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 $n = 2^k p_1 \dots p_m$, where $k \geq 0$ and $p_1, \dots, p_m$ 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 $(1 + x)\,(1 - x + \dots + (-1)^{a-1} x^{a-1})$.

[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.

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

2- Wednesday August 31, 2011.

Paradoxes

Before 1905, when RUSSELL found a *paradox* with the "set of all sets",[1] mathematicians used the term *set* without having defined it, and the paradox was resolved by finding a reasonable definition of the properties which characterize sets, and RUSSELL's idea became a proof that the collection of all sets is not itself a set.

More than fourty years ago, I read an interesting explanation, giving the essence of Russell's paradox: one defines a book as something published, i.e. having an ISBN number (International Standard Book Number),[2] and a catalog as any book just containing a list of books, so that a catalog of catalog is then such a book containing only the ISBN numbers of catalogs; among such catalogs of catalogs, there are those who list their own ISBN number and those who do not list their own ISBN number. One can make the complete list $\mathcal{L}$ of all catalogs of catalogs which do not list their own ISBN number and have no other book in the list, but it is a manuscript and not a book! If one publishes $\mathcal{L}$ into a book $\mathcal{B}$ (i.e. by asking for an ISBN number, and putting it on the cover of the list), then $\mathcal{B}$ will be incomplete, because it should contain the reference to $\mathcal{B}$, since it is a catalog of catalogs which does not list itself; however, if one adds to $\mathcal{L}$ the ISBN number of the book which one is going to publish (while putting it also on the cover of the list), one obtains a book $\mathcal{B}'$ which is not what one wants, since it lists its own reference and it should not: therefore the answer is a manuscript but not a book.

Ancient Greeks discussed of a fake paradox, of a Cretan saying that 'all Cretans are liers': if one assumes that a lier is someone who never says the truth, then it means that there is a Cretan who is truthful, and that the one who speaks then is a lier.[3]

A theory is *consistent* if there is no proposition P such that P and its negation can be proved true by using the axioms of the theory.[4] One should notice that it is still not known if ZF (Zermelo–Fraenkel set theory),[5,6] the standard foundation of modern mathematics, is consistent.[7]

---

[1] Bertrand Arthur William, third earl RUSSELL, Welsh mathematician, 1872–1970. He received the Nobel Prize in Literature in 1950, in recognition of his varied and significant writings in which he champions humanitarian ideals and freedom of thought. He worked in Cambridge, England.

[2] The former *ISBN code* was a $[10, 9]$-code over F_{11} ($\simeq \mathbb{Z}_{11}$) and the verification of the code $c_1c_2 \cdots c_{10}$ is that one must have $c_1 + 2c_2 + 3c_3 + \ldots + 10c_{10} = 0 \pmod{11}$; the first part of an ISBN codeword was the *group identifier*, which identified a country or a language area, the second part was the *publisher identifier*, which identified a specific publisher in the group, the third part was the *title identifier*, which identified a specific publication of the publisher; the length of the three parts varied, but the total length was 9, and the *check-digit* x_{10} was written X if it was 10. The revised ISBN code uses a 13-digit number, and the verification of the code $c_1c_2 \cdots c_{13}$ is that one must have $c_1 + 3c_2 + c_3 + 3c_4 + \ldots + c_{11} + 3c_{12} + c_{13} = 0 \pmod{10}$. The ISBN numbers of my first three books, are 978-3-540-35743-8, 978-3-540-71482-8, and 978-3-540-77561-4, so that 978-3-540 seems to identify Springer (Berlin Heidelberg New York), but the ISBN number of my fourth book published by the same publisher is 978-3-642-05194-4.

[3] Ancient Greeks made the mistake in negating the proposition as 'all Cretans are truthful' instead of the correct 'there exists a Cretan who is truthful'; unfortunately, many non-mathematicians still make such silly confusions nowadays.

[4] In such a case, all the propositions in this theory are both true and false, so that such a theory is useless.

[5] Ernst Friedrich Ferdinand ZERMELO, German mathematician, 1871–1953. He worked at Georg-August-Universität, Göttingen, Germany, in Zürich, Switzerland, and at Freiburg im Breisgau, Germany. Zermelo's theorem (conjectured by CANTOR), that every set can be well-ordered, is named after him. The Zermelo–Fraenkel set theory is partly named after him.

[6] Adolf Abraham Halevi FRAENKEL, German-born mathematician, 1891–1965. He worked in Marburg, Germany, and at the Hebrew University in Jerusalem (Israel). The Zermelo–Fraenkel set theory is partly named after him.

[7] ZFC denotes Zermelo–Fraenkel set theory with the axiom of choice.

It was not so easy to imagine that there could exist a consistent theory $\mathcal{T}$ with a proposition P which cannot be proved to be true using only the axioms of $\mathcal{T}$, but the negation of P cannot be proved to be true either using only the axioms of $\mathcal{T}$, and such a proposition is called *undecidable*: in this case one may create two consistent theories, $\mathcal{T}_1$ obtained by adding to the axioms of $\mathcal{T}$ that P is true, and $\mathcal{T}_2$ obtained by adding to the axioms of $\mathcal{T}$ that P is false. GÖDEL had the idea that some paradoxical sentences could be coded into mathematical propositions,[8] and he was able to do it using the integers $\mathbb{N}$, so that his theorem is that in any consistent theory $\mathcal{T}$ which contains $\mathbb{N}$, there is an undecidable proposition.

When HILBERT made a famous list of problems in 1900, he could not imagine for example that CH (the continuum hypothesis) is undecidable:[9] CH, which was conjectured by CANTOR in 1877, states that there is no set whose *cardinality* is strictly between that of $\mathbb{N}$ (denoted $\aleph_0$) and that of $\mathbb{R}$, but the work of GÖDEL in 1940 and that of Paul COHEN in 1963 showed that,[10] assuming that ZF set theory is consistent, CH is undecidable.

A paradox may then result from a lack of correct mathematical definitions, or by using an undecidable proposition, but often it corresponds to a wrong intuition about some mathematical question. After proving that there is a bijection between the interval $I = [0, 1] \subset \mathbb{R}$ and the square $I \times I \subset \mathbb{R}^2$, CANTOR wrote to DEDEKIND 'I see it, but I do not believe it!'.[11]

Before describing more paradoxes, I first recall definitions related to an *order* on a set X: it is a *binary relation* $\mathcal{R}$ on $X \times X$,[12] which is *reflexive* (i.e. for all $a \in X$ one has $a \mathcal{R} a$), *anti-symmetric* (i.e. for all $a, b \in X$, $a \mathcal{R} b$ and $b \mathcal{R} a$ imply $b = a$), and *transitive* (i.e. for all $a, b, c \in X$, $a \mathcal{R} b$ and $b \mathcal{R} c$ imply $a \mathcal{R} c$); it is also called a *partial order* (and sometimes X is called a *poset*, an abbreviation of partially ordered set) by opposition to a *total order* (i.e. such that for all $a, b \in X$, either $a \mathcal{R} b$ or $b \mathcal{R} a$, which maybe both if $b = a$), also called a *linear order*; a *chain* is any subset $A \subset X$ such that the restriction of $\mathcal{R}$ to $A \times A$ is a total order.

$\mathcal{R}$ is usually thought as similar to $a \leq b$ in $\mathbb{R}$, $A \subset B$ for subsets of a set, $a \mid b$ (i.e. a divides b) for positive integers, so that one says that an ordered set X has a *minimum* α if $\alpha \mathcal{R} x$ for all $x \in X$ (and the minimum is unique, although there is not necessarily one),[13] and X has a *maximum* ω if $x \mathcal{R} \omega$ for all $x \in X$ (and the maximum is unique, although there is not necessarily one). A total order on X is called a *well order* if every nonempty subset of X has a minimum.

An element a is *minimal* if $x \mathcal{R} a$ implies $x = a$;[14] an element z is *maximal* if $z \mathcal{R} x$ implies $x = z$. For a subset $A \subset X$, an *upper bound* of A is any $y \in X$ such that $a \mathcal{R} y$ for all $a \in A$, and the *least upper bound* of A, if it exists, is the minimum of all upper bounds; a *lower bound* of A is any $x \in X$ such that $x \mathcal{R} a$ for all $a \in A$, and the *greatest lower bound* of A, if it exists, is the maximum of all lower bounds.

Zermelo's theorem, conjectured by CANTOR, says that every non-empty set can be equipped with a well order.

---

[8] Kurt GÖDEL, Czech-born mathematician, 1906–1978. He worked in Vienna, Austria, and at IAS (Institute for Advanced Study), Princeton, NJ.

[9] David HILBERT, German mathematician, 1862–1943. He worked in Königsberg (then in Germany, now Kaliningrad, Russia) and at Georg-August-Universität, Göttingen, Germany. Hilbert spaces are named after him.

[10] Paul Joseph COHEN, American mathematician, 1934–2007. He received the Fields Medal in 1966 for his fundamental work on the foundations of set theory. He worked at Stanford University, Stanford, CA.

[11] Of course, such a bijection cannot be *continuous*, since its inverse would be continuous (by an argument of *compactness*), and then I minus an *interior* point (which is not *connected*) would be *homeomorphic* to a square minus a point (which is connected).

[12] It means that there is a subset $Y \subset X \times X$ and instead of writing $(a, b) \in Y$ one writes $a \mathcal{R} b$.

[13] One says that *uniqueness* holds for a problem in mathematics if when a_1 and a_2 are two solutions then they must coincide, but there might be no solutions, and *existence* of a solution is a different question. To avoid confusion, one may prefer to say "if a solution exists, it is unique".

[14] In the positive integers with the order $a \mid b$, then 1 is the minimum, but if one removes 1, then there is no minimum and the minimal elements are precisely the *prime numbers* (recalling that 1 is not considered a prime number).

Zorn's lemma,[15] which was actually used by BOCHNER 7 years before Max ZORN,[16] says that if every chain in a non-empty ordered set X has a least upper bound in X, then X has a maximal element.

The *axiom of choice* says that if I is a non-empty index set and for each $i \in I$ one has a non-empty set X_i, then the product $\prod_{i\in I} X_i$ is non-empty, i.e. it is possible to choose an $x_i \in X_i$ for every $i \in I$ and consider the point $x = (x_i, i \in I)$ in the product.

Despite the use of different terms (theorem, lemma, axiom) these three statements are equivalent, but some forms are more natural, and a few questions of maximality occur in algebra, for which one naturally uses "Zorn's lemma"; I do not recall seeing a direct use of Zermelo's theorem in algebra.

The axiom of choice permits to construct surprising sets, and it looks like paradoxes because it contradicts some intuition, which then appears to be misleading. One may want to avoid using the axiom of choice, as the constructivists do, so that such strange constructions cannot be done.

The *Hausdorff–Banach–Tarski paradox* is an improvement of an idea of HAUSDORFF by BANACH and TARSKI,[17,18,19], so that it is sometimes called the Banach–Tarski paradox: it implies that if A is a solid ball of radius 1 in $\mathbb{R}^3$ and B is a solid ball of radius 2 in $\mathbb{R}^3$, then there is an integer N and a *partition* of A as the (disjoint) union of $A_1, \dots, A_N$ and a *partition* of B as the (disjoint) union of $B_1, \dots, B_N$ such that for $i = 1, \dots, N$, the subset B_i is obtained from A_i by a rigid displacement.[20]

The paradox comes from the fact that rigid displacements conserve volume, so that one (mistakenly) thinks that for each $i \in \{1, \dots, N\}$ the volume of B_i is equal to the volume of A_i, which would imply that the volume of B is equal to the volume of A, and this is obviously not the case.

The resolution of the paradox is that some A_i are *non-measurable* sets, so that it is impossible to define their volume in a consistent way. The construction actually shows that one cannot define a *finitely additive measure* on bounded sets of $\mathbb{R}^3$,[21] with the property that it is invariant by translations and rotations, and that it coincides with the usual (Lebesgue) measure for cubes,[22] or for the *σ-algebra* of Borel sets.[23,24,25]

HAUSDORFF was actually generalizing a previous construction of a non-measurable subset of the circle

[15] Max August ZORN, German-born mathematician, 1906–1993. He worked at UCLA (University of California at Los Angeles), Los Angeles, CA, and at University of Indiana, Bloomington, IN, where I met him in 1980. "Zorn's lemma" is named after him, but it was used 7 years before he did by BOCHNER.

[16] Salomon BOCHNER, Polish-born mathematician, 1899–1982. He worked in München (Munich), Germany, and after 1933 at Princeton University, Princeton, NJ. He used "Zorn's lemma" 7 years before Max ZORN.

[17] Felix HAUSDORFF, German mathematician, 1869–1942. He worked in Leipzig, in Greifswald and in Bonn, Germany. He wrote literary and philosophical work under the pseudonym of Paul MONGRÉ. Hausdorff topologies and Hausdorff measures are named after him.

[18] Stefan BANACH, Polish mathematician, 1892–1945. He worked in Lwów (then in Poland, now Lvov, Ukraine). There is a Stefan Banach International Mathematical Center in Warsaw, Poland. The term Banach space was introduced by FRÉCHET.

[19] Alfred TARSKI (TEITELBAUM), Polish-born mathematician, 1902–1983. He worked in Warsaw, Poland, and at UCB (University of California at Berkeley), Berkeley, CA.

[20] A rigid displacement is a rotation followed by a translation, i.e. a mapping $x \mapsto a + M\,x$ for all $x \in \mathbb{R}^3$, with $a \in \mathbb{R}^3$ and $M \in S\mathbb{O}_3$ (or a translation followed by a rotation, but in general translations and rotations do not commute, since $a + M\,x = M\,(x + b)$ for $b = M^{-1}a = M^T a$).

[21] I.e. a mapping μ from the set bounded subsets of $\mathbb{R}^3$ into $[0, \infty] \subset \mathbb{R} \cup \{\infty\}$, with the property that $\mu(X \cup Y) = \mu(X) + \mu(Y)$ whenever X and Y are disjoint.

[22] Henri Léon LEBESGUE, French mathematician, 1875–1941. He worked in Rennes, in Poitiers, and he held a chair at Collège de France (mathématiques, 1921–1941) in Paris, France. The spaces L^p were named Lebesgue spaces in his honour by F. RIESZ, and the Lebesgue integration theory named after him was discovered two years before him by W.H. YOUNG.

[23] Félix Édouard Justin Émile BOREL, French mathematician, 1871–1956. He worked in Lille and in Paris, France. Borel functions, measures, or sets are named after him.

[24] A σ-algebra $\mathcal{A}$ is a family of subsets (of a set Z) which is stable by complementation and stable by countable unions.

[25] The σ-algebra of Borel sets is the smallest σ-algebra which contains the open sets.

$\mathbb{S}^1$ by VITALI,[26] which implies that there is no *σ-additive measure* on all subsets of $\mathbb{S}^1$ which is invariant by rotation.[27]

What constitutes a proof?

A proof of existence of a solution of a problem may be constructive, in which case it describes an algorithm which constructs a solution, or a sequence which converges to a solution, but if one only knows that a subsequence (of a sequence which one constructs) converges to a solution, it is not considered a constructive proof.

For example, if a real continuous function f from $[0,1]$ satisfies $f(0)\,f(1) < 0$, then there exits $z \in (0,1)$ with $f(z) = 0$, and one constructs a solution in the following way. If for $0 \le a_n < b_n \le 1$ one has $f(a_n)\,f(b_n) < 0$, then one evaluates $f(c_n)$ for $c_n = \frac{a_n+b_n}{2}$, and there are three cases: if $f(c_n) = 0$, then c_n is a solution; if $f(a_n)\,f(c_n) < 0$, one takes $a_{n+1} = a_n$ and $b_{n+1} = c_n$, and one repeats the algorithm, while if $f(a_n)\,f(c_n) > 0$, one takes $a_{n+1} = c_n$ and $b_{n+1} = b_n$, and one repeats the algorithm. Since $b_{n+1} - a_{n+1} = \frac{b_n - a_n}{2}$ for all n if one has not the chance to fall on a solution at some step, it implies that a_n and b_n are Cauchy sequences, which both converge to a solution z (because $\mathbb{R}$ is complete).

On the other hand, if a real continuous function f on a connected subset $X \subset \mathbb{R}^N$ for $N \ge 2$ is such that there exist $a, b \in X$ with $f(a) < 0 < f(b)$, then there exists $z \in X$ with $f(z) = 0$ by an argument of connectedness, i.e. $f(X)$ is connected, hence it contains the interval $[f(a), f(b)]$, which contains 0, but there is no precise algorithm behind this proof.

Brouwer's fixed point theorem,[28] that if f is continuous from a (non-empty) *compact* and *convex* set $K \subset \mathbb{R}^N$ into itself has at least one fixed point, i.e. some $z \in K$ satisfies $f(z) = z$, is not constructive for $N \ge 2$,[29] but BROUWER did not like his non-constructive existence proof, and after that he turned to constructivism for the rest of his life.

There is a different question than using non-constructive proofs, which is to be reasonably sure that there is no gap left in a proof which is very long.

At ICM78, the International Congress of Mathematicians of 1978 in Helsinki, Finland, I heard a talk about the classification of *finite simple groups*, by Daniel GORENSTEIN,[30] who was involved in the work. The search for the classification started in 1955, and it was "completed" around 1983: besides a few general families, there are 26 exceptions called *sporadic groups*. However, one may wonder if the "proof" is complete and correct, since it is made up of tens of thousands of pages in about 500 articles written by about 100 authors. Soon after the "completion", specialists started writing simpler proofs in order to reduce the length to something more reasonable.

There was a long standing conjecture, that colouring plane maps of connected countries could always be done with at most four colours, and many years ago there was a "computer proof" of it, because there was too much work involved in checking nearly two thousand cases, and a program was written for a computer to check all these cases.

What is sad about such "proofs" is that no really new mathematical idea has appeared to make the proof easily understandable, and one should remember that doing research in mathematics is about creating new knowledge, but also about discovering simplifying ideas which make those too long "proofs" clearer, if not simple!

---

[26] Giuseppe VITALI, Italian mathematician, 1875–1932. He worked in Modena, in Padova (Padua), and in Bologna, Italy. The department of pure and applied mathematics of Università degli Studi di Modena e Reggio Emilia is named after him.

[27] A σ-additive measure ν defined on a σ-algebra $\mathcal{A}$ is a mapping from $\mathcal{A}$ into $[0,\infty] \subset \mathbb{R} \cup \{\infty\}$ with the property that $\nu\big(\cup_{i\in I} A_i\big) = \sum_i \nu(A_i)$ whenever I is countable, and the A_i are disjoint and belong to $\mathcal{A}$.

[28] Luitzen Egbertus Jan BROUWER, Dutch mathematician, 1881–1966. He worked in Amsterdam, The Netherlands.

[29] For $N = 1$, $K = [a,b]$, and if neither a nor b are fixed points of f, then the function $f(x) - x$ changes sign on the interval $[a,b]$, hence it vanishes at a point.

[30] Daniel GORENSTEIN, American mathematician, 1923–1992. He worked at Clark University, Worcester, MA, at Northeastern University, Boston, MA, and at Rutgers University, Piscataway, NJ.

For doing research, it seems useful to learn enough about what has been done before, but maybe one should not learn too much, because at some point once should realize that a lot of what is published is not really research but development, i.e. using known ideas on various new problems. That one often confuses research and development seems to be a result of the "publish or perish" philosophy, which pushes against discovering simplifying ideas, because writing too much of the same thing is considered good by administrators!

In the early 1980s, I went to a Bourbaki seminar, which met a few times a year at IHP (Institut Henri Poincaré) in Paris, and I heard Jean-Pierre SERRE talk,[31] about a proof by Pierre DELIGNE, of conjectures by WEIL. Jean-Pierre SERRE started by saying that the proof used a tool generalizing an idea of Alexandre GROTHENDIECK, and it involved sheaf theory with p-adic numbers, I think, but since this was not written and only a handful of people would be able to write it down, he assumed that the extension mentioned was correct, and he explained what the proof was after that. Many years after, I heard that a group had worked at constructing the required extension, and it took about 500 pages to write it down!

Additional footnotes: CLARK,[32] FRÉCHET,[33] HARDINGE,[34] HARDY,[35] RIESZ F.,[36] RIESZ M.,[37] RUTGERS,[38] YOUNG L.C.,[39] YOUNG W.H..[40]

---

[31] Jean-Pierre SERRE, French mathematician, born in 1926. He received the Fields Medal in 1954 for his work in algebraic topology. He received the Wolf Prize in 2000 for his many fundamental contributions to topology, algebraic geometry, algebra, and number theory and his inspirational lectures and writing. He received the Abel Prize in 2003 for playing a key role in shaping the modern form of many parts of mathematics, including topology, algebraic geometry and number theory. He held a chair at Collège de France (algebra and geometry, 1956–1994), Paris, France.

[32] Jonas Gilman CLARK, American industrialist, 1815–1900. Clark University, Worcester, MA, is named after him.

[33] Maurice René FRÉCHET, French mathematician, 1878–1973. He worked in Poitiers, in Strasbourg and in Paris, France. Fréchet spaces (which are locally convex, metrizable and complete vector spaces) are named after him.

[34] Sir Charles HARDINGE, 1st baron HARDINGE of Penshurst, English diplomat, 1858–1944. He was Viceroy and Governor-General of India (1910–1916).

[35] Godfrey Harold HARDY, English mathematician, 1877–1947. He worked in Cambridge, in Oxford, England, holding the Savilian chair of geometry (1920–1931), and in Cambridge again, holding the Sadleirian chair of pure mathematics (1931–1942).

[36] Frigyes (Frederic) RIESZ, Hungarian mathematician, 1880–1956. He worked in Kolozsvár (then in Hungary, now Cluj-Napoca, Romania), in Szeged and in Budapest, Hungary. He introduced the spaces L^p in honor of LEBESGUE and the spaces $\mathcal{H}^p$ in honor of HARDY, but no spaces are named after him; the Riesz operators have been introduced by his younger brother Marcel RIESZ.

[37] Marcel RIESZ (younger brother of Frigyes (Frederic) RIESZ), Hungarian-born mathematician, 1886–1969. He worked in Stockholm and in Lund, Sweden. The Riesz operators are named after him.

[38] Henry RUTGERS, American colonel, 1745–1830. Rutgers University, Piscataway, NJ, is named after him.

[39] Laurence Chisholm YOUNG, English-born mathematician, 1905–2000. He worked in Cape Town, South Africa, and at University of Wisconsin, Madison, WI, where I first met him during my first trip to United States, in the spring of 1971. Young measures are named after him, and he introduced them in the Calculus of Variations. I pioneered their use in partial differential equations (from continuum mechanics) in the late 1970s, not knowing at the time that he introduced them, as I heard about them as parametrized measures in seminars on control theory.

[40] William Henry YOUNG, English mathematician, 1863–1942. He worked in Liverpool, England, in Calcutta, India, holding the first Hardinge professorship (1913–1917), in Aberystwyth, Wales, and in Lausanne, Switzerland. He is said to have discovered Lebesgue integration two years before LEBESGUE. There are many results attributed to him which may be joint work with his wife, Grace CHISHOLM-YOUNG, English mathematician, 1868–1944, as they collaborated extensively; their son Laurence is known for his own mathematical results.

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

3- Friday September 2, 2011.

The basic algebraic structures depend upon the number of operations used. With one *binary operation* satisfying some properties, a natural structure is that of a *group*, and with two binary operations (addition and multiplication) satisfying some properties a natural structure is that of a *ring*, with a particular case of a *field*. With addition and a second operation external, a natural structure is that of a *vector space* over a field F or a *module* over a ring R, depending upon the *scalars* belonging to F or R.

Between sets, one uses arbitrary *mappings*, but when one restricts attention to sets which have a particular algebraic structure,[1] one considers mappings which are adapted to the *category* of sets considered, *homomorphisms* in the case of *groups*, *rings*, or *fields*, *linear mappings* in the case of *vector spaces*, for example. In general, these particular mappings are called *morphisms*, and one uses a list of (Greek) prefixes which give information about them: an *injective* (one-to-one) mapping is called a *monomorphism*, a *surjective* (onto) mapping is called an *epimorphism*, a *bijective* (injective and surjective) mapping is called an *isomorphism*; a mapping from a set into itself is called an *endomorphism*, and an isomorphism of a set onto itself is called an *automorphism*.

If two sets with some algebraic structures are proved to be isomorphic, it means that by changing the names of elements and the names of the operations they are somewhat the same, and sometimes such a result is not so obvious and one needs a mathematician's mind for discovering it. Of course, it is part of the mathematician's job to observe similarities between situations, and to go from the general case to the particular examples, and out of a few examples to imagine a general situation.

Parables are like general theorems, and they can be transmitted by people who do not necessarily understand all the various applications of the teaching: if after stating a general theorem one gives an example, weaker students may only understand the example while stronger students foresee that the theorem applies to many situations. Since the gospels say that the disciples of Jesus often asked for examples,[2] it suggests that they did not understand what the teaching they received was about.[3]

Definition 3.1: A binary operation $*$ on a set X is *associative* if for all $a, b, c \in X$ one has $a * (b * c) = (a * b) * c$, so that one may write $a * b * c$ without ambiguity.

A binary operation $*$ on a set X is *commutative* if for all $a, b \in X$ one has $a * b = b * a$.

A binary operation $*$ on a set X has an *identity* e if for all $a \in X$ one has $a * e = e * a = a$.

For a binary operation $*$ on a set X which has an identity e, one says that an element a has an *inverse* a^{-1} if $a^{-1} * a = a * a^{-1} = e$.

Remark 3.2: An identity is unique: if both e_1 and e_2 are identities, then $e_1 * e_2$ is equal to e_1 because e_2 is an identity, and it is equal to e_2 because e_1 is an identity. Actually, once one has written a proof, it is useful to check what one has really used and what more general statements one can deduce: here, one may define an *identity on the left* e_ℓ if for all $a \in X$ one has $e_\ell * a = a$, and an *identity on the right* e_r if for all $b \in X$ one has $b * e_r = b$; then, if both e_ℓ and e_r exist, one considers $e_\ell * e_r$ and one deduces that $e_\ell = e_r$.

[1] Or non-algebraic, like *topological spaces*, where one restricts attention to *continuous mappings*.

[2] Jesus of Nazareth, Jewish religious teacher, 7 BCE–30 CE (or 2 BCE–36 CE). He is believed by Christians to be the (unique) son of God, and the messiah whom Jews were waiting for, hence its title Christ, which comes from the Greek Christos. Of course, I consider that he was only human, and I often refer to him as the Teacher. According to the gospels, he practiced meditation past the point where one can do miracles, but without using that power for a personal advantage. He was executed by the Romans, probably because some of his followers believed him to be the messiah whom Jews were waiting for, and whom they expected to put an end to the Roman occupation of Palestine.

[3] I deduce that Jesus of Nazareth existed, because the evangelists did not perceive that by repeating the stories they showed that the disciples were not so bright, hence they were not bright enough themselves for inventing such a character as Jesus: the only person who seems to have taught in parables before is the Buddha, and the story of Jesus of Nazareth does not resemble that of the Buddha.

If $*$ is associative, such an inverse is unique. More generally, one says that a has a *left inverse* α if $\alpha * a = e$, and that it has a *right inverse* β if $a * \beta = e$, and then if $*$ is associative and both α and β exist, one has $\alpha = \alpha * e = \alpha * a * \beta = e * \beta = \beta$.

Definition 3.3: A *group* $(G, *, e)$ is a set G equipped with an associative binary operation $*$ with identity $e \in G$ and such that each $a \in G$ has an inverse. An *Abelian group* is a group for which the operation is commutative, and in this case one uses $+$ for the operation, 0 for the identity, and $-a$ for a^{-1}.

A *monoid* $(M, *, e)$ is a set M equipped with an associative binary operation $*$ with identity $e \in M$.

A *semigroup* $(S, *)$ is a set S equipped with an associative binary operation $*$. It has the *cancellation property* if $a * b = a * c$ implies $b = c$ and if $a * b = c * b$ implies $a = c$.[4]

Remark 3.4: When one uses a multiplicative notation, it is common not to write a symbol for the operation, i.e. instead of writing $a \cdot b$, or $a * b$, or $a \star b$, for example, one writes $a\,b$, and then one has $(a\,b)^{-1} = b^{-1}a^{-1}$ (since $b^{-1}a^{-1}a\,b = b^{-1}e\,b = b^{-1}b = e$ and $a\,b\,b^{-1}a^{-1} = a\,e\,a^{-1} = a\,a^{-1} = e$).

One writes 0 for the identity if the operation is $+$, only used for a commutative operation, and in multiplicative notation one also writes 1 for the identity.

There are actually two mappings involved for a group, the operation $*$ which is a (surjective) mapping of $G \times G$ onto G and the inverse mapping $a \mapsto a^{-1}$ which is a bijection of G onto G.

By an abuse of language, one says a group G, so that which binary operation is considered and which is the identity must be clear, but in situations where one feels that there could be some confusion, it is better to give different names to the various operations which appear in a formula, of course.

Although $\mathbb{N}$ with addition is not a group, there is a natural symmetrization which embeds it into the additive *Abelian group* $\mathbb{Z}$ (since addition is *commutative*), and it is surprising that inventing zero took so long, and it seems that the Arab mathematicians learned it from the Indian mathematicians before it was introduced in Europe.[5] Inventing zero and negative numbers should have been obvious for merchants, who would understand their financial situation as the amount of cash a (or the value of the merchandise) they have and the amount b they borrowed, and consider their wealth to be a pair (a, b) with a different symbol to use for a if they are broke, or for b if they have reimbursed all their debts, but it may have been difficult to imagine an ideal world where one can borrow without interest so that the wealth of (a, b) is the same as that of $(a + c, b + c)$ after borrowing a positive amount c, so that there is a natural equivalence relation behind the definition of $a - b$ even though b may be $\geq a$, and this is formalized as Lemma 3.5.

Recall that an *equivalence relation* on a set X is a binary relation $\mathcal{R}$ which is *reflexive* (i.e. $a\,\mathcal{R}\,a$ for all $a \in X$), *symmetric* (i.e. $a\,\mathcal{R}\,b$ implies $b\,\mathcal{R}\,a$) and *transitive* (i.e. $a\,\mathcal{R}\,b$ and $b\,\mathcal{R}\,c$ imply $a\,\mathcal{R}\,c$), so that one can define the *equivalence class* of a as $\overline{a} = \{b \mid a\,\mathcal{R}\,b\}$, observe that two equivalence classes are either equal or disjoint, and define the *quotient set* $X/\mathcal{R}$ whose elements are the equivalence classes, with a natural *projection* π from X onto $X/\mathcal{R}$ which to each a associates its equivalence class $\overline{a}$. One then observes that if f is a mapping from X into Y which has the property that $a\,\mathcal{R}\,b$ implies $f(a) = f(b)$, then f factorizes as $f = \overline{f} \circ \pi$ for a mapping $\overline{f}$ from $X/\mathcal{R}$ into Y (defined by $\overline{f}(\overline{a}) = f(b)$ for any $b \in \overline{a}$).

Lemma 3.5: Let S be a (non-empty) semigroup with commutative operation $*$ having the cancellation property.

The relation $\mathcal{R}$ defined on $S \times S$ by '$(a, b)\,\mathcal{R}\,(c, d)$ means $a * d = b * c$' is an equivalence relation.

The operation $\star$ defined on $S \times S$ by $(a_1, b_1) \star (a_2, b_2) = (a_1 * a_2, b_1 * b_2)$ is compatible with $\mathcal{R}$ and induces on the quotient $G = S \times S/\mathcal{R}$ a binary operation $\overline{\star}$, which gives G an Abelian group structure, with

[4] One may define cancellation properties on the left or on the right, of course.

[5] In his *Ecclesiastical History of the English People*, written in 731, Bede popularized the dating system with AD (Anno Domini) invented in 525 by Dionysius the Humble for replacing the Diocletian years, and he invented the dating system with BC (Before Christ), without a year zero, so that the year preceding 1AD is 1BC. Since it is silly to confuse numbering systems with religious questions, it is better to use CE (Common Era) instead of AD, and BCE (Before Common Era) instead of BC. Confusing astronomical questions with religious ones should also be avoided, and the astronomical corrections introduced in 1582 for starting the Gregorian calendar were difficult to accept for some Protestant countries, and England switched to it in 1752, or for Greek Orthodox countries, and Greece switched to it in 1923, Russia having done it just after its "October revolution" in 1917, which for us occurred in November.

the identity 0 being the equivalence class of (s,s) for any $s \in S$, and the inverse of the equivalence class of (a,b) being the equivalence class of (b,a).

S is embedded into G by the mapping j with $j(a)$ being the equivalence class of $(a*s,s)$ for all $s \in S$, and one has $j(a*b) = j(a)\,\overline{\star}\,j(b)$ for all $a,b \in S$.

Proof: $\mathcal{R}$ is reflexive since $(a,b)\,\mathcal{R}\,(a,b)$ means $a*b = b*a$ and $*$ is assumed commutative. $\mathcal{R}$ is symmetric since $(c,d)\,\mathcal{R}\,(a,b)$ means $c*b = d*a$, which is the same as $a*d = b*c$ by commutativity. $\mathcal{R}$ is transitive since $(a_1,b_1)\,\mathcal{R}\,(a_2,b_2)$ and $(a_2,b_2)\,\mathcal{R}\,(a_3,b_3)$ mean $a_1*b_2 = b_1*a_2$ and $a_2*b_3 = b_2*a_3$, so that $a_1*b_2*b_3 = b_1*a_2*b_3 = b_1*b_2*a_3$, hence $b_2*a_1*b_3 = b_2*b_1*a_3$ by commutativity, which implies $a_1*b_3 = b_1*a_3$ by the cancellation property.

One needs to show that if $(a_1,b_1)\,\mathcal{R}\,(c_1,d_1)$ and $(a_2,b_2)\,\mathcal{R}\,(c_2,d_2)$ then $(a_1*a_2, b_1*b_2)\,\mathcal{R}\,(c_1*c_2, d_1*d_2)$; indeed, one has $a_1*d_1 = b_1*c_1$ and $a_2*d_2 = b_2*c_2$, so that using commutativity $(a_1*a_2)*(d_1*d_2) = (a_2*d_2)*(a_1*d_1) = (b_2*c_2)*(b_1*c_1) = (b_1*b_2)*(c_1*c_2)$. This shows that $\star$ implies an operation $\overline{\star}$ on the quotient. Associativity of $*$ implies associativity of $\star$, which implies associativity of $\overline{\star}$, and commutativity of $*$ implies commutativity of $\star$, which implies commutativity of $\overline{\star}$, of course. Since all (s,s) are equivalent, its equivalence class 0 is the identity of $\overline{\star}$ if $(a,b)\star(s,s)$ is equivalent to (a,b) for all (a,b), which follows from the cancellation property. Then, $(a,b)\star(b,a) = (a+b, a+b)$ by commutativity.

Since $(a*s,s)\,\mathcal{R}\,(a*t,t)$ by commutativity, it follows that $j(a)$ is well defined, and then $j(a*b)$ is the equivalence class of $\big((a*b)*(s*t),(s*t)\big) = (a*s,s)\star(b*t,t)$, i.e. $j(a)\overline{\star}j(b)$.

Example 3.6: If S is the positive integers ($\mathbb{N}^\times = \mathbb{N}\setminus\{0\}$) with addition, then G is (isomorphic) to $\mathbb{Z}$.

If S is the positive integers with multiplication, then G is (isomorphic) to the multiplicative group $\mathbb{Q}_+$, the positive rationals.

If $S = \mathbb{Z}^* = \mathbb{Z}\setminus\{0\}$ with multiplication, then G is (isomorphic) to the multiplicative group $\mathbb{Q}^* = \mathbb{Q}\setminus\{0\}$, the non-zero rationals.[6]

Definition 3.7: If $(G_1,*_1,e_1)$ and $(G_2,*_2,e_2)$ are two groups and f is a mapping from G_1 into G_2,[7] then f is an *homomorphism* if $f(a\,*_1\,b) = f(a)\,*_2\,f(b)$ for all $a,b \in G_1$.

The *kernel* of an homomorphism f is the inverse image of $\{e_2\}$,[8] i.e. $f^{-1}(\{e_2\}) = \{a \in G_1 \mid f(a) = e_2\}$.

The groups G_1 and G_2 are said to be *isomorphic* if there exists an isomorphism from G_1 onto G_2 (whose inverse is then an isomorphism from G_2 onto G_1), and one then writes $G_1 \simeq G_2$.

Lemma 3.8: If f is an homomorphism from G_1 into G_2, then $f(e_1) = e_2$ and $f(a^{-1}) = \big(f(a)\big)^{-1}$ for all $a \in G_1$.

Proof: For $a \in G_1$, one has $a = a\,e_1$, so that $f(a) = f(a)\,f(e_1)$ and (by multiplying on the left by the inverse of $f(a)$) $e_2 = f(e_1)$. Then one has $a\,a^{-1} = e_1$, so that $f(a)\,f(a^{-1}) = e_2$ and (by multiplying on the left by the inverse of $f(a)$) $f(a^{-1}) = \big(f(a)\big)^{-1}$.

Remark 3.9: If S is an Abelian group, the symmetrization process of Lemma 3.5 produces an Abelian group G which is isomorphic to S, with j being an isomorphism from S onto G.

Example 3.10: The *logarithm*, introduced by NAPIER,[9] is defined by $\log(a) = \int_1^a \frac{dx}{x}$ for $a \in \mathbb{R}_+$, which

[6] For a ring R, one denotes R^* the multiplicative group of units, i.e. of elements of R which have an inverse for multiplication. For an integral domain D (i.e. a commutative ring without zero-divisors) and $S = D\setminus\{0\}$ with multiplication one obtains $F^* = F\setminus\{0\}$ where F is the field of fractions of D.

[7] By an abuse of language, one usually says that f is a mapping from a group G_1 into a group G_2, and that it is an homomorphism if ..., and I shall write in this way in the sequel.

[8] If f is a mapping from a set X into a set Y, one associates a (push forward) mapping $f_>$ from $\mathcal{P}(X)$ into $\mathcal{P}(Y)$ defined by $f_>(A) = \{f(a) \mid a \in A\}$ for all $A \subset X$, and a (pull backward) mapping $f^<$ from $\mathcal{P}(Y)$ into $\mathcal{P}(X)$ defined by $f^<(B) = \{a \in X \mid f(a) \in B\}$ for all $B \subset Y$. This good notation was introduced by my colleagues Walter NOLL and Juan SCHÄFFER, who improved on a notation f_* and f^* from a book by MAC LANE and Garrett BIRKHOFF, but these notations are not common and almost everyone in mathematics writes $f(A)$ for $\{f(a) \mid a \in A\}$, and $f^{-1}(B)$ for $\{a \in X \mid f(a) \in B\}$, although it may be a little confusing in some cases.

[9] John NAPIER, Scottish mathematician, 1550–1617. He invented a form of logarithms in 1614, and

requires defining a so-called Riemann integral (since the function $x \mapsto \frac{1}{x}$ is continuous on $\mathbb{R}_+$),[10] whose intuition was clear to many a long time before, since ARCHIMEDES is credited for computing the area below a parabola,[11] without even having an equation for the parabola since the invention of analytic geometry (i.e. the introduction of algebraic notation in geometry) is attributed to DESCARTES;[12] the result ARCHIMEDES was the most proud of was that the surface area of a sphere of radius R is equal to the lateral area of a tangent cylinder of radius R and height $2R$, and he had asked that his tomb show a sphere and a cylinder, and when Cicero was named governor of Sicily,[13] this information permitted him to find the tomb (without the help of the people of Syracuse, who had forgotten where it was). By a simple change of variable, one proves that $\log(a\,b) = \log(a) + \log(b)$ for $a, b \in \mathbb{R}_+$, and this shows that the logarithm is an homomorphism from the multiplicative (Abelian) group $\mathbb{R}_+$ into the additive (Abelian) group $\mathbb{R}$, and it is actually an isomorphism, whose inverse is the *exponential*.

However, the multiplicative (Abelian) group $\mathbb{Q}_+$ is not isomorphic to the additive (Abelian) group $\mathbb{Q}$, because in $\mathbb{Q}$ the equation $x + x = a$ has a solution for all $a \in \mathbb{Q}$, while in $\mathbb{Q}_+$ the equation $x^2 = a$ only has a solution if $a = \frac{m^2}{n^2}$ for m, n positive integers (and relatively prime).

Besides $\mathbb{Z}$, there is a natural family of finite Abelian groups, the group $\mathbb{Z}_n$ of integers modulo n (and $\mathbb{Z}_n$ has n elements), introduced by GAUSS for reasons from number theory.[14]

Looking for finite groups, one has to consider the group of permutations of n objects (with $n \geq 2$), which is the *symmetric group* S_n (which has $n!$ elements), and only S_2 is Abelian and isomorphic to $\mathbb{Z}_2$.

Some particular non-Abelian groups are found by considering the groups of symmetries of various regular objects, like that of a regular polygon with n sides (with $n \geq 3$), which is the *dihedral group* D_n (which has $2n$ elements), and it reduces to the Abelian group $\mathbb{Z}_n$ if one restricts attention to symmetries conserving the orientation (i.e. if one rejects *mirror symmetries*), so that $\mathbb{Z}_n$ is isomorphic to the *group of rotations* by angles which are multiples of $\frac{2\pi}{n}$, or to the multiplicative group of nth roots of unity in $\mathbb{C}$; D_3 is actually isomorphic to S_3. The group of symmetries of a rhombus which is not a square or that of a rectangle which is not a square is $\mathbb{Z}_2 \times \mathbb{Z}_2$, called the *Klein four-group* V,[15] which is not isomorphic to $\mathbb{Z}_4$, while $\mathbb{Z}_2 \times \mathbb{Z}_3$ is isomorphic to $\mathbb{Z}_6$, and we shall see the relation with the *Chinese remainder theorem*.

One non-Abelian group of order 8 is the *quaternion group* Q_8, which has some relation with the *quaternions* introduced by HAMILTON.[16]

We shall have to understand questions of product of groups, of quotient of groups, and other ways to construct new groups, and in what ways problems of groups appear in questions from outside mathematics.

Additional footnotes: BEDE,[17] Garrett BIRKHOFF,[18] .../...

---

suggested an improvement into the actual form to BRIGGS, who published his tables of logarithms in 1617, with whole credit to NAPIER, who had just died.

[10] Georg Friedrich Bernhard RIEMANN, German mathematician, 1826–1866. He worked at Georg-August-Universität, Göttingen, Germany. The Riemann ζ function is named after him, although EULER had studied it in his thesis. Riemannian manifolds and Riemannian geometry are named after him, as well as Riemann surfaces for functions of a complex variable, and Riemann invariants for conservation laws in continuum mechanics.

[11] ARCHIMEDES, Greek mathematician, 287 BCE–212 BCE. He worked in Siracusa (Syracuse), then a Greek colony, now in Italy.

[12] René DESCARTES, French mathematician and philosopher, 1596–1650. Université de Paris 5 is named after him. The terms Cartesian coordinates and Cartesian products are derived from his name (written in Latin as CARTESIUS, possibly DES CARTES in French).

[13] Marcus TULLIUS Cicero, Roman orator and politician, 106 BCE–43 BCE.

[14] And also for questions of calendar, I believe.

[15] Felix Christian KLEIN, German mathematician, 1849–1925. He worked at Georg-August-Universität, Göttingen, Germany.

[16] Sir William Rowan HAMILTON, Irish mathematician, 1805–1865. He worked in Dublin, Ireland.

[17] (The venerable) BEDE, English monk and historian, 673–735. He popularized the new dating system with AD (Anno Domini) in his *Ecclesiastical History of the English People*, and invented the dating system with BC (Before Christ), so that there is no year zero in the calendar.

[18] Garrett BIRKHOFF, American mathematician, 1911–1996. He worked at Harvard University, Cambridge,

BRIGGS,[19] Buddha,[20] DIOCLETIAN,[21] DIONYSIUS the Humble,[22] Gregory XIII,[23] GRESHAM,[24] JULIUS Caesar,[25] MAC LANE,[26] Walter NOLL,[27] Juan SCHÄFFER.[28]

MA.

[19] Henry BRIGGS, English mathematician, 1561–1630. He worked at Gresham college, London, and then in Oxford, England, holding the first Savilian chair of geometry(1619–1630). He was the first to publish a table of logarithms, following the suggestions of NAPIER.

[20] Siddhartha Gautama, Indian religious teacher, 563 BCE–483 BCE. Buddhists follow his teachings, and consider that he was the historical Buddha for our era.

[21] Gaius Aurelius Valerius DIOCLETIANUS (DIOCLES), Roman military and political leader, 244–311. He was Roman emperor from 284 to 305.

[22] DIONYSIUS the Humble (DIONYSIUS Exiguus), Greek Orthodox monk, 470–540. He invented a new system of numbering years to replace the Diocletian years, with AD (Anno Domini), thus starting the Christianized version of the Julian calendar.

[23] Gregory XIII (Ugo BONCOMPAGNI), Italian Pope, 1502–1585. He was elected Pope in 1572. The Gregorian calendar is named after him.

[24] Sir Thomas GRESHAM, English merchant and financier, 1519–1579. He left the money used for founding Gresham College in London, England, in 1597.

[25] Gaius JULIUS Caesar, Roman military and political leader, 100 BCE–44 BCE. The qualifier Caesar for the Roman emperors (which transformed into Kayser in Germany, and Czar in Russia) comes from his cognomen, and the Julian calendar also refers to him.

[26] Saunders MAC LANE, American mathematician, 1909–2005. He worked at Harvard, Cambridge, MA and at University of Chicago, Chicago, IL.

[27] Walter NOLL, German-born mathematician, born in 1925. He works at CMU (Carnegie Mellon University), Pittsburgh, PA, where he has been my colleague since I moved there, in 1987.

[28] Juan Jorge SCHÄFFER, Austrian-born mathematician, born in 1930. He works at CMU (Carnegie Mellon University), Pittsburgh, PA, where he has been my colleague since I moved there, in 1987.

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

4- Wednesday September 7, 2011.

Definition 4.1: If G is a group and $a \in G$, then for $n > 0$ one writes a^n for $a \cdots a$ with n factors a, for $n < 0$ one writes $a^n = a^{-1} \cdots a^{-1}$ with $|n|$ factors a^{-1}, and one writes $a^0 = e$.

One says that a and b *commute* if $b\,a = a\,b$.

Remark 4.2: One checks easily that for all $m, n \in \mathbb{Z}$ and all $a \in G$ one has $a^m a^n = a^{m+n}$, and it means that the mapping $n \mapsto a^n$ is an homomorphism from $\mathbb{Z}$ into G.

If a commutes with b,[1] then a commutes with b^{-1}, since by multiplying $b\,a = a\,b$ on the left and on the right by b^{-1} gives $a\,b^{-1} = b^{-1}a$. If a commutes with b and c, then a commutes with $b\,c$ since $a\,(b\,c) = (a\,b)\,c = (b\,a)\,c = b\,(a\,c) = b\,(c\,a) = (b\,c)\,a$. One deduces that if a and b commute, then a^m commutes with b^n for all $m, n \in \mathbb{Z}$.

Definition 4.3: If G is a group, a subset $H \subset G$ is a *subgroup* of G if

i) $e \in H$

ii) for all $h_1, h_2 \in H$, one has $h_1 h_2 \in H$,

iii) for all $h \in H$, one has $h^{-1} \in H$,

and one writes $H \leq G$. A subgroup H of G is called *proper* if $H \neq G$, and it is called *non-trivial* if $H \neq \{e\}$.

Remark 4.4: It is equivalent to say that for $H \subset G$, H is a subgroup of G if[2]

a) $H \neq \emptyset$,

b) for all $h_1, h_2 \in H$, one has $h_1 h_2^{-1} \in H$.

Indeed, taking $h_2 = h_1 \in H$ gives $e \in H$, and then taking $h_1 = e$ shows that $h_2^{-1} \in H$, and then replacing h_2 by h_2^{-1} gives $h_1 h_2 \in H$.

The notation $\leq$ for subgroups is natural because it is an order relation.

Definition 4.5: For a subgroup H of G, a *left coset* of H in G is any subset of the form $a\,H = \{a\,h \mid h \in H\}$ for some $a \in G$, and a *right coset* of H in G is any subset of the form $H\,b = \{h\,b \mid h \in H\}$ for some $b \in G$. The *order* of H, written $|H|$, is its cardinality (i.e. its number of elements if H is finite), and the *index* of H, written $[G\!:\!H]$,[3] is the cardinality of the set of left cosets (equal to the cardinality of the set of right cosets).[4]

H is a *normal subgroup* of G if for all $g \in G$ one has $g\,H = H\,g$, or equivalently $g\,H\,g^{-1} = H$ for all $g \in G$, [5] and one writes $H \lhd G$.

Remark 4.6: Left cosets form a partition of G (and right cosets also form a partition of G), i.e. if $a\,H \cap b\,H \neq \emptyset$ then $a\,H = b\,H$:[6] indeed, $a\,h_1 = b\,h_2$ implies $b = a\,h_1 h_2^{-1}$, so that $b\,h = a\,h_1 h_2^{-1} h \in a\,H$ for all $a \in H$, implying $b\,H \subset a\,H$, and reversing the roles of a and b gives $a\,H \subset b\,H$.

In order to check that H is a normal subgroup of G, it is enough to show that $g\,H\,g^{-1} \subset H$ for all $g \in G$, because by multiplying by g^{-1} on the left and by g on the right, one deduces that $H \subset g^{-1} H\,g$ for all $g \in G$, and by replacing g by g^{-1} it is the same as $H \subset g\,H\,g^{-1}$ for all $g \in G$.

---

[1] The relation 'commutes with' in a group G is reflexive and symmetric, but it is not always transitive if G is non-Abelian.

[2] One should not forget a), since b) is true for the empty set $\emptyset$, because all propositions beginning by $\forall h \in H$ are true if $H = \emptyset$.

[3] In the case where a field F is an extension of a field E, the same notation $[F\!:\!E]$ is also used to denote the dimension of F over E. The context should then make clear which notation is used.

[4] There is a bijection from left cosets to right cosets, since the bijection $g \mapsto g^{-1}$ maps the left coset $a\,H$ onto the right coset $H\,a^{-1}$.

[5] One should notice that $a\,H = H\,a$ does not mean that a commutes with the elements of H, but that for $h \in H$ there exist $h_1, h_2 \in H$ such that $a\,h = h_1 a$ and $h\,a = a\,h_2$

[6] Said otherwise, if $a\,\mathcal{R}\,b$ means $b \in a\,H$, then $\mathcal{R}$ is an equivalence relation: reflexivity follows from $a = a\,e$, symmetry follows from $b = a\,h$ implying $a = b\,h^{-1}$, and transitivity follows from $b = a\,h_1$ and $c = b\,h_2$ implying $c = a\,(h_1 h_2)$.

The relation $\triangleleft$ is not always a transitive relation (hence not an order relation) in a non-Abelian group, i.e. $G_1 \triangleleft G_2 \triangleleft G_3$ and G_3 non-Abelian do not imply that G_1 is a normal subgroup of G_3,[7] but if G is an Abelian group, all its subgroups are normal subgroups.

Lemma 4.7: If f is an homomorphism from a group G_1 into a group G_2, then the image $f(G_1)$ is a subgroup of G_2 and the kernel of f (i.e. $H = f^{-1}(\{e_2\})$) is a normal subgroup of G_1.
Proof: Since $f(e_1) = e_2$, one has $e_2 \in f(G_1)$. If $a, b \in f(G_1)$, then $a = f(\alpha), b = f(\beta)$ for some $\alpha, \beta \in G_1$, so that $a\,b^{-1} = f(\alpha)f(\beta)^{-1} = f(\alpha)f(\beta^{-1}) = f(\alpha\,\beta^{-1}) \in f(G_1)$, hence $f(G_1)$ is a subgroup of G_2.

For $g \in G_1$ and $h \in H$ (i.e. $h \in G_1$ and $f(h) = e_2$) one has $f(g\,h\,g^{-1}) = f(g)\,f(h)\,f(g^{-1}) = f(g)\,e_2\,f(g)^{-1} = e_2$, so that $g\,H\,g^{-1} \subset H$, hence $H \triangleleft G_1$.

Definition 4.8: If $A \subset G$, the *subgroup generated by* A, denoted $\langle A\rangle$, is the smallest subgroup of G containing A. The *order* of an element $g \in G$ is the order of the subgroup $\langle g\rangle$ generated by g. A group G is *cyclic* if it is generated by one element element $a \in G$, i.e. $G = \langle a\rangle$, and each such a is then called a *generator* of G; a group G is *finitely generated* if $G = \langle A\rangle$ for a finite set A.

Remark 4.9: Because an intersection of subgroups of G is obviously a subgroup of G, $\langle A\rangle$ is just the intersection of all subgroups of G containing A (and there is at least G in the list); notice that $\langle\emptyset\rangle = \{e\}$. If $A \neq \emptyset$, then for each $a \in A$ all the terms a^n for $n \in \mathbb{Z}$ belong to $\langle A\rangle$, and then $\langle A\rangle$ contains the products of elements of this form, so that it contains $\{a_1^{k_1} \cdots a_m^{k_m} \mid m \geq 1, a_1, \ldots, a_m \in A, k_1, \ldots, k_m \in \mathbb{Z}\}$, and since this set is obviously a subgroup of G it is equal to $\langle A\rangle$. In particular, for each $g \in G$ one has $\langle g\rangle = \{g^n \mid n \in \mathbb{Z}\}$.

Either g has infinite order and $\langle g\rangle \simeq \mathbb{Z}$, or g has finite order so that $g^m = g^n$ for some $m \neq n$, hence $g^k = e$ for some $k \geq 1$; let d be the smallest positive integer with $g^d = e$, so that $\{g, \ldots, g^d = e\}$ has d distinct elements; for each $n \in \mathbb{Z}$, the Euclidean division gives $n = d\,q + r$ for a quotient $q \in \mathbb{Z}$ and a remainder $r \in \{0, \ldots, d-1\}$, and then $g^n = (g^d)^q g^r = g^r$, so that $\langle g\rangle = \{e, g, \ldots, g^{d-1}\}$. In particular d is the order of g, and $g^k = e$ implies that k is a multiple of d.

Lemma 4.10: The subgroups of $\mathbb{Z}$ have the form $m\,\mathbb{Z}$ for $m \in \mathbb{N}$, so that a subgroup H which is proper ($H \neq \mathbb{Z}$) and non-trivial ($H \neq \{0\}$) is made of the multiples of an integer $m \geq 2$.
Proof: If a subgroup H of $\mathbb{Z}$ is non-trivial, it contains a smallest positive element m, and for each $h \in H$, the Euclidean division gives $h = m\,q + r$ for a quotient $q \in \mathbb{Z}$ and a remainder $r \in \{0, \ldots, m-1\}$, but since $r \in H$ (because h and $m\,q$ belong to H) one deduces that $r = 0$ by the choice of m.

Remark 4.11: $\mathbb{Z}$ has a second operation, multiplication, which makes it a (commutative) *ring*, but it has special properties which are not shared by all rings,[8] and it took some time to discover which definitions to take for general rings; it is then useful to wonder if all the notions invented are really natural.

For groups, the notion of a normal subgroup is natural: on one hand it characterizes the kernels of homomorphisms (which are the natural mappings between groups), and on the other hand (as we shall see in another lecture) it is the right notion for having an operation on the left cosets (or right cosets) so that a *quotient group* can be defined. For rings, the kernel of an homomorphism is an *ideal*, and it is also related to defining a *quotient ring*, but $\mathbb{Z}$ is special because its ideals coincide with its subgroups.

$\mathbb{Z}$ has no *zero divisor*, i.e. non-zero elements a, b such that $a\,b = 0$, and since it is commutative it is an example of an *Integral Domain* (abbreviated ID).

In order to generalize the existence of the Euclidean division in $\mathbb{Z}$, one invented the notion of an *Euclidean domain*.

Since the ideals/subgroups of $\mathbb{Z}$ are generated by one element, one invented the notion of *principal ideal*, which are generated by one element (similar to the notion of cyclic groups for groups) and of *Principal Ideal Domain* (abbreviated PID), whose all ideals are principal. One then generalized the notion by defining a *Noetherian ring*,[9] whose all ideals are finitely generated, and all these notions will become more natural

[7] Counter-examples with G_1 not a normal subgroup of G_3 will be shown later in the course.

[8] In this course, all the rings will be assumed to be *unital*, i.e. have an identity for multiplication, denoted 1, which is different from 0, the identity for addition, which is denoted +.

[9] Max NOETHER, German mathematician, 1844–1921. He worked in Heidelberg and in Erlangen, Germany.

when one will consider polynomials with coefficients in general rings.[10]

Remark 4.12: In $\mathbb{N}$, a *prime* p is any integer ≥ 2 such that its only divisors are 1 and p (so that 1 is not considered a prime), but the general notion for rings gives $\pm p$ in the case of $\mathbb{Z}$, so that there is a particular choice which is made in deciding that primes are positive. This is due to the fact that a *unit* in a commutative ring is an element which has an inverse for multiplication, and that the units in $\mathbb{Z}$ are ± 1, and some general notions are only defined up to *associates* (and b is an associate of a means $b = a\,u$ for a unit u); however, one also needs to define an *irreducible* element in a general ring, and the notions of prime and irreducible coincide if the ring is a *Unique Factorization Domain* (abbreviated UFD), implied by being a PID.

