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

1- Monday August 29, 2011.

Historical considerations

The word *algebra* comes from the title of a book in Arabic by AL KHWARIZMI,[1] who worked in Baghdad, then capital of the Muslim world, in the academy "bayt al-hikma" (house of wisdom) founded by the Caliph HARUN AL-RACHID for translating Persian texts into Arabic,[2] to which (his second son) the Caliph AL MA'MUN gave the goal of translating Greek philosophical and mathematical texts into Arabic.[3,4] The influence of this academy on mathematics can be appreciated using the *MacTutor History of Mathematics archive, http://www-groups.dcs.st-and.ac.uk/ history/*,[5] a site created by two mathematicians from St Andrews in Scotland,[6] O'CONNOR and ROBERTSON:[7,8] their data base shows no Arabic names for mathematicians born before 750, but among the 36 names of those who were born between 750 and 1000, 29 are Arabic (i.e. 80 per cent) and 7 are Indian (i.e. 20 per cent).[9] The situation changes after 1000,[10] and this academy ended in 1258 when Baghdad was destroyed by the Mongols invasion (and after three years without a Caliph, the new Abbasid Caliph ruled from Egypt),[11] and it was said that the waters of the Tigris river ran

[1] Abu Ja'far Muhammad ibn Musa AL KHWARIZMI (or better KHAWARIZMI), "Arab" mathematician, 780–850. It is not known where he was from, but he worked in Baghdad, now capital of Iraq. The word "algebra" was derived from the title of his treatise *al-kitab al-mukhtasar fi hisab al-jabr w'al-muqabala*, and the word "algorithm" was coined from his name.

[2] HARUN AL-RACHID (or better AR-RACHID), fifth Caliph of the Abbasid dynasty, 763–809. He became Caliph in 786, and his time was marked by scientific, cultural and religious prosperity; art and music also flourished significantly during his reign, and he established the library bayt al-hikma (house of wisdom) and gave it the goal of translating Persian texts into Arabic. He ruled the Muslim world from Baghdad (on the Tigris river, now in Iraq) until 796, and after that from Ar Raqqah (on the Euphrates river, in actual Syria).

[3] Abu al-'Abbas 'abd Allah AL MA'MUN ibn Harun, seventh Caliph of the Abbasid dynasty, 786–833. He became Caliph in 813, and ruled over the Muslim world from Baghdad, now capital of Iraq. He gave the academy "bayt al-hikma" (house of wisdom), founded by his father HARUN AL-RACHID, the goal of translating Greek philosophical and mathematical texts into Arabic.

[4] My father had told me that the translations were made in two steps, probably because Greek was mostly known by Christians, since the original language of the "New Testament" is Greek and they used a version of the "Old Testament" in Greek (the Septuagint, made in Alexandria by seventy two Jewish scholars), so that some Christian scholars translated the Greek texts into Syriac (which was used for the Christian liturgy in the Middle East, Syriac being the dialect of Aramaic spoken in Mesopotamia), and then some Moslem scholars translated the text from Syriac into Arabic (which are two Semitic languages).

[5] The influence on philosophy can be seen in the fact that some texts by PLATO or ARISTOTLE would have been lost if they had not been translated into Arabic: in Europe, copying manuscripts was done by monks, and since the church had no interest in the philosophy of the ancient Greeks (since they were "pagans"), the corresponding manuscripts were lost by natural decay.

[6] St Andrews is known as the Home of the Golf, and claims a 600 year history of the Links.

[7] John J. O'CONNOR, British mathematician, born in 1945. He works at University of St Andrews, St Andrews, Scotland.

[8] Edmund Frederick ROBERTSON, Scottish mathematician, born in 1943. He works at University of St Andrews, St Andrews, Scotland.

[9] One should pay attention that names in Persian were often known by their Arabic translation, for example.

[10] Among the 32 names of those who were born between 1000 and 1250, 14 are European (i.e. 44 per cent), 8 are Arabic (i.e. 25 percent), 6 are Chinese (i.e. 19 percent) and 4 are Indian (i.e. 12 per cent), and among the 46 names of those who were born between 1250 and 1500, 32 are European (i.e. 69 per cent), 7 are Arabic (i.e. 15 percent), 5 are Indian (i.e. 11 percent) and 1 is Chinese (i.e. 2 per cent).

[11] AL 'ABBAS ibn 'abd al-Muttalib, 566–652. He was the uncle of MUHAMMAD, and the Abbasid Caliphs

black for six months with ink from the enormous quantities of books from all the libraries in Baghdad which had been thrown into the river. However, the decline of mathematics in the "Arab world" had obviously started earlier!

Although many of the early names in the MacTutor data base are not those of people we now call mathematicians, since one finds there astronomers and philosophers, I find it useful to compare with what happened to the Greek names before: among the 55 names of those born before our era, 46 are Greek (i.e. 84 per cent), 5 are Indian (i.e. 9 per cent), and 2 are Chinese (i.e. 4 per cent), and then among the 31 names of those born between 0 and 500, 18 are Greek (i.e. 58 per cent), 8 are Chinese (i.e. 25 per cent), and 2 are Indian (i.e. 6 per cent), and finally, among the 7 names of those born between 500 and 750, 5 are Indian (i.e. 71 per cent) and 1 is Chinese (i.e. 15 per cent). How should one explain that there are no Greek names among mathematicians from this data base who were born between 500 and 1500? Could it be that the Academy, a kind of university founded by PLATO in Athens around 387 BCE (before common era),[12] and which was closed in 529 by the Christian emperor Justinian I,[13] for being a pagan establishment, was the main place where mathematics and philosophy were taught together with a critical mind?

Certainly, the program of the Caliph AL MA'MUN to have Greek philosophical and mathematical texts translated into Arabic, and the contact with the Indian mathematicians was crucial for the extraordinary presence of Arabic names in mathematics for a few centuries, and their disappearance may have had the same reasons than for the disappearance of Greek names, a mixture of religious and political constraints. One may also notice that the Romans favoured the art of the engineer but produced almost no mathematicians, and apart from a Roman architect in the first century BCE, the MacTutor data base only has one Roman mathematician in the fifth century.

