**21-373, Algebraic Structures**, Department of Mathematical Sciences, Carnegie Mellon University
**Fall 2011**: (Math Studies Section) Monday, Wednesday, Friday, 10:30 am, Porter Hall 226B.
Luc TARTAR, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

13- Wednesday September 28, 2011.

**Remark 13.1**: Conjugation in $S_n$ is simply changing the name of elements: if a permutation $\pi$ has a cycle $(a_1 \cdots a_k)$, and $\sigma \in S_n$, then $\sigma\,\pi\,\sigma^{-1}$ has a cycle $\big(\sigma(a_1) \cdots \sigma(a_k)\big)$, so that two permutations which have the same pattern in their cycle decomposition are conjugate in $S_n$. However, the situation becomes different in $A_n$, since one wants to impose that $\sigma \in A_n$: although 3-cycles are all conjugate in $S_n$ for all $n \geq 3$, one needs $n \geq 5$ for showing that all 3-cycles are conjugate in $A_n$, and the result does not hold for $n = 3$ or $n = 4$.

After noticing that one always assume that the elements of a $k$-cycle are distinct, that $(a\,b)$ and $(b\,a)$ denote the same transposition which is its own inverse, and that $(a\,b\,c)$, $(b\,c\,a)$, and $(c\,a\,b)$ denote the same 3-cycle, what happens for $n = 4$ is that when one conjugates a 3-cycle $(a\,b\,c)$ by a transposition $\tau = (x\,y)$ either $x$ or $y$ belongs to $\{a, b, c\}$, and for $n = 3$ both $x$ and $y$ belong to $\{a, b, c\}$: since $(a\,b)\,(a\,b\,c)\,(a\,b) = (a\,c\,b)$, one deduces that for $n = 3$ $(a\,b\,c)$ and $(a\,c\,b)$ are exchanged in conjugating by any transposition, so that they are not conjugate in $A_3$ (which also follows from the fact that $A_3$ is Abelian, since it is isomorphic to $\mathbb{Z}_3$); for $n = 4$, one also observes that for $d \notin \{a, b, c\}$ one has $(a\,d)\,(a\,b\,c)\,(a\,d) = (b\,c\,d)$, and one deduces that the eight 3-cycles in $A_4$ split into two classes, $X = \{(1\,2\,3), (1\,3\,4), (1\,4\,2), (2\,4\,3)\}$ and $Y = \{(1\,2\,4), (1\,3\,2), (1\,4\,3), (2\,3\,4)\}$, and that conjugation by a transposition takes a cycle of one class into any cycle in the other class, so that (since elements of $A_4$ are products of an even number of transpositions) $X$ and $Y$ are conjugacy classes in $A_4$.

**Lemma 13.2**: For $n \geq 5$, the alternating group $A_n$ is simple.[1]
*Proof*: $A_n$ is generated by all 3-cycles: indeed, every element of $A_n$ is a product of terms of the form $(a\,b)\,(c\,d)$ or $(a\,b)\,(a\,c)$, where $a, b, c, d$ are distinct, and one has $(a\,b)\,(c\,d) = (a\,c\,b)\,(a\,c\,d)$ and $(a\,b)\,(a\,c) = (a\,c\,b)$.

Given distinct $r, s \in \{1, \ldots, n\}$, $A_n$ is generated by the 3-cycles $(r\,s\,k)$, for $k = 1, \ldots, n$ with $r \neq k \neq s$: indeed, any 3-cycle is of the form $(r\,s\,a)$ or $(r\,a\,s)$ if it uses both $r$ and $s$, of the form $(r\,a\,b)$ if it only uses $r$, of the form $(s\,a\,b)$ if it only uses $s$, or of the form $(a\,b\,c)$ if it uses neither $r$ nor $s$, where $a, b, c$ are distinct and distinct from $r, s$ (hence $n \geq 5$); then one has $(r\,a\,s) = (r\,s\,a)\,(r\,s\,a)$, then $(r\,a\,b) = (r\,s\,b)\,(r\,a\,s)$, then $(s\,a\,b) = (r\,b\,s)\,(r\,s\,a)$, and $(a\,b\,c) = (r\,a\,s)\,(r\,s\,c)\,(s\,a\,b)$.

All 3-cycles are conjugate in $A_n$, since if $a, b, c, d, e$ are distinct (which uses $n \geq 5$), conjugating $(a\,b\,c)$ by $(c\,e)$ in $S_n$ gives $(a\,b\,e)$ and then conjugating by $(d\,e)$ in $S_n$ gives $(a\,b\,d)$, which is then conjugate to $(a\,b\,c)$ in $A_n$; repeating the operation of changing one element of the 3-cycle shows that all 3-cycles are conjugate in $A_n$. If $N$ is a normal subgroup of $A_n$ containing a 3-cycle, then it contains all the 3-cycles, which generate $A_n$, so that $N = A_n$.

