arbitrary subset G of S_n. If the subset is a subgroup then we shall speak of a **permutation group of degree** n.

Besides the functional notation, I shall often use the exponential notation for permutations, which means if g is a permutation on Ω and x is an element of Ω I denote by x^g the image element of x under g. The choice of notation will be evident from the context or it will be set by some explicit remark.

2.1 Actions

Let X be a set and let G be a group. We shall say that G **acts** or **operates** on X if a mapping $\mu : X \times G \to X$ is defined, for which we shall write x^g instead of $\mu\big((x,g)\big)$, satisfying the following properties:

1) $x^{gh} = (x^g)^h$, for all $x \in X$, $g, h \in G$;

2) $x^1 = x$, for all $x \in X$ (where 1 denotes the identity element of G).

Proposition 2.1 *Let G be a group acting on the set X. For each element $g \in G$ the mapping $\varphi_g : X \to X$, $x \mapsto x^g$ is a permutation on X. The mapping $\varphi : G \to \mathrm{Sym}(X)$, $g \mapsto \varphi_g$ is a group homomorphism. It is sometimes called the* **permutation representation** *of G on X or the* **representation** *of G as a* **permutation group** *on X.*

In order to define an action of a group G on a set X it is sufficient to know the homomorphism φ, in which case x^g is defined as x^{φ_g}. Therefore the study of the actions of a given group on a given set essentially amounts to the study of the homomorphisms mapping that group to the full symmetric group on the given set.

2.2 Notation and some definitions

The kernel of the homomorphism φ is called the **kernel** of the representation and is sometimes denoted by $G_{(X)}$. The quotient group $G^X = G/G_{(X)}$, which is isomorphic to a subgroup of $\mathrm{Sym}(X)$, is called the group **induced** by G on X. If the kernel of the representation φ is trivial then we say that G acts **faithfully** on X or that the action of G on X is **faithful**. In such case φ is an isomorphism and G turns out to be isomorphic to a permutation group on X.

We say that the action of G on X is **transitive** or that G is **transitive** on X if whenever x, y are (not necessarily distinct) elements of X there exist a group element $g \in G$ with $x^g = y$. More generally we define the G–**orbit of** x to be the set

$$\mathrm{orb}_G(x) = \{x^g\,;\, g \in G\}.$$

The orbits of the group G on X form a partition of the set X. A transitive group G on X is said to be **regular** if whenever x and y are in X there exists a unique group element g in G with $x^g = y$.

Example a). The general linear group $G = GL(d, F)$ consists of all non–singular $d \times d$ square matrices with entries in the field F. The group G acts on the set X of all non–zero vectors in F^d.

Example b). The group G also acts on the set Y consisting of all 1–dimensional vector subspaces of F^d. We have that $G_{(Y)}$ is the subgroup of scalar matrices, (matrices of type λI_d with $\lambda \in F^*$. We have thus $G^Y = PGL(d, F)$.

Example c). Let G be a group, let H be a subgroup of G (we write $H \leq G$). Let $\Omega = (G : H)$ be the set of all right cosets of H in G. The action of G on $(G : H)$ by right multiplication is defined by $\mu\big((Hx, g)\big) = Hxg$.

Example d). Let X be a set of cardinality 10. Let G be the subgroup of S_{10} preserving the Petersen graph on the vertex–set X. The group G is isomorphic to S_5 in its action on the set of all 2–element subsets of $\{1, 2, 3, 4, 5\}$. This action is faithful.

Example e). Each group can be regarded as a regular permutation group on itself: $\varphi_g : G \to G$, $x \mapsto xg$. The representation φ is known as the right regular Cayley representation. This theorem shows that the whole theory of groups can in principle be embodied into the theory of permutation groups.

Example f). A group G acts on itself by conjugation: for any elements x, g in G define $x^g = g^{-1}xg$. The orbits in this action are the conjugacy classes of elements of G. For example two elements of $\mathrm{Sym}(n)$ are conjugate if and only if their decomposition into disjoint cycles has the same shape. Quite similarly G acts on the set of its subgroups by conjugation: if $H \leq G$ and g is an element of G we define $H^g = g^{-1}Hg$. The orbits of this action are the conjugacy classes of subgroups G.

2.3 Stabilizers

The subgroup $G_x = \{g \in G;\ x^g = x\} \leq G$ is called the **stabilizer** of the element x in G.

Proposition 2.2 i) *If $y = x^g$ then $G_y = g^{-1}G_x g$.* ii) *If the group G is transitive on X then*

$$G_{(X)} = \bigcap_{y \in X} G_y = \bigcap_{g \in G} g^{-1}G_x g$$

is the largest subgroup of G_x which is normal in G.

A transitive group is regular if and only if the stabilizer G_x of one element is reduced to the identity.

Proposition 2.3 (Lagrange). $|\mathrm{orb}_G(x)| = |G : G_x|$.

Proof. It is sufficient to observe that $x^g = x^h$ implies $gh^{-1} \in G_x$, that is g and h lie in one and the same right coset of G_x in G. □

If the group G acts on X and Y is a subset of X then we define $Y^g = \{y^g\,;\, y \in Y\}$. The **setwise stabilizer** of Y in G to be the subgroup of G consisting of all group elements g such that $Y^g = Y$ holds. The **elementwise** (or **pointwise**) **stabilizer** of Y in G is defined to be the subgroup of G consisting of all group elements g such that $y^g = y$ holds for each element $y \in Y$. We sometimes denote by $G_{\{Y\}}$ and $G_{(Y)}$ the setwise and elementwise stabilizer of Y in G respectively. If $Y = \{y_1, \ldots, y_r\}$ we shall also denote by $G_{y_1 \ldots y_r}$ the elementwise stabilizer of Y in G.

A group G is said to act **semiregularly** on X if the stabilizer G_x reduces to the identity for each $x \in X$. In the finite case Lagrange's theorem shows that if G acts semiregularly on X then all G–orbits on X have the same length and this length is equal to the group order $|G|$, which is thus a divisor of $|X|$.

2.4 Comparison of actions

Suppose that a given group G acts simultaneously on the set Γ and on the set Σ. These actions are said to be **isomorphic** if there exists a bijective mapping $\varphi : \Gamma \to \Sigma$ such that the relation

$$\varphi(x^g) = (\varphi(x))^g$$

holds for x in Γ. Note that x^g is an element of Γ, while $\varphi(x)$ is an element of Σ. Note further that $G_x = G_{\varphi(x)}$.

Proposition 2.4 *If G acts transitively on X and $x \in X$ then the actions of G on X and of G on $(G : G_x)$ are isomorphic.*

Proof. Define $\varphi : (G : G_x) \to X$, $G_x g \mapsto x^g$. This is a well defined bijective mapping. It yields an isomorphism of actions because the relation $\varphi\big((G_x h)g\big) = \varphi(G_x hg) = x^{hg} = (x^h)^g = \big(\varphi(G_x h)\big)^g$ holds. □

Proposition 2.5 *If $H, K < G$, then the actions of G on $(G : H)$ and on $(G : K)$ are isomorphic if and only if the subgroups H and K are conjugate in G.*

Proof. The actions in question are transitive. In each such action the stabilizers are thus conjugate. The stabilizer of the coset Hx in the action of G on $(G : H)$ by right multiplication is the subgroup $x^{-1}Hx$. The stabilizer of the coset Kx in the action of G on $(G : K)$ by right multiplication is the subgroup $x^{-1}Kx$.

If the two actions are isomorphic and $\varphi : (G : H) \to (G : K)$ realizes the isomorphism then the stabilizer of Hx is equal to the stabilizer of $\varphi(Hx) = Ky$, that is $x^{-1}Hx = y^{-1}Ky$. From that, we obtain the relation $K = (xy^{-1})^{-1}H(xy^{-1})$.

Suppose conversely that $K = g^{-1}Hg$ holds for some element g in G. Define $\varphi : (G : H) \to (G : K)$, $Hx \mapsto Kg^{-1}x$. It is verified that φ yields an isomorphism betweeen the two actions. □

Example d) **revisited.** Set $G = S_5$ and let Ω be the set of all transpositions in S_5; the group G acts on Ω by conjugation. The stabilizer of the transposition (12) in this action is its centralizer (the subgroup consisting of all permutations commuting with the given transposition): this stabilizer is isomorphic to the direct product $S_2 \times S_3$. Hence this action can equivalently be seen on $(S_5 : S_2 \times S_3)$ or on the set of all 2–element subsets of a set of cardinality five. In order to obtain the Petersen graph, we join two transpositions by an edge if and only if they commute.

Let the group G act on Γ, let the group H act on Σ. We shall say that the two actions are **similar** if there exists a bijective map $\varphi : \Gamma \to \Sigma$ and a group isomorphism $\psi : G \to H$ such that the relation $\varphi(x^g) = (\varphi(x))^{(\psi(g))}$ holds for x in Γ.

Example g). Set $G = GL(d, F) = H$. Let Γ be the set of all 1–dimensional vector subspaces of F^d. Let Σ be the set of all hyperplanes, that is the set of all $(d-1)$–dimensional vector subspaces of F^d. The natural actions of G on Γ and of H on Σ are similar, if one defines, with the obvious meaning of symbols,

$$\varphi : \Gamma \to \Sigma, \quad (a_1, \ldots, a_d) \to [a_1, \ldots, a_d], \qquad \psi : G \to H, \quad A \to (A^t)^{-1}.$$

For $d > 2$ these actions are not isomorphic.

Example h). The subgroups G, H of $\mathrm{Sym}(X)$ are conjugate in $\mathrm{Sym}(X)$ if and only if the actions of G and H on X are similar.

2.5 Applications of the concept of group action to the Theory of Groups

Perhaps the most famous of all such applications is the following famous property of finite groups

Proposition 2.6 (Sylow's Theorem). *Let G be a finite group with $|G| = p^m r$ where p is a prime, $m \geq 0$ and r is a positive integer which is not divisible by p.*

(a) *The group G admits a subgroup of order p^m. Such a subgroup is called a* **Sylow p–subgroup of** *G.*

(b) *If H is a Sylow p–subgroup of G and J is a p–subgroup of G then we have $J \leq H^g = g^{-1}Hg$ for a suitable $g \in G$. In particular, any two Sylow p–subgroups are conjugate in G.*

(c) *Denoting by $\mathcal{S}_p$ the set of all Sylow p–subgroups of G and setting $n = |\mathcal{S}_p|$ we have $n = |G : N_G(H)|$, n is a divisor of r and the relation $n \equiv 1 \mod p$ holds* (here $N_G(H)$ denotes the *normalizer* of H in G).

Proof. The proof by H. Wielandt can be found for example in the textbooks by Huppert or Rose. □

2.6 Multiple transitivity and primitivity

Let k be an integer with $k \leq |X|$. We shall say that the group G acts k–transitively on X if whenever $(x_1, x_2, \ldots, x_k)$, $(y_1, y_2, \ldots, y_k)$ are k–tuples of distinct elements of X there exists a group element $g \in G$ such that the relation $x_i^g = y_i$ holds for $i = 1, 2, \ldots, k$.

Note that 1–transitivity is the same as transitivity. Furthermore, k–transitivity implies $(k-1)$–transitivity for $k \geq 2$.

A group G acting k–transitively on X is said to act **sharply** k–transitively on X if the group element g subject to $x_i^g = y_i$ for $i = 1, 2, \ldots, k$ is not only assumed to exist but it is also assumed to be **unique**. It is immediately seen that this request is equivalent to the assumption that the elementwise stabilizer of any k distinct elements reduces to the identity.