It has been known since the ancient Greeks that every integer $n \geq 2$ has a unique factorization $n = p_1^{k_1} \cdots p_r^{k_r}$ where $p_1, \ldots, p_r$ are distinct primes (which one orders by $p_1 < p_2 < \ldots$, and this selection using the order relation cannot be done in a general UFD) and $k_1, \ldots, k_r \geq 1$. For two integers $m, n \geq 2$, using the distinct primes $p_1, \ldots, p_s$ appearing in their factorizations, one has $m = p_1^{\alpha_1} \cdots p_s^{\alpha_s}$ and $n = p_1^{\beta_1} \cdots p_s^{\beta_s}$ with $\alpha_i, \beta_i \geq 0$ and one of them ≥ 1 for $i = 1, \ldots, s$, and the *greatest common divisor* (abbreviated gcd) of m and n, denoted (m, n) is $d = p_1^{\gamma_1} \cdots p_s^{\gamma_s}$ with $\gamma_i = \min\{\alpha_i, \beta_i\}$ for $i = 1, \ldots, s$.

Since it is difficult to factorize large numbers,[11] it is useful to observe that there is a simple algorithm for computing the gcd of n_1 and n_2 with $n_1 > n_2 > 1$,[12] and LAMÉ has estimated the number of operations it may take,[13] and it involves the *Fibonacci sequence*,[14] which itself uses the *golden ratio* $\rho = \frac{1+\sqrt{5}}{2}$, and the number of steps is $\leq \frac{\log(n_2)}{\log(\rho)} + 4$.[15]

Definition 4.13: The *Euler function* φ is defined for $n \geq 1$ by $\varphi(n)$ equal to the number of integers $k \in \{1, \ldots, n\}$ which are *relatively prime* with n, i.e. with $(k, n) = 1$.

Remark 4.14: By looking at the algorithm for finding the gcd, one sees that if $d = (n_1, n_2)$ then there exist $\alpha, \beta \in \mathbb{Z}$ such that $d = \alpha\, n_1 + \beta\, n_2$ (Bachet's identity).[16] One deduces that for $n \geq 2$ and $a \neq 0$, the equation $a\,x + b = 0 \pmod{n}$ has a solution $x \in \mathbb{Z}$ if and only if b is a multiple of the gcd (a, n), and x is then defined modulo $\frac{n}{(a,n)}$. In particular, a has an inverse modulo n if and only if $(a, n) = 1$, so that $\varphi(n)$ is the number of units in the ring $\mathbb{Z}_n$.

---

[10] Why care about polynomials with coefficients in general rings? Even though one is interested in polynomials with coefficients in a field F like $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$, one first observes that polynomials in one variable form a ring denoted $F[x]$ which is an Euclidean domain (since there is an Euclidean algorithm for polynomials with coefficients in a field), hence a PID, but the polynomials in two variables $F[x, y]$ is not a PID, and since one may consider it as $R[x]$ with $R = F[y]$, it is useful to discover a property that $R[x]$ inherits when R has it: being a UFD (unique factorization domain), or being a Noetherian ring are such properties.

[11] This difficulty is used in *public key cryptography*, like for the *RSA system*, named after RIVEST, Adi SHAMIR, and ADLEMAN: one sends messages in a "secure" way to a person by encrypting x as $y = x^d \pmod{n}$, and this person knows a value of e for decrypting by $x = y^e \pmod{n}$, and it works if $d\,e = 1 \pmod{\varphi(n)}$ by Euler's theorem (and x relatively prime with n). The RSA method chooses $n = p_1 p_2$ with two distinct large primes (about one hundred decimal digits nowadays) p_1, p_2, so that $\varphi(n) = (p_1 - 1)\,(p_2 - 1)$, and d must be chosen relatively prime with $\varphi(n)$. Although n is known, its factorization is kept secret, and the actual state of the art does not permit to find the factorization in a reasonable amount of time.

[12] The algorithm consists in first dividing n_1 by n_2, i.e. $n_1 = q_1 n_2 + n_3$ with $0 \leq n_3 < n_2$, then dividing n_2 by n_3, i.e. $n_2 = q_2 n_3 + n_4$ with $0 \leq n_4 < n_3$, and repeating this operation until $n_k = 0$, so that the gcd is n_{k-1} and the algorithm has used $k - 2$ steps.

[13] Gabriel LAMÉ, French mathematician, 1795–1870. He worked in St. Petersburg, Russia and in Paris, France. Lamé's system in linearized elasticity is named after him.

[14] It is defined by $F_0 = F_1 = 1$ and $F_n = F_{n-1} + F_{n-2}$ for all $n \geq 2$: since $n_{k-1} \geq 1 = F_1$ and $n_{k-2} \geq 2 = F_2$, one has $n_{k-3} \geq n_{k-2} + n_{k-1} \geq F_3$ (because $q_{k-3} \geq 1$), and by induction $n_2 \geq F_{k-2}$, which shows that if $F_{\ell+1} > n_2 \geq F_\ell$, the gcd is found after at most $\ell + 2$ steps of the algorithm (and if $n_1 = F_{\ell+1}$ and $n_2 = F_\ell$, one finds that $n_j = F_{\ell+2-j}$ for $j \leq \ell + 1$).

[15] Using $\rho^2 = \rho + 1$ and $\frac{1}{\rho} = \rho - 1 = \frac{\sqrt{5}-1}{2}$, one deduces that $F_n = a\,\rho^n + b\,\rho^{-n}$ if $a + b = 1$ and $a\,\rho + b\,\rho^{-1} = 1$, i.e. $a = \rho^{-2}, b = \rho^{-1}$, hence $F_n \geq \rho^{n-2}$ and the number of steps is $\leq \frac{\log(n_2)}{\log(\rho)} + 4$.

[16] Claude Gaspard BACHET, sieur de Méziriac, French mathematician, 1581–1638.

Theorem 4.15: (Fermat's theorem) If p is prime and a is not a multiple of p, then $a^{p-1} = 1 \pmod{p}$.

Theorem 4.16: (Euler's theorem) If $n \geq 2$ and a is relatively prime with n, then $a^{\varphi(n)} = 1 \pmod{n}$.

Remark 4.17: For p prime, one has $\varphi(p) = p - 1$, so that Euler's theorem is a generalization of Fermat's theorem. Since FERMAT did not give proofs of his statements, other mathematicians had to supply a written proof for everyone to be sure that his statements were correct; it was probably while he was seeking a proof of Fermat's theorem that EULER found a proof which implies the stronger statement.

Lagrange's theorem implies that in a finite group G every element $g \in G$ satisfies $g^{|G|} = e$, since the order d of g divides $|G|$, and from $g^d = e$ one takes the mth power with $m = \frac{|G|}{d}$ and one obtains $g^{|G|} = e$. If one observes that the units in a ring R form a multiplicative group, denoted R^*, Euler's theorem is the preceding observation for $G = \mathbb{Z}_n^*$, which has order $\varphi(n)$, and Fermat's theorem is the case where n is a prime p.

Lemma 4.18: For each d dividing n (with $n \geq 2$), $\mathbb{Z}_n$ has exactly $\varphi(d)$ elements of order d, so that $\sum_{d|n} \varphi(d) = n$. For each d dividing n, $\mathbb{Z}_n$ has exactly one subgroup of order d.
Proof: Since one deals with addition, one uses the additive notation.[17] An element a has order d if $d\,a$ is a multiple of n and no smaller integer than d has this property. Since d divides n, let $n = d\,\delta$, so that $a = k\,\delta$, and then $j\,a$ is a multiple of n if and only if $j\,k$ is a multiple of d, and the smallest such j is $\frac{d}{(k,d)}$, so that it is d if and only if $(k, d) = 1$, and there are $\varphi(d)$ such values for k. Since every integer $\in \{0, \ldots, n-1\}$ has an order which divides n, one deduces that $\sum_{d|n} \varphi(d) = n$.

Each element of order d generates a subgroup of order d, but all the $\varphi(d)$ such elements generates the same subgroup, because it is isomorphic to $\mathbb{Z}_d$, and $\mathbb{Z}_d$ has exactly $\varphi(d)$ generators.

Lemma 4.19: (Chinese remainder theorem) If $m_1, \ldots, m_k$ are pairwise relatively prime (so that the prime factors of m_i do not appear as prime factors of m_j for $j \neq i$), then any system of equation $x = a_i \pmod{m_i}$ for $i = 1, \ldots, k$ has exactly one solution defined modulo n, where $n = m_1 \cdots m_k$. In particular, $\varphi(n) = \varphi(m_1) \cdots \varphi(m_k)$.
Proof: For each $a \in \mathbb{Z}$, and each $i \in \{1, \ldots, k\}$, one associates the remainders a_i of the division of a by m_i, and then $a, b \in \mathbb{Z}$ have the same images if and only if $b - a$ is a multiple of m_i for all i, and this means that $b - a$ is a multiple of n. This shows that the mapping restricted to $\{0, \ldots, n-1\}$ is injective, but since the image belongs to the product $\{(a_1, \ldots, a_k) \mid 0 \leq a_i \leq m_i - 1, i = 1, \ldots, k\}$ which has n elements, it is also surjective.

An integer $a \in \mathbb{Z}$ is relatively prime with n if it has no common prime factors with n, which is that it has no common prime factors with any of the m_i, i.e. each a_i is relatively prime with m_i, and since there are $\varphi(m_i)$ such values of a_i, and there is an inverse mapping from the $a_i, i \in I$, to the solution x of the congruences in $\{0, \ldots, n-1\}$, the number of such a belonging to $\{0, \ldots, n-1\}$ is $\varphi(m_1) \cdots \varphi(m_k)$.

Definition 4.20: A mapping f from $\mathbb{N}^\times$ to $\mathbb{N}$ (or to $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$) is *multiplicative* if $f(a\,b) = f(a)\,f(b)$ whenever $(a, b) = 1$, and $f(1) = 1$.[18]

f is *completely multiplicative* if $f(a\,b) = f(a)\,f(b)$ for all a, b, and $f(1) = 1$.

Remark 4.21: The Euler function φ is multiplicative, and other multiplicative functions are used in number theory, but the basic observation is that given any list $a_{p,k}$ indexed on the primes p and the positive integers $k \geq 1$, there exists a unique multiplicative function f such that $f(p^k) = a_{p,k}$ for all primes p and all $k \geq 1$, since each n has a factorization $n = p_1^{k_1} \cdots p_r^{k_r}$, and one must have $f(n) = f(p_1^{k_1}) \cdots f(p_r^{k_r}) = a_{p_1,k_1} \cdots a_{p_r,k_r}$. Similarly, given any list a_p indexed on the primes, there exists a unique completely multiplicative function g such that $g(p) = a_p$ for all prime p, since one must have $g(n) = f(p_1)^{k_1} \cdots f(p_r)^{k_r} = a_{p_1}^{k_1} \cdots a_{p_r}^{k_r}$.

---

[17] So that e is replaced by 0, and $a^d = e$ is replaced by $d\,a = 0$. When working in $\mathbb{Z}_n$, one often switches from using equivalence classes or elements of $\mathbb{Z}$, so that $a = b$ is interpreted as $a = b \pmod{n}$ if $a, b \in \mathbb{Z}$.

[18] Often, $f(n)$ is only defined for $n \geq 2$ and satisfies $f(a\,b) = f(a)\,f(b)$ whenever $(a, b) = 1$ and $a, b \geq 2$, so that after defining $f(1) = 1$ it becomes true for $a, b \geq 1$. A basic example is to consider a polynomial $P \in \mathbb{Z}[x]$, i.e. having integer coefficients, and for $n \geq 2$ to define $f(n)$ as the number of solutions of $P(x) = 0$ modulo n, and the Chinese remainder theorem shows that for $a, b \geq 2$ and relatively prime one has $f(a\,b) = f(a)\,f(b)$.

Definition 4.22: A *primitive root modulo* n is any integer (when it exists) whose powers give (modulo n) all the integers relatively prime with n, i.e. it is a generator of the multiplicative group $\mathbb{Z}_n^*$ of units in $\mathbb{Z}_n$ (so that it cannot exist unless this group is cyclic).

Remark 4.23: Since for a prime p and $k \geq 1$ one has $\varphi(p^k) = p^k - p^{k-1}$ (because there are p^{k-1} multiples of p in $\{0, \ldots, p^k - 1\}$), one sees that besides $\varphi(2) = 1$, all other $\varphi(p^k)$ are even, so that Euler's theorem is not optimal if n has two distinct odd prime factors: for example, $\varphi(35) = \varphi(5)\,\varphi(7) = 4 \cdot 6 = 24$, but for a relatively prime with 35 one has $a^4 = 1 \pmod 5$ and $a^6 = 1 \pmod 7$, so that (12 being the lcm of 4 and 6) a^{12} is $= 1 \pmod 5$ and $= 1 \pmod 7$, hence $= 1 \pmod{35}$, and it means that in $\mathbb{Z}_{35}^*$ (which has 24 elements) all the orders of elements are divisors of 12, so that $\mathbb{Z}_{35}^*$ is not cyclic and there does not exist a primitive root modulo 35.

If a is odd one has $a^2 = 1 \pmod 8$, since $(2n+1)^2 = 4n\,(n+1) + 1$ and $n\,(n+1)$ is even, so that Euler's theorem is not optimal for $n = 8$. By induction, using $(1 + b\,2^j)^2 = 1 + c\,2^{j+1}$ with $c = b + b^2 2^{j-1}$ for $j \geq 1$, one deduces that $a^{2^{k-2}} = 1 \pmod{2^k}$ for $k \geq 3$, and since $2^{k-2} = \frac{\varphi(2^k)}{2}$, Euler's theorem is not optimal for $n = 2^k$ and $k \geq 3$. One deduces that the only possible values n for which a primitive root modulo n may exist are $n = 2, 4, p^k$, or $2p^k$ for an odd prime p and $k \geq 1$. Since $\mathbb{Z}_2^* = \{1\}$ a primitive root modulo 2 is 1, and since $\mathbb{Z}_4^* = \{1, 3\}$ with $3 \cdot 3 = 1 \pmod 4$ a primitive root modulo 4 is 3.

It was shown by LEGENDRE,[19] and by GAUSS that for each odd prime p a primitive root modulo p exists, so that $\mathbb{Z}_p^*$ (with multiplication) is cyclic, i.e. isomorphic to $\mathbb{Z}_{p-1}$ (with addition) and since $\mathbb{Z}_{p-1}$ has $\varphi(p-1)$ generators, there are actually $\varphi(p-1)$ primitive roots modulo p; however, the proof of existence is a counting argument which is not an algorithm, so that it does not tell how to find such a primitive root. An important ingredient in the proof (which will be shown later in the course) is that a polynomial of degree d with coefficients in a field (here $\mathbb{Z}_p$) cannot have more than d roots.[20] Starting from a primitive root a modulo an odd prime p, it will be shown how to construct a primitive root b modulo $n = p^k$, and a primitive root c modulo $2p^k$, so that the values of n for which $\mathbb{Z}_n^*$ is cyclic are $n = 2, 4, p^k$, or $2p^k$ for an odd prime p and $k \geq 1$; there are $\varphi\big(\varphi(n)\big)$ primitive roots modulo n for such values of n, and for $n = p^k$ or $2p^k$ one has $\varphi(n) = p^{k-1}(p-1)$, so that there are $p^{k-2}(p-1)\,\varphi(p-1)$ primitive roots modulo n.

It will also be shown later that for any field F, if G is a finite subgroup of the multiplicative group F^*, then G is cyclic; the proof involves degrees of elements, and the fact that a polynomial of degree d with coefficients in F cannot have more than d roots.

Additional footnotes: ADLEMAN,[21] RIVEST,[22] Adi SHAMIR,[23] WEIZMANN.[24]

---

[19] Adrien-Marie LEGENDRE, French mathematician, 1752–1833. He worked in Paris, France.

[20] We have seen that $x^2 = 1$ has 4 roots in $\mathbb{Z}_8$, but this happens because $\mathbb{Z}_8$ is not an ID (integral domain), since $2 \cdot 4 = 0$ in $\mathbb{Z}_8$).

[21] Leonard Max ADLEMAN, American computer scientist and biologist, born in 1945. He works at USC (University of Southern California), Los Angeles, CA. The RSA public key cryptography algorithm, which he introduced in 1977 with RIVEST and Adi SHAMIR, is partially named after him.

[22] Ronald Linn RIVEST, American cryptologist, born in 1947. The RSA public key cryptography algorithm, which he introduced in 1977 with A. SHAMIR and ADLEMAN, is partially named after him.

[23] Adi SHAMIR, Israeli cryptologist, born in 1952. He works at the Weizmann Institute of Science, Rehovot, Israel. The RSA public key cryptography algorithm, which he introduced in 1977 with RIVEST and ADLEMAN, is partially named after him.

[24] Chaim WEIZMANN, Russian-born chemist, 1874–1952. He was the first president of Israel, 1949–1952. The Weizmann Institute of Science, Rehovot, Israel, is named after him.

Luc TARTAR, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

5- Friday September 9, 2011.

Definition 5.1: If $(G_i, *_i, e_i), i \in I$, is a family of groups indexed by a non-empty set I, then the product $G = \prod_{i \in I} G_i$ has a structure of group, called the *direct product*, where the operation $*$ is defined by $a * b = \{a_i *_i b_i, i \in I\}$ for $a = \{a_i, i \in I\}$, $b = \{b_i, i \in I\}$.[1]

Remark 5.2: Of course, the structure described is that of a group, since $*$ is obviously associative, the identity element is $e = \{e_i, i \in I\}$, and the inverse of $a = \{a_i, i \in I\}$ is $a^{-1} = \{a_i^{-1}, i \in I\}$. The direct product is Abelian if and only if G_i is Abelian for all $i \in I$.[2]

If for each $i \in I$, the coordinate a_i has a finite order m_i in G_i, then if I is finite a has a finite order equal to the least common multiple of all the m_i, but if I is infinite this "least common multiple" could be infinite.

Lemma 5.3: If $m_1, \dots, m_k$ are pairwise relatively prime, then $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$ is isomorphic to $\mathbb{Z}_n$ with $n = m_1 \cdots m_k$.
Proof: The mapping which to $a \in \mathbb{Z}$ associates $(a_1, \dots, a_k)$, where a_i is (the equivalence class of) the remainder in the division of a by m_i for $i = 1, \dots, k$ is an homomorphism, and since two integers differing from a multiple of n have the same image, it defines an homomorphism from $\mathbb{Z}_n$ into $\mathbb{Z}_{m_1} \times \cdots \times \mathbb{Z}_{m_k}$; by the Chinese remainder theorem, this homomorphism is a bijection, so that it is an isomorphism.[3]

Remark 5.4: Comparing the orders of elements gives a simple way to show that two groups are not isomorphic.

$\mathbb{Z}_4$ and $\mathbb{Z}_2 \times \mathbb{Z}_2$ both have 4 elements, but they are not isomorphic: $\mathbb{Z}_4$ has 1 element of order 2 (which is 2) and 2 elements of order 4 (which are 1 and 3); $\mathbb{Z}_2 \times \mathbb{Z}_2$ has 3 elements of order 2 (which are $(0,1)$, $(1,0)$, and $(1,1)$) and 0 element of order 4.

Similarly, $\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ all have 8 elements, but no two of these groups are isomorphic: $\mathbb{Z}_8$ has 1 element of order 2 (which is 4), 2 elements of order 4 (which are 2 and 6), and 4 elements of order 8 (which are 1, 3, 5, and 7); $\mathbb{Z}_2 \times \mathbb{Z}_4$ has 3 elements of order 2 (which are $(0,2)$, $(1,0)$, and $(1,2)$), 4 elements of order 4 (which are $(0,1)$, $(0,3)$, $(1,1)$, and $(1,3)$), and 0 element of order 8; $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ has 7 elements of order 2 (which are all the elements different from the identity $(0,0,0)$), 0 element of order 4, and 0 element of order 8.

There are two non-Abelian groups of order 8, the *dihedral group* D_4, and the *quaternion group* Q_8,[4] which are not isomorphic (and not isomorphic to any of the three Abelian groups of order 8, of course).

D_4 is the group of symmetries of a square,[5] and it has 5 elements of order 2 (which are the four mirror symmetries, and R_{180}, the rotation of 180 degrees), 2 elements of order 4 (which are R_{90} and R_{270}, the rotations of 90 degrees and of 270 degrees), and 0 element of order 8.

$Q_8 = \{\pm 1, \pm \mathbf{i}, \pm \mathbf{j}, \pm \mathbf{k}\}$, with $\mathbf{i}^2 = \mathbf{j}^2 = \mathbf{k}^2 = -1$ and $\mathbf{i}\,\mathbf{j}\,\mathbf{k} = -1$,[6] and it has 1 element of order 2 (which is -1), 6 elements of order 4 (which are $\pm\mathbf{i}$, $\pm\mathbf{j}$, and $\pm\mathbf{k}$), and 0 element of order 8.

---

[1] In the case of rings, the direct product has a structure of rings, where the product is done coordinate by coordinate, but the product of two rings is never an integral domain, since $(0,1) \cdot (1,0) = (0,0)$; in particular, a product of fields is not a field.

[2] We shall see later in the course that in some cases one can put on $G_1 \times G_2$ another group structure, called a semi-direct product, and this semi-direct group can be non-Abelian even with G_1 and G_2 Abelian.

[3] If a bijection f from G_1 into G_2 is an homomorphism (with respect to group structures on G_1 and G_2), then the inverse f^{-1} is an homomorphism from G_2 into G_1: indeed, if $a, b \in G_2$, then $a = f(\alpha), b = f(\beta)$ for $\alpha = f^{-1}(a), \beta = f^{-1}(b) \in G_1$, and since $f(\alpha\,\beta) = f(\alpha)\,f(\beta) = a\,b$ one has $f^{-1}(a\,b) = \alpha\,\beta = f^{-1}(a)\,f^{-1}(b)$, showing that f^{-1} is an homomorphism.

[4] The relation with the division ring of quaternions (introduced by HAMILTON) is described below.

[5] For $n \geq 3$, the dihedral group D_n is the group of symmetries of a regular polygon with n sides, and it has $2n$ elements; D_3 is isomorphic to the symmetry group S_3, of permutations of 3 objects. The symmetry group S_n of permutations of n objects has order $n!$.

[6] This implies $\mathbf{i}\,\mathbf{j} = \mathbf{k} = -\mathbf{j}\,\mathbf{i}$, $\mathbf{j}\,\mathbf{k} = \mathbf{i} = -\mathbf{k}\,\mathbf{j}$, $\mathbf{k}\,\mathbf{i} = \mathbf{j} = -\mathbf{i}\,\mathbf{k}$.

Remark 5.5: Comparing the subgroups and their inclusions gives another (less simple) way to show that two groups are not isomorphic.

$\mathbb{Z}_4$ has 1 subgroup H of order 2, with $\{0\} \leq H \leq \mathbb{Z}_4$; $\mathbb{Z}_2 \times \mathbb{Z}_2$ has 3 subgroups H_1, H_2, H_3 of order 2, with $\{0\} \leq H_1, H_2, H_3 \leq \mathbb{Z}_2 \times \mathbb{Z}_2$, and no relation of order between H_1, H_2, and H_3.

$\mathbb{Z}_8$ has 1 subgroup H of order 2, and 1 subgroup K of order 4, with $\{0\} \leq H \leq K \leq \mathbb{Z}_8$.

$\mathbb{Z}_2 \times \mathbb{Z}_4$ has 3 subgroups or order 2, and 2 subgroups of order 4, so that there is (at least) one subgroup of order 2 which is not included in a subgroup of order 4, and the reason is that among the 3 elements of order 2 (which are $(0,2)$, $(1,0)$, and $(1,2)$), only 1 can be divided by 2 (i.e. $(0,2) = (0,1)+(0,1) = (0,3)+(0,3) = (1,1)+(1,1) = (1,3)+(1,3)$), and the subgroup $H_0 = \{(0,0),(0,2)\}$ is actually the intersection of the 2 subgroups K_1, K_2 of order 4 (with $K_1 = \{(0,0),(0,1),(0,2),(0,3)\}$ and $K_2 = \{(0,0),(1,1),(0,2),(1,3)\}$, which are isomorphic to $\mathbb{Z}_4$), and the other 2 subgroups H_1, H_2 of order 2 (with $H_1 = \{(0,0),(1,0)\}$ and $H_2 = \{(0,0),(1,2\}$) are not comparable, so that besides the relations $\{(0,0)\} \leq H_0 \leq K_1, K_2 \leq \mathbb{Z}_2 \times \mathbb{Z}_4$ one has $\{(0,0)\} \leq H_1, H_2 \leq \mathbb{Z}_2 \times \mathbb{Z}_4$.

$\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$ has 7 subgroups $H_1, \ldots, H_7$ of order 2, 0 subgroup of order 4, and $\{(0,0)\} \leq H_1, \ldots, H_7 \leq \mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$.

D_4 has 5 subgroups of order 2 (H_0 generated by R_{180}, and $H_1, \ldots, H_4$ generated by the 4 mirror symmetries), and 1 subgroup K of order 4 (generated by R_{90} or by R_{270}, and isomorphic to $\mathbb{Z}_4$), and one has $\{(0,0)\} \leq H_0 \leq K \leq D_4$ and $\{(0,0)\} \leq H_1, \ldots, H_4 \leq D_4$.

Q_8 has 1 subgroup H of order 2 (which is $\{+1,-1\}$) and 3 subgroups I, J, K of order 4 (with $I = \{\pm 1, \pm \mathbf{i}\}$, $J = \{\pm 1, \pm \mathbf{j}\}$, and $K = \{\pm 1, \pm \mathbf{k}\}$, isomorphic to $\mathbb{Z}_4$), and one has $\{(0,0)\} \leq H \leq I, J, K \leq Q_8$.

Remark 5.6: We shall see later a general structure property for finite Abelian groups, but for understanding about finite non-Abelian groups, we shall need some general tools, like Cauchy's theorem and its generalizations, the Sylow's theorems,[5] and learn about group actions.

Definition 5.7: If p is prime, and a is not a multiple of p, then a is a *quadratic residue modulo p* if there exists $x \in \mathbb{Z}$ with $x^2 = a \pmod{p}$, and it is a *quadratic non-residue modulo p* if there does not exist such an x. The *Legendre symbol* $\left(\frac{a}{p}\right)$ is only defined for p prime and a not a multiple of p,[6] as $+1$ if a is a quadratic residue modulo p, and as -1 if a is a quadratic non-residue modulo p. One obviously has $\left(\frac{b}{p}\right) = \left(\frac{a}{p}\right)$ if $b = a \pmod{p}$, and $\left(\frac{a^2}{p}\right) = +1$ (for a not a multiple of p).

Remark 5.8: It seems natural to have wondered about solving equations of degree 2, but one should remember that thinking in terms of equations modulo n was initiated by Gauss, so that the initial motivation of mathematicians was certainly different.

The formula $(a^2+b^2)(\alpha^2+\beta^2) = (a\,\alpha - b\,\beta)^2 + (a\,\beta + b\,\alpha)^2$ is now known as Brahmagupta's identity,[7] and it is related to complex numbers since it says that $|z_1 z_2|^2 = |z_1|^2 |z_2|^2$ for all $z_1, z_2 \in \mathbb{C}$. Girard conjectured that a positive integer is the sum of two squares if and only if its factorization has the primes of the form $4m+3$ at an even power,[8] and Fermat claimed to have a proof (using his method of descent to show that every prime of the form $4m+1$ is the sum of two squares), but Euler was the first to publish a proof. If an odd prime p can be written as $a^2 + b^2$, it implies (by multiplying by the inverse of a modulo p) that -1 is a quadratic residue modulo p, and the first step was to show that it is not true if p is of the form $4n+3$ (or $4n-1$), and it is true if p is of the form $4n+1$.

Theorem 5.9: (Euler) If p is an odd prime, then for a not a multiple of p one has $a^{\frac{p-1}{2}} = \left(\frac{a}{p}\right) \pmod{p}$, so that -1 is a quadratic residue modulo p if and only if $\frac{p-1}{2}$ is even, i.e. p has the form $4n+1$, and $\left(\frac{a\,b}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ for all a, b not multiples of p.

---

[5] Peter Ludwig Mejdell Sylow, Norwegian mathematician, 1832–1918. After being a high school teacher in Fredrikshald (now Halden), he worked in Kristiania (now Oslo), Norway.

[6] Jsevenrm ACOBI has extended the definition of the Legendre symbol to $\left(\frac{a}{n}\right)$ with a and n non-zero integers; however, although $\left(\frac{a}{n}\right) = -1$ implies that there is no solution of $x^2 = a \pmod{n}$, one cannot conclude if n is not a prime and $\left(\frac{a}{n}\right) = +1$.

[7] Brahmagupta, Indian mathematician and astronomer, 598–670.

[8] Albert Girard, French mathematician, 1595–1632.

Proof: Since $p = 2m+1$, and $a^{2m} = 1 \pmod p$ by Fermat's theorem, it means that $a^m = \pm 1 \pmod p$, because $\mathbb{Z}_p$ is a field.[9] Every square $a = x^2$ (with $x \neq 0 \pmod p$) satisfies $a^m = 1 \pmod p$ since $(x^2)^m = x^{p-1} = 1 \pmod p$ by Fermat's theorem, and since $-x$ and x have the same square (and $-x \neq x \pmod p$ since p is odd) there are exactly m non-zero squares modulo p; because the polynomial equation $x^m = 1 \pmod p$ cannot have more than m distinct solutions since $\mathbb{Z}_p$ is a field,[10] one knows all of them and they are the quadratic residues modulo p which are those a satisfying $\left(\frac{a}{p}\right) = +1$, and the quadratic non-residues modulo p are those b satisfying $\left(\frac{b}{p}\right) = -1$. Applying to $a = -1$, one finds that $\left(\frac{-1}{p}\right) = +1$ if and only if $\frac{p-1}{2}$ is even. Then one has $\left(\frac{a\,b}{p}\right) = (a\,b)^{\frac{p-1}{2}} = a^{\frac{p-1}{2}}\,b^{\frac{p-1}{2}} = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p$, and since the Legendre symbol only take the values ± 1 (and $p \neq 2$) one deduces that $\left(\frac{a\,b}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \pmod p$.

Remark 5.10: One then has a surprising result, that if $x^2 = a \pmod p$ has no solution x, and $y^2 = b \pmod p$ has no solution y, then there exists a solution z of $z^2 = a\,b \pmod p$, but the proof has given no algorithm for finding such a solution.

For going further, one needs to compute $\left(\frac{2}{p}\right)$ (by a lemma of GAUSS), and prove the law of quadratic reciprocity, which says that if p and q are distinct odd primes, then $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$ if either p or q has the form $4n+1$, and that $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$ if both p and q have the form $4n+3$: it was conjectured by LEGENDRE and EULER could not prove it, but GAUSS published six different proofs (and two more were found in his papers after he died). However, one difficulty with computing Legendre symbols is that one needs to know the factorization into prime factors of the numbers which one uses.

Remark 5.11: Using the *scalar product* (V,W) and the *cross product* $V \times W$ for vectors $V, W \in \mathbb{R}^3$,[11] HAMILTON wanted to define an associative multiplication which is distributive with respect to addition,[12] and he found a way with pairs of a scalar and a vector: it is natural to define addition as $(a,V)+(\alpha,W) = (a+\alpha, V+W)$, and his unusual multiplication is $(a,V)\cdot(\alpha,W) = (a\,\alpha-(V,W), a\,W+\alpha\,V+V\times W)$: distributivity with respect to addition is clear, and associativity follows easily from the formula for the double cross product, $V\times(W\times X) = (V,X)\,W-(V,W)\,X$. Using the notation $\mathbf{i}$, $\mathbf{j}$, and $\mathbf{k}$ for the canonical (orthonormal) basis of $\mathbb{R}^3$, and b,c,d for the components of a vector $V \in \mathbb{R}^3$, one then writes $\mathbb{H} = \{a+b\,\mathbf{i}+c\,\mathbf{j}+d\,\mathbf{k} \mid a,b,c,d \in \mathbb{R}\}$; an element $a+b\,\mathbf{i}+c\,\mathbf{j}+d\,\mathbf{k}$ is called a *quaternion*. One checks easily that $\mathbf{i}\cdot\mathbf{i} = \mathbf{j}\cdot\mathbf{j} = \mathbf{k}\cdot\mathbf{k} = -1$ and $\mathbf{i}\cdot\mathbf{j} = \mathbf{k} = -\mathbf{j}\cdot\mathbf{i}$, $\mathbf{j}\cdot\mathbf{k} = \mathbf{i} = -\mathbf{k}\cdot\mathbf{j}$, $\mathbf{k}\cdot\mathbf{i} = \mathbf{j} = -\mathbf{i}\cdot\mathbf{k}$. One writes $N\big((a,V)\big) = a^2+|V|^2$, or $N(a+b\,\mathbf{i}+c\,\mathbf{j}+d\,\mathbf{k}) = a^2+b^2+c^2+d^2$, called the *norm* of the quaternion,[13] and has $N\big((a,V)\cdot(\alpha,W)\big) = N\big((a,V)\big)\,N\big((\alpha,W)\big)$, i.e. $(a^2+b^2+c^2+d^2)\,(\alpha^2+\beta^2+\gamma^2+\delta^2) = (a\,\alpha-b\,\beta-c\,\gamma-d\,\delta)^2+(a\,\beta+b\,\alpha+c\,\delta-d\,\gamma)^2+(a\,\gamma-b\,\delta+c\,\alpha+d\,\beta)^2+(a\,\delta+b\,\gamma-c\,\beta+d\,\alpha)^2$, attributed to EULER, and it may have been known to BACHET, who conjectured that every positive integer is the sum of four squares; FERMAT claimed to have a proof, but LAGRANGE was the first to publish a proof. If $N\big((a,V)\big) \neq 0$, the multiplicative inverse of (a,V) is $\lambda\,(a,-V)$, with $\lambda\,N\big((a,V)\big) = 1$, so that $\mathbb{H}$ is a division ring.

The quaternion group Q_8 is then a subgroup of the multiplicative group $\mathbb{H}^* = \mathbb{H}\setminus\{(0,0)\}$, obtained by imposing $a \in \mathbb{Z}$ and $V \in \mathbb{Z}^3$, which gives a set stable by multiplication, and imposing $N\big((a,V)\big) = 1$, for the inverse to have also its components in $\mathbb{Z}$: then only one component a,b,c,d is non-zero, and equal to ± 1.

Additional footnotes: JACOBI.[14]

---

[9] Since $z = a^m$ satisfies $z^2 = 1$, and $z^2-1 = (z-1)\,(z+1)$ can only be 0 if $z-1$ or $z+1$ is 0.

[10] For any commutative ring R, one notes $R[x]$ the polynomials with coefficients in R, and if $P(x)$ is such a polynomial of degree $n \geq 1$, and $a \in R$, one can perform the Euclidean division of $P(x)$ by $x-a$, which gives $P(x) = (x-a)\,Q(x)+P(a)$ with Q of degree $n-1$; one deduces that $P(a) = 0$ if and only if P is divisible par $x-a$. If R is an integral domain and $P(b) = 0$ for $b \neq a$, then $Q(b) = 0$, and one divides Q by $x-b$, and by induction on n there cannot exist more than n distinct roots of P.

[11] For $i = 1,2,3$, the component $(V\times W)_i$ is $\sum_{j,k}\varepsilon_{i,j,k}V_jW_k$, where ε is the *completely antisymmetric tensor*, such that $\varepsilon_{i,j,k} = 0$ if two indices coincide, and if they are distinct it is the signature of the permutation $(1,2,3) \mapsto (i,j,k)$, i.e. $\varepsilon_{1,2,3} = \varepsilon_{2,3,1} = \varepsilon_{3,1,2} = +1$, and $\varepsilon_{1,3,2} = \varepsilon_{2,1,3} = \varepsilon_{3,2,1} = -1$.

[12] Sir William Rowan HAMILTON, Irish mathematician, 1805–1865. He worked in Dublin, Ireland.

[13] In analysis, the norm would be the square root of $a^2+b^2+c^2+d^2$.

[14] Carl Gustav Jacob JACOBI, German mathematician, 1804–1851. He worked in Königsberg (then in Germany, now Kaliningrad, Russia) and Berlin, Germany.

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

6- Monday September 12, 2011.

Remark 6.1: If $P \in \mathbb{Z}[x]$, i.e. if P is a polynomial with integer coefficients, then $P(a) \in \mathbb{Z}$ for all $a \in \mathbb{Z}$, and it is easy to see that if P has an integer root a, i.e. $P(a) = 0$, then a divides the constant coefficient, which is $P(0)$, but such an argument does not work if one looks for solutions modulo n for some $n \geq 2$. If for $n \geq 2$, one defines $f(n)$ as the number of solutions in $\mathbb{Z}_n$ of the equation $P(a) = 0 \pmod{n}$, then the Chinese remainder theorem shows that $f(m\,n) = f(m)\,f(n)$ whenever m and n are relatively prime (and ≥ 2), so that by defining $f(1) = 1$ one deduces that f is a multiplicative function.

Remark 6.2: Before the Euler function φ, other particular multiplicative functions had been introduced in number theory, like $\sigma_k(n) = \sum_{d|n} d^k$, so that $\sigma_0(n)$ is the number of divisors of n, and $\sigma_1(n)$ is the sum of divisors of n (including n), which appears in the definition of a *perfect number* n, which is equal to the sum of its proper divisors, i.e. such that $\sigma_1(n) = 2n$. It was noticed early that 6 and 28 are perfect, and EUCLID observed that if $p = 2^m - 1$ is prime, then $2^{m-1}(2^m - 1)$ is a perfect number,[1] but such primes are now called *Mersenne primes*.[2] The next two perfect numbers are 496 $(16 \cdot 31)$ and 8 128 $(64 \cdot 127)$, noticed by NICOMACHUS,[3] and the next is 33 550 336, which was recorded in 1456 by an unknown mathematician, and then CATALDI found the next two (8 589 869 056 and 137 438 691 328) in 1588.[4]

It is not known if there are infinitely many Mersenne primes, and the first 40 correspond to m equal to 2, 3, 5, 7, 13, 17, 19,[5] 31,[6] 61, 89, 107, 127, 521, 607, 1 279, 2 203, 2 281, 3 217, 4 253, 4 423, 9 689, 9 941, 11 213, 19 937, 21 701, 23 209, 44 497, 86 243, 110 503, 132 049, 216 091, 756 839, 859 433, 1 257 787, 1 398 269, 2 976 221, 3 021 377, 6 972 593, 13 466 917, 20 996 011, and it is not clear what the next value of m is, but 7 more are known (24 036 583, 25 964 951, 30 402 457, 32 582 657, 37 156 667, 42 643 801, 43 112 609). ALHAZEN (Ibn al-Haytham) conjectured that every even perfect number has the form used by EUCLID,[7] and this was proved by EULER.[8]

It is not known if there exist odd perfect numbers.

Definition 6.2: For two mappings f, g from $\mathbb{N}^\times$ into $\mathbb{Z}$ (or $\mathbb{Q}$, $\mathbb{R}$, or $\mathbb{C}$) one defines $h = f \star g$ by $h(n) = \sum_{d|n} f(d)\,g\big(\frac{n}{d}\big)$.

---

[1] Since $\sigma_1(2^{m-1}) = 1 + 2 + \ldots + 2^{m-1} = 2^m - 1$, and for p prime $\sigma_1(p) = p + 1$, then $2^{m-1}p$ perfect means $(2^m - 1)\,(p + 1) = 2^m p$, i.e. $p = 2^m - 1$.

[2] Marin MERSENNE, French mathematician, 1588–1648. Mersenne primes numbers (of the form $2^k - 1$) are named after him.

[3] NICOMACHUS of Gerasa (now Jarash, Jordan), Greek mathematician, 60–120.

[4] Pietro Antonio CATALDI, Italian mathematician, 1548–1626. He worked in Perugia and in Bologna, Italy.

[5] CATALDI proved that $2^{19} - 1$ is prime by dividing it by all the primes up to its square root, so that he first computed all the primes up to 750.

[6] EULER first showed that all prime divisors of $2^{31} - 1$ must have the form $248n + 1$ or $248n + 63$, and then he divided $2^{31} - 1$ by all such primes less than 46 339: since 31 is prime it is the order of 2 in $\mathbb{Z}_p^*$, so that 31 divides $p - 1$, and since $p - 1$ is even, one has $p = 62r + 1$ for some r; since $2^{32} = 2 \pmod{p}$, 2 is a quadratic residue modulo p, which means that $p = \pm 1 \pmod{8}$, and $p = 8s + 1$ implies $r = 4n$, while $p = 8s - 1$ implies $r = 4n + 1$, hence the forms $248n + 1$ or $248n + 63$ for p. EULER had used the same argument for showing that $F_5 = 2^{32} + 1$ is not prime: if p is an odd prime divisor of F_5, 2 has order 64 in $\mathbb{Z}_p^*$ (since the order divides 64 but does not divide 32), so that $p = 64a + 1$, and then by restricting the trials to such primes he found that 641 is a divisor of F_5; actually, since 2 is a quadratic residue modulo p (because $p = 1 \pmod{8}$), one has $2 = b^2 \pmod{p}$, then b has order 128 in $\mathbb{Z}_p^*$, so that p has the form $128c + 1$.

[7] ALHAZEN (Abu 'Ali al-Hasan ibn al-Hasan ibn al-Haytham), Persian mathematician, 965–1040.

[8] If $2^k M$ is perfect with $k \geq 1$ and M odd, then $\sigma_1(2^k M) = (2^{k+1} - 1)\,\sigma_1(M) = 2^{k+1} M$, so that $2^{k+1} - 1$ divides M, so that $M = (2^{k+1} - 1)\,r$ and $\sigma_1(M) = 2^{k+1} r$; $r = 1$ gives $\sigma_1(M) = 2^{k+1} = M + 1$, hence M must be prime; $r > 1$ implies $\sigma_1(M) \geq 1 + r + M$, which is $1 + 2^{k+1}\,r$, a contradiction.

Remark 6.3: That $\star$ is commutative is seen by replacing d by $\frac{n}{d}$, or by writing in a symmetric way $h(n) = \sum_{d_1 d_2 = n} f(d_1)\, g(d_2)$. Then $(f \star g) \star k = \ell$ means $\ell(n) = \sum_{d_1 d_2 d_3 = n} f(d_1)\, g(d_2)\, k(d_3)$, which is also the formula for $f \star (g \star k)$, so that $\star$ is associative. There is an identity element δ defined by $\delta(1) = 1$ and $\delta(n) = 0$ for $n \geq 2$.

In analysis, $\star$ is the symbol for convolution, which here is related to using the multiplicative group $\mathbb{R}_+$ and its Haar measure $\frac{dt}{t}$:[9] for continuous functions with compact support in $(0, \infty)$, $h = f \star g$ means $h(x) = \int_0^\infty f(s)\, g\big(\frac{t}{s}\big)\, \frac{ds}{s}$, but in order to deduce Definition 6.2, one must let the continuous functions approach combination of Dirac masses at the integer points.[10]

Lemma 6.4: If f and g are multiplicative functions, then $f \star g$ is multiplicative, and the set of multiplicative functions with $\star$ (and δ as identity) is a group.
Proof: For a_1 and a_2 relatively prime (so that they have different prime factors), and d a divisor of $a_1 a_2$, one has a unique decomposition as $d = d_1 d_2$ where d_1 is a divisor of a_1 and d_2 is a divisor of a_2. Then $h(a_1 a_2) = \sum_{d | a_1 a_2} f(d)\, g\big(\frac{a_1 a_2}{d}\big) = \sum_{d_1 | a_1, d_2 | a_2} f(d_1 d_2)\, g\big(\frac{a_1 a_2}{d_1 d_2}\big)$, but since $f(d_1 d_2) = f(d_1)\, f(d_2)$ and $g\big(\frac{a_1 a_2}{d_1 d_2}\big) = g\big(\frac{a_1}{d_1}\big)\, g\big(\frac{a_2}{d_2}\big)$, one has $h(a_1 a_2) = \sum_{d_1 | a_1, d_2 | a_2} f(d_1)\, f(d_2)\, g\big(\frac{a_1}{d_1}\big)\, g\big(\frac{a_2}{d_2}\big)$, which is $\sum_{d_1 | a_1} f(d_1)\, g\big(\frac{a_1}{d_1}\big)$ times $\sum_{d_2 | a_2} f(d_2)\, g\big(\frac{a_2}{d_2}\big)$ i.e. $h(a_1)\, h(a_2)$.

For constructing the inverse of f, one looks for a multiplicative function ψ such that $f \star \psi(p^k) = \delta(p^k)$ for all primes p and all $k \geq 1$, and one checks that it characterizes all the values of $\psi(p^k)$, and there is a unique extension to all values $n \in \mathbb{N}^\times$, and the product $f \star \psi$ is then a multiplicative function taking the same values than δ on the powers of primes, so that it is δ. For doing this, one first takes $\psi(1) = 1$, so that $f \star \psi(1) = 1 = \delta(1)$; then $f \star \psi(p) = \delta(p) = 0$ gives $\psi(p) + f(p) = 0$, so that $\psi(p)$ is defined (and belongs to $\mathbb{Z}$ if f takes its values in $\mathbb{Z}$); $f \star \psi(p^2) = \delta(p^2) = 0$ gives $\psi(p^2) + f(p)\, \psi(p) + f(p^2) = 0$, so that $\psi(p^2)$ is defined (and belongs to $\mathbb{Z}$ if f takes its values in $\mathbb{Z}$), and by induction one deduces that all the values $\psi(p^k)$ are characterized.

Definition 6.5: The multiplicative function μ defined by $\mu(1) = 1$ and, for each prime p, $\mu(p) = -1$ and $\mu(p^k) = 0$ for $k \geq 2$ is the *Möbius function*.[11]

Remark 6.6: Apart from $n = 1$, one has $\mu(n) \neq 0$ only if n is square-free, i.e. $n = p_1 \cdots p_k$ for distinct primes, in which case $\mu(n) = (-1)^k$.

Lemma 6.7 (Möbius's inversion formula) If for any function f one defines F by $F(n) = \sum_{d | n} f(d)$ for all n, then one has $f(n) = \sum_{d | n} \mu(d)\, F\big(\frac{n}{d}\big)$.
Proof: If one defines $\mathbf{1}$ by $\mathbf{1}(n) = 1$ for all n, so that $\mathbf{1}$ is completely multiplicative, then one checks that $\mu \star \mathbf{1}(1) = 1$ and $\mu \star \mathbf{1}(p^k) = 0$ for all primes p and all $k \geq 1$, so that $\mu \star \mathbf{1} = \delta$. Then the formula defining F is precisely $F = \mathbf{1} \star f$, so that $\mu \star F = \mu \star (\mathbf{1} \star f) = (\mu \star \mathbf{1}) \star f = \delta \star f = f$, which is Möbius's inversion formula.

Remark 6.8: The "Riemann" *zeta function*, defined by $\zeta(s) = \sum_{n=1}^\infty \frac{1}{n^s}$ was introduced by EULER in his thesis, and he observed that it factorizes as $\prod_p \frac{1}{1 - \frac{1}{p^s}}$, where the product is indexed by primes, but EULER lived much before CAUCHY had properly defined the notions of convergence of series of functions, and the definition of holomorphic or meromorphic functions of a complex variable z, so that such questions concerning the zeta function were not done by EULER but by RIEMANN; besides the obvious fact that the series converges uniformly if $\Re(s) > 1$, he showed that the zeta function can be extended analytically to the whole complex plane except for a simple pole at $s = 1$ (where $\zeta(s)$ behave as $\frac{1}{s-1}$), and that this meromorphic

[9] Alfréd HAAR, Hungarian mathematician, 1885–1933. He worked at Georg-August-Universität, Göttingen, Germany, in Kolozsvár (then in Hungary, now Cluj-Napoca, Romania), in Budapest and in Szeged, Hungary.

[10] Paul Adrien Maurice DIRAC, English physicist, 1902–1984. He received the Nobel Prize in Physics in 1933, jointly with Erwin SCHRÖDINGER, for the discovery of new productive forms of atomic theory. He worked in Cambridge, England, holding the Lucasian chair (1932–1969).

[11] August Ferdinand MÖBIUS, German mathematician, 1790–1868. He worked in Leipzig, Germany. The Möbius function and the Möbius inversion formula are named after him. The "Möbius" strip is also named after MÖBIUS, but it was introduced before him by LISTING.

function satisfies a functional equation $\zeta(s) = 2^s \pi^{s-1} \sin\left(\frac{\pi\, s}{2}\right) \Gamma(1-s)\, \zeta(1-s)$, or more symmetrically $\Gamma\left(\frac{s}{2}\right) \pi^{-s/2} \zeta(s) = \Gamma\left(\frac{1-s}{2}\right) \pi^{-(1-s)/2} \zeta(1-s)$, where the *Gamma function* is given by $\Gamma(z) = \int_0^{+\infty} t^{-z} e^{-t}\, dt$ (introduced by EULER) and satisfies $\Gamma(z+1) = z\, \Gamma(z)$ and $\Gamma(n) = (n-1)!$ for all $n \in \mathbb{N}^\times$. Besides "trivial zeros" at $-2, -4, \ldots$, the zeros of the zeta function lie in the *critical strip* $0 < \Re(s) < 1$ and the *Riemann hypothesis* is a conjecture by RIEMANN that they all lie on the line $\Re(s) = \frac{1}{2}$: there is a one million dollar Clay Prize for proving (or disproving) this conjecture.[12]

Remark 6.9: DIRICHLET generalized such remarks by associating to a function f its *Dirichlet series* $F(s) = \sum_{n=1}^{\infty} \frac{f(n)}{n^s}$;[13] if f satisfies a growth estimate $|f(n)| \leq A\, n^\alpha$ for all $n \in \mathbb{N}^\times$ with $\alpha \geq 0$, then $F(s)$ is well defined for $\Re(s) > \alpha + 1$ with a bound $|F(s)| \leq A\, \frac{\Re(s)-\alpha}{\Re(s)-\alpha-1}$.[14]

If g satisfies a growth estimate $|g(n)| \leq B\, n^\alpha$ for all $n \in \mathbb{N}^\times$ with $\alpha \geq 0$, then the Dirichlet series $G(s)$ is well defined for $\Re(s) > \alpha + 1$ with a bound $|G(s)| \leq B\, \frac{\Re(s)-\alpha}{\Re(s)-\alpha-1}$, and if $h = f \star g$, then it satisfies the growth estimate $|h(n)| \leq A\, B\, n^\alpha \sigma_0(n)$ for all $n \in \mathbb{N}^\times$,[15] and its Dirichlet series is $H(s) = F(s)\, G(s)$ in the region $\Re(s) > \alpha + 1$,[16] with the bound $|H(s)| \leq A\, B\, \frac{(\Re(s)-\alpha)^2}{(\Re(s)-\alpha-1)^2}$.

If f is multiplicative and satisfies $|f(n)| \leq n^\alpha$ for all $n \in \mathbb{N}^\times$ with $\alpha \geq 0$, then for $\Re(s) > \alpha + 1$ the Dirichlet series $F(s)$ can be written as an *Euler product* $\prod_p F_p(s)$ over the primes, where $F_p(s) = \sum_{k \geq 0} \frac{f(p^k)}{p^{k\, s}}$, so that $|F_p(s)| \leq \frac{1}{1-p^{\alpha-s}}$ and the product is uniformly convergent.

In particular, the Dirichlet series $M(s) = \sum_{n \geq 1} \frac{\mu(n)}{n^s}$ (uniformly convergent in $\Re(s) > 1$) associated to the Möbius function is $\frac{1}{\zeta(s)}$, so that the Riemann hypothesis is equivalent to the conjecture that $M(s)$ extends to an holomorphic function in $\Re(s) > \frac{1}{2}$.

The Dirichlet series $\Phi(s) = \sum_{n \geq 1} \frac{\varphi(n)}{n^s}$ (uniformly convergent in $\Re(s) > 2$) associated to the Euler function is $\frac{\zeta(s-1)}{\zeta(s)}$.

Additional footnotes: GREEN,[17] LISTING,[18] LUCAS H.,[19] PERSE,[20] SCHRÖDINGER.[21]

---

[12] Landon Thomas CLAY, American investment banker and philanthropist, born in 1926.

[13] Johann Peter Gustav LEJEUNE DIRICHLET, German mathematician, 1805–1859. He worked in Breslau (then in Germany, now Wrocław, Poland), in Berlin, and at Georg-August-Universität, Göttingen, Germany. Dirichlet series, and the Dirichlet conditions are named after him. The Dirichlet principle was named after DIRICHLET by RIEMANN, who was probably unaware that GAUSS and GREEN had used the same idea before him.

[14] By comparing a series with an integral: if ψ is a positive non-increasing function, then $\int_1^\infty \psi(x)\, dx \leq \sum_{n=1}^\infty \psi(n) \leq \psi(1) + \int_1^\infty \psi(x)\, dx$.

[15] Since each term $f(d) g\left(\frac{n}{d}\right)$ is bounded in absolute value by $A\, d^\alpha B\, \frac{n^\alpha}{d^\alpha} = A\, B\, n^\alpha$, and there are $\sigma_0(n)$ divisors d of n.

[16] For $\Re(s) > \alpha + 1$ one can make the product of the two series giving $F(s)$ and $G(s)$ and sum it in any way one likes, so that by pairing the terms in $f(d_1) g(d_2)$ corresponding to a value $d_1 d_2 = n$, the Dirichlet series for h appears.

[17] George GREEN, English mathematician, 1793–1841. He was a miller, and he wrote interesting articles before starting studying at Cambridge, at age 40; he received a Perse fellowship at Cambridge, England, but he did not live long afterward.

[18] Johann Benedict LISTING, German mathematician, 1808–1882. He worked at Georg-August-Universität, Göttingen, Germany. He introduced the "Möbius" strip before MÖBIUS.

[19] Reverend Henry LUCAS, English clergyman and philanthropist, 1610–1663. The Lucasian chair in Cambridge, England, is named after him.

[20] Stephen PERSE, English philanthropist, 1548–1615.

[21] Erwin Rudolf Josef Alexander SCHRÖDINGER, Austrian-born physicist, 1887–1961. He received the Nobel Prize in Physics in 1933, jointly with Paul Adrien Maurice DIRAC, for the discovery of new productive forms of atomic theory. He worked in Vienna, Austria, in Jena and in Stuttgart, Germany, in Breslau (then in Germany, now Wrocław, Poland), in Zürich, Switzerland, in Berlin, Germany, in Oxford, England, in Graz, Austria, and in Dublin, Ireland.

Luc TARTAR, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

7- Wednesday September 14, 2011.

Remark 7.1: When one has an equivalence relation $\mathcal{R}$ on a set X, it defines a partition of X into equivalence classes and a quotient set $X/\mathcal{R}$ whose elements are the equivalence classes, and there is a natural (surjective) *projection* π from X onto $X/\mathcal{R}$ which to $x \in X$ associates its equivalence class $\pi(x) = \{y \in X \mid y\,\mathcal{R}\,x\}$. If a mapping f from X into a set Y has the property that $x\,\mathcal{R}\,y$ implies $f(x) = f(y)$, then it defines a mapping $\overline{f}$ from $X/\mathcal{R}$ into Y defined by $\overline{f}\big(\pi(x)\big) = f(x)$ for all $x \in X$,[1] and one has $f = \overline{f} \circ \pi$.

If G is a group, what kind of equivalence relation $\mathcal{R}$ can one put on G so that the quotient set $G/\mathcal{R}$ is a group and π is an homomorphism? The kernel of π should be a normal subgroup, and since $x\,\mathcal{R}\,y$ means $\pi(x) = \pi(y)$, or equivalently $\pi(x\,y^{-1}) = e$, i.e. $x\,y^{-1} \in N$, the equivalence class of x is the coset $N\,y$, which by the normality of N is equal to $y\,N$.

Said otherwise, suppose that H is a subgroup of G and one wonders if one can define an operation on cosets $x\,H$ by deciding that for making the product of $a\,H$ by $b\,H$, one picks an element $x \in a\,H$, an element $y \in b\,H$ and the product is the coset containing $x\,y$: it only makes sense if this coset is independent of the choice of x and y, and since a particular choice is $x = a, y = b$, one must be sure that $x = a\,h_1, y = b\,h_2$ implies $x\,y = a\,b\,h_3$ (with $h_1, h_2, h_3 \in H$, as suggested by the choice of notation, but the quantifiers are 'for all h_1, h_2 there exists h_3')); since $a\,h_1\,b\,h_2 = a\,b\,h_3$ is equivalent to $h_1 b = b\,h_3 h_2^{-1}$, it means that $b\,H = H\,b$, and because b is arbitrary, H must be a normal subgroup of G.

Definition 7.2: If G is a group and N is a normal subgroup of G, one denotes G/N the *quotient group* defined by the operation $(a\,N)\,(b\,N) = (a\,b)\,N$.

Lemma 7.3: (first isomorphism theorem for groups) If ψ is an homomorphism of a group G_1 into a group G_2, then $\psi(G_1)$ is subgroup of G_2 which is isomorphic to $G_1/\psi^{-1}(\{e\})$.
Proof: It was shown before that $\psi(G_1)$ is a subgroup of G_2 (and it follows from $\psi(a)\,\psi(b) = \psi(a\,b)$), and that $\psi^{-1}(e)$ is a normal subgroup of G_2, so that since $\psi(a) = \psi(b)$ whenever $\pi(a) = \pi(b)$ there is a factorization $\psi = \overline{\psi} \circ \pi$, where $\overline{\psi}$ is an homomorphism from $G_1/\psi^{-1}(e)$ into G_2, which is injective (since its kernel is the identity of the quotient group), and it becomes surjective if one considers it as an homomorphism from $G_1/\psi^{-1}(e)$ onto $\psi(G_1)$, so that it then is a bijection, hence an isomorphism between these two groups.