The rest of the proof consists in creating a 3-cycle from whatever there is in $N$, assumed to be a normal subgroup, and one considers different cases according to the length of the disjoint cycles for some elements of $N$, the first case being that of an element with a cycle of length $\geq 4$. If $\sigma = (a_1 \cdots a_r)\,\tau \in N$ with $r \geq 4$, and $\tau$ is a permutation using other elements than $a_1, \ldots, a_r$, one uses $\delta = (a_1 a_2 a_3) \in A_n$, and one writes that $\sigma^{-1}(\delta\,\sigma\,\delta^{-1}) \in N$ (since $(\delta\,\sigma\,\delta^{-1}) \in N$, because $N$ is a normal subgroup), and it is $\tau^{-1}(a_1 a_r a_{r-1} \cdots a_2)\,(a_1 a_2 a_3)\,(a_1 a_2 \cdots a_r)\,\tau\,(a_1 a_3 a_2) = (a_1 a_3 a_r) \in N$, so that $N = A_n$ since $N$ contains a 3-cycle. If an element contains at least two cycles of length 3, i.e. $\sigma = (a_1 a_2 a_3)\,(a_4 a_5 a_6)\,\tau \in N$, one uses $\delta = (a_1 a_2 a_4) \in A_n$ and one has $\sigma^{-1}(\delta\,\sigma\,\delta^{-1}) = \tau^{-1}(a_4 a_6 a_5)\,(a_1 a_3 a_2)\,(a_1 a_2 a_4)\,(a_1 a_2 a_3)\,(a_4 a_5 a_6)\,\tau\,(a_1 a_4 a_2) = (a_1 a_4 a_2 a_6 a_3) \in N$, so that $N$ contains a 5-cycle, hence $N = A_5$ by the preceding case. If an element contains exactly one cycle of length 3, i.e. $\sigma = (a_1 a_2 a_3)\,\tau \in N$ (and $\tau$ is a product of disjoint 2-cycles not using $a_1, a_2, a_3$), then $\sigma^2 = (a_1 a_2 a_3)\,\tau\,(a_1 a_2 a_3)\,\tau = (a_1 a_2 a_3)^2 = (a_1 a_3 a_2) \in N$, so that $N = A_n$ since $N$ contains a 3-cycle. If an element contains only disjoint 2-cycles, i.e. $\sigma = (a_1 a_2)(a_3 a_4)\,\tau \in N$ (and $\tau$ is a product of disjoint 2-cycles not using $a_1, a_2, a_3, a_4$), one uses $\delta = (a_1 a_2 a_3) \in A_n$ and one has $\rho = \sigma^{-1}(\delta\,\sigma\,\delta^{-1}) = \tau^{-1}(a_3 a_4)(a_1 a_2)(a_1 a_2 a_3)(a_1 a_2)(a_3 a_4)\tau\,(a_1 a_3 a_2) = (a_1 a_3)(a_2 a_4) \in N$; if $b$ is distinct from $a_1, a_2, a_3, a_4$ (hence $n \geq 5$), and $\eta = (a_1 a_3 b)$, then $\rho\,(\eta\,\rho\,\eta^{-1}) = (a_1 a_3)(a_2 a_4)(a_1 a_3 b)(a_1 a_3)(a_2 a_4)(a_1\,b\,a_3) = (a_1 a_3 b) \in N$.

[1] Since $A_2 = \{e\}$ and $A_3 \simeq \mathbb{Z}_3$, they are simple, but $A_4$ is not simple, and it has a unique Sylow 2-subgroup which a normal subgroup of order 4, isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

**Remark 13.3**: Besides the first infinite family of *cyclic groups* $\mathbb{Z}_p$ for $p$ prime, which gives all the finite Abelian simple groups (apart from the trivial case $G = \{e\}$), and the second infinite family of *alternating groups* $A_n$ for $n \geq 5$ (which contains the finite non-Abelian simple group of lowest order 60, but not the next one, which has order 168, while $A_6$ has order 360), there are 16 other infinite families of finite non-Abelian simple groups, and the first 9 are *Chevalley groups*,[2] $A_n(q)$ (linear groups) excepted $A_1(2)$ (isomorphic to $S_3$) and $A_1(3)$ (isomorphic to $A_4$); $B_n(q), n \geq 2$ (orthogonal groups) excepted $B_2(2)$ (isomorphic to $S_6$); $C_n(q), n \geq 3$ (symplectic groups), $D_n(q), n \geq 4$ (orthogonal groups), $E_6(q)$, $E_7(q)$, $E_8(q)$, $F_4(q)$, $G_2(q)$ excepted $G_2(2)$; they are version of *Lie groups* built of the finite fields $F_q$ (with $q$ a power of a prime $p$).[3]