Formulas for roots of polynomials

Of course, there were results in algebra before the name was coined, and one often refers to DIOPHANTUS as the "father of algebra",[14] although many of the techniques he used for solving *linear* or *quadratic* equations had been known to the Babylonians. Ancient mathematicians had difficulties with notations, in particular they had no zero or minus sign, so that they looked for positive solutions, first rational numbers,[15] then square roots of rationals, which appeared naturally in solving quadratic equations, and they may have considered these square roots with a geometric interpretation based on *Pythagoras's theorem* for example.[16]

The formula for solving *cubic* equations only appeared in the 16th century, and it uses square roots and cubic roots: it was found by TARTAGLIA,[17] who made the mistake of telling it to CARDANO,[18] who published it under his name, so that it is now known as "Cardano's formula", but since it had been found earlier by DEL FERRO,[19] it would be more natural to call it the Del Ferro–Tartaglia–Cardano formula.

---

claimed the caliphate (which they took from the Umayyads) because he was their ancestor, and they ruled from 750 to 1258 from Baghdad (now in Iraq), and from 1261 to 1517 from Cairo, Egypt.

[12] PLATO, Greek philosopher, 427 BCE–347 BCE. He worked in Athens, Greece, presiding over the Academy which he founded around 387 BCE, and which lasted until 529, when it was closed down by the Christian emperor Justinian I (for being a pagan establishment).

[13] Justinian I (Flavius Petrus SABBATIUS), 482–565. Byzantine emperor from 527 to 565, he ruled from Constantinople (now Istanbul, Turkey).

[14] DIOPHANTUS of Alexandria, Greek mathematician, 200–284. He is often referred to as the 'father of algebra', although many of his techniques were known to the Babylonians.

[15] Egyptian did not use positive rationals as $\frac{a}{b}$ for two positive integers a, b, but as a sum of terms of the form $\frac{1}{n}$ for a positive integer n.

[16] PYTHAGORAS, Greek mathematician, 580–520 BCE. Triples of integers satisfying $a^2+b^2=c^2$ are named Pythagorean triples after him, as the theorem that the square of the hypothenuse of a right triangle is the sum of the squares of the other two sides.

[17] Niccolo Fontana TARTAGLIA, Italian mathematician, 1499–1557. He worked in Venezia (Venice), Italy.

[18] Girolamo CARDANO, Italian mathematician, 1501–1576. He worked in Milano (Milan), Pavia, and Roma (Rome), Italy. Cardano's formula is named after him, somewhat wrongly since he published something that TARTAGLIA had shown him, and the formula had actually been derived before, by DEL FERRO.

[19] Scipione DEL FERRO, Italian mathematician, 1465–1526. He worked in Bologna, Italy.

Solving a quadratic equation $x^2 + a\,x + b = 0$ was known to the Babylonians, when the *discriminant* $\Delta = a^2 - 4b$ is ≥ 0 (for $a, b \in \mathbb{R}$), so that there are real roots $x_\pm = \frac{-a\pm\sqrt{\Delta}}{2}$, but if the discriminant Δ is < 0, the equation has no roots, so that there is no reason to try to give a meaning to $\sqrt{\Delta}$.

The situation is different for a cubic equation $x^3+a\,x^2+b\,x+c = 0$, first reduced to solving $y^3+p\,x+q = 0$ (by choosing $y = x + \frac{a}{3}$), and then the idea is to use $(\alpha + \beta)^3 = \alpha^3 + \beta^3 + 3\alpha\,\beta\,(\alpha + \beta)$, so that $\alpha + \beta$ is a root if $3\alpha\,\beta = -p$ and $\alpha^3 + \beta^3 = -q$, i.e. α^3 and β^3 are the roots of $z^2 + q\,z - \frac{p^3}{27} = 0$; if the discriminant $\Delta = q^2 + \frac{4p^3}{27}$ is ≥ 0, there is only one root, given by $\sqrt[3]{\frac{q}{2} - \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}} + \sqrt[3]{\frac{q}{2} + \sqrt{\frac{q^2}{4} + \frac{p^3}{27}}}$, but if Δ is < 0 there are three real roots, and it was for resolving this paradox that BOMBELLI invented complex numbers.[20]

Solving a *quartic* equation $x^4 + a\,x^2 + b\,x + c = 0$ was done by FERRARI,[21] a student of CARDANO, who used the factorization $(x^2 + \alpha\,x + \beta)\,(x^2 - \alpha\,x + \gamma)$, and noticed that α^2 is the root of a cubic equation.[22]

The question was then of solving a *quintic* equation (i.e. one of degree 5) by radicals,[23] and it was only shown in the beginning of the 19th century that it is not always possible,[24] by ABEL,[25] who was actually filling a gap in an argument of RUFFINI;[26] GALOIS then found a way to explain which polynomial equations (of degree 5 or higher) are *solvable by radicals*;[27] a part of his argument is that there is no algebraic way to distinguish between i and $-i$ in the construction of complex numbers, i.e. there are two choices for the orientation of the *Argand plane* representing $\mathbb{C}$,[28] or more generally there are n choices for an nth root; since all the choices create permutations between the roots of the polynomial, he considered *groups of permutation* (i.e. arbitrary *finite groups* since any *group* of *order* n is isomorphic to a *subgroup* of the *symmetric group* S_n by *Cayley's theorem*)[29] and *automorphisms* of *fields*, since changing i into $-i$ defines an automorphism of $\mathbb{C}$, and a similar situation appears for the fields generated by the roots of a polynomial.

Geometric constructions with straightedge and compass

EUCLID initialized the question of geometric constructions with compass and straightedge (which has no marks on it, unlike a ruler),[30] and one can actually do these constructions with the compass alone, as observed by MASCHERONI,[31] but the argument had been printed in 1672 by MOHR.[32] EUCLID constructed

[20] Rafael BOMBELLI, Italian mathematician, 1526–1572. He worked in Roma (Rome), Italy.

[21] Lodovico FERRARI, Italian mathematician, 1522–1565. He worked in Milano (Milan), Italy.

[22] One has $\beta + \gamma - \alpha^2 = a$, $\alpha(\gamma - \beta) = b$, and $\beta\,\gamma = c$, so that $2\beta = a + \alpha^2 - \frac{b}{\alpha}$, $2\gamma = a + \alpha^2 + \frac{b}{\alpha}$, and $4c = (a + \alpha^2)^2 - \frac{b^2}{\alpha^2}$, hence $y = \alpha^2$ is a root of the equation $y\,(a + y)^2 - 4c\,y - b^2 = 0$.