Sharp 1–transitivity is the same as regularity.

Let G be a group acting on X and let Δ be a subset of X. For $g \in G$ we define $\Delta^g = \{x^g \, ; \, g \in G\}$. We shall say that Δ is a **block of imprimitivity** (or simply a block) for G on X if for each $g \in G$ we either have $\Delta^g = \Delta$ or $\Delta^g \cap \Delta = \emptyset$.

Let G be a transitive on X. If Δ is a block of imprimitivity for G on X then the family $\mathcal{F} = \{\Delta^g \, ; \, g \in G\}$ is a partition of X. It is fairly easy to see that G acts on $\mathcal{F}$, in other words $\mathcal{F}$ is a G–invariant partition of X. If, conversely, a G–invariant partition is assigned, then its members are blocks of imprimitivity for G on X. That is the reason why such a G–invariant partition is called a **system of blocks of imprimitivity** for G on X. For a transitive group G it is thus essentially equivalent to assign a single block of imprimitivity or a full system of blocks of imprimitivity.

A group acting transitively on X always admits two systems of blocks of imprimitivity, the one consisting of the single block X and the one consisting of all singletons $\{x\}$ as x varies in X. These are called the **trivial** systems of blocks of imprimitivity.

Let the group G act transitively on X. We say that G acts **primitively** on X if the unique systems of blocks of imprimitivity for G on X are the trivial ones. A transitive group is primitive if and only if the stabilizer of one element is a maximal subgroup.

Proposition 2.7 *If G is 2–transitive on X then G is primitive.*

Proof. Let Γ be a block with $|\Gamma| \geq 2$. Let $x, y \in \Gamma$, $x \neq y$. For each $u \in X$ there exists $h \in G$ with $x^h = x$, $y^h = u$. Hence $x \in \Gamma^h \cap \Gamma$, $\Gamma^h = \Gamma$, $u \in \Gamma^h = \Gamma$, $X \subseteq \Gamma$. □

Proposition 2.8 *Let G be a group acting transitively on X. We have that G is k–transitive on X if and only if G_x is $(k-1)$–transitive on $X \setminus \{x\}$.*

Proposition 2.9 *If G is k–transitive on X then $n(n-1)\ldots(n-k+1)$ is a divisor of $|G|$ and the equality $|G| = n(n-1)\ldots(n-k+1)$ holds if and only if G is sharply k–transitive on X.*

Example i). S_n is sharply n–transitive on $\{1, 2, \ldots, n\}$.

Example ii). A_n is sharply $(n-2)$–transitive on $\{1, 2, \ldots, n\}$.

Example iii). $PGL(2, F)$ is 3–transitive but not 4–transitive (except for $|F| = 3$). The 3–transitivity is sharp.

Example iv). $PGL(d, F)$ is 2–transitive but not 3–transitive if $d > 2$, since it cannot map a triple of collinear points to a triple of non–collinear points.

A normal subgroup of a group G containing no proper subgroup which is normal in G is called a **minimal** normal subgroup of G. The following result goes back to W. Burnside, *Theory of groups of finite order*, Cambridge Univ. Press, Cambridge 1911, p.202:

Proposition 2.10 *A* 2*–transitive group has a unique minimal normal subgroup, which is elementary abelian or simple.*

The statement of Burnside's theorem is sufficient to explain the interest in simple groups. As a matter of fact the classification of finite simple groups has produced, among other important consequences, a classification of finite primitive permutation groups, the so called O'Nan–Scott theorem. A proof of this result is presented in the paper by M.W. Liebeck, C. Praeger, J. Saxl, *On the O'Nan–Scott theorem for finite primitive permutation groups*, Journal of the Australian Mathematical Society 44 (1988) 389–396. I also refer to the paper P.J. Cameron, *Finite permutation groups and finite simple groups*, Bulletin of the London Mathematical Society 13 (1981) 1–22 for a more thorough account of the role of simple groups.

We conclude with a property which will be useful later on.

Proposition 2.11 *Let H be a permutation group on a finite set X and assume that there exists a prime p such that for each $x \in X$ there is an element of order p in H fixing x and no other element of X. Then H is transitive on X.*

Proof. Assume Y and Z are distinct orbits of H on X. Pick an element $y \in Y$: since there exists a permutation in H fixing y and permuting all other elements of X into cycles of length p, we see that p divides both $|Y| - 1$ and $|Z|$. Taking an element $z \in Z$ instead and repeating the same argument, we see that p divides $|Y|$ and $|Z| - 1$, a contradiction. There is thus just one H–orbit,that is X itself. □

3 Collineation groups: some classics and the role of perspectivities

A *collineation* of a projective plane π is simply an automorphism of π. The action of a collineation is faithful on the point–set of π (it is also faithful on the line–set of π) and so I shall usually identify a collineation with the permutation it induces on the point–set of π. Here is a quick review of some elementary but important properties of collineations.

Proposition 3.1 *A collineation in a* (*not necessarily finite*) *projective plane π fixing every point on each of two distinct lines is the identical collineation.*

Proof. Let ℓ_1 and ℓ_2 be the pointwise fixed lines and let Q be their common point. Let P be a point off ℓ_1 and ℓ_2. Consider two distinct points A_1 and B_1 on ℓ_1 other than Q. Let the line PA_1 meet ℓ_2 in A_2. Let the line PB_1 meet ℓ_2 in B_2. Since A_1 and A_2 are distinct fixed points on the line PA_1, we have that this line is fixed and, similarly, the line PB_1 is fixed. The point P is the common point of two distinct fixed lines and so it is itself a fixed point. □

Proposition 3.2 *A collineation in a* (*not necessarily finite*) *projective plane π fixing every point on one line and two further points off the line is the identical collineation.*

Proof. The same argument of the previous proof shows that each point off the pointwise fixed line and off the line joining the two extra fixed points is itself a fixed point. So there must be a further line which is pointwise fixed and we are back to the case of the previous proposition. □

3.1 Perspectivities

An **axial** collineation is one fixing each point of a line ℓ, called the **axis**. A **central** collineation is one fixing each line through a point C, called the **center**.

Proposition 3.3 *Each axial collineation is central. Each central collineation is axial. The fixed points of a non–identical central collineation are the center itself and all points on the axis, while the fixed lines are the axis and all lines through the center. A central collineation g is completely determined by its center C, its axis ℓ and the mapping $P \mapsto P^g$ of any point P not on ℓ and different from C.*

Proof. Let g be a non–identical axial collineation with axis ℓ. If g fixes a point C off the axis ℓ, then each line though C is fixed, since it contains two distinct fixed points, namely C and the point of intersection with ℓ. Hence C is the center of g in this case.

Assume g fixes no point off the line ℓ. Consider an arbitrary point P off the line ℓ. The point P^g is distinct from P. The line a joining P to P^g meets ℓ at a fixed point A and we have thus $a = AP = AP^g = A^gP^g = a^g$. Hence every point P off the axis lies on a fixed line. Should two such fixed lines meet off the axis ℓ, then their common point would be a fixed point off the axis, contradicting our assumption. Hence any two fixed lines meet in one and the same point of the axis which is thus the center of g.

We have proved that a collineation with an axis must also have a center. The dual argument shows that each central collineation is axial. The statement on fixed points and fixed lines is an immediate consequence of the two previous propositions.

It is immediately seen that if two central collineations have distinct centers then they have distinct actions on at least one point off the axes and off the line joining the centers. Similarly, two axial collineations with distinct axes have distinct actions on at least one line.

Assume g and h are central collineations with the same center C and the same axis ℓ. If there exists a point P distinct from the center and off the axis with $P^g = P^h$, then the collineation gh^{-1} fixes each point on ℓ, each line through C and the point P, and so gh^{-1} is the identity. □

A **perspectivity** is a central collineation. Since a central collineation is also an axial collineation, it turns out that the terms *perspectivity*, *central collineation* and *axial collineation* are synonymous. We shall speak for short of a C–ℓ perspectivity to mean a perspectivity with center C and axis ℓ. We distinguish further between a **homology** when the center lies off the axis and an **elation** when the center is on the axis.

The fixed points of a non–identical perspectivity are the center itself and all points on the axis; the fixed lines are the axis and all lines through the center. A perspectivity acts thus semiregularly on the points of each line through the center other than the center itself and the point of intersection of the line with the axes (dually: on the lines of each pencil through a point of the axis other than the axis itself and the line of the pencil through the center). The case of a perspectivity of order 2 will be of special interest and we record it as a separate statement.

Proposition 3.4 *A perspectivity of order* 2 *of a finite projective plane is an elation or a homology according as the order of the plane is even or odd respectively.* □

The set of all collineations of π with given center or with given axis or with given center and axis clearly forms a group. More generally, for a given collineation group G of π one can consider the subgroups of G consisting of all perspectivities with given center C or with given axis ℓ or with center C and axis ℓ: these subgroups will be denoted by $G(C)$, $G(\ell)$ and $G(C, \ell)$ respectively.

Proposition 3.5 *Let A and B be distinct points on a line ℓ. Let g be a non–identical A–ℓ elation. Let h be a non–identical B–ℓ elation. The product gh is an elation with axis ℓ whose center C is different from both A and B.*

Proof. Clearly gh is an axial collineation with axis ℓ. In order to see that gh is an elation we must show it does not fix any point off the axis ℓ. Let P be one such point and assume $P^{gh} = P$. Then $P^g = P^{h^{-1}}$, the points A, P, P^g are collinear and so are the points B, P, $P^{h^{-1}}$. Since $P \neq P^g$ and $P \neq P^{h^{-1}}$ the relation $P^g = P^{h^{-1}}$ forces $A = B$, a contradiction. Hence $f = gh$ is an elation with axis ℓ.

Let C denote the center of f. If $C = A$ then $h = g^{-1}f$ should also be an elation with center A, a contradiction. Similarly we cannot have $C = B$ and the assertion is proved. □

3.2 Local versus global properties

Given a point C and a line ℓ we say that the plane π is C–ℓ **transitive** if for any pair of distinct points P and Q which are collinear with C and not on ℓ there exists a C–ℓ perspectivity mapping P to Q.

It is known that the existence of central collineations is related to the validity of special instances of Desargues' theorem.

Proposition 3.6 *A plane π is C–ℓ transitive if and only if the Theorem of Desargues holds for all triangles which are perspective with respect to C and having two pairs of corresponding sides intersect on ℓ, whence the third pair also intersect on ℓ.*

Proof. A thorough discussion can be found in §20.2 of M. Hall, *The Theory of Groups*, Macmillan, New York 1959. □

The detailed analysis of the "configuration" formed by the point–line pairs (C, ℓ) for which the plane π is C–ℓ transitive is the essence of the so called Lenz–Barlotti classification that was mentioned in lecture 1. A projective plane is said to be **desarguesian** if the theorem of Desargues holds universally. In view of the previous result a projective plane is desarguesian if and only if it is C–ℓ transitive for each possible point–line pair (C, ℓ). In the language of the Lenz–Barlotti classification such a plane is of Lenz–Barlotti type VII.2, the highest possible.

A line ℓ of π such that for each point P on ℓ the plane π is P–ℓ transitive is said to be a **translation line** and π is said to be a **translation plane** with respect to ℓ. In this case every conceivable elation with axis ℓ actually exists.