Besides these 16 infinite families, there are 26 exceptional simple groups named *sporadic groups*, the two smaller being (two of the) *Mathieu groups*,[4] $M_{11}$, order $7,920 = 2^4 \cdot 3^2 \cdot 5 \cdot 11$, which is a *4-transitive permutation group* on 11 points,[5] and $M_{12}$, order $95,040 = 2^6 \cdot 3^3 \cdot 5 \cdot 11$, which is a 5-transitive permutation group on 12 points; the 26th sporadic group is the *Fischer–Griess monster group* $M$,[6,7] which has order $2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71$, i.e. it has more than $8 \cdot 10^{53}$ elements.[8]

**Remark 13.4**: After $A_5$ which has order 60, the next non-Abelian finite simple group comes from the family $A_n(q)$, also written $PSL_{n+1}(q)$ or $PSL(n+1, q)$, where $PSL$ stands for *projective special linear group*: for a field $F$, if $V$ is a *vector space* of *dimension* $m$ over $F$ (i.e. $V$ is isomorphic to $F^m$), $GL(V)$ (also written $GL_m(F)$) is the *general linear group* of invertible linear mappings from $V$ into $V$, which is like invertible $m \times m$ matrices with entries in $F$, $SL(V)$ (also written $SL_m(F)$) is the *special linear group* of elements of $GL(V)$ having *determinant* $+1$, and the term projective applied to a group $\Gamma$ (here either $GL_m(F)$ or $SL_m(F)$) consists in taking the quotient $\Gamma/Z(\Gamma)$ of the group $\Gamma$ by its center $Z(\Gamma)$;[9] then, for $q$ a power of a prime $p$, there is a field $F_q$ of order $q$, and $PSL_k(q)$ or $PSL(k, q)$ means $PSL_k(F_q)$.

$A_n(q)$ has order $\frac{1}{(n+1,q-1)}\, q^{n\,(n+1)/2} \prod_{i=1}^{n}(q^{i+1}-1)$, and besides the excluded cases $A_1(2) = PSL_2(\mathbb{Z}_2) \simeq S_3$ and $A_1(3) = PSL_2(\mathbb{Z}_3) \simeq A_4$, one has $A_1(5) = PSL_2(\mathbb{Z}_5) \simeq A_5$, and $A_1(7) = PSL_2(\mathbb{Z}_7)$ is the second finite simple non-Abelian group, which has order 168, and it is actually isomorphic to $A_2(2) = PSL_3(\mathbb{Z}_2)$.

**Remark 13.5**: Etymology of *geometry* is about measuring the earth, involving lengths and one type of angles, but there are two types of angles used in *spherical trigonometry*,[10] and this must have been classical at the time when MAUPERTUIS headed a French expedition to Lapland in 1736–37 for measuring the length of one degree of the meridian,[11] which confirmed that the earth is oblate, i.e. flatter at the poles, which I think NEWTON had conjectured.[12] The question of conserving angles in maps was crucial for sailing, once the compass (a Chinese invention introduced in Europe by Marco POLO) permitted to find the direction of

[2] Claude CHEVALLEY, French mathematician (born in South Africa) 1909–1984. He was a founding member of the Bourbaki group. He worked at Princeton University, Princeton, NJ, Columbia University, New York, NY, and at Université Paris VII (Denis Diderot), Paris, France.

[3] Marius Sophus LIE, Norwegian mathematician, 1842–1899. He worked in Kristiania (now Oslo), Norway. Lie groups and Lie algebras are named after him.

[4] Émile Léonard MATHIEU, French mathematician, 1835–1890. He worked in Besançon, and in Nancy, France.

[5] An action of a group $G$ on a set $X$ is *transitive* if for each $x, y \in X$ there exists $g \in G$ such that $g\,x = y$, i.e. the orbit of any $x \in X$ is the whole $X$; it is *n-transitive* if $X$ has at least $n$ elements and for every two $n$-tuples $x_1, \ldots, x_n$ and $y_1, \ldots, y_n$ in $X$ there exists $g \in G$ such that $g\,x_j = y_j$ for $j = 1, \ldots, n$.

[6] Bernd FISCHER, German mathematician, born in 1936. He worked at the Johann Wolfgang Goethe-Universität, Frankfurt am Main, and in Bielefeld, Germany.