[23] Solving by radicals means using nth roots for various values of n, and it can be considered a question of analysis when one deals with $\mathbb{R}$ or $\mathbb{C}$, and one way to approximate $\sqrt[n]{a}$ (and computers use a variant) is to iterate the function f defined by $f(x) = \frac{1}{n+1}\big(n\,x + \frac{a}{x^{n-1}}\big)$, because its only fixed point is $\sqrt[n]{a}$, and the convergence is quite fast, since $f'(\sqrt[n]{a}) = 0$.

[24] Notice the difficulty of imagining that a formula which one has sought for a few centuries does not exist, and then of imagining how one can *prove* that it does not exist! It goes further than saying that a few lines of attack on a problem have not worked. It is even more difficult to imagine that there are properties which are undecidable, i.e. they are neither true nor false.

[25] Niels Henrik ABEL, Norwegian mathematician, 1802–1829. The Abel Prize is named after him. Commutative groups are called Abelian.

[26] Paolo RUFFINI, Italian mathematician and physician, 1765–1822. He worked in Modena, Italy. His "proof" that some quintic equations cannot be solved by radicals contained a small gap, filled by ABEL.

[27] Évariste GALOIS, French mathematician, 1811–1832. Galois theory is named after him.

[28] Jean Robert ARGAND, Swiss mathematician, 1768–1822. He worked as an accountant in Paris, France.

[29] Arthur CAYLEY, English mathematician, 1821–1895. He worked in Cambridge, England, holding the Sadleirian chair of pure mathematics (1863–1895).

[30] EUCLID of Alexandria, Greek mathematician, about 325 BCE–265 BCE. It is not known where he was born, but he worked in Alexandria, Egypt, shortly after it was founded by Alexander the Great, in 331 BCE. The Euclidean division algorithm, and Euclidean rings are named after him.

[31] Lorenzo MASCHERONI, Italian mathematician, 1750–1800. He worked in Pavia, Italy.

[32] Georg MOHR, Danish mathematician, 1640–1697.

regular polygons with 3 sides (triangle), 4 sides (square), 5 sides (pentagon), or 15 sides (pentadecagon), and he certainly knew how to double the number of sides, since bisecting an angle is easily done. In the 16th century, VIÈTE rediscovered a result which AL BIRUNI had already obtained more than five centuries earlier,[33,34] that constructing a regular polygon with 9 sides (enneagon) is related to the solution of a third degree equation. One had to wait until GAUSS (when he was 19 years old, in 1796) for the first non-trivial construction:[35] a regular polygon with 17 sides (heptadecagon). GAUSS stated that the problem of trisecting an angle (i.e. dividing any angle into three equal angles) or of duplicating a cube (i.e. constructing $\sqrt[3]{2}$) cannot be done with straightedge and compass, but he gave no proof, and these statements were proved in 1837 by WANTZEL,[36] who also characterized the integers n for which one can construct a regular polygon with n sides: either $n = 2^j$ with $j \geq 2$ or $n = 2^k p_1 \ldots p_m$, where $k \geq 0$ and $p_1, \ldots, p_m$ are distinct *Fermat primes*,[37] i.e. of the form $F_n = 2^{2^n} + 1$,[38] not to be confused with the Fibonacci sequence.[39] FERMAT mistakenly stated that F_n is prime for every n, but EULER showed in 1732 that F_5 is divisible by 641,[40] and more generally that if F_n is not prime its factors have the form $k\,2^{n+1} + 1$;[41] no Fermat prime has been found yet with $n > 5$, so that the only known Fermat primes at the moment correspond to $n = 0, 1, 2, 3, 4$, i.e. 3, 5, 17, 257 and 65 537.

Learning how to draw a perpendicular to a given line, then parallel lines, one can construct points with coordinates in $\mathbb{Q}$ by *Thales's theorem*,[42] and the basic observation for showing that some constructions cannot be done with straightedge and compass is to notice that, if one starts with two points at distance 1 for example, the points of the plane which can be constructed by straightedge and compass have their coordinates in various *field extensions* of $\mathbb{Q}$, whose *degree over* (this involves the notion of *dimension* in *vector spaces*) $\mathbb{Q}$ are powers of 2.[43] That the duplication of the cube is impossible with straightedge and compass follows from the fact that $\sqrt[3]{2}$ belongs to $\mathbb{Q}[\sqrt[3]{2}]$ which is an extension of $\mathbb{Q}$ of order 3, and can then only be included in extensions whose order is a multiple of 3; that the trisection of some angles is impossible is similar, after noticing that $\cos 20°$ is a root of an *irreducible polynomial* of degree 3.

Algebra versus analysis

Although reals had been used for a long time, $\mathbb{R}$ was not correctly defined until CANTOR and DEDEKIND in the second part of the 19th century,[44,45] but the construction of $\mathbb{R}$ from $\mathbb{Q}$ belongs to *analysis*, and not to

[33] François VIÈTE, French mathematician, 1540–1603.

[34] Abu Ar-Rayhan Muhammad ibn Ahmad AL BIRUNI al-Khwarizmi, Uzbek-born mathematician, 973–1048.

[35] Johann Carl Friedrich GAUSS, German mathematician, 1777–1855. He worked at Georg-August-Universität, Göttingen, Germany. Gaussian functions, and many theorems are named after him.

[36] Pierre-Laurent WANTZEL, French mathematician, 1814–1848.

[37] Pierre DE FERMAT, French mathematician, 1601–1665. He worked (as a lawyer and government official) in Toulouse, France. There are a few "theorems" attributed to him, but since he rarely explained his proofs in his letters, and he also made some mistakes, one should probably call them conjectures: some famous mathematicians (like EULER) proved and then improved most of what he had said in letters.

[38] An integer of the form $2^m + 1$ cannot be prime if m is not a power of 2, because if $m = a\,b$ with a odd, then $2^m + 1 = x^a + 1$ with $x = 2^b$, which can be written $(1 + x)\,(1 - x + \ldots + (-1)^{a-1} x^{a-1})$.

[39] Fibonacci (Leonardo PISANO), Italian mathematician, 1170–1250. He worked in Pisa, Italy.