Proposition 3.7 *A sufficient condition for a line ℓ to be a translation line for the plane π is that π be A–ℓ transitive and B–ℓ transitive for two distinct points A, B on ℓ.*

Proof. Let P, Q be distinct points off the line ℓ such that the line PQ meets ℓ at a point C which is different from both A and B. Let the lines AP and BQ meet at a point R. Let g be the A–ℓ elation mapping P to R; let h be the B–ℓ elation mapping R to Q. Then gh is an elation with axis ℓ such that $P^{gh} = R^h = Q$ holds, and so the center of gh is C. We have proved that π is C–ℓ transitive. □

Translation planes form a chapter of their own in the theory of finite planes. They can be studied from different points of view. The most famous textbook on this subject is perhaps H. Lüneburg, *Translation planes*, Springer, Berlin, 1980. The most recent treatment is probably that by M. Biliotti, V. Jha, N.L. Johnson, *Foundations of Translation Planes*, Dekker, New York, 2001.

Proposition 3.8 (Baer). *Let G be a collineation group of π. If for two distinct centers A and B on ℓ the groups $G(A, \ell)$ and $G(B, \ell)$ are non–trivial, then the subgroup T consisting of all elations with axis ℓ in G is elementary abelian.*

Proof. Take non–identical elations $g \in G(A, \ell)$ and $h \in G(B, \ell)$ and let P be a point not on ℓ. The points A, P, P^g are on a line a, the points B, P, P^h are on a line b. The points A, P^h, P^{hg} are also on a line a' and the points B, P^g, P^{gh} are on a line b'. We have $a' = a^h$ and $b' = b^g$, hence the common point of a' and b' must be simultaneously equal to P^{hg} and to P^{gh}. We conclude that $P^{hg} = P^{gh}$ holds for each point P off the line ℓ. Since the relation also holds for all points on ℓ, we have $hg = gh$.

We have proved that g commutes elementwise with each group $G(C, \ell)$ whenever C is a point on ℓ different from A. Let g' be a non–identical collineation in $G(A, \ell)$ with $g' \neq g$. We know from Proposition 3.5 that $g'h$ is a C–ℓ elation for some center C which is different from both A and B. As before we must have $g(g'h) = (g'h)g$, whence also $(gg')h = g(g'h) = (g'h)g = g'(hg) = g'(gh) = (g'g)h$, that is $(gg')h = (g'g)h$, yielding $gg' = g'g$. We have proved that any two elations with axis ℓ in G commute and so T is abelian.

As a non–trivial finite group T contains some element g of prime order p. Assume g is an A–ℓ elation. Let h be a non–identical B–ℓ elation in G with $B \neq A$. Then gh is a C–ℓ elation in G with $C \neq A, B$. We have $(gh)^p = g^p h^p = h^p$. Since $(gh)^p \in G(C, \ell)$, $h^p \in G(B, \ell)$ and these subgroups have only the identity in common, we see that h^p is the identity.

Hence the fact that g has order p implies that every non–trivial elation in G with axis ℓ and center different from A has order p. Similarly, the fact that h has order p implies that every non–trivial elation in $G(A, \ell)$ has order p.

We have proved that T is an abelian group in which every non–trivial element has order p, that means T is an elementary abelian p–group. □

3.3 Involutions and Baer collineations

Consider a plane π of square order n admitting a Baer subplane. A **Baer collineation** g of π is a collineation fixing a Baer subplane π_0 elementwise (pointwise and linewise). An involution (collineation of order 2) which is a Baer collineation is called a **Baer involution**.

Proposition 3.9 (Baer). *Let g be an involution of a finite projective plane π of order n. Then either n is a square and g is a Baer involution or g is a perspectivity.*

Proof. Assume the point P is not fixed by g. Then P and P^g are distinct points which are exchanged by g, and so the line joining them is a line through P which is fixed by g.

Assume the point P is fixed by g. Let Q be another point and assume the line $\ell = PQ$ is not fixed by g. Then the point Q^g is not on ℓ and we have $\ell^g = PQ^g$. Take a point R on ℓ other than P, Q. The point R^g is on ℓ^g and is distinct from P and Q^g. The lines RQ^g and QR^g are exchanged by g and their common point S is distinct from P and is fixed from g. The line joining S to P is a line through P which is fixed by g.

We have proved that each point lies on a fixed line. Dually, each line contains a fixed point. Assume there exists a quadrangle of fixed elements; then the fixed elements of g form a proper subplane π_0 of π the order of which we denote by m. The counting argument involved in the proof of Proposition 1.2 shows that if $n > m^2$ then there is a line of π missing π_0. This possibility is excluded by the previous observation that each line of π must contain a fixed point. We conclude that π_0 is a Baer subplane and g is a Baer involution in this case.

Assume no quadrangle of fixed elements exists. We prove first of all that there is a line containing three fixed points. Pick a line ℓ_1 and a fixed point P_1 on ℓ_1. Choose a second line ℓ_2 not through P_1 and let P_2 be a fixed point on ℓ_2. The line P_1P_2 is fixed. Choose a third point Q on P_1P_2. If Q is fixed then the line P_1P_2 has the required property. If not, then a line ℓ_3 through Q other than P_1P_2 contains a fixed point P_3 not on P_1P_2. Take a line ℓ_4 not through any one of the points P_1, P_2, P_3, and let P_4 be a fixed point on ℓ_4. Since we are assuming that no quadrangle of fixed elements exists, we see that P_4 must lie on one of the sides of the triangle $P_1P_2P_3$, and this side is the line with the required property.

If ℓ is a line with three fixed points then there is at most one fixed point P off ℓ, because otherwise a quadrangle of fixed elements should exist. Take a point Q on ℓ. Choose a line through Q other that ℓ itself and (possibly) PQ. This line must contain a fixed point which, by our choice, must lie on ℓ, hence it must be Q. We conclude that ℓ is pointwise fixed by g and the assertion follows. □

3.4 Some characterizations of finite desarguesian planes in terms of collineations

A **Moufang plane** is a projective plane in which every line is a translation line. The coordinate structure of a Moufang plane is an alternative division ring, that is a set with two binary operations (addition and multiplication) satisfying the following properties: i) the additive structure is an abelian group; ii) both distributive laws hold; iii) multiplication has an identity element and each non–zero element has a multiplicative inverse; iv) the identities $a^{-1}(ab) = b = (ba)a^{-1}$ hold for each non–zero element a and arbitrary element b; v) the alternative laws $a(ab) = (aa)b$, $(ba)a = b(aa)$ hold for arbitrary elements a, b. The Artin–Zorn theorem states that in every finite alternative division ring multiplication is associative and consequently each such ring is actually a finite field by the theorem of Wedderburn. Each finite Moufang plane is therefore desarguesian.

The connection between projective and affine planes is assumed for the next property.

Proposition 3.10 *Suppose that there exists a line ℓ of π such that for all points C on ℓ the groups of all C–ℓ elations have the same order $r > 1$. Then ℓ is a translation line for π.*

Proof. For each point C on ℓ we define T_C to be the group of all C–ℓ elations; we denote by T the group of all elations with axis ℓ, that is $T = \cup_{C\in\ell}T_C$ (this is is sometimes referred to as the *translation group* of π, or better, of the affine plane obtained from π when ℓ is viewed as a line at infinity). If C_1, C_2 are distinct points on ℓ then the subgroups T_{C_1}, T_{C_2} have only the identity in common. We have thus $|T| = (n + 1)(r - 1) + 1$. The group T acts semiregularly off the line ℓ (in fact a non–identical elation fixes precisely the points of its axis). As a consequence each T–orbit of points off the axis ℓ has length $|T|$, which is thus a divisor of n^2, the number of "affine" points: say $n^2 = [(n + 1)(r - 1) + 1]m$ for some positive integer m. Since $r - 1 > 0$ we have $m < n$. We also have $n^2 \equiv 1 \mod n+1$ and if we interpret the equation $n^2 = [(n+1)(r-1)+1]m$ modulo $n+1$ we obtain $n^2 \equiv m \mod n+1$. The relation $m \equiv 1 \mod n + 1$ with $m < n$ yields $m = 1$, whence also $|T| = n^2$, in other words T permutes the n^2 "affine" points in a single orbit and the assertion follows. □

Proposition 3.11 (Gleason's theorem). *If for any incident point–line pair (P, ℓ) of π there exists a non–trivial P–ℓ elation, then π is desarguesian.*

Proof. By a previous result if the line ℓ admits non–trivial elations for two distinct centers on ℓ, then all elations with axis ℓ form an elementary abelian p–group for some prime p. By the dual of this statement if the point P is the center of non–trivial elations for two distinct lines through P, then the elations with center P form an elementary abelian p–group (where p is the same prime as before). For any incident point–line pair (P, ℓ) of π the group of all P–ℓ elations is an elementary abelian p–group.

Take a given line a of π and let A be an arbitrary point on A. Choose another line b through A and consider a non–trivial A–b elation. This elation has order p and fixes the line a through its center: since A is the unique fixed point on a, all other orbits have length p. By Proposition 2.11 the group of all collineations of π fixing a is transitive on the points of a. In particular, the groups of all C–a elations as C varies on a are all conjugate in this group and have thus the same size $r > 1$. Proposition 3.10 shows that a is a translation line. Each line of π is thus a translation line for π, hence π is a finite Moufang plane, therefore also a desarguesian plane. □

Proposition 3.12 (the Ostrom–Wagner theorem). *If π admits a collineation group G acting doubly transitively on points, then π is desarguesian and G contains all elations of π, whence also $PSL(3,n)$ (the subgroup generated by all elations).*

Proof. We only prove the first part of the statement under the further assumption that n is not a square. Since every 2–transitive group has even order, we see that G contains an involution g. As the order of the plane is not a square, we see that g cannot be a Baer involution and so it is an elation or a homology according as n is even or odd. In the general case the proof must be modified by showing that in any case at least one involution in G is a perspectivity.

We want to prove that if n is odd then G still contains elations. Let the involutory homology g have center C and axis d; choose a point D on d and a point B off d, $B \neq C$. By 2–transitivity there exists a collineation $f \in G$ with $C^f = C$, $D^f = B$. The involutory homology $h = f^{-1}gf$ has center C and axis d^f, a line through B hence different from d. The collineation gh fixes each line through C and so it is a central collineation with center C. Assume gh fixes a line t not through C. If $t^g \neq t$ then gh fixes the two distinct lines t and t^g not through C, hence gh is the identity, yielding $g = h$, a contradiction since g and h have distinct axes. Hence $t^g = t$, showing that t is the axis of both g and h, again a contradiction. We conclude that the central collineation gh fixes no line off the center and so its axis is incident with the center, that is gh is an elation.

Consider an elation in G with center C and axis ℓ and let A be another point on ℓ. By 2–transitivity G contains a collineation j exchanging A and C. Then j fixes ℓ. As a consequence the stabilizer of ℓ in G acts transitively on the points of ℓ, yielding in particular that the subgroups of G consisting of all elations with axis ℓ and center in a given point P of ℓ have the same order $r > 1$. By Propostition 3.10 ℓ is a translation line for π. Since G is 2–transitive on points, G can map a given pair of points on ℓ onto any other pair, hence can map ℓ onto any other line. Every line is thus a translation line and π is a Moufang plane. A finite Moufang plane is desarguesian as we already observed. □

We observe that the Ostrom–Wagner theorem has no analogue for finite affine planes: the Hering plane of order 27 is non–desarguesian and its full collineation group is doubly transitive on affine points, see p.236 in Dembowski's book.