[7] Robert Louis GRIESS, Jr., American mathematician, born in 1945. He works at University of Michigan, Ann Arbor, MI.

[8] More precisely 808,017,424,794,512,875,886,459,904,961,710,757,005,754,368,000,000,000 elements.

[9] The center of a group is a characteristic subgroup, hence a normal subgroup.

[10] Instead of angles and sides for a planar triangle, since the length of a side on the sphere corresponds to an angle with its vertex at the center of the sphere.

[11] Pierre Louis Moreau DE MAUPERTUIS, French-born mathematician, 1698–1759. He worked in Paris, France, and in Berlin, then capital of Prussia, now capital of Germany.

[12] Sir Isaac NEWTON, English mathematician, 1643–1727. He worked in Cambridge, England, holding the Lucasian chair (1669–1701). There is an Isaac Newton Institute for Mathematical Sciences in Cambridge,

the (magnetic) North Pole;[13] finding the latitude was easy at night (in the northern hemisphere) by looking at the polar star,[14] but finding the longitude was not possible before one had improved the clocks, and this problem of finding one's position changed in the 20th century after the development of radio-goniometry and more recently of GPS (Global Positioning System): the mathematical study of *conformal transformations* (differentiable mappings conserving orientation and angles) is an extension of the question of maps for sailors; special ones are the stereographic projection (usually made around a pole, where one does not navigate), the Mercator projection on a cylinder,[15] more practical but distorting away from the equator, and the Lambert projections on cones,[16] which can be adapted to be accurate at any given latitude, so that sailors use these maps nowadays (even with a GPS system). A mapping (from a metric space into another) which conserves distances is called an *isometry*, and if it maps an Euclidean space of dimension $n$ (over $\mathbb{R}$) into itself such a mapping is automatically *affine*, i.e. it has the form $x \mapsto a + M\,x$ for some $a \in \mathbb{R}^N$ and some linear mapping $M$ from $\mathbb{R}^n$ into itself, but for being an isometry $M$ must belong to the *orthogonal group* $\mathbb{O}(n)$, the subgroup of the *general linear group* $GL(n, \mathbb{R})$ (of invertible linear maps from $\mathbb{R}^n$ into itself) of those $M$ satisfying $M^T M = I$; this implies that the *determinant* of $M$ is $\pm 1$, and those $M$ of determinant $+1$ form the *special orthogonal group* $S\mathbb{O}(n)$, whose elements are called *rotations*. The affine conformal mappings are those affine mappings which conserve orientation (i.e. have positive determinant) and angles, and they correspond to a larger group than $S\mathbb{O}(n)$, those $M$ such that $\lambda\,M \in S\mathbb{O}(n)$ for some $\lambda > 0$; a differentiable mapping $u$ is a conformal mapping if $det(\nabla\,u) > 0$ and $\nabla\,u^T \nabla\,u = \mu\,I$ for a positive function $\mu$. A rotation in the plane, i.e. an element of $S\mathbb{O}(2)$, has the form $\begin{pmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{pmatrix}$ for some $\theta \in \mathbb{R}$, so that if a mapping $(x, y) \mapsto \big(P(x, y), Q(x, y)\big)$ is conformal one has $\frac{\partial P}{\partial x} = \frac{\partial Q}{\partial y}$ and $\frac{\partial P}{\partial y} = -\frac{\partial Q}{\partial x}$, which is the Cauchy–Riemann system characterizing an *holomorphic* function $f(z) = P(x, y) + i\,Q(x, y)$ of $z = x + i\,y$ (from an open set of $\mathbb{C}$ into $\mathbb{C}$), i.e. a mapping which is differentiable in the complex sense, and it is locally the sum of its Taylor expansion.[17]

**Remark 13.6**: Greek geometers used geometry in a more abstract sense, talking about lines and planes with some axioms concerning them, and one axiom of EUCLID is that from a point outside a line there is exactly one parallel to the line, and many mathematicians tried to prove this result: the situation was not yet so clear in the beginning of the 19th century, so that after BOLYAI and LOBACHEVSKY published their work on non-Euclidean geometries,[18,19] GAUSS wrote to a friend that he had already done that (which is perfectly possible, since GAUSS was a mathematical genius) but that he could not have mentioned having worked

England. The unit of force is named after him, and a Newton is the force necessary to accelerate the unit of mass (a kilogram) to the unit of acceleration (a meter per square second).

[13] Marco POLO, Italian merchant, 1254–1324. Born in the republic of Venezia (Venice), he traveled to China with his father and his uncle, and he became famous by his book on what he learned during his travels.