[40] Leonhard EULER, Swiss-born mathematician, 1707–1783. He worked in St Petersburg, Russia, in Berlin, Germany, and then again in St Petersburg. A few of the subjects to which his name is attached are the Euler equation for inviscid fluids, the Euler φ function, the Euler Γ function, and the Euler constant.

[41] If p is a prime dividing F_n, then p is odd and if a is a *primitive root* modulo p (i.e. the smallest $b > 0$ with $a^b = 1 \pmod{p}$ is $b = p - 1$), then $2 = a^c \pmod{p-1}$ gives $a^{2^n c} = -1 \pmod{p}$, so that $2^n c = \frac{p-1}{2} \pmod{p-1}$, i.e. $c\,2^{n+1} = (2d + 1)\,(p - 1)$, hence $2d + 1$ divides c, and $p = k\,2^{n+1} + 1$.

[42] THALES of Miletus, Greek mathematician, 624–547 BCE.

[43] The points constructed after n steps are in an *intermediate field* K_n between $\mathbb{Q}$ and $\mathbb{R}$, with $K_0 = \mathbb{Q}$, and either $K_{n+1} = K_n$ or K_{n+1} is a field extension of K_n of order 2.

[44] Georg Ferdinand Ludwig Philipp CANTOR, Russian-born German mathematician, 1845–1918. He worked in Halle, Germany. The Cantor set is named after him.

[45] Julius Wihelm Richard DEDEKIND, German mathematician, 1831–1916. He worked in Brunswick,

algebra, because *only finite sums are considered in algebra*: the formula $1 + \frac{1}{10} + \ldots + \frac{1}{10^n} + \ldots = \frac{10}{9}$ belongs to analysis, and it created a lot of trouble to ZENO and his followers,[46] concerning the paradox of ACHILLES and the tortoise,[47] because they could not understand that summing an infinite number of positive rationals does not always give $+\infty$. However, for a prime p, the formula $1 + p + \ldots + p^n + \ldots = \frac{1}{1-p}$ has a meaning in $\mathbb{Q}_p$, the field of *p-adic numbers*, constructed by HENSEL as the *completion* of $\mathbb{Q}$ for a different *metric* than the usual one (which gives $\mathbb{R}$),[48] but for any *ring* R, the formula $1 + x + \ldots + x^n + \ldots = (1 - x)^{-1}$ is true in $R[[x]]$,[49] the ring of *formal power series with coefficients in* R, and this is pure algebra!

The place of algebra inside mathematics

The qualifier algebraic appears in the names of some "branches" of mathematics, like *algebraic geometry*, which one should compare to *analytic geometry* and *differential geometry*, and the first considers sets defined by polynomial equations, the second enlarges the class of functions used and considers *analytic functions*, while the third enlarges it more and considers *differentiable* functions.[50] Similarly, *algebraic topology* should be compared to *general topology* (sometimes called *point set topology*) and *differential topology*.[51] Similarly, *algebraic number theory* should be compared to *analytic number theory*.

In the early 1970s, I had the occasion to have lunch (in the cafeteria of École Polytechnique in Paris) with Charles PISOT,[52] who was a good specialist of analytic number theory, and he mentioned that, like many other specialists of number theory, he regularly received some supposed proof of FLT ("Fermat's last theorem", which then was a conjecture), and he did not want to lose time reading the arguments until he found a flaw, and he did not want either to reject them by saying to their authors that since they were not professional mathematicians they could not prove such a difficult conjecture.[53] Fortunately, Marc KRASNER had made an interesting observation,[54] which permitted to rule out most of the tentative proofs: he had

---

Germany.

[46] ZENO of Elea, Greek mathematician, 490BCE–425BCE. He worked in Elea, a Greek colony in Lucania, in southern Italy.

[47] ACHILLES, Greek mythological hero, a central character of the Trojan War.

[48] Kurt Wilhelm Sebastian HENSEL, German mathematician, 1861–1941. He worked in Marburg, Germany. Hensel's lemma is named after him.

[49] One should pay attention to notation: if R is a ring, then $R[x]$ is the *ring of polynomials with coefficients in* R, i.e. the smallest ring containing R and x; if R is an *integral domain*, then $R(x)$ is the smallest field containing R and x, and it is the *ring of fractions* of $R[x]$ (which is itself an integral domain). If F is a field, $F((x))$ denotes the *field of formal Laurent series*, which is the field of fractions of $F[[x]]$.

[50] One reason to make a distinction on the differentiability of the functions one uses is related to a question of localization: a non-zero function of class C^∞ in an open set of $\mathbb{R}^N$ can nevertheless be identically 0 in a small ball, but that is not true for analytic functions. Among analytic functions, the entire functions can be extended to the whole $\mathbb{C}^N$, and polynomials appear as those which are *regular at* ∞, i.e. in the *Aleksandrov one-point compactification* of $\mathbb{C}^N$).

[51] I think that algebraic geometry started for answering questions of POINCARÉ, which had to do with parametrizations in questions of *classical mechanics* (i.e. the 18th century point of view which uses *ordinary differential equations*, by opposition to *continuum mechanics*, the 19th century point of view which uses *partial differential equations*) when a system of rigid bodies contains or not some gyroscopes; a second period started with the ideas about *sheaf theory* of Jean LERAY, who told me that as a consequence of his election at Collège de France instead of WEIL, the whole Bourbaki group started acting aggressively against him, and his ideas were then plagiarized by Henri CARTAN; a third period started with the ideas of Alexandre GROTHENDIECK.

[52] Charles PISOT, French mathematician, 1910–1984. He worked in Paris, France. Pisot numbers are named after him.

[53] My former colleague Yves MEYER, who is a good specialist of harmonic analysis, told me that there was a conjecture whose proof had escaped the best specialists in the field, and someone discovered an elementary proof, but then he never proved anything important in his life, because he decided not to learn much, believing (probably wrongly) that every conjecture has a simple proof!