Remark 7.4: The same approach works for a *ring* R (even without imposing the existence of an identity for multiplication, which one then denotes 1),[2] which is an Abelian group (with operation noted $+$, identity noted 0, and inverse noted $-$) with an associative multiplication written without a symbol, which is distributive with respect to addition on both sides, i.e. $a\,(b + c) = a\,b + a\,c$ and $(a + b)\,c = a\,c + b\,c$ for all $a, b, c \in R$. One then defines an *ideal* J as any subgroup of R which has the property that for all $r \in R$ and all $j \in J$, both $r\,j$ and $j\,r$ belong to J.[3]

One then defines a *ring-homomorphism* ψ from a ring R_1 into a ring R_2 as a mapping satisfying $f(a+b) = f(a) + f(b)$ and $f(a\,b) = f(a)\,f(b)$ for all $a, b \in R_1$, so that it is an homomorphism of groups, and the kernel of f is $f^{-1}(\{0\}) = \{a \in R_1 \mid f(a) = 0\}$, which is a subgroup of R (automatically normal since R is Abelian), but the kernel is actually an ideal of R_1 since $f(j) = 0$ implies $f(r\,j) = f(r)\,f(j) = 0$ and $f(j\,r) = f(j)\,f(r) = 0$ for all $r \in R_1$.

An equivalence relation $\mathcal{R}$ on a ring R is adapted to the ring structure if the quotient $R/\mathcal{R}$ is a ring and the projection π is a ring-homomorphism, so that the kernel of π (which is the inverse image of $\{0\}$) is an ideal J of R, and then $\pi(x) = \pi(y)$ means $\pi(x - y) = 0$, i.e. $y \in x + J$, but since $\pi(a\,b) = \pi(a)\,\pi(b)$ it means that $(a + j_1)\,(b + j_2) = a\,b + j_3$ (with $j_1, j_2, j_3 \in J$, as suggested by the choice of notation, but the

[1] For the definition to make sense, it is necessary that $\pi(x) = \pi(y)$ implies $f(x) = f(y)$, which is precisely the hypothesis made, since $\pi(x) = \pi(y)$ is equivalent to $x\,\mathcal{R}\,y$.

[2] Some authors call a *rng* (i.e. ring without the letter i) such a ring without an identity for multiplication.

[3] An ideal is also called a *two-sided ideal*, because one defines a *left ideal* as any subgroup $J \leq R$ with the property that for all $r \in R$ and all $j \in J$, $r\,j \in J$, and a *right ideal* as any subgroup $J \leq R$ with the property that for all $r \in R$ and all $j \in J$, $j\,r \in J$.

quantifiers are 'for all j_1, j_2 there exists j_3), so that by taking $j_1 = 0$ one finds that $a\,j_2 \in J$ and by taking $j_2 = 0$ one finds that $j_1 b \in J$, and since a, b are arbitrary in R and j_1, j_2 are arbitrary in J, one deduces that J is an ideal.

Said otherwise, suppose that H is a subgroup of R (for addition) and one wonders if one can define a multiplication on cosets $x + H$ by deciding that for making the product of $a + H$ by $b + H$, one picks an element $x \in a + H$, an element $y \in b + H$ and the product is the coset containing $x\,y$: it only makes sense if this coset is independent of the choice of x and y, and since a particular choice is $x = a, y = b$, one must be sure that $x = a + h_1, y = b + h_2$ implies $x\,y = a\,b + h_3$ (with $h_1, h_2, h_3 \in H$, as suggested by the choice of notation, but the quantifiers are 'for all h_1, h_2 there exists h_3')); the choice $h_1 = 0$ implies that $a\,h_2 \in H$ for all $a \in R$ and all $h_2 \in H$, and the choice $h_2 = 0$ implies that $h_1 b \in H$ for all $b \in R$ and all $h_1 \in H$, i.e. H is an ideal of R.

Definition 7.5: If R is a ring and J is an ideal of R, one denotes R/J the *quotient ring* defined by the addition $(a + J) + (b + J) = (a + b)\,J$ and the multiplication $(a + J)\,(b + J) = (a\,b)\,J$.

Lemma 7.6: (first isomorphism theorem for rings) If ψ is a ring-homomorphism of a ring R_1 into a ring R_2, then $\psi(R_1)$ is subring of R_2 which is ring-isomorphic to $R_1/\psi^{-1}(\{0\})$.
Proof: That $\psi(R_1)$ is a subring of R_2 follows from $\psi(a) + \psi(b) = \psi(a + b)$ and $\psi(a)\,\psi(b) = \psi(a\,b)$, and it was shown that $\psi^{-1}(\{0\})$ is an ideal of R_2, so that since $\psi(a) = \psi(b)$ whenever $\pi(a) = \pi(b)$ there is a factorization $\psi = \overline{\psi} \circ \pi$, where $\overline{\psi}$ is an homomorphism from $R_1/\psi^{-1}(\{0\})$ into R_2, which is injective (since its kernel is the 0 of the quotient ring), and it becomes surjective if one considers it as a ring-homomorphism from $R_1/\psi^{-1}(\{0\})$ onto $\psi(R_1)$, so that it then is a bijection, hence a ring-isomorphism between these two rings.

Definition 7.7: If G is a group, then for $a, g \in G$, the *conjugate* of a by g is $a^g = g\,a\,g^{-1}$, and the *conjugate of a subgroup* H by g is $H^g = \{g\,h\,g^{-1} \mid h \in H\}$, which is a subgroup of G (and a subgroup H is normal if and only if $H^g = H$ for all $g \in G$).[4] The *conjugation by* g is the automorphism $\psi_g \in Aut(G)$ defined by $\psi_g(x) = g\,x\,g^{-1}$ for all $x \in G$. The *conjugacy class* of a is $\{a^g \mid g \in G\}$.

Remark 7.8: The fact that $\psi_g(x\,y) = g\,x\,y\,g^{-1} = g\,x\,g^{-1} g\,y\,g^{-1} = \psi_g(x)\,\psi_g(y)$ show that ψ_g is an homomorphism of G into G (i.e. an endomorphism), but $\psi_g\big(\psi_h(x)\big) = \psi_g(h\,x\,h^{-1}) = g\,h\,x\,h^{-1} g^{-1} = (g\,h)\,x\,(g\,h)^{-1} = \psi_{g\,h}(x)$ shows that $\psi_g \circ \psi_h = \psi_{g\,h}$, and in particular ψ_g is invertible with inverse $\psi_{g^{-1}}$ (since ψ_e is the identity mapping id_G on G), so that ψ_g is an isomorphism of G onto G (i.e. an automorphism). The set of automorphism of G, denoted $Aut(G)$, is a group for the operation of composition, whose identity is $e = id_G$, and the relation $\psi_g \circ \psi_h = \psi_{g\,h}$ for all $g, h \in G$ shows that the mapping $g \mapsto \psi_g$ is an homomorphism from G into $Aut(G)$.

If G is Abelian, then $\psi_g = id_G$ for all $g \in G$, all subgroups are normal, and each conjugacy class is reduced to one element.

Definition 7.9: One says that a subgroup $H \leq G$ is *characteristic* in G, and one writes $H\,char\,G$, if (and only if) $\psi(H) = H$ for all $\psi \in Aut(G)$,[5] the group of automorphisms of G.

Remark 7.10: Being a characteristic subgroup is a stronger property than being a normal subgroup, since normality is $\psi_g(H) = H$ for all $g \in G$ (or simply $\psi_g(H) \subset H$ for all $g \in G$), where ψ_g is the automorphism of conjugation by g.

Lemma 7.11: $A\,char\,B\,char\,C$ implies $A\,char\,C$, and $A\,char\,B \triangleleft C$ implies $A \triangleleft C$.
Proof: In the first case, for $\varphi \in Aut(C)$ one has $\varphi(B) = B$, so that $\varphi\big|_B \in Aut(B)$, and then $\varphi(A) = \varphi\big|_B(A) = A$.

In the second case, for $c \in C$ one has $\varphi_c(B) = B$, so that $\varphi_c\big|_B \in Aut(B)$, and then $\varphi_c(A) = \varphi_c\big|_B(A) = A$.

Remark 7.12: In general $A \triangleleft B \triangleleft C$ does not imply $A \triangleleft C$.

---

[4] Since $\big(H^{g_1}\big)^{g_2} = H^{g_2 g_1}$ for all $g_1, g_2 \in G$, $K = H^g$ is equivalent to $H = K^{g^{-1}}$, and one deduces that H is normal if and only if $H^g \subset H$ for all $g \in G$.

[5] It is enough that $\psi(H) \subset H$ for all automorphisms of G, because ψ^{-1} being also an automorphism, one has $\psi^{-1}(H) \subset H$, and then applying ψ gives $H \subset \psi(H)$.

For example, let C be the dihedral group D_4 which has order 8, and is generated by a which has order 4 and b which has order 2, satisfying $b\,a = a^3 b$,[6] so that $b\,a^2 = a^3 b\,a = a^6 b = a^2 b$, and $b\,a^3 = a^2 b\,a = a^5 b = a\,b$. Since b commutes with a^2, $B = \{e, a^2, b, a^2 b\}$ is a subgroup of C, which is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$,[7] and which is a normal subgroup of C, since B has index 2 in C. Since B is Abelian, $A = \{e, b\}$ is a normal subgroup of B. However, $a\,b\,a^{-1} = a\,b\,a^3 = a^2 b$, so that A is not stable by ψ_a, hence A is not a normal subgroup of C.

Example 7.13: $G = \mathbb{Z}_n$ is Abelian, so that $\psi_g = id_G$ for all $g \in G$, but $Aut(G)$ is not reduced to one element, and it actually has $\varphi(n)$ elements, and $Aut(G)$ is isomorphic to Z_n^*, the multiplicative group of units of the ring $\mathbb{Z}_n$. Indeed, if ψ is an automorphism of G, it sends any generator of $\mathbb{Z}_n$ to a generator of $\mathbb{Z}_n$, i.e. 1 is sent to an element $a \in \mathbb{Z}_n^*$, so that x is sent to $a\,x$ modulo n, and if another automorphism ψ' is the multiplication by $b \in \mathbb{Z}_n^*$, then the composition of ψ and ψ' is the multiplication by $a\,b$.

All the subgroups of $\mathbb{Z}_n$ are characteristic subgroups, since for every d dividing n there is exactly one subgroup of order d, and any automorphism must send this subgroup of order d on itself, so that it is a characteristic subgroup.

Example 7.14: $G = \mathbb{Z}_2 \times \mathbb{Z}_2$ is Abelian, so that $\psi_g = id_G$ for all $g \in G$, but $Aut(G)$ is not reduced to one element, and it actually has 6 elements, and $Aut(G)$ is isomorphic to the symmetric group S_3. Indeed, if ψ is an automorphism, it sends any element of order 2 to an element of order 2, and there are 3 of them: $G = \{e, a, b, c\}$ with $a^2 = b^2 = c^2 = e$, $a\,b = b\,a = c$, $b\,c = c\,b = a$, and $c\,a = a\,c = b$; once $\psi(a)$ and $\psi(b)$ are chosen distinct among a, b, c, the image $\psi(c)$ is the third one, so that any permutation of a, b, c gives an automorphism of G.

There are 3 subgroups of order 2, which are normal since G is Abelian, but none of them is a characteristic subgroup, since they are permuted by the automorphisms.

Example 7.15: $G = \mathbb{Z}_2 \times \mathbb{Z}_4$ is Abelian, so that $\psi_g = id_G$ for all $g \in G$, but $Aut(G)$ is not reduced to one element. G has 4 elements of order 4 ($(0,1), (0,3), (1,1), (1,3)$), and 3 elements of order 2 ($(0,2), (1,0), (1,2)$) so that it has 2 subgroups of order 4 and 3 subgroups of order 2, but the intersection of the two subgroups of order 4 is a subgroup of order 2, generated by $(0,2)$, so that this subgroup is characteristic (among the elements or order 2, $(0,2)$ is the only one which is divisible by 2).

Since G is generated by 2 of the elements of order 4, like $a = (0,1)$ and $b = (1,1)$, so that the other elements of order 4 are $3a$ and $3b$, and the elements of order 2 are $2a = 2b$, $b - a$, and $b + a$. There are then 4 automorphisms, obtained by sending (a, b) on either (a, b), $(3a, b)$, $(a, 3b)$, or $(3a, 3b)$, and $Aut(G)$ is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.[8]

---

[6] For example, a is the rotation of angle $\frac{\pi}{2}$ (like multiplication by i in $\mathbb{C}$), and b is a mirror symmetry (like complex conjugation in $\mathbb{C}$), so that $b\,a(z) = b(i\,z) = -i\overline{z} = a^3 b(z)$, hence $b\,a = a^3 b$.

[7] Since it is a subgroup, and a^2, b, and $a^2 b$ have order 2.

[8] These are given by mappings $(x, y) \in \mathbb{Z}_2 \times \mathbb{Z}_4 \mapsto (\alpha\,x + \beta\,y, \gamma\,x + \delta\,y) \in \mathbb{Z}_2 \times \mathbb{Z}_4$ with the matrix $\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ given by $\begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, $\begin{pmatrix} 1 & 0 \\ 2 & 3 \end{pmatrix}$, $\begin{pmatrix} 3 & 0 \\ 2 & 1 \end{pmatrix}$, $\begin{pmatrix} 3 & 0 \\ 0 & 3 \end{pmatrix}$.

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

8- Friday September 16, 2011.

Remark 8.1: For any set X, one denotes S_X the set of bijections of X into X, which is a group under the operation of composition of mappings (which is easily seen to be associative), with identity element $e = id_X$, the identity mapping id_X, defined by 'for all $x \in X$, $id_X(x) = x$' (which even makes sense if $X = \emptyset$), and the inverse of f is the inverse mapping f^{-1} defined by $f^{-1}\big(f(x)\big) = x$ for all $x \in X$.[1]

If $X = \{1, \dots, n\}$, a bijection from X into X is called a *permutation* of the elements $1, \dots, n$, and there are $n!$ of them, since there are n choices for the image of 1, then only $n-1$ choices for the image of 2 (because the image of 1 should only appear once), $n-2$ choices for the image of 3, and so on; instead of S_X, one writes S_n, and it is called the *symmetric group* S_n on n elements. Since $n!$ grows very fast, and $10! = 3\ 628\ 800$, a result like Cayley's theorem that any subgroup of order n is isomorphic to a subgroup of S_n may not be of much practical use for large n: saying that all groups of size 10 appear (isomorphically) as some subgroups of a group of order 3 628 800 is not so relevant if one notices that any Abelian group of order 10 is isomorphic to $\mathbb{Z}_{10}$,[2] and any non-Abelian group of order 10 is isomorphic to the dihedral group D_5;[3] since D_5 is the symmetry group of a regular pentagon, it appears as a subgroup of S_n for $n \geq 5$, while S_n contains an isomorphic copy of $\mathbb{Z}_{10}$ for $n \geq 7$ (using as generator a permutation with a cycle of length 5 and a cycle of length 2).[4]

S_n is non-Abelian for $n \geq 3$, while S_2 is isomorphic to $\mathbb{Z}_2$ (and $S_1 = \{e\}$).

Remark 8.2: One may write a permutation $\sigma \in S_n$ as $\begin{pmatrix} 1 & 2 & \dots & n \\ \sigma(1) & \sigma(2) & \dots & \sigma(n) \end{pmatrix}$, by putting the elements in a first row and their images by σ in the second row, but it more useful to write σ as a product of disjoint *cycles*: one builds an oriented graph with vertices $1, \dots, n$ by putting an oriented edge between i and $\sigma(i)$ for $i = 1, \dots, n$, and the connected components of the graph are the cycles, so that they use different subsets of $\{1, \dots, n\}$; one writes $(a_1 \ \dots \ a_k)$ with distinct elements $a_1, \dots, a_k$ for a cycle of length k (or period k), which means that a_1 is sent to a_2, a_2 is sent to a_3, and so on, until a_n is sent to a_1; for simplicity, one does not write the cycles (a) of length 1, and then every permutation is written as a product of cycles, using different elements of $\{1, \dots, n\}$.

Since any cycle $(a_1 \ \dots \ a_k)$ has order k, one deduces that the order of a permutation is the least common multiple of the lengths of its cycles. The maximum order of elements of S_n is then 3 for S_3, 4 for S_4, 6 for S_5 and S_6, 12 for S_7, 15 for S_8, 20 for S_9, 30 for S_{10}.

Lemma 8.3: Any permutation $\sigma \in S_n$ (for $n \geq 2$) can be written as a product of *transpositions*, which are the particular permutations having only one cycle of length 2, i.e. $(i\,j)$ for $i \neq j$.
Proof: By induction on n: it is true for $n = 2$ since $S_2 = \{e, \tau\}$ for $\tau = (1\,2)$ and $e = \tau^2$. If it is proved for n and $\sigma \in S_{n+1}$, one writes σ has a product of disjoint cycles; if σ is not a cyclic permutation $(a_1 \dots a_{n+1})$, then each cycle is a product of transpositions by the induction hypothesis and σ then is such a product of transpositions. If $\sigma = (a_1 \dots a_{n+1})$ is a cyclic permutation, then $(a_1 a_2)\,(a_1 \dots a_{n+1}) = (a_2 \dots a_{n+1})$, which is a product of transpositions $\tau_1 \cdots \tau_k$ by the induction hypothesis, so that $\sigma = (a_1 a_2)\,\tau_1 \cdots \tau_k$.

---

[1] Since one also uses f^{-1} for pre-images of subsets, let us use the notation $f^<$ instead, defined by $f^<(A) = \{x \in X \mid f(x) \in A\}$ for all $A \in \mathcal{P}(X)$ (i.e. for all $A \subset X$), and notice that for a bijection f one has $f^<\big(\{f(x)\}\big) = \{x\}$ for all $x \in X$. If instead of $f^<$ one writes f^{-1}, then for a bijection f one has two notations f^{-1}, one applying to elements and the other applying to subsets, and a subset with one element is written $\{x\}$, which belongs to $\mathcal{P}(X)$, and it should not be confused with the element x, which belongs to X.

[2] If n is square-free, every Abelian group of order n is isomorphic to $\mathbb{Z}_n$.

[3] If n is odd, every non-Abelian group of order $2n$ is isomorphic to the dihedral group D_n.

[4] For $n = 8$, the order of S_8 is 40 320, and S_8 then contains isomorphic copies of the three Abelian groups of order 8 ($\mathbb{Z}_8$, $\mathbb{Z}_2 \times \mathbb{Z}_4$, and $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_2$), and of the two non-Abelian groups of order 8 (D_4 and $\mathbb{Q}_8$), but for $n < 8$, S_n does not contain a copy of $\mathbb{Z}_8$.

Definition 8.4: The *signature* of a permutation $\sigma \in S_n$ is $\prod_i (-1)^{\ell_i - 1}$ where the ℓ_i are the lengths of the disjoint cycles (of length ≥ 2) forming σ.[5] It is an homomorphism from S_n into the multiplicative group $\{+1, -1\}$, whose kernel is called the *alternating group* A_n, which is the subgroup of *even permutations* in S_n, i.e. those which are the product of an even number of transpositions, so that $A_n \lhd S_n$, and $S_n / A_n \simeq \mathbb{Z}_2$ for all $n \geq 2$. For $n \geq 2$, $|A_n| = \frac{n!}{2}$, so that $A_2 \simeq \{e\}$, $A_3 \simeq \mathbb{Z}_3$.

Remark 8.5: For the definition to make sense, one has to check that multiplying σ by any transposition multiplies the signature by -1, so that if $\tau_1, \ldots, \tau_m$ are transpositions one has $signature(\tau_1 \cdots \tau_m) = (-1)^m$, and since every permutation is a product of transpositions one deduces that $signature(\sigma_1 \sigma_2) = signature(\sigma_1)\, signature(\sigma_2)$ for any two permutations $\sigma_1, \sigma_2 \in S_n$.

One then wants to show that for $i \neq j$ one has $signature\big((i\,j)\,\sigma\big) = -signature(\sigma)$, and there are two cases to consider. In the first case, i and j belong to two different cycles of σ, so that σ contains a product $(i\, a_1 \ldots a_k)\,(j\, b_1 \ldots b_\ell)$ and one notices that $(i\,j)\,(i\, a_1 \ldots a_k)\,(j\, b_1 \ldots b_\ell) = (j\, b_1 \ldots b_\ell i\, a_1 \ldots a_k)$, and this form is valid even if there are no as or no bs, so that σ has one cycle of length $k+1$ and one cycle of length $\ell + 1$, contributing to $(-1)^{k+\ell}$ in the definition of $signature(\sigma)$, while $(i\,j)\,\sigma$ has one cycle of length $k + \ell + 2$ contributing to $(-1)^{k+\ell+1}$ in the definition of $signature\big((i\,j)\,\sigma\big)$. In the second case, i and j belong to the same cycle of σ, so that σ contains $(i\, a_1 \ldots a_k j\, b_1 \ldots b_\ell)$ and $(i\,j)\,(i\, a_1 \ldots a_k j\, b_1 \ldots b_\ell) = (i\, a_1 \ldots a_k)\,(j\, b_1 \ldots b_\ell)$, and this form is valid even if there are no as or no bs, so that σ has one cycle of length $k+\ell+2$ contributing to $(-1)^{k+\ell+1}$ in the definition of $signature(\sigma)$, and $(i\,j)\,\sigma$ has one cycle of length $k+1$ and one cycle of length $\ell + 1$, contributing to $(-1)^{k+\ell}$ in the definition of $signature\big((i\,j)\,\sigma\big)$.

Remark 8.6: A_3 is simple, since it is isomorphic to $\mathbb{Z}_3$ (and $\mathbb{Z}_n$ is simple if and only if n is prime), and it will be shown in another lecture that A_n is simple for all $n \geq 5$, but Lemma 8.7 shows that A_4 is not simple.

Lemma 8.7: One has $N = \{e, (12)\,(34), (13)\,(24), (14)\,(23)\} \lhd S_4$, so that $N \lhd A_4$. One has $A_4 / N \simeq \mathbb{Z}_3$, and $S_4 / N \simeq S_3$ (and $S_4 / A_4 \simeq \mathbb{Z}_2$).
Proof: Since an element like $(12)\,(34)$ is the product of the two transpositions (12) and (34), one has $N \subset A_4$, and N is a subgroup isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, since $(12)\,(34)\,(13)\,(24) = (14)\,(23)$ and $\big((12)\,(34)\big)^2 = e$, for example. If $\sigma \in S_4$ and one considers $\sigma\,(12)\,(34)\,\sigma^{-1}$, for example, this permutation transposes $\sigma(1)$ and $\sigma(2)$ and it transposes $\sigma(3)$ and $\sigma(4)$, so that it belongs to N, showing that N is a normal subgroup of S_4, hence a normal subgroup of A_4. Because $|A_4| = 12$, A_4 / N has order 3, and is isomorphic to $\mathbb{Z}_3$. S_4 / N has order 6, and could be isomorphic to $\mathbb{Z}_6$ or to S_3, but if it was isomorphic to Z_6 there would exist $a \in S_4$ with $a, \ldots, a^6$ belonging to six different N-cosets, but in S_4 the only possible orders for an element are 1, 2, 3, or 4, so that S_4 / N must be isomorphic to S_3.

Remark 8.8: Lemma 8.7 actually shows that S_4 is a *solvable* group, but it can be shown that S_n is not a solvable group for $n \geq 5$. This is related to the method of GALOIS for characterizing the polynomials P over a field E whose roots can be given by a formula using only radicals: one defines the *splitting field extension* F for P over E, and the *Galois group* $G = Aut_E(F)$ of automorphisms of F fixing E, and the condition is that G be solvable, and this means that there exists a *subnormal series* $G_0 = \{e\} \leq G_1 \leq \ldots \leq G_k = G$ (i.e. such that $G_i \lhd G_{i+1}$ for $i = 0, 1, \ldots, k-1$) for which G_{i+1} / G_i is Abelian for $i = 0, \ldots, k-1$. The case of S_4 corresponds to $\{e\} \lhd N \lhd A_4 \lhd S_4$.

Lemma 8.9: (Cauchy's theorem) Let p be a prime number, and let G be a finite group whose order is a multiple of p. Then, there exists an element $h \in G$ of order p, or equivalently there exists a subgroup $H \leq G$ of order p (so that there exist at least $p-1$ elements of order p). More precisely, the number of subgroups or order p is equal to 1 modulo p.
Proof: Let $\Gamma = G \times \cdots \times G$ (with p factors). One defines the mapping π from Γ into itself by $\pi\big((g_1, \ldots, g_p)\big) = (g_2, \ldots, g_p, g_1)$, and one writes $\pi\, x$ for $\pi(x)$; one notices that $\pi^p \gamma = \gamma$ for all $\gamma \in \Gamma$.

Let $X \subset \Gamma$ be the subset of $x = (g_1, \ldots, g_p)$ satisfying $g_1 \cdots g_p = e$, so that $|X| = |G|^{p-1}$ is a multiple of p, since $g_1, \ldots, g_{p-1}$ may be chosen arbitrarily, and then g_p is determined. For $x \in X$, one has $g_2 \cdots g_p g_1 = g_1^{-1}(g_1 \cdots g_p)\, g_1 = g_1^{-1} e\, g_1 = e$, so that π maps X into itself. If $\pi\, x \neq x$, then $x, \pi\, x, \ldots, \pi^{p-1} x$ are all distinct elements of X, and this is where the fact that p is a prime is used, because if $\pi^j x = \pi^k x$ for $0 \leq j < k \leq p-1$, then $\pi^\ell x = x$ for $\ell = k - j$, so that $\pi^{m\,\ell} x = x$ for all $m \geq 1$, and using for m the inverse of ℓ modulo p

[5] Another definition of $signature(\sigma)$ is $(-1)^m$, where m is the number of pairs $i < j$ such that $\sigma(i) > \sigma(j)$.

(so that $m\,\ell = 1 + n\,p$) one deduces that $\pi\,x = x$. A consequence is that X is made up of such subsets of p elements, together with the particular $x \in X$ satisfying $\pi\,x = x$, and the number of those must then be a multiple of p (and $\neq 0$ since $(e, \ldots, e)$ belongs to it).

Since $\pi\,x = x$ implies $g_1 = g_2 = \cdots = g_p$, one has $x = (h, \ldots, h)$ with $h \in G$ satisfying $h^p = e$, and the number of such h is a (non-zero) multiple of p, so that there are at least $p-1$ solutions of $h^p = e$ with $h \neq e$, which all have order p; a subgroup of order p is $H = \{e, h, \ldots, h^{p-1}\}$ for such a $h \neq e$.

Let the number of h be $k\,p$, and correspond to j distinct subgroups of order p; since two such subgroups are equal or intersect only at e (by Lagrange's theorem, because p is prime), one has $k\,p = j\,(p-1) + 1$, so that $j = 1 + p\,(j-k)$.

Remark 8.10: The preceding proof uses an action of the group $\mathbb{Z}_p$, and remarks about the size of orbits. The general question of action of a group on a set will be studied in the next lecture.

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

9- Monday September 19, 2011.

Definition 9.1: An *action of a group G on a set X* is an homomorphism from G into S_X, the group of bijections of X. Equivalently, it is a mapping from $G \times X$ into X satisfying $e\,x = x$ for all $x \in X$, and $g_1(g_2 x) = (g_1 g_2)\,x$ for all $g_1, g_2 \in G$ and all $x \in X$, where $g\,x$ denotes the image of (g, x) by the mapping.[1]

For $x \in X$, the *orbit of x* is $\{g\,x \mid g \in G\} \subset X$, the *stabilizer of x* is $Stab(x) = \{g \in G \mid g\,x = x\} \subset G$.

Remark 9.2: For example, an action of $\mathbb{Z}_n$ on X is the same as having a bijection f from X onto itself satisfying $f \circ \cdots \circ f = id_X$, where there are n factors.

An action of $\mathbb{Z}_2 \times \mathbb{Z}_2$ on X is the same as having two bijections f and g from X onto itself satisfying $f \circ f = g \circ g = id_X$ and $f \circ g = g \circ f$.

Lemma 9.3: The relation $x \mathcal{R} y$ if and only if there exists $g \in G$ with $g\,x = y$ is an equivalence relation, and the equivalence classes are the orbits, which then form a partition of X.
Proof: For all $x \in X$ one has $x \mathcal{R} x$, because $e\,x = x$; $x \mathcal{R} y$ means $g\,x = y$ for some $g \in G$, which is equivalent to $x = g^{-1} y$, implying $y \mathcal{R} x$; $x \mathcal{R} y$ and $y \mathcal{R} z$ mean $g\,x = y$ and $h\,y = z$ for some $g, h \in G$, so that $h\,g\,x = z$, implying $x \mathcal{R} z$. The definition of the equivalence class of x coincides with the definition of the orbit of x.

Lemma 9.4: For $x \in X$, $Stab(x) \leq G$. The mapping $g\,x \mapsto g\,Stab(x)$ is a bijection between the orbit of x and the left cosets of $Stab(x)$, so that the size of the orbit of x is the index of $Stab(x)$, which both divide the order of G if it is finite. In particular, for a prime p, and for any action of $\mathbb{Z}_p$, the orbits have size 1 or size p.
Proof: Because $e\,x = x$, one has $e \in Stab(x)$; if $g_1, g_2 \in Stab(x)$, then $g_1 x = g_2 x = x$ implies $(g_1\,g_2)\,x = g_1 x = x$, so that $g_1 g_2 \in Stab(x)$, and $g_1^{-1} x = g_1^{-1}(g_1 x) = x$, so that $g_1^{-1} \in Stab(x)$.

The mapping is well defined if $g_1 x = g_2 x$ implies $g_1 Stab(x) = g_2 Stab(x)$: indeed, $g_1 x = g_2 x$ means $g_2^{-1} g_1 x = x$, i.e. $g_2^{-1} g_1 \in Stab(x)$, which implies $g_1 \in g_2 Stab(x)$ so that $g_1 Stab(x) \subset g_2 Stab(x)$, and exchanging the roles of g_1 and g_2 gives equality. Then, the size of the orbit of x is the number of left cosets of $Stab(x)$, i.e. the index of $Stab(x)$, which by Lagrange's theorem divides the order of G if G is a finite group.

Example 9.5: G acts on itself by left multiplication:[2] $X = G$ and (g, x) is mapped to the usual product $g\,x$ in G for all $g, x \in G$. G is isomorphic to a subgroup of S_G, and in particular every group of order n is isomorphic to a subgroup of the symmetric group S_n (Cayley's theorem).
Proof: For $x, g_1, g_2 \in G$, (e, x) is mapped to $e\,x = x$, and $(g_1, g_2 x)$ is mapped to $g_1(g_2 x) = (g_1 g_2)\,x$. Then, the homomorphism from G into S_G is injective, because if $g \in G$ is mapped to the identity of S_G, it means that $g\,x = x$ for all $x \in G$, and taking $x = e$ gives $g = e$; the first isomorphism theorem tells then that G is isomorphic to the image, which is a subgroup of S_G.

Example 9.6: G acts on itself by conjugation: $X = G$ and (g, x) is mapped to $x^g = g\,x\,g^{-1}$.[3] The orbit of $x \in G$ is called the *conjugacy class* of x, and the stabilizer of x is called the *centralizer of x*, i.e. $C_G(x) = \{g \in G \mid g\,x = x\,g\}$,[4] and the size of the conjugacy class is the index of the centralizer (so that its size divides the order of G if G is finite).
Proof: For $x, g, h \in G$, one has $e\,x = x^e = x$, and $(x^g)^h = h\,(g\,x\,g^{-1})\,h^{-1} = (h\,g)\,x\,(h\,g)^{-1} = x^{h\,g}$.

---

[1] In some concrete examples the notation $g\,x$ may lead to confusion, like for Example 9.6 and Example 9.7 below, and it is better to avoid it.

[2] Using right multiplication, i.e. $(g, x) \mapsto x\,g$, does not satisfy the axioms if G is not Abelian, because $(g_1\,g_2, x)$ is mapped to $x\,g_1 g_2$, while (g_2, x) is mapped to $x\,g_2$, and $(g_1, x\,g_2)$ is mapped to $x\,g_2 g_1$.

[3] Here the notation $g\,x$ for (g, x) would be a little misleading. Notice that the notation x^g may also be confused with a power of x in some cases.

[4] If G is Abelian, then the conjugacy class of each $x \in G$ is reduced to $\{x\}$, and $C_G(x) = G$ for all $x \in G$; conversely, if $C_G(x) = G$ for all $x \in G$, then G is Abelian.

Example 9.7: G acts on the set of its subgroups by conjugation:[5] (g, H) is mapped to $H^g = \{g\,h\,g^{-1} \mid h \in H\}$. The stabilizer of $H \leq G$ is called the *normalizer* $N_G(H) = \{g \in G \mid g\,H = H\,g\}$ of H in G, so that one has $H \lhd N_G(H) \leq G$.

Lemma 9.8: $N_G(H)$ is the largest subgroup of G in which H is normal.[6]
Proof: For $K \leq G$, the condition $H \lhd K$ is equivalent to $k\,H = H\,k$ for all $k \in K$, i.e. $K \leq N_G(H)$.

Remark 9.9: If G acts on X, then G acts on any subset of X which is a union of orbits. If $H \leq G$, then H acts on each G-orbit, which is then partitioned as a union of H-orbits.

Definition 9.10: If p is prime and divides the order of a finite group G, a *p-subgroup* H of G is any subgroup whose order is a power of p. If p^n is the highest power of p which divides $|G|$, any $H \leq G$ with $|H| = p^n$ is called a *Sylow-p subgroup* of G.

Remark 9.11: Sylow's theorem will be proved in another lecture, and its proof will use action by conjugation on subgroups, and it is stated here and then used on two examples: if p is a prime and G is a group of order $|G| = p^n a$ (with $n \geq 1$) and p does not divide a, then, every p-subgroup of G is included in a Sylow p-subgroup, all Sylow p-subgroups are conjugate, and their number n_p is congruent to 1 modulo p, and divides $|G|$, so that it divides a. In particular, if there is a unique Sylow p-subgroup, then it is a normal subgroup (and a normal Sylow p-subgroup is unique).

Example 9.12: For a group G of order 15, then $n_3 = 1 \pmod 3$ and n_3 divides 5, so that $n_3 = 1$ and there is only one Sylow 3-subgroup H_3, $n_5 = 1 \pmod 5$ and n_5 divides 3, so that $n_5 = 1$ and there is only one Sylow 5-subgroup H_5, and since both H_3 and H_5 are normal subgroups of G it will be shown that $G \simeq H_3 \times H_5$, and since $H_3 \simeq \mathbb{Z}_3$ and $H_5 \simeq \mathbb{Z}_5$, one has $G \simeq \mathbb{Z}_{15}$ by the Chinese remainder theorem.

Example 9.13: For a group G of order 21, then $n_3 = 1 \pmod 3$ and n_3 divides 7, so that n_3 is either 1 or 7, $n_7 = 1 \pmod 7$ and n_7 divides 3, so that $n_7 = 1$ and there is only one Sylow 7-subgroup H_7, which is a normal subgroup of G.

If $n_3 = 1$, there is only one Sylow 3-subgroup H_3, which is a normal subgroup of G, and in this case $G \simeq \mathbb{Z}_{21}$.

If $n_3 = 7$, there are 7 Sylow-3 subgroups $K_1, \ldots, K_7$, and since $K_i \cap K_j = \{e\}$ for $i \neq j$, there are 14 elements of order 2, which with the 6 elements of order 7 in H_7 and e make up the group. For each K_i, the action by conjugation generates an orbit of size 7 (since it gives all the K_j), so that the index of the stabilizer (called the normalizer of K_i) is 7, i.e. $N_G(K_i) = K_i$. That such a non-Abelian group of order 21 exists, will have to be shown, and it will be constructed as a semi-direct product.

[5] If $H \leq G$, and $g \in G$, then $g\,H$ is not a subgroup of G unless $g \in H$, but $H^g = g\,H\,g^{-1}$ is always a subgroup of G, hence the action of Example 9.6 leads to Example 9.7 for the set X of subgroups of G.

[6] If G is Abelian, then $N_G(H) = G$ for all $H \leq G$.

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

10- Wednesday September 21, 2011.

Definition 10.1: If N and H are two groups, a *semi-direct product* of N and H is a group denoted $G = N \times_\psi H$ obtained by choosing an homomorphism ψ of H into $Aut(N)$, the group of automorphisms of N, and defining on the product $N \times H$ the operation $\star_\psi$ by $(n_1, h_1) \star_\psi (n_2, h_2) = \big(n_1 \psi_{h_1}(n_2), h_1 h_2\big)$, where one writes ψ_h for $\psi(h)$.

Lemma 10.2: With the notation of Definition 10.2, G is a group, with identity $e = (e_N, e_H)$, and the inverse of (n, h) is $(\psi_{h^{-1}}(n^{-1}), h^{-1})$.

$\widetilde{N} = \{(n, e_H) \mid n \in N\}$ is a normal subgroup of G isomorphic to N, $\widetilde{H} = \{(e_N, h) \mid h \in H\}$ is a subgroup of G isomorphic to H, and one has $\widetilde{N} \cap \widetilde{H} = \{e\}$. Moreover, there exists an homomorphism χ from G into $\widetilde{H}$, which when restricted to $\widetilde{H}$ is the identity, and whose kernel is $\widetilde{N}$, namely $\chi : (n, h) \mapsto (e_N, h)$.

This group is non-Abelian, except if ψ is the trivial homomorphism (with kernel H), in which case the group is the usual product of groups, which is Abelian if and only if both N and H are Abelian.
Proof: The operation $\star_\psi$ is associative: $\big((n_1, h_1) \star_\psi (n_2, h_2)\big) \star_\psi (n_3, h_3) = (n_1 \psi_{h_1}(n_2), h_1 h_2) \star_\psi (n_3, h_3) = (n_1 \psi_{h_1}(n_2)\, \psi_{h_1 h_2}(n_3), h_1 h_2 h_3)$, and then $(n_1, h_1) \star_\psi \big((n_2, h_2) \star_\psi (n_3, h_3)\big) = (n_1, h_1) \star_\psi (n_2 \psi_{h_2}(n_3), h_2 h_3) = \big(n_1 \psi_{h_1}\big(n_2 \psi_{h_2}(n_3)\big), h_1 h_2 h_3\big)$, which are equal because $\psi_{h_1}\big(n_2 \psi_{h_2}(n_3)\big) = \psi_{h_1}(n_2)\, \psi_{h_1}\big(\psi_{h_2}(n_3)\big)$ since $\psi_{h_1} \in Aut(N)$, and because $\psi_{h_1} \circ \psi_{h_2} = \psi_{h_1 h_2}$ since ψ is an homomorphism. The identity is (e_N, e_H), since $(e_N, e_H) \star_\psi (n, h) = (e_N \psi_{e_H}(n), h)$ and $(n, h) \star_\psi (e_N, e_H) = (n\, \psi_h(e_N), h)$, which are equal to (n, h) because $\psi_{e_H} = id_N$ and $\psi_h(e_N) = e_N$ for all $h \in H$. The inverse of (n, h) is $(\psi_{h^{-1}}(n^{-1}), h^{-1})$, since $(n, h) \star_\psi (\psi_{h^{-1}}(n^{-1}), h^{-1}) = \big(n\, \psi_h\big(\psi_{h^{-1}}(n^{-1})\big), e_H\big)$ and $(\psi_{h^{-1}}(n^{-1}), h^{-1}) \star_\psi (n, h) = \big(\psi_{h^{-1}}(n^{-1})\, \psi_{h^{-1}}(n), e_H\big)$, which are equal to (e_N, e_H) because $\psi_h \circ \psi_{h^{-1}} = \psi_{e_H} = id_N$ and $\psi_{h^{-1}}(n^{-1})\, \psi_{h^{-1}}(n) = \psi_{h^{-1}}(e_N) = e_N$ for all $h \in H$.

$\widetilde{N}$ is a subgroup of G isomorphic to N because $(n_1, e_H) \star_\psi (n_2, e_H) = (n_1 n_2, e_H)$ for all $n_1, n_2 \in N$. It is a normal subgroup because for all $n' \in N$ and all $(n, h) \in G$ one has $(n, h) \star_\psi (n', e_N) = (n'', e_N) \star_\psi (n, h)$ with $n'' = n\, \psi_h(n')\, n^{-1}$ (since $n\, \psi_h(n') = n'' n = n'' \psi_{e_N}(n)$).

$\widetilde{H}$ is a subgroup of G isomorphic to H because $(e_N, h_1) \star_\psi (e_N, h_2) = (e_N, h_1 h_2)$ for all $h_1, h_2 \in H$.

Since $\chi\big((n, h)\big) = (e_N, h)$ for all $n \in N, h \in H$, and the second components in the operation $\star_\psi$ use the product in H, χ is an homomorphism, and it is the identity if one restricts it to $\widetilde{H}$ since it consists of using $n = e_N$, and its kernel is the set of (n, h) with $h = e_H$, i.e. $\widetilde{N}$.

If $N \times_\psi H$ is Abelian, then using $n_1 = n_2 = e_N$ shows that H is Abelian, and then one must have $n_1 \psi_{h_1}(n_2) = n_2 \psi_{h_2}(n_1)$ for all $h_1, h_2 \in H, n_1, n_2 \in N$; using $h_1 = h_2 = e_H$ shows that N is Abelian, and then using $h_1 = e_H$ gives $n_1 n_2 = n_2 \psi_{h_2}(n_1)$, i.e. $n_1 = \psi_{h_2}(n_1)$ for all $h_2 \in H, n_1 \in N$, or $\psi_{h_2} = id_N$ for all $h_2 \in H$, so that ψ is the trivial homomorphism of H into $Aut(N)$.

Remark 10.3: Since a semi-direct product uses an homomorphism ψ from H into $Aut(N)$, it is useful to know if a non-trivial ψ exists, since a trivial ψ gives the direct product.

For example, if $H = \mathbb{Z}_p$ for a prime p, a nontrivial ψ exists if and only if there exists an element of order p in $Aut(N)$, and in the case where N is finite, it is equivalent to p dividing the order of $Aut(N)$, by Cauchy's theorem.

One has seen that $Aut(\mathbb{Z}_n)$ is isomorphic to $\mathbb{Z}_n^*$, which has order $\varphi(n)$, so that for $p = 2$ it is always possible if $n \geq 3$ (since 1 and 2 are the only values n for which $\varphi(n)$ is odd), and we shall see below that $\mathbb{Z}_n \times_\psi \mathbb{Z}_2$ is isomorphic to the dihedral group D_n. Actually, there is a non-trivial homomorphism from $\mathbb{Z}_2$ into $Aut(N)$ for any Abelian group N, since there is a natural element of order 2 in $Aut(N)$, which is inversion inv, i.e. $n \mapsto inv(n) = n^{-1}$;[1] because $inv \circ inv = id_N$, there is then an homomorphism ψ of $\mathbb{Z}_2$ in $Aut(N)$, given by $\psi(0) = id_N$ and $\psi(1) = inv$, hence one can then construct the non-Abelian group $N \star_{inv} \mathbb{Z}_2$, which has twice the number of elements of N if N is finite.

Lemma 10.4: If $p < q$ are (distinct) primes, and $q \neq 1 \pmod p$, every group G of order $p\,q$ is isomorphic to $\mathbb{Z}_{p\,q}$, but if $q = 1 \pmod p$, there exists a non-Abelian group G of order $p\,q$ of the form $\mathbb{Z}_q \times_\psi \mathbb{Z}_p$.

[1] For a non-Abelian group G, the mapping $g \mapsto g^{-1}$ is not an homomorphism, which would require the inverse of $a\,b$ to be $a^{-1} b^{-1}$, and it is not the case for at least one pair $a, b \in G$.

Proof: By Sylow's theorem, as seen for the case of $|G| = 15$, there is one (normal) Sylow q-subgroup H_q isomorphic to $\mathbb{Z}_q$, and if $q \neq 1 \pmod p$ there is one (normal) Sylow p-subgroup H_p isomorphic to $\mathbb{Z}_p$, so that G is isomorphic to $H_p \times H_q \simeq \mathbb{Z}_{p\,q}$, but if $q = 1 \pmod p$ there is the possibility that there are q Sylow p-subgroup $K_1, \ldots, K_q$ (isomorphic to $\mathbb{Z}_p$), and indeed such a non-Abelian group can be constructed in the form $\mathbb{Z}_q \times_\psi \mathbb{Z}_p$ for a non-trivial homomorphism ψ from $\mathbb{Z}_p$ into $Aut(\mathbb{Z}_q)$, since $Aut(\mathbb{Z}_q)$ has order $q-1$, which is a multiple of p.

Remark 10.5: Since $Aut(\mathbb{Z}_q)$ is isomorphic to $\mathbb{Z}_q^*$, and it was mentioned that $\mathbb{Z}_q^*$ is cyclic, it is isomorphic to $\mathbb{Z}_{q-1}$. For any n, it was shown that for any divisor d of n, $\mathbb{Z}_n$ has exactly one subgroup of order d (and $\varphi(d)$ elements of order d), so that if p divides $q-1$ there is exactly one subgroup of order p of $Aut(\mathbb{Z}_q)$, so that there is no choice for the image $\psi(\mathbb{Z}_p)$ if ψ is a non-trivial homomorphism from $\mathbb{Z}_p$ into $Aut(\mathbb{Z}_q)$, but there are as many different ψ than elements in $Aut(\mathbb{Z}_p)$, i.e. $p-1$.

For $p = 3, q = 7$, ψ must send 1 onto an element of order 3 in $\mathbb{Z}_7^*$, and these are the quadratic residues different from 1, i.e. 2 and 4: one semi-direct product then consists in putting on $\mathbb{Z}_7 \times \mathbb{Z}_3$ the operation $(n_1, h_1) \star (n_2, h_2) = (n_1 2^{h_1} n_2, h_1 h_2)$, and the other semi-direct product consists in putting on $\mathbb{Z}_7 \times \mathbb{Z}_3$ the operation $(n_1, h_1) \star (n_2, h_2) = (n_1 4^{h_1} n_2, h_1 h_2)$, where the first components are taken modulo 7 and the second components are taken modulo 3.

Example 10.6: The dihedral group D_n is the group of symmetries of a regular polygon with n sides, and such a polygon can considered as the set of nth root of unity in $\mathbb{C}$, i.e. if $\omega = e^{\frac{2i\,\pi}{n}}$, the polygon is $\{1, \omega, \ldots, \omega^{n-1}\}$. If a denotes the multiplication by ω, i.e. a rotation of $\frac{2\pi}{n}$ and b is complex conjugation, then $D_n = \{e, a, \ldots, a^{n-1}, b, b\,a, \ldots, b\,a^{n-1}\}$.[2] Since $b\,a$ applied to $z \in \mathbb{C}$ gives $\overline{\omega\,z} = \overline{\omega}\,\overline{z}$, which is $a^{-1}b$ applied to z (since $\overline{\omega} = \frac{1}{\omega}$), one deduces that $b\,a = a^{-1}b$. Then, $b\,a^{k+1} = b\,a\,a^k = a^{-1}b\,a^k$, and one finds by induction that $b\,a^k = a^{-k}b$ for all non-negative integers k; if $k < 0$, then $k + m\,n \geq 0$ for some $m \in \mathbb{N}$, so that using $a^n = e$ one deduces that $b\,a^k = b\,a^{k+m\,n} = a^{-k-m\,n}b = a^{-k}b$.

In this example $a^n = b^2 = e$, so that $b^{-1} = b$, but without using this information one has $(b\,a^k)^{-1} = (a^{-k}b)^{-1}$ for all $k \in \mathbb{Z}$, i.e. $b^{-1}a^k = a^{-k}b^{-1}$, so that one may push b or b^{-1} to the right through any power of a and change the sign of the exponent of a; by induction, one deduces that $b^\ell a^k = a^{(-1)^\ell k}b^\ell$ for all $k, \ell \in \mathbb{Z}$; then $(a^\alpha b^\beta)\,(a^\gamma b^\delta) = a^\alpha (b^\beta\,a^\gamma)\,b^\delta = a^{\alpha+(-1)^\beta\gamma}b^{\beta+\delta}$, and in the case of D_n the sum of exponents for a is taken in $\mathbb{Z}_n$, and the sum of exponent of b is taken in $\mathbb{Z}_2$.

One recognizes here a semi-direct product with $\psi_h(a^\gamma) = a^{(-1)^\beta\gamma}$ for $h = b^\beta$, i.e. $\psi_h = inv^\beta$, so that it is an example of the procedure mentioned for $N \times_{inv} \mathbb{Z}_2$.

[2] From a geometrical point of view, if one wants to send 1 onto ω^k, either one keeps orientation and one uses a rotation of angle $\frac{2k\,\pi}{n}$, i.e. a^k, or one changes orientation, in which case one uses complex conjugation before using a rotation of angle $\frac{2k\,\pi}{n}$, i.e. $a^k b$.

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

11- Friday September 23, 2011.

Lemma 11.1: (second isomorphism theorem)[1] If $H \leq G$, and $N \triangleleft G$, then,
a) $H\,N = N\,H \leq G$,
b) $N \cap H \triangleleft H$, and $H\,N/N \simeq H/(N \cap H)$.

Proof: a) That N is a normal subgroup of G means $g\,N = N\,g$ for all $g \in G$, so that $h\,N = N\,h$ for all $h \in H$, which implies $H\,N = N\,H$, and this implies that it is a subgroup of G.

b) Let π be the projection of G onto G/N, which is a (surjective) homomorphism, and restrict it to H, so that the kernel of $\pi|_H$ is $N \cap H$, which is then a normal subgroup of H. By the first homomorphism theorem, $H/(N \cap H)$ is isomorphic to the image of H by $\pi|_H$, which is the set of cosets $h\,N$ for $h \in H$, i.e. the quotient of $H\,N$ by N (and N is a normal subgroup of $H\,N$ since $N \leq H\,N \leq G$).

Remark 11.2: More generally if $H, N \leq G$ and $H \leq N_G(N)$, one replaces G by the normalizer $N_G(N)$, and a) holds with $H\,N = N\,H \leq N_G(N)$ and b) is unchanged.

If $N \leq H \leq G$, then $H\,N = N\,H = H$, so that a) is true, and if one adds $N \triangleleft G$, then $N \triangleleft H$, which is the first part of b), and the second part is obvious since both sides are H/N.

If $H \leq N \leq G$, then $H\,N = N\,H = N$, so that a) is true, and one does not need to add $N \triangleleft G$, for having b) since $N \cap H$ being H is a normal subgroup of H, and the second part is obvious since both sides are $\{e\}$ as quotient of a group by itself.

Lemma 11.3: Let $K, L \leq G$ be such $K \cap L = \{e\}$. Then, each $g \in K\,L$ can be written in a unique way as $g = k\,\ell$ with $k \in K, \ell \in L$.

If $K \cap L \neq \{e\}$, with K and L finite, then $|K\,L| = \frac{|K|\,|L|}{|K \cap L|}$.

Proof: By definition, each $g \in K\,L$ can be written as $g = k\,\ell$ for some $k \in K$ and $\ell \in L$, so that only uniqueness must be proved. If $k_1\ell_1 = k_2\ell_2$, one deduces that $k_2^{-1}k_1 = \ell_2\ell_1^{-1}$, which then belongs to both K and L, and must be e, but $k_2^{-1}k_1 = e$ means $k_1 = k_2$, and $\ell_2\ell_1^{-1} = e$ means $\ell_1 = \ell_2$.

$K\,L$ is the union of the cosets $k\,L$ for $k \in K$. One has $k_1L = k_2L$ if and only if $k_2^{-1}k_1 \in L$, so that it belongs to $K \cap L$; for each $k_1 \in K$, there are exactly $|K \cap L|$ elements $k_2 \in K$ giving the same coset as k_1, so that there are $\frac{|K|}{|K \cap L|}$ distinct cosets, and each coset has size $|L|$, hence the size of $K\,L$.

Lemma 11.4: Let $G = K \times L$ for groups K and L, and let $K_1 = K \times \{e\} \simeq K$ and $L_1 = \{e\} \times L \simeq L$. Then, $K_1, L_1 \triangleleft G$, $G = K_1L_1 = L_1K_1$, with $K_1 \cap L_1 = \{e\}$.

Conversely, if $K, L \triangleleft G$ for a group G, with $K \cap L = \{e\}$ and $G = K\,L$, then elements from K and L commute (so that $G = L\,K$) and $G \simeq K \times L$ via the homomorphism $g = k\,\ell \mapsto (k, \ell)$.

Proof: The kernel of the projection π_1 of G onto K is L_1, and the kernel of the projection π_2 of G onto L is K_1, so that K_1 and L_1 are normal subgroups of G (since π_1 and π_2 are homomorphisms). Then $g = (k, \ell) = (k, e) \cdot (e, \ell) \in K_1L_1$ and $g = (e, \ell) \cdot (k, e) \in L_1K_1$. Finally, $g = (k, \ell) \in K_1$ means $\ell = e$, and $g \in L_1$ means $k = e$, so that $g \in K_1 \cap L_1$ means $g = (e, e) = e$ (which means $(e_K, e_L) = e_G$, of course).

Because K is a normal subgroup of G, one has $g\,K = K\,g$ for all $g \in G$, so that $\ell\,K = K\,\ell$ for all $\ell \in L$, which implies $L\,K = K\,L$, which is G. In particular, for $k \in K$ one has $\ell\,k = k_1\,\ell$ for some $k_1 \in K$, but also, because L is a normal subgroup of G, one has $\ell\,k = k\,\ell_1$ for some $\ell_1 \in L$; then, $k_1\,\ell = k\,\ell_1$ implies $k_1 = k$ and $\ell_1 = \ell$ by the uniqueness (resulting from $K\mathcal{L} = \{\rceil\}$), so that k and ℓ commute. The mapping ψ from G into $K \times L$ such that $g = k\,\ell$ gives $\psi(g) = (k, \ell)$ is well defined, because k and ℓ are uniquely defined; ψ is an homomorphism, since if $g' = k'\ell'$, one has $g\,g' = (k\,\ell)\,(k'\ell') = (k\,k')\,(\ell\,\ell')$ (because ℓ and k' commute), so that $\psi(g\,g') = (k\,k', \ell\,\ell') = (k, \ell)\,(k', \ell') = \psi(g)\,\psi(g')$. Of course, ψ is bijective because for every $(k, \ell) \in K \times L$, there is exactly one g with $\psi(g) = (k, \ell)$, which is $g = k\,\ell$.

Theorem 11.5: (Sylow's theorems) Let p be a prime dividing $|G|$ and such that $|G| = p^n a$ (with $n \geq 1$) and p does not divide a. Then, every subgroup of G whose order is a power of p is included in a Sylow

[1] It is also called the diamond isomorphism theorem.

p-subgroup, all Sylow p-subgroups are conjugate, and their number is congruent to 1 modulo p, and divides $|G|$, so that it divides a.
Proof: a) Let Σ be the family of p-subgroups of G, which by Cauchy's theorem is not empty. Let Ω be the elements of Σ which are maximal for inclusion; because $|\Sigma| < \infty$, every element of Σ is included in an element of Ω. If G acts on subgroups by conjugation, then G acts on Σ (since conjugate subgroups have the same order), and G acts on Ω (since conjugation preserves inclusion).

b) If $P \in \Omega$, one considers the P-action on Ω (i.e. for $Q \in \Omega$ the orbit is made of the $g\,Q\,g^{-1}$ for $g \in P$), and one shows that P is the only fixed point of this action. Indeed, if $Q \in \Omega$ is fixed by P it means that $P \leq N_G(Q)$, so that $P\,Q \leq G$. By Lagrange's theorem, $|P \cap Q|$ is a power of p (so that $P \cap Q \in \Sigma$), and by the formula for the size of a product ($|P\,Q| = \frac{|P|\,|Q|}{|P \cap Q|}$) $P\,Q \in \Sigma$, but since $P\,Q$ contains both P and Q (since $e \in P \cap Q$), one has $P = P\,Q = Q$ by maximality of P and of Q.

c) All elements of Ω are conjugate. If it was not true, there would exist $P \in \Omega$ having orbit A, and $Q \in \Omega$ having orbit B, with A and B disjoint. Then in the P-action on A and on B, P is the only fixed point, and all the other orbits have a size dividing $|P|$, i.e. a power of p, so that $|A|$ is congruent to 1 and $|B|$ is congruent to 0 modulo p; using then the Q-action on A and on B gives a contradiction, that $|A|$ is congruent to 0 and $|B|$ is congruent to 1 modulo p.

d) If $P \in \Omega$, then by c) its orbit is Ω and $|\Omega|$ is congruent to 1 modulo p, but the size of the orbit divides $|G|$, so that it divides a.

e) Any Sylow-p subgroup is necessarily maximal, and belongs to Ω; conversely, one needs to show that every $H \in \Omega$ must be a Sylow-p subgroup. By d) the orbit of H is Ω and its size b is congruent to 1 modulo p and divides a, but it is also the index of $N_G(H)$ in G, so that the order of $N_G(H)$ is $p^n c$ with $b\,c = a$. If H was not a Sylow-p subgroup, its order would be p^m for $1 \leq m < n$, and the order of $N_G(H)$ being $p^n c$, the quotient space $N_G(H)/H$ (defined since $H \triangleleft N_G(H)$) would have order $p^{n-m}c$ which is a multiple of p, hence by Cauchy's theorem it would have a subgroup K order p; if π denotes the projection of $N_G(H)$ onto $N_G(H)/H$ the subgroup $\pi^{-1}(K)$ of $N_G(H) \leq G$ would have order a power of p and would contain H strictly, contradicting the maximality of H.