[14] Before the compass, Norse men were not afraid to sail in high sea (when others only navigated near the coasts, even in the Mediterranean sea), navigating eastward or westward: in this way, they discovered Iceland and settled there, and according to Icelandic sagas, they then discovered Greenland, and according to the Vinland saga, they once were thrown out of their way by a storm and landed in a place where grapes grew, which must have been Labrador, too cold now for grapes to grow, but the weather must have been much warmer around the year 1000 since one could sail from Iceland to Greenland without finding icebergs on one's way (and the much warmer climate in these days cannot be explained by accusing the industry of having sent too much green-house gases in the atmosphere!).

[15] Gerardus MERCATOR (Gerhard KREMER), Flemish-born geographer and cartographer, 1512–1594. He worked in Cleve, Germany.

[16] Johann Heinrich LAMBERT, French-born mathematician, 1728–1777. He worked in Berlin, Germany. Lambert's (conformal) projections, and Lambert's law for radiation are named after him.

[17] Brook TAYLOR, English mathematician, 1685–1731. He worked in London, England. The Taylor expansion is named after him.

[18] János BOLYAI, Hungarian mathematician, 1802–1860.

[19] Nikolai Ivanovich LOBACHEVSKY, Russian mathematician, 1792–1856.

on non-Euclidean geometries, because it could have damaged his career.[20] Without going into defining Riemannian manifolds, it is easy to understand what the mathematical problem is by trying to define a "line" on a sphere: since there are (complex) lines on a complex sphere but no (real) lines on a real sphere,[21] the main idea is to extend a property of lines in $\mathbb{R}^3$ (with its usual *Euclidean structure*), that a line is the shortest path between two of its points.[22] One then decides that a "line" on a surface (embedded in $\mathbb{R}^3$, with its usual Euclidean structure) is any smooth curve on the surface which gives the shortest path between two near-by points on it,[23] called a *geodesics* of the surface,[24] and for a sphere a geodesics is a *great circle*,[25] intersection of the sphere with a plane going through the center of the sphere; a consequence is that two distinct "lines" on the sphere always intersect, at exactly two antipodal points, and two distinct points belong to exactly one line if (and only if) they are not antipodal, but they belong to infinitely many lines if they are antipodal. It is "natural" then to consider the *quotient space* obtained by identifying antipodal points, and observe that it gives an example of the real *projective plane* $\mathbb{R}P^2$.

Pappus of Alexandria is considered the father of projective geometry,[26] and something similar was rediscovered for perspective in painting, probably by della Francesca:[27] for perspective, the painter does

[20] Since one would have considered as mad anyone who thought that there could exist another geometry than that of Euclid, on which everything had been based. Of course, considering that the gravitational field on earth is constant is just an approximation, but it is good enough for the small size of the constructions built on earth.

[21] Through $a = (1,0,0) \in \mathbb{C}^3$, belonging to the "unit sphere" $\mathbb{S}^2 \subset \mathbb{C}^3$, having equation $x_1^2 + x_2^2 + x_3^2 = 1$, one considers the line parametrized by $a + t\,b$ for $t \in \mathbb{C}$ (and $b \neq 0$), which belongs to the unit sphere if (and only if) $b_1 = 0$ and $b_2^2 + b_3^2 = 0$, so that $b_3 = \pm i\, b_2$ (and $b_2 \neq 0$). Notice that there is another notion of "unit sphere" when one puts on $\mathbb{C}^3$ an *Hermitian structure*, for example $(x,y) = x_1\overline{y_1} + x_2\overline{y_2} + x_3\overline{y_3}$, corresponding to the distance $d(x,y) = (x-y, x-y)^{1/2}$, which is invariant by translations and associated to the norm $||x|| = (x,x)^{1/2}$, and as in any metric space, one may consider the (closed) unit ball centered at $0$ ($\{x \in \mathbb{C}^3 \mid ||x|| \leq 1\}$), and its boundary ($\{x \in \mathbb{C}^3 \mid ||x|| = 1\}$) is also called the unit sphere.

[22] If one parametrizes a smooth curve in $\mathbb{R}^3$ (with its usual Euclidean structure) by $M(t)$, then the length of the curve between two points $A_1 = M(t_1)$ and $A_2 = M(t_2)$ (with $t_1 < t_2$) is $\int_{t_1}^{t_2} \big|\big|\frac{dM}{dt}\big|\big|\,dt$, which by the triangle inequality applied to (Riemann) integrals is $\geq \big|\big|\int_{t_1}^{t_2} \frac{dM}{dt}\,dt\big|\big| = ||M(t_2) - M(t_1)||$, the distance from $A_1$ to $A_2$ along the line that they define.

[23] It is true of great circles on a sphere, but given two non-antipodal points on such a circle, only one side gives the shortest distance, which explains the reason of mentioning near-by points.