[54] Marc KRASNER, French mathematician, 1912–1985. He worked in Paris, France.

found a ring of complex *algebraic numbers* having the same divisibility properties than $\mathbb{Z}$ (i.e. it is a UFD = *unique factorization domain*) but "Fermat's last theorem" does not hold.[55] Then, for rejecting a tentative proof he asked the author "do you only use divisibility properties?" and the answer was always "yes", of course, so that he said "then your argument is flawed", and the author asked "why?", and he mentioned Krasner's counter-example, and invariably the various authors told him "but I do not use complex numbers", so that he could deduce that these authors did not understand elementary logic!

In some way, Krasner's counter-example suggests that any proof of FLT "uses analysis", and I have been told that WILES used parametrization of *elliptic curves* by *modular functions* in his "proof",[56] completed with the help of R. TAYLOR.[57]

I find important to avoid believing that one branch of mathematics is superior to another, since it is akin to having a racist point of view, i.e. feeling superior to others for one silly reason or another, and one should learn about the damages created by such points of view in the past in order to avoid similar mistakes nowadays.

I always mention the silly classification of (Auguste) COMTE concerning sciences:[58,59] he had put *mathematics* first, then *astronomy*, then *physics*, then *chemistry*, and then *biology*, and he did not rank "social sciences", although he seems to have been the inventor of sociology. COMTE was good enough in mathematics to have studied at École Polytechnique in Paris,[60] although he only followed classes during one year,[61] and he seems to have also studied in medical school (in Montpellier, France) for a short time. The presence of astronomy (which is not considered an independent science nowadays) is probably responsible for what I call a Comte complex which some French physicists have:[62] maybe they chose to study physics because they did not feel good enough to study mathematics, and they then tried to go to astrophysics, the modern name for astronomy, and they usually end up not being mathematicians,[63] and not really good physicists

---

[55] So that there are solutions of $x^n + y^n = z^n$ for some $n \geq 3$ and non-zero elements x, y, z of the ring.

[56] Andrew John WILES, English-born mathematician, born in 1955. He works at Princeton University, Princeton, NJ. He received the Wolf Prize for 1995/96 "for spectacular contributions to number theory and related fields, major advances on fundamental conjectures, and for settling Fermats last theorem", jointly with Robert P. LANGLANDS.

[57] Richard Lawrence TAYLOR, British-born mathematician, born in 1962. He held that Savilian chair of geometry at Oxford, England (1995–1996), and he works at Harvard University, Cambridge, MA.

[58] Isidore Auguste Marie François Xavier COMTE, French philosopher, 1798–1857. He worked in Paris, France.

[59] I find important not to use the sentence "mathematics and science", which tends to make people believe that mathematics is not part of the sciences, and maybe this results from a sense of superiority that some mathematicians may have over physicists, chemists, and biologists.

[60] In my days (1965–1967) one entered École Polytechnique by a competition for 300 places for French men, and women were only allowed to compete in the early 1970s (but since the school has a military status, women had to enroll in the army if they succeeded), and the status has evolved since. In the 19th century, the number of places must have been much smaller, but since COMTE ranked 4th, he must have been gifted for mathematics.

[61] For political reasons, the whole body of students was dismissed in 1816. The school had been created in 1794 in the new French Republic, and Napoléon gave it a military status in 1804. Students entered École Polytechnique because of their scientific interests, and they usually preferred republican values, so that they did not like the emperor so much, but after Napoléon abdicated in 1814 (and was exiled to Isola d'Elba) the monarchy was reinstalled and they hated the king much more, hence when Napoléon made his return (for 100 days after escaping from Isola d'Elba, until he was defeated at Waterloo) the students were favorable to Napoléon, which explains why they were later punished.

[62] I first understood this effect after the talk of a French "physicist" in the late 1970s, because he had been unable to describe what was the game he and other physicists were playing and why they were playing it, but he repeated a few times that he had read some books by Jean DIEUDONNÉ, as if he wanted to convince that he was good at mathematics! He gave an explicit formula giving solutions of $u_{tt} - u_{xx} = e^u$, mentioning that he did not know if all solutions were of this form, and I checked that it was easy to prove.

[63] In particular, because they do not react to pseudo-logic of the form "since the game A implies the result

(so that they can hardly talk with an experimental physicist).

Comte's classification is silly because one needs different abilities for being a good mathematician, a good physicist, a good chemist, or a good biologist, and one should not despise people who master an art that one does not know.

The same is true for mathematics, and algebra, analysis, or geometry require different intuitions, so that one rarely finds mathematicians who excel in all these branches. Actually, the multiplication of sub-branches in mathematics is related to an over-specialization, maybe because the level decreases, or maybe because one does not know how to train people to be good at simplifying proofs and finding unifying concepts, so that the job of the next generation of students will become more easy, hence they will be better prepared for going further on the quest for new knowledge. As a consequence of the failure to simplify, there are too many results which have been proved, with not so many relations between them, and anyone gets quickly saturated, so that it is crucial to discover *structures*,[64] and here it will mean *algebraic structures*: the first ones are groups, rings, fields, and vector spaces (or more generally modules), and it is important to know their basic properties, but it is also useful to know why the notion were introduced, and to know old and new problems, which may force to discover new structures, or at least explain in a better way how to use some of the structures which have already been found.

Some of these problems may come from outside mathematics, so that it is useful to be aware of domains of applications: when I was professor at Université de Paris Sud, in Orsay, France, I once asked a question concerning *Galois theory* and *coding theory* during a faculty meeting, but I was mainly addressing my colleague John Coates,[65] by saying "I have heard that Galois theory has applications to coding theory; why is it that you do not want to tell it to the students?". No one had answered, but a few years later a friend mentioned that some French mathematicians were saying that Galois theory is very important because it has applications to coding theory, and it made me think that those who were using this kind of argument had probably been strong advocates of never mentioning applications a few years before that, and I also wondered how much of Galois theory is really used in coding theory, and I planned to learn more on that question, but my guess was that besides using finite fields, there was probably little of Galois theory necessary for coding theory. I never read much, but sometimes a book comes to my attention, and since I found a chapter on coding theory in a book that I received from a publisher (because I have been teaching algebra for a few years), I started looking at it at the end of the 2010 Spring semester, but I stopped short of reading about *BCH codes*, in part because I had to teach a course in the Fall of 2010 on elliptic curves, a subject on which I knew very little; it was then just before the last lectures of the 2011 Spring semester that I read the part on BCH codes. As we shall see later, very little of Galois theory is needed in coding theory, but since Galois theory contains some beautiful insights about algebra, it is worth learning it, and it may help understand questions in other areas of mathematics, or even some problems related to applications, may be in area which one has not thought about yet.