What is known for projective planes if 2–transitivity is replaced by primitivity? I found some references in the paper by F. Buekenhout, A. Delandtsheer, J. Doyen, *Finite Linear Spaces with Flag–Transitive Groups*, Journal of Combinatorial Theory, Series A, 49 (1988) 268–291. Tim Penttila has suggested me to look at the paper by W.M. Kantor *Primitive permutation groups of odd degree, and an application to finite projective planes*, Journal of Algebra 106 (1987) 15–45. Indeed, Theorem B of that paper gives the relevant information.

Proposition 3.13 *If a finite projective plane π of order n admits a collineation group G acting primitively on points, then either π is desarguesian and G contains $PSL(3,n)$ or n^2+n+1 is a prime and G is a regular group or a Frobenius group of order dividing $(n^2+n+1)(n+1)$ or $(n^2+n+1)n$.*

It is interesting to read Bill Kantor's comment on his own proof:

> "The proof of the Ostrom–Wagner Theorem is both elegant and informative. By contrast, our proof of Theorem B uses a sledgehammer approach, involving detailed properties of all finite simple groups. In fact, the proof uses relatively little concerning projective planes."

4 An exercise: a non–classical representation of a classical group

Let F be a (not necessarily finite) commutative field of characteristic $\neq 2$. We have seen in lecture 2 how the projective general linear group $PGL(d,F)$ is defined. In case $d = 2$ the group $PGL(2,F)$ is often represented as the group of all fractional linear transformations on the projective line $PG(1,F) = F \cup \{\infty\}$. These are the mappings

$$F \cup \{\infty\} \to F \cup \{\infty\}, \qquad x \mapsto \frac{ax+b}{cx+d}$$

where $ad - bc \neq 0$ and the usual conventions on dealing with 0 and ∞. This representation yields a sharply 3–transitive permutation representation on $PG(1,F)$.

Consider a non–empty irreducible conic Ω in the projective plane $PG(2, F)$. We have that Ω consists of all points (X_0, X_1, X_2) satisfying an equation of the form

$$\begin{pmatrix} X_0 & X_1 & X_2 \end{pmatrix} \cdot A \cdot \begin{pmatrix} X_0 \\ X_1 \\ X_2 \end{pmatrix} = 0$$

for a suitable 3×3 matrix A with entries in F and $\det(A) \neq 0$

By the fundamental theorem of projective geometry every collineation of $PG(2, F)$ is induced by a semilinear transformation of the underlying vector space (see the textbook by D.R. Hughes, F.C. Piper, *Projective Planes*, Springer, Berlin 1971), and so the full collineation group of $PG(2, F)$ is $P\Gamma L(3, F)$. Here '3' is the dimension of the underlying vector space. The collineations which are induced by linear transformations of the underlying vector space are called linear collineations, forming a normal subgroup $PGL(3, F)$ of $P\Gamma L(3, F)$.

What is the setwise stabilizer of Ω in the linear and in the full collineation group of $PG(2, F)$ respectively? Quoting from page 348 of F. Buekenhout, *Étude intrinsèque des ovales*, Rendiconti di Matematica e Applicazioni (5), 25 (1966) 333–393:

> "On sait que ce groupe est isomorphe à un groupe projectif à une dimension $PGL_2(K)$ [J. Dieudonné, *La géométrie des groupes classiques*, Springer, Berlin 1955] et il est bien connu que le normalisateur d'un tel groupe dans le groupe symétrique des permutations de la droite est le groupe $P\Gamma L_2(K)$"

Here we go with explicit calculations, see §II.7 in Hughes–Piper's textbook.

The process of reducing a conic to its *canonical* form is probably still taught in most undergraduate courses and so nobody should be surprised by the statement that an appropriate choice of coordinates yields for Ω the equation

$$X_0 X_2 = X_1^2$$

or, equivalently, the matrix A can be chosen of the form

$$\begin{pmatrix} 0 & 0 & -1 \\ 0 & 2 & 0 \\ -1 & 0 & 0 \end{pmatrix}.$$

We have $\Omega = \{(1, t, t^2);\ t \in F\} \cup \{(0, 0, 1)\}$. For a, b, c, d in $\mathbf{F}$ we define the matrix

$$M = \begin{pmatrix} d^2 & 2dc & c^2 \\ db & da + cb & ca \\ b^2 & 2ba & a^2 \end{pmatrix}.$$

The relation $\det(M) = (ad - bc)^3$ shows that if $ad - bc \neq 0$ then M induces a linear collineation φ of $PG(2, F)$. We assume that φ multiplies M by the column–vector representing a point and write the outcome as a row–vector. We have thus

$$\begin{aligned} &(1, t, t^2)^\varphi = ((d + ct)^2, (d + ct)(b + at), (b + at)^2)), \\ &(0, 0, 1)^\varphi = (c^2, ca, a^2), \end{aligned}$$

and so φ fixes Ω inducing on it the fractional linear transformation

$$t \mapsto \frac{at + b}{ct + d}.$$

Hence if we let a, b, c, d vary on F subject to $ad - bc \neq 0$, we obtain a collineation group of $PG(2, F)$ which is clearly isomorphic to $PGL(2, F)$. Since the quadratic character of $(ad - bc)^3$ is the same as that of $ad - bc$ we have that the linear collineations induced by the matrices in which $ad - bc$ is a square form a subgroup isomorphic to $PSL(2, F)$.

The conic Ω is also clearly invariant under the collineation $(X_0, X_1, X_2) \mapsto (X_0^\sigma, X_1^\sigma, X_2^\sigma)$ induced by an arbitrary automorphism σ of the field F. We have

$$\begin{aligned} &(1, t, t^2) \mapsto (1^\sigma, t^\sigma, (t^2)^\sigma) = (1, t^\sigma, (t^\sigma)^2), \\ &(0, 0, 1) \mapsto (0^\sigma, 0^\sigma, 1^\sigma) = (0, 0, 1). \end{aligned}$$

If we add all these collineations as σ varies in $\mathrm{Aut}(F)$, we obtain a representation of $P\Gamma L(2, F)$ fixing the conic Ω.

In the terminology of lecture 2 we have shown that the action of the setwise stabilizer on Ω is similar to the natural action of $P\Gamma L(2,F)$ on the projective line. Students attending seminars at the Università della Basilicata were always confused by the fact that, whenever talking of the projective general linear group, Gábor Korchmáros always drew a circle while I was drawing a straight line instead ... !

Assume F is a finite field $F = GF(q)$. The group $PGL(d, F)$ admits a cyclic collineation group acting transitively on the points of $PG(d-1, F)$. This group is a so called **Singer cycle**, named after J. Singer, *A theorem in finite projective geometry and some applications to number theory*, Transactions of the American Mathematical Society 43 (1938) 377–385. Abelian transitive permutation groups are regular (see for instance Corollary 5.3.1. in M. Hall, *The Theory of Groups*, Macmillan, New York 1959) and consequently a Singer cycle is regular on the corresponding geometry.

How do we see Singer cycles of $PGL(2,F) = PGL(2,q)$? Let us restrict our attention to the case q odd. Let ω be a non–square in $GF(q)$ (for instance ω can be chosen to be a primitive element in $GF(q)$). A fairly standard argument shows that the 2×2 matrices

$$\begin{pmatrix} a & b \\ \omega b & a \end{pmatrix}$$

as a and b vary over $GF(q)$ form a field under matrix addition and multiplication (the construction of complex numbers from the reals is presented in this manner in several textbooks). This field is necessarily $GF(q^2)$ and so, in particular, the non–zero matrices of this form (i.e. those for which a and b are not simultaneously zero) form the multiplicative subgroup thereof, hence a cyclic subgroup of order $q^2 - 1$.

We conclude that the group C of fractional linear transformations

$$x \mapsto \frac{ax+b}{\omega bx + a}$$

as a, b vary in $GF(q)$, $(a,b) \neq (0,0)$ is cyclic of order $q+1$ (get rid of scalar transformations occurring for $b = 0$).

The thorough study of subgroups of $PGL(2,q)$ can be traced back to E.H. Moore at the end of the nineteenth century. In the monumental monograph by L.E. Dickson (*a life's work* according to J.C. Fisher) *Linear groups with an exposition of the Galois field theory*, Teubner, Leipzig 1901, the proof that $PSL(2,q)$ is a simple group (when $q \neq 2,3$) is obtained by inspecting the list of *all* subgroups of $PSL(2,q)$ and their conjugacy classes.

Let me mention in passing that it has been cojuectured the a finite projective planes admitting a collineation group acting transitively on points must be desarguesian. I think it was M. Hall in his paper *Cyclic projective planes*, Duke Mathematical Journal 14 (1947) 1079–1090, who first stated this conjecture for cyclic groups. I refer to §4.4 in Dembowski's book for a wider treatment of this difficult topic.

5 Some recent results on collineation groups fixing an oval

The appearance of Beniamino Segre's paper *Ovals in a finite projective plane*, Canadian Journal of Mathematics 7 (1955) 414–416, has given rise to a number of investigations aiming at characterizing "classical" objects (the irreducible conics in this case) by their incidence properties.

A slightly different point of view is suggested by the property we have proved in lecture 4 that a conic in a desarguesian finite projective plane (of odd order) is left invariant by a collineation group acting 2–transitively on the points of the conic.

It was Judita Cofman in her paper *Double transitivity in finite affine and projective planes*, Proceedings of the projective geometry conference, University of Illinois, Chicago, (1967) 16–19, who started investigating the opposite direction. In other words, let π be a finite projective plane of odd order n with an oval Ω. Assume Ω is left invariant by a collineation group G of π acting doubly transitively on the points of Ω. Is it possible to say something on π and G? In fact she proved that if all involutions in G are homologies then π is desarguesian and G contains $PSL(2,n)$. On p.218 of his book, Dembowski conjectures that "the condition that all involutions in G be central collineations is probably superfluous."

William M. Kantor, in his paper *On unitary polarities of finite projective planes*, Canadian Journal of Mathematics 23 (1971) 1060-1077, reached the same conclusion as Cofman under the weaker assumption that G contains *some* involutory homologies.

Gábor Korchmáros confirmed Dembowski's conjecture: in the paper *Una proprietà gruppale delle involuzioni planari che mutano in sè un'ovale di un piano proiettivo finito*, Annali di Matematica Pura ed Applicata (4) 116 (1978) 185–205, he reached the same conclusion under the sole assumption of the 2–transitivity of G on Ω.

The story was only apparently over. The result in the next proposition was proved in the paper by M. Biliotti, G. Korchmáros, *Collineation groups which are primitive on an oval of a projective plane of odd order*, Journal of the London Mathematical Society (2) 33 (1986) 525–534.

Proposition 5.1 *Assume G acts primitively on the points of Ω. Then π is desarguesian, Ω is a conic and either G contains a normal subgroup acting on the points of Ω as $PSL(2,n)$ in its natural doubly transitive permutation representation, or $n = 9$ and G acts on Ω as* Alt(5) *or* Sym(5) *in the primitive permutation representation of degree* 10.

The proof of this result requires a very detailed analysis and quite a good deal of group theory, although the underlying idea is quite easy to explain and involves the consideration of an elementary abelian 2–subgroup E of G. The involutory homologies in E together with the identity form a subgroup V of E of order at most 4.