[24] If one parametrizes a smooth curve in $\mathbb{R}^3$ (with its usual Euclidean structure) by $M(s)$, where $s$ is the *arc-length* along the curve, then $\tau(s) = \frac{dM}{ds}$ is a unit vector; differentiating $||\tau(s)||^2 = 1$ gives $\frac{d\tau}{ds} = \frac{n(s)}{R(s)}$ where $0 < R(s) \leq \infty$ is the *radius of curvature* (and $\frac{1}{R}$ is the *curvature*) and $n$ is a unit vector orthogonal to $\tau$ (the principal *normal* if $R \neq \infty$); assuming that $R \neq \infty$, and differentiating $||n(s)||^2 = 1$ and $\big(\tau(s), n(s)\big) = 0$ one deduces that $\frac{dn}{ds} = -\frac{\tau(s)}{R(s)} + \frac{b(s)}{T(s)}$ for a unit vector $b$ orthogonal to $\tau$ and $n$, and $\frac{1}{T}$ is the *torsion*, and one deduces that $\frac{db}{ds} = -\frac{n(s)}{T}$ by differentiating $||b(s)||^2 = 1$, $\big(\tau(s), b(s)\big) = 0$ and $\big(n(s), b(s)\big) = 0$. If one perturbs this curve by $M(s) + t\,V(s)$ for $t$ small and $V$ smooth and $0$ outside $(s_1, s_2)$ (and $s_1 < s_2$), its length between $M(s_1)$ and $M(s_2)$ is $\int_{s_1}^{s_2} \big|\big|\frac{dM}{ds} + t\,\frac{dV}{ds}\big|\big|\,ds$; if $V(s) = \alpha(s)\,\tau(s) + \beta(s)\,n(s) + \gamma(s)\,b(s)$ with $\alpha, \beta, \gamma$ smooth, then $\big|\big|\tau + t\,\frac{dV}{ds}\big|\big|^2 = 1 + 2t\,\frac{d\alpha}{ds} - 2t\,\frac{\beta}{R} + O(t^2)$, so that $\int_{s_1}^{s_2} \big|\big|\frac{dM}{ds} + t\,\frac{dV}{ds}\big|\big|\,ds = s_2 - s_1 - t\int_{s_1}^{s_2} \frac{\beta}{R}\,ds + O(t^2)$: if for all $t$ small the length of the perturbed curve is $\geq s_2 - s_1$, one deduces that $\int_{s_1}^{s_2} \frac{(V,n)}{R}\,ds = 0$. If the curve lies on a smooth surface and gives the shortest distance on the surface between $M(s_1)$ and $M(s_2)$, then one applies the preceding computation to any $V$ such that $V(s)$ is tangent to the surface at $M(s)$ (by using the implicit function theorem), and one deduces that at points where the radius of curvature $R(s)$ is finite one has $n(s) = \pm\nu\big(M(s)\big)$, where $\nu(M)$ is the normal to the surface at $M$.

[25] The radius of curvature $R(s)$ of a smooth curve on a sphere of radius $R_0$ satisfies $0 \leq R(s) \leq R_0$, and for a geodesics it has to be $R_0$, from which one deduces that geodesics are great circles.

[26] Pappus of Alexandria, "Egyptian" mathematician, 290–350. He worked in Alexandria, Egypt.

[27] Piero della Francesca, Italian mathematician and painter, 1412–1492. He worked in Arezzo, and in Borgo San Sepulchro, Italy.

not use the whole projective plane, since his frame is limited; using the painter's eye as origin, and the frame a vertical $(x,y)$ plane at $z=1$ (with $x$ and $z$ axes horizontal), the painter draws what he sees at $(x,y,z)$ with $z>1$ at the point $\left(\frac{x}{z},\frac{y}{z}\right)$ of the frame; the mapping from any plane not going through the origin to the frame is an example of projective transformation. The mathematical theory was extended in the 17th century by DESARGUES and by PASCAL,[29,30] and projective properties of conic sections were rediscovered by PONCELET,[31] since he did not have access to a scientific library.[32]

New applications of projective geometry have appeared more recently, in robotics, for the question of identifying what a robot "sees" through its cameras.

**Definition 13.7**: A set $P\neq\emptyset$ is a projective plane if it has subsets called lines such that any two distinct points define a unique line, and any two distinct lines intersect at a unique point. One has a notion of duality, by defining $P'$ such that the points of $P'$ are the lines of $P$ and the lines of $P'$ are the points of $P$.[33]

For each field $F$ and each integer $n\geq 1$, one obtains the *projective space* $FP^n$ of dimension $n$ over $F$ by considering in $F^{n+1}\setminus\{0\}$ the equivalence relation $a\,\mathcal{R}\,b$ if and only if $b=\lambda\,a$ for some $\lambda\in F^*=F\setminus\{0\}$.