Remark 11.6: G has a unique Sylow-p subgroup if and only if it has a normal Sylow-p subgroup, and in this case the subgroup is characteristic. Indeed, the conjugates of the Sylow p-subgroup H are all the Sylow-p subgroups, i.e. they are equal to H, i.e. H is normal, and conversely. Then, if $\psi \in Aut(G)$ it must map H to a subgroup of the same size, and there is only H.

12- Monday September 26, 2011.

Lemma 12.1: If P is a Sylow-p subgroup of G, it is the unique Sylow-p subgroup of $Q = N_G(P)$, and $N_G(Q) = Q$.
Proof: P is a normal subgroup $N_G(P)$, which has size $p^n b$ for a divisor b of a, so that P is a Sylow-p subgroup of $N_G(P)$, hence it is its only Sylow-p subgroup.

For $r \in N_G(Q)$, the conjugate P^r is a Sylow-p subgroup of Q^r, but $Q^r = Q$ by definition of $N_G(Q)$, so that P^r is a Sylow-p subgroup of Q, and it must then be P, but $P^r = P$ means $r \in N_G(P)$ by definition, so that $r \in Q$.

Lemma 12.2: If $|G| = 2p$ for a group G, with p an *odd prime*, then G is either isomorphic to $\mathbb{Z}_{2p}$ or to D_p.
Proof: The number n_2 of Sylow-2 subgroups is either 1 or p, and the number n_p of Sylow-p subgroups is 1. If $n_2 = 1$, one concludes as seen before that $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_p$, which is $\simeq \mathbb{Z}_{2p}$ by the Chinese remainder theorem.

If $n_2 = p$, one wants to show that $G \simeq D_p$. Let $N = \{e, \alpha, \alpha^2, \ldots, \alpha^{p-1}\} \triangleleft G$ be the Sylow-p subgroup, and let $H_j = \{e, b_j\}$, $j = 1, \ldots, p$ be the Sylow-2-subgroups, which are all conjugate, so that for each j there is k such that $\alpha\, H_j \alpha^{-1} = H_k$, i.e. $\alpha\, b_j \alpha^{-1} = b_k$. One cannot have $k = j$, since it would imply that b_j commutes with α hence with all elements of N, and then G would coincide with the product $H_j \times N$ generated by N and b_j, so that G would be Abelian (which only occurs if $n_2 = 1$); the same argument shows that $\alpha^\ell b_j \alpha^{-\ell} \neq b_j$ when ℓ is not a multiple of p, so that starting from b_1 and conjugating with α generates all the b_j, and one can then change the indexing so that $\alpha^\ell b_1 \alpha^{-\ell} = b_{1+\ell}$ for all ℓ. Since $N \triangleleft G$, one has $b_1 \alpha\, b_1^{-1} = \alpha^m$ for some $m \in \{2, \ldots, p-1\}$, since $m = 0$ would imply $\alpha = e$ and $m = 1$ would imply that b_1 and α commute; from $b_1 \alpha = \alpha^m b_1$, one deduces by induction that $b_1 \alpha^j = \alpha^{j\,m} b_1$ for all j, and then $b_{1+\ell} = \alpha^\ell b_1 \alpha^{-\ell} = \alpha^{\ell - \ell\, m} b_1$, which is $a^\ell b_1$ if one takes $a = \alpha^{1-m}$, which is a generator of N, and this gives the structure of D_p.

Lemma 12.3: If a group G has a normal subgroup N and a subgroup H such that $N \cap H = \{e\}$ and $N\,H = G$ (hence $H\,N = N\,H$),[1] then G is isomorphic to a semi-direct product $N \times_\psi H$ for the automorphism ψ from H into $Aut(N)$ given by $\psi_h(n) = h\,n\,h^{-1}$ for $n \in N, h \in H$.
Proof: Every $g \in G$ can be written in a unique way as $g = n\,h$ for some $n \in N, h \in H$, and the mapping $g \mapsto (n, h)$ is a bijection (but not an homomorphism in general). The definition of ψ by $\psi_h(n) = h\,n\,h^{-1}$ shows that $\psi \in Aut(N)$ because N is a normal subgroup. The product of $g_1 = n_1 h_1$ by $g_2 = n_2 h_2$ in G consists in writing $n_1 h_1 n_2 h_2$ and then wondering for which $n \in N, h \in H$ this product is $n\,h$, and since $n_1 h_1 n_2 h_2 = n_1 (h_1 n_2 h_1^{-1})\, h_1 h_2$, one has $n = n_1 (h_1 n_2 h_1^{-1}) \in N$ (because $h_1 n_2 h_1^{-1} \in N$ since N is normal) and $h = h_1 h_2 \in H$, and it is exactly what $(n_1, h_1) \star_\psi (n_2, h_2)$ gives.

Lemma 12.4: Let G be a finite *simple* group acting on a set X, then any orbit *not reduced to a point* has a size s such that $s! \geq |G|$.

If H is a *proper* subgroup of G (i.e. $H \neq G$), then the index i of H satisfies $i! \geq |G|$.
Proof: Let Y be an orbit not reduced to a point and having size $s > 1$, then the action restricted to Y is an homomorphism of G into S_Y (the group of bijection of Y onto itself), and its kernel is then a normal subgroup of G, which is then either $\{e\}$ or G, since G is simple. The kernel is not G, since it would imply $|Y| = 1$, so that it is $\{e\}$ and the mapping from G into S_Y is injective, so that S_Y contains an isomorphic copy of G, and this implies $|G| \leq |S_Y| = s!$.

One considers the action of G on the set X of left cosets of H by multiplication from the left. This action is an injective mapping from G into S_X, and the size of the orbit is the index i of H in G, and $|H| < |G|$ implies $i > 1$, so that by the first part one must have $i! \geq |G|$.

Remark 12.5: For a finite simple group, one has $n_p > 1$ for each prime p dividing $|G|$ since no Sylow p-subgroup can be a normal subgroup, but Lemma 12.4 gives a much stronger property, than $n_p! \geq |G|$ for each prime p dividing $|G|$.

[1] If G is finite, it is equivalent to $|N|\,|H| = |G|$.

Since the index of a subgroup cannot be too small, a finite simple group lacks large proper subgroups, and it is useful to observe that Lagrange's theorem says that if $|G| = n$, and $H \leq G$ with $|H| = d$, then d is a divisor of n, but that it is not true that for every divisor d of n there exists a subgroup of G of size d: the smallest value of n for which one has a counter-example is $n = 12$, since A_4 has order 12, but has no subgroup of order 6.

Indeed, A_4 has eight elements of order 3 which are the cyclic permutations of three elements in $\{1, 2, 3, 4\}$ (for example, the two ones fixing 1 are $(2\,3\,4)$ and its square $(2\,4\,3)$), and three elements of order 2, which are $(1\,2)\,(3\,4)$, $(1\,3)\,(2\,4)$, and $(1\,4)\,(2\,3)$, which with e form the normal subgroup N (isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$) mentioned before; if A_4 had a subgroup H of order 6, H could not be isomorphic to $\mathbb{Z}_6$, since no element of A_4 (or even of S_4) has order 6, so that H would be isomorphic to S_3, but S_3 has three elements of order 2 (the transpositions), hence H would contain the three elements of order 2 in A_4, and this would contradict Lagrange's theorem, since H would contain N which has order 4.

Remark 12.6: It will be shown in another lecture that A_n is simple for $n \geq 5$, so that since it has order $\frac{n!}{2}$, the smallest value of s for which $s! \geq |A_n|$ is n, hence for $n \geq 5$ the proper subgroups of A_n have index $\geq n$. For A_5, which has order 60, it implies that there is no subgroup of A_5 of order 15, 20, or 30 (the divisors d of 60 such that $d < 60$ and $\frac{60}{d} < 5$).

Remark 12.7: If p is prime, any group of order p is isomorphic to $\mathbb{Z}_p$, which is simple, so that one may wonder if 60 is the smallest composite integer n for which there exists a simple group of order n.

The structure theorem of finite Abelian groups will be shown in another lecture, and it says that a non-trivial finite Abelian group G is isomorphic to $\mathbb{Z}_{d_1} \times \cdots \times \mathbb{Z}_{d_k}$ with $k \geq 1$ and d_i divides d_{i+1} for $i = 1, \ldots, k-1$, hence an Abelian group G is simple if and only if $G \simeq \mathbb{Z}_p$ for a prime p.

It will be shown in another lecture that if $n = p^k$ for a prime p and $k \geq 2$, and G has order n, its center $Z(G)$ is non-trivial (i.e. $\neq \{e\}$), and since $Z(G)$ is a characteristic subgroup of G, hence a normal subgroup of G, G is not simple.[2]

For $6 < n \leq 24$ and n composite having at least two prime divisors (since one is not interested in powers of primes), there is no group of order n which is simple: there cannot be more than two prime divisors since $2 \cdot 3 \cdot 5 = 30 > 24$, and if $n = p^\alpha q^\beta$ with primes $p < q$, one needs to have $n_p, n_q \geq 4$, so that because n_p divides q^β and n_q divides p^α, 2 and 3 must only appear with an exponent ≥ 2, and this constraint is sufficient for eliminating all these values of n.

For $24 < n \leq 120$ and n composite having at least two prime divisors, one must have $n_p \geq 5$ for each prime divisor p, so that for the integers of the form $p^\alpha q^\beta$ with primes $p < q$, 2 must only appear with an exponent ≥ 3, and 3 must only appear with an exponent ≥ 2: if I have made no errors, only 19 such integers (with exactly two distinct prime divisors) pass this first test,[3] and there are also 13 integers with three distinct prime divisors.[4] One then uses the more precise constraint of imposing on n_p the two congruences of the Sylow's theorem, for each prime divisor of n, and I find that the integers remaining after this test are 30 ($n_2 \in \{5, 15\}$, $n_3 = 10$, $n_5 = 6$), 56 ($n_2 = 7$, $n_7 = 8$), 60 ($n_2 \in \{5, 15\}$, $n_3 = 10$, $n_5 = 6$), 80 ($n_2 = 5$, $n_5 = 16$), 90 ($n_2 \in \{5, 9, 15, 45\}$, $n_3 = 10$, $n_5 = 6$), 105 ($n_3 \in \{5, 7, 35\}$, $n_5 = 21$, $n_7 = 15$), 112 ($n_2 = 7$, $n_7 = 8$), and 120 ($n_2 \in \{5, 15\}$, $n_3 = 10$, $n_5 = 6$). Then, one checks if the order of elements predicted by these values of n_p are compatible with the size of the group, and no simple group of order 30 exists, since $n_3 = 10$ implies the existence of exactly 20 elements of order 3, and $n_5 = 6$ implies the existence of exactly 24 elements of order 5, already too much for a group of order 30. That no simple group of order 56 exists is similar, since $n_7 = 8$ implies the existence of exactly 48 elements of order 7, so that only 8 elements remain, enough for just one Sylow 2-subgroup (of order 8). The smallest value of n is then 60.[5]

---

[2] To be complete, one should observe that $Z(G) = G$ means that G is Abelian.

[3] I find 35, 40, 45, 55, 56, 63, 65, 72, 77, 80, 85, 88, 95, 99, 104, 112, 115, 117, and 119.

[4] I find 30, 42, 60, 66, 70, 78, 84, 90, 102, 105, 110, 114, and 120.

[5] There is no simple group of order 80, since $n_5 = 16$ implies the existence of exactly 64 elements of order 5, so that only 16 elements remain, enough for just one Sylow 2-subgroup (of order 16). There is no simple group of order 105, since $n_5 = 21$ implies the existence of exactly 84 elements of order 5, $n_7 = 15$ implies the existence of exactly 90 elements of order 7, already too much for a group of order 105. That there are no simple groups of order 90, 112, or 120 is more technical to prove.

Remark 12.8: In order to understand which are the groups of order 12 (up to isomorphism), one starts with what Sylow's theorem implies. One has $n_2 = 1 \pmod 2$ and n_2 divides 3, so that $n_2 \in \{1, 3\}$, and one has $n_3 = 1 \pmod 3$ and n_3 divides 4, so that $n_3 \in \{1, 4\}$.

The case $n_2 = n_3 = 1$ implies the existence of a unique normal Sylow 2-subgroup H_2 (of order 4, hence isomorphic to either $\mathbb{Z}_4$ or to $\mathbb{Z}_2 \times \mathbb{Z}_2$), and of a unique normal Sylow 3-subgroup H_3 (of order 3, hence isomorphic to $\mathbb{Z}_3$), and since $H_2 \cap H_3 = \{e\}$ and $|G| = |H_2|\,|H_3|$, one deduces that G is isomorphic to $H_2 \times H_3$; this means that G is Abelian, and either isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_3$, which is isomorphic to $\mathbb{Z}_{12}$ by the Chinese remainder theorem, or isomorphic to $(\mathbb{Z}_2 \times \mathbb{Z}_2) \times \mathbb{Z}_3$, which is isomorphic to $\mathbb{Z}_2 \times (\mathbb{Z}_2 \times \mathbb{Z}_3)$, itself isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_6$ by the Chinese remainder theorem.

The case $n_2 = 3$ and $n_3 = 4$ cannot happen, because $n_3 = 4$ implies the existence of exactly 8 elements of order 3, so that only 4 elements remain, enough for just one Sylow 2-subgroup (of order 4).

Remark 12.9: A (non-Abelian) group G of order 12 with $n_2 = 1, n_3 = 4$ has a unique Sylow 2-subgroup H_2 (of order 4) which is a normal subgroup of G, and four Sylow 3-subgroups K_1, K_2, K_3, K_4 (of order 3). Since $H_2 \cap K_j = \{e\}$ by Lagrange's theorem, and $|G| = |H_2|\,|K_j|$, G is isomorphic to a (non-trivial) semi-direct product $H_2 \times_\psi \mathbb{Z}_3$ (since $K_j \simeq \mathbb{Z}_3$) for a (non-trivial) homomorphism ψ from $\mathbb{Z}_3$ into $Aut(H_2)$. In the case of A_4, the Sylow 2-subgroup is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, and since H_2 is either isomorphic to $\mathbb{Z}_4$ or to $\mathbb{Z}_2 \times \mathbb{Z}_2$, it is useful to observe that only the trivial homomorphism exists from $\mathbb{Z}_3$ into $Aut(\mathbb{Z}_4)$: indeed, $Aut(\mathbb{Z}_4)$ is isomorphic to the multiplicative group $\mathbb{Z}_4^*$ of units of the ring $\mathbb{Z}_4$ (the multiplicative group $\{1, 3\}$ modulo 4), i.e. isomorphic to the additive group $\mathbb{Z}_2$, and only the trivial homomorphism exists from $\mathbb{Z}_3$ into $\mathbb{Z}_2$; this shows that H_2 must be isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Since $\mathbb{Z}_2 \times \mathbb{Z}_2$ has three elements (a, b, and c) of order 2 (which satisfy $a\,b = b\,a = c$, $b\,c = c\,b = a$ and $c\,a = a\,c = b$), one has an automorphism of $\mathbb{Z}_2 \times \mathbb{Z}_2$ for each permutation of a, b, and c, so that $Aut(\mathbb{Z}_2 \times \mathbb{Z}_2) \simeq S_3$; S_3 has a unique subgroup of order 3, which corresponds to the cyclic permutations, so that one non-trivial homomorphism ψ sends $1 \in \mathbb{Z}_3$ to the automorphism induced by the cyclic permutation $(a\,b\,c)$, and $2 \in \mathbb{Z}_3$ to the automorphism induced by the cyclic permutation $(a\,b\,c)^2 = (a\,c\,b)$. The other non-trivial homomorphism is ψ^2 (which is ψ^{-1} since ψ has order 3), i.e. sends $1 \in \mathbb{Z}_3$ to the automorphism induced by the cyclic permutation $(a\,c\,b)$, and $2 \in \mathbb{Z}_3$ to the automorphism induced by the cyclic permutation $(a\,b\,c)$.

Remark 12.10: A (non-Abelian) group G of order 12 with $n_2 = 3, n_3 = 1$ has three Sylow 2-subgroups L_1, L_2, L_3 (of order 4), and a unique Sylow 3-subgroup H_3 (of order 3) which is a normal subgroup of G. Since $H_3 \cap L_j = \{e\}$ by Lagrange's theorem, and $|G| = |H_3|\,|L_j|$, G is isomorphic to a (non-trivial) semi-direct product $\mathbb{Z}_3 \times_\psi L_j$ (since H_3 is isomorphic to $\mathbb{Z}_3$) for a (non-trivial) homomorphism ψ from L_j into $Aut(\mathbb{Z}_3)$, and L_j is either homomorphic to $\mathbb{Z}_4$ of to $\mathbb{Z}_2 \times \mathbb{Z}_2$.

Since $Aut(\mathbb{Z}_3)$ is isomorphic to the multiplicative group $\mathbb{Z}_3^*$ of non-zero elements of the field $\mathbb{Z}_3$ (the multiplicative group $\{1, 2\}$ modulo 3), i.e. isomorphic to the additive group $\mathbb{Z}_2$, a non-trivial homomorphism of a group Γ into $Aut(\mathbb{Z}_3)$ exists if and only if Γ has a subgroup N of index 2 (which is automatically a normal subgroup of Γ), so that N is sent to the identity of $Aut(\mathbb{Z}_3)$ and the other coset $a\,N$ (for $a \notin N$) is then to the other element of $Aut(\mathbb{Z}_3)$.

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 π 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 ≥ 4. If $\sigma = (a_1 \cdots a_r)\,\tau \in N$ with $r \geq 4$, and τ 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 τ 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 τ 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 Γ (here either $GL_m(F)$ or $SL_m(F)$) consists in taking the quotient $\Gamma/Z(\Gamma)$ of the group Γ 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 ± 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 μ. 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 τ (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 τ 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 α, β, γ 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 ∞ in a particular way: one first adds a point at ∞ in the direction $(\cos\theta, \sin\theta)$ for each θ modulo 2π, 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 θ the point at ∞ in the direction θ and the point at ∞ 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 ∞.[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 ∞ 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 ∞ containing all the $q + 1$ points added at ∞.

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 $c = a_2 a_1^{-1}$, and then all the elements $(0, a_2)$ with $a_2 \neq 0$ belong to the same equivalence class, which one naturally calls ∞.

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.

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

14- Friday September 30, 2011.

Remark 14.1: $G = S_5$ has only one subgroup of order 60, which is A_5: if there was $H \leq G$ with $H \neq A_5$, one would choose $a \in A_5 \setminus H$, so that $G = H \cup (a\,H)$ (because $|H| = 60$ and $a \notin H$) and taking the intersection with A_5, the union of $H \cap A_5$ and $(a\,H) \cap A_5$ would be A_5, but $(a\,H) \cap A_5 = a\,(H \cap A_5)$ since $a \in A_5$,[1] so that $K = H \cap A_5$ would be a subgroup of A_5 and $a\,K$ would have the same number of elements as K, which would imply that K has size 30, a contradiction since A_5 is simple hence has no proper subgroup of index ≤ 4 (because $4! < |A_5|$).

Remark 14.2: 5-cycles belong to A_5, and (by putting 1 as the first element of a cycle) there are 4! of them, which makes 24 elements of order 5. 4-cycles are odd permutations, which do not belong to A_5. 3-cycles belong to A_5, and there are $\binom{5}{3} = 10$ subsets of 3 elements, and each subset $\{a, b, c\}$ corresponds to two 3-cycles ($(a\,b\,c)$ and its square $(a\,c\,b)$), which makes 20 elements of order 3. A permutation having one 3-cycle and one 2-cycle is an odd permutation, as well as a 2-cycle, so that they do not belong to A_5. A permutation with two disjoint 2-cycles belongs to A_5, and for those fixing one element in $\{1, 2, 3, 4, 5\}$ there are 3, which makes 15 elements of order 2.

Remark 14.3: Each 5-cycle $\sigma \in A_5$ generates a cyclic subgroup H of order 5, $\{e, \sigma, \sigma^2, \sigma^3, \sigma^4\}$, so that there are 6 such Sylow 5-subgroups. Interpreting a cycle like $(1\,2\,3\,4\,5)$ as a rotation of $\frac{2\pi}{5}$ of a regular pentagon with vertices named 1, 2, 3, 4, 5 (in this order), one can then interpret the five mirror symmetries as $(2\,5)\,(3\,4)$, $(1\,3)\,(4\,5)$, $(1\,5)\,(2\,4)$, $(1\,2)\,(3\,4)$, and $(1\,4)\,(2\,3)$, which with H form a subgroup K isomorphic to D_5. Since each of these six isomorphic copies of D_5 use up five elements of order 2 and there are only 15 of them, one expects that each element of order 2 is associated with two unrelated 5-cycles (i.e. generating different cyclic subgroups): for example $(2\,5)\,(3\,4)$ is associated with $\sigma = (1\,2\,3\,4\,5)$ (and its powers $\sigma^2 = (1\,3\,5\,2\,4)$, $\sigma^3 = (1\,4\,2\,5\,3)$, and $\sigma^4 = (1\,5\,4\,3\,2)$) but also with $\pi = (1\,2\,4\,3\,5)$ (and its powers $\pi^2 = (1\,4\,5\,2\,3)$, $\pi^3 = (1\,3\,2\,5\,4)$, and $\pi^4 = (1\,5\,3\,4\,2)$).

Each K is the normalizer of the cyclic subgroup H since H is a normal subgroup of K and the only subgroup containing K is A_5 (because A_5 has no subgroups of order 20 or 30), but A_5 has no normal proper non-trivial subgroup.

Actually, any subgroup L of G of order 10 should contain a subgroup of order 5, i.e. one of the H_j, and since H_j is automatically a normal subgroup of L, L must be equal to $K_j = N_G(H_j)$.

Remark 14.4: Each 3-cycle $\sigma \in A_5$ generates a cyclic subgroup H of order 3, $\{e, \sigma, \sigma^2\}$, so that there are 10 such Sylow 3-subgroups. Considering a cycle like $(1\,2\,3)$, one can add to H the three elements (of order 2) $\tau\,(4\,5)$ where τ is a transposition on $\{1, 2, 3\}$, and obtain a subgroup K isomorphic to S_3.[2] Since each of these ten isomorphic copies of S_3 use up three elements of order 2 and there are only 15 of them, one expects that each element of order 2 is associated with two unrelated 3-cycles (i.e. generating different cyclic subgroups): for example $(1\,2)\,(3\,4)$ is associated with $\sigma = (1\,2\,5)$ (and its square $\sigma^2 = (1\,5\,2)$) but also with $\pi = (3\,4\,5)$ (and its square $\pi^2 = (3\,5\,4)$).

Each H is a normal subgroup of the corresponding K, but since A_5 has subgroups of order 12, it is simpler to invoke Sylow's theorem for being sure that K is the normalizer of H (since the orbit of H by conjugation has size 10, hence the normalizer $N_G(H)$ has order 6), and then since H is a Sylow 3-subgroup and $K = N_G(H)$, one has $N_G(K) = K$, so that if $K \leq L \leq G$ with $K \neq L$, one must have $L = G$, since Lagrange's theorem implies that the order of L is a strict multiple of 6 and a divisor of 60, so that it could only be 12 or 30 or 60, but there is no subgroup of A_5 of order 30, and the subgroups of order 12 cannot contain K, since K would automatically be a normal subgroup of such a subgroup of order 12.

Actually, any subgroup M of G of order 6 should contain a subgroup of order 3, i.e. one of the H_j, and since H_j is automatically a normal subgroup of M, M must be equal to $K_j = N_G(H_j)$. However,

[1] If $a\,h = b \in A_5$ with $h \in H$, then $h = a^{-1}b$ belongs to A_5, so that $h \in H \cap A_5$, hence $b = a\,h \in a\,(H \cap A_5)$.

[2] If $h \in H = \{e, (1\,2\,3), (1\,3\,2)\}$, then $h\,\big(\tau\,(4\,5)\big) = (h\,\tau)\,(4\,5)$, and $h\,\tau$ is a transposition on $\{1, 2, 3\}$, while the product of $\tau_1(4\,5)$ by $\tau_2(4\,5)$ is $\tau_1\tau_2$, which belongs to H.

there are (at least) two subgroups of G of order 12 containing H, since there are two distinct elements $a, b \in \{1,2,3,4,5\}$ left invariant by the 3-cycles σ and σ^2 of H_j, so that H_j is included in the isomorphic copy of A_4 leaving a fixed, and in the isomorphic copy of A_4 leaving b fixed, and the intersection of these two subgroups of order 12 leave a and b fixed, so that it is H.

Remark 14.5: Let K_1, K_2, K_3, K_4, K_5 be the five subgroups of A_5 of order 12 and isomorphic to A_4, where K_j are the permutations in A_5 which leave j fixed. K_j has a normal subgroup N_j isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, containing 3 elements of order 2, which are not repeated since for $j \neq i$ the intersection $K_i \cap K_j$ are the permutations in A_5 which leave both i and j fixed, which is one of the Sylow 3-subgroup (containing no element of order 2), so that the five Sylow 2-subgroups of A_5 are the N_j, and one has $N_G(N_j) = K_j$, since it contains K_j but cannot be larger (because a subgroup containing strictly a subgroup of order 12 must have order 60).

Remark 14.6: All the subgroups of order 3, 4, or 5 of A_5 have been accounted for, since they are the Sylow p-subgoups (10 subgroups of order 3, 5 subgroups of order 4, 6 subgroups of order 5), and their normalizers have been identified (10 subgroups of order 6 isomorphic to S_3, 5 subgroups of order 12 isomorphic to A_4, 6 subgroups of order 10 isomorphic to D_5).

Any subgroup K of order 6 contains a subgroup H of order 3, which is automatically normal in K, so that K is $N_G(H)$ for a Sylow 3-subgroup H, hence it is isomorphic to S_3, and there are 10 of them.

Any subgroup K of order 10 contains a subgroup H of order 5, which is automatically normal in K, so that K is $N_G(H)$ for a Sylow 5-subgroup H, hence it is isomorphic to D_5, and there are 6 of them.

Let K be a subgroup of order 12, which contains a 3-cycle $(x\,y\,z)$ and an element $(a\,b)\,(c\,d)$ of order 2. If the element $\in \{1,2,3,4,5\}$ fixed by $(a\,b)\,(c\,d)$ is also fixed by $(x\,y\,z)$, they belong to one K_j isomorphic to A_4, and the subgroup generated by $(x\,y\,z)$ and $(a\,b)\,(c\,d)$ must be K_j, or it would be a subgroup of order 6, automatically normal in K, but any subgroup of order 6 has been identified to be $N_G(H)$ for a Sylow 3-subgroup H, hence is its own normalizer. If the element $\in \{1,2,3,4,5\}$ fixed by $(a\,b)\,(c\,d)$ belongs to $\{x,y,z\}$, say it is x, one arrives at a contradiction: either the element of order 2 sends y onto z, and both elements belong to the normalizer $N_G(H)$ of the Sylow 3-subgroup generated by $(x\,y\,z)$, which is its own normalizer and cannot belong to a subgroup of order 12, or the element of order 2 sends y onto an element different from x and z, and the situation is like having $(1\,2\,3)$ and $(2\,4)\,(3\,5)$, but the product $(1\,2\,3)\,(2\,4)\,(3\,5)$ is $(1\,2\,4\,3\,5)$, which has order 5. The subgroups of order 12 are then the 5 subgroups isomorphic to A_4.

There are 15 subgroups of order 2, of the form $\{e, \sigma\}$ for an element $\sigma = (a\,b)\,(c\,d)$ of order 2, but what is the normalizer K of $\{e,\sigma\}$? It is the centralizer of σ, i.e. the subgroup of elements of A_5 which commute with σ, and it contains the Sylow 2-subgroup H containing σ, since H is Abelian, isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, so that its order is a multiple of 4 which divides 60, i.e. it is 4 or 12, or 60, but it must then be 4, so that $K = H$, since if it was 12 or 60 K would contain an isomorphic copy of A_4 containing σ, but in A_4 an element of order 2 does not commute with an element of order 3.[3]

Lemma 14.7: Let G be any *simple* group of order 60, and for $p = 2, 3, 5$, let n_p be the number of Sylow p-subgroups of G. Then, one has $n_2 = 5$, $n_3 = 10$, and $n_5 = 6$. Each Sylow-2 subgroup H_i is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$, and two distinct Sylow 2-subgroups only intersect at $\{e\}$, so that the five Sylow 2-subgroups make 15 elements of order 2. Each Sylow-3 subgroup K_j is isomorphic to $\mathbb{Z}_3$, its normalizer $N_G(K_j)$ has order 6 and is isomorphic to S_3, and the ten Sylow 3-subgroups make 20 elements of order 3. Each Sylow-5 subgroup L_k is isomorphic to $\mathbb{Z}_5$, its normalizer $N_G(L_k)$ has order 10 and is isomorphic to D_5, and the six Sylow 5-subgroups make 24 elements of order 5.

Proof: Since G is simple with $4! = 24 < |G| < 5! = 120$, each n_p is ≥ 5. By the Sylow's theorem, $n_2 = 1 \pmod 2$ and divides 15, so that $n_2 \in \{5, 15\}$, $n_3 = 1 \pmod 3$ and divides 20, so that $n_3 = 10$, and $n_5 = 1 \pmod 5$ and divides 12, so that $n_5 = 6$. The ten Sylow 3-subgroups contain 20 elements of order 3, and the six Sylow 5-subgroups contain 24 elements of order 5, so that at most 15 elements can have order $\notin \{1,3,5\}$, and the last element is e. One wants to show that $n_2 = 5$ and that two distinct Sylow 2-subgroups only intersect at $\{e\}$, so that the five Sylow 2-subgroups use up the 15 elements. If it was not true, either $n_2 = 5$ and two distinct Sylow 2-subgroups H and H' would contain $g \neq e$, or $n_2 = 15$, and by the pigeon-hole

[3] Without loss of generality, one may take the element of order 3 to be $(1\,2\,3)$ and the element of order 2 to be $(1\,2)\,(3\,4)$, and $(1\,2\,3)\,(1\,2)\,(3\,4) = (1\,3\,4)$, while $(1\,2)\,(3\,4)\,(1\,2\,3) = (2\,4\,3)$.

principle there would exist two distinct Sylow 2-subgroups intersecting at more than $\{e\}$ (or there would be 45 elements of order 2 or 4), and one shows that it leads to a contradiction.

Since g must have order 2 (because $H \neq H'$), let $L = N_G(\langle g \rangle)$ be the normalizer of the subgroup $\langle g \rangle = \{e, g\}$ generated by g; since H and H' are Abelian (isomorphic to $\mathbb{Z}_4$ or to $\mathbb{Z}_2 \times \mathbb{Z}_2$), H and H' are subgroups of L, hence by Lagrange's theorem the order of L is a multiple of 4 which divides 60, so that the only possibilities are 4, 12, 20, or 60: 4 is excluded because it implies $H = H'$, 20 is excluded because the index of a subgroup must be ≥ 5, 60 is excluded because it implies that $\langle z \rangle$ is a normal subgroup of G, hence $|L| = 12$. Since L has index 5, there is an injective homomorphism from G into S_5, so that G is isomorphic to a subgroup of S_5 of order 60, hence $L = A_5$, but in A_5 two distinct Sylow 2-subgroups only intersect at $\{e\}$.

If H is a Sylow-3 subgroup, its orbit by conjugation has size 10, which is the index of its normalizer $N_G(H)$ so that $N_G(H)$ has order 6, and a group of order 6 is either isomorphic to $\mathbb{Z}_6$ or to S_3, but $\mathbb{Z}_6$ is excluded since G contains no element of order 6. If H is a Sylow-5 subgroup, its orbit by conjugation has size 6, which is the index of its normalizer $N_G(H)$ so that $N_G(H)$ has order 10, and a group of order 10 is either isomorphic to $\mathbb{Z}_{10}$ or to D_5, but $\mathbb{Z}_{10}$ is excluded since G contains no element of order 10.

If the Sylow 2-subgroup H_j is isomorphic to $\mathbb{Z}_4$, then it contains exactly one subgroup K_j of order 2, with $K_j = \{e, a_j\}$ where a_j is the only element of order 2 in H_j, so that the (two) automorphisms of H_j maps a_j onto itself, i.e. K_j is a characteristic subgroup of H_j, and since H_j is a normal subgroup of its normalizer $N_G(H_j)$, one deduces that K_j is a normal subgroup of $N_G(H_j)$, and $N_G(H_j)$ is a subgroup of G of order 12 (since the orbit of H_j under conjugation by G has size 5). Since $N_G(H_j)/K_j$ has order 6, it is either isomorphic to $\mathbb{Z}_6$ or to S_3; if π is the projection of $N_G(H_j)$ onto $N_G(H_j)/K_j$ and L is a subgroup of order 2 of $N_G(H_j)/K_j$, then $\pi^{-1}(L)$ is a subgroup of order 4 of $N_G(H_j)$, i.e. a Sylow 2-subgroup of $N_G(H_j)$, and H_j is the only one since it is a normal subgroup of $N_G(H_j)$, and because $L = \pi\big(\pi^{-1}(L)\big)$, there is only one subgroup of order 2 of $N_G(H_j)/K_j$, which is then $\simeq \mathbb{Z}_6$ (since S_3 has three subgroups of order 2). There is then an element $b \in N_G(H_j)$ such that $\pi(b)$ has order 6 in $N_G(H_j)/K_j$, and this means that $b, b^2, b^3 \notin K_j$ but $b^6 \in K_j$, hence b must have order 6 or 12 in G, and there is no such element, hence $H_j \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$, so that it has three elements of order 2, hence G has fifteen elements of order 2.

Remark 14.8: If H is a Sylow 2-subgroup, its normalizer $N_G(H)$ is isomorphic to a semi-direct product $(\mathbb{Z}_2 \times \mathbb{Z}_2) \times_\psi \mathbb{Z}_3$: one knows that H is isomorphic to $\mathbb{Z}_2 \times \mathbb{Z}_2$ and that its normalizer $N_G(H)$ has order 12, and contains eight elements of order 3 besides e and the three elements of order 2 in H (since H is the only Sylow 2-subgroup of $N_G(H)$), so that $N_G(H)$ has four Sylow-3 subgroups, hence it is not Abelian, and it is then a semi-direct product $H \times_\psi K$ where K is a Sylow-3 subgroup.

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

15- Monday October 3, 2011.

Definition 15.1: For a group G, the *center* $Z(G)$ is the set of elements which commute with all elements of G, so that $Z(G) = G$ if and only if G is Abelian.

Lemma 15.2: $Z(G)\, char\, G$, and $N \leq Z(G)$ implies $N \triangleleft G$.[1]

In the G-action on G by conjugation, $Z(G)$ is the kernel of the homomorphism from G into S_G, and it is the set of fixed points.[2]

Proof: If $z \in Z(G)$ and $g \in G$, one has $z\,g = g\,z$, and if ψ is any automorphism of G one deduces that $\psi(z)\,\psi(g) = \psi(z\,g) = \psi(g\,z) = \psi(g)\,\psi(z)$, so that $\psi(z)$ commutes with all elements in $\psi(G)$, which is G, and this proves that $\psi(z) \in Z(G)$. Then, $\psi\big(Z(G)\big) \subset Z(G)$ for all $\psi \in Aut(G)$ implies $\psi\big(Z(G)\big) = Z(G)$ for all $\psi \in Aut(G)$,[3] i.e. $Z(G)$ is characteristic in G.

For $g \in G$, the conjugation ψ_g is the identity on $Z(G)$ (since $\psi_g(x) = g\,x\,g^{-1} = x\,g\,g^{-1} = x$ for all $x \in Z(G)$), so that it is the identity on N, hence $\psi_g(N) = N$, and since it holds for all $g \in G$ it means $N \triangleleft G$.

An element $g \in G$ belongs to the kernel of the homomorphism from G into S_G if $h \mapsto h^g = g\,h\,g^{-1}$ is the identity mapping, i.e. $g\,h\,g^{-1} = h$ for all $h \in G$, which is $g\,h = h\,g$ for all $h \in G$, i.e. $g \in Z(G)$. If an element $a \in G$ is a fixed point of the action by conjugation, it means that $g\,a\,g^{-1} = a$ for all $g \in G$, i.e. $g\,a = a\,g$ for all $g \in G$, so that $a \in Z(G)$.

Lemma 15.3: If $G/Z(G)$ is cyclic, then G is Abelian, so that $Z(G) = G$.
Proof: $Z(G)$ is a normal subgroup of G by Lemma 15.2, and if the quotient is generated by $a\,Z(G)$, then $G = \{a^n z \mid n \in \mathbb{Z}, z \in Z(G)\}$, and since $(a^n z)\,(a^m z') = a^{n+m} z\,z' = (a^m z')\,(a^n z)$, G is Abelian.

Definition 15.4: For a prime p, a *p-group* is a group (not necessarily finite) in which the order of every element is finite and is a power of p (so that the trivial group $\{e\}$ is a p-group, and a non-trivial finite p-group has order p^k for some $k \geq 1$ by Cauchy's theorem).

Lemma 15.5: If G is a non-trivial finite p-group, then p divides $|Z(G)|$, so that the center $Z(G)$ is not reduced to $\{e\}$.
Proof: In the action of G by conjugation, the size of any orbit divides the order of G, so that it is a power of p. Because the size of an orbit is 1 only for the elements of $Z(G)$ by Lemma 15.2, and all other orbits have for size a multiple of p, the order of $Z(G)$ must be a multiple of p.

Remark 15.6: This shows the result mentioned before, that no simple group G has order p^k with p prime and $k \geq 2$, since either $Z(G) \neq G$ and it is a non-trivial and proper normal subgroup, or $Z(G) = G$ in which case G is Abelian, and has a normal subgroup of order p by Cauchy's theorem.

Lemma 15.7: If p is a prime, and G is a group of order p^2, then G is Abelian, and it is isomorphic to either $\mathbb{Z}_p \times \mathbb{Z}_p$ or $\mathbb{Z}_{p^2}$.
Proof: By Lemma 15.5, the order of $Z(G)$ is a multiple of p, so that $G/Z(G)$ has order 1 or p, hence it is either the trivial group or it is isomorphic to $\mathbb{Z}_p$, i.e. it is a cyclic group, so that G is Abelian by Lemma 15.3. By Cauchy's theorem, there is an element $a \in G$ of order p, generating a subgroup H of order p; let $b \notin H$, generating a subgroup K: if K contains H it must coincide with G,[4] in which case G is cyclic and isomorphic to $\mathbb{Z}_{p^2}$, or K has size p with $H \cap K = \{e\}$, and $G = \{a^m b^n \mid m, n \in \{0, \ldots, p-1\}\}$ which is isomorphic to $\mathbb{Z}_p \times \mathbb{Z}_p$.

---

[1] Notice that Lemma 7.11, which says that $A\, char\, B \triangleleft C$ implies $A \triangleleft C$ does not apply here.

[2] An action of a group G on a set X is an homomorphism ψ from G into S_X (the group of bijections of X onto itself, with composition), so that the kernel of ψ is a (normal) subgroup of G, while the set of fixed points is a subset of X, namely those $x \in X$ for which that stabilizer $Stab_x$ is G (so that orbit of x is reduced to $\{x\}$). Here $X = G$.

[3] Since ψ is invertible, applying ψ^{-1} to $\psi\big(Z(G)\big) \subset Z(G)$ gives $Z(G) \subset \psi^{-1}\big(Z(G)\big) \subset Z(G)$.

[4] By Lagrange's theorem, the order of a subgroup of G can only be 1, p, or p^2.

Remark 15.8: A group G of order p^3 is not necessarily Abelian, since there are two distinct non-Abelian groups of order 8, the dihedral group D_4 and the quaternion group Q_8.

Remark 15.9: It was mentioned that the only simple Abelian groups are the $\mathbb{Z}_p$ for p prime as a consequence of the structure theorem of finite Abelian groups which will be proven in another lecture, and it says that a non-trivial finite Abelian group G is isomorphic to some product $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k}$ for some $k \geq 1$ with n_i dividing n_{i+1} for $i = 1, \ldots, k-1$: then, a product $G = K \times L$ of two non-trivial Abelian groups K, L has $K \times \{e\}$ and $\{e\} \times L$ as normal subgroups, which are different from $\{e\}$ or G, so that it is not simple.

Actually, the structure theorem of finite Abelian groups is a particular case of the structure theorem of finitely generated Abelian groups, which are of the form $\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_k} \times \mathbb{Z}^r$ for an integer $r \geq 0$.

Definition 15.10: In a group G, the *commutator* of g and h is $[g,h] = g\,h\,g^{-1}h^{-1} = g\,(g^{-1})^h = h^g h^{-1}$. The subgroup generated by the set of commutators of G is denoted $[G,G]$. The *derived subgroups* of G are $G^{(0)} = [G,G]$, and then $G^{(n+1)} = [G^{(n)}, G^{(n)}]$ for $n \geq 0$.

Lemma 15.11: One has $[g,h] = e$ if and only if g and h commute. For every $g, h, a \in G$, one has $[g,h]^a = [g^a, h^a]$.
Proof: $[g,h] = e$ means $g\,h\,g^{-1}h^{-1} = e$, so that $g\,h\,g^{-1} = h$ and $g\,h = h\,g$. Actually, $x \mapsto x^a = a\,x\,a^{-1}$ is an automorphism of G, and for any homomorphism ψ from G into G (endomorphism), one has $\psi([g,h]) = [\psi(g), \psi(h)]$: indeed, $\psi(x\,y) = \psi(x)\,\psi(y)$ for all $x, y \in G$, and $\psi(x^{-1}) = \big(\psi(x)\big)^{-1}$ for all $x \in G$, so that $\psi(g\,h\,g^{-1}h^{-1}) = \psi(g)\,\psi(h)\,\psi(g^{-1})\,\psi(h^{-1}) = \psi(g)\,\psi(h)\,\big(\psi(g)\big)^{-1}\,\big(\psi(h)\big)^{-1} = [\psi(g), \psi(h)]$.

Lemma 15.12: If $N \lhd G$, then $[g\,N, h\,N] = [g,h]\,N$, and G/N is Abelian if and only if N contains all commutators, i.e. $[G,G] \leq N$.
Proof: Because N is a normal subgroup, $n_1 g = g\,n_2$ so that one can move an element of N to the right almost as if it was in the center of G, but in doing so the element of N changes name: $(g\,n_1)\,(h\,n_2)\,(g\,n_3)^{-1}(h\,n_4)^{-1} = g\,n_1 h\,n_2 n_3^{-1} g^{-1} n_4^{-1} h^{-1} = g\,h\,(n_5 n_2 n_3^{-1}) g^{-1} n_4^{-1} h^{-1} = g\,h\,g^{-1}(n_6 n_4^{-1}) h^{-1} = g\,h\,g^{-1}h^{-1} n_7 \in [g,h]\,N$; then, n_7 can be any element in N, by taking $n_1 = n_2 = n_3 = e$ and defining n_4 by $h\,n_4 = n_7^{-1} h$.

G/N is Abelian if and only if $[g\,N, h\,N] = e\,N = N$ for all $g, h \in G$, i.e. if and only $[g,h]\,N = N$ for all $g, h \in G$, or $[g,h] \in N$ for all $g, h \in G$.

Lemma 15.13: $[G,G]\,char\,G$, so that $G^{(n)}\,char\,G^{(m)}$ if $0 \leq m \leq n$, hence $G^{(n)}\,char\,G$, which implies $G^{(n)} \lhd G$.
Proof: An element $a \in [G,G]$ has the form $a = [g_1, h_1]^{n_1} \cdots [g_k, h_k]^{n_k}$ for some $g_1, \ldots, g_k, h_1, \ldots, h_k \in G$, $n_1, \ldots, n_k \in \mathbb{Z}$, and $k \geq 1$, and for $\psi \in Aut(G)$ one has $\psi(a) = [\psi(g_1), \psi(h_1)]^{n_1} \cdots [\psi(g_k), \psi(h_k)]^{n_k} \in [G,G]$, so that $\psi([G,G]) \subset [G,G]$ for all $\psi \in Aut(G)$, hence $\psi([G,G]) = [G,G]$ for all $\psi \in Aut(G)$.

Remark 15.14: If G is a non-Abelian simple group, then $[G,G] = G$, since $[G,G]$ is a normal subgroup of G, so that it must be either $\{e\}$ or G, but $[G,G] = \{e\}$ means that G is Abelian.

Since A_5 is non-Abelian and simple, one has $[A_5, A_5] = A_5$, and then $[A_5, A_5] \subset [S_5, S_5] \subset A_5$ since $A_5 \lhd S_5$ with S_5/A_5 Abelian (isomorphic to $\mathbb{Z}_2$), so that $[S_5, S_5] = A_5$.

One has $\{e\} \lhd N \lhd A_4 \lhd S_4$, with $N = \{e, (1\,2)\,(3\,4), (1\,3)\,2\,3\,4), (1\,4)\,(2\,3)\}$, and N is Abelian ($\simeq \mathbb{Z}_2 \times \mathbb{Z}_2$) so that $[N,N] = \{e\}$; A_4/N is Abelian, isomorphic to $\mathbb{Z}_3$, so that $[A_4, A_4] \leq N$, and S_4/A_4 is Abelian, isomorphic to $\mathbb{Z}_2$, so that $[S_4, S_4] \leq A_4$, and let us show that $[A_4, A_4] = N$ and $[S_4, S_4] = A_4$. One has $[A_4, A_4] \neq \{e\}$ since A_4 is not Abelian, but because it is a characteristic subgroup of A_4 it cannot contain one element of order 2 without containing the two others since the three elements of order 2 are conjugate, hence $[A_4, A_4] = N$. One has $N = [A_4, A_4] \leq [S_4, S_4] \leq A_4$, and by Lagrange's theorem a subgroup H satisfying $N < H \leq A_4$ must coincide with A_4, so one must only show that $N \neq [S_4, S_4]$: indeed, $N = [S_4, S_4]$ would imply that S_4/N is Abelian, while it is isomorphic to S_3, because it cannot be isomorphic to $\mathbb{Z}_6$, since there would exist $a \in S_4$ with $a, \ldots, a^6$ belonging to six different N-cosets, contradicting the fact that in S_4 the order of an element is 1, 2, 3, or 4.

Remark 15.15: A group G is called *solvable* if there exists a *subnormal series* $G_0 = \{e\} \lhd G_1 \lhd \cdots \lhd G_k = G$ with G_i/G_{i-1} Abelian for $i = 1, \ldots, k$, and it can be shown that G is solvable if and only a derived subgroup $G^{(n)}$ is $\{e\}$ (so that S_4 is solvable but not S_5), and then $G^{(n)} \lhd \cdots \lhd G^{(0)} = [G,G] \lhd G$ provides a *normal series*, i.e. one which besides $G_{i-1} \lhd G_i$ and G_i/G_{i-1} Abelian for $i = 1, \ldots, k$, also satisfies $G_{i-1} \lhd G$ for $i = 2, \ldots, k-1$.

16- Wednesday October 5, 2011.

Remark 16.1: The reason for the definition of solvability of a group comes from Galois theory, and is related to the question of which polynomial equations can be solved by radicals. RUFFINI had found a way to prove that there exist polynomials of degree 5 with integer coefficients whose roots cannot be expressed by radicals, but his "proof" contained a gap, which ABEL filled. GALOIS went further and explained how (in principle) one can discover if a given polynomial $P \in \mathbb{Z}[x]$ (i.e. with integer coefficients) and of any degree ≥ 5 has its roots expressed by radicals or not: there is a natural field extension K of $\mathbb{Q}$ to consider, the smallest field ($\subset \mathbb{C}$) containing $\mathbb{Q}$ and the roots of P (called a *splitting field extension* of P over $\mathbb{Q}$), and one then considers the group G of automorphisms of K fixing $\mathbb{Q}$ (the *Galois group* $Aut_{\mathbb{Q}}(K)$), and there is a correspondence between the subgroups of G and the intermediate fields between $\mathbb{Q}$ and K; then, the fact that one can go from $\mathbb{Q}$ to K by successively adding m-th roots taken in the successive extensions expresses exactly the property that G is solvable.

For a polynomial $P \in \mathbb{Z}[x]$ of degree 5 which has three real roots and two (conjugate) non-real roots, one then shows that the Galois group is isomorphic to S_5, which is not solvable, hence has its roots which cannot be expressed by radicals.

Remark 16.2: For proving the characterization mentioned before (that a group G is solvable if and only if a derived group $G^{(n)}$ must be $\{e\}$) there are a few natural observations: one starts from a subnormal series $(G_i, i = 0, \ldots, k)$ which witnesses that G is solvable, and one proves that if $H \leq G$ the sequence $(H_i = G_i \cap H, i = 0, \ldots, k)$ is a subnormal series in H, which then witnesses that H is solvable; if N is a normal subgroup of G (with π the projection of G onto G/N), one proves that the sequence $(G_i^* = \pi\, G_i \simeq G_i N/N, i = 0, \ldots, k)$ is a subnormal series in G/N, which then witnesses that G/N is solvable. Then, if G is a group which contains a normal subgroup N which is solvable (witnessed by a subnormal series $(N_i, i = 0, \ldots, k)$) with G/N solvable (witnessed by a subnormal series $(Q_j, j = 0, \ldots, \ell)$), one proves that G is solvable by considering $M_j = \pi^{-1} Q_j$ (with π the projection of G onto G/N) and noticing that $M_j \triangleleft M_{j+1}$ and that M_{j+1}/M_j is isomorphic to Q_{j+1}/Q_j, and then $N_0 \leq \ldots \leq N_k = N = M_0 \leq M_1 \leq \ldots \leq M_\ell = G$ witnesses that G is solvable.

Remark 16.3: The Brauer–Fowler theorem,[1,2] proved in 1955, states that if a group G has even order > 2 then it has a proper subgroup H with $|H| > |G|^{1/3}$: BRAUER and FOWLER showed that if G has exactly m elements of order 2, and $n = \frac{|G|}{m}$, then G contains a proper subgroup H whose index (> 1) is either 2 or $< \frac{n\,(n+2)}{2}$, so that if v is the maximal order of a proper subgroup, then either $v = \frac{|G|}{2}$ or $2|G| < v^2(v+1)$. They also showed that G contains a proper (but possibly trivial) normal subgroup N with G/N isomorphic to a subgroup of S_u with either $u = 2$ or $u < \frac{n\,(n+2)}{2}$, so that either $[G\!:\!N] = 2$ or $[G\!:\!N] < \big(\frac{n\,(n+2)}{2}\big)!$; they deduced that if moreover G is simple, then $|G| < \big(\frac{n\,(n+1)}{2}\big)!$.

BRAUER and FOWLER also observed that there exist only a finite number of simple groups in which the centralizer $C_G(a)$ of an element a of order 2 (called an *involution*) is isomorphic to a given group, and this suggested that finite simple groups could be classified by studying the centralizers of their involutions, a program that was later realized in the classification of finite simple groups. Since their result only apply to groups of even order, they mentioned a conjecture that all groups of odd order are solvable.

Remark 16.4: It was BURNSIDE who had conjectured in 1911 that every non-Abelian finite simple group has even order,[3] and one of his best known contributions to group theory is his $p^a q^b$ theorem, that every

[1] Richard Dagobert BRAUER, German-born mathematician, 1901–1977. He worked in Toronto (Ontario), at University of Michigan, Ann Arbor, MI, and at Harvard University, Cambridge, MA. The Brauer–Fowler theorem is partly named after him.

[2] Kenneth Arthur FOWLER, American mathematician. He worked at San José State University, San José, CA. The Brauer–Fowler theorem is partly named after him.

[3] William BURNSIDE, English mathematician, 1852–1927. He worked at the Royal Naval College in Greenwich, England.

finite group whose order is divisible by fewer than three distinct primes is solvable.

A *CA group* is a group such that the centralizer of every non-trivial element is Abelian, and in 1957, SUZUKI showed that all CA groups of odd order are solvable,[4] and he later classified all the simple CA groups, and more generally all simple groups such that the centralizer of any involution has a normal 2-Sylow subgroup.[5]

A *CN group* is a group such that the centralizer of every non-trivial element is *nilpotent*, and in 1960 FEIT,[6] HALL,[7] and THOMPSON showed that every CN group of odd order is solvable.[8] Their proof, similar to SUZUKI's proof, was about 17 pages long, which at the time was thought to be very long for a proof in group theory.

In 1963, FEIT and THOMPSON proved what can be thought of as the next step in this process, the Feit–Thompson theorem: they showed that there is no (non-cyclic) simple group of odd order such that every proper subgroup is solvable, and this proves that every finite group of odd order is solvable, as a minimal counter-example must be a simple group such that every proper subgroup is solvable. Although the proof follows the same general outline as the CA theorem and the CN theorem, the details are much more complicated, and the article is 255 pages long!

Remark 16.5: A group G is called *nilpotent* if there exists a finite normal series (so that $G_i \triangleleft G$, implying $G_i \triangleleft G_{i+1}$) such that $G_{i+1}/G_i \leq Z(G/G_i)$ for $i = 0, \ldots, k-1$, and since the center of a group is Abelian, G_{i+1}/G_i is then Abelian, so that every nilpotent group is solvable.

Since an element a in a ring R is called *nilpotent* if $a^n = 0$ for some $n \geq 1$, one may wonder if using the same term is consistent: for $g \in G$, one has a mapping ad_g from G into G defined by $ad_g(x) = [g, x]$, and the definition implies that, for every $g \in G$, ad_g maps G_{i+1} into G_i for $i = 0, \ldots, k-1$,[9] so that $ad_{g_k} \circ \cdots \circ ad_{g_1}$ maps G onto $\{e\}$ for all $g_1, \ldots, g_k \in G$; however, there is no obvious ring structure in this context.

For a group G, the *ascending central series* is defined by $Z_0(G) = \{e\}$, $Z_{n+1}(G)/Z_n(G) = Z\big(G/Z_n(G)\big)$, and it satisfies $[G, Z_{n+1}(G)] \leq Z_n(G)$ for all $n \geq 0$, and the *descending central series* is defined by $L_1(G) = G$, $L_{n+1}(G) = [G, L_n(G)]$, and it satisfies $L_n(G)\, char\, G$ for all $n \geq 1$, so that $L_n(G) \triangleleft G$ for all $n \geq 1$, and $L_n/L_{n+1} \leq Z(G/L_{n+1})$. One then shows that a group G is nilpotent if and only if its ascending central series reaches G, or if and only if its descending central series reaches $\{e\}$.

Remark 16.6: If p is prime, any finite p-group G is nilpotent. If G is a nilpotent group, then $H < G$ implies $H < N_G(H)$. If G is a finite nilpotent group, and a prime p divides $|G|$, then it has a unique Sylow-p subgroup (which is then a normal subgroup of G). If G is a finite nilpotent group, then it is isomorphic to

---

[4] Michio SUZUKI, Japanese-born mathematician, 1926–1998. He worked at University of Illinois at Urbana-Champaign, IL.

[5] He also found in 1960 an overlooked family of simple groups of Lie type in the process, that are now called *Suzuki groups*, an infinite family of the only non-Abelian simple groups whose order is not divisible by 3: the smallest, of order 29,120, was the first simple group of order less than 1 million to be discovered since Dickson's list of 1900.

[6] Walter FEIT, Austrian-born mathematician, 1930–2004. He worked at Cornell University, Itaca, NY, and at Yale University, New Haven, CT. The Feit–Thompson theorem is partly named after him.

[7] Marshall HALL, American mathematician, 1910–1990. He worked OSU (Ohio State University) Columbus, OH, at Caltech (California Institute of Technology) Pasadena, CA, and at Emory University, Oxford, GA.

[8] John Griggs THOMPSON, American-born mathematician, born in 1932. He received the Fields Medal in 1970. He received the Wolf Prize in 1992, for his profound contributions to all aspects of finite group theory and connections with other branches of mathematics, jointly with Lennart CARLESON. He worked at the University of Chicago, Chicago, IL, University of Cambridge, Cambridge, England, holding the Rouse Ball professorship, and at University of Florida, Gainesville, FL. He received the Abel Prize in 2008 jointly with Jacques TITS, for their profound achievements in algebra and in particular for shaping modern group theory. The Feit–Thompson theorem is partly named after him.

[9] Because $G_{i+1}/G_i \leq Z(G/G_i)$ for $i = 0, \ldots, k-1$ is equivalent to $[G_{i+1}, G] \leq G_i$ for $i = 0, \ldots, k-1$, and of course if $H, K \leq G$ one writes $[H, K]$ for the subgroup generated by all the commutators $[h, k]$ with $h \in H, k \in K$. An important observation is that if $H \leq G$, $K \triangleleft G$ (which implies $H\,K = K\,H \leq G$), and if one has $[G, H] \leq K$, then $H\,K/K \leq Z(G/K)$.

the product of its Sylow subgroups. A direct product of a finite number of nilpotent groups is nilpotent. If G is a finite group, then G is nilpotent if and only if it is isomorphic to a product of finite p groups.

Remark 16.7: D_n is solvable for all $n \geq 3$, but it is nilpotent if only if n is a power of 2: one has $a^\alpha b = b\, a^{-\alpha}$ for all $\alpha \in \mathbb{Z}$, and one deduces that $[a^\alpha, a^\beta b] = a^{2\alpha}$ and $[a^\alpha b, a^\beta b] = a^{2\alpha - 2\beta}$ for all $\alpha, \beta \in \mathbb{Z}$. This shows that $L_1(D_n) = [D_n, D_n] = \{a^{2\gamma} \mid \gamma \in \mathbb{Z}\}$, which is Abelian, so that D_n is solvable. By induction $L_j(D_n) = \{a^{2^j \gamma} \mid \gamma \in \mathbb{Z}\}$ for $j \geq 1$, so that D_n is nilpotent if and only if n is a power of 2.