Proposition 5.2 *Let π be a finite projective plane of odd order n with an oval Ω. If V is a Klein 4–group of collineations of π fixing Ω, then V contains at least one involutory homology inducing an even permutation on Ω.*

Proof. The proof requires an analysis of the behavior of possibly existing Baer involutions in V: that was done by pure counting arguments in Propositions 2.2 and 2.3 of the quoted paper by Biliotti and Korchmáros.

A subgroup of V of index at most 2 must induce even permutations on Ω.

If n is a non–square then V contains no Baer involutions and the assertion is clear.

Assume n is a square with $\sqrt{n} \equiv -1 \mod 4$. According to the quoted Propositions each Baer involution induces an odd permutation on Ω in this case and so there must exist a homology in V.

Assume n is a square with $\sqrt{n} \equiv 1 \mod 4$. If all collineations in V induce even permutations on Ω, then the quoted Propositions yield that the three involutions in V cannot simultaneously be Baer involutions. Assume the collineations in V inducing even permutations on Ω form a subgroup W of index 2 in V. If both involutions in $V \setminus W$ are Baer involutions then the same Propositions show that their product is a homology inducing an even permutation on Ω. Assume the involution f in W is a Baer involution, one of the involutions in $V \setminus W$, say g, is a homology and the other one is a Baer involution. Since $n \equiv 1 \mod 4$ and g induces an odd permutation on Ω, we see that the axis a of g must be disjoint from Ω. The homology $f^{-1}gf$ has axis a^f, but the relation $f^{-1}gf = g$ yields $a^f = a$, and so a is a line of the fixed Baer subplane of f missing Ω. Since case ii) of Proposition 2.2 in the paper by Biliotti and Korchmáros applies here we have a contradiction. □

Going back to our original 2–group E, if $V < E$ then the previous Proposition shows that the product of any two collineations in $E \setminus V$ (these are Baer involutions) must lie in V and so $|E : V| = 2$ and consequently the relation $|E| \leq 8 = 2^3$ holds.

In other words the conclusion is that 2^3 is the largest possible order of an elementary abelian 2–subgroup of G, a property which is often expressed by saying that the 2*–rank* of G is at most 3.

The key idea in the proof of the result on primitive ovals is based on the consideration of a minimal normal subgroup of the group G under consideration. Minimal normal subgroups have the important property of being *characteristically simple*. A characteristically simple group is one in which the unique characteristic subgroups are the trivial subgroup and the entire group. A finite characteristically simple group can be represented as the direct product of finitely many pairwise isomorphic finite simple groups, hence either cyclic of prime order or non–abelian simple.

Let M be a minimal normal subgroup of the group G in the statement of Proposition 5.1. As a non–trivial normal subgroup of a primitive group, M must be transitive on the oval Ω. If M is the direct product of cyclic groups of the same prime order, in other words if M is elementary abelian, then as a transitive abelian permutation group on Ω, the group M must be regular on Ω. Since the cardinality of Ω is $n+1$, an even number, we have that M is an elementary abelian 2–group. By the 2–rank property the size of M must be 4 or 8, hence n must be 3 or 5, in either case the plane π must be desarguesian and a direct verification is possible. If M is the direct product of pairwise isomorphic non–abelian simple groups, then since each non–abelian finite simple group contains at least two commuting involutions, hence a Klein 4–group, we have that if the number of pairwise isomorphic factors in the direct product is greater than one, then the group M has 2–rank at least 4, which is impossible. We conclude that the number of factors is just one, that is M is a non–abelian finite simple group. Since M itself leaves the oval Ω invariant we also see that the 2–rank of M is at most 3.

The relevant fact is that non–abelian finite simple groups of 2–rank not exceeding 3 are classified by the work of G. Stroth, *Über Gruppen mit* 2*–Sylow Durchschnitten vom Rang* ≤ 3, Journal of Algebra 43 (1976) 398–456. The detailed analysis of Stroth's fairly long list yielded not only the result on primitive ovals, but also further developments like the following result, which is Theorem A in M. Biliotti, G. Korchmáros, *Collineation groups preserving an oval in a projective plane of odd order*, Journal of the Australian Mathematical Society Series A 48 (1990) 156–170. It is quite satisfactory within our context.

Proposition 5.3 *If π is a finite projective plane of odd order n with an oval Ω which is left invariant by a non–abelian simple collineation group M, then M must be isomorphic to $PSL(2,q)$ with q odd ≥ 5.*

A collineation group of a projective plane is said to be **irreducible** if it fixes no point, line or triangle of the plane. If, further, the group fixes no proper subplane setwise then it is said to be **strongly irreducible** on the plane. The possible structures and actions of irreducible collineation groups of finite projective planes were investigated by Christoph Hering. His paper *On the structure of finite collineation groups of projective planes*, Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg 49 (1977) 95–101, started a systematic study of irreducible collineation groups of finite projective planes and eventually led to a satisfactory classification theorem when the existence of non–trivial perspectivities is assumed.

Hering's techniques and results played a crucial role in the quoted results by Biliotti, Korchmáros and many others. For example M.R. Enea, G. Korchmáros and I, in our paper *Irreducible Collineation Groups fixing an Oval*, Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg 69 (1999) 259–264, consider an oval in a finite projective plane of odd order which is fixed by an irreducible collineation group whose order is divisible by four. We show that such a group must contain involutory perspectivities. We apply Hering's classification and prove the following result.

Proposition 5.4 *Let G be a collineation group of an odd–order finite projective plane π. Assume that G fixes an oval Ω and $|G| \equiv 0 \mod 4$. Then G is a minimal irreducible collineation group of π if and only if G is isomorphic to $PSL(2,q)$ for some odd prime $q \geq 5$ with $q^2 \not\equiv 1 \mod 5$* (here "minimal" means G contains no proper subgroup which is still irreducible).

Recent papers have treated interesting situations in which the collineation group under consideration is neither transitive on the oval nor irreducible on the plane. M.R. Enea, G. Korchmáros, in their paper *$\mathcal{I}$–transitive ovals in projective planes of odd order*, Journal of Algebra 208 (1998) 604–618, have proved the following result.

Proposition 5.5 *Let π be a finite projective plane of odd order n containing an oval Ω. Assume a collineation group G of π fixes Ω and acts transitively on the set of internal points. Then one of the following situations occurs:*

I) *G acts doubly transitively on Ω;*

II) *G fixes a point X on Ω and acts on $\Omega \setminus \{X\}$ as a primitive permutation group of affine type. If, in addition, each involution in G is an involutory homology, then G is 2–transitive on $\Omega \setminus \{X\}$ and one of the following two possibilities occurs:*

IIa) *G is a subgroup of $A\Gamma L(1,n)$;*

IIb) *$n \in \{5^2, 7^2, 11^2, 23^2, 29^2, 59^2\}$ and G acts on $\Omega \setminus \{X\}$ as a sharply 2–transitive permutation group of affine linear transformations over an irregular nearfield of order n.*

They also suggest the following

Exercise. Let π be a finite projective plane of odd order n containing an oval Ω and let G be a collineation group of π fixing Ω. The group G acts transitively on the set of external points if and only if it acts 2–transitively on Ω.

The following solutions of the Exercise were worked out in Brescia during the Summer School. I recall that a group G is said to act 2–homogeneously on a set X if it acts transitively on the 2–element–subsets of X.

Solution 1 (T. Penttila & M. Law)**.** The group G is transitive on external points to Ω if and only if it is 2–homogeneous on the points of Ω.

- A finite sharply 2–homogeneous group H has odd order. If not there exists an invoution $h \in H$ and if $x^h \neq x$ we have that $\{x, x^h\}$ is stabilized by h.

- A finite 2–homogeneous group is transitive. Apply Block's lemma: the incidence matrix of 1–sets versus 2–sets has rank the number of 1–sets.

- A finite sharply 2–homogeneous group has degree $d \equiv 3 \mod 4$ (both d and $\binom{d}{2}$ are odd).

- G is transitive on external points to Ω if and only if G is 2–transitive on Ω. (if G is transitive on external points to Ω then, since G has even degree $n+1$, it is not sharply 2–homogeneous, so it is 2–transitive on Ω; the converse is clear)

Solution 2 (A. Bonisoli). Assume G is transitive on external points. Then G is 2–homogeneous on Ω. I show first of all that G is transitive on Ω. Consider the partition of Ω into 2–element subsets obtained by intersecting Ω with the secants throuh a given internal point P, say $\Lambda = \{\{R_1, S_1\}, \{R_2, S_2\}, \ldots, \{R_{(n+1)/2}, S_{(n+1)/2}\}\}$. For $i = 1, \ldots, (n+1)/2$ there exists $g_i \in G$ with $\{R_1, S_1\}^{g_i} = \{R_i, S_i\}$ and we may assume the labelling to be such that $R_1^{g_i} = R_i$, $S_1^{g_i} = S_i$.

The points R_1, R_2, … , $R_{(n+1)/2}$ lie thus in one and the same G–orbit and so do the points S_1, S_2, … , $S_{(n+1)/2}$. Since n is odd, $n \geq 3$, we have $(n+1)/2 \geq 2$. There exists $g \in G$ with $\{R_1, R_2\}^g = \{S_1, S_2\}$. We conclude that R_1 lies in the same G–orbit as either S_1 or S_2 and so all points R_1, R_2, … , $R_{(n+1)/2}$, S_1, S_2, … , $S_{(n+1)/2}$ lie in the same G–orbit, in other words G is transitive on Ω. In particular $n+1$ is a divisor of $|G|$.

Let O be an external point. We have $|G| = \binom{n+1}{2}|G_O|$ whence $2|G|/(n+1) = n|G_O|$ and so 2 is an integer dividing $n|G_O|$ and since n is odd we obtain that $|G_O|$ is even and so, in particular, G_O contains involutions.

I claim that G_O contains an involution exchanging R, S, the points at which the tangents through O touch Ω. Let j be an involution in G_O and assume $R^j = R$, $S^j = S$. The collineation j cannot fix Ω elementwise, otherwise j is the identity because the action on Ω is faithful. Hence there are two points R', S' on Ω which are exchanged by j. If O' is the external point obtained as the intersection of the tangents to Ω at R' and S', then j is an involution in $G_{O'}$ exchanging the two tangents through O'. Since $G_{O'}$ is conjugate to G_O in G we see that we must be able to find an involution in G_O exchanging the two tangents through O.

All we are left to prove is that if $X \in \Omega$, then G_X is transitive on $\Omega \setminus \{X\} = \{X_1, X_2, \ldots, X_n\}$. We know that for $i = 1, 2, \ldots, n$ there exists $h_i \in G$ with $\{X, X_1\}^{h_i} = \{X, X_i\}$. If $X^{h_i} \neq X$ then choose an involution j exchanging X, X_i and obtain $X^{h_i j} = (X^{h_i})^j = X_i^j = X$, $X_1^{h_i j} = (X_1^{h_i})^j = X^j = X_i$. We conclude that we can map X_1 to any other point of $\Omega \setminus \{X\}$ by a collineation in G fixing X, and so G_X is transitive on $\Omega \setminus \{X\}$.

The following result is proved in the paper by A. Aguglia and myself, *Intransitive collineation groups of ovals fixing a triangle*, which has just been submitted for publication.