**Remark 13.8**: Lengths and angles on the sphere are not part of the definition of a projective plane. Another way of describing the real projective plane $\mathbb{R}P^2$ is to start with the real plane $\mathbb{R}^2$ and add a "line" at $\infty$ in a particular way: one first adds a point at $\infty$ in the direction $(\cos\theta,\sin\theta)$ for each $\theta$ modulo $2\pi$, and this gives a topological space homeomorphic to the closed disc $(\{(x,y)\in\mathbb{R}^2\mid x^2+y^2\leq 1\})$ or to the closed upper hemisphere $(\{(x,y,z)\in\mathbb{R}^3\mid z\geq 0, x^2+y^2+z^2=1\})$, which are manifolds with boundary, and then one obtains the real projective plane $\mathbb{R}P^2$ by identifying for each $\theta$ the point at $\infty$ in the direction $\theta$ and the point at $\infty$ in the direction $\theta+\pi$, which gives a (non-orientable) compact manifold (without boundary).

**Remark 13.0**: A projective line $(n=1)$ consists in adding to $F$ one point, considered to be at $\infty$.[34]

If $F$ is finite and has $q$ elements, then $F^{n+1}\setminus\{0\}$ has $q^{n+1}-1$ elements, and each equivalence class has $q-1=|F^*|$ elements, so that the projective space $FP^n$ has $\frac{q^{n+1}-1}{q-1}=1+q+\ldots+q^n$ elements, hence $FP^2$ has $q^2+q+1$ elements: in the usual plane $F^2$ there are $q+1$ lines through the origin, $q$ having the form $\{(a,\lambda\,a)\mid a\in F\}$ for $\lambda\in F$, and one having the form $\{(0,a)\mid a\in F\}$, and one obtains $FP^2$ by adding a point at $\infty$ in each of these $q+1$ directions, so that each line in $FP^2$ has $q+1$ points, and that is true of the line at $\infty$ containing all the $q+1$ points added at $\infty$.

$FP^2$ satisfies the properties of a projective plane: a point in $FP^2$ corresponds to a line (subspace of dimension 1) through 0, and a line in $FP^2$ corresponds to a plane (subspace of dimension 2) through 0; two distinct points in $FP^2$ correspond to two distinct lines generating a plane, i.e. they define a line in $FP^2$; two distinct lines in $FP^2$ correspond to two distinct subspaces of dimension 2, so that their union is $F^3$, and their intersection must then have dimension 1, so that it corresponds to a point in $FP^2$.

**Remark 13.11**: There is no field with 1 element, but $1^1+1+1=3$ and there is a projective plane with 3 elements, like the three vertices of a triangle, with the three lines being the three sides of the triangle; more

[29] Girard DESARGUES, French mathematician, 1591–1661.

[30] Blaise PASCAL, French mathematician and philosopher, 1623–1662. The Université de Clermont-Ferrand II, Aubière, France, is named after him. The unit of pressure is named after him, and a Pascal is the pressure created by a unit of force (a Newton) acting on a unit of surface (a square meter). Pascal's triangle showing the binomial coefficients is named after him, although it was found a few centuries before PASCAL, by AL KARAJI and by HALAYUDHA, then by Xian JIA, and later by Omar KHAYYÁM.

[31] Jean Victor PONCELET, French engineer, 1788–1867.

[32] PONCELET was a military engineer in the French army led by Napoléon to Russia, and he was wounded and left for dead near Smolensk, and once taken prisoner he had to walk almost one thousand miles from november to february to attain Saratov, on the Volga river, where he was assigned to reside until the war was over (two years later, in 1814), and he still had to walk back for another four months after being released. While in Saratov, he decided to write down all the mathematics that he had learned, and he extended what he had been taught.

[33] Assuming $P$ has at least two elements and two lines, $(P')'=P$.

[34] If $a=(a_1,a_2)$ satisfies $a_1\neq 0$, it belongs to the equivalence class of $(1,c)$ with $c=a_2a_1^{-1}$, and then all the elements $(0,a_2)$ with $a_2\neq 0$ belong to the same equivalence class, which one naturally calls $\infty$.

generally, for each $k \geq 2$ there is a projective plane with a line $D$ containing $k$ distinct points $M_1, \ldots, M_k$, and only one point $M_0$ not in $D$, and $k$ more lines $M_0 M_j$ for $j = 1, \ldots, k$. One usually excludes these trivial finite projective planes by *imposing that there are at least three distinct points on each line.*

Besides the trivial finite projective planes, it is not difficult to show that if a finite projective plane has a line $D$ with $k \geq 3$ distinct points and at least two distinct points not on the line, then all lines have $k$ distinct points and by each point there are $k$ different lines,[35] so that there are $(k-1)^2$ points not on the line and the total number of points is $n = k^2 - k + 1$, and the number of lines is the quotient of $\binom{n}{2}$ and $\binom{k}{2}$, which is $n$: if $k = q + 1$ it gives $n = q^2 + q + 1$ points.