One should remember that there is no such things as "pure mathematics" on one side and "applied mathematics" on the other side, but mathematicians who are interested in questions from outside mathematics will use all the power of the mathematical techniques which they already know for solving the problems which interest them, even if they were only used before on problems internal to mathematics, and it does not make these techniques "impure" in this way! The problem is usually that a mathematical technique may already exist which would be extremely useful in some applications, but that it is only known by people who have no interest in applications, and mathematicians specialists of one branch who need some understanding about another branch of mathematics are almost in the same situation as Feynman,[66] who had said that

B, which looks like what is observed, "then" nature plays game A", which non-mathematicians often use, while students in mathematics fail their exams if they confuse 'A implies B' with 'B implies A'.

[64] I had asked Laurent Schwartz if Bourbaki had played a role in advocating the importance of structures in mathematics, and he answered yes, but since he had been a member of Bourbaki, this point of view may be biased.

[65] John Henry Coates, Australian-born mathematician, born in 1945. He worked at Harvard University, Cambridge, MA, at Stanford University, Stanford, CA, at ANU (Australian National University), Canberra, Australia, at Université Paris Sud in Orsay, France, where he was my colleague from 1978 to 1982, and since 1986 he holds the Sadleirian chair of pure mathematics in Cambridge, England.

[66] Richard Phillips Feynman, American physicist, 1918–1988. He received the Nobel Prize in Physics

it was more efficient for him to develop the mathematics which he needed, because it would be too long to look for a mathematician who would understand what he was trying to do, and who would also know if that had already been done!

Learning a new piece of mathematics is like visiting a new country, and it is more easy with a good guide, but if the country is wide enough two guides may choose to show different things, so that even after visiting one place it is useful to visit it again in order to appreciate in a better way some things which had not been clear enough on a preceding visit!

Additional footnotes: I have the habit of giving in footnotes biographical information on people alluded to in the text, and I use their first name for those whom I have met. One reason is to show that the creation of knowledge is international, in particular in sciences, and to mention where and when some new ideas appeared. When new names appear in the footnotes, I put the information about them at the end, in additional footnotes, and since there may be new names appearing in such additional footnotes, I continue until exhaustion (and I put these additional footnotes in alphabetic order): my experience is that the algorithm stops, but the first few lectures have a lot more footnotes than the following ones, since I do not repeat the biographical information on someone who has already been mentioned. Some of the names may have become so familiar that one may forget that they refer to real persons, like for CMU, named after CARNEGIE,[67] and A. MELLON.[68]

'ABD AL-MUTTALIB,[69] ALEKSANDROV,[70] D'ALEMBERT,[71] Alexander,[72] ARISTOTLE,[73] BECQUEREL,[74] BOLZANO,[75] Bourbaki,[76] BUNYAKOVSKY,[77] .../...

in 1965, jointly with Sin-Itiro TOMONAGA and Julian SCHWINGER, for their fundamental work in quantum electrodynamics, with deep-ploughing consequences for the physics of elementary particles. He worked at Cornell University, Ithaca, NY, and at Caltech (California Institute of Technology), Pasadena, CA.

[67] Andrew CARNEGIE, Scottish-born businessman and philanthropist, 1835–1919. Besides endowing the school which became Carnegie Tech (Carnegie Institute of Technology), and CMU (Carnegie Mellon University) when it merged in 1967 with the Mellon Institute of Industrial Research, he funded about three thousand public libraries, and those in United States are named Carnegie libraries.

[68] Andrew William MELLON, American financier and philanthropist, 1855–1937. He funded the Mellon Institute of Industrial Research in Pittsburgh, PA, which merged in 1967 with Carnegie Tech (Carnegie Institute of Technology) to form CMU (Carnegie Mellon University).

[69] 'ABD AL-MUTTALIB, grandfather of MUHAMMAD, and father of AL 'ABBAS (ibn 'abd al-Muttalib), ancestor of the Abbasid Caliphs (750–1258 in Baghdad, 1261–1517 in Cairo).

[70] Pavel Sergeevich ALEKSANDROV, Russian mathematician, 1896–1982. He worked in Smolensk, and in Moscow, Russia.

[71] Jean LE ROND, known as D'ALEMBERT, French mathematician, 1717–1783. He worked in Paris, France.

[72] Alexandros Philippou Makedonon, 356–323 BCE, was king of Macedon as Alexander III, and is referred to as Alexander the Great, in relation with the large empire that he conquered.

[73] ARISTOTLE, Greek philosopher, 384 BCE–322 BCE.

[74] Antoine Henri BECQUEREL, French physicist, 1852–1908. He received the Nobel Prize in Physics in 1903, in recognition of the extraordinary services he has rendered by his discovery of spontaneous radioactivity, jointly with Pierre CURIE and Marie SKŁODOWSKA-CURIE. He worked in Paris, France.

[75] Bernhard Placidus Johann Nepomuk BOLZANO, Czech mathematician and philosopher, 1781–1848. He worked in Prague (then in Austria, now capital of the Czech Republic). He introduced the concept of "Cauchy sequences" a few years before CAUCHY did. The Bolzano–Weierstrass theorem is partly named after him.

[76] Nicolas Bourbaki is the pseudonym of a group of mathematicians, mostly French.

[77] Viktor Yakovlevich BUNYAKOVSKY, Ukrainian-born mathematician, 1804–1889. He worked in St Petersburg, Russia. He studied with CAUCHY in Paris (1825), and he proved the "Cauchy–Schwarz" inequality in 1859, 25 years before SCHWARZ.

CASORATI,[78] É. CARTAN,[79] Henri CARTAN,[80] CAUCHY,[81] Charles X,[82] CORNELL,[83] CRAFOORD,[84] CURIE P. & M.,[85] Pierre DELIGNE,[86] DIDEROT,[87] Jean DIEUDONNÉ,[88] FIELDS,[89] .../...

---

[78] Felice CASORATI, Italian mathematician, 1835–1890. He worked in Pavia and in Milano (Milan), Italy. The Casorati–Weierstrass theorem (that in any neighbourhood of an essential singularity of a function of one complex variable it comes arbitrarily close to any given value) is partly named after him, but he included it in his 1868 treatise on complex numbers, while WEIERSTRASS only proved it in an article in 1876.