Proposition 5.6 *Let π be a finite projective plane of odd order n containing an oval Ω. If a collineation group G of π satisfies the properties*

(a) *G fixes Ω and the action of G on Ω yields precisely two orbits Ω_1 and Ω_2,*

(b) *G has even order and a faithful primitive action on Ω_2,*

(c) *G fixes neither points nor lines but fixes a triangle ABC in which the points A, B, C are not on the oval Ω,*

then $n \in \{7, 9, 27\}$, the orbit Ω_2 has length 4 and G acts naturally on Ω_2 as A_4 or S_4.

Each order $n \in \{7, 9, 27\}$ does furnish at least one example for the above situation; the determination of the planes and the groups which do occur is complete for $n = 7$, 9; the determination of the planes is possibly still incomplete for $n = 27$.

Note the assumption of faithfulness in (b): a collineation group fixing an oval has a faithful action on the oval itself. If this group has more than one orbit on the oval, then the action might no longer be faithful on the single orbits.

6 Benz–geometries with many symmetries

The plane sections of a non–degenerate quadric $\mathcal{Q}$ in 3–dimensional projective space form the classical model of a "circle" geometry called a Möbius, Laguerre or Minkowski plane, depending on whether $\mathcal{Q}$ is an elliptic quadric, a quadratic cone or a hyperbolic quadric respectively. These models are also said to be "miquelian" because they are characterized by the validity of Miquel's configurational condition.

These geometries admit a unified axiomatic treatment and it is now customary to call them "Benz planes" after Walter Benz, see F. Buekenhout, *Les plans de Benz: une approche unifiée des plans de Moebius, Laguerre et Minkowski*, Journal of Geometry 17 (1981) 61–68.

Also for these geometries the approach based on automorphism groups has been pursued. Let us consider for example Möbius planes, which are probably more commonly known as **inversive planes**: in the finite case they are precisely the 3–$(n^2+1, n+1, 1)$ designs for some positive integer n (called the **order**). The following result was proved by C. Hering, *Endliche zweifach transitive Möbiusebenen ungerader Ordnung*, Archiv der Mathematik 18 (1967) 107–110.

Proposition 6.1 *A finite inversive plane of odd order admitting an automorphism group acting doubly transitively on points is necessarily miquelian.*

The same conclusion holds if "doubly transitively" is replaced by "primitively" in the above statement. This my result in *Point–primitive inversive planes of odd order*, Bulletin of the London Mathematical Society 25 (1993) 377-384.

6.1 Permutation sets and (B)–geometries

Formally speaking, a permutation on X is a special subset of the cartesian product $X \times X$, but it is sometimes more convenient to use standard functional notation for permutations. Therefore if g is a permutation on X and x, y are elements of X the relations $(x, y) \in g$ and $g(x) = y$ will have the same meaning and I shall use either one of them according to convenience.

Let H be a permutation set X. For arbitrary elements $x_1, x_2, \ldots, x_r \in X$ we denote by $H_{x_1 \ldots x_r}$ the subset of H consisting of all permutations fixing each one of the given elements. If x, y are distinct elements of X we denote by $H(y \mapsto x)$ the subset of H consisting of all permutations mapping y to x. If $g \in \mathrm{Sym}(X)$ then $\mathrm{Fix}(g)$ is the set of all fixed points of g.

Adopting the terminology of B. Polster, *Invertible Sharply n–Transitive Sets*, Journal of Combinatorial Theory, Series A 81 (1998) 231–254, we shall say that the permutation set H on X is **invertible** if H contains the identity and if whenever a permutation g lies in H then so does its inverse g^{-1}. Every permutation group is clearly invertible.

Let d be a positive integer. A permutation set H on X is said to be **sharply** d**–transitive** on X if whenever $(x_1, x_2, \ldots, x_d)$ and $(y_1, y_2, \ldots, y_d)$ are d–tuples of distinct elements of X there exists precisely one permutation $h \in H$ with $h(x_i) = y_i$ for each index $i = 1, 2, \ldots, d$. We have already remarked that for permutation groups this definition is usually given by saying that H is d–transitive and the stabilizer of d elements reduces to the identity: for general permutation sets the two formulations are **NOT** equivalent.

If H is a permutation set on X and $f \in \mathrm{Sym}(X)$ then we write $Hf = \{hf : h \in H\}$ and $fH = \{fh : h \in H\}$. If H is a sharply d–transitive permutation set on X which does not contain the identical permutation and h is any fixed permutation in H, then the permutation set $h^{-1}H$ is sharply d–transitive on X and contains the identical permutation. When dealing with sharply d–transitive permutation sets it can therefore always be assumed without loss of generality that the identical permutation lies in the set.

It is precisely Minkowski planes which can be described by sharply 3–transitive permutation sets. That led to the consideration of the geometric structure arising from an *arbitrary* permutation set H on X. This structure is called a (B)–**geometry** by W. Benz in his monograph *Vorlesungen über Geometrie der Algebren*, Springer, Berlin 1973, and it can be described by a very simple set of axioms. Italian readers who are interested in a very detailed description of the geometric aspects of sharply d–transitive permutation set are encouraged to get hold of Volume III of B. Segre's *Istituzioni di Geometria Superiore*, Istituto Matematico "G. Castelnuovo", Roma, 1965. Pier Vittorio Ceccherini was personally involved in the preparation of those lecture notes and he confirms that only a limited number of copies were produced, mainly for library distribution. I must therefore be counted as one of the lucky owners.

The (B)–geometry $\mathcal{M}(H)$ associated to the permutation set H on X is defined as follows. The **points** of $\mathcal{M}(H)$ are the elements of the cartesian product $X \times X$. The **blocks** (or **circles**) of $\mathcal{M}(H)$ are the elements of H. We distinguish further subsets of $X \times X$, namely, if a is any element of X we define $(a)_+ = \{(a, y) |\ y \in X\}$, $(a)_- = \{(x, a) |\ x \in X\}$; we set $\mathcal{L}_+ = \{(a)_+ |\ a \in X\}$, $\mathcal{L}_- = \{(a)_- | a \in X\}$, $\mathcal{L} = \mathcal{L}_+ \cup \mathcal{L}_-$; the elements of $\mathcal{L}_+$ resp. $\mathcal{L}_-$ resp. $\mathcal{L}$ will be called **positive generators** resp. **negative generators** resp. **generators**. Point–block incidence and point–generator incidence is simply given by $\in$ in the natural way.

Each family of generators yields a partition of the point set of $\mathcal{M}(H)$ and thus an equivalence relation: if P, Q are points of $\mathcal{M}(H)$ we define $P \|_+ Q$ if and only if P and Q lie on the same positive generator (**plus–parallelism**); we define $P \|_- Q$ if and only if P and Q lie on the same negative generator (**minus–parallelism**); we shall say that P and Q are **parallel** and write $P \| Q$ if there exists a generator to which both P and Q belong; otherwise we shall say that P and Q are **non–parallel** or **independent**.

An easy check shows that for $|X| \geq 3$ the incidence structure $\mathcal{M}(H)$ satisfies the following properties:

(1) to given points A, B there exists a unique point P such that $A \|_+ P \|_- B$;

(2) if P is a point and g is a block there exist uniquely determined points P_+, $P_- \in g$ such that $P_+ \|_+ P \|_- P_-$;

(3) there exist three pairwise non–parallel points.

The above properties (1), (2), (3) form the axiomatic definition of what W. Benz calls a (B)–**geometry**; he also shows that each (B)–geometry can be described as the incidence structure $\mathcal{M}(H)$ associated to a suitable permutation set H in the manner described above.

Under a (B)–geometry we shall thus always understand the incidence structure $\mathcal{M}(H)$ associated to a non–empty permutation set H on a set X. Even without explicit mention, whenever we want to avoid trivial cases we shall also assume $|X| \geq 3$ which amounts to axiom (3).

In the (B)–geometry $\mathcal{M}(H)$ the cardinality of each generator is equal to the cardinality of each block, which is in turn equal to the cardinality of the set X on which the permutations in G operate; to each positive generator and each negative generator there exists precisely one point belonging to both; the same happens for each generator and each block.

If f, g are blocks of the (B)–geometry $\mathcal{M}(H)$ we shall say that f and g are i–**secant** if $|f \cap g| = i$; in particular we shall say that f and g are **disjoint** resp. **tangent** resp. **secant** blocks if they are 0–secant resp. 1–secant resp. 2–secant; tangent blocks with P as common point will be said to be **tangent at** P. Further terminology of common use in geometry will be adopted whenever convenient.

Both properties defined above for H, that of being invertible and that of being sharply d–transitive, can be entirely phrased in geometric terms inside the corresponding (B)–geometry.

If h is any given permutation in H, the mapping

$$X \times X, \qquad (x, y) \mapsto (h^{-1}(y), h(x))$$

is called the **block symmetry** with respect to h. It is easily seen that it is an involutory permutation of $X \times X$ fixing the block h pointwise, that is fixing each point $(x, h(x))$. In general this block symmetry will NOT be an automorphism of the (B)–geometry arising from H: as a matter of fact the image of the block $f \in H$ is the permutation $hf^{-1}h$, which, without further conditions, is NOT an element of H in general. It will always be an automorphism whenever H is a permutation *group*. If h is the identity permutation, the given mapping will be an automorphism if and only if for any block $f \in H$ the inverse permutation f^{-1} is also a block, which means $f^{-1} \in H$, in other words, H is invertible. We have thus seen that the request that a permutation set be invertible amounts to the request that, in the corresponding (B)–geometry the block–symmetry with respect to a specified block is actually an automorphism.

Assume that $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, ... , $P_d = (x_d, y_d)$, are points of the (B)–geometry. A necessary condition for the existence of a block of the (B)–geometry containing all of these points is that these points be pairwise independent. The sharp d–transitivity of the permutation set H on X amounts to the condition that for any d pairwise independent points there exists a unique block of the (B)–geometry containing them.

The (B)–geometry arising from a sharply 2–transitive finite permutation set H is precisely a finite affine plane. The unique little difference is that when an affine plane is treated as a (B)–geometry, there are two pencils of parallel lines which play the somewhat special role of generators. According to Dembowski it was E. Witt in Section IV of his paper *Über Steinersche Systeme*, Abhandlunhgen aus dem Mathematischen Seminar der Universität Hamburg 12 (1938) 265–275, who first pointed out the connection between finite affine planes and sharply 2–transitive sets of permutations.

The (B)–geometry arising from a sharply 3–transitive finite permutation set H is a finite Minkowski plane. Taking H to be $PGL(2, q)$ we obtain a miquelian Minkowski plane, in other words we obtain the geometry of plane sections of a hyperbolic quadric in $PG(3, q)$. The "flocks" of such quadrics are classified by the result of Laura Bader and Guglielmo Lunardon *On the flocks of* $Q^+(3, q)$, Geometriae Dedicata 29 (1989) 177–183. Nicola Durante and Alessandro Siciliano give a new proof of that result in their paper *(B)–geometries and flocks of hyperbolic quadrics*, which has been presented in a talk at the conference "Combinatorics 2002." Their proof uses concepts from (B)–geometry such as the so called "rectangle condition," which has been used by W. Benz and H. Karzel in various other contexts.

I am interested here in sharply d–transitive finite permutation sets with $d \geq 4$. In the known examples, if such a permutation set contains the identity it is always a group. In other words, by a previous observation, for $d \geq 4$ the known examples for sharply d–transitive finite permutation sets are *cosets* of groups. Since sharply d–transitive finite permutation groups are well classified, we know what we are talking about...!