One can construct an infinite p-group G_1 which is nilpotent, and an infinite p-group G_2 which is not nilpotent.

Additional footnotes: Ball R.,[10] Bonaparte,[11] Lennart Carleson,[12] Dickson,[13] Emory,[14] Fourier,[15] Misha Gromov,[16] Jacques Tits.[17]

[10] Walter William Rouse Ball, English mathematician, 1850–1925. He worked in Cambridge, England. The Rouse Ball professorship at Cambridge, England, is named after him.

[11] Napoléon Bonaparte (Napoleone Buonaparte), French general, 1769–1821. He became Premier Consul after his coup d'état in 1799, was elected Consul à vie in 1802, and he proclaimed himself emperor in 1804, under the name Napoléon I (1804–1814, and 100 days in 1815).

[12] Lennart Axel Edvard Carleson, Swedish mathematician, born in 1928. He received the Wolf Prize in 1992, for his fundamental contributions to Fourier analysis, complex analysis, quasi-conformal mappings and dynamical systems, jointly with John G. Thompson, for his profound contributions to all aspects of finite group theory and connections with other branches of mathematics. He received the Abel Prize in 2006 for his profound and seminal contributions to harmonic analysis and the theory of smooth dynamical systems. He worked at Uppsala, Sweden, at UCLA (University of California at Los Angeles), Los Angeles, CA, and at the Royal Institute of Technology, Stockholm, Sweden.

[13] Leonard Eugene Dickson, American mathematician, 1874–1954. He worked at the University of Chicago, Chicago, IL.

[14] John Emory, American clergyman, 1789–1835. He was elected bishop of the Methodist Episcopal Church in 1832. Emory University, Oxford, GA, is named after him.

[15] Jean-Baptiste Joseph Fourier, French mathematician, 1768–1830. He worked in Auxerre, in Paris, France, accompanied Bonaparte in Egypt, was prefect in Grenoble, France, until the fall of Napoléon I, and worked in Paris again. The first of three universities in Grenoble, France, Université de Grenoble I, is named after him, and the Institut Fourier is its department of mathematics. Fourier series and Fourier integrals are named after him.

[16] Mikhail Leonidovich Gromov, Russian-born mathematician, born in 1943. He received the Wolf Prize in 1993, for his revolutionary contributions to global Riemannian and symplectic geometry, algebraic topology, geometric group theory and the theory of partial differential equations, jointly with Jacques Tits, for his pioneering and fundamental contributions to the theory of the structure of algebraic and other classes of groups and in particular for the theory of buildings. He works at IHES (Institut des Hautes Études Scientifiques) at Bures sur Yvette, France, and at NYU (New York University), New York, NY.

[17] Jacques Tits, Belgian-born mathematicia, born in 1930. He received the Wolf Prize in 1993, for his pioneering and fundamental contributions to the theory of the structure of algebraic and other classes of groups and in particular for the theory of buildings, jointly with Mikhael Gromov. He received the Abel Prize in 2008 jointly with John G. Thompson, for their profound achievements in algebra and in particular for shaping modern group theory. He worked at the Free University of Brussels, Bruxelles (Brussels), Belgium, in Bonn, Germany, and at Collège de France, Paris, France.

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

17- Friday October 7, 2011.

Definition 17.1: If X is a set, a *word* on X is a finite sequence (possibly empty) from $X \times \mathbb{Z}$, and one writes $x_1^{n_1} \cdots x_k^{n_k}$ for the word whose entry $\#i$ is (x_i, n_i).

A word is *reduced* if neither of the two following *reduction rules* applies: $a\, x^m x^n\, b$ is replaced by $a\, x^{m+n} b$, and $a\, x^0 b$ is replaced by $a\, b$, for any two words a, b (possibly empty).

Lemma 17.2: Any word can be reduced by finitely many applications of the reduction rules, and the reduced word does not depend upon the order of the operations of reduction.
Proof: Each application of the reduction rules makes the length of the word decrease, so that only a finite number of reductions can be done; the empty word is reduced.

Various applications of the first reduction rule are independent, i.e. they can be done in any order. An application of the second reduction rule may have the effect that more successive powers of the same x appear, but applying the first reduction rule to these powers of x before or after applying the second reduction rule makes no difference, so that whatever the order of the operations of reduction, the result is always the same.

Lemma 17.3: The set R of reduced word is a group for the operation where $a\, b$ is the reduced form of the *concatenation* $a \star b$ (made of a on the left and b on the right). It is called the *free group* on X,[1] and denoted $Fr(X)$.
Proof: Associativity applies to concatenation, i.e. $(a \star b) \star c = a \star (b \star c)$, and the reduced form is either the reduced form of $(a\, b) \star c$, which is $(a\, b)\, c$, or the reduced form of $a \star (b\, c)$, which is $a\, (b\, c)$, and these reduced forms are equal by Lemma 17.2, so that the operation is associative. The identity is the empty word, and the inverse of $x_1^{n_1} \cdots x_\ell^{n_\ell}$ is $x_\ell^{-n_\ell} \cdots x_1^{-n_1}$.

Lemma 17.4: (universal property) Identifying $x \in X$ with $i(x) = x^1 \in Fr(X)$, one has $\langle X \rangle = Fr(X)$, and for any group G and any mapping f from X into G, there is a unique homomorphism $\psi(f)$ from $Fr(X)$ into G which extends f. Moreover, these properties characterize $Fr(X)$ up to an isomorphism.
Proof: An element of $Fr(X)$ is either the empty word, or has the form $x_1^{n_1} \cdots x_\ell^{n_\ell}$ with $n_1, \ldots, n_\ell \in \mathbb{Z} \setminus \{0\}$, and $x_j \neq x_k$ whenever $|j - k| = 1$, and such an element belongs to $\langle X \rangle$, which then coincides with $Fr(X)$. If F is an homomorphism from $Fr(X)$ into G extending f, i.e. such that $F(x) = f(x)$ for every $x \in X$, then one must have $F(x_1^{n_1} \cdots x_\ell^{n_\ell}) = F(x_1^{n_1}) \cdots F(x_\ell^{n_\ell}) = \big(F(x_1)\big)^{n_1} \cdots \big(F(x_\ell)\big)^{n_\ell} = \big(f(x_1)\big)^{n_1} \cdots \big(f(x_\ell)\big)^{n_\ell}$, so that F can only be given by the preceding formula, and one must check that this formula defines an homomorphism, which is the desired $\psi(f)$. For proving it, one notices that the same formula applies to all words even if they are not reduced, so that one automatically has $F(a \star b) = F(a)\, F(b)$ for all words, and then that the reduction rules do not affect the value of F, i.e. $F(a\, x^m x^n b) = F(a) \big(F(x)\big)^m \big(F(x)\big)^n F(b)$, which is $F(a) \big(F(x)\big)^{m+n} F(b)$, i.e. $F(a\, x^{m+n} b)$, and, similarly, that $F(a\, x^0 b) = F(a)\, e\, F(b)$, which is $F(a)\, F(b)$, i.e. $F(a\, b)$.

Denoting i the injection of X into $Fr(X)$, one has $\psi(f) \circ i = f$ for all f; one then assumes that there is another solution $\widetilde{X}$ of the universal problem, with $\widetilde{i}$ the injection of X into $\widetilde{X}$ and $\widetilde{\psi}(f)$ the corresponding extension of f, so that one has $\widetilde{\psi}(f) \circ \widetilde{i} = f$ for all f. Then $\psi(\widetilde{i})$ is an homomorphism from $Fr(X)$ into $\widetilde{X}$, and $\widetilde{\psi}(i)$ is an homomorphism from $\widetilde{X}$ into $Fr(X)$, and they satisfy $\psi(\widetilde{i}) \circ i = \widetilde{i}$ and $\widetilde{\psi}(i) \circ \widetilde{i} = i$ on X; one deduces that $\psi(\widetilde{i}) \circ \widetilde{\psi}(i) \circ \widetilde{i} = \widetilde{i}$ on X, so that the two homomorphisms $\psi(\widetilde{i}) \circ \widetilde{\psi}(i)$ and id (the identity mapping) coincide on $\widetilde{i}(X)$, and then on the subgroup it generates, i.e. $\widetilde{X}$; similarly $\widetilde{\psi}(i) \circ \psi(\widetilde{i})$ is id on $Fr(X)$, so that $\psi(\widetilde{i})$ is an isomorphism from $Fr(X)$ onto $\widetilde{X}$, with inverse $\widetilde{\psi}(i)$.

Lemma 17.5: A mapping f from X_1 into X_2 induces an homomorphism $\psi(f)$ from $Fr(X_1)$ into $Fr(X_2)$, such that $\psi(f) \circ i_1 = i_2 \circ f$, where i_k is the injection of X_k into $Fr(X_k)$. If g is a mapping from X_2 into X_3 and $h = g \circ f$, then $\psi(h) = \psi(g) \circ \psi(f)$, so that a bijection f from X_1 onto X_2 induces an isomorphism

[1] It is free of any relations, like those considered in Lemma 17.8.

$\psi(f)$ from $Fr(X_1)$ onto $Fr(X_2)$. If $|X| = n$, one speaks of $Fr(X)$ as *the free group on n elements*, so that if a group G has a generating set $\{g_1, \ldots, g_n\}$, it is an homomorphic image of the free group on n elements.
Proof: An homomorphism ψ from a group G_1 into a group G_2 is uniquely determined by its values on a generating set Z_1 of G_1; here $G_k = Fr(X_k)$ and $Z_k = i_k(X_k)$. Because $\psi(h)$ and $\psi(g) \circ \psi(f)$ coincide on $i_1(X_1)$, which generates $Fr(X_1)$, they are equal. If $g = f^{-1}$, $h = id$ and $\psi(id) = id$ (where id denotes the identity mapping on various sets). On then uses $X_1 = \{1, \ldots, n\}$, $X_2 = \{g_1, \ldots, g_n\}$ with $f(i) = g_i$, $i = 1, \ldots, n$.

Lemma 17.6: If for a group G a subset $Y \subset G$ is stable by conjugation (i.e. for all $g \in G$, $y \in Y$ implies $y^g \in Y$), then $\langle Y \rangle \lhd G$. For $X \subset G$, the smallest $N \lhd G$ containing X is $\langle Y_X \rangle$ for $Y_X = \bigcup_{g \in G} X^g$.
Proof: To prove that $\langle Y \rangle$ is a normal subgroup of G, one must show that $a \in \langle Y \rangle$ and $g \in G$ imply $a^g \in \langle Y \rangle$. Indeed, since $a = y_1^{n_1} \cdots y_k^{n_k}$ for some $y_1, \ldots, y_k \in Y$, $n_1, \ldots, n_k \in \mathbb{Z}$, and $k \geq 1$, one has $a^g = (y_1^g)^{n_1} \cdots (y_k^g)^{n_k}$, and because Y is stable by conjugation one has $y_1^g, \ldots, y_k^g \in Y$, so that $a^g \in \langle Y \rangle$.

If N is normal and contains X, then N contains X^g for all $g \in G$, i.e. N contains Y_X, so that N must contain $\langle Y_X \rangle$; on the other hand Y_X is stable by conjugation (because $(X^g)^h = X^{g\,h}$), so that $\langle Y_X \rangle$ is normal subgroup of G, and it then is the smallest normal subgroup of G containing X.

Lemma 17.7: For $E \subset Fr(X)$, let N be the smallest normal subgroup of $Fr(X)$ containing E (as in Lemma 17.6), then the quotient group $Fr(X)/N$ has a universal property: if G is a group and f is a mapping from X into G such that, whenever $x_1^{n_1} \cdots x_k^{n_k} \in E$ one has $\big(f(x_1)\big)^{n_1} \cdots \big(f(x_k)\big)^{n_k} = e$, then there is an homomorphism $\chi(f)$ from $Fr(X)/N$ into G such that $\chi(f) \circ \pi = \psi(f)$, or $\chi(f) \circ \pi \circ i = f$, where π is the projection from $Fr(X)$ onto $Fr(X)/N$.
Proof: The kernel of the homomorphism $F = \chi(f)$ contains all the words $x_1^{n_1} \cdots x_k^{n_k}$ which belong to E, and since it is a normal subgroup of $Fr(X)$, it must contain N. Then F induces a map $\overline{F}$ from $Fr(X)/N$ into G by $\overline{F}(a\,N) = F(a)$, and $\overline{F}$ is the desired $\chi(f)$.

Lemma 17.8: If $G = \langle g_1, \ldots, g_n \rangle$ (with not necessarily distinct g_i), and equations $E_1, \ldots, E_m$ hold in G, where each equation is of the form $\gamma_1^{n_1} \cdots \gamma_k^{n_k} = e$, where $\gamma_i \in \{g_1, \ldots, g_n\}$, $n_i \in \mathbb{Z}$ for $i = 1, \ldots, k$ (and $k \geq 1$); let $X = \{x_1, \ldots, x_n\}$ and $E^* \subset Fr(X)$ be the corresponding set of $y_1^{n_1} \cdots y_k^{n_k}$, where $y_i = x_j$ if $\gamma_i = g_j$, and let N be the smallest normal subgroup of $Fr(X)$ containing E^*, then there is a surjective homomorphism from $Fr(X)/N$ onto G.
Proof: One defines f from X into G by $f(x_i) = g_i$ for $i = 1, \ldots, n$, and Lemma 17.7 applies to E^*, and the desired homomorphism is $F = \chi(f)$, which is surjective because $F(x_i N) = g_i$ for $i = 1, \ldots, n$, and the g_i generate G.

Remark 17.9: *Changing the notation* used before, D_n, the dihedral group of degree $n \geq 3$ (and order $2n$) is generated by a and b, where a is complex conjugation, and b is multiplication by $e^{2i\,\pi/n}$, so that $a^2 = b^n = e$, and $D_n = \{e, b, \ldots, b^{n-1}, a, a\,b \ldots, a\,b^{n-1}\}$, with the relation $b^k a = a\,b^{-k}$ for all $k \in \mathbb{Z}$.

In the complex plane $\mathbb{C}$, the property $c\,a = a\,c^{-1}$ is true if a is complex conjugation and c is multiplication by any complex number ρ of modulus 1, since $\rho^{-1} = \overline{\rho}$, and for any $z \in \mathbb{C}$ one has $c\,a(z) = \rho\,\overline{z} = \overline{\overline{\rho}\,z} = \overline{\rho^{-1}\,z} = a\,c^{-1}(z)$. Since $a^2 = e$, and $c\,a = a\,c^{-1}$ is equivalent to $a\,c\,a\,c = e$, it is useful to deduce the consequences in a purely algebraic way.

Lemma 17.10: If in a group G one has $a^2 = e$ and $a\,b\,a\,b = e$,[2] then $a\,b^k = b^{-k}a$ for all $k \in \mathbb{Z}$ (equivalently $b^\ell a = a\,b^{-\ell}$ for all $\ell \in \mathbb{Z}$), and more generally, $a^{\alpha_1} b^{\beta_1} \cdots a^{\alpha_m} b^{\beta_m} = a^\alpha b^\beta$ with $\alpha = \alpha_1 + \ldots + \alpha_m \pmod 2$, and $\beta = (-1)^{\alpha_2 + \ldots + \alpha_m}\beta_1 + (-1)^{\alpha_3 + \ldots + \alpha_m}\beta_2 + \ldots + (-1)^{\alpha_m}\beta_{m-1} + \beta_m$.
Proof: Multiplying $a\,b\,a\,b = e$ by $b^{-1}a$ on the right, one deduces that $a\,b = b^{-1}a$, which after multiplying by a on the left and on the right gives $a\,b^{-1} = b\,a$. Then, one uses induction for deducing that $a\,b^k = b^{-k}a$ for $k \geq 1$ from $a\,b = b^{-1}a$, and similarly $a\,b^{-k} = b^k a$ for $k \geq 1$ is deduced from $a\,b^{-1} = b\,a$: indeed, $a\,b^k = b^{-k}a$ implies $a\,b^{k+1} = (a\,b^k)\,b = (b^{-k}a)\,b = b^{-k}(b^{-1}a) = b^{-(k+1)}a$. Then, in a general term $a^{\alpha_1} b^{\beta_1} \cdots a^{\alpha_m} b^{\beta_m}$ one can push all the powers of a to the left, and a power b^γ will stay b^γ if the sum of powers of a to the right of it is even, or be changed into $b^{-\gamma}$ if the sum of powers of a to the right of it is odd.

Remark 17.11: One deduces that if $G = \langle a, b \rangle$, with $a^2 = e$ and $a\,b\,a\,b = e$, then $G = \{b^k, k \in \mathbb{Z}\} \bigcup \{a\,b^\ell \mid \ell \in \mathbb{Z}\}$ and for all $k, \ell \in \mathbb{Z}$ one has $b^k\,b^\ell = b^{k+\ell}$, $b^k\,(a\,b^\ell) = a\,b^{-k+\ell}$, $(a\,b^k)\,b^\ell = a\,b^{k+\ell}$, $(a\,b^k)\,(a\,b^\ell) = b^{-k+\ell}$.

[2] With $a \neq b$, it happens if G contains a copy of $\mathbb{Z}_2 \times \mathbb{Z}_2$, or a copy of D_n for some $n \geq 3$.

Lemma 17.12: If $X = \{x_1, x_2\}$, then the smallest normal subgroup N of $Fr(X)$ containing x_1^2 and $x_1x_2x_1x_2$ is made up of the words $x_1^{\alpha_1}x_2^{\beta_1}\cdots x_1^{\alpha_m}x_2^{\beta_m}$ (reduced so that no exponent is 0 except perhaps α_1 if the word starts with a power of x_2, or β_m if the word ends with a power of x_1) such that $\alpha_1 + \ldots + \alpha_m = 0 \pmod 2$ and $(-1)^{\alpha_2+\ldots+\alpha_m}\beta_1 + (-1)^{\alpha_3+\ldots+\alpha_m}\beta_2 + \ldots + (-1)^{\alpha_m}\beta_{m-1} + \beta_m = 0$.
Proof: If N is any normal subgroup of $Fr(X)$, and if $s\,t \in N$ for two words $s, t \in Fr(X)$, and $u \in N$, then $s\,u\,t \in N$, since it is $(s\,u\,s^{-1})\,(s\,t)$ and $s\,u\,s^{-1} \in N$ since $N \triangleleft Fr(X)$. One assumes then that x_1^2 and $x_1x_2x_1x_2$ belong to N, and one has $x_2x_1x_2x_1 = x_1^{-1}(x_1x_2x_1x_2)x_1 \in N$ since $N \triangleleft Fr(X)$. Using $s = t = x_1x_2$ and $u = x_2x_1x_2x_1$ gives $x_1x_2^2x_1x_2x_1^2x_2 \in N$, and inserting x_1^{-2} to cancel x_1^2 gives $x_1x_2^2x_1x_2^2 \in N$, and by induction $x_1x_2^kx_1x_2^k \in N$ for $k \geq 1$; by conjugation with x_1^{-1}, one deduces that $x_2^kx_1x_2^kx_1 \in N$ since $N \triangleleft Fr(X)$, and by inversion one deduces that the same holds with k replaced by $-k$. One can then replace a piece of a word $x_2^\beta x_1$ by $x_1x_2^{-\beta}$, by inserting x_1^2 on the left and $x_1x_2^{-\beta}x_1x_2^{-\beta}$ on the right, giving $x_1^2(x_2^\beta x_1)\,x_1x_2^{-\beta}x_1x_2^{-\beta}$, which is $x_1x_2^{-\beta}$ after insertions of x_1^{-2} and cancellations; this gives a way to start from an element of N and create other elements of N by pushing the x_1 to the left, so that their total number must be even, and no x_2 should be left. Finally, one checks that the family considered is stable by multiplication and inversion, so that it defines a subgroup, and that it is stable by conjugation by x_1 or by x_2 (hence by any element of $Fr(X)$), so that it is a normal subgroup of $Fr(X)$.

Remark 17.13: If $G = \langle a, b\rangle$, and $a^2 = e$, $b^n = e$, $a\,b\,a\,b = e$, then $G = \{e, b, \ldots, b^{n-1}, a, a\,b, \ldots, a\,b^{n-1}\}$, and G is isomorphic to D_n if one adds $e \neq a \neq b \neq e$ and $n \geq 3$.[3] More generally, $a^{\alpha_1}b^{\beta_1}\cdots a^{\alpha_m}b^{\beta_m} = a^\alpha b^\beta$ if $\alpha = \alpha_1 + \ldots + \alpha_m \pmod 2$, and $\beta = (-1)^{\alpha_2+\ldots+\alpha_m}\beta_1 + (-1)^{\alpha_3+\ldots+\alpha_m}\beta_2 + \ldots + (-1)^{\alpha_m}\beta_{m-1} + \beta_m \pmod n$. This follows from Lemma 17.10 if one notices that b^β only depends upon what β is modulo n.

[3] If $e \neq a \neq b \neq e$ and $n = 2$, then $G \simeq \mathbb{Z}_2 \times \mathbb{Z}_2$. If $a = e \neq b$, or if $a = b \neq e$, then $G \simeq \mathbb{Z}_2$ if n is even, and $G = \{e\}$ if n is odd. If $a \neq b = e$, then $G \simeq \mathbb{Z}_2$. If $a = b = e$, then $G = \{e\}$.

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

18- Monday October 10, 2011.

Definition 18.1: A *ring* is a set R equipped with operations $+$ and $\times$ (but the sign for multiplication is usually not written), $(R,+)$ being an Abelian group (with identity 0, and the inverse of x being written $-x$), $\times$ being associative (i.e. $(a\,b)\,c = a\,(b\,c)$ for all $a,b,c \in R$), and *distributive* from both sides with respect to $+$ (i.e. $a\,(b+c) = a\,b + a\,c$ and $(a+b)\,c = a\,c + b\,c$ for all $a,b,c \in R$).

A ring is *commutative* if $\times$ is commutative, i.e. $a\,b = b\,a$ for all $a,b \in R$.

A ring is *unital* if it has a 1 (identity for $\times$, assumed $\neq 0$ for the ring not to be reduced to 0), and in this case a *unit* is any element which has an inverse for multiplication; instead of unital ring, one also uses the terms *unit ring* or *ring with identity*.

A non-zero element $a \in R$ is a *zero-divisor* if there exists a non-zero b (also a zero-divisor) such that $a\,b = 0$. A ring R is an *integral domain* if it is commutative, unital with $1 \neq 0$, and has no *zero-divisor*, so that $a\,b = 0$ implies $a = 0$ or $b = 0$.

A *division ring* is a unital ring for which every non-zero element has an inverse for multiplication (so that it has no zero-divisor).

A *field* is a commutative division ring, i.e. an integral domain for which every non-zero element has an inverse for multiplication.

Remark 18.2: When I was a student (in the mis 1960s), being unital was included in the definition of a ring, and what one now calls a division ring was called a field, so that one stated *Wedderburn's theorem* (which should be called *Dickson–Wedderburn theorem*) as "every finite field is commutative",[1] but now that one has added commutativity in the axioms of fields, it is stated as "every finite division ring is a field".

Lemma 18.3: If a finite ring R with more than one element has no zero-divisor, then it is a division ring (hence it is a field by Wedderburn's theorem).
Proof: $R^* = R \setminus \{0\}$ is non-empty, and multiplication on R^* is regular, so that for $a \in R^*$ the mapping $x \mapsto x\,a$ is injective (because $x\,a = y\,a$ implies $(x-y)\,a = 0$, hence $x - y = 0$), but an injective mapping from a finite set into itself is surjective (hence bijective), so that there is a unique element $\ell_a \in R^*$ satisfying $\ell_a a = a$; one deduces that $\ell_a\,a\,b = a\,b$ for all $b \in R^*$, and since $a\,b$ can be any element of R^* one deduces that all ℓ_a coincide, hence there exists a *left-identity* λ such that $\lambda\,r = r$ for all $r \in R^*$ (and it is also true for $r = 0$). Similarly, using the mapping $x \mapsto a\,x$, one finds a unique element $r_a \in R^*$ such that $a\,r_a = a$, and then all r_a coincide, so that there exists a *right-identity* ρ such that $r\,\rho = r$ for all $r \in R^*$ (and it is also true for $r = 0$). Then $\lambda = \rho$, which one then denotes 1, by considering $\lambda\,\rho$, which is ρ because λ is a left-identity, and which is λ because ρ is a right-identity.

By the same argument, every $a \in R^*$ has a left inverse b satisfying $b\,a = 1$ and a right inverse c satisfying $a\,c = 1$, but $b\,a\,c = (b\,a)\,c = 1\,c = c$ and it also is $= b\,(a\,c) = b\,1 = b$, so that every non-zero element has an inverse.

Remark 18.4: Lemma 18.3 is not true for infinite rings, since even for a field F the polynomial ring $F[x]$ will be shown to be an integral domain, and even a PID (principal ideal domain), or even more an Euclidean domain, but not a field, since only the non-zero constants have an inverse in $F[x]$.

For mappings from a set X into itself, with composition as an associative operation and id_X as identity, an element f has a left inverse g (such that $g \circ f = id_X$) if and only if f is injective, and it has a right inverse h (such that $f \circ h = id_X$) if and only if f is surjective. One way of using this idea for creating a ring R such that some elements have many different left inverses or many different right inverses (but not both), is to consider a field F, the vector space $V = F^{\mathbb{N}^\times}$, and $R = L(V;V)$ the ring of all linear mappings from V into itself: the mapping which to $x = (x_1, x_2, \ldots)$ associates $(0, x_1, x_2, \ldots)$ is linear and injective but not

[1] Joseph Henry Maclagan WEDDERBURN, Scottish-born mathematician, 1882–1948. He worked at Princeton University, Princeton, NJ. Wedderburn's theorem is named after him, but since his first "proof" contained a gap (only discovered later) and DICKSON published another proof after, but before WEDDERBURN published two other proofs, it should be named the Dickson–Wedderburn theorem.

surjective and has for left inverses any linear mapping which to $y = (y_1, y_2, \ldots)$ associates $y_1 v + (y_2, y_3, \ldots)$ where $v \in V$ is an arbitrary vector; the mapping which to $x = (x_1, x_2, \ldots)$ associates $(x_2, x_3, \ldots)$ is linear and surjective but not injective and has for right inverses any linear mapping which to $y = (y_1, y_2, \ldots)$ associates $(\ell(y), y_1, y_2, \ldots)$ where ℓ is an arbitrary linear mapping from V into F, i.e. $\ell(y) = \sum_j \lambda_j y_j$ with $\lambda_j \in F$ for all j but only a finite number of λ_j being $\neq 0$.

If in a unital ring an element x has a left inverse y and a right inverse z, i.e. $y\,x = x\,z = 1$, then one has $z = y$, because $y\,x\,z = (y\,x)\,z = 1\,z = z$, and $y\,x\,z = y\,(x\,z) = y\,1 = y$.

Definition 18.5: A *left-ideal* J of a ring R is an additive subgroup of R such that $r\,j \in J$ for all $r \in R$ and all $j \in J$; a *right-ideal* J of a ring R is an additive subgroup of R such that $j\,r \in J$ for all $r \in R$ and all $j \in J$; an *ideal* of R (also called a *two-sided ideal*) is both a left-ideal and a right-ideal.

If J is an ideal of R, then the quotient group R/J has a ring structure, since $(a + j_1)\,(b + j_2) \in a\,b + J$ for all $j_1, j_2 \in J$.

Remark 18.6: Left-ideals or right-ideals are particular subrings of R,[2] but even if R is unital they are not necessarily unital. If R is a unital ring, any left-ideal or right-ideal containing a unit must coincide with R (since it then contains 1), so that if R is a division ring (or a field) the only left-ideals or right-ideals are $\{0\}$ and R.

If R is unital with multiplicative identity 1_R, it may exist a proper ideal J which is also unital with multiplicative identity $1_J \neq 1_R$: for $R = \mathbb{Z}_n$ with $n = m\,k$ and $(m, k) = 1$, let ℓ satisfy $\ell\,m = 1 \pmod{k}$ (so that one may impose that $\ell \in \{1, \ldots, k-1\}$), then $J = \{0, m, \ldots, (k-1)\,m\}$ is an ideal whose product is defined by $(m\,x)\,(m\,y) = m\,z$ with $z = m\,x\,y \pmod{k}$, so that $1_J = \ell\,m$.[3]

If R is unital and J is an ideal, then the quotient ring R/J is unital, with $1_J = 1_R + J$, but if R is not unital, it is possible that a quotient R/J be unital: if $R_0 = \mathbb{Z}_{20}$ and $R = 2R_0$, which is an ideal of R_0 hence a ring, then R is not unital,[4] but if $J = 5R = 10R_0$ (so that $J = \{0, 10\}$), then R/J is isomorphic to $2\mathbb{Z}_{10} = \{0, 2, 4, 6, 8\}$ which has $1_{2\mathbb{Z}_{10}} = 6$.

Definition 18.7: For a subset X of a ring R, the *ideal generated by* X,[5] denoted (X), is the smallest ideal containing X, i.e. the intersection of all ideals containing X (so that $(\emptyset) = \{0\}$). A *finitely generated ideal* is an ideal (X) for a finite set X, a *principal ideal* is any ideal (a) generated by one element.

A ring R is a *principal ideal ring* if every ideal of R is principal; a *principal ideal domain*, abbreviated *PID*, is an integral domain (i.e. a unital ring which is commutative and has no zero-divisor) in which every ideal is principal.

Lemma 18.8: In a ring R, for $a \in A$, one has $(a) = \left\{r\,a + a\,s + n\,a + \sum_{i=1}^m r_i a\,s_i \mid n \in \mathbb{Z}, m \geq 1, r, r_1, \ldots, r_m, s, s_1, \ldots, s_m \in R\right\}$.

Proof: For $n \in \mathbb{N}^\times$ and $r \in R$, $n\,r$ means $r + \ldots + r$ with n terms, and $(-n)\,r$ means $n\,(-r)$, so that although R may not be unital (so that $1 + \ldots + 1$ does not make sense), $n\,r \in R$ and one checks that the distributivity implies that for all $r, s \in R$ and $m, n \in \mathbb{Z}$ one has $(m\,r)\,(n\,s) = (m\,n)\,(r\,s)$. If J is an ideal containing a, it then contains terms like $r\,a, a\,s, n\,a, r\,a\,s$ for $r, s \in R$ and $n \in \mathbb{Z}$, hence it contains $J_a = \left\{r\,a + a\,s + n\,a + \sum_{i=1}^m r_i a\,s_i \mid n \in \mathbb{Z}, m \geq 1, r, r_1, \ldots, r_m, s, s_1, \ldots, s_m \in R\right\}$. On the other hand, J_a is a subgroup, and for any $\rho \in R$ and $x \in J_a$ one has $\rho\,x \in J_a$ and $x\,\rho \in J_a$, so that J_a is an ideal, which is then the smallest ideal containing a.

Remark 18.9: If R is a commutative unital ring, one then has $(a) = \{r\,a \mid r \in R\}$, and more generally $(a_1, \ldots, a_m) = \left\{\sum_{i=1}^m r_i a_i \mid r_1, \ldots, r_m \in R\right\}$.

---

[2] It is important here not to impose a unit for multiplication in the definition of a ring. Actually, it is a simple way to construct rings which are not unital: in $\mathbb{Z}$ (which is an integral domain), the ideals have the form $n\,\mathbb{Z}$ for $n \in \mathbb{N}$, and for $n \geq 2$ the ring $n\,\mathbb{Z}$ is not unital.

[3] For example, in $\mathbb{Z}_{10}$, $J = \{0, 2, 4, 6, 8\}$ and $1_J = 6$.

[4] Since 1_R would be $2a$ for some a, with the property that $2a \cdot 2x = 2x \pmod{20}$ for all x, which is false for x odd.

[5] One could as well consider the smallest left-ideal containing X, or the smallest right-ideal containing X: they exist, since any intersection of left-ideals is a left-ideal and any intersection of right-ideals is a right-ideal.

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

19- Wednesday October 12, 2011.

Definition 19.1: The *characteristic* of a unital ring R is the smallest $n \geq 2$ such that $n\,1 = 0$ if there exists a non-zero integer m with $m\,1 = 0$, or it is 0.

Remark 19.2: For $n \geq 2$, the characteristic of $\mathbb{Z}_n$ is n; for $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, the characteristic is 0.

Using $(m_1 1)\,(m_2 1) = (m_1 m_2)\,1$, one deduces that if R is unital with no zero-divisor (in particular for an integral domain), then the characteristic is either 0 or a prime p.

Definition 19.3: In a ring R, if $A_1, \ldots, A_m$ are ideals (with $m \geq 2$), then $A_1 \cdots A_m$ denotes the sums of products of the form $a_1 \cdots a_m$ with $a_j \in A_j$ for $j = 1, \ldots, m$.[1] In particular, if A is an ideal of R, then $A^m = \left\{ \sum_{i=1}^{n} a_{i,1} \cdots a_{i,m} \mid a_{i,j} \in A \text{ for } i = 1, \ldots, n, j = 1, \ldots, m, n \geq 1 \right\}$.

Remark 19.4: If R is commutative and unital,[2] $A_1 \cdots A_m$ is the smallest ideal containing $A_1, \ldots, A_m$, since any ideal containing $A_1, \ldots, A_m$ must contain terms like $a_1 \cdots a_m$ with $a_j \in A_j$ for $j = 1, \ldots, m$, hence sums of such products, and the set of such finite sums is an ideal.

Definition 19.5: If $x, y \in R$ and R is a commutative ring, one says that x *divides* y, noted $x \mid y$, if there exists $r \in R$ such that $r\,x = y$. One says that x and y are *associates* if x divides y and y divides x.

Remark 19.6: If R is commutative and unital, then x divides y if and only if $y \in (x)$, since in this case the ideal generated by x is $(x) = \{r\,x \mid r \in R\}$, and one deduces that x and y are associates if and only if $(x) = (y)$.

In $2\mathbb{Z}_{16}$, which is not unital (since $2x\,2y = 2y \pmod{16}$ is false for y odd), one has $6 + 6 + 6 = 2 \pmod{16}$, so that $2 \in (6)$, hence $(2) = (6) = 2\mathbb{Z}_{16}$, but 6 does not divide 2, since $2x \cdot 6 = 2 \pmod{16}$ is false for all x.

If R is an integral domain (i.e. commutative, unital, and with no zero-divisor), then x and y are associates if and only if $y = x\,u$ for a unit u (so that $x = y\,u^{-1}$ and u^{-1} is a unit), since when x, y are non-zero, $y = x\,u$ and $x = y\,v$ imply $u\,v = 1$.

In $\mathbb{Z}_{12}$ (which is commutative and unital, but not an integral domain), 4 divides 8, since $2 \cdot 4 = 8$ (modulo n for all n), but also 8 divides 4, since $2 \cdot 8 = 16 = 4 \pmod{12}$. However 2 is not a unit.

Definition 19.7: A ring R is *Noetherian* if it satisfies the *ascending chain condition* on ideals,[3] i.e. if $J_1 \subset J_2 \subset \cdots \subset J_k \subset \cdots$ are ideals of R, then there exists n with $J_n = J_{n+1} = \cdots$, and one also says that every increasing sequence of ideals becomes constant; equivalently, every non-empty family of ideals has a maximal element.[4] A ring R is *Artinian* if it satisfies the *descending chain condition* on ideals of R, i.e. if $\cdots \subset J_k \subset \cdots \subset J_2 \subset J_1$ are ideals, then there exists n with $\cdots = J_{n+1} = J_n$,[5] and one also says that every decreasing sequence of ideals becomes constant; equivalently, every non-empty family of ideals has a minimal element.

Lemma 19.8: A ring R is Noetherian if and only if every ideal of R is finitely generated (so that principal ideal rings, and in particular PID, are Noetherian).

---

[1] Recall that for subgroups $H, K \leq G$, $H\,K$ is just the set of elements of the form $h\,k$ with $h \in H, k \in K$.

[2] If R is not commutative, then one must also consider for any permutation σ (of $\{1, \ldots, n\}$) terms $a_1 \cdots a_m$ with $a_j \in A_{\sigma(j)}$ for $j = 1, \ldots, m$.

[3] Emmy Amalie NOETHER, German-born mathematician, 1882–1935. Until 1933 she worked at Georg-August-Universität, Göttingen, Germany, and then in Bryn Mawr, PA.

[4] If a non-empty family $\mathcal{I}$ of ideals had no maximal element, one would pick any $J_1 \in \mathcal{I}$, and since J_1 is not maximal there would exist $J_2 \neq J_1$ with $J_1 \subset J_2$, and by induction one would obtain an increasing sequence of ideals which would not become constant, since all its terms are distinct. Conversely, any increasing sequence of ideals $J_1 \subset J_2 \subset \cdots \subset J_k \subset \cdots$ contains a maximal element, which is J_n for some n, so that $J_{n+k} = J_n$ for all $k \in \mathbb{N}$.

[5] Emil ARTIN, Austrian-born mathematician, 1898–1962. He worked in Hamburg, Germany, at University of Notre Dame, IN, at Indiana University, Bloomington, IN, and at Princeton University, Princeton, NJ.

Proof: Assumes that R is Noetherian but there exists an ideal J of R which is not finitely generated, then one constructs by induction a sequence $r_k \in J$, $k \geq 1$, such that $r_{k+1} \notin (r_1, \ldots, r_k)$ for all $k \geq 1$, and then $J_k = (r_1, \ldots, r_k)$ would be an increasing sequence of ideals which is not eventually constant.

If every ideal is finitely generated and $J_1 \subset J_2 \subset \ldots$ is an increasing sequence of ideals, one defines $J_\infty = \bigcup_{k \geq 1} J_k$, so that J_∞ is an ideal,[6] and by hypothesis J_∞ is generated by a finite set X, but X being finite one has $X \subset J_m$ for some m large enough, and since it implies $(X) \subset J_m$, one deduces that $J_n = J_m$ for all $n \geq m$.

Remark 19.9: $\mathbb{Z}$ is not Artinian (since (2^n) is a decreasing sequence of ideals which does not become constant), but it is Noetherian since it is a PID: indeed, an ideal being an additive subgroup has the form $n\,\mathbb{Z}$ for some n, and $n\,\mathbb{Z} = (n)$. It is useful to recall the proof based on the Euclidean division algorithm: if $J \subset \mathbb{Z}$ is an ideal, either it is $\{0\}$ or it contains a positive integer, so that it contains a smallest positive integer $d \in J$, and then any $n \in \mathbb{Z}$ may be written as $n = d\,q + r$ for a *quotient* $q \in \mathbb{Z}$ and a *remainder* $r \in \{0, \ldots, r-1\}$, but then $r \in J$ (since n and $d\,q$ belong to J), so that r must be 0 by definition of d.

The property of $\mathbb{Z}$ being a PID easily gives Bachet's theorem,[7] that if a, b are positive integers and their gcd (greatest common divisor) is d, then there exists $x, y \in \mathbb{Z}$ such that $a\,x + b\,y = d$. One should observe that the usual way to compute the gcd is to look at the factorization using a common list of (distinct) prime numbers $p_1, \ldots, p_k$, so that $a = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ and $b = p_1^{\beta_1} \cdots p_k^{\beta_k}$ with $\alpha_j, \beta_j \geq 0$ and $\max\{\alpha_j, \beta_j\} \geq 1$ for $j = 1, \ldots, k$, and then the gcd (a, b) is $d = p_1^{\gamma_1} \cdots p_k^{\gamma_k}$ with $\gamma_j = \min\{\alpha_j, \beta_j\}$ for $j = 1, \ldots, k$. The theorem of Bachet then introduces addition in a problem where everyone was thinking in term of multiplication, a little like for the *Goldbach conjecture*,[8] that every even integer ≥ 4 is the sum of two primes, an additive question about primes, whose definition only involves multiplication.

Since $a = b\,q + r$ implies that the ideal (a, b) generated by a and b coincides with (b, r) generated by b and r,[9] it gives a quite efficient algorithm for finding the gcd of two numbers, with a number of operations estimated by Lamé: if $a, b \leq Fib_n$, the nth Fibonacci number, the number of operations is bounded by n; in contrast, no efficient algorithm for factorization of integers is known, and cryptography uses this fact extensively.

Remark 19.10: It will be seen that for a field F the ring $F[x]$ of polynomials in one variable with coefficients in F is a PID, and even an Euclidean domain, but the ring $F[x_1, x_2]$ of polynomials in two variables with coefficients in F is not a PID, and since it is isomorphic to $R[x_2]$ with $R = F[x_1]$, one deduces that if a ring R is a PID, then the ring $R[x]$ of polynomials in one variable with coefficients in R is not necessarily a PID. It is then useful to find properties $\mathcal{P}$ such that if R has property $\mathcal{P}$, then $R[x]$ has property $\mathcal{P}$: being commutative, being unital, being an integral domain are such properties, and then two such other properties have been found, being a UFD (unique factorization domain) or being Noetherian, and *Hilbert's basis theorem* (which will be proved in another lecture) states that for R a commutative ring, $R[x]$ is a Noetherian ring if and only if R is a Noetherian ring.

One of the goals of Hilbert was to understand ideals in $F[x_1, \ldots, x_N]$, for example comparing the ideal $\mathcal{I}_1 = (P_1, \ldots, P_m)$ generated by polynomials in $F[x_1, \ldots, x_N]$, and the ideal $\mathcal{I}_2$ of polynomials which are 0 on the set of common zeros of $P_1, \ldots, P_m$: one has $\mathcal{I}_1 \subset \mathcal{I}_2$, and *Hilbert's nullstellensatz* states that if F is algebraically closed,[10] then $P \in \mathcal{I}_2$ if and only if P belongs to the radical of $\mathcal{I}_1$, i.e. there exists $k \geq 1$ with $P^k \in \mathcal{I}_1$; a weaker form is that if the set of common zeros of $P_1, \ldots, P_m$ is empty, then $1 \in \mathcal{I}_1$.

Such questions which interested algebraists in the 19th century were considered "pure mathematics" until recently, but since applications of algebra have appeared, it is useful to wonder if they were thought of by mathematicians who had an interest in questions from outside mathematics, or if they were imagined by engineers who had enough background in algebra for solving the questions which they had encountered.

---

[6] If $a, b \in J_\infty$, then $a \in J_j$ and $b \in J_k$ and one may assume that $j \leq k$ (or one exchanges a and b), so that $a, b \in J_k$, hence $a + b \in J_k \subset J_\infty$; of course $-a \in J_j \subset J_\infty$ and $r\,a, a\,r \in J_j \subset J_\infty$ for all $r \in R$.

[7] Claude Gaspard Bachet, sieur de Méziriac, French mathematician, 1581–1638.

[8] Christian Goldbach, German-born mathematician, 1690–1764. He worked in St Petersburg, Russia.

[9] Notice the danger of confusion with the notation: (a, b) either designates the gcd of a and b, or the ideal generated by a and b.

[10] A field F is algebraically closed if every non constant $P \in F[x]$ has a root. $\mathbb{C}$ is algebraically closed, but not $\mathbb{R}$ or $\mathbb{Q}$.

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

20- Friday October 14, 2011.

Remark 20.1: In vector spaces (over a field F) one has a notion of *dimension*, so that inside a subspace of finite dimension d, all the proper subspaces have a dimension $< d$, but this property is not true for modules (over a ring R), and a ring R (which is an R-module) may be finitely generated (by 1 if it is unital) and have an ideal (which is an R-submodule) which is not finitely generated: in $R = \mathbb{Z}[x_1, x_2, \ldots]$, the (unital) ring of all polynomials in infinitely many variables (but a given polynomial is a finite sum of monomials, hence uses only a finite number of variables), the ideal $J = (x_1, x_2, \ldots)$ is not finitely generated. Indeed, if it was generated by $\{P_1, \ldots, P_k\}$ it would be generated by $\{x_1, \ldots, x_m\}$ if the variables appearing in $P_1, \ldots, P_k$ have an index $\leq m$, but all polynomials in $(x_1, \ldots, x_m)$ give the value 0 if one evaluates them at $x_1 = \ldots = x_m = 0$ and $x_{m+1} = 1$, while x_{m+1} is not 0 at this point, so that $x_{m+1} \notin (x_1, \ldots, x_m)$.

Definition 20.2: If R is an integral domain, its *field of fractions* F is defined as the equivalence classes of pairs (a, b) with $a, b \in R$ and $b \neq 0$ for the equivalence relation $(a, b) \mathcal{R} (c, d)$ if and only if $a\,d = b\,c$ (similar to $\frac{a}{b} = \frac{c}{d}$ for usual fractions). On F, addition corresponds to $(a, b) + (c, d) = (a\,d + b\,c, b\,d)$ (similar to $\frac{a}{b} + \frac{c}{d} = \frac{a\,d + b\,c}{b\,d}$ for usual fractions), and multiplication to $(a, b)\,(c, d) = (a\,c, b\,d)$ (similar to $\frac{a}{b}\,\frac{c}{d} = \frac{a\,c}{b\,d}$ for usual fractions), which are compatible with the equivalence relation $\mathcal{R}$, and it makes F a field.

Remark 20.3: It was mentioned that since addition on $\mathbb{N}$ is commutative, associative, and regular (i.e. $a + x = a + y$ implies $x = y$), it should have been natural to invent $\mathbb{Z}$ as the set of pairs (a, b) with the intuition that it means $a - b$, with the interpretation that it is like for a merchant to measure his wealth by his availablecash amount $a \in \mathbb{N}$ and the amount $b \in \mathbb{N}$ which he has borrowed (in an ideal world where one can borrow without interest).

Once one notices what is used in the construction, the same idea applies to $\mathbb{N}^\times$ for multiplication and creates the multiplicative group $\mathbb{Q}_+$, but then there is a natural symmetrization for addition on $\mathbb{Q}_+$ or a natural symmetrization for multiplication on $\mathbb{Z}$, which both permit to define $\mathbb{Q}$. If one looks at what is needed for this scheme to work, one arrives naturally at the situation described in Definition 20.2 for any integral domain, but one can be more general.

If R is a commutative ring and $D \subset R$ is non-empty, stable by multiplication (i.e. $d_1, d_2 \in D$ implies $d_1 d_2 \in D$) and contains no zero-divisor, it is natural to construct a commutative unital ring (denoted $D^{-1}R$) which contains (an isomorphic copy of) R as a subring and such that every element of D is a unit in $D^{-1}R$: the equivalence relation $\mathcal{R}$ is defined on $R \times D$ (with (r, d) intuitively meaning $\frac{r}{d}$) by $(r_1, d_1) \mathcal{R} (r_2, d_2)$ meaning $r_1\,d_2 = r_2\,d_1$, addition is defined on $R \times D$ by $(r_1, d_1) + (r_2, d_2) = (r_1 d_2 + r_2 d_1, d_1 d_2)$ and multiplication is defined on $R \times D$ by $(r_1, d_1) \cdot (r_2, d_2) = (r_1 r_2, d_1 d_2)$, and both these operations extend to the quotient $R \times D / \mathcal{R}$, and give a structure of commutative unital ring; the element 1 is the equivalence class of (d, d) for any $d \in D$ (and one has $(d_1, d_1)\,\mathcal{R}\,(d_2, d_2)$ for all $d_1, d_2 \in D$); that $D^{-1}R$ contains (an isomorphic copy of) R is seen by mapping $r \in R$ to the equivalence class of $(r\,d, d)$ (which intuitively means $\frac{r\,d}{d}$) for any if $d \in D$ (and one has $(r\,d_1, d_1)\,\mathcal{R}\,(r\,d_2, d_2)$ for all $d_1, d_2 \in D$); that elements of D become units in $D^{-1}R$ is related to the fact that the inverse of the equivalent class of $(d\,d_1, d_1)$ is the equivalent class of $(d_2, d\,d_2)$ for any $d_1, d_2 \in D$. For example, if $R = \mathbb{Z}$ and $D = \{2, \ldots, 2^n, \ldots\}$, then one obtains the elements of $\mathbb{Q}$ whose reduced form has a denominator which is a power of 2. Definition 20.2 corresponds to the possibility of taking $D = R \setminus \{0\}$, and in this case $D^{-1}R$ is a field.

Of course, Definition 20.2 (or the generalization just mentioned) makes sense if one checks what it claims, that $\mathcal{R}$ is an equivalence relation on $R \times D$, that the addition or the multiplication of two elements of $R \times D$ gives something equivalent if one replaces each of the two elements by an equivalent element, that associativity holds for addition and for multiplication, that 0 corresponds to $(0, d)$ and $-(r, d)$ corresponds to $(-r, d)$, and that multiplication is distributive with respect to addition: it is a little tedious but it presents no real difficulty.

Definition 20.4: If R_1, R_2 are two rings, a mapping f from R_1 into R_2 is a *ring-homomorphism* if $f(x+y) = f(x) + f(y)$ for all $x, y \in R_1$, and $f(x\,y) = f(x)\,f(y)$ for all $x, y \in R_1$. The *kernel* of f is $\{x \in R_1 \mid f(x) = 0\}$.

Remark 20.5: If f is a ring-homomorphism from R_1 into R_2, then its kernel $ker(f) = f^{-1}(\{0\})$ is an ideal of R_1 (since $f(a) = 0$ implies $f(r\,a) = f(a\,s) = 0$ for all $r, s \in R$), and its image $f(R_1)$ is a subring of R_2, so that f induces an injective ring-homomorphism from the quotient $R_1/ker(f)$ into R_2, hence $R_1/ker(f)$ is isomorphic to the image $f(R_1)$ as rings (first isomorphism theorem).

A ring-homomorphism f from R_1 into R_2 is an homomorphism of the additive groups, so that $f(0) = 0$ and $f(-r) = -f(r)$ for all $r \in R_1$, but one should pay attention that R_1 may be unital while R_2 may not be unital, so that one may wonder what $f(1_{R_1})$ is. For example, $R_1 = \mathbb{Z}_5$ is a field, and $R_2 = 2\mathbb{Z}_{20}$ is a ring which is not unital, and the mapping defined by $f(x) = 16x \pmod{20}$ is a ring homomorphism from R_1 into R_2, because $16 \cdot 5 = 0 \pmod{20}$ and $16x \cdot 16y = 16x\,y \pmod{20}$ for all x, y (since $256 = 16 \pmod{20}$; one has $f(R_1) = 4\mathbb{Z}_{20}$, and $f(1_{R_1}) = 1_{f(R_1)} = 16$.

In general $f(1_{R_1})$ is an element of R_2 which is *idempotent*, i.e. satisfies $r^2 = r$, since $1^2 = 1$ implies $\big(f(1)\big)^2 = f(1)$. If R is an integral domain then only 0 and 1_R are idempotent (since $r\,(r-1) = 0$ implies $r = 0$ or $r - 1 = 0$), but if $n = m_1 m_2$ with $m_1, m_2 \geq 2$ and relatively prime, then $\mathbb{Z}_n$ (which is commutative and unital) has (at least) two idempotent elements different from 0 or 1: $a = 0 \pmod{m_1}$ and $a = 1 \pmod{m_2}$ gives a idempotent; $b = 1 \pmod{m_1}$ and $b = 0 \pmod{m_2}$ gives b idempotent. Actually, if R is commutative and $r \in R$ is idempotent, the ideal $J = (r)$ is unital with $1_J = r$ (since $r\,(r\,x) = r\,x$ for all $x \in R$), and defining f by $f(x) = r\,x$ gives a ring-homomorphism from R into J.

If V is a vector space of dimension ≥ 2 over a field F, then $R = L(V;V)$ is a non-commutative unital ring (with identity denoted I), and a nilpotent element P is called a *projection*: $X = ker(P)$ and $Y = ker(I - P)$ are supplementary vector subspaces (i.e. such that $X \cap Y = \{0\}$ and $X + Y = V$) so that every $v \in V$ has a unique decomposition $x = (I - P)\,x + P\,x$ into an element of X (which is $x - P\,x$) plus an element of Y (which is $P\,x$). In general, if V_1 is a subspace, a projection onto V_1 is specified as being parallel to a subspace V_2 which is supplementary to V_1, and P is defined by $P\,v = v$ if $v \in V_1$ and $P\,v = 0$ is $v \in V_2$.

Remark 20.6: If two elements a, b in a ring R commute, then one has the binomial formula $(a+b)^k = \sum_{j=0}^{k} \binom{k}{j} a^j b^{k-j}$, obtained in developing $(a+b)\cdots(a+b)$ and observing that (because a and b commute) there are as many terms $a^j b^{k-j}$ as subsets of size j in $\{1, \ldots, k\}$, but if R is not unital, one may prefer to write it $(a+b)^k = a^k + \sum_{j=1}^{k-1} \binom{k}{j} a^j b^{k-j} + b^k$ for avoiding a^0 and b^0, since one cannot use the convention that it means 1_R which does not exist, or one may say that the convention is that $a^0 x$ means x for all $x \in R$.

If R is a commutative unital ring of *prime* characteristic p, then $(a+b)^p = a^p + b^p$ for all $a, b \in R$, because one has $\binom{p}{k} = 0 \pmod{p}$ if $k \neq 0, p$ (since p is prime), and $p\,r = 0$ for all $r \in R$.

Definition 20.7: An integral domain R is an *Euclidean domain* if there is a function V (sometimes called valuation,[1] or norm,[2] or gauge) from $R \setminus \{0\}$ into $\mathbb{N}$ such that, for all $a, b \in R$ with $b \neq 0$ one can write $a = b\,q + r$ with either $r = 0$ or $V(r) < V(b)$ (one usually adds $V(x) \leq V(x\,y)$ for all $x, y \neq 0$, shown to be superfluous by K. Rogers & E. G. Straus,[3,4] by replacing V by W defined by $W(x) = \min_{z \neq 0} V(x\,z)$.)

Remark 20.8: This definition, obviously suggested by the Euclidean division algorithm in $\mathbb{Z}$, may have been introduced by Gauss for what one now calls the *Gaussian integers*, $\mathbb{Z}[i] = \{z = a + i\,b \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$.

Definition 20.9: A *polynomial* P over a ring R is a list $(a_0, \ldots, a_n, \ldots)$ with $a_i \in R$ for all $i \geq 0$, and only a finite number of a_i are $\neq 0$, and one also writes $P = \sum_{n \geq 0} a_n x^n$. The *ring of polynomials* $R[x]$ is the set of all polynomials over R equipped with addition and multiplication defined as follows:[5] if $P = \sum_n a_n x^n$

[1] The term valuation will be used for polynomials with a different meaning, while V will be the degree of the polynomial.

[2] In algebra, the term "norm" is used with a different meaning than in analysis, where a norm $||\cdot||$ is defined on a vector space V over $\mathbb{R}$ of $\mathbb{C}$, and satisfies $||x|| > 0$ if $x \in V \setminus \{0\}$, $||v + w|| \leq ||v|| + ||w||$ for all $v, w \in V$, and $||\lambda\,v|| = |\lambda|\,||v||$ for all $v \in V$ and all scalars λ (in $\mathbb{R}$ or $\mathbb{C}$.

[3] Kenneth Rogers, English-born mathematician, 1930–2010. He worked at University of Hawaii at Manoa, Honolulu, HI.

[4] Ernst Gabor Straus, German-born mathematician, 1922–1983. He worked at UCLA (University of California at Los Angeles) Los Angeles, CA.

[5] Checking that $R[x]$ has all the properties for being a ring is not difficult, but it is a little tedious.

and $Q = \sum_n b_n x^n$, then $P + Q = \sum_n c_n x^n$ and $PQ = \sum_n d_n x^n$, with $c_n = a_n + b_n$ for all $n \geq 0$, and $d_n = \sum_{j=0}^{n} a_j b_{n-j}$ for all $n \geq 0$.[6]

For $P \neq 0$, the *degree* of P, denoted $deg(P)$, is the highest n for which $a_n \neq 0$, and the *valuation* of P, denoted $val(P)$, is the smallest n for which $a_n \neq 0$, so that $val(P) \leq deg(P)$ for $P \neq 0$. For $P, Q \neq 0$, one has $deg(P + Q) \leq \max\{deg(P), deg(Q)\}$ and $deg(PQ) \leq deg(P) + deg(Q)$, $val(P + Q) \geq \min\{val(P), val(Q)\}$ and $val(PQ) \geq val(P) + val(Q)$.

If R is unital, a non-zero polynomial P is *monic* if a_n is a unit for $n = deg(P)$, but one often impose $a_n = 1$ for monic polynomials.

Remark 20.10: The degree of a non-zero constant (i.e. $P = a_0 \neq 0$) is 0, and some authors consider that the zero polynomial has degree 0, but a better convention is to consider that $deg(0) = -\infty$ and $val(0) = +\infty$ (so that $deg(0) < val(0)$), and this permits to have $deg(PQ) = deg(P) + deg(Q)$ and $val(PQ) = val(P) + val(Q)$ if R has no zero divisors, for all $P, Q \in R[x]$. One reason for this convention comes from the generalizations to the ring of *formal power series* $R[[x]]$, and the ring of *formal Laurent series* $R((x))$.[7]

Lemma 20.11: If R is commutative, then $R[x]$ is commutative. If R is unital, then $R[x]$ is unital, and a product of monic polynomials is monic. If R has no zero divisor, then $R[x]$ has no zero divisor, and $deg(PQ) = deg(P) + deg(Q)$ for non-zero polynomial $P, Q \in R[x]$. If R is an integral domain, then $R[x]$ is an integral domain.