[79] Élie Joseph CARTAN, French mathematician, 1869–1951. He worked in Montpellier, in Lyon, in Nancy, and in Paris, France.

[80] Henri Paul CARTAN, French mathematician, 1904–2008. He received the Wolf Prize in 1980 for pioneering work in algebraic topology, complex variables, homological algebra and inspired leadership of a generation of mathematicians, jointly with Andrei N. KOLMOGOROV. He worked in Lille, in Strasbourg, in Paris, and at Université Paris Sud, Orsay, France, retiring in 1975 just before I was hired there. Theorems attributed to CARTAN are often the work of his father Élie CARTAN.

[81] Augustin Louis CAUCHY, French mathematician, 1789–1857. He was made baron by Charles X. He worked in Paris, France, went in exile after the 1830 revolution and worked in Torino (Turin), Italy, returned from exile after the 1848 revolution, and worked in Paris again. The Cauchy stress tensor in elasticity is named after him. Cauchy sequences are named after him, but were introduced before by BOLZANO. The Cauchy–Schwarz inequality is partly named after him, but was proved before by BUNYAKOVSKY.

[82] Charles-Philippe de France, 1757–1836, comte d'Artois, duc d'Angoulême, pair de France, was king of France from 1824 to 1830 under the name Charles X.

[83] Ezra CORNELL, American philanthropist, 1807–1874. Cornell University, Ithaca, NY, is named after him.

[84] Holger CRAFOORD, Swedish industrialist and philanthropist, 1908–1982. He invented the artificial kidney, and he and his wife (Anna-Greta CRAFOORD, 1914–1994) established the Crafoord Prize in 1980 by a donation to the royal Swedish academy of sciences, to reward and promote basic research in scientific disciplines that fall outside the categories of the Nobel Prize, including mathematics, geoscience, bioscience (particularly in relation to ecology and evolution), and astronomy.

[85] Pierre CURIE, French physicist, 1859–1906, and his wife Marie SKŁODOWSKA-CURIE, Polish-born physicist, 1867–1934, received the Nobel Prize in Physics in 1903, in recognition of the extraordinary services they have rendered by their joint researches on the radiation phenomena discovered by Professor Henri BECQUEREL, jointly with Henri BECQUEREL; Marie SKŁODOWSKA-CURIE also received the Nobel Prize in Chemistry in 1911, in recognition of her services to the advancement of chemistry by the discovery of the elements radium and polonium, by the isolation of radium and the study of the nature and compounds of this remarkable element. They worked in Paris, France. Université Paris VI, Paris, is named after them, UPMC (Université Pierre et Marie Curie).

[86] Pierre DELIGNE, Belgian-born mathematician, born in 1944. He worked at IHES (Institut des Hautes Études Scientifiques) in Bures sur Yvette, France, and at IAS (Institut for Advanced Study), Princeton, NJ. He received the Fields Medal in 1978 for his work in algebraic geometry. He received the Crafoord Prize in 1988, jointly with Alexandre GROTHENDIECK, who declined it.

[87] Denis DIDEROT, French philosopher and writer, 1713–1784. He worked in Paris, France, and he was co-editor of the Encyclopédie with D'ALEMBERT. Université Paris 7, Paris, France, is named after him.

[88] Jean Alexandre Eugène DIEUDONNÉ, French mathematician, 1906–1992. He worked in Rennes, in Nancy, France, in São Paulo, Brazil, at University of Michigan, Ann Arbor, MI, at Northwestern University, Evanston, IL, at IHES (Institut des Hautes Études Scientifiques), Bures sur Yvette, France, where he dedicated his enormous energy helping Alexandre GROTHENDIECK write his ideas, expressed in SGAD (Séminaire de Géométrie Algébrique et Différentielle), and in Nice, France. Université de Nice Sophia-Antipolis has its research unit in mathematics named after him, the Laboratoire Jean-Alexandre Dieudonné.

[89] John Charles FIELDS, Canadian mathematician, 1863–1932. He worked in Meadville, PA, and in Toronto, Ontario. The Fields Medal is named after him.

George II,[90] Alexandre GROTHENDIECK,[91] HARVARD,[92] KOLMOGOROV,[93] LANGLANDS,[94] LAURENT,[94] Jean LERAY,[95] Yves MEYER,[96] MUHAMMAD,[97] NOBEL,[98] POINCARÉ,[99] PURDUE,[100] SADLEIR,[101] SAVILE,[102] Laurent SCHWARTZ,[1037] SCHWARZ,[104] .../...

---

[90] Georg Augustus, 1683–1760. Duke of Brunswick-Lüneburg (Hanover), he became king of Great Britain and Ireland in 1727, under the name of George II. Georg-August-Universität in Göttingen, Germany, is named after him.

[91] Alexander GROTHENDIECK, German-born mathematician, born in 1928. He received the Fields Medal in 1966 for his work in algebraic geometry. He received the Crafoord Prize in 1988, jointly with Pierre DELIGNE, but he declined it. He worked at CNRS (Centre National de la Recherche Scientifique), at IHES (Institut des Hautes Études Scientifiques) in Bures sur Yvette, and in Montpellier, France.

[92] John HARVARD, English clergyman, 1607–1638. Harvard University, Cambridge, MA, is named after him.

[93] Andrey Nikolayevich KOLMOGOROV, Russian mathematician, 1903–1987. He received the Wolf Prize in 1980, for deep and original discoveries in Fourier analysis, probability theory, ergodic theory and dynamical systems, jointly with Henri CARTAN. He worked at Moscow State University and at the Steklov Institute, Moscow, Russia.

[94] Robert Phelan LANGLANDS, Canadian-born mathematician, born in 1936. He worked at Princeton University, Princeton, NJ, as Yale University, New Haven, CT, and at IAS (Institute for Advanced Study), Princeton, NJ. He received the Wolf Prize for 1995/96 "for his path-blazing work and extraordinary insight in the fields of number theory, automorphic forms and group representation", jointly with Andrew J. WILES.

[94] Pierre Alphonse LAURENT, French mathematician, 1813–1854. Laurent series are named after him, although WEIERSTRASS had introduced the notion in 1841, two years before him.