Proposition 6.2 *Each invertible sharply d–transitive finite permutation set with $d \geq 4$ is a group.*

Pasquale Quattrocchi and I proved this result in a paper with the same title in the Journal of Algebraic Combinatorics 12 (2000) 239-248. I shall illustrate some of the ideas behind the proof and show how the computer comes into play.

The corresponding property does not hold for $d = 1$. For each positive integer m a 1–factorization of the complete graph on $2m$ vertices is known to exist and it can be represented by a sharply 1–transitive permutation set of degree $2m$ consisting of the identity and $2m-1$ fixed–point–free involutions (each 1–factor yields the involution in which the edges of the 1–factor appear as 2–cycles); such a permutation set is clearly invertible but is certainly not a group whenever m is not a power of 2, because a finite group in which each non–identical element has order 2 must be an elementary abelian 2–group.

The corresponding property does not hold for $d = 2$ either: in geometric terms that follows from the existence of non–nearfield planes admitting involutory perspectivities. Whether it holds for $d = 3$ is still an open question as far as I know. There do exist sharply 3–transitive finite permutation sets containing the identity which are not groups, but these examples are not invertible. Every finite Minkowski plane in which EACH block–symmetry is an automorphism does arise from a sharply 3–transitive GROUP, as N. Percsy proved in his paper *Finite Minkowski Planes in which every circle symmetry is an automorphism*, Geometriae Dedicata 10 (1981) 269–282. Here is the formulation of the result in terms of permutations. Assume G is a sharply 3–transitive finite permutation set of even degree containing the identity permutation and such that if f, g are permutations in G, then the permutation $fg^{-1}f$ also lies in G. Then G is a group. The same conclusion holds under the weaker condition that $fg^{-1}f$ be in G whenever f, g have at least two fixed points, as G. Korchmáros and I have shown in *A Characterization of the sharply* 3*–transitive finite permutation groups*, European Journal of Combinatorics 11 (1990) 213–228.

Observe that if X is an arbitrary infinite set and d is an arbitrary positive integer, then there always exists an invertible sharply d–transitive permutation set on X, which in general is not a group. That follows from the constructions in the following papers, based on a suitable use of transfinite induction: W. Heise, K. Sörensen, *Scharf n–fach transitive Permutationsmengen*, Abh. Math. Sem. Univ. Hamburg 43 (1975) 144–145; P. Lancellotti, *Una nuova classe di insiemi di permutazioni strettamente n–transitivi*, Atti Sem. Mat. Fis. Univ. Modena 30 (1981) 83–93.

I finally remark that, besides requiring the computer checks that I am going to describe, our proofs rely essentially on the uniqueness of the sharply 3–transitive permutation sets of degree ten proved by G.F. Steinke in *A remark on Benz planes of order* 9, Ars Combinatoria 34 (1992) 257–267. In turn, that ultimately rests on the uniqueness of the projective planes of order nine, another computer result that C.W.H. Lam, G. Kolesowa, L. Thiel illustrated in their paper *A computer search for finite projective planes of order* 9, Discrete Mathematics 92 (1991) 187–195.

7 Computer algebra packages may be of help

The first purpose of this lecture is to give yet another example of a typical use of the computer in solving problems in discrete mathematics. Although each instance of such a problem generally involves finitely many elements, the problem itself may have infinitely many instances, one for each value of some parameter, for instance the number of vertices of a graph, or the number of points of a block of a design and so on. Sometimes the problem admits a reduction to the consideration of finitely many special cases. The size of these special cases is often so large that, if one does not have any other information, the computer turns out to be the best and sometimes unique choice. Perhaps the most famous situation of this kind is the Four Color Theorem. Here I will present a proof of Proposition 6.2.

The second purpose is to show that the use of computer packages like GAP or MAGMA can make life easier. GAP (*Groups, Algorithms, and Programming*), is distributed free of charge by the GAP Group, previously in Aachen (Germany) and currently in St. Andrews (United Kingdom). MAGMA is developed by the Computational Algebra Group based at the University of Sydney and has platform–dependent licence fees. Both packages have Web pages, from which download and installation informations for most platforms can be retrieved:

```
http://www-gap.dcs.st-and.ac.uk/~gap
http://magma.maths.usyd.edu.au/magma/
```

The syntax of these packages is quite close to the usual mathematical language and the fact that many useful “data structures” (such as permutations) are already “built in” the language often reduce the work of the programmer to just a few lines of code. I do know researchers who prefer to develop their own code, two examples that I am personally aware of are Alan Prince using Fortran and Ivano Pinneri using Pascal.

Of course choices of software always depend on very personal habits. No matter what the choice is, I feel I can recommend the golden rule that one learns in any basic course on computer programming: make your programs intelligible to third parties, including yourselves.

7.1 The Mathieu group of degree 11

The proof of Proposition 6.2 moves its first step from the smallest case $d = 4$. Assume $|X| \geq 7$ and let G be an invertible sharply 4–transitive permutation set on X. It was proved by P. Quattrocchi, C. Fiori, in their paper *A result concerning the existence of certain Minkowski–*2*–structures*, Journal of Geometry 14 (1980) 139–142, that under these assumptions we must have $|X| = 11$: this is the reduction result that I was previously referring to.

Is G then necessarily a group, whence the Mathieu group of degree 11? Partial answers had been given in two previous papers, both focusing attention on the involutions in G: A. Bonisoli, T. Grundhöfer, *On the uniqueness of the Minkowski* 2*–structure of order* 9 *possessing a reflection*, Research Report, Modena, November 1987; P. Quattrocchi, G. Rinaldi, *Insiemi di permutazioni strettamente* 4*–transitivi e gruppo di Mathieu* M_{11}, Bollettino dell'Unione Matematica Italiana (7) 11–B (1997) 319–325.

We shall now see that the answer to the previous question is affirmative under even milder assumptions. Setting $X = \{1,2,3,4,5,6,7,8,9,10,11\}$ we assume that G is a sharply 4–transitive permutation set on X containing the identical permutation. We have $|\mathrm{Fix}(gf^{-1})| \leq 3$ for any two distinct permutations f, g in G. In particular each non–identical permutation in G has at most three fixed points.

We denote by M the Mathieu group of degree 11 in its sharply 4–transitive permutation representation. The Mathieu group is uniquely determined up to permutation isomorphism: that is established for instance in §5.8 of the book by M. Hall, *The Theory of Groups*, Macmillan, New York 1959. In other words, the sharply 4–transitive subgroups of S_{11} form a single conjugacy class: we may take for M any specific version of the Mathieu group of degree 11, I have chosen the one given by M. Hall, hence M will be the subgroup generated by the permutations

$$(1,2,3,4,5,6,7,8,9,10,11) \qquad (2,5,6,10,4)(3,9,11,8,7) \qquad (2,6,5,4)(3,7,11,8)$$

and I will denote the set of all involutions in M.

Let J be a subset of S_{11} with the following properties:

a1) $|J| = 165$;

a2) each permutation in J is an involution with three fixed points;

a3) $I_1 \subseteq J$;

a4) $|\mathrm{Fix}(ts)| \leq 3$ for any two distinct $t, s \in J$.

Proposition 7.1 *There are precisely two subsets of S_{11} satisfying the above properties, namely the set I of all involutions in M and a subset I^* such that the subgroup $\langle I^* \rangle$ is conjugate to M in S_{11}.*

Proof. The fact that I satisfies properties a1), a2), a3), a4) follows easily from the property that M is a sharply 4–transitive permutation group of degree 11, see again §5.8 in M. Hall's book.

The rest of the assertion has been verified by computer through the GAP program FIRST.G enclosed here below. We summarize here the relevant steps.

Let T denote the set of all involutions in S_{11} with precisely three fixed points. The centralizer in S_{11} of an involution in T is easily seen to have order $6 \cdot 24 \cdot 16$ and so the cardinality of T is 17325.

Set $I' = I \setminus I_1$ and define $I'' = \{h \in T \setminus I : |\mathrm{Fix}(hj)| \leq 3 \text{ for all } j \in I_1\}$. We have $|I''| = 120$ and the subgroup of S_{11} generated by $I^* = I'' \cup I_1$ is a conjugate M^* of M in S_{11}.

Form a graph Γ on the set of vertices $V(\Gamma) = I' \cup I''$: two distinct involutions $a, b \in I' \cup I''$ are declared to be adjacent if and only if $|\mathrm{Fix}(ab)| > 3$. That means a, b cannot sit together in a sharply 4–transitive permutation set.

Since I' is a subset of M and M is sharply 4–transitive, we see that no two vertices in I' are adjacent and so I' is an independent subset of size 120 in Γ. Similarly, I'' is another independent subset of size 120 in Γ. In particular Γ is a bipartite graph with bipartition $\{I', I''\}$. Now a candidate subset J with the required properties must be of the form $J = I_1 \cup J'$ where J' is an independent subset of size 120 in Γ.

The graph Γ is regular (of degree 16) and so the complement $J'' = V(\Gamma) \setminus J'$ is also an independent subset of size 120 in Γ. Clearly $\{J', J''\}$ is a bipartition of Γ.