Proof: Of course, the identity in $R[x]$ is $1 = (1, 0, \ldots, 0, \ldots)$. If $n = deg(P)$ and $m = deg(Q)$ then $deg(PQ) \leq m + n$ and $d_{m+n} = a_m b_n$, which is $\neq 0$ if R has no zero divisor, in which case $deg(PQ) = m + n$; similarly, $a_m b_n$ is a unit if a_m and b_n are units.

[6] Notice that x is not an element of R, and that it commutes with all elements of R; if R is unital, then $x = (0, 1, 0, \ldots, 0, \ldots) \in R[x]$.

[7] 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.

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

21- Monday October 17, 2011.

Lemma 21.1: Every Euclidean domain R is a PID.
Proof: Let J be an ideal of R. Since $\{0\} = (0)$, one may assume that $J \neq \{0\}$, so that the set of non-negative integers $\{V(j) \mid j \in J \setminus \{0\}\}$ is not empty, and it then has a smallest element n_0, which is $V(j_0)$ for some non-zero $j_0 \in J$. For $a \in J$, one has $a = j_0 q + r$ with either $r = 0$, or $r \neq 0$ and $V(r) < V(j_0)$, but the latter cannot hold, since $j_0 q \in J$, which implies $r = a - j_0 q \in J$, so that $V(r) \geq n_0 = V(j_0)$, a contradiction; hence $r = 0$, so that $J = (j_0)$.

Lemma 21.2: (Euclidean division algorithm) If R is a unital commutative ring and $A, B \in R[x]$ with B monic,[1] then $A = B\,q + r$, with $q, r \in R[x]$, and either $r = 0$ or $deg(r) < deg(B)$; q is called the *quotient* and r the *remainder* of the (Euclidean) division of A by B, and they are uniquely determined.
Proof: If $deg(B) = m$ so that b_m is a unit, then one may choose $q = 0$ and $r = P$ if $n = deg(P) < m$, and if $n \geq m$ one uses an induction on n, writing $A = B\,b_m^{-1} a_n x^{n-m} + A_1$ with $deg(A_1) \leq n - 1$, and one concludes by the induction hypothesis.

If $A = B\,q_1 + r_1 = B\,q_2 + r_2$, and if one had $q_1 \neq q_2$, it would imply that $deg\big(B\,(q_1 - q_2)\big) = deg(r_2 - r_1) < m$, but if $deg(q_2 - q_1) = s \geq 0$ one would have $q_2 - q_1 = c_s x^s + \textit{lower order terms}$ with $c_s \neq 0$, which would imply $b_m c_s = 0$ for killing the term in x^{m+s} in $B\,(q_1 - q_2)$, hence $c_s = 0$ since b_m has an inverse for multiplication; this shows that $q_2 = q_1$, which then implies $r_2 = r_1$.

Lemma 21.3: If F is a field, then $F[x]$ is an Euclidean domain, hence a PID.
Proof: By Lemma 21.2, the Euclidean division is defined by any non-zero $B \in F[x]$, and the degree serves as the desired function V.

Definition 21.4: The *polynomial function* associated to $P = a_0 + \ldots + a_n x^n \in R[x]$ is the mapping $r \mapsto P(r) = a_0 + a_1 r + \ldots + a_n r^n$, and $\alpha \in R$ is a *root* of P (or a *zero* of P) if $P(\alpha) = 0$.

Remark 21.5: One should not confuse a polynomial with the polynomial function that it defines: if F is a finite field of order q (which is a power of a prime p), then every non-zero a satisfies $a^{q-1} = 1$, since its order in the multiplicative group F^* must divide the order of F^*,[2] which is $q - 1$, and one deduces that $a^q = a$, which is also valid for $a = 0$, so that the polynomial $x^q - x$ is non-zero but takes the value 0 at all points of F.

This cannot happen in an infinite field (or an infinite integral domain), since in that case a polynomial of degree n cannot have more than n roots, by the following Lemma 21.6.

Lemma 21.6: If R is a commutative ring, then for $P, Q \in R[x]$ and $r \in R$ one has $(P+Q)(r) = P(r) + Q(r)$ and $(P\,Q)(r) = P(r)\,Q(r)$. If moreover R is unital, then $\alpha \in R$ is a root of $P \in R[x]$ if and only if $P = (x - \alpha)\,Q$ for some $Q \in R[x]$. As a consequence, if R is an integral domain, and $P \in R[x]$ is non-zero, then P cannot have d distinct roots with $d > deg(P)$.
Proof: $(P + Q)(r) = P(r) + Q(r)$ holds without commutativity of R, and $(P\,Q)(r) = P(r)\,Q(r)$ is true if $a_i r^i b_j r^j = a_i b_j r^{i+j}$ for all i, j, which is the case if r commutes with all the coefficients b_j of Q, hence it is true for all $r \in R$ if R is commutative.

Since $x - \alpha$ is monic (and one needs R to be unital for having $x \in R[x]$), $P = (x - \alpha)\,Q + r$ holds by Lemma 21.2, and r is a constant, and one wants to show that this constant is $P(\alpha)$: as in footnote # 1, by

[1] If R is unital but not commutative, one may be interested in solving $A = B\,q_1 + r_1$ or in solving $A = q_2 B + r_2$, with either $r_j = 0$ or $deg(r_j) < deg(B)$, and it may happen that $q_1 \neq q_2$. In the case $B = x - \alpha$, with $A = a_0 + \ldots + a_n x^n$, with $\alpha, a_0, \ldots, a_n \in R$, one has $x^k - \alpha^k = (x - \alpha)\,(x^{k-1} + \ldots + \alpha^{k-1}) = (x^{k-1} + \ldots + \alpha^{k-1})\,(x - \alpha)$ for $k \geq 1$, so that after multiplication by a_k on the right or on the left and summing in k, one has $A - \sum_{k=0}^{n} \alpha^k a_k = B\,q_1$ with $q_1 = \sum_{k=1}^{n} (x^{k-1} + \ldots + \alpha^{k-1})\,a_k$, or $A - A(\alpha) = q_2 B$ with $q_2 = \sum_{k=1}^{n} a_k (x^{k-1} + \ldots + \alpha^{k-1})$.

[2] In a unital ring R, R^* denotes the multiplicative group of units of R, so that if F is a field, $F^* = F \setminus \{0\}$.

multiplying $x^k - \alpha^k = (x-\alpha)\,(x^{k-1} + \ldots + \alpha^{k-1})$ for $k \geq 1$ by a_k and summing in k, one deduces that $P - P(\alpha) = (x-\alpha)\,Q$ with $Q = \sum_{k=1}^{n} a_k (x^{k-1} + \ldots + \alpha^{k-1})$.

If R is an integral domain, and $P \in R[x]$ is non-zero, and has distinct roots $\alpha_1, \ldots, \alpha_d$, then $P = (x-\alpha_1)\,Q_1$ and one has $0 = P(\alpha_j) = (\alpha_j - \alpha_1)\,Q_1(\alpha_j)$, and since $\alpha_j - \alpha_1 \neq 0$ for $j \neq 1$, one deduces that Q_1 has distinct roots $\alpha_2, \ldots, \alpha_d$, and one concludes by induction on d that P is divisible by $(x-\alpha_1) \cdots (x-\alpha_d)$, so that the degree of P is $\geq d$ (since in an integral domain the degree of a product of non-zero polynomials is the sum of their degrees).

Remark 21.7: Since a odd implies $a^2 = 1 \pmod 8$, $x^2 - 1$ has four roots in $\mathbb{Z}_8$, namely $1, 3, 5, 7$, corresponding to the factorizations $x^2 - 1 = (x-1)\,(x+1) = (x-3)\,(x+3) = (x-5)\,(x+5) = (x-7)\,(x+7) \pmod 8$, showing that the hypothesis that R has no zero divisors is crucial for the last result of Lemma 21.6 to hold, that there are not more roots than the degree of the polynomial.

Remark that $\mathbb{Z}_8$ is a principal ideal ring, since all its ideals are principal, because besides $\{0\} = (0)$ and $\mathbb{Z}_8 = (1)$ the ideals of $\mathbb{Z}_8$ are $2\mathbb{Z}_8 = \{0, 2, 4, 6\} = (2)$ and $4\mathbb{Z}_8 = \{0, 4\} = (4)$, but it is not a PID, since it is not an integral domain (because 2, 4, and 6 are zero-divisors).

Definition 21.8: If R is a commutative unital ring, and $P \in R[x]$, then $a \in R$ is called a *multiple root* of P if $P = (x-a)^k Q$ for some $Q \in R[x]$ and $k \geq 2$, in which case it is a *root of multiplicity* k (or order k) if P cannot be written as $(x-a)^{k+1} Q_1$ with $Q_1 \in R[x]$, and a is a *simple root* if it is a root but not a multiple root, in which case one counts its "multiplicity" as 1.

Remark 21.9: In the case where R is an integral domain, if P has distinct roots $a_1, \ldots, a_m$ with respective multiplicities $k_1, \ldots, k_m$ then $s = \sum_{j=1}^{m} k_j \leq deg(P)$, and one says that P has s roots *counting multiplicity*.

After proving a criterion for multiple roots using the derivative of a polynomial, the following question will be to describe if there are non-constant polynomials without roots, and the notion of algebraically closed field will be introduced, an example being $\mathbb{C}$, while $\mathbb{R}$ is not algebraically closed and there are polynomials of degree 2 in $\mathbb{R}[x]$ without roots, namely $a\,x^2 + b\,x + c$ when $b^2 < 4a\,c$, but in $\mathbb{Q}$ it will be shown (by Eisenstein's criterion) that there are polynomials in $\mathbb{Q}[x]$ of any degree $d \geq 2$ which are irreducible,[3] i.e. cannot be factored into a product of polynomials of lower order.

The notion of irreducible elements will be introduced in a general context, and compared to another related notion, of prime elements.

Remark 21.10: For $D \in \mathbb{Z}$ not a square, $\mathbb{Z}[\sqrt{D}] = \{z = a + b\sqrt{D} \mid a, b \in \mathbb{Z}\} \subset \mathbb{C}$ (or $\subset \mathbb{R}$ if $D > 0$) is an integral domain; defining the conjugate of $z = a + b\sqrt{D}$ to be $\overline{z} = a - b\sqrt{D}$, one writes $N(z) = z\,\overline{z} = a^2 - D\,b^2$, and from the fact that $\overline{z_1 z_2} = \overline{z_1}\;\overline{z_2}$, one deduces that $N(z_1 z_2) = N(z_1)\,N(z_2)$, so that if z is a unit one must have $N(z) = \pm 1$ (and for $D > 0$ the equation $a^2 - D\,b^2 = \pm 1$ is wrongly called Pell's equation);[4] conversely, if $N(z) = \pm 1$, then z is a unit, and its inverse is $\pm\overline{z}$.

Gauss had found nine values of $D < 0$ (namely $-1, -2, -3, -7, -11, -19, -43, -67, -163$) for which $\mathbb{Z}[\sqrt{D}]$ is a PID, and his conjecture that there are no further values was proved one hundred years later by Heegner,[5] Baker,[6] and Stark.[7]

In $\mathbb{Z}[\sqrt{10}]$, one has $(4 + \sqrt{10})\,(4 - \sqrt{10}) = 6 = 2 \cdot 3$, so that there not a unique factorization of 6 as a product of irreducible elements, which like $4 \pm \sqrt{10}, 2, 3$ cannot be written as $z_1\,z_2$ with neither z_1 nor z_2 a unit, because one would have $N(z) \in \{\pm 2, \pm 3\}$, which is impossible, since it implies $a^2 = \pm 2 \pmod 5$.

---

[3] Ferdinand Gotthold Max Eisenstein, German mathematician, 1823-1852. Eisenstein series are named after him.

[4] John Pell, English mathematician, 1611–1685. Pell's equation is named after him, although he had little to do with it, and it had been studied first by Brahmagupta.

[5] Kurt Heegner, German mathematician, 1893–1965. Heegner numbers are named after him.

[6] Alan Baker, English mathematician, born in 1939. He received the Fields Medal in 1970. He worked at University College, London, and at Cambridge, England.

[7] Harold Mead Stark, American mathematician, born in 1939. He worked at University of Michigan, Ann Arbor, MI, at MIT (Massachusetts Institute of Technology), Cambridge, MA, and at UCSD (University of California at San Diego), La Jolla, CA.

Luc TARTAR, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

22- Wednesday October 19, 2011.

Definition 22.1: If $P = a_0 + a_1 x + \ldots + a_n x^n \in R[x]$, the *derivative of* P, noted P' is $P' = a_1 + 2a_2 x + \ldots + n\, a_n x^{n-1} \in R[x]$.

Remark 22.2: One has $(P+Q)' = P' + Q'$, and $(P\,Q)' = P'Q + P\,Q'$ for all $P, Q \in R[x]$: if $P = a_0 + a_1 x + \ldots + a_n x^n$ and $Q = b_0 + b_1 x + \ldots + b_m x^m$, then for $k \geq 1$ the coefficient of x^k in $P\,Q$ is $\sum_{j=0}^{k} a_j b_{k-j}$, so that the coefficient of x^{k-1} in $(P\,Q)'$ is $k\,\big(\sum_{j=0}^{k} a_j b_{k-j}\big) = \sum_{j=0}^{k} k\,(a_j b_{k-j})$, but for $0 \leq j \leq k$ one has $k\,(a_j b_{k-j}) = (j\,a_j)\,b_{k-j} + a_j\big((k-j)\,b_{k-j}\big)$,[1] and $\sum_{j=0}^{k} (j\,a_j)\,b_{k-j}$ is the coefficient of x^{k-1} in $P'Q$, while $\sum_{j=0}^{k} a_j\big((k-j)\,b_{k-j}\big)$ is the coefficient of x^{k-1} in $P\,Q'$.

If R is commutative, or simply if P and P' commute, one deduces by induction on ℓ that $(P^\ell)' = \ell\, P^{\ell-1} P'$ for $\ell \geq 2$: the preceding case with $Q = P$ gives $(P^2)' = P'P + P\,P'$, which is $2P\,P'$ since P and P' commute; then for $\ell > 2$ one uses $Q = P^{\ell-1}$, so that by the induction hypothesis one has $Q' = (\ell-1)\,P^{\ell-2} P'$, hence $(P^\ell)' = (P\,Q)' = P'Q + P\,Q' = P'P^{\ell-1} + P\,(\ell-1) P^{\ell-2} P'$, which is $\ell\, P^{\ell-1} P'$ since P and P' commute.

If P is a constant, i.e. $P = a_0$, then $P' = 0$, but in some rings it may happen that a non-constant polynomial has a zero derivative: for example, if R is an integral domain with characteristic p (necessarily a prime), then $P' = 0$ means $j\,a_j = 0$ for all $j \geq 0$, but since for $a_j \neq 0$ it implies that j is a multiple of the characteristic p, one deduces that $P' = 0$ if and only if P is a polynomial in x^p, i.e. it has the form $\sum_{\ell=0}^{m} b_\ell x^{\ell\, p}$.

Lemma 22.3: If R is a commutative unital ring, then α is a multiple root of $P \in R[x]$ if and only if $P(\alpha) = 0$ and $P'(\alpha) = 0$.
Proof: If α is a root of multiplicity $k \geq 2$, one has $P = (x-\alpha)^k Q$ (with $Q(\alpha) \neq 0$), so that $P' = k\,(x-\alpha)^{k-1} Q + (x-\alpha)^k Q'$, hence $P(\alpha) = 0$ and $P'(\alpha) = 0$. Conversely, if $P(\alpha) = 0$ one has $P = (x-\alpha)\,Q_1$, so that $P' = Q_1 + (x-\alpha)\,Q_1'$, hence $P'(\alpha) = Q_1(\alpha)$; if $P(\alpha) = 0$ and $P'(\alpha) = 0$, one deduces that $Q_1(\alpha) = 0$, so that $Q_1 = (x-\alpha)\,Q_2$, hence $P = (x-\alpha)^2 Q_2$, i.e. α is a multiple root of P (of multiplicity $k \geq 2$).

Remark 22.4: If R is a commutative unital ring and α is a root of multiplicity $k \geq 2$, then $P = (x-\alpha)^k Q$ with $Q(\alpha) \neq 0$, so that $P' = k\,(x-\alpha)^{k-1} Q + (x-\alpha)^k Q' = (x-\alpha)^{k-1} Q_1$ with $Q_1 = k\,Q + (x-\alpha) Q'$, hence α is a root of multiplicity at least $k-1$ of P'. Since $Q_1(\alpha) = k\,Q(\alpha)$, it may happen that $k\,Q(\alpha) = 0$ although $Q(\alpha) \neq 0$: if R is an integral domain, it means that R has a finite characteristic, which must be a prime p, and k is a multiple of p.

If α is a root of multiplicity $k \geq 3$, then $P(\alpha) = 0$ and the successive derivatives of P up to order $k-1$ are 0 at α. If R is an integral domain of characteristic p, the converse holds if $k \leq p$, and the proof is by induction on k: since $P(\alpha) = P'(\alpha) = 0$ implies $P = (x-\alpha)^2 Q$, it is true for $k = 2$; assume that $k \geq 3$ (so that $p \geq 3$) and that it has been proved up to $k-1$, so that $P = (x-\alpha)^{k-1} Q$, and then the derivative of order $k-1$ has a term in $(k-1)!\,Q$ and all other terms have $x-\alpha$ as a factor, so that the $(k-1)$th derivative of P evaluated at α is $(k-1)!\,Q(\alpha)$, and since $(k-1)!$ is not a multiple of p and the $(k-1)$th derivative of P evaluated at α is 0 by hypothesis, one deduces that $Q(\alpha) = 0$, so that $Q = (x-\alpha)\,Q_1$ and $P = (x-\alpha)^k Q_1$.

One has almost used Leibniz's formula giving the kth derivative of a product,[2] that if one denotes $P^{(j)}$ the jth derivative of P, so that $P^{(1)}$ means P' and $P^{(0)}$ means P, then Leibniz's formula is that $(P\,Q)^{(k)} = \sum_{j=0}^{k} \binom{k}{j} P^{(j)} Q^{(k-j)}$, and it was proved for $k = 1$, and the proof is by induction on k, and it follows easily by using the properties of binomial coefficients.

---

[1] Although R may not be commutative, for $a, b \in R$ and $\ell \in \mathbb{Z}$, one has $\ell\,(a\,b) = (\ell\,a)\,b = a\,(\ell\,b)$: for $\ell > 0$, it is about adding ℓ copies of $a\,b$, and the formula follows from distributivity; for $\ell < 0$, it is a consequence of $-(a\,b) = (-a)\,b = a\,(-b)$, which is about having $0 = (a\,b) + (-a)\,b = (a\,b) + a\,(-b)$, which again follows from distributivity.

[2] Gottfried Wilhelm VON LEIBNIZ, German mathematician, 1646–1716. He worked in Frankfurt, in Mainz, Germany, in Paris, France, and in Hanover, Germany, but never in an academic position.

Remark 22.5: If R is a commutative unital ring, one can prove Taylor's expansion for polynomials: the usual formula taught in analysis is $P(x+h) = P(x) + P'(x)\,h + \frac{P''(x)\,h^2}{2!} + \ldots$, but for a polynomial the sum is finite, since $P^{(n+1)} = 0$ if P has degree n; since a term $\frac{P^{(j)}(x)\,h^j}{j!}$ appears, which may not make sense in some rings because one cannot always divide elements of R by $j!$, one should pay attention to the notation. If $P = x^k$ then $P^{(j)} = k \cdots (k+1-j)\,x^{k-j}$ if $j \leq k$ and 0 if $j > k$, so that $\frac{P^{(j)}(x)\,h^j}{j!} = \binom{k}{j} x^{k-j} h^j$ and since $\binom{k}{j}$ is an integer, one never divides an element of R by an integer. Then the proof is obtained by writing the binomial formula for $(x+h)^k$, which one multiplies by a_k before summing in k.

In particular, if $P \in \mathbb{Z}[x]$, then one has observed that $\frac{P^{(j)}}{j!} \in \mathbb{Z}[x]$, so that if $a, h \in \mathbb{Z}$ one has $P(a+h) = P(a) + P'(a)\,h + \sum_{j=2}^{deg(P)} c_j h^j$, with $c_j \in \mathbb{Z}$ for $j = 2, \ldots, deg(P)$. In the following application, if p is a prime and h is a multiple of p^m (with $m \geq 1$), then $P(a+h) = P(a) + P'(a)\,h \pmod{p^{2m}}$.

Remark 22.6: If $P \in \mathbb{Z}[x]$ and $f(N)$ is the number of solutions in $\mathbb{Z}_N$ of $P(x) = 0 \pmod{N}$, then f is a multiplicative function by the Chinese remainder theorem, so that one must just wonder how many solutions there is modulo p^k for a prime p and an integer $k \geq 1$. If a_1 is a solution of $P(a_1) = 0 \pmod{p}$ and one has $P'(a_1) \neq 0 \pmod{p}$, then one can construct a sequence $a_2, \ldots, a_k$ such that $a_j = a_{j-1} \pmod{p^{j-1}}$ for $j = 2, \ldots, k$ and $P(a_k) = 0 \pmod{p^k}$, so that $P'(a_k) = P'(a_1) \neq 0 \pmod{p}$. For example, one looks for $a_2 = a_1 + b_1 p$, and one uses the Taylor expansion, which gives $P(a_2) = P(a_1) + P'(a_1)\,b_1 p + \ldots$ where the terms not written contain $b_1 p$ to a power ≥ 2, so that $P(a_2) = P(a_1) + P'(a_1)\,b_1 p \pmod{p^2}$; since $P(a_1) = 0 \pmod{p}$, one has $P(a_1) = c_1 p \pmod{p^2}$ for some $c_1 \in \mathbb{Z}$, so that $P(a_2) = 0 \pmod{p^2}$ is equivalent to $c_1 + P'(a_1)\,b_1 = 0 \pmod{p}$, which has a unique solution b_1 modulo p, because $P'(a_1)$ has an inverse modulo p.

Essentially, it is the same idea used in a method of NEWTON for solving equations, which is now known as the *Newton–Raphson method*:[3] if f is a differentiable function on $\mathbb{R}$ and $f'(x_0) \neq 0$, a guess for a solution of $f(x) = 0$ is to replace $f(x) = 0$ by $f(x_0) + f'(x_0)\,(x - x_0) = 0$, so that one takes $x_1 = x_0 - \frac{f(x_0)}{f'(x_0)}$, and the iterative method $x_{n+1} = x_n - \frac{f(x_n)}{f'(x_n)}$ converges under some condition.[4]

HENSEL must have thought of this analogy when he invented the p-adic numbers $\mathbb{Q}_p$ in 1897,[5] by using a different metric on $\mathbb{Q}$ (hence on $\mathbb{Z}$) than the usual one, so that the sequence a_k constructed converges to an element of $\mathbb{Q}_p$. For example, if $P = x^2 - 2$ and $p = 7$, then $P(3) = 7 = 0 \pmod{7}$ and $P'(3) = 6 \neq 0 \pmod{7}$, so that the method creates a sequence of integers, which converges in Q_7 to a root of P, but is this root $+\sqrt{2}$ or $-\sqrt{2}$? For example, $1 + 2 + \ldots + 2^n + \ldots$ converges in $\mathbb{Q}_2$, to -1, and it is quite similar to what will be shown later for formal power series that $(1-x)^{-1} = 1 + x + \ldots + x^n + \ldots$, but it then must be explained in what sense one may take $x = 2$ in this formula.

Definition 22.7: A field F is said to be *algebraically closed* if every non-constant polynomial has a root, hence a polynomial $P \in F[x]$ of degree $n \geq 1$ can be written as $a_n\,(x-\alpha_1) \cdots (x-\alpha_n)$ for some $\alpha_1, \ldots, \alpha_n \in F$.

Remark 22.8: It will be shown that $\mathbb{C}$ is algebraically closed, but $\mathbb{R}$ is obviously not since $x^2 + 1$ has no root. $P = (x^2+1)\,(x^2+2)$ has no roots, but it can be "reduced", because $P = P_1 P_2$ with $P_1 = x^2 + 1$ and $P_2 = x^2 + 2$, so that one will need a notion of irreducibility for polynomials in $R[x]$, but the definitions will actually be given for general rings. Irreducible polynomials of degree ≥ 2 in $\mathbb{R}[x]$ must have degree 2, and $x^2 + A\,x + B$ is irreducible if and only if $A^2 < 4B$, but the situation is different for $\mathbb{Q}[x]$ and for every $m \geq 2$ there is an irreducible polynomial in $\mathbb{Q}[x]$ of degree m.

---

[3] Joseph RAPHSON, English mathematician, c. 1648–1715. The Newton–Raphson method is partly named after him: he published it in 1690, and it is simpler than the method that NEWTON wrote in 1671, but which was only published in 1736.

[4] For example, if $|f'(x)| \geq \frac{1}{2}\,|f'(x_0)|$ and $|f''(x)| \leq M$ on $I = [x_0 - a, x_0 + a]$, one deduces that $|x_{n+1} - x_n| \leq \frac{2|f(x_n)|}{|f'(x_0)|}$ and $|f(x_{n+1})| \leq \frac{M\,|x_{n+1} - x_n|^2}{2} \leq \frac{2M\,|f(x_n)|^2}{|f'(x_0)|^2}$ as long as the points stay in I; if $2M\,|f(x_0)| \leq \theta\,|f'(x_0)|^2$ with $\theta < 1$, then $|f(x_n)| \leq \theta^{2^n - 1} |f(x_0)|$ as long as the points stay in I, which is the case if $2|f(x_0)| \leq (1-\theta)\,a\,|f'(x_0)|$.

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

23- Monday October 24, 2011.

Theorem 23.1: (fundamental theorem of algebra) $\mathbb{C}$ is algebraically closed.
Proof: This proof is attributed to GAUSS, and it uses analysis. If $P \in \mathbb{C}[x]$ is not constant, then $|P(z)| \to +\infty$ as $|z| \to +\infty$, so that there exists $z_0 \in \mathbb{C}$ where $|P|$ attains its minimum; if one had $P(z_0) \neq 0$, then one would use the Taylor expansion of P at z_0, which implies $P(z) = P(z_0) + a\,(z - z_0)^m Q(z - z_0)$, with $a \neq 0$, $m \geq 1$ and $Q(0) = 1$, one would choose ξ such that $a\,\xi^m = -P(z_0)$, and observing that $P(z_0 + \varepsilon\,\xi) = P(z_0)(1 - \varepsilon^m) + o(|\varepsilon^{m+1}|)$, one would have $|P(z_0 + \varepsilon\,\xi)| < |P(z_0)|$ for $\varepsilon > 0$ small.

Remark 23.2: That analysis is used in a proof which seems to be pure algebra is actually quite natural, since although $\mathbb{C}$ is constructed from $\mathbb{R}$ by algebra, the definition of $\mathbb{R}$ involves analysis. The basic property is that if $P \in \mathbb{R}[x]$ and $deg(P)$ is odd, then P has at least one root $\alpha \in \mathbb{R}$, by an argument of connectedness: for $|x|$ very large, P looks like an odd power, so that one can find $y, z \in \mathbb{R}$ with $P(y) < 0 < P(z)$, and then, since P is a continuous function, it must have a root between y and z.

In France, Theorem 23.1 is attributed to D'ALEMBERT,[1] but it seems unlikely that he had a proof, so that he may have conjectured it. There is a proof by LAPLACE which continues the case of an odd degree by considering $n = 2^k m$ for m odd,[2] by induction on k, but his proof was not accepted as valid at the time, because it assumes that the roots exist somewhere, and the method of construction of a splitting field extension was not so clear before GALOIS.

There is a proof by ARTIN which is also pure algebra after the first step of considering odd degree for $\mathbb{R}[x]$, but it uses Galois theory, for considering the Galois group of a splitting field extension, the Galois correspondence between subgroups of the Galois group and intermediate fields, and Sylow's theorem for the Galois group.

Definition 23.3: Let R be a commutative unital ring. An element $c \in R$ is called *irreducible* if $c \neq 0$, c is not a unit, and $c = a\,b$ implies that either a or b is a unit (i.e. either a or b is associate to c); if c is not irreducible, it is then called *reducible*.

An element $q \in R$ is called a *prime* if $q \neq 0$, q is not a unit, and q divides $a\,b$ implies that either q divides a or q divides b.

Remark 23.4: If R is an integral domain, then $deg(P_1 P_2) = deg(P_1) + deg(P_2)$ for all non-zero $P_1, P_2 \in R[x]$, so that $R[x]$ is an integral domain and the units of $R[x]$ are the constants which are units in R. $P = 2x$ is irreducible in $\mathbb{Q}[x]$, but it is reducible in $\mathbb{Z}[x]$ because 2 is not a unit in $\mathbb{Z}$.

If F is a field, all polynomials $P \in F[x]$ of degree 1 are irreducible, and a non-zero polynomial $P \in F[x]$ of degree $n \geq 2$ is irreducible if and only if it cannot be written as $P = P_1 P_2$ with both P_1 and P_2 having degree ≥ 1. If $P \in F[x]$ is a polynomial of degree 2 or 3, it is irreducible if and only if it has no root, since by writing $P = P_1 P_2$ with both P_1 and P_2 having degree ≥ 1, either P_1 or P_2 has degree 1, hence has a root, which is a root of P.

A field F is algebraically closed if and only if the irreducible polynomials in $F[x]$ are the polynomials of degree 1.

Lemma 23.5: If $P \in \mathbb{R}[x]$, and if $a \in \mathbb{C}$ is a root of P (considered as an element of $\mathbb{C}[x]$), then $\overline{a}$ is a root of P, having the same multiplicity than a. Every $P \in \mathbb{R}[x]$ of degree $n \geq 1$ can then be written as $c \prod_{i=1}^{m} (x - r_i) \prod_{j=1}^{k} (x - z_j)\,(x - \overline{z_j})$ for elements $r_1, \ldots, r_m \in \mathbb{R}$, $z_1, \ldots, z_k \in \mathbb{C} \setminus \mathbb{R}$, and $m + 2k = n$, and $(x - z_j)\,(x - \overline{z_j}) = x^2 - 2\Re(z_j)\,x + |z_j|^2 \in \mathbb{R}[x]$ can be any polynomial $x^2 + a_j x + b_j$ with $a_j^2 < 4 b_j$. An irreducible polynomial $P \in \mathbb{R}[x]$ either has degree 1, with $P = a_0 + a_1 x$ with $a_1 \neq 0$, or has degree 2, with $P = a_0 + a_1 x + a_2 x^2$ with $a_2 \neq 0$ and $a_1^2 < 4 a_0 a_2$.
Proof: For $P \in \mathbb{R}[x]$, one has $\overline{P(a)} = P(\overline{a})$ for all $a \in \mathbb{C}$, and the same property holds for the successive derivatives of P, so that if a is a root of P of multiplicity k, the derivatives of P up to order $k - 1$ at a

[1] Jean LE ROND, known as D'ALEMBERT, French mathematician, 1717–1783. He worked in Paris, France.
[2] Pierre-Simon LAPLACE, French mathematician, 1749–1827. He was made comte in 1806 by Napoléon I and marquis in 1817 by Louis XVIII. He worked in Paris, France.

are 0 but not the kth derivative, so that the same is true at $\overline{a}$, hence $\overline{a}$ is also a root of multiplicity k. If $a \in \mathbb{C} \setminus \mathbb{R}$, then $\overline{a} \neq a$, so that putting the two factors $(x-a)^k$ and $(x-\overline{a})^k$ together gives $\left((x-a)\,(x-\overline{a})\right)^k$, and $(x-a)\,(x-\overline{a})$ is irreducible in $\mathbb{R}[x]$ but not in $\mathbb{C}[x]$. There are then irreducible polynomials of degree 2, which are those whose complex roots are not real (i.e. those with discriminant < 0).

Remark 23.6: If $P(x) \geq 0$ for all $x \in \mathbb{R}$, then each real root has an even multiplicity, so that $c \prod_{i=1}^{m}(x-r_i) = Q^2$ for some $Q \in \mathbb{R}[x]$, and if $\prod_{j=1}^{k}(x-z_j) = R + i\,S$ for $R, S \in \mathbb{R}[x]$, then $\prod_{j=1}^{k}(x-z_j)\,(x-\overline{z_j}) = (R+i\,S)\,(\overline{R+i\,S}) = R^2+S^2$, so that $P = (Q\,R)^2 + (Q\,S)^2$ is a sum of two squares of polynomials.

If $P \in \mathbb{R}[x_1, x_2]$ has degree 4 and satisfies $P(x_1, x_2) \geq 0$ for all $x_1, x_2 \in \mathbb{R}$, HILBERT proved in 1888 that P is the sum of three squares of polynomials, but that for degree ≥ 6 there are non-negative polynomials which are not sums of squares of polynomials, and the same negative result holds for degree 4 in three real variables.[3] HILBERT did not exhibit counter-examples, and the simplest ones were shown by MOTZKIN in the 1960s,[4] using the arithmetic-geometric inequality:[5] $x_1^2x_2^2 + x_2^2x_3^2 + x_3^2x_1^2 + 1 \pm 4x_1x_2x_3 \geq 0$ in $\mathbb{R}^3$, and $x_1^4x_2^2 + x_1^2x_2^4 + 1 - 3x_1^2x_2^2 \geq 0$ in $\mathbb{R}^2$, but these polynomials cannot be written as sums of squares of polynomials.[6]

E. ARTIN showed that any non-negative polynomial in ℓ real variables can be written as a sum of squares of rational fractions.

Definition 23.7: For a polynomial $P = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}[x]$, one defines the *content* $C(P)$ of P as the *gcd* of $a_0, \ldots, a_n$; one calls a polynomial $P \in \mathbb{Z}[x]$ *primitive* if $C(P) = 1$ (so that one always has $P = C(P)P_0$ with P_0 primitive).

Lemma 23.8: (Gauss's lemma)[7] One has $C(P\,Q) = C(P)C(Q)$ for all $P, Q \in \mathbb{Z}[x]$; equivalently, the product of primitive polynomials in $\mathbb{Z}[x]$ is primitive.
Proof: Let $P_0 = a_0 + \ldots \in \mathbb{Z}[x]$ and $Q_0 = b_0 + \ldots \in \mathbb{Z}[x]$ be primitive, but assume that $P_0Q_0 = c_0 + \ldots$ is not primitive, so that there exists a prime p which divides all c_k. Since p does not divide all a_i, there exists $i_0 \geq 0$ such that $p \mid a_i$ for $i < i_0$ but p does not divide a_{i_0} (which is then $\neq 0$), and since p does not divide all b_j, there exists $j_0 \geq 0$ such that $p \mid b_j$ for $j < j_0$ but p does not divide b_{j_0} (which is then $\neq 0$); however, this leads to a contradiction, since $c_{i_0+j_0} - a_{i_0}b_{j_0} = \sum_{i<i_0} a_ib_{i_0+j_0-i} + \sum_{j<j_0} a_{i_0+j_0-j}b_j$, which is a multiple of p, and since p divides $c_{i_0+j_0}$ it must divide $a_{i_0}b_{j_0}$.[8]

Lemma 23.9: If $P \in \mathbb{Z}[x]$ is primitive of degree ≥ 1 then it is irreducible in $\mathbb{Z}[x]$ if and only if it is irreducible in $\mathbb{Q}[x]$.
Proof: Notice that the result is not true if $C(P) > 1$: for example, $2 + 2x$ is reducible in $\mathbb{Z}[x]$ because 2 and $1 + x$ are not units in $\mathbb{Z}[x]$. Since one assumes $C(P) = 1$, if P is reducible in $\mathbb{Z}[x]$ then $P = P_1P_2$ with $P_1, P_2 \in \mathbb{Z}[x]$ and neither P_1 nor P_2 being a constant different from ± 1, so that the degrees of P_1, P_2 are

[3] For a non-negative polynomial of degree 2 in ℓ real variables, Gauss's decomposition of quadratic forms shows it is a sum of at most ℓ squares of affine functions plus a non-negative constant.

[4] Theodore Samuel MOTZKIN, German-born mathematician, 1908–1970.

[5] For $a_1, \ldots, a_m > 0$, one has $\sqrt[m]{a_1 \cdots a_m} \leq \frac{a_1+\ldots+a_m}{m}$, which after writing $a_j = e^{b_j}$ is just the convexity of the exponential function.

[6] If $x_1^2x_2^2 + x_2^2x_3^2 + x_3^2x_1^2 + 1 \pm 4x_1x_2x_3 = \sum_j Q_j^2$, each Q_j must have degree ≤ 1 in each variable and total degree ≤ 2, and the Q_j cannot have terms in x_1, x_2, x_3 since it would create terms in x_1^2, x_2^2, x_3^2 with positive coefficients, but it implies that there is no term in $x_1x_2x_3$ in Q_j^2. If $x_1^4x_2^2 + x_1^2x_2^4 + 1 - 3x_1^2x_2^2 = \sum_j Q_j^2$, each Q_j must have degree ≤ 2 in each variable and total degree ≤ 3, and the Q_j cannot have terms in x_1^2, x_2^2 since it would create terms in x_1^4, x_2^4 with positive coefficients, but then the Q_j could not have terms in x_1, x_2 either, since it would create terms in x_1^2, x_2^2 with positive coefficients, hence the term in $x_1^2x_2^2$ in Q_j^2 has a coefficient which is ≥ 0.

[7] Since GAUSS was a mathematical genius, he proved many results, and a few different ones are known as Gauss's lemma.

[8] Said otherwise, the projection π from $\mathbb{Z}$ onto $\mathbb{Z}_p$ induces a ring-homomorphism from $\mathbb{Z}[x]$ into $\mathbb{Z}_p[x]$, and the images $\pi(P_0), \pi(Q_0) \in \mathbb{Z}_p[x]$ of $P_0, Q_0 \in \mathbb{Z}[x]$ are assumed to satisfy $\pi(P_0\,Q_0) = 0$, but since it means $\pi(P_0)\,\pi(Q_0) = 0$ and $\mathbb{Z}_p[x]$ is an integral domain, either $\pi(P_0) = 0$ or $\pi(Q_0) = 0$, i.e. all the coefficients of P_0 or all the coefficients of Q_0 are multiple of p.

≥ 1, and P is reducible in $\mathbb{Q}[x]$. Conversely, if $P = P_1P_2$ in $\mathbb{Q}[x]$, then there exist positive integers m_1, m_2 such that $P_1 = \frac{Q_1}{m_1}$ and $P_2 = \frac{Q_2}{m_2}$ with $Q_1, Q_2 \in \mathbb{Z}[x]$, and then by Gauss's lemma one has $C(Q_1)C(Q_2) = C(Q_1Q_2) = C(m_1m_2P) = m_1m_2$, and $P = \frac{Q_1Q_2}{m_1m_2} = \frac{Q_1}{C(Q_1)}\,\frac{Q_2}{C(Q_2)}$ is the product of two polynomials in $\mathbb{Z}[x]$.

Lemma 23.10: (Eisenstein's criterion) If $P = a_0 + a_1x + \ldots + a_nx^n \in \mathbb{Z}[x]$ and a prime p divides $a_0, \ldots, a_{n-1}$ but not a_n, and p^2 does not divide a_0, then P is irreducible in $\mathbb{Q}[x]$ (and if $C(P) = 1$ it is irreducible in $\mathbb{Z}[x]$).

Proof: One notices that p does not divide $C(P)$, since p does not divide a_n, and by dividing P by $C(P)$, one may then assume that P is primitive. If $P = Q_1Q_2$ with $Q_1, Q_2 \in \mathbb{Q}[x]$, one may assume that $Q_1, Q_2 \in \mathbb{Z}[x]$ by Lemma 23.9. One has $Q_1 = b_0 + \ldots + b_{m_1}x^{m_1}$ and $Q_2 = c_0 + \ldots + c_{m_2}x^{m_2}$ with $m_1, m_2 < n$, and then because $p \mid a_0 = b_0c_0$ one has either $p \mid b_0$ or $p \mid c_0$, but not both because p^2 does not divide a_0, so that one may assume that $p \mid b_0$ but p does not divide c_0; then, $p \mid a_1 = b_0c_1 + b_1c_0$ implies $p \mid b_1c_0$, hence $p \mid b_1$, and then $p \mid a_2 = b_0c_2 + b_1c_1 + b_2c_0$ implies $p \mid b_2$, and by induction one finds that p divides all b_i (because $m_1 < n$), which is a contradiction since it implies that p divides all a_k.[9]

Remark 23.11: One may generalize Gauss's lemma and Eisenstein's criterion to the case where $\mathbb{Z}$ is replaced by a UFD (unique factorization domain) D, and $\mathbb{Q}$ is replaced by F, the field of fractions of D.

By Eisenstein's criterion, there are irreducible polynomials in $\mathbb{Q}[x]$ of any degree.

It can be shown that for every prime p and every $m \geq 2$ there exists an irreducible polynomial in $\mathbb{Z}_p[x]$ of degree m, but it is not so elementary: writing $F_0 = \mathbb{Z}_p$, and denoting $q = p^m$, one first invokes the construction of a splitting field extension F for the polynomial $Q = x^q - x$ over F_0; then, since F is an F_0-vector space, it has characteristic p, and from $(a+b)^p = a^p + b^p$ for all $a, b \in F$, one deduces that $(a+b)^q = a^q + b^q$ for all $a, b \in F$, and this permits to show that the roots of Q form a field, which is F, and since these roots are distinct because $Q' = -1$ (hence a multiple root cannot exist), F has q elements, i.e. F is an F_0-vector space of dimension m; then, to each non-zero $a \in F$ is attached an irreducible polynomial P_a of degree $\leq m$ such that $P_a(a) = 0$ (and P_a divides Q), and for being sure that one P_a has degree m, one observes that the (Abelian) multiplicative group $F^* = F \setminus \{0\}$ is cyclic (or order $q-1$) and any of its generators (and there are $\varphi(q-1)$ of them) is such an a.

[9] Said otherwise, Q_1 and Q_2 define polynomials $\pi(Q_1), \pi(Q_2) \in \mathbb{Z}_p[x]$ and $\pi(Q_1)\,\pi(Q_2) = c\,x^n$ in $\mathbb{Z}_p[x]$ with $0 \neq c \in \mathbb{Z}_p$, so that one must have $\pi(Q_1) = a\,x^{m_1}$ and $\pi(Q_2) = b\,x^{m_2}$ with $a\,b = c$ and $m_1 + m_2 = n$ (since $\mathbb{Z}_p[x]$ is a PID, hence a UFD). Then, Q_1 has all its coefficients up to degree $m_1 - 1$ which are multiple of p, and Q_2 has all its coefficients up to degree $m_2 - 1$ which are multiple of p, hence P has all its coefficients up to degree $\min\{m_1, m_2\} - 1$ which are multiple of p^2.

25- Wednesday November 2, 2011.

Definition 25.1: The ring $R((x))$ of *formal Laurent series* with coefficients in R is the set of elements of R indexed by $\mathbb{Z}$, i.e. $\{a_n \mid n \in \mathbb{Z}\}$, such that $a_n = 0$ for all $n \leq m$ for some $m \in \mathbb{Z}$, and it is interpreted as $\sum_{n\in\mathbb{Z}} a_n x^n$.

For $A = \sum_{n\in\mathbb{Z}} a_n x^n \in R((x))$ and $B = \sum_{n\in\mathbb{Z}} b_n x^n \in R((x))$, one has $A + B = C = \sum_{n\in\mathbb{Z}} c_n x^n$ and $A\,B = D = \sum_{n\in\mathbb{Z}} d_n x^n$, with $c_n = a_n + b_n$ for all $n \in \mathbb{Z}$, and $d_n = \sum_{j\in\mathbb{Z}} a_j b_{n-j}$ for all $n \in \mathbb{Z}$, noticing that the sum defining each d_n only has a finite number of non-zero terms.

The valuation of a non-zero element is the largest $m \in \mathbb{Z}$ such that $a_n = 0$ for all $n < m$.

Remark 25.2: If F is a field, then $F[[x]]$ is an integral domain, and its field of fractions is isomorphic to $F((x))$: indeed, a non-zero element in $R[[x]]$ has the form $a_m x^m(1 + B)$ with $a_m \neq 0$ and $val(B) \geq 1$, and for defining its inverse one needs to notice that $a_m^{-1} \in F$, $x^{-m} \in F((x))$, and the inverse of $1 - B \in F[[x]]$ is $1 + B + B^2 + \ldots \in F[[x]] \subset F((x))$. Conversely, any non-zero element $A \in F((x))$ with $val(A) < 0$ may be written as $\frac{x^m A}{x^m}$ with $m = -val(A)$ and one has $x^m A \in F[[x]]$.

Remark 25.3: The motivation for the ring of formal power series $R[[x]]$ and the ring of formal Laurent series $R((x))$ is to mimic at an algebraic level something done in analysis concerning Taylor expansions of differentiable functions in an open set of $\mathbb{R}$ or of $\mathbb{C}$. Although every function f which is indefinitely differentiable around a point x_0 can be well approached in a small ball $B(x_0, r)$ by the Taylor expansion of f at order n with an error in r^{n+1}, the Taylor series might diverge at any other point than x_0; if the Taylor expansion converges at other points it defines an *analytic function* in the case of $\mathbb{R}$, called an *holomorphic function* in the case of $\mathbb{C}$, and the radius of convergence of the power series is limited by the nearest singularity in the complex plane: for example, the Taylor expansion of $f(x) = \frac{1}{1+x^2}$ (which is analytic on the whole $\mathbb{R}$) at $x_0 \in \mathbb{R}$ has a radius of convergence $\sqrt{1 + x_0^2}$, which is the distance to the two singularities of f in $\mathbb{C}$, which are $\pm i$.

If f is holomorphic in a disc minus its center z_0, it might be that z_0 is a *removable singularity*, i.e. one can extend f by continuity at z_0; it might be that z_0 is a *pole*, i.e. the function tends to ∞ when one approaches z_0,[1] and in this case each pole has a finite order $m \geq 1$ so that $(z - z_0)^m f$ is continuous and non-zero at z_0, and it is at such poles that one uses a "Laurent" series (introduced before LAURENT by WEIERSTRASS); it might be that z_0 is an *essential singularity*, i.e. the function has no limit when one approaches z_0, and in this case the set of values taken by f in any small pointed disc around z_0 is dense in $\mathbb{C}$, as was proved by CASORATI and then WEIERSTRASS, a result then improved by PICARD,[2] who proved that f takes all values of $\mathbb{C}$ except possibly one in any small pointed disc around z_0.[3]

Definition 25.4: In a ring R, an ideal P is called *prime* if $P \neq R$ and if for any two ideals A, B of R satisfying $A\,B \subset P$ one has $A \subset P$ or $B \subset P$ (recall that $A\,B$ is the set of finite sums of terms like $a\,b$ with $a \in A$ and $b \in B$).

An ideal M is called *maximal* if it is a proper ideal (i.e. $M \neq R$) and it is maximal (for inclusion) among proper ideals (i.e. $M \subset N$ and N is a proper ideal, then $N = M$).

Remark 25.5: A prime element was defined at Definition 23.3 for a commutative unital ring R, by $q \neq 0$, q not a unit, and q divides $a\,b$ implies that either q divides a or q divides b. Since the definition mentions units, the ring has to be unital, but one could avoid this hypothesis by asking that $(q) \neq R$, which makes sense in a general ring, and for a commutative unital ring it is equivalent to q not being a unit, since $(q) = \{r\,q \mid r \in R\}$ in this case.

Lemma 25.6: In a commutative unital ring R, a non-zero element $q \in R$ is prime if and only if the ideal (q) which it generates is a prime ideal.

---

[1] One works with $\mathbb{C}\,P^1$, the projective 1-dimensional space, which adds to $\mathbb{C}$ only one point at infinity.

[2] Charles Émile PICARD, French mathematician, 1856–1941. He worked in Toulouse and in Paris, France.

[3] For example, $f(z) = e^{1/z}$ has an essential singularity at 0, and it avoids the value 0.

Proof: Suppose (q) is a prime ideal, and q divides $a\,b$, so that $a\,b \in (q)$, but in a commutative unital ring one has $(a)\,(b) = (a\,b)$, so that $(a)\,(b) \subset (q)$, hence either $(a) \subset (q)$ or $(b) \subset (q)$, but $(x) \subset (q)$ implies $x \in (q)$, i.e. q divides x.

Suppose q is prime, and two ideals A, B are such that $A\,B \subset (q)$: if one does not have $A \subset (q)$, there exists $a \in A \setminus (q)$ and since for every $b \in B$ one has $a\,b \in A\,B \subset (q)$ and q does not divide a, q must then divide b, so that $b \in (q)$, hence $B \subset (q)$.

Lemma 25.7: In a commutative unital ring R, an ideal P is prime if and only if for all $a, b \in R$, $a\,b \in P$ implies $a \in P$ or $b \in P$; in particular, the trivial ideal $\{0\}$ is prime if and only if R is an integral domain.
Proof: If P is prime and $a\,b \in P$ then $(a)(b) = (a\,b) \subset P$, so that $(a) \subset P$ or $(b) \subset P$, i.e. $a \in P$ or $b \in P$. Conversely, if A and B are ideals such that $A\,B \subset P$ but $A \not\subset P$, then there exists $a \in A \setminus P$ and for all $b \in B$ one has $a\,b \in P$, so that $b \in P$, hence $B \subset P$.

In particular, $\{0\}$ is a prime ideal if and only if there is no zero-divisor, and since R is a commutative unital ring, it means that it is an integral domain.

Lemma 25.8: If R is a commutative unital ring, and J is a proper ideal of R (i.e. $J \neq R$), then the quotient R/J is an integral domain if and only if J is prime.
Proof: Since R/J is a commutative unital ring, it is an integral domain if and only if it has no zero-divisor, but a zero-divisor is $a\,J$ with $a \notin J$ for which there exists $b\,J$ with $b \notin J$ such that $a\,b \in J$, i.e. J is not prime.

Remark 25.9: Since the initial reason for a general definition of primes was to extend the notion of primes in $\mathbb{Z}$ (actually in $\mathbb{N}$) to a general ring, it is useful to observe that, when applied to $\mathbb{Z}$, the general definition gives either a prime p or $-p$.[4]

The general definition of irreducible elements applied to $\mathbb{Z}$ also gives $\pm p$ for a prime p, but the initial difficulty was to observe that there are rings where unique factorization does not hold, and that a definition of irreducible elements is needed.

As mentioned at the end of lecture 21, $(4+\sqrt{10})\,(4-\sqrt{10}) = 6 = 2\cdot 3$ in $\mathbb{Z}[\sqrt{10}]$, and $4+\sqrt{10}, 4-\sqrt{10}, 2, 3$ are irreducible. Since multiples of 2 have the form $a + b\sqrt{10}$ with a, b even, neither $4+\sqrt{10}$ nor $4-\sqrt{10}$ are multiples of 2, hence 2 is not prime in $\mathbb{Z}[\sqrt{10}]$; similarly, 3 is not prime in $\mathbb{Z}[\sqrt{10}]$, since neither $4+\sqrt{10}$ nor $4-\sqrt{10}$ are multiples of 3, which have the form $a+b\sqrt{10}$ with a, b multiple of 3. $4+\sqrt{10}$ and $4-\sqrt{10}$ are not prime either since they divide neither 2 nor 3, and it is checked more easily by noticing that $N(4\pm\sqrt{10}) = 6$ while $N(2) = 4$ and $N(3) = 9$, which are not multiples of 6, where $N(a+b\sqrt{10}) = a^2 - 10b^2$, which satisfies $N(z_1 z_2) = N(z_1)\,N(z_2)$ for all $z_1, z_2 \in \mathbb{Z}[\sqrt{10}]$.

Lemma 25.10: If R is a commutative unital ring, and J is a proper ideal of R (i.e. $J \neq R$), then the quotient R/J is a field if and only if J is maximal.
Proof: If J is maximal and $a \notin J$, then the ideal generated by $\{a\} \cup J$ is R (since it contains J strictly and J is maximal), so that 1 can be expressed as $r_0 a + j$ with $j \in J$ for some $r_0 \in R$ (but $r_0 \notin J$ since $J \neq R$), and this shows that the inverse of $a + J$ in the quotient is $r_0 + J$, so that every non-zero element of R/J has an inverse, hence R/J is a field. Conversely, if R/J is a field and $a \notin J$, then $a + J$ has an inverse $b + J$ in the quotient, so that $a\,b \in 1 + J$, hence the ideal generated by a and J contains 1, so that it is R, which shows that there cannot be a proper ideal containing J strictly (since it would contain some $a \notin J$), i.e. J is maximal.

Remark 25.11: If R is a commutative unital ring, every maximal (proper) ideal is prime, since every field is an integral domain, and the converse is obviously not true: for example if $D \in \mathbb{Z}$ is not a square, then $\mathbb{Z}[\sqrt{D}]$ is an integral domain, but not a field since $z = a + b\sqrt{D}$ is a unit if and only if $N(z) = \pm 1$, with $N(a + b\sqrt{D}) = a^2 - D\,b^2$, so that since $\mathbb{Z}[\sqrt{D}] = \mathbb{Z}[x]/(x^2 - D)$, one finds that $(x^2 - D)$ is a prime ideal but not a maximal ideal of $\mathbb{Z}[x]$.

Of course, each proper ideal J is contained in a maximal ideal M by Zorn's lemma, and the hypothesis of Zorn's lemma consists in checking that if $J_i, i \in I$, is a totally ordered family of proper ideals (indexed by a nonempty set I) then it has a least upper bound (in the ordered set of proper ideals), which is simply $\bigcup_{i\in I} J_i$: the fact that it is an additive subgroup of R relies on the fact that if $i_1 \neq i_2$ one of the two ideals

[4] General definitions cannot actually differentiate between the various associates of an element.

J_{i_1} and J_{i_2} is included in the other, and the union is a proper ideal, since if it contained 1, then 1 would belong to one J_i, which then would not be proper.

In a field F the only ideals are $\{0\}$ and F, and $\{0\}$ is both prime and maximal.

Remark 25.12: If R is an integral domain, every prime element is irreducible: if $p = a\,b$ then $p \mid a$ or $p \mid b$, and if $p \mid a$, one has $a = p\,x$, so that $p = a\,b = p\,x\,b$, i.e. $1 = x\,b$, so that b is a unit.

The converse is not true, since one has seen a few irreducible elements of $\mathbb{Z}[\sqrt{10}]$ which are irreducible but not prime, and for $D \in \mathbb{Z}$ not a square $\mathbb{Z}[\sqrt{D}]$ is an integral domain.

The next step will be to compare irreducible elements and prime elements, and define what a UFD (unique factorization domain) is.

Luc TARTAR, University Professor of Mathematics, Wean Hall 6212, tartar@cmu.edu

26- Friday November 4, 2011.

Lemma 26.1: If R is an integral domain, then $c \neq 0$ is irreducible if and only if (c) is maximal in the set of all proper principal ideals, i.e. $(c) \subset (d)$ implies $(d) = (c)$ or $(d) = R$.

If R is a PID, every irreducible element is prime (recall that in an integral domain every prime element is irreducible).
Proof: If c is irreducible and $(c) \subset (d)$, it means that $c = d\,x$ for some $x \in R$, which implies that either d is a unit, in which case $(d) = R$, or x is a unit, in which case $d = x^{-1}c$ and $(d) \subset (c)$, so that $(d) = (c)$. Conversely, if (c) is maximal in the set of proper principal ideals and $c = a\,b$, then one deduces that $(c) \subset (a)$, so that either $(a) = R$, in which case a is a unit, or $(a) = (c)$, which implies $a = c\,x$, so that $c = a\,b = c\,x\,b$, i.e. $1 = x\,b$ (since R is an integral domain and $c \neq 0$), so that b is a unit.

In a PID, prime is then equivalent to irreducible, because maximality among proper principal ideals is the same as maximality among proper ideals, since all ideals are principal, so that if c is irreducible then (c) is a maximal proper ideal, hence a prime ideal, showing that c is prime.

Definition 26.2: A ring R is called a *UFD*, which stands for *unique factorization domain*, if it is an integral domain such that every $r \neq 0$ which is not a unit has a factorization $r = a_1 \cdots a_m$, where $a_1, \ldots, a_m$ are irreducible, and the factorization is unique in the sense that if $r = b_1 \cdots b_n$, where $b_1, \ldots, b_n$ are irreducible, then $m = n$ and there exists a permutation σ such that for $i = 1, \ldots, n$ one has $b_i = a_{\sigma(i)} u_i$ where u_i is a unit (i.e. b_i is an associate of $a_{\sigma(i)}$).

Lemma 26.3: Every PID is a UFD.
Proof: Assume that R is a PID, so that R is Noetherian.[1] Let $r \neq 0$, which is not a unit. If r is reducible, write $r = r_1 r_2$, where neither r_1 nor r_2 are units; if one of them, say r_1, is reducible, write $r_1 = r_{1,1} r_{1,2}$, where neither $r_{1,1}$ nor $r_{1,2}$ are units; if the process was not terminating, there would exist an infinite ascending sequence of ideals $(r) \subset (r_1) \subset (r_{1,1}) \subset \ldots$, where all inclusions are proper, contradicting the fact that R is Noetherian.

For showing the uniqueness, one proceeds by induction of the minimum number n of irreducible factors. If $n = 0$, then r is a unit, and $r = q\,c$ with q irreducible would give a contradiction, since it implies that q is a unit. If $n \geq 1$ and $r = p_1 \cdots p_n = q_1 \cdots q_m$ with $m \geq n$, then p_1 is prime (since in a PID irreducible elements are prime), and it divides $q_1 \cdots q_m$, so that it must divide a factor, say q_1: one then has $q_1 = p_1 u$ for a unit u, and then $p_2 \cdots p_n = (u\,q_2) \cdots q_m$, and one uses the induction hypothesis.