**Remark 13.12**: The case $q = 2$ gives the Fano plane,[36] whose realization is to consider a triangle with the seven points being the vertices, the middle of the sides and the center of gravity (intersection of the three medians), and the seven lines are the three sides, the three medians, and a supplementary "line" going through the three middles of the sides.

The case $q = 3$ has thirteen points and thirteen lines of four points, and can be realized easily with a deck of 52 cards.[37]

**Remark 13.13**: A finite field $F$ has a finite characteristic $p$ which is a prime, and a prime field $F_0$ generated by 0 and 1 which is isomorphic to $\mathbb{Z}_p$, and since $F$ is a vector space over $F_0$ it has a dimension $k \geq 1$, and the number $q$ of elements of $F$ is then $p^k$; conversely, it is a side result of Galois theory that for each prime $p$ and each $k \geq 1$ there is a field with $p^k$ elements, unique up to an isomorphism. One may then wonder if there exists a finite projective plane with lines having $q + 1$ points if $q > 1$ is not a power of a prime (i.e. $q = 6, 10, 12, 15, \ldots$), and it has been shown that no such finite projective plane exists for $q = 6$ and $q = 10$, but it is not yet known what the situation is for $q \geq 12$.

Additional footnotes: al Karaji,[38] Goethe,[39] Halayudha,[40] Hermite,[41] Jia,[42] Khayyám.[43]

[35] If the points on $D$ are $M_1, \ldots, M_k$, and two points not on $D$ are $A$ and $B$, one may assume that the line $AB$ intersects $D$ at $M_1$. Through any point not in $D$ (in particular $A$ and $B$) there are $k$ lines, since each of these lines must intersect $D$; this shows that if all points belong to $k$ lines then all lines contain $k$ points. Using the line $AM_2$, one finds that $B, M_1, M_3, \ldots, M_k$ belong to $k$ lines, and using the line $AM_3$, one finds that $B$ and $M_2$ belong to $k$ lines.

[36] Gino Fano, Italian mathematician, 1871–1952. He worked in Messina, and in Torino (Turin), Italy.

[37] For example, using X for 10, J for jack, Q for queen, and K for king, one may write the four lines through 1 as 1234, 1567, 189X, 1JQK, using the rows of the matrix $M = \begin{pmatrix} 5 & 6 & 7 \\ 8 & 9 & X \\ J & Q & K \end{pmatrix}$, and the three other lines through 2 as 258J, 269Q, 27XK, using the columns of $M$, and the three other lines through 3 as 359K, 36XJ, 378Q, using the parallels to the first diagonal of $M$, and the three other lines through 4 as 45XQ, 468K, 479J, using the parallels to the second diagonal of $M$, giving the thirteen desired lines.

[38] Abu Bekr ibn Muhammad ibn al-Husayn al-Karaji, "Iraqi" mathematician, 953–1029. Although he was born in Baghdad (now in Iraq), and worked there, and his name is sometimes written al-Karkhi related to Karkh, a suburb of Baghdad, his family may have originated in Karaj, now in Iran. His work contained "Pascal's triangle", possibly before Halayudha.

[39] Johann Wolfgang von Goethe, German writer, 1749–1832. The Johann-Wolfgang-Goethe-Universität in Frankfurt am Main, Germany is named after him.

[40] Halayudha, Indian mathematician, 10th century. His work contained "Pascal's triangle" around 975, possibly before al Karaji.

[41] Charles Hermite, French mathematician, 1822–1901. He worked in Paris, France. Hermitian spaces and Hermite polynomials are named after him.

[42] Xian Jia, Chinese mathematician, 1010–1070. His work included "Pascal's triangle".

[43] Omar Khayyam (Ghiyath al-Din Abu'l-Fath Umar ibn Ibrahim Al-Nisaburi al Khayyami), Persian mathematician, astronomer, and poet, 1048–1131. He worked in Samarkand, Uzbekistan, in Esfahan (Ispahan), Iran, and in Merv (Mary), Turkmenistan. "Pascal's triangle" appears in his 1070 treatise, but it had appeared before in the work of al Karaji.