[95] Jean LERAY, French mathematician, 1906–1998. He received the Wolf Prize in 1979, for pioneering work on the development and application of topological methods to the study of differential equations, jointly with André WEIL. He worked in Nancy, France, in a prisoner of war camp in Austria (1940–1945), at IAS (Institute for Advanced Study), Princeton, NJ, and he held a chair at Collège de France (théorie des équations différentielles et fonctionnelles, 1947–1978) in Paris, France.

[96] Yves François MEYER, French mathematician, born in 1939. He worked at Université Paris Sud XI, Orsay (where he was my colleague from 1975 to 1979), at École Polytechnique, Palaiseau, at Université Paris IX-Dauphine, Paris, and at ENS-Cachan (Ecole Normale Supérieure de Cachan), Cachan, France.

[97] MUHAMMAD ibn 'Abdullah, Arab mystic and legislator, 570–632. He was the prophet of Islam. He lived in Mecca, and in Medina, now in Saudi Arabia.

[98] Alfred Bernhard NOBEL, Swedish industrialist and philanthropist, 1833–1896. He created a fund to be used as awards for people whose work most benefited humanity.

[99] Jules Henri POINCARÉ, French mathematician, 1854–1912. He worked in Paris, France. There is now an Institut Henri Poincaré (IHP), dedicated to mathematics and theoretical physics, part of UPMC (Université Pierre et Marie Curie), Paris.

[100] John PURDUE, American industrialist, 1802–1876. Purdue University, West Lafayette, IN, is named after him.

[101] Lady Mary SADLEIR (born LORYMER), –1706. In 1701, she funded lectures in algebra at Cambridge, England, which started in 1710; it transformed into a professorship in 1860.

[102] Sir Henry SAVILE, English mathematician, 1549–1622. In 1619, he founded professorships of geometry and astronomy at Oxford, England.

[1037] Laurent SCHWARTZ, French mathematician, 1915–2002. He received the Fields Medal in 1950 for his work in functional analysis. He worked in Nancy, in Paris, France, at École Polytechnique, which was first in Paris (when he was my teacher in 1965–1966), and then in Palaiseau, and at Université Paris 7 (Denis Diderot), Paris.

[104] Hermann Amandus SCHWARZ, German mathematician, 1843–1921. He worked at ETH (Eidgenössische Technische Hochschule), Zürich, Switzerland, and in Berlin, Germany. The Cauchy–Schwarz inequality is partly named after him, but was proved before by BUNYAKOVSKY.

Schwinger,[105] Stanford,[106] Steklov,[107] Tomonaga,[108] Umayya,[109] 'Uthman.[110] Weierstrass,[111] Weil,[112] Wolf,[113] Yale.[114]

---

[105] Julian Seymour Schwinger, American physicist, 1918–1994. He received the Nobel Prize in Physics in 1965, jointly with Sin-Itiro Tomonaga and Richard Phillips Feynman, for their fundamental work in quantum electrodynamics, with deep-ploughing consequences for the physics of elementary particles. He worked at UCB (University of California at Berkeley), Berkeley, CA, at Purdue University, West Lafayette, IN, and at Harvard University, Cambridge, MA.

[106] Leland Stanford, American businessman, 1824–1893. Stanford University, as the city of Stanford where it is located, are named after him.

[107] Vladimir Andreevich Steklov, Russian mathematician, 1864–1926. He worked in Kharkov, and in St Petersburg (then Petrograd, USSR), Russia. The Steklov Institute of Mathematics, Moscow, Russia, is named after him.

[108] Sin-Itiro Tomonaga, Japanese-born physicist, 1906–1979. He received the Nobel Prize in Physics in 1965, jointly with Julian Schwinger and Richard Feynman, for their fundamental work in quantum electrodynamics, with deep-ploughing consequences for the physics of elementary particles. He worked in Tokyo, Japan, in Leipzig, Germany, in Tsukuba, Japan, and at IAS (Institute for Advanced Study), Princeton, NJ.

[109] Umayya ibn 'abd Shams, Arab leader. He was the ancestor of the Umayyad Caliphs, who ruled from 661 to 744 from Damascus, Syria, from 744 to 750 from Harran (now in Turkey), and then went in exile (after being overthrown by the Abbassids) and ruled from Cordoba, Spain, as Emirs from 756 to 929, and as Caliphs from 929 to 1031. He was the grandfather of the (third) Caliph 'Uthman ibn 'Affan, and he was a cousin of 'abd al-Muttalib, grandfather of Muhammad.

[110] 'Uthman ibn 'Affan, Arab leader, 579–656. He became the third Caliph in 644, ruling from Medina, Arabia, until he was assassinated in 656. It was him who created the official version of the Quran, charging a committee to only accept a saying of Muhammad if two persons had heard him say it.

[111] Karl Theodor Wilhelm Weierstrass, German mathematician, 1815–1897. He first taught in high schools in Münster, in Braunsberg, Germany, and then he worked in Berlin, Germany. The Bolzano–Weierstrass theorem is partly named after him. The Weierstrass theorem of approximation by polynomials is named after him. The Casorati–Weierstrass theorem (that in any neighbourhood of an essential singularity of a function of one complex variable it comes arbitrarily close to any given value) is partly named after him, but he published it in 1876, and Casorati had included it in his 1868 treatise on complex numbers.

[112] André Weil, French-born mathematician, 1906–1998. He received the Wolf Prize in 1979, for his inspired introduction of algebro-geometry methods to the theory of numbers, jointly with Jean Leray. He worked in Aligarh, India, in Haverford, PA, in Swarthmore, PA, in São Paulo, Brazil, in Chicago, IL, and at IAS (Institute for Advanced Study), Princeton, NJ.

[113] Ricardo Wolf, German-born inventor, diplomat and philanthropist, 1887–1981. He emigrated to Cuba before World War I; from 1961 to 1973 he was Cuban Ambassador to Israel, where he stayed afterwards. The Wolf Foundation was established in 1976 with his wife, Francisca Subirana-Wolf, 1900–1981, "to promote science and art for the benefit of mankind".

[114] Elihu Yale, American-born English philanthropist, Governor of Fort St George, Madras, India, 1649–1721. Yale University, New Haven, CT, is named after him.