Lemma 26.4: In a UFD every irreducible element is prime.
Proof: If p is irreducible and $p \mid a\,b$ for some $a, b \in R$, then $a\,b = p\,c$ for some $c \in R$, and writing a, b, and c as products of irreducible elements, p must be associate to one of the irreducible elements occurring in the factorizations of a or b, so that p divides a or b.

Remark 26.5: Bézout's theorem,[2] is that the gcd of polynomials $P_1, \ldots, P_m \in F[x]$ for a field F can be written as $\sum_i Q_i P_i$ for some polynomials $Q_1, \ldots, Q_m \in F[x]$, and the proof is the same than for Bachet's theorem for the gcd in $\mathbb{Z}$: the ideal in $F[x]$ generated by $P_1, \ldots, P_m$ is principal, since $F[x]$ is a PID, i.e. made of the multiple of a polynomial D, which one may choose to be monic (and restrict to the case where the coefficient of highest order is $+1$), and D is obviously the gcd of $P_1, \ldots, P_m$.

If R is a UFD one can find a gcd for any finite number of elements $r_1, \ldots, r_m \in R$, but one has only the multiplicative approach: in the factorizations of $r_1, \ldots, r_m$, one avoids repeating associates by writing the list $s_1, \ldots, s_n$ of irreducible elements appearing in the factorizations, with s_i not being an associate of s_j for

[1] One may use the initial Definition 19.7, that an ascending chain of ideals becomes constant: it means $(a_1) \subset (a_2) \subset \ldots \subset (a_n) \subset \ldots$ and the union is an ideal, equal to (b), and b must belong to some (a_{n_0}), so that $(a_n) = (a_{n_0})$ for $n \geq n_0$. It is quicker to use Lemma 19.8, that a ring is Noetherian if and only if each of its ideals is finitely generated.

[2] Étienne BÉZOUT, French mathematician, 1730–1783. He worked in Paris, France. Bézout's theorem is named after him.

$i \neq j$, and then each r_i has a factorization $r_i = u_i s_1^{k_1(i)} \cdots s_n^{k_n(i)}$ with $k_\ell(i) \geq 0$ for $\ell = 1, \ldots, n$, and u_i is a unit; a gcd is then $s_1^{\kappa_1} \cdots s_n^{\kappa_n}$, with $\kappa_\ell = \min_i k_\ell(i)$ for $\ell = 1, \ldots, n$, and it is defined up to an associate.

Remark 26.6: It will be shown in another lecture that if R is a UFD then $R[x]$ is also a UFD (and if $R[x]$ a UFD then R is a UFD), and that if R is Noetherian then $R[x]$ is also Noetherian (and if $R[x]$ is Noetherian then R is Noetherian). If R is a PID, then it is not always true that $R[x]$ is a PID: for example, if F is a field, $F[x]$ is a PID, but $F[x_1, x_2]$ is not a PID (and $F[x_1, x_2]$ is isomorphic to $R[x_2]$ with $R = F[x_1]$). However, by induction on n, $F[x_1, \ldots, x_n]$ is both a UFD and Noetherian.

Remark 26.7: We have now seen two ways to construct fields, the first one is to start from an integral domain and to consider its field of fractions, and the second one is to start from a field F, and to consider the quotient of the ring of polynomial $F[x]$ by the ideal generated by an irreducible polynomial $P \in F[x]$, and this ideal is maximal because $F[x]$ is a PID.[3]

Since $x^2 - 2$ is irreducible in $\mathbb{Q}[x]$ (but not in $\mathbb{R}[x]$), the quotient $\mathbb{Q}[x]/(x^2 - 2)$ is a field, denoted $\mathbb{Q}[\sqrt{2}]$. In each coset one considers the element of the form $a + b\,x$ with $a, b \in \mathbb{Q}$, and for finding to which coset a polynomial $P \in \mathbb{Q}[x]$ belongs, one divides P by $x^2 - 2$ and one takes the remainder. Since $x^2 = 2 \pmod{x^2 - 2}$, one may then consider that $x = \sqrt{2}$, and one then writes $\mathbb{Q}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Q}\}$, but one could as well consider that $x = -\sqrt{2}$, because at an algebraic level there is no reason to make any difference between the two cases. If one considers that $x = \sqrt{2}$, it is important to use the *conjugation*, which sends $z = a + b\sqrt{2}$ to $\overline{z} = a - b\sqrt{2}$, and conjugation is an automorphism of $\mathbb{Q}[\sqrt{2}]$: indeed, $\overline{z_1 + z_2} = \overline{z_1} + \overline{z_2}$ and $\overline{z_1 z_2} = \overline{z_1}\,\overline{z_2}$ for all $z_1, z_2 \in \mathbb{Q}[\sqrt{2}]$, which show that conjugation is a ring-homomorphism, and it is injective because $\overline{1} = 1$,[4] and surjective because $\overline{\overline{z}} = z$ for all $z \in \mathbb{Q}[\sqrt{2}]$. For $z = a + b\sqrt{2} \neq 0$, the multiplicative inverse if $\frac{\overline{z}}{N(z)}$ with $N(z) = z\,\overline{z} = a^2 - 2b^2 \in \mathbb{Q}^*$, which satisfies $N(z_1 z_2) = N(z_1)\,N(z_2)$ for all $z_1, z_2 \in \mathbb{Q}[\sqrt{2}]$.

Notice that $\mathbb{Z}[\sqrt{2}] = \{a + b\sqrt{2} \mid a, b \in \mathbb{Z}\}$ is an integral domain, subring of $\mathbb{Q}[\sqrt{2}]$, and that its field of fraction is isomorphic to $\mathbb{Q}[\sqrt{2}]$: if the inverse of $a + b\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$ is $c + d\sqrt{2} \in \mathbb{Q}[\sqrt{2}]$, then for $m \in N^\times$ multiple of the denominators of c and of d, one may write $c + d\sqrt{2} = \frac{m\,c + m\,d\sqrt{2}}{m}$, and $m\,c + m\,d\sqrt{2} \in \mathbb{Z}[\sqrt{2}]$.

With (a, b) interpreted as $a + b\,x$, one then has put on $\mathbb{Q} \times \mathbb{Q}$ a structure of field with $(a_1, b_1) + (a_2, b_2) = (a_1 + a_2, b_1 + b_2)$ and $(a_1, b_1) \star (a_2, b_2) = (a_1 a_2 + 2b_1 b_2, a_1 b_2 + b_1 a_2)$.

Remark 26.8: Since $x^3 - 2$ is irreducible in $\mathbb{Q}[x]$ (but not in $\mathbb{R}[x]$), the quotient $\mathbb{Q}[x]/(x^3 - 2)$ is a field, which one denotes $\mathbb{Q}[\sqrt[3]{2}]$. In each coset one considers the element of the form $a + b\,x + c\,x^2$ with $a, b, c \in \mathbb{Q}$, i.e. for finding to which coset $P \in \mathbb{Q}[x]$ belongs, one divides P by $x^3 - 2$ and one takes the remainder. Since $x^3 = 2 \pmod{x^3 - 2}$, one may then consider that $x = \sqrt[3]{2}$, and one writes $\mathbb{Q}[\sqrt[3]{2}] = \{a + b\sqrt[3]{2} + c\sqrt[3]{4} \mid a, b, c \in \mathbb{Q}\}$, but in this case there is no automorphism of $\mathbb{Q}[\sqrt[3]{2}]$ to consider. For $z = a + b\sqrt[3]{2} + c\sqrt[3]{4} \neq 0$, there is a multiplicative inverse, but it is not as simple as in the previous example to explain how to compute it.

If (a, b, c) is interpreted as $a + b\,x + c\,x^2$, then one has put on $\mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}$ a structure of field with $(a_1, b_1, c_1) + (a_2, b_2, c_2) = (a_1 + a_2, b_1 + b_2, c_1 + c_2)$ and $(a_1, b_1, c_1) \star (a_2, b_2, c_2) = (a_1 a_2 + 2b_1 c_2 + 2c_1 b_2, a_1 b_2 + b_1 a_2 + 2c_1 c_2, a_1 c_2 + a_2 c_1 + b_1 b_2)$.

In $\mathbb{Q}[\sqrt[3]{2}]$, the polynomial $x^3 - 2$ is not irreducible, since $x^3 - 2 = (x - \sqrt[3]{2})\,(x^2 + \sqrt[3]{2}\,x + \sqrt[3]{4})$, but $x^2 + \sqrt[3]{2}\,x + \sqrt[3]{4}$ is irreducible in $\mathbb{Q}[\sqrt[3]{2}]$.

Remark 26.9: It looks feasible to check directly that the operations $+, \star$ on $\mathbb{Q} \times \mathbb{Q}$ mentioned at Remark 26.7 define a field. However, checking that the operations $+, \star$ on $\mathbb{Q} \times \mathbb{Q} \times \mathbb{Q}$ mentioned at Remark 26.8 define a field seems a daunting task. The power of algebra is precisely that one should avoid doing that, and observe that $\star$ is the product of the polynomials $a_1 + b_1 x + c_1 x^2$ and $a_2 + b_2 x + c_2 x^2$ when x^3 is replaced by 2, and that if the coefficients $a_1, b_1, c_1, a_2, b_2, c_2$ belong to a commutative ring R, one is considering the ring structure of the quotient $R[x]/(x^3 - 2)$, which is unital if R is unital, an integral domain if R is an integral domain where no element has cube 2, and a field if moreover R is a field.

---

[3] If P has degree ≥ 2, this new field is not isomorphic to F, and it is a *finite extension* (hence an *algebraic extension*) of F. If F is algebraically closed, P must have degree 1, and one finds a field isomorphic to F, because there is no algebraic extension of F different from F itself, but one may consider a *transcendental extension* like $F(x)$, which is the field of fractions of $F[x]$.

[4] If ψ is a ring-homomorphism from a field F (or a division ring) into a ring R, then ψ is injective if and only if $\psi(1) \neq 0$, since for $x \neq 0$ one has $\psi(x)\,\psi(x^{-1}) = \psi(x\,x^{-1}) = \psi(1) \neq 0$, so that $\psi(x) \neq 0$, hence $ker(\psi) = \{0\}$.

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

27- Monday November 7, 2011.

Lemma 27.1: If p is an odd prime of the form $4m+1$, then p is the sum of two squares.
Proof: (probably due to EULER) Since -1 is a quadratic residue modulo p, there exists z with $z^2+1 = 0 \pmod p$, i.e. $z^2+1 = j\,p$ for some integer j. One considers the integers $z\,x-y$ modulo p, for all the integers x, y satisfying $0 \leq x, y < \sqrt{p}$. Since the number of pairs is $(\lfloor\sqrt{p}\rfloor+1)^2 > p$, the pigeon-hole principle implies the existence of two distinct pairs $(x_1, y_1), (x_2, y_2)$ such that $z\,x_1 - y_1 = z\,x_2 - y_2 \pmod p$, i.e. $z\,(x_1-x_2) = y_1 - y_2 \pmod p$, and taking the squares one finds that $(x_1-x_2)^2 + (y_1-y_2)^2$ is a non-zero multiple of p; then $(x_1-x_2)^2 + (y_1-y_2)^2 \leq 2(\lfloor\sqrt{p}\rfloor)^2 < 2p$, so that $(x_1-x_2)^2 + (y_1-y_2)^2 = p$.

Remark 27.2: The argument of FERMAT (who claimed to have proved this result) might have been to start by choosing among all the integer solutions of $a^2+b^2 = j\,p$ for an integer j (with a and b not multiples of p) one for which j is minimum. By eventually changing signs, one may assume that both a and b are positive, and one must have $0 < a, b < p$, since replacing a or b by the remainder of the division by p would make the value of j smaller; actually, one has $0 < a, b < \frac{p}{2}$, since if one had $\frac{p}{2} < a < p$, one could replace a by $p-a$ and make the value of j smaller, hence one has $a^2+b^2 < \frac{p^2}{2}$ and $j < \frac{p}{2}$; also, a and b are relatively prime, since if their gcd d was > 1, then $\frac{a}{d}$ and $\frac{b}{d}$ would give a smaller value of j.

If there was an odd prime p of the form $4m+1$ which is not the sum of two squares, one would take the smallest, for which j would be > 1 and equal to a product of (non necessarily distinct) primes $j = q_1 \cdots q_\ell$, with $2 \leq q_1 \leq \ldots \leq q_\ell \leq j < \frac{p}{2}$; since $a^2+b^2 = 0 \pmod{q_k}$ and a and b are relatively prime, one would deduce that $q_k = 2$ or an odd prime of the form $4m+1$ (since it implies that -1 is a quadratic residue modulo q_k), hence q_k would be a sum of two squares (since it is $< p$, supposed to the smallest which cannot be written as a sum of two squares), and one concludes by showing that if $a^2+b^2 = k\,q$ and q is prime with $q = \alpha^2+\beta^2$, then $\frac{a^2+b^2}{q} = k$ is the sum of two squares: starting from $k\,q = q_1 \cdots q_\ell p$, and repeating this argument for $q_1, \ldots, q_\ell$ then implies that p is the sum of two squares.

If a or b is a multiple of q, then both are multiples of q by the equation, and $\frac{k}{q} = \left(\frac{a}{q}\right)^2 + \left(\frac{b}{q}\right)^2$ is a sum of two squares, so that $k = \frac{k}{q}\,q$ is also the sum of two squares by Brahmagupta's identity. If a and b are not multiple of q, then $a^2+b^2 = 0 \pmod q$, and if a' is an inverse of a modulo q, $z = b\,a'$ solves $z^2 = -1 \pmod q$; similarly, $\alpha^2+\beta^2 = 0 \pmod q$ and if α' is an inverse of α modulo q, $z_1 = \beta\,\alpha'$ solves $z_1^2 = -1 \pmod q$, so that $z_1 = \pm z$; after eventually changing β into $-\beta$, one may assume that $z_1 = z$, so that one has $b = a\,z \pmod q$ and $\beta = \alpha\,z \pmod q$, hence $b\,\alpha - a\,\beta = 0 \pmod q$. Since Brahmagupta's identity gives $(a\,\alpha+b\,\beta)^2 + (b\,\alpha-a\,\beta)^2 = (a^2+b^2)\,(\alpha^2+\beta^2) = 0 \pmod q$, one deduces that $a\,\alpha+b\,\beta = 0 \pmod q$, hence $\left(\frac{a\,\alpha+b\,\beta}{q}\right)^2 + \left(\frac{b\,\alpha-a\,\beta}{q}\right)^2 = \frac{a^2+b^2}{q} = k$ is a sum of two squares.

Lemma 27.3: An integer $n \in \mathbb{Z}$ is a prime element in $\mathbb{Z}[\sqrt{D}]$ (for $D \in \mathbb{Z}$ not a square) if and only if $n = \pm p$ where p is a prime integer such that D is a quadratic non-residue modulo p.
Proof: One must reject the composite n, so that $n = \pm p$ for a prime integer p; then, $(a+b\sqrt{D})\,(c+d\sqrt{D})$ is a multiple of p if both $a\,c+b\,d\,D$ and $a\,d+b\,c$ are multiple of p, and one wants to know if it implies that a and b are multiple of p or that c and d are multiple of p.

If $D = E^2 \pmod p$ for some $E \in \mathbb{Z}$, then $(E+\sqrt{D})\,(E-\sqrt{D}) = E^2-D$ is a multiple of p, but neither $E+\sqrt{D}$ nor $E-\sqrt{D}$ are multiple of p, so that one may assume that D is not a quadratic residue modulo p.

If $a \neq 0 \pmod p$, then it has an inverse a^{-1} modulo p, and one has $c = -a^{-1}b\,d\,D \pmod p$ and then $a\,d = a^{-1}b^2 d\,D \pmod p$; if $b = 0 \pmod p$, then both c and d are $= 0 \pmod p$, so that one considers the case $b \neq 0 \pmod p$: one must then have $d = 0 \pmod p$, since $d \neq 0 \pmod p$ implies $a = a^{-1}b^2 D \pmod p$, so that D is a square modulo p, and $d = 0 \pmod p$ implies $c = 0 \pmod p$.

The case $c \neq 0 \pmod p$ is similar, and the case $a = c = 0 \pmod p$ implies $b\,d = 0 \pmod p$ so that either b or d is a multiple of p.

Remark 27.4: In the ring $\mathbb{Z}[\sqrt{-1}]$ of Gaussian integers, an integer $n \in \mathbb{Z}$ is a prime element if and only if $n = \pm p$ where p is an odd prime integer of the form $4n+3$, but there are other prime elements, besides considering the associates, obtained by multiplying by units, which are $\{\pm 1, \pm i\}$.

Remark 27.5: In $\mathbb{Z}[\sqrt{D}]$ with $D < 0$, a unit $a + b\sqrt{D}$ must satisfy $a^2 - D\,b^2 = 1$, so that only ± 1 are units if $D < -1$.

One considers now the case $D > 0$ (not a square), for which the description of units is more elaborate; one recalls that for $r = a + b\sqrt{D}$ one writes $N(r) = a^2 - D\,b^2$, and that a unit of $\mathbb{Z}[\sqrt{D}]$ is a solution of $N(r) = \pm 1$. There always exist (infinitely many) solutions $r \in \mathbb{Z}[\sqrt{D}]$ of $N(r) = +1$, but there are values of D for which there is no solution of $N(r) = -1$: for example, $y^2 - 3x^2 = -1$ has no integer solution, since it would imply $y^2 = 2 \pmod 3$, and 2 is a quadratic non-residue modulo 3. For an integer solution of $N(r) = -1$ to exist, it is necessary that D is not divisible by 4 or by any odd prime of the form $4m + 3$, since -1 is a quadratic non-residue modulo these values, but it is not sufficient, and there are no integer solutions of $N(r) = -1$ for $D = 34$.[1]

It is not difficult for some small positive values of D to find the smallest positive solution of $y^2 - D\,x^2 = +1$: for example $y^2 - 10x^2 = +1$ gives $19^2 = 361 = 10.6^2 + 1$, and the smallest positive solution of $y^2 - 10x^2 = -1$ is $3^2 = 9 = 10.1^2 - 1$, and one has $(3 + \sqrt{10})^2 = 19 + 6\sqrt{10}$; in this example, all the units are of the form $\pm(3 + \sqrt{10})^n$ for some $n \in \mathbb{Z}$, and $(3 + \sqrt{10})^{-1} = -3 + \sqrt{10}$.

However, for some not so big values of D, like 61, trial and error for finding the smallest solution is not a good method.

Remark 27.6: For $D > 0$ not a square, the equation $y^2 - D\,x^2 = +1$ was wrongly called *Pell's equation* by Euler,[2] and it has been suggested that Euler had confused Brouckner,[3] who had worked on the equation, with Pell, who had little to do with it. The equation had been studied in India as early as Brahmagupta, but the first general method was given by Bhaskara (II) in 1150,[4] with some later examples by Narayana,[5] although a proof that the algorithm of Bhaskara (II) always terminates in a finite number of steps was only found by Lagrange in 1768.

It was Fermat who issued a challenge concerning this equation in 1657, to Frenicle,[6] Brouckner, and Wallis,[7] one of them being the case $D = 61$, whose smallest solution ($x = 226\ 153\ 980, y = 1\ 766\ 319\ 049$) had been found by Bhaskara (II). Brouckner discovered a method which is essentially the method of continued fractions (for $\sqrt{D}$) which was later developed rigorously by Lagrange in 1766; Frenicle tabulated the (smallest) solutions for $D \leq 150$, but he did not publish his results and they were then lost; since Brouckner had boasted to be able to solve any example, Frenicle challenged him with the case $D = 313$, and Brouckner sent him the smallest solution ($x = 1\ 819\ 380\ 158\ 564\ 160, y = 32\ 188\ 120\ 829\ 134\ 849$), claiming that it had taken him an hour or two.

Remark 27.7: For showing that there exists a non-trivial integer solution of $y^2 - D\,x^2 = +1$, i.e. with $x \neq 0$, one may use a constructive method based on continued fractions, described further on, but there is also a non-constructive argument which uses a Diophantine approximation result of Dirichlet, that if θ is irrational, there are infinitely many pairs $a \in \mathbb{Z}, n \in \mathbb{N}^\times$ satisfying $\left|\theta - \frac{a}{n}\right| < \frac{1}{n^2}$.

For proving this result, one notices that for any $\theta \in \mathbb{R} \setminus \mathbb{Q}$ and any $N \in \mathbb{N}^\times$ there exists $a \in \mathbb{Z}$ and $n \in \{1, \ldots, N\}$ with $|n\,\theta - a| < \frac{1}{N+1}$: for $j = 1, \ldots, N$, one considers $a_j \in \mathbb{Z}$ with $\frac{-1}{2} < \varepsilon_j = j\,\theta - a_j < \frac{1}{2}$,

[1] Using the fact that $u = 35 - 6\sqrt{34}$ is a unit of $\mathbb{Z}[\sqrt{34}]$ satisfying $N(u) = 1$, one can deduce that there is no $v = y + x\sqrt{34}$ satisfying $N(v) = -1$: one considers the smallest $x > 0$ and one chooses $y > 0$, and then one observes that $w = u\,v = (35y - 6 \cdot 34\,x) + (35x - 6y)\sqrt{34}$ satisfies $N(w) = -1$, and since $y^2 - 34x^2 = -1$ implies $y < x\sqrt{34}$, so that $6y < 6x\sqrt{34} < 35x$, the value $x' = 35x - 6y$ is positive, and should then be $\geq x$, but it means $6y < 34x$, from which one deduces that $36(34x^2 - 1) < 34^2 x^2$, i.e. $68x^2 < 36$, which does not hold for an integer.

[2] John Pell, English mathematician, 1611–1685. Pell's equation is named after him, although he had little to do with it, and it had been studied first by Brahmagupta.

[3] William Brouckner, Irish-born mathematician, 1620–1684. He became the second viscount Brouckner of Castles Lyons at the death of his father, who had bought the title. He worked in London, England.

[4] Bhaskara, Indian mathematician and astronomer, 1114–1185. Known as Bhaskara (II) and Bhaskara Acharya (the teacher), his work on differential calculus predates the work of Newton by five centuries.

[5] Narayana Pandit, Indian mathematician, c. 1340–1400.

[6] Bernard Frenicle de Bessy, French mathematician, 1605–1675.

[7] John Wallis, English mathematician, 1616–1703. He held the Savilian chair of geometry at Oxford, England.

the inequalities being strict because θ is irrational, but $\frac{-1}{2}$ and $\frac{1}{2}$ should be identified, as if one imagines the real line wrapped around a circle of perimeter 1, and one looks at $\theta, 2\theta, \dots, N\,\theta$, which correspond to points $\varepsilon_j, j = 1, \dots, N$ on the circle; assume by contradiction that all these points satisfy $|\varepsilon_j| \geq \frac{1}{N+1}$, then the N values fall in the remaining part of the circle, which is an interval of length $1 - \frac{2}{N+1} = \frac{N-1}{N+1}$, corresponding to $N-1$ intervals of size $\frac{1}{N+1}$, and one may consider that these intervals are open, since no ε_i can be equal to $\frac{\ell}{N+1}$ for an integer ℓ, since θ is irrational; by the pigeon-hole principle, one of these small open intervals receives ε_j and ε_k for some $j < k$, hence $|(k\,\theta - a_k) - (j\,\theta - a_j)| < \frac{1}{N+1}$, so that one has $|n\,\theta - a| < \frac{1}{N+1}$ for $n = k - j \in \{1, \dots, N-1\}$ and $a = a_k - a_j \in \mathbb{Z}$, contradicting the hypothesis. Each such pair $(a, n) \in \mathbb{Z} \times \mathbb{N}^\times$ satisfies $\left|\theta - \frac{a}{n}\right| < \frac{1}{n^2}$, and there must be infinitely many distinct pairs, since $|n\,\theta - a|$ cannot be 0, and must tend to 0 as N tends to $+\infty$.

Using $\theta = \sqrt{D}$ (irrational since $D > 0$ is not a square) one has infinitely many pairs (a, n) such that $|n\sqrt{D} - a| < \frac{1}{n}$, and for any such pair, the integer $|a^2 - D\,n^2|$ is $= |a - n\sqrt{D}|\,|a + n\sqrt{D}| < \frac{1}{n}\left(\frac{1}{n} + 2n\sqrt{D}\right) \leq 1 + 2\sqrt{D}$, so that since there are only finitely many integers $m \in \mathbb{Z}$ with $|m| \leq 1 + 2\sqrt{D}$, there exists $m \in \mathbb{Z}$ which can be written as $a^2 - D\,n^2$ for infinitely many distinct pairs (a, n), and one may assume that $a, n \geq 0$ without changing $a^2 - D\,n^2$, and removing at most one pair one may assume that $a, n > 0$. One uses again the pigeon-hole principle by considering classes modulo $|m|$, and one finds two values $\xi, \eta \in \{1, \dots, |m|\}$ with infinitely many distinct pairs (x, y) of positive integers satisfying $y^2 - D\,x^2 = m$, $x = \xi \pmod{|m|}$, $y = \eta \pmod{|m|}$, and one chooses two distinct pairs (x_1, y_1) and (x_2, y_2) (with $0 < x_1 < x_2$ for example). Since $y_1 y_2 - D\,x_1 x_2 = 0 \pmod{|m|}$ and $y_1 x_2 - y_2 x_1 = 0 \pmod{|m|}$, one defines $Y = \frac{y_1 y_2 - D\,x_1 x_2}{m} \in \mathbb{Z}$ and $X = \frac{y_1 x_2 - y_2 x_1}{m} \in \mathbb{Z}$, and one notices that $m^2(Y^2 - D\,X^2) = (y_1 y_2 - D\,x_1 x_2)^2 - D\,(y_1 x_2 - y_2 x_1)^2 = (y_1^2 - D\,x_1^2)\,(y_2^2 - D\,x_2^2) = m^2$, so that one has $Y^2 - D\,X^2 = 1$, and it remains to notice that it is not a trivial solution with $X = 0$, since it would mean that (x_1, y_1) and (x_2, y_2) are on the same line $y_j = t\,x_j$, which intersects the hyperbola $y^2 - D\,x^2 = m$ at only one point in the positive quadrant.

Remark 27.8: The subject of continued fractions seems to have started with the work of Bombelli and of Cataldi,[8] for extracting square roots,[9] but Archimedes had used the case $d = 3$ for constructing the rational approximation $\frac{1351}{780}$ of $\sqrt{3}$, following Pythagoras who had used the case $d = 2$ for constructing rational approximations of $\sqrt{2}$, much after Baudhayana,[10] who had found the solutions (12,17) and (408,577) of "Pell's equation".

Definition 27.9: For $a_0, a_1, \dots, a_n \in \mathbb{R}$, all positive except possibly a_0, the *continued fraction* denoted $\langle a_0, a_1, \dots, a_n \rangle$ is the quantity

$$a_0 + \cfrac{1}{a_1 + \cfrac{1}{\ddots + \cfrac{1}{a_{n-1} + \cfrac{1}{a_n}}}}.$$

If $a_0, \dots, a_n$ are integers, the continued fraction is called *simple*.

Remark 27.10: Looking for a continued fraction expansion of the rational number $r = \frac{a}{b}$ (with a and b relatively prime) follows closely the Euclidean algorithm for finding the gcd of a and b, and one discovers that there are (exactly) two ways of writing r as a continued fraction, one having the form $\langle a_0, a_1, \dots, a_n \rangle$ with $a_n > 1$ for some n, and the other being $\langle a_0, a_1, \dots, a_n - 1, 1 \rangle$.

By induction, one then observes that for $k \geq 1$ and any $x \in \mathbb{R}$ one has

$$\langle a_0, a_1, \dots, a_{k-1}, x \rangle = \frac{x\,p_{k-1} + p_{k-2}}{x\,q_{k-1} + q_{k-2}}$$

[8] Pietro Antonio Cataldi, Italian mathematician, 1548–1626. He worked in Perugia and in Bologna, Italy.

[9] If $a > 0$, then the mapping $f : x \mapsto \frac{1}{2}\left(x + \frac{a}{x}\right)$ has $\sqrt{a}$ as its unique fixed point in $\mathbb{R}_+$, and since $f'(\sqrt{a}) = 0$ the convergence of the iterative method is very fast (quadratic), and basically it is the algorithm used in computers for extracting square roots. Starting with the integer $m = \lfloor \sqrt{a} \rfloor$ (i.e. such that $m^2 \leq a < (m+1)^2$) and applying the algorithm generates a sequence of rationals converging fast to $\sqrt{a}$, but it is different from the one given by the continued fraction expansion of $\sqrt{a}$.

[10] Baudhayana, Indian mathematician, c. 800 BCE.

with

$$p_{-1} = 1, q_{-1} = 0, p_0 = a_0, q_0 = 1; p_k = a_k p_{k-1} + p_{k-2}, q_k = a_k q_{k-1} + q_{k-2} \text{ for all } k \geq 1,$$

so that $c_k = \langle a_0, a_1, \ldots, a_k \rangle$, which is called the kth *convergent* of the continued fraction $\langle a_0, a_1, \ldots, a_n \rangle$, satisfies

$$c_k = \langle a_0, a_1, \ldots, a_k \rangle = \frac{p_k}{q_k} \text{ for } k \geq 0.$$

By induction, one then shows that

$$p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1} \text{ for all } k \geq 1,$$

which implies that p_k and q_k are relatively prime, and

$$c_k - c_{k-1} = \frac{(-1)^{k-1}}{q_{k-1} q_k} \text{ for } k \geq 1;$$

similarly, one has $p_k q_{k-2} - p_{k-2} q_k = (-1)^k a_k$ for all $k \geq 1$. One deduces that $c_0 < c_2 < \cdots < c_3 < c_1$.

Lemma 27.11: If $a_0, a_1, \ldots$ is an infinite sequence of integers, all positive except possibly a_0, and $c_n = \langle a_0, a_1, \ldots, a_n \rangle$, then $\ell = \lim_{n \to \infty} c_n$ exists, and is denoted $\langle a_0, a_1, \ldots \rangle$, so that

$$\langle a_0, a_1 \ldots \rangle = a_0 + \frac{1}{\langle a_1, a_2, \ldots \rangle}.$$

Every irrational ξ is the limit of a unique infinite continued fraction.

Proof: Since the increasing sequence c_{2n} converges to a limit $\leq c_1$, the decreasing sequence c_{2n+1} converges to a limit $\geq c_0$, and these limits are equal because $|c_k - c_{k-1}| = \frac{1}{q_{k-1} q_k}$ for $k \geq 1$ and q_k tends to ∞ as $k \to \infty$; actually, since $q_0 = 1$, $q_1 = a_1 q_0 \geq 1$ and $q_k = a_k q_{k-1} + q_{k-2} \geq q_{k-1} + q_{k-2}$ for all $k \geq 2$, one deduces that

$$q_k \geq F_k \text{ for all } k \geq 0, \text{ where } F_k \text{ is the Fibonacci sequence,}$$

and the Fibonacci sequence grows as ρ^k for the golden ratio $\rho = \frac{1+\sqrt{5}}{2}$.

If an infinite continued fraction has limit ξ, one must have $a_0 = \lfloor \xi \rfloor$ (i.e. a_0 is the integer satisfying $a_0 \leq \xi < a_0 + 1$), so that $\xi = a_0 + \frac{1}{\xi_1}$ with $\xi_1 > 1$, and one reiterates the process with ξ_1, so that $a_1 = \lfloor \xi_1 \rfloor$, and so on, showing that $\xi = \langle a_0, a_1, \ldots, a_k, \xi_{k+1} \rangle$, which by Remark 27.10 implies $\xi = \frac{\xi_{k+1} p_k + p_{k-1}}{\xi_{k+1} q_k + q_{k-1}}$, hence

$$\xi - \frac{p_k}{q_k} = \frac{p_{k-1} q_k - p_k q_{k-1}}{q_k (\xi_{k+1} q_k + q_{k-1})} = \frac{(-1)^k}{q_k (\xi_{k+1} q_k + q_{k-1})}, \text{ so that } \left| \xi - \frac{p_k}{q_k} \right| \leq \frac{1}{q_k q_{k+1}} \text{ for } k \geq 0,$$

since $\xi_{k+1} q_k + q_{k-1} \geq a_{k+1} q_k + q_{k-1} = q_{k+1}$, and because $q_k \to \infty$ as $k \to \infty$, it shows that $\xi = \langle a_0, a_1, \ldots \rangle$. One has $\langle a_0, a_1 \ldots \rangle = a_0 + \frac{1}{\langle a_1, a_2, \ldots \rangle}$, and more generally $\xi_k = \langle a_k, a_{k+1}, \ldots \rangle$ for all $k \geq 1$.

Definition 27.12: The infinite simple continued fraction $\langle a_0, a_1, \ldots, a_{n-1}, \overline{b_0, b_1, \ldots, b_{m-1}} \rangle$ is called *periodic*, and the bar indicates that the sequence $b_0, b_1, \ldots, b_{m-1}$ is repeated indefinitely; if the continued fraction has the form $\langle \overline{b_0, b_1, \ldots, b_{m-1}} \rangle$, it is called *purely periodic*.

Remark 27.13: A purely periodic continued fraction $\xi = \langle \overline{b_0, b_1, \ldots, b_{m-1}} \rangle$ is of the form $\frac{\xi\, p_{m-1} + p_{m-2}}{\xi\, q_{m-1} + q_{m-2}}$, since it can be written as $\langle b_0, b_1, \ldots, b_{m-1}, \overline{b_0, b_1, \ldots, b_{m-1}} \rangle$, showing that ξ is a quadratic irrational, i.e. the solution of a quadratic equation $A\,\xi^2 + B\,\xi + C = 0$ with integer coefficients A, B, C, $A = q_{m-1} \neq 0$, and discriminant $B^2 - 4A\,C$ positive and not a square (since $B^2 - 4A\,C = D^2$ gives $\xi = \frac{-B \pm D}{2A} \in \mathbb{Q}$). For example, if $\xi = \langle \overline{1} \rangle$ (i.e. all a_j are equal to 1), then one has $\xi = 1 + \frac{1}{\xi}$, so that ξ is the positive root of $z^2 - z - 1 = 0$, i.e. the golden ratio $\frac{1+\sqrt{5}}{2}$.

More generally, a periodic continued fraction $\eta = \langle a_0, a_1, \ldots, a_{n-1}, \overline{b_0, b_1, \ldots, b_{m-1}} \rangle$ is of the form $\frac{\xi\, p_{n-1} + p_{n-2}}{\xi\, q_{n-1} + q_{n-2}}$ for the quadratic irrational $\xi = \langle \overline{b_0, b_1, \ldots, b_{m-1}} \rangle$, hence η is also a quadratic irrational.[11]

[11] Since $\eta = \frac{\xi\, p_{n-1} + p_{n-2}}{\xi\, q_{n-1} + q_{n-2}}$ implies $\xi = \frac{-\eta\, q_{n-2} + p_{n-2}}{\eta\, q_{n-1} - p_{n-1}}$, and $A\,\xi^2 + B\,\xi + C = 0$ implies $A\,(-\eta\, q_{n-2} + p_{n-2})^2 + B\,(-\eta\, q_{n-2} + p_{n-2})\,(\eta\, q_{n-1} - p_{n-1}) + C\,(\eta\, q_{n-1} - p_{n-1})^2 = 0$, hence η is a quadratic irrational.

The converse, that any quadratic irrational has a periodic continued fraction expansion was proved by LAGRANGE (Lemma 27.15), using an algorithm of EULER (Lemma 27.14), essentially the same that BROUCKNER had used (without mentioning continued fractions), and closely related to a "cyclic method" of BHASKARA (II); the characterization of those quadratic irrationals which have a purely periodic continued fraction expansion, implicit in the work of LAGRANGE, was proved in 1828 by GALOIS (Lemma 27.17).

Lemma 27.14: (EULER) A quadratic irrational ξ_0 can be written as $\frac{r_0+\sqrt{d}}{s_0}$, where d is a positive integer which is not a square, and r_0 and s_0 are integers, $s_0 \neq 0$, and $s_0 \mid d - r_0^2$ (and $m \mid n$ means that m divides n).[12] The continued fraction of ξ_0 (which begins with $a_0 = \lfloor \xi_0 \rfloor$) satisfies

$$\xi_k = \frac{r_k + \sqrt{d}}{s_k} \text{ for } k \geq 0,$$

with

$$r_{k+1} = a_k s_k - r_k \text{ with } a_k = \lfloor \xi_k \rfloor, s_{k+1} = \frac{d - r_{k+1}^2}{s_k} \text{ for } k \geq 0,$$

and is such that

$$r_k, s_k \text{ are integers}, s_k \neq 0, s_k \mid d - r_k^2, s_k \mid d - r_{k+1}^2 \text{ for } k \geq 0.$$

Since $\lfloor \sqrt{d} \rfloor \leq \sqrt{d} < \lfloor \sqrt{d} \rfloor + 1$, one has $\lfloor \xi_k \rfloor = \lfloor \frac{r_k+\sqrt{d}}{s_k} \rfloor = \lfloor \frac{r_k+\lfloor \sqrt{d} \rfloor}{s_k} \rfloor$ if $s_k > 0$ (and $= \lfloor \frac{r_k+\lfloor \sqrt{d} \rfloor+1}{s_k} \rfloor$ if $s_k < 0$), so that one needs to compute $\lfloor \sqrt{d} \rfloor$ once, and then the algorithm can be followed using integer arithmetic; a simpler formula is also $s_{k+1} = s_{k-1} + a_k(r_k - r_{k+1})$.[13]

Proof: Since $A\,\xi_0^2 + B\,\xi_0 + C = 0$ for integers A, B, C with $A \neq 0$, one has $\xi_0 = \frac{-B \pm \sqrt{B^2 - 4A\,C}}{2A}$, and one may choose $d = B^2 - 4A\,C$, $r_0 = \mp B$, $s_0 = \pm 2A$, so that $d - r_0^2 = -4A\,C$ is a multiple of s_0. Then one proceeds by induction on k: r_{k+1} is an integer, equal to $-r_k$ modulo s_k, so that $d - r_{k+1}^2 = d - r_k^2 = 0 \pmod{s_k}$, showing that s_{k+1} is a non-zero integer, which divides $d - r_{k+1}^2$ since the quotient is s_k, and then $\xi_{k+1} = \frac{1}{\xi_k - a_k} = \frac{s_k}{r_k + \sqrt{d} - a_k s_k} = \frac{s_k}{-r_{k+1} + \sqrt{d}} = \frac{s_k(r_{k+1}+\sqrt{d})}{d - r_{k+1}^2} = \frac{r_{k+1}+\sqrt{d}}{s_{k+1}}$.

Lemma 27.15: (LAGRANGE) The continued fraction expansion of any quadratic irrational ξ_0 is periodic.

Proof: One has $\left(\xi_0 - \frac{p_k}{q_k}\right)\left(\overline{\xi_0} - \frac{p_k}{q_k}\right) = \frac{1}{q_k^k(\xi_{k+1}q_k + q_{k+1})\,(\overline{\xi_{k+1}}q_k + q_{k+1})}$, because $\xi_0 - \frac{p_k}{q_k} = \frac{(-1)^k}{q_k(\xi_{k+1}q_k + q_{k+1})}$ (Lemma 27.11), and since $\frac{p_k}{q_k}$ converges to ξ, being alternatively above or below, it eventually falls between ξ_0 and $\overline{\xi_0}$ (which is $\neq \xi_0$), and both sides then being negative one has $\overline{\xi_{k+1}}q_k + q_{k+1} < 0$ for some k, so that $\overline{\xi_{k+1}} < 0$. Since $\xi_{m+1} = \frac{1}{\xi_m - a_m}$, one has $\overline{\xi_{m+1}} = \frac{1}{\overline{\xi_m} - a_m}$, so that $\overline{\xi_m} < 0$ implies $\overline{\xi_{m+1}} < 0$, but also $\overline{\xi_{m+1}} > -1$ since $a_m \geq 1$, hence $-1 < \overline{\xi_n} < 0$ for n large enough. From $1 < \xi_n - \overline{\xi_n} = \frac{2\sqrt{d}}{s_n}$, one deduces that $0 < s_n < 2\sqrt{d}$, and from $\xi_n = \frac{r_n+\sqrt{d}}{s_n}$, one deduces $\frac{r_n^2 - d}{s_n^2} = \xi_n\overline{\xi_n} < 0$, so that $-\sqrt{d} < r_n < \sqrt{d}$, but also $r_n > 0$ since $0 < \xi_n + \overline{\xi_n} = \frac{2r_n}{s_n}$. For n large enough, the pair (r_n, s_n) can take at most $2d$ different values, hence there exist $m < n$ with $r_m = r_n$ and $s_m = s_n$, and the recurrence relation of Lemma 27.14 then shows that the continued fraction is periodic.

Definition 27.16: A continued fraction expansion is *reduced* if $\xi_0 > 1$ and $\overline{\xi_0} = \frac{r - \sqrt{d}}{s}$ satisfies $-1 < \overline{\xi_0} < 0$.[14]

Lemma 27.17: (GALOIS) A quadratic irrational $\xi_0 = \frac{r_0+\sqrt{d}}{s_0}$ has a purely periodic continued fraction expansion if and only if it is reduced. If $\xi_0 = \langle \overline{a_0, a_1, \ldots, a_{m-1}} \rangle$, then $\frac{-1}{\overline{\xi_0}} = \langle \overline{a_{m-1}, a_{m-2}, \ldots, a_0} \rangle$.

---

[12] If $\xi = \frac{a+b\sqrt{d}}{c}$ for integers a, b, c, d, with $c \neq 0$ and d not a square, then one writes it $\frac{R+\sqrt{D}}{S}$ with $R = a\,c$, $D = b^2c^2d$, and $S = c^2$, and one has $S \mid D - R^2$.

[13] From $s_k s_{k+1} = d - r_{k+1}^2$ and $s_{k-1}s_k = d - r_k^2$, one deduces that $s_k(s_{k+1} - s_{k-1}) = r_k^2 - r_{k+1}^2 = (r_k - r_{k+1})\,(r_k + r_{k+1})$, and then one uses $r_k + r_{k+1} = a_k s_k$.

[14] When d_1 is an integer which is not a square, conjugation acts on the field $\mathbb{Q}[\sqrt{d_1}]$ by $\overline{a + b\sqrt{d_1}} = a - b\sqrt{d_1}$, and conjugation is an automorphism of the field $\mathbb{Q}[\sqrt{d_1}]$. If $d_2 = d_1 e^2$ for a positive integer e, then $\mathbb{Q}[\sqrt{d_2}]$ is a subfield of $\mathbb{Q}[\sqrt{d_1}]$, and the conjugate of $a + b\sqrt{d_2}$ in $\mathbb{Q}[\sqrt{d_2}]$ coincides with the conjugate of $a + b\,e\sqrt{d_1}$ in $\mathbb{Q}[\sqrt{d_1}]$.

Proof: In the proof of Lemma 27.15 it was shown that if $\overline{\xi_m} < 0$ then ξ_{m+1} is reduced, so that ξ_0 reduced implies ξ_k reduced for all $k \geq 1$ (and this uses the assumption that $\xi_0 > 1$, in order to have $a_0 \geq 1$). By Lemma 27.15, there exists an integer $m \geq 1$ and $j \geq 0$ such that $\xi_j = \xi_{m+j}$, and if $j \geq 1$, one wants to show that it implies $\xi_{j-1} = \xi_{m+j-1}$, so that by repeating the argument it is true for $j = 0$, i.e. one has a purely periodic continued fraction; for proving this, one notices that there is a unique (positive) integer k such that $k + \frac{1}{\xi_j}$ is reduced (so that $\xi_{j-1} = k + \frac{1}{\xi_j} = k + \frac{1}{\xi_{m+j}} = \xi_{m+j-1}$, and $k \geq 1$): indeed, one must have $-1 < k + \frac{1}{\overline{\xi_j}} < 0$, which means $\lfloor \frac{1}{\overline{\xi_j}} \rfloor = -k - 1$.

For the converse, one assumes that $\xi_0 = \langle \overline{a_0, \ldots, a_{m-1}} \rangle$. The case $m = 1$ corresponds to $\xi_0 = a_0 + \frac{1}{\xi_0}$, so that $\xi_0^2 - a_0 \xi_0 - 1 = 0$, i.e. $\xi_0 = \frac{a_0 + \sqrt{a_0^2+4}}{2} > 1$ and $\overline{\xi_0} = \frac{a_0 - \sqrt{a_0^2+4}}{2}$, so that $\xi_0 \overline{\xi_0} = -1$. If $m > 1$, one defines $\eta_j = \frac{-1}{\overline{\xi_j}}$ for $j \geq 0$, and one notices that the formula $\xi_j = a_j + \frac{1}{\xi_{j+1}}$ gives $\overline{\xi_j} = a_j + \frac{1}{\overline{\xi_{j+1}}}$, i.e. $\eta_{j+1} = a_j + \frac{1}{\eta_j}$; one deduces that $\eta_0 = \eta_m = \langle a_{m-1}, \eta_{m-1} \rangle = \langle a_{m-1}, a_{m-2}, \eta_{m-2} \rangle = \ldots = \langle a_{m-1}, a_{m-2}, \ldots, a_0, \eta_0 \rangle$, so that $\eta_0 = \langle \overline{a_{m-1}, a_{m-2}, \ldots, a_0} \rangle$, and in particular $\eta_0 > 1$, so that ξ_0 is reduced.

Lemma 27.18: If d is a positive integer which is not a square, the continued fraction expansion of $\sqrt{d}$ has the form $\langle a_0, \overline{a_1, a_2, \ldots, a_2, a_1, 2a_0} \rangle$, where $a_0 = \lfloor \sqrt{d} \rfloor$.
Proof: Let $\xi = a_0 + \sqrt{d} > 1$, so that $\overline{\xi} = a_0 - \sqrt{d}$ satisfies $-1 < \overline{\xi} < 0$, i.e. ξ is reduced, hence it has a purely periodic expansion $\langle \overline{2a_0, a_1, a_2, \ldots, a_n} \rangle = \langle 2a_0, a_1, a_2, \ldots, a_n, \overline{2a_0, a_1, a_2, \ldots, a_n} \rangle$ by Lemma 27.17, hence $\sqrt{d} = \langle a_0, \overline{a_1, a_2, \ldots, a_n, 2a_0} \rangle$ after subtracting a_0. By Lemma 27.17, one also has $\frac{-1}{\overline{\xi}} = \langle \overline{a_n, a_{n-1}, \ldots, a_1, 2a_0} \rangle$, and since it is $\frac{1}{\sqrt{d} - a_0}$, one deduces that $\sqrt{d} - a_0 = \langle 0, \overline{a_n, a_{n-1}, \ldots, a_1, 2a_0} \rangle$, hence $\sqrt{d} = \langle a_0, \overline{a_n, a_{n-1}, \ldots, a_1, 2a_0} \rangle$ after adding a_0, so that the sequence $a_1, a_2, \ldots, a_n$ coincides with $a_n, a_{n-1}, \ldots, a_1$, proving the desired symmetry.

Remark 27.19: The preceding proof applies if $\sqrt{d}$ is replaced by $\frac{\sqrt{d}}{s}$ for a positive integer $s < \sqrt{d}$, and a_0 is taken to be $\lfloor \frac{\sqrt{d}}{s} \rfloor$.

Conversely, if $\eta = \langle b_0, \overline{b_1, b_2, \ldots, b_2, b_1, 2b_0} \rangle$, then $\eta = \sqrt{r}$ for a rational $r > 1$: since η is a quadratic irrational, one may write it $\eta = \frac{A + \sqrt{D}}{B}$, and because $\eta = b_0 + \frac{1}{\zeta}$ with $\zeta = \langle \overline{b_1, b_2, \ldots, b_2, b_1, 2b_0} \rangle$, one has $\frac{-1}{\overline{\zeta}} = \langle \overline{2b_0, b_1, b_2, \ldots, b_2, b_1} \rangle = b_0 + \eta$, but $\frac{-1}{\overline{\zeta}} = b_0 - \overline{\eta}$, which implies $\eta + \overline{\eta} = 0$, i.e. $A = 0$, and since $2b_0 > 0$, one has $b_0 \geq 1$, corresponding to $B < \sqrt{D}$.

Lemma 27.20: Let $\frac{p_k}{q_k}$ denote the kth convergent of $\sqrt{d}$, and let r_k and s_k be defined as in Lemma 27.14 (so that $r_0 = 0$ and $s_0 = 1$), then for any $k \geq 0$ one has

$$\frac{p_k + q_k \sqrt{d}}{p_{k-1} + q_{k-1} \sqrt{d}} = \frac{r_{k+1} + \sqrt{d}}{s_k}.$$

Proof: For $k = 0$ one has $r_0 = 0, s_0 = 1, r_1 = a_0 s_0 - r_0 = a_0$, so that the right hand side is $a_0 + \sqrt{d}$; one has $p_{-1} + q_{-1}\sqrt{d} = 1, p_0 + q_0 \sqrt{d} = a_0 + \sqrt{d}$, so that the left hand side is also $a_0 + \sqrt{d}$. One proves the result by induction, assuming that the formula is true for k, and one uses the relations $p_{k+1} = a_{k+1} p_k + p_{k-1}$, $q_{k+1} = a_{k+1} q_k + q_{k-1}$, $s_{k+1} = \frac{d - r_{k+1}^2}{s_k}$, $r_{k+2} = a_{k+1} s_{k+1} - r_{k+1}$, so that one has $p_{k+1} + q_{k+1}\sqrt{d} = a_{k+1}(p_k + q_k \sqrt{d}) + p_{k-1} + q_{k-1}\sqrt{d}$, and $\frac{p_{k+1} + q_{k+1}\sqrt{d}}{p_k + q_k \sqrt{d}} = a_{k+1} + \frac{p_{k-1} + q_{k-1}\sqrt{d}}{p_k + q_k \sqrt{d}}$, which is $a_{k+1} + \frac{s_k}{r_{k+1} + \sqrt{d}}$ by the induction hypothesis, i.e. $a_{k+1} + s_k \frac{\sqrt{d} - r_{k+1}}{d - r_{k+1}^2} = a_{k+1} + \frac{\sqrt{d} - r_{k+1}}{s_{k+1}} = \frac{a_{k+1} s_{k+1} - r_{k+1} + \sqrt{d}}{s_{k+1}} = \frac{r_{k+2} + \sqrt{d}}{s_{k+1}}$.

Lemma 27.21: Suppose that the continued fraction expansion of $\sqrt{d}$ has period m, with $\frac{p_k}{q_k}$ denoting the kth convergent of $\sqrt{d}$, and r_k and s_k being defined as in Lemma 27.14 (so that $r_0 = 0$ and $s_0 = 1$); then one has

i) $p_{k-1}^2 - d\, q_{k-1}^2 = (-1)^k s_k$ for all $k \geq 0$,
ii) $s_k > 0$ for all $k \geq 0$,
iii) $s_k = 1$ if and only if $m \mid k$.

Hence $p_{j\,m-1}^2 - d\, q_{j\,m-1}^2 = 1$ for $j = 1, 2, 3, \ldots$ if m is even; if m is odd, one has $p_{j\,m-1}^2 - d\, q_{j\,m-1}^2 = -1$ for $j = 1, 3, 5, \ldots$ and $p_{j\,m-1}^2 - d\, q_{j\,m-1}^2 = 1$ for $j = 2, 4, 6, \ldots$.

Proof: Using Lemma 27.20, one has $\frac{p_k+q_k\sqrt{d}}{p_{k-1}+q_{k-1}\sqrt{d}} = \frac{r_{k+1}+\sqrt{d}}{s_k}$, and taking conjugates $\frac{p_k-q_k\sqrt{d}}{p_{k-1}-q_{k-1}\sqrt{d}} = \frac{r_{k+1}-\sqrt{d}}{s_k}$, so that the product gives $\frac{p_k^2-q_k^2\sqrt{d}}{p_{k-1}^2-q_{k-1}^2\sqrt{d}} = -\frac{d-r_{k+1}^2}{s_k^2} = -\frac{s_{k+1}}{s_k}$, since $d-r_{k+1}^2 = s_k s_{k+1}$; i) then follows from $p_{-1}^2 - d\,q_{-1}^2 = s_0$, which is true, since $p_{-1}=1$, $q_{-1}=0$, and $s_0=1$.

ii) then follows from the fact that any odd convergent is $> \sqrt{d}$ and any even convergent is $< \sqrt{d}$.

Since $\sqrt{d}$ has the form $\langle a_0, \overline{a_1, \ldots, a_{m-1}, 2a_0}\rangle$, one has $\xi_m = \xi_{2m} = \ldots = \langle \overline{2a_0, a_1, \ldots, a_{m-1}}\rangle = a_0 + \sqrt{d}$ (with $a_0 = \lfloor \sqrt{d} \rfloor$), hence by Lemma 27.14 $r_m = r_{2m} = \ldots = a_0$ and $s_m = s_{2m} = \ldots = 1$. Assume that $s_k = 1$ for some $k \geq 1$; then, since ξ_j has a purely periodic continued fraction expansion for all $j \geq 1$, it is reduced, so that $-1 < \overline{\xi_j} < 0$, and because $\overline{\xi_j} = \frac{r_j - \sqrt{d}}{s_j}$, one deduces that $-1 < r_k - \sqrt{d} < 0$, i.e. $r_k = \lfloor \sqrt{d} \rfloor = a_0$ and $\xi_k = a_0 + \sqrt{d}$, so that k must be a multiple of m by definition of m.

Remark 27.22: There are actually no other positive integer solutions of $y^2 - d\,x^2 = \pm 1$ than those mentioned in Lemma 27.21 (Lemma 27.29), and in particular the condition for an integer solution of $y^2 - d\,x^2 = -1$ to exist is that the continued fraction expansion of $\sqrt{d}$ has an odd period. As mentioned in a previous footnote, since $y^2 = -1 \pmod{d}$ implies that -1 is a quadratic residue modulo any prime divisor of d, it is necessary that d is not a multiple of 4 or of any odd prime number of the form $4m+3$; however, these conditions are not sufficient, since $34 = 2 \cdot 17$ satisfies these conditions, but $34 = \langle 5, \overline{1, 4, 1, 10}\rangle$, which shows an even period: indeed, $\sqrt{34} = 5 + (\sqrt{34} - 5)$ and $\frac{1}{\sqrt{34}-5} = \frac{\sqrt{34}+5}{9} = 1 + \frac{\sqrt{34}-4}{9}$, $\frac{9}{\sqrt{34}-4} = \frac{\sqrt{34}+4}{2} = 4 + \frac{\sqrt{34}-4}{2}$, $\frac{2}{\sqrt{34}-4} = \frac{\sqrt{34}+4}{9} = 1 + \frac{\sqrt{34}-5}{9}$, $\frac{9}{\sqrt{34}-5} = \sqrt{34} + 5 = 10 + (\sqrt{34} - 5)$.

Lemma 27.23: If p is an odd prime of the form $4m+1$, and n is an odd integer, then there is an integer solution of $y^2 - p^n x^2 = -1$, so that (by Lemma 27.29) $\sqrt{p^n}$ has a continued fraction expansion with an odd period.

Proof: For $d = p^n$, one considers the smallest positive integer solution (u, v) of $v^2 - d\,u^2 = 1$, and since $d = 1 \pmod 4$ one has $v^2 - u^2 = 1 \pmod 4$, which implies that v is odd and u is even, i.e. $v = 2t+1, u = 2s$, and the equation becomes $t\,(t+1) = d\,s^2$. Since a prime factor of $t\,(t+1)$ cannot divide both t and $t+1$, either $t = d\,a^2, t+1 = b^2$ with $s = a\,b$, or $t = a^2, t+1 = d\,b^2$ with $s = a\,b$; in the first case one would deduce that $b^2 - d\,a^2 = 1$, contradicting the fact that one started with the smallest positive integer solution, so that one has the second situation, which implies $a^2 - d\,b^2 = -1$.

Lemma 27.24: (LEGENDRE) If d is a positive integer which is not a square, and is such that $\sqrt{d}$ has a continued fraction expansion with an odd period, then it has a representation $d = a^2 + b^2$ which is primitive, i.e. with a and b relatively prime.

Proof: By Lemma 27.18, $\sqrt{d} = \langle a_0, \overline{a_1, \ldots, a_k, a_k, \ldots, a_1, 2a_0}\rangle$, so that $\xi_{k+1} = \langle \overline{a_k, \ldots, a_1, 2a_0, a_k, \ldots, a_1}\rangle$ is reduced and $\xi_{k+1} = \frac{-1}{\overline{\xi_{k+1}}}$ by Lemma 27.17, hence $\xi_{k+1}\overline{\xi_{k+1}} = -1$, and since $\xi_{k+1} = \frac{r_{k+1}+\sqrt{d}}{s_{k+1}}$ by Lemma 27.14, it means $r_{k+1}^2 + s_{k+1}^2 = 1$.

If a prime p would divide both r_{k+1} and s_{k+1}, it would divide d by the equation, and it would also divide s_k, since one has $d - r_{k+1}^2 = s_k s_{k+1}$ by Lemma 27.14, which implies $s_k = s_{k+1}$. By Lemma 27.21, one has $p_{k-1}^2 - d\,q_{k-1}^2 = (-1)^k s_k$, and $p_k^2 - d\,q_k^2 = (-1)^{k+1} s_{k+1}$, so that p would divide p_{k-1}^2 and p_k^2, i.e. it would divide both p_{k-1} and p_k, contradicting the relation $p_k q_{k-1} - p_{k-1} q_k = (-1)^{k-1}$ (Remark 27.10).