As the graph Γ is connected, it admits precisely one bipartition, which means $\{J', J''\} = \{I', I''\}$ and the assertion follows. □

```
###################################################################################
#  file "FIRST.G", a GAP program
###################################################################################
#  Lines beginning with "#" are comments. It can either be loaded into GAP by a
#  Read() command or the lines which are not comments can be typed in sequence
#  directly from the keyboard
###################################################################################
   S11:=SymmetricGroup(11);
   a:=(1,2)(3,4)(5,6)(7,8);
   T:=ConjugacyClass(S11,a);
###################################################################################
#  We have constructed the full symmetric group S11 of degree 11 and the conjugacy
#  class T of all involutions in S11 with 3 fixed points
###################################################################################
   x:=(1,2,3,4,5,6,7,8,9,10,11);
   y:=(2,5,6,10,4)(3,9,11,8,7);
   z:=(2,6,5,4)(3,7,11,8);
   M:=Subgroup(S11,[x,y,z]);
###################################################################################
#  The group  M  is a version of the Mathieu group of degree 11. This can be tested
#  in many ways, for instance by checking that it is a non--abelian simple group of
#  order 7920
###################################################################################
   M_1:=Stabilizer(M,1);
   M_12:=Stabilizer(M_1,2);
   M_123:=Stabilizer(M_12,3);
###################################################################################
#  M_1 is the stabilizer in M of the element 1;
#  M_12 is the elementwise stabilizer in M of the set {1,2};
#  M_123 is the elementwise stabilizer in M of the set {1,2,3}: it is a quaternion
#  group of order 8
###################################################################################
   for h in M_123 do
      if Order(h)=2 then f:=h; break; fi;
   od;
   I:=ConjugacyClass(M,f);
   I_1:=ConjugacyClass(M_1,f);
###################################################################################
#  We have constructed the unique involution  f  in M_123, the subset  I  of all
#  involutions in  M and the subset I_1 of all involutions in  M  fixing the
#  element  1
###################################################################################
   IDASH:=Difference(I,I_1); IDDASH:=[];
   for h in Difference(T,I) do
      flag:=true;
      for j in I_1 do
         if NrMovedPointsPerm(h*j)<8 then
            flag:=false; break;
         fi;
      od;
      if (flag=true) then IDDASH:=Union(IDDASH,[h]); fi;
   od;
###################################################################################
#  We have constructed two subsets IDASH and IDDASH of S11, both consisting of
#  involutions with precisely three fixed points: IDASH  simply consists of the
#  involutions in  I  which do not fix the element  1, while IDDASH consists of all
#  involutions with three fixed points which are not in I and are "compatible"
#  with each involution in  I_1
###################################################################################
   MSTAR:=Subgroup(S11,Union(I_1,IDDASH));
   INVO:=Union(IDASH,IDDASH);
   v:=Length(INVO);
   A:=[];
   for i1 in [1..v] do
      A[i1]:=[];
      for i2 in [1..v] do
         k:=NrMovedPointsPerm(INVO[i1]*INVO[i2]);
         if ((0<k) and (k<8)) then
               A[i1][i2]:=1;
            else
               A[i1][i2]:=0;
         fi;
      od;
   od;
###################################################################################
```

```
#  We have contructed the adjacency matrix A of the graph GAMMA having the union of
#  IDASH and IDDASH as the set of vertices. Two vertices are declared to be
#  adjacent if and only if the corresponding involutions are "incompatible"
###################################################################################
   RequirePackage("grape");
###################################################################################
#  The previous statement is the standard way to extend GAP by a so called
#  "Share Package", in this case GRAPE developed by L.H. Soicher (QMW, University
#  of London). This Share Package allows one to deal with graphs and their
#  automorphisms
###################################################################################
   GG:=Group( () );
   GAMMA:=Graph(GG,[1..v],OnPoints,function(i1,i2)
      return A[i1][i2]=1;end,true);
###################################################################################
#  We have constructed the graph GAMMA on  v  vertices having the matrix  A
#  defined above as  its adjacency matrix; a graph in GRAPE always comes with an
#  automorphism group GG, but since we are not particularly interested in the
#  automorphisms of our graph  GAMMA  we have defined GG  to be the trivial group.
#  We shall now test some graph-theoretical properties for  GAMMA
###################################################################################
   IsSimpleGraph(GAMMA);
###################################################################################
#  GRAPE usually deals with directed graphs, which become simple as soon as their
#  adjacency matrix is symmetric with zero's on the main diagonal
###################################################################################
   IsRegularGraph(GAMMA);
   IsConnectedGraph(GAMMA);
   IsBipartite(GAMMA);
###################################################################################
#  The meaning of the properties is self-explanatory. They prove that the two sets
#  IDASH  and  IDDASH  form the UNIQUE bipartition for the graph  GAMMA
###################################################################################
   Runtime();
###################################################################################
#  This command gives the amount of CPU time in milliseconds expired since the
#  beginning of our GAP session. I obtained 1405100 milliseconds on a 32 bit
#  Pentium Pro II under Windows 95 running GAP with 24 MBytes of RAM
###################################################################################
```

After such a proof of Proposition 7.1, Werner Heise will probably reinforce his belief that Pasquale Quattrocchi's electronic virginity is corrupted forever ... !

Proposition 7.2 *A sharply* 3*–transitive permutation set of degree* 10 *containing the identity is a group.*

Proof. This result is the formulation in terms of permutation sets of the uniqueness of the Minkowski planes of order 9 proved by G.F. Steinke in *A remark on Benz planes of order* 9, Ars Combinatoria 34 (1992) 257–267. □

There are only two types of sharply 3–transitive groups of degree 10, namely $PGL(2,9)$ and another subgroup of $P\Gamma L(2,9)$ usually denoted by $M(3^2)$. It is known that the group $PGL(2,9)$ cannot be a one–point–stabilizer in a sharply 4–transitive permutation set of degree 10. Hence G_x is isomorphic to $M(3^2)$ and admits thus a transitive extension which is precisely the Mathieu group.

In other words we have that for each $x \in X$ the stabilizer G_x is a conjugate of M_x in S_{11}. After possibly replacing G by a suitable conjugate hGh^{-1} in S_{11}, we may assume $G_1 = M_1$.

Let J denote the set of involutions in G. We have that J is the union of the sets J_x as x varies in X. In particular $J \neq \emptyset$; since each involution in G_x has two fixed points on $X \setminus \{x\}$, every involution in J has precisely three fixed points on X.

The stabilizer of two points in G_x is a quaternion group of order 8. To any given three elements x, y, $z \in X$ there exists thus a unique involution in J fixing x, y and z. Distinct choices of x, y, z yield distinct involutions in

J, as each non–identical permutation in G has at most three fixed points, whence

$$|J| = \left(\begin{array}{c} 11 \\ 3 \end{array} \right) = 165.$$

It is now clear that J satisfies properties a1), a2), a3) and a4) above. Proposition 7.1 yields $J = I$ or $J = I^*$: again, after possibly replacing G and M by suitable conjugates fGf^{-1}, fMf^{-1} with $f \in S_{11}$, we may limit our discussion to the former case.

Thus far M and G share the stabilizer of the element 1 and the involutions. The idea is now that of showing that M and G share more and more elements untill they share everything. The proof is obtained through the next properties, requiring a combined use of combinatorial arguments and elementary facts from group theory.

Proposition 7.3 *We have $G_x = M_x$ for each $x \in X$.*

Proof. The assertion is true if $x = 1$. Assume $x \neq 1$. As a 3–transitive permutation group on $X \setminus \{x\}$, the group M_x acts primitively on $X \setminus \{x\}$; in particular the stabilizer M_{1x} is a maximal subgroup of M_x and so, since I_x contains at least one involution not fixing 1, we have $\langle M_{1x}, I_x \rangle = M_x$.

Since both M_1 and I are in G, we have that G_x contains M_{1x} and I_x. We already remarked that G_x is a group, whence $M_x = \langle M_{1x}, I_x \rangle \leq G_x$; the equality $|G_x| = |M_x|$ yields now $G_x = M_x$. □

Let F denote the subset of G consisting of all permutations in G with at least one fixed point. We have $F = \cup_{x \in X} G_x = \cup_{x \in X} M_x$.

Proposition 7.4 *We have $|F \cap G(y \mapsto x)| = 444$ for any two distinct elements $x, y \in X$.*

Proof. We have

$$F \cap G(y \mapsto x) = \bigcup_{\substack{z \in X \\ z \notin \{x,y\}}} G(y \mapsto x)_z.$$

The principle of inclusion–exclusion has been invoked several times at this Summer School and we apply it here to compute the cardinality of the right–hand–side as

$$\sum_{\substack{z \in X \\ z \notin \{x,y\}}} |G(y \mapsto x)_z| \; - \sum_{\substack{z,u \in X \\ z,u \notin \{x,y\} \\ z \neq u}} |G(y \mapsto x)_{zu}| \; + \sum_{\substack{z,u,w \in X \\ z,u,w \notin \{x,y\} \\ |\{z,u,w\}| = 3}} |G(y \mapsto x)_{zuw}|.$$

The sharp 4–transitivity of G on X yields

$$|G(y \mapsto x)_z| = 72, \quad |G(y \mapsto x)_{zu}| = 8, \quad |G(y \mapsto x)_{zuw}| = 1,$$

whence

$$|F \cap G(y \mapsto x)| = 9 \cdot 72 - \left(\begin{array}{c} 9 \\ 2 \end{array} \right) \cdot 8 + \left(\begin{array}{c} 9 \\ 3 \end{array} \right) \cdot 1 = 444$$

□

Proposition 7.5 *We have $G(y \mapsto x) = M(y \mapsto x)$ for all pairs x, y of distinct elements in X.*

Proof. Let g be an arbitrary permutation in $F \cap G(y \mapsto x)$. The permutation set $G(y \mapsto x)g^{-1}$ contains the identity, fixes x and acts sharply 3–transitively on $X \setminus \{x\}$. Proposition 7.2 shows that $G(y \mapsto x)g^{-1}$ is a group. More precisely, since $G(y \mapsto x)g^{-1}$ fixes x, it is a conjugate in S_{11} of M_x fixing x, i.e. $G(y \mapsto x)g^{-1} = hM_xh^{-1}$ for some permutation $h \in S_{11}$ with $h(x) = x$. We have thus $G(y \mapsto x) = hM_xh^{-1}g$ and consequently $hM_xh^{-1}g = hM_xh^{-1}k$ for any two $g, k \in F \cap G(y \mapsto x)$. Since g and k also lie in the Mathieu group M we also have $M(y \mapsto x) = M_xg = M_xk$. We obtain $gk^{-1} \in M_x \cap hM_xh^{-1}$ and so the intersection $M_x \cap hM_xh^{-1}$ contains all 444 distinct permutations gk^{-1} obtained when g is fixed and k varies over the 444 permutations in $F \cap G(y \mapsto x)$. As both M_x and hM_xh^{-1} are groups of order 720 we see that $M_x = hM_xh^{-1}$ is the unique possibility and the assertion follows. □

Proposition 7.6 *We have $G = M$ and so we conclude that a sharply 4–transitive permutation set of degree 11 containing the identity is a group, a copy of the Mathieu group of degree 11.*

Proof. An immediate consequence of the above discussion and of the relations

$$G = G_x \cup \Big(\bigcup_{\substack{y \in X \\ y \neq x}} G(y \mapsto x) \Big), \qquad M = M_x \cup \Big(\bigcup_{\substack{y \in X \\ y \neq x}} M(y \mapsto x) \Big).$$

□

7.2 Degrees 12, 13 and more

The next step in the proof of Proposition 6.2 are the following two properties.

Proposition 7.7 *A sharply* 5*–transitive permutation set of degree* 12 *containing the identity is necessarily a group, a copy of the Mathieu group of degree* 12*.*

Proposition 7.8 *There exists no sharply* 6*–transitive permutation set on* 13 *elements.*

They are obtained in much the same way as Proposition 7.6, with the information on the one–point–stabilizers coming from the previous degrees and computer checks on the involutions of similar nature and complexity as that illustrated in Proposition 7.1. Running times returned by a `Runtime()` command were 354760 milliseconds for degree 12 on a 32 bit Pentium Pro II under Windows 95 running GAP with 24 MB RAM and 4603960 milliseconds for degree 13 on a 32 bit Pentium Pro II under Windows NT running GAP with 48 MB RAM.

Proposition 7.8 was actually the beginning of my involvement in this whole matter. I happened to attend the closing lecture of the 17–th British Combinatorial Conference in 1997, in which John H. Conway presented his beautiful puzzle M_{13} based on the projective plane of order 3. My attention was unavoidably attracted by properties (2) and (4) in Section 2 of the written version of the lecture, appearing in *Surveys in Combinatorics, 1997*, R.A. Bailey ed., pp. 1–11, Cambridge University Press, Cambridge 1997. Having worked on sharply multiply transitive permutation sets which are not groups, I was more and more "puzzled" by the statement that M_{13} yielded a sharply 6–transitive permutation set on 13 letters. It was in the process of reconstructing M_{13} with the Computer Algebra packages, that I kept getting a `false` whenever I was issuing the appropriate command checking sharp 6–transitivity...!

Proposition 7.9 *Let d be an integer, $d \geq 6$. There exists no invertible sharply d–transitive permutation set of degree $\geq d+3$.*

Proof. The proof is obtained essentially by considering the stabilizers and applying induction on d. □

Putting it all together we have the final statement

Proposition 7.10 *Let G be an invertible sharply d–transitive permutation set on a finite set X. If $d \geq 6$ then G is either S_d, S_{d+1} or A_{d+2}. If $d = 5$ then G is either S_5, S_6, A_7 or the Mathieu group of degree* 12*. If $d = 4$ then G is either S_4, S_5, A_6 or the Mathieu group of degree* 11*.*