Remark 27.25: If p is odd prime of the form $4m+1$, then the continued fraction expansion of $\sqrt{p}$ has an odd period (because Lemma 27.29 asserts that all solutions are given by Lemma 27.21), and the algorithm of Lemma 27.14 starts by defining $r_0 = 0$, $s_0 = 1$, $a_0 = \lfloor \sqrt{p} \rfloor$, and then $r_{k+1} = a_k s_k - r_k$, $s_{k+1} = \frac{p - r_{k+1}^2}{s_k}$, $a_{k+1} = \lfloor \frac{r_{k+1}+\sqrt{p}}{s_{k+1}} \rfloor = \lfloor \frac{r_{k+1}+a_0}{s_{k+1}} \rfloor$, so that $r_1 = a_0$, $s_1 = p - a_0^2$, $a_1 = \lfloor \frac{2a_0}{p-a_0^2} \rfloor$, and then one may use the simpler formula $s_{k+1} = s_{k-1} + a_k(r_k - r_{k+1})$, and a solution is found once one finds an integer j such that $s_j = s_{j+1}$.

Remark 27.26: Continued fractions of $\sqrt{d}$ which have period 1 correspond to $\langle n, \overline{2n}\rangle = \sqrt{n^2+1}$ for an integer $n \geq 1$;[15] for values $d < 100$ one finds $\sqrt{2}, \sqrt{5}, \sqrt{10}, \sqrt{17}, \sqrt{26}, \sqrt{37}, \sqrt{50}, \sqrt{65}, \sqrt{82}$.

[15] If $\xi = \langle n, \overline{2n}\rangle$ and $\alpha = \langle \overline{2n}\rangle$, then $\xi = n + \frac{1}{\alpha}$ and $\alpha = 2n + \frac{1}{\alpha}$, or $\alpha^2 - 2n\,\alpha - 1 = 0$, so that $\alpha = n + \sqrt{n^2+1}$, $\frac{1}{\alpha} = \frac{n - \sqrt{n^2+1}}{-1}$, and then $\xi = \sqrt{n^2+1}$.

Continued fractions of $\sqrt{d}$ which have period 2 correspond to $\langle n, \overline{a, 2n}\rangle = \sqrt{n^2 + \frac{2n}{a}}$ for integers $a, n \geq 1$ with $a \neq 2n$,[16] so that a must divide $2n$ (and $a \neq 2n$), and one obtains the integers $\sqrt{n^2+b}$ with $b > 1$ dividing $2n$; for values $d < 100$ one finds $\sqrt{3}$, $\sqrt{6}, \sqrt{8}$, $\sqrt{11}, \sqrt{12}, \sqrt{15}$, $\sqrt{18}, \sqrt{20}, \sqrt{24}$, $\sqrt{27}, \sqrt{30}, \sqrt{35}$, $\sqrt{38}, \sqrt{39}, \sqrt{40}, \sqrt{42}, \sqrt{48}$, $\sqrt{51}, \sqrt{56}, \sqrt{63}$, $\sqrt{66}, \sqrt{68}, \sqrt{72}, \sqrt{80}$, $\sqrt{83}, \sqrt{84}, \sqrt{87}, \sqrt{90}, \sqrt{99}$.

For primes $d < 100$, one finds

$$\sqrt{3} = \langle 1, \overline{1, 2}\rangle$$
$$\sqrt{5} = \langle 2, \overline{4}\rangle$$
$$\sqrt{7} = \langle 2, \overline{1, 1, 1, 4}\rangle$$
$$\sqrt{11} = \langle 3, \overline{3, 6}\rangle$$
$$\sqrt{13} = \langle 3, \overline{1, 1, 1, 1, 6}\rangle$$
$$\sqrt{17} = \langle 4, \overline{8}\rangle$$
$$\sqrt{19} = \langle 4, \overline{2, 1, 3, 1, 2, 8}\rangle$$
$$\sqrt{23} = \langle 4, \overline{1, 3, 1, 8}\rangle$$
$$\sqrt{29} = \langle 5, \overline{2, 1, 1, 2, 10}\rangle$$
$$\sqrt{31} = \langle 5, \overline{1, 1, 3, 5, 3, 1, 1, 10}\rangle$$
$$\sqrt{37} = \langle 6, \overline{12}\rangle$$
$$\sqrt{41} = \langle 6, \overline{2, 2, 12}\rangle$$
$$\sqrt{43} = \langle 6, \overline{1, 1, 3, 1, 5, 1, 3, 1, 1, 12}\rangle$$
$$\sqrt{47} = \langle 6, \overline{1, 5, 1, 12}\rangle$$
$$\sqrt{53} = \langle 7, \overline{3, 1, 1, 3, 14}\rangle$$
$$\sqrt{59} = \langle 7, \overline{1, 2, 7, 2, 1, 14}\rangle$$
$$\sqrt{61} = \langle 7, \overline{1, 4, 3, 1, 2, 2, 1, 3, 4, 1, 14}\rangle$$
$$\sqrt{67} = \langle 8, \overline{5, 2, 1, 1, 7, 1, 1, 2, 5, 16}\rangle$$
$$\sqrt{71} = \langle 8, \overline{2, 2, 1, 7, 1, 2, 2, 16}\rangle$$
$$\sqrt{73} = \langle 8, \overline{1, 1, 5, 5, 1, 1, 16}\rangle$$
$$\sqrt{79} = \langle 8, \overline{1, 7, 1, 16}\rangle$$
$$\sqrt{83} = \langle 9, \overline{9, 18}\rangle$$
$$\sqrt{89} = \langle 9, \overline{2, 3, 3, 2, 18}\rangle$$
$$\sqrt{93} = \langle 9, \overline{1, 1, 1, 4, 6, 4, 1, 1, 1, 18}\rangle$$
$$\sqrt{97} = \langle 9, \overline{1, 5, 1, 1, 1, 1, 1, 1, 5, 1, 18}\rangle.$$

For composites $d < 100$ which are not squares and have period at least 4, one finds

$$\sqrt{14} = \langle 3, \overline{1, 2, 1, 6}\rangle$$
$$\sqrt{21} = \langle 4, \overline{1, 1, 2, 1, 1, 8}\rangle$$
$$\sqrt{22} = \langle 4, \overline{1, 2, 4, 2, 1, 8}\rangle$$
$$\sqrt{28} = \langle 5, \overline{3, 2, 3, 10}\rangle$$
$$\sqrt{32} = \langle 5, \overline{1, 1, 1, 10}\rangle$$
$$\sqrt{33} = \langle 5, \overline{1, 2, 1, 10}\rangle$$
$$\sqrt{34} = \langle 5, \overline{1, 4, 1, 10}\rangle$$
$$\sqrt{44} = \langle 6, \overline{1, 1, 1, 2, 1, 1, 1, 12}\rangle$$
$$\sqrt{45} = \langle 6, \overline{1, 2, 2, 2, 1, 12}\rangle$$
$$\sqrt{46} = \langle 6, \overline{1, 3, 1, 1, 2, 6, 2, 1, 1, 3, 1, 12}\rangle$$
$$\sqrt{52} = \langle 7, \overline{4, 1, 2, 1, 4, 14}\rangle$$
$$\sqrt{54} = \langle 7, \overline{2, 1, 6, 1, 2, 14}\rangle$$
$$\sqrt{55} = \langle 7, \overline{2, 2, 2, 14}\rangle$$
$$\sqrt{57} = \langle 7, \overline{1, 1, 4, 1, 1, 14}\rangle$$
$$\sqrt{58} = \langle 7, \overline{1, 1, 1, 1, 1, 1, 14}\rangle$$
$$\sqrt{60} = \langle 7, \overline{1, 2, 1, 14}\rangle$$
$$\sqrt{62} = \langle 7, \overline{1, 6, 1, 14}\rangle$$
$$\sqrt{69} = \langle 8, \overline{3, 3, 1, 4, 1, 3, 3, 16}\rangle$$
$$\sqrt{70} = \langle 8, \overline{2, 1, 2, 1, 2, 16}\rangle$$
$$\sqrt{74} = \langle 8, \overline{1, 1, 1, 1, 16}\rangle$$
$$\sqrt{75} = \langle 8, \overline{1, 1, 1, 16}\rangle$$
$$\sqrt{76} = \langle 8, \overline{1, 2, 1, 1, 5, 4, 5, 1, 1, 2, 1, 16}\rangle$$
$$\sqrt{77} = \langle 8, \overline{1, 3, 2, 3, 1, 16}\rangle$$
$$\sqrt{78} = \langle 8, \overline{1, 4, 1, 16}\rangle$$
$$\sqrt{85} = \langle 9, \overline{4, 1, 1, 4, 18}\rangle$$
$$\sqrt{86} = \langle 9, \overline{3, 1, 1, 1, 8, 1, 1, 1, 3, 18}\rangle$$
$$\sqrt{88} = \langle 9, \overline{2, 1, 1, 1, 2, 18}\rangle$$
$$\sqrt{91} = \langle 9, \overline{1, 1, 5, 1, 5, 1, 1, 18}\rangle$$
$$\sqrt{92} = \langle 9, \overline{1, 1, 2, 4, 2, 1, 1, 18}\rangle$$
$$\sqrt{94} = \langle 9, \overline{1, 2, 3, 1, 1, 5, 1, 8, 1, 5, 1, 1, 3, 2, 1, 18}\rangle$$
$$\sqrt{95} = \langle 9, \overline{1, 2, 1, 18}\rangle$$
$$\sqrt{96} = \langle 9, \overline{1, 3, 1, 18}\rangle$$
$$\sqrt{98} = \langle 9, \overline{1, 8, 1, 18}\rangle.$$

Continued fractions of $\sqrt{d}$ which have period 3 correspond to $\langle n, \overline{a, a, 2n}\rangle$ for integers $a, n \geq 1$ with $a \neq 2n$; if $\xi = \langle n, \overline{a, a, 2n}\rangle$ and $\alpha = \langle \overline{a, a, 2n}\rangle$, $\beta = \langle \overline{a, 2n, a}\rangle$, $\gamma = \langle \overline{2n, a, a}\rangle$, then $\xi = n + \frac{1}{\alpha}$, $\alpha = a + \frac{1}{\beta}$, $\beta = a + \frac{1}{\gamma}$, and $\gamma = 2n + \frac{1}{\alpha} = \frac{2n\,\alpha+1}{\alpha}$, so that $\beta = a + \frac{\alpha}{2n\,\alpha+1} = \frac{(2n\,a+1)\,\alpha+a}{2n\,\alpha+1}$, $\alpha = a + \frac{2n\,\alpha+1}{(2n\,a+1)\,\alpha+a}$ or $(2n\,a+1)\,\alpha^2 - 2n\,(a^2+1)\,\alpha - (a^2+1) = 0$, hence $\alpha = \frac{n\,(a^2+1)+\sqrt{n^2(a^2+1)^2+(2n\,a+1)\,(a^2+1)}}{2n\,a+1}$, $\frac{1}{\alpha} = \frac{n\,(a^2+1)-\sqrt{n^2(a^2+1)^2+(2n\,a+1)\,(a^2+1)}}{-(a^2+1)}$, and $\xi = \frac{\sqrt{n^2(a^2+1)^2+(2n\,a+1)\,(a^2+1)}}{a^2+1}$. Period 3 then corresponds to $d = n^2 + \frac{2n\,a+1}{a^2+1}$, with a^2+1 dividing $2n\,a+1$, and $a \neq 2n$, so that a must be even; using $a = 2b$ for $b \geq 1$, one must have $4b^2+1$ dividing $4b\,n+1$ and $n > b$, and since $4b$ is relatively prime with b^2+1 it gives $n = b + (4b^2+1)\,k$ for $k \geq 1$, corresponding to the value $d = (b + (4b^2+1)\,k)^2 + 4b\,k + 1$, the only value below 100 being 41.

Lemma 27.27: For an irrational ξ, suppose integers a and b with b positive have the property that $|b\,\xi - a| < |v\,\xi - u|$ for all integers u, v such that $1 \leq v \leq b$ and $\frac{u}{v} \neq \frac{a}{b}$, then $\frac{a}{b}$ is a convergent of the continued fraction expansion of ξ.

[16] If $\xi = \langle n, \overline{a, 2n}\rangle$ and $\alpha = \langle \overline{a, 2n}\rangle$, $\beta = \langle \overline{2n, a}\rangle$, then $\xi = n + \frac{1}{\alpha}$, $\alpha = a + \frac{1}{\beta}$, and $\beta = 2n + \frac{1}{\alpha} = \frac{2n\,\alpha+1}{\alpha}$, so that $\alpha = a + \frac{\alpha}{2n\,\alpha+1}$ or $2n\,\alpha^2 - 2n\,a\,\alpha - a = 0$, hence $\alpha = \frac{n\,a+\sqrt{n^2a^2+2n\,a}}{2n}$, $\frac{1}{\alpha} = \frac{n\,a-\sqrt{n^2a^2+2n\,a}}{-a}$, and $\xi = \frac{\sqrt{n^2a^2+2n\,a}}{a}$.

Suppose integers c and d with d positive have the property that $|d\,\xi - c| < |q_k\xi - p_k|$ (from the continued fraction expansion of ξ), then $d \geq q_{k+1}$.

Suppose integers c and d with d positive have the property that $\left|\xi - \frac{c}{d}\right| < \left|\xi - \frac{p_k}{q_k}\right|$ for $k \geq 1$, then $d > q_k$. *Proof*: Let $c_k = \frac{p_k}{q_k}$ be the kth convergent of ξ. One cannot have $\frac{a}{b} < c_0$, since it implies $|b\,\xi - a| \geq \left|\xi - \frac{a}{b}\right| > |\xi - c_0| = |q_0\xi - p_0|$, because $q_0 = 1$, and this contradicts the hypothesis. By Lemma 27.11 $\left|\xi - \frac{p_k}{q_k}\right| \leq \frac{1}{q_k\,q_{k+1}}$ for $k \geq 0$, so that $|q_0\xi - p_0| \leq \frac{1}{q_1}$, and one cannot have $\frac{a}{b} > c_1$, since it implies $\left|\xi - \frac{a}{b}\right| > \left|\xi - c_1\right|$, so that after multiplication by b one has $|b\,\xi - a| > \frac{|b\,p_1 - a\,q_1|}{q_1} \geq \frac{1}{q_1}$ (because $b\,p_1 - a\,q_1$ is a non-zero integer), so that $|b\,\xi - a| > |q_0\xi - p_0|$, contradicting the hypothesis. There must exist an integer n such that $\frac{a}{b}$ falls between c_{n-1} and c_{n+1} (which are on the same side of ξ, while c_n is on the other side), and one then assumes that it is not one of them (or the result is proved); it follows that $\left|\frac{a}{b} - c_{n-1}\right| < |c_n - c_{n-1}|$, which after multiplication by $b\,q_n q_{n-1}$ gives $q_n|b\,q_{n-1} - a\,p_{n-1}| < b\,|p_n q_{n-1} - p_{n-1}q_n| = b$ (by Remark 27.10), and since $b\,q_{n-1} - a\,p_{n-1}$ is a non-zero integer it implies that $q_n \leq b$. One also has $\left|\frac{a}{b} - \xi\right| > |c_{n+1} - \xi|$,[17] which implies $|b\,\xi - a| > \frac{|b\,p_{n+1} - a\,q_{n+1}|}{q_{n+1}} \geq \frac{1}{q_{n+1}}$, but since it is $\geq |q_n\xi - p_n|$ (by Lemma 27.11) one obtains a contradiction.

Let b be the smallest positive integer such that there exists an integer a such that $|b\,\xi - a| < |q_k\xi - p_k|$, so that one has $b \leq d$; by the first part, it follows that $\frac{a}{b}$ is a convergent of ξ, i.e. $\frac{a}{b} = \frac{p_m}{q_m}$, and one must have $m \geq k+1$, hence $b \geq q_{k+1}$, because convergents are successively closer to ξ: indeed, one has $\xi - \frac{p_k}{q_k} = \frac{(-1)^k}{q_k(\xi_{k+1}q_k + q_{k-1})}$ by Lemma 27.11, which implies $\left|\xi - \frac{p_k}{q_k}\right| \leq \frac{1}{q_k q_{k+1}}$, and then one notices that $\xi_{k+1}q_k + q_{k-1} < q_k(a_{k+1}+1) + q_{k-1} = q_k + q_{k+1} \leq a_{k+2}q_{k+1} + q_k = q_{k+2}$, so that $|q_k\xi - p_k| = \frac{1}{\xi_{k+1}q_k + q_{k-1}} > \frac{1}{q_{k+2}} \geq |q_{k+1}\xi - p_{k+1}|$, which is a stronger inequality than $\left|\xi - \frac{p_k}{q_k}\right| > \left|\xi - \frac{p_{k+1}}{q_{k+1}}\right|$.

If one had $\left|\xi - \frac{c}{d}\right| < \left|\xi - \frac{p_k}{q_k}\right|$ and $d \leq q_k$, then after multiplying by d one would have $|d\,\xi - c| \leq \frac{d}{q_k}\,|q_k\xi - p_k| \leq |q_k\xi - p_k|$, hence $d \geq q_{k+1}$ by the second part, a contradiction since $q_{k+1} > q_k$ for $k \geq 1$ (but one may have $q_1 = q_0 = 1$).

Lemma 27.28: Suppose p and q are positive integers satisfying $\left|\xi - \frac{p}{q}\right| < \frac{1}{2q^2}$ for an irrational ξ, then $\frac{p}{q}$ is a convergent of the continued fraction expansion of ξ.
Proof: Let u and v be integers, with v positive, and such that $|v\,\xi - u| \leq |q\,\xi - p|$ and $\frac{u}{v} \neq \frac{p}{q}$. By the triangle inequality, $\left|\frac{u}{v} - \frac{p}{q}\right| \leq \left|\frac{u}{v} - \xi\right| + \left|\xi - \frac{p}{q}\right|$, and after multiplying by $q\,v$ and using the fact that $q\,u - p\,v$ is a non-zero integer one deduces that $1 \leq |q\,u - p\,v| \leq q\,|v\,\xi - u| + v\,|q\,\xi - p| \leq (q+v)\,|q\,\xi - p| < \frac{q+v}{2q}$, so that $v > q$. One concludes by applying the first part of Lemma 27.27.[18]

Lemma 27.29: Suppose (p, q) is a positive solution of $p^2 - d\,q^2 = \pm 1$, then $\frac{p}{q}$ is a convergent of the continued fraction expansion of $\sqrt{d}$.
Proof: In order to apply Lemma 27.28, one shows that $\left|\sqrt{d} - \frac{p}{q}\right| < \frac{1}{2q^2}$. Because $|p - q\,\sqrt{d}|\,(p + q\,\sqrt{d}) = 1$, one needs to shows that $p + q\,\sqrt{d} > 2q$, and since $p^2 \geq d\,q^2 - 1 \geq (d-1)\,q^2$, one has $p \geq \sqrt{d-1}\,q$, and $\sqrt{d} + \sqrt{d-1} \geq \sqrt{2} + 1 > 2$ for $d \geq 2$.

[17] Since $c_{n-1}, \frac{a}{b}, c_{n+1}, \xi$ are on this order on the real line (either ascending or descending).

[18] The conclusion $v \geq q$ would be enough for applying Lemma 27.27, and it follows from $\left|\xi - \frac{p}{q}\right| \leq \frac{1}{2q^2}$, but it is equivalent to $\left|\xi - \frac{p}{q}\right| < \frac{1}{2q^2}$ since equality would imply that ξ is rational.

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

28- Wednesday November 9, 2011.

Definition 28.1: A *vector space* over a field F (or an *F-vector space*) is an Abelian group for addition $+$ (with identity 0 and inverse of x denoted $-x$), and a *scalar multiplication* (since the elements of F are called *scalars*), which is a mapping from $F \times V$ into V, with the image of (λ, v) denoted $\lambda\, v$, satisfying

$\lambda\,(v_1 + v_2) = \lambda\, v_1 + \lambda\, v_2$ for all $\lambda \in F$ and all $v_1, v_2 \in V$,
$(\lambda_1 + \lambda_2)\, v = \lambda_1 v + \lambda_2 v$ for all $\lambda_1, \lambda_2 \in F$ and all $v \in V$,
$\lambda_1(\lambda_2 v) = (\lambda_1 \lambda_2)\, v$ for all $\lambda_1, \lambda_2 \in F$ and all $v \in V$,
$1\, v = v$ for all $v \in V$,

which imply $\lambda\, 0 = 0$ for all $\lambda \in F$, and $0\, v = 0$ for all $v \in V$.

A *linear mapping* from an F-vector space V_1 into an F-vector space V_2 is a mapping L from V_1 into V_2 such that

$L(v + w) = L(v) + L(w)$ for all $v, w \in V_1$,
$L(\lambda\, v) = \lambda\, L(v)$ for all $\lambda \in F$ and all $v \in V_1$,

and the set $L(V_1; V_2)$ of all linear mappings from V_1 into V_2 is an F-vector space.[1] The *kernel* of a linear mapping L is $L^{-1}(\{0\}) = \{v_1 \in V_1 \mid L(v_1) = 0\} \subset V_1$, and the *range* of L is the image $\{L(v_1) \mid v_1 \in V_1\} \subset V_2$. For an F-vector space V, the *general linear group* $GL(V)$ is the multiplicative group of all *invertible linear mappings* from V into itself.[2]

A *bilinear mapping* B from $V_1 \times V_2$ into V_3, where V_1, V_2, V_3 are F-vector spaces, is a mapping such that $v_1 \mapsto B(v_1, v_2)$ is linear (from V_1 into V_3) for all $v_2 \in V_2$ and $v_2 \mapsto B(v_1, v_2)$ is linear (from V_2 into V_3) for all $v_1 \in V_1$.

Examples 28.2: If I is non-empty and for each $i \in I$ one is given an F-vector space V_i, then the product $\prod_{i \in I} V_i$ has a natural structure of F-vector space.[3] A particular case is when all V_i are equal to an F-vector space W, which corresponds to considering the (F-vector space of) mappings from I into W; this example is encountered with $W = F$ and $I = \mathbb{N}$ in the case of the ring of formal power series $F[[x]]$. Other F-vector spaces already encountered are the ring of polynomials $F[x]$, the ring of formal Laurent series $F((x))$, as well as any quotient ring $F[x]/(P_0)$ for some $P_0 \in F[x]$.

In the case P_0 is an irreducible polynomial of degree n, then $K = F[x]/(P_0)$ is a field, and as an F-vector space it is isomorphic to F^n, since each coset $P + (P_0)$ corresponds to $r + (P_0)$ where $r = a_0 + \ldots + a_{n-1} x^{n-1}$ is the remainder in the Euclidean division of P by P_0, and $a_0, \ldots, a_{n-1}$ may be chosen independently in F.

$F[x]$, $F[x]/(P_0)$, $F[[x]]$, and $F((x))$ also have a multiplication, and they are particular cases of an F-vector space V having a product given by a bilinear mapping from $V \times V$ into V, in which case V is called an *algebra* over F.

Remark 28.3: If R is a ring but not a field, one has a similar notion of R-module, or more precisely of left R-module and right R-module in the case where R is not commutative, and the structure of modules is not as simple of that of vector spaces, in particular because one cannot define a notion of dimension, or use a basis as for a vector space. However, if D is a division ring, then the properties of a D-module are exactly similar to that of a vector space.

Definition 28.4: If V is an F-vector space, a *linear combination* of elements of a non-empty subset $A \subset V$ is any element of the form $\sum_{i=1}^{n} \lambda_i a_i$ with $a_1, \ldots, a_n \in A$ and $\lambda_1, \ldots, \lambda_n \in F$; *span*$(A) = \{\sum_{i=1}^{n} \lambda_i a_i \mid n \in \mathbb{N}^\times, a_1, \ldots, a_n \in A, \lambda_1, \ldots, \lambda_n \in F\}$ is the vector *subspace generated by A*. Distinct elements $a_1, \ldots, a_n \in V$ are *linearly dependent* if $\sum_{i=1}^{n} \lambda_i a_i = 0$ and not all λ_i are equal to 0; a non-empty subset $A \subset V$ is *linearly*

[1] If $L_1, L_2 \in L(V_1; V_2)$, then $L_1 + L_2$ is the mapping $v \mapsto L_1(v) + L_2(v)$ for all $v \in V_1$, and for $\lambda \in F$, $\lambda\, L_1$ is the mapping $v \mapsto \lambda\, L_1(v)$ for all $v \in V_1$.

[2] Notice that $GL(V)$ is not a vector space. It is a pointed cone in the vector space $L(V; V)$, i.e. one can multiply an element $A \in GL(V)$ by $\lambda \in F^*$, but 0 is not allowed.

[3] If $a = (a_i, i \in I), b = (b_i, i \in I) \in \prod_{i \in I} V_i$, and $\lambda \in F$, then $c = a + b$ and $d = \lambda\, a$ are the elements of $\prod_{i \in I} V_i$ defined by $c_i = a_i + b_i$, $d_i = \lambda\, a_i$ for all $i \in I$.

independent if no non-empty finite subset of A is linearly dependent, i.e. if $n \geq 1$ and $\sum_{i=1}^{n} \lambda_i a_i = 0$ for distinct elements $a_1, \ldots, a_n \in A$ imply $\lambda_i = 0$ for $i = 1, \ldots, n$. A *basis* of an F-vector space V is a linearly independent set which spans V.

Lemma 28.5: If V is an F-vector space, and $v_1, \ldots, v_n \in V$ for $n \geq 1$, then any $n+1$ (or more) vectors in $span(v_1, \ldots, v_n)$ are linearly dependent.
Proof: One first checks the case $n = 1$, i.e. one considers two vectors, $w_1 = \alpha\, v_1, w_2 = \beta\, v_1$ for some $\alpha, \beta \in F$: since $\beta\, w_1 - \alpha\, w_2 = 0$, it proves linear dependence if α or β is non-zero, but if $\alpha = \beta = 0$ then $w_1 = w_2 = 0$ and any of the two vectors is linearly dependent (since $1\, w_j = w_j = 0$).

One proves the general case by induction on n: one assumes that $n \geq 2$ and that the result is proved for a number of vectors $\leq n-1$, and one chooses $w_1, \ldots, w_{n+1}$ which are linear combinations of $v_1, \ldots, v_n$, i.e. one writes $w_j = \sum_{i=1}^{n} \lambda_{j,i} v_i$ for some $\lambda_{j,i} \in F, i = 1, \ldots, n, j = 1, \ldots, n+1$; if all $\lambda_{j,n}$ are 0, then $span(v_1, \ldots, v_n) = span(v_1, \ldots, v_{n-1})$, and the induction hypothesis applies; if $\lambda_{j_0,n} \neq 0$, then for $j \neq j_0$ one considers the vectors $z_j = w_j - \lambda_{j_0,n}^{-1} \lambda_{j,n} w_{j_0}$ for $j \neq j_0$, which are linear combinations of $v_1, \ldots, v_{n-1}$, hence the induction hypothesis applies and there exist $\mu_j \in F$ for $j \neq j_0$, not all equal to 0, and such that $\sum_{j \neq j_0} \mu_j z_j = 0$, so that it means $\sum_j \mu_j w_j = 0$ if one defines $\mu_{j_0} = -\sum_{j \neq j_0} \lambda_{j_0,n}^{-1} \lambda_{j,n} \mu_j$, and since not all μ_j are 0 the w_j are linearly dependent.

Definition 28.6: An F-vector space V is *finite-dimensional* if it is generated by finitely many elements, and its *dimension* is the number of elements in a basis (indeed independent of the basis by Lemma 28.5).

Remark 28.7: Every F-vector space V has a basis, because a basis is a maximal family of linearly independent vectors $\{e_i \mid i \in I\}$, since if $W = span(e_i, i \in I)$ was different from V, adding to the family $e_i, i \in I$ any element in $V \setminus W$ would contradict the maximality; then such a maximal family exists by a simple application of "Zorn's lemma". If $f_j, j \in J$ is another basis, then I and J have the same cardinal, even in the case where I (and then J by Lemma 28.5) is infinite: for $i \in I$, e_i can be expressed as a linear combination of the f_j, with non-zero coefficient for $j \in A(i)$, but since $i' \neq i$ could have $A(i') = A(i)$, one puts a total order on I (for example a well order by Zermelo's theorem), and one denotes $\alpha(i)$ the order of i in the set $A^{-1}\big(A(i)\big)$ of indices i' having the same image than i (noticing that this set is finite and has a number of element at most that of $A(i)$ by Lemma 28.5); then the mapping $i \mapsto \big(\alpha(i), A(i)\big)$ is injective from I into $\mathbb{N} \times \mathcal{P}_{finite}(J)$, where $\mathcal{P}_{finite}(J)$ denotes the set of finite subsets of J, and since for J infinite $\mathcal{P}_{finite}(J)$ has the same cardinal than J, and $\mathbb{N} \times J$ has the same cardinal than J, one deduces that $cardinal(I) \leq cardinal(J)$; reversing the roles gives $cardinal(J) \leq cardinal(I)$, hence $cardinal(J) = cardinal(I)$ by the Schröder–Bernstein theorem.[4,5]

Definition 28.8: The *prime subfield* F_0 of a field F is the subfield generated by 0 and 1. If F has *characteristic* 0, the prime subfield is isomorphic to $\mathbb{Q}$, and if F has finite characteristic, necessarily a prime p, then the prime subfield is isomorphic to $\mathbb{Z}_p$.

If E is a subfield of F, one says that F is an *extension field* of E, or that F/E is a *field extension*. F is an E-vector space, whose dimension is denoted $[F:E]$, and F is called a *finite-dimensional extension* (or a *finite extension*) if $[F:E] < \infty$, and an *infinite-dimensional extension* (or *infinite extension*), if $[F:E] = \infty$.

Lemma 28.9: If F is a finite field, then $|F| = p^k$ for a prime p (the characteristic of F) and a positive integer k.
Proof: Let F_0 be the prime subfield of F, isomorphic to $\mathbb{Z}_p$ for the characteristic p of F. Then F is an F_0-vector space, necessarily of finite dimension k, so that F is isomorphic to F_0^k as F_0-vector spaces.

Remark 28.10: It can be shown that, for each prime p and each $k \geq 1$, there is only one finite field with $q = p^k$ elements, up to isomorphism (as fields), and one denotes it F_q.

---

[4] Friedrich Wilhelm Karl Ernst Schröder, German mathematician, 1841–1902. He worked in Darmstadt, and in Karlsruhe, Germany. The Schröder–Bernstein theorem is partly named after him (Cantor stated it without giving a proof, which Bernstein provided in 1898, and Schröder obtained it independently the same year).

[5] Felix Bernstein, German mathematician, 1878–1956. He worked at Georg-August-Universität, Göttingen, Germany. The Schröder–Bernstein theorem is partly named after him (Cantor stated it without giving a proof, which Bernstein provided in 1898, and Schröder obtained it independently the same year).

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

29- Friday November 11, 2011.

Definition 29.1: If F is a field extension of E, $a \in F$ is called *algebraic* over E if (and only if) there exists a non-zero $P \in E[x]$ with $P(a) = 0$, and it is said to be algebraic of *order* d if d is the smallest degree of such a polynomial P ($d = 1$ corresponding to elements of E). It a is not algebraic, it is called *transcendental* over E. F is called an *algebraic extension* if all its elements are algebraic over E.

If $A \subset F$ ($A \neq \emptyset$), then $E[A]$ denotes the smallest subring of F containing E and A, and $E(A)$ denotes the smallest subfield of F containing E and A, and for $A = \{a_1, \ldots, a_m\}$, one writes $E[a_1, \ldots, a_m]$ for $E[A]$, and $E(a_1, \ldots, a_m)$ for $E(A)$.

Remark 29.2: The notation $E[x]$ for polynomials with coefficients in E is consistent, by taking $F = E(x)$, the field of fractions of $E[x]$.

Since the ring $E[a_1, \ldots, a_m]$ must contain all monomials in $a_1, \ldots, a_m$, as well as sums of such monomials, it must contain $\{P(a_1, \ldots, a_m) \mid P \in E[x_1, \ldots, x_n]\}$, but this set is a ring, so that it coincides with $E[a_1, \ldots, a_m]$.

Then, $E(a_1, \ldots, a_m)$ is the field of fractions of $E[a_1, \ldots, a_m]$, i.e. $\big\{P(a_1, \ldots, a_m)\big(Q(a_1, \ldots, a_m)\big)^{-1} \mid P, Q \in E[x_1, \ldots, x_n], Q(a_1, \ldots, a_m) \neq 0\big\}$.

It may happen that $E[A]$ is actually a field, which then coincides with $E(A)$. For example, if $a \in F$, then $E[a]$ is a field if and only if a is algebraic over E: if $a \neq 0$ has an inverse, it should be $P(a)$ for some $P \in E[x]$, and $a^{-1} = P(a)$ implies $Q(a) = 0$ with $Q = x\,P - 1$; conversely if $a \neq 0$ is algebraic of degree $d \geq 2$ (since $d = 1$ gives $a \in E$, and $E[a] = E$), one has $a^d = c_0 + c_1 a + \ldots + c_{d-1} a^{d-1}$, and one proves easily by induction that a^n is an E-linear combination of $1, a, \ldots, a^{d-1}$ for all $n \geq d$; for proving the same result for $n < 0$, it suffices to show it for a^{-1}, but since $a\,(a^{d-1} - c_1 - \ldots - c_{d-1} a^{d-2}) = c_0$ and $c_0 \neq 0$ (or the degree of a would be $< d$) one has $a^{-1} = c_0^{-1}(a^{d-1} - c_1 - \ldots - c_{d-1} a^{d-2})$.

Remark 29.3: A finite extension is automatically algebraic: if $[F : E] = m$, then for any $a \in F$, the elements $1, a, \ldots, a^m$ are $m + 1$ elements in an E-vector space of dimension m, so that they are E-linearly dependent, i.e. $\sum_{j=0}^{m} \lambda_j a^j = 0$ with $\lambda_0, \ldots, \lambda_m \in E$ not all 0, which means that the non-zero polynomial $P = \lambda_0 + \lambda_1 x + \ldots + \lambda_m x^m \in E[x]$ has degree $\leq m$ and satisfies $P(a) = 0$.

There are infinite extensions which are algebraic, and for example the real numbers which are algebraic over $\mathbb{Q}$ form a field $A_{\mathbb{R}}$ such that $[A_{\mathbb{R}} : \mathbb{Q}] = +\infty$; the complex numbers which are algebraic over $\mathbb{Q}$ form a field $A_{\mathbb{C}}$ and $[A_{\mathbb{C}} : A_{\mathbb{R}}] = 2$, since $A_{\mathbb{C}} = A_{\mathbb{R}}[\sqrt{-1}]$.

However, a *finitely generated extension* (i.e. $F = E(A)$ for a non-empty finite set A) is not necessarily algebraic: for example, $F(x)$ is generated by x, but x is transcendental over F.

Remark 29.4: In the beginning, the case considered for algebraic or transcendental numbers was $E = \mathbb{Q}$ and $F = \mathbb{R}$ (or $\mathbb{C}$), and the definition of transcendental numbers seems due to EULER, but LIOUVILLE seems to have been the first to prove (in 1844) that they exist,[1] and in 1851 he showed an explicit way to construct some real numbers which are transcendental, like $\sum_{k \in \mathbb{N}} 10^{-k!}$ (or more generally $\sum_{k \in \mathbb{N}} 10^{-f(k)}$ if $f(k)$ tends to $+\infty$ fast enough as k tends to $+\infty$), as a consequence of his observation that if ξ is algebraic of order $d \geq 2$, then there exists a constant C such that for each positive integer n, the distance of ξ to the rationals of the form $\frac{a}{n}$ ($a \in \mathbb{Z}$) is $\geq \frac{C}{n^d}$.[2]

CANTOR observed in 1874 that the set of algebraic numbers is infinite and countable (since $\mathbb{Z}[x]$ is countable), and in 1878 he proved that there are as many transcendental numbers as real numbers, so that it became useless to construct just a few transcendental numbers.

---

[1] Joseph LIOUVILLE, French mathematician, 1809–1882. He held a chair at Collège de France (mathématiques, 1851–1882) in Paris, France.

[2] Since $P(\xi) = 0$ and $P'(\xi) \neq 0$, the ratio $\frac{P(x)}{|x - \xi|}$ is bounded above by $C_1 > 0$ if $x \in (\xi - 1, \xi + 1)$; then, using the fact that $P \in \mathbb{Z}[x]$ and that $n^d P\big(\frac{a}{n}\big)$ is a non-zero integer, one has $1 \leq \big|n^d P\big(\frac{a}{n}\big)\big| \leq C_1 n^d \big|\xi - \frac{a}{n}\big|$ if $\frac{a}{n} \in (\xi - 1, \xi + 1)$, hence taking the minimum over $a \in \mathbb{Z}$ one has the desired property with $C = \frac{1}{C_1}$.

In 1761, LAMBERT had proved that π is irrational and conjectured that π and e are transcendental: HERMITE proved in 1873 that e is transcendental, and by a small technical improvement of his method, using $e^{i\pi} = -1$, LINDEMANN proved in 1882 that π is transcendental,[3] which implied that squaring the circle is impossible (i.e. one cannot construct π with straightedge and compass).

Lemma 29.5: If F is a field extension of E, $[F:E] = 1$ if and only if $F = E$.

If E_2 is a field extension of E_1 and E_3 is a field extension of E_2, then E_3 is a field extension of E_1 and $[E_3:E_1] = [E_3:E_2]\,[E_2:E_1]$; in particular, $[E_2:E_1]$ divides $[E_3:E_1]$ if $[E_3:E_1] < \infty$.

Proof: If $F \neq E$, then 1 is not a basis of F considered as an E-vector space, so that $[F:E] > 1$.

If $\{a_i, i \in I\}$ is a basis of E_2 as an E_1-vector space, and $\{b_j, j \in J\}$ is a basis of E_3 as an E_2-vector space, then $\{c_{i,j} = a_i b_j \mid (i,j) \in I \times J\}$ is a basis of E_3 as an E_1-vector space: one first notices that $\{c_{i,j} \mid (i,j) \in I \times J\}$ is an E_1-linearly independent set, since if (for a finite sum) $\sum_{(i,j)\in I\times J} \lambda_{i,j} a_i b_j = 0$ with $\lambda_{i,j} \in E_1$ for all $(i,j) \in I \times J$, then, writing $\mu_j = \sum_{i\in I} \lambda_{i,j} a_i \in E_2$ for all $j \in J$, it means $\sum_{j\in J} \mu_j b_j = 0$, so that $\mu_j = 0$ for all $j \in J$, and then $\sum_{i\in I} \lambda_{i,j} a_i = 0$ implies $\lambda_{i,j} = 0$ for all $i \in I$; one then notices that $\{c_{i,j} \mid (i,j) \in I \times J\}$ is a set of generators of E_3 as an E_1-vector space, since any $v \in E_3$ can be written as an E_2-linear combination $v = \sum_{j\in J} \beta_j b_j$ with $\beta_j \in E_2$ for all $j \in J$, and then each β_j can be written as an E_1-linear combination $\beta_j = \sum_{i\in I} \alpha_{i,j} a_i$ with $\alpha_{i,j} \in E_1$ for all $i \in I$, so that $v = \sum_{(i,j)\in I\times J} \alpha_{i,j} a_i b_j$.

Remark 29.6: Lemma 29.5 permits to settle two other (and simpler) questions concerning constructions with straightedge and compass, the duplication of the cube (i.e. constructing $\sqrt[3]{2}$), and the trisection of an angle (i.e. constructing $\cos\frac{\theta}{3}$ in terms of $\cos\theta$ for any angle θ). GAUSS had stated that they were impossible, but without publishing a proof, which was supplied in 1837 by WANTZEL.

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, and for what concerns later constructions, the basic observation is that, since one starts with two points at distance 1, the points of the plane which can be constructed by straightedge and compass have their coordinates in various field extensions of $\mathbb{Q}$, whose dimensions over $\mathbb{Q}$ are powers of 2. Indeed, the intersection of two (non-parallel) lines whose equations have coefficients in a field extension K_n of $\mathbb{Q}$ requires solving a linear system with coefficients in K_n, and it gives an intersection point with coordinates in K_n; however, if a line intersects a circle or if two circles intersect and their equations have coefficients in K_n, then one has to compute the two square roots of an element of K_n, which may exist in K_n or may require the introduction of a field extension K_{n+1} of K_n with $[K_{n+1}:K_n] = 2$; since one starts with $K_1 = \mathbb{Q}$, all the fields involved then have a dimension over $\mathbb{Q}$ which is a power of 2 by Lemma 29.5.

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 a field extension of $\mathbb{Q}$ of dimension 3, which by Lemma 29.5 can only be included in a finite field extension of $\mathbb{Q}$ it its dimension over $\mathbb{Q}$ is a multiple of 3, which is not the case for powers of 2.

That the trisection of an angle like $60°$ is impossible is done in a similar way, by noticing that $\cos 20°$ is a root of an irreducible polynomial $P \in \mathbb{Q}[x]$ of degree 3. By De Moivre's formula,[4] $\cos 3\theta = \cos^3\theta - 3\cos\theta\sin^2\theta = 4\cos^3\theta - 3\cos\theta$, and since one then wants to solve $4\cos^3 20° - 3\cos 20° = \frac{1}{2}$, it remains to show that $P = 8x^3 - 6x - 1$ is an irreducible polynomial in $\mathbb{Q}[x]$,[5] equivalent to showing that it has no root in $\mathbb{Q}$ (since it has degree ≤ 3): if $\frac{a}{b}$ is a root of P with $a, b \in \mathbb{Z}, b \neq 0$ and $(a,b) = 1$, then $8a^3 - 6a\,b^2 - b^3 = b^3 P\left(\frac{a}{b}\right) = 0$, so that a divides 1 and b^2 divides 8, but $a = 1$ and $b = \pm 1, \pm 2$ does not work.

[3] Carl Louis Ferdinand VON LINDEMANN, German mathematician, 1852–1939. He worked in Freiburg, in Königsberg (then in Germany, now Kaliningrad, Russia), and in München (Munich), Germany.

[4] Abraham DE MOIVRE, French-born mathematician, 1667–1754. He moved to London, England, but could not obtain an academic position

[5] In the 11th century, AL BIRUNI had noticed that constructing a regular polygon with 9 sides (enneagon) is related to the solution of a third degree equation, and this was rediscovered by VIÈTE in the 16th century, and since it corresponds to finding $\cos 40°$, their equation was $8x^3 - 6x + 1 = 0$.

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

30- Monday November 14, 2011.

Remark 30.1: ANAXAGORAS was the first to consider squaring the circle with straightedge and compass,[1] although the question of approximating the area of a disc by the area of a square appears in the "Rhind Papyrus",[2] also named the Ahmes Papyrus,[3] after the ancient Egyptian scribe who copied (around 1650 BCE) an earlier work from about 2000 BCE, where one approximates π by $\frac{16^2}{9^2}$ (≈ 3.16).[4]

Remark 30.2: EUCLID certainly knew how to double the number of sides of a regular polygon, since bisecting an angle is easily done with straightedge and compass, and he constructed regular polygons with 3 sides (triangle), 4 sides (square), 5 sides (pentagon), or 15 sides (pentadecagon).

The construction of an equilateral triangle corresponds to computing $\xi = e^{2i\,\pi/3}$, which solves $\xi^3 = 1$, but since $\xi \neq 1$ one has $P(\xi) = 0$ with $P = x^2 + x + 1$, whose roots are ξ and ξ^2 ($= \overline{\xi} = \frac{1}{\xi}$). Instead of using the explicit formula for the roots, one divides by ξ and one considers the equation for $\eta = \xi + \frac{1}{\xi}$ (which is $\xi + \overline{\xi} = 2\cos\frac{2\pi}{3}$), and the equation becomes $\eta + 1 = 0$: it gives $\cos\frac{2\pi}{3} = -\frac{1}{2}$, from which one deduces $\sin\frac{2\pi}{3} = \frac{\sqrt{3}}{2}$. It is not difficult to deduce a geometric construction.

The construction of a regular pentagon corresponds to computing $\xi = e^{2i\,\pi/5}$, which solves $\xi^5 = 1$, but since $\xi \neq 1$ one has $P(\xi) = 0$ with $P = x^4 + x^3 + x^2 + x + 1$, whose roots are ξ, ξ^2, ξ^3 ($= \overline{\xi^2} = \frac{1}{\xi^2}$), and ξ^4 ($= \overline{\xi} = \frac{1}{\xi}$). One divides by ξ^2 and one considers the equation for $\eta = \xi + \frac{1}{\xi}$ (which is $\xi + \overline{\xi} = 2\cos\frac{2\pi}{5}$), and since $\eta^2 = \xi^2 + \frac{1}{\xi^2} + 2$, the equation becomes $\eta^2 + \eta - 1 = 0$, whose roots are $2\cos\frac{2\pi}{5}$ and $2\cos\frac{4\pi}{5}$: it gives $\cos\frac{2\pi}{5} = \frac{-1+\sqrt{5}}{4}$ and $\cos\frac{4\pi}{5} = \frac{-1-\sqrt{5}}{4}$, from which one deduces $\sin\frac{2\pi}{5} = \frac{\sqrt{10+2\sqrt{5}}}{4}$ and $\sin\frac{4\pi}{5} = \frac{\sqrt{10-2\sqrt{5}}}{4}$. It is not difficult to deduce a geometric construction.

One can then deduce $\cos\frac{2\pi}{15}$ by trigonometry, since $\frac{2\pi}{15} = 2\,\frac{2\pi}{5} - \frac{2\pi}{3}$, but geometrically, EUCLID probably drew on the same circle a regular (equilateral) triangle and a regular pentagon with a common vertex at angle $\theta = 0$, and noticed that there are vertices at angles $\frac{2\pi\,k}{15}$ with $k = 0, 5, 10$ for the triangle and $k = 0, 3, 6, 9, 12$ for the pentagon, so that between $k = 5, 6$ or $k = 9, 10$ one can measure the side of the regular pentadecagon. More generally, if one knows how to construct a regular polygon with m sides and a regular polygon with n sides, one can deduce a way to construct a regular polygon whose number of sides is the least common multiple ℓ of m and n, since with a common vertex at angle $\theta = 0$ one has vertices at angles $\frac{2\pi\,k}{\ell}$ with either k a multiple of $a = \frac{\ell}{m}$ or a multiple of $b = \frac{\ell}{n}$, and one can find $\alpha \in \{1, \ldots, m-1\}$ and $\beta \in \{1, \ldots, n-1\}$ such that $|a\,\alpha - b\,\beta| = 1$, because $(a, b) = 1$.

Remark 30.3: One had to wait until 1796 for a new step, when GAUSS (who was 19 years old) showed that a regular polygon with 17 sides (heptadecagon) can be constructed with straightedge and compass. He may have extended the previous algebraic computations to the polynomial $1 + x + \ldots + x^{16}$ as follows.

---

[1] ANAXAGORAS of Clazomenae, Ionian-born Greek mathematician, 499 BCE–428 BCE. He worked in Athens, Greece, and then in Lampsacus, Ionia (now in Turkey).

[2] Alexander Henry RHIND, Scottish lawyer and Egyptologist, 1833–1863. The "Rhind Papyrus" (which he acquired in 1858 in Luxor, Egypt) is named after him, but also called the Ahmes Papyrus, after its Egyptian scribe.

[3] AHMES, Egyptian scribe, about 1680 BCE–1620 BCE. He copied the "Rhind Papyrus".

[4] It approximates the surface of a disc of diameter D by that of a square of side $\frac{8D}{9}$, so that ancient Egyptians were looking for a rational approximation of $\frac{\sqrt{\pi}}{2}$, which is approximately 0.886226925. The continued fraction expansion of $\frac{\sqrt{\pi}}{2}$ is $\langle 0, 1, 7, 1, 3, 1, \ldots \rangle$ (since $\frac{1}{0.886226925} \approx 1.12837917$, $\frac{1}{0.12837917} \approx 7.78942565$, $\frac{1}{0.78942565} \approx 1.26674374$, $\frac{1}{0.26674374} \approx 3.74891647$, $\frac{1}{0.74891647} \approx 1.3352624$); the approximation $\langle 0, 1, 7 \rangle = \frac{7}{8}$ is exactly 0.87500000 (an error below of around $11.2\,10^{-3}$), the next approximation $\langle 0, 1, 7, 1 \rangle = \frac{8}{9}$ is approximately 0.888888889 (an error above of around $2.6\,10^{-3}$), and the following approximation $\langle 0, 1, 7, 1, 3 \rangle = \frac{31}{35}$ is approximately 0.885714286 (an error below of around $0.5\,10^{-3}$).

For $z = e^{2i\,\pi/17}$, let $A = z + z^2 + z^4 + z^8 + z^{16} + z^{32} + z^{64} + z^{128} = z + z^2 + z^4 + z^8 + z^9 + z^{13} + z^{15} + z^{16}$ (using $z^{17} = 1$, and noticing that $z^{256} = z$ since $2^8 = 256 = 16^2 = 17 \cdot 15 + 1$), and let A' be the sum of the other positive powers of z, i.e. $A' = z^3 + z^5 + z^6 + z^7 + z^{10} + z^{11} + z^{12} + z^{14}$, so that $A + A' + 1 = 0$. If one shows that $A\,A' = -4$, one deduces that A and A' are the solutions of $X^2 + X - 4 = 0$, but we shall check directly that $A^2 + A = 4$, and the second root being $-A - 1$ it is A'.

Let $B = z + z^4 + z^{16} + z^{64} = z + z^4 + z^{13} + z^{16}$, and $B' = z^2 + z^8 + z^{32} + z^{128} = z^2 + z^8 + z^9 + z^{15}$, so that $B + B' = A$, and one checks easily that $B\,B' = \sum_{k=1}^{16} z^k = -1$, so that B and B' are the solutions of $X^2 - A\,X - 1 = 0$.

In developing B^2, one finds that the sum of squares is B' and the double products give $2(2 + C)$ with $C = z^3 + z^5 + z^{12} + z^{14}$; in developing $(B')^2$, one finds that the sum of squares is B and the double products give $2(2 + C')$ with $C' = z^6 + z^7 + z^{10} + z^{11}$. Since $C + C' = A' = -A - 1$, one deduces that $A^2 = B^2 + (B')^2 + 2B\,B' = \big(B' + 2(2 + C)\big) + \big(B + 2(2 + C')\big) - 2 = A + 6 + 2(-A - 1) = -A + 4$.

A and A' being the solutions of $X^2 + X - 4 = 0$, one has $A = \frac{-1+\sqrt{17}}{2}$ and $A' = \frac{-1-\sqrt{17}}{2}$ because $A > 0$.[5]

B and B' being the solutions of $X^2 - A\,X - 1 = 0$, one has $B = \frac{A+\sqrt{A^2+4}}{2}$ and $B' = \frac{A-\sqrt{A^2+4}}{2}$ because $B > 0$:[6] one has $4(A^2+4) = (-1+\sqrt{17})^2 + 16 = 34 - 2\sqrt{17}$, and $4((A')^2+4) = (1+\sqrt{17})^2 + 16 = 34 + 2\sqrt{17}$, so that $4B = -1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}}$, hence $16B^2 = 52 - 4\sqrt{17} - 2\sqrt{34 - 2\sqrt{17}} + 2\sqrt{17}\,\sqrt{34 - 2\sqrt{17}}$.

One checks easily that $C\,C' = \sum_{k=1}^{16} z^k = -1$, so that C and C' are the roots of $X^2 - A'\,X - 1$, i.e. $C = \frac{A'+\sqrt{(A')^2+4}}{2}$, and $C' = \frac{A'-\sqrt{(A')^2+4}}{2}$,[7] so that $4C = -1 - \sqrt{17} + \sqrt{34 + 2\sqrt{17}}$.

Let $D = z + z^{16}$ and $D' = z^4 + z^{13}$, so that $D + D' = B$, and one checks easily that $D\,D' = C$, so that D and D' are the roots of $X^2 - B\,X + C$, i.e. $D = \frac{B+\sqrt{B^2-4C}}{2}$ and $D' = \frac{B-\sqrt{B^2-4C}}{2}$.[8] Since $D = 2\cos\frac{2\pi}{17}$, one has $16\cos\frac{2\pi}{17} = 4B + \sqrt{16B^2 - 64C}$, and $16B^2 - 64C = 68 + 12\sqrt{17} - 2\sqrt{34 - 2\sqrt{17}} - 16\sqrt{34 + 2\sqrt{17}} + 2\sqrt{17}\,\sqrt{34 - 2\sqrt{17}}$; if one notices that $\sqrt{17}\,\sqrt{34 - 2\sqrt{17}} = 4\sqrt{34 + 2\sqrt{17}} - \sqrt{34 - 2\sqrt{17}}$, which by putting $\sqrt{2\sqrt{17}}$ in factor, is the same as $\sqrt{17}\,\sqrt{\sqrt{17} - 1} = 4\sqrt{\sqrt{17} + 1} - \sqrt{\sqrt{17} - 1}$, itself a particular case (for $a = 4$) of the identity[9,10]

$$\sqrt{a^2+1}\,\sqrt{\sqrt{a^2+1} - 1} = a\sqrt{\sqrt{a^2+1} + 1} - \sqrt{\sqrt{a^2+1} - 1} \text{ for all } a \in \mathbb{R}, a > 0,$$

one deduces that $16B^2 - 64C = 68 + 12\sqrt{17} - 4\sqrt{34 - 2\sqrt{17}} - 8\sqrt{34 + 2\sqrt{17}}$, hence

$$16\cos\frac{2\pi}{17} = -1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} + 2\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}.$$

Remark 30.4: In 1797, MASCHERONI proved that any geometric construction which can be done with straightedge and compass can be done with compass alone, and one now calls this result the Mohr–Mascheroni theorem, because one discovered afterward (in 1928) that it appeared in a book by MOHR, printed in 1672.

In 1801, GAUSS published a book (which he had finished writing in 1798) in Latin, Disquisitiones Arithmeticae, where (among other things) he proved a sufficient condition for a regular polygon with n sides to be constructed with straightedge and compass, that n is a power of 2 multiplied by a product of different

[5] Only z^8 and z^9 have negative real part, and z, z^2, z^{15}, z^{16} have their argument in $\big(-\frac{\pi}{4}, +\frac{\pi}{4}\big)$ so that the sum of their real parts is $> 4\,\frac{\sqrt{2}}{2} = 2\sqrt{2} > 2$, implying $A > 0$.

[6] Since z, z^4, z^{13}, z^{16} have positive real parts, one has $B > 0$.

[7] Since the sum of the real parts of z^3 and z^5 is > 0, one has $C > 0$.

[8] Since $\Re(z) > \Re(z^4) > 0$, one has $D > D' > 0$.

[9] With $b^2 = a^2 + 1$, it means $b\sqrt{b-1} = a\sqrt{b+1} - \sqrt{b-1}$, or $(b+1)\sqrt{b-1} = a\sqrt{b+1}$, equivalent to comparing the squares $(b+1)^2\,(b-1) = a^2(b+1)$, which is true because $a^2 = (b+1)\,(b-1)$.

[10] I followed an exercise in a book for making these computations (in the Spring of 2010), but since it is easy to make mistakes in long computations, I checked if the value appeared on the Internet, and the form there was different from mine. I carefully checked my computations, but I could not find anything wrong, so that I guessed that the two forms gave the same value, and this is how I discovered this identity.

Fermat primes, and he must have understood the small piece of Galois theory which he needed (more than ten years before GALOIS was born). Although GAUSS also stated that it is a necessary condition for the construction to be possible, he never published a proof.

In 1822, PONCELET conjectured that any geometric construction which can be done with straightedge and compass can be done with straightedge alone, if one is given a circle and its center,[11] and in 1833 STEINER proved this conjecture,[12] which one calls the Poncelet–Steiner theorem.

In 1837, WANTZEL proved GAUSS's conjecture, and he could rely on Galois theory, in the case of a *cyclotomic extension*, which consists in adding $e^{2i\pi/n}$ to $\mathbb{Q}$, and his result follows from the fact that $[\mathbb{Q}(e^{2i\pi/n}):\mathbb{Q}] = \varphi(n)$ (for the Euler function φ), using the remark that $\varphi(n)$ is a power of 2 if and only if n is a power of 2 times a product of different Fermat primes: the sufficient condition follows from the fact that φ is a multiplicative function, so that if $n = 2^m p_1 \cdots p_r$ for distinct Fermat primes $p_1, \ldots, p_r$, then $\varphi(n) = \varphi(2^m)\,\varphi(p_1)\cdots\varphi(p_r) = 2^{m-1}(p_1-1)\cdots(p_r-1)$, which is a power of 2, since $p-1$ is a power of 2 for every Fermat prime p; conversely, if $\varphi(n)$ is a power of 2 and n contains an odd prime p to a power k, then $\varphi(n)$ is a multiple of $\varphi(p^k) = p^{k-1}(p-1)$, which can only be a power of 2 if $k = 1$ and $p - 1 = 2^\ell$, but if $2^\ell + 1$ is prime, then ℓ is a power of 2.

Definition 30.5: If E is a field and $Q \in E[x]$, one says that Q *splits over* E if (and only if) it is a product of linear factors (i.e. of degree 1). For $P \in E[x]$, a field extension F of E is called a *splitting field extension for* P *over* E if (and only if)

i) P splits over F

ii) F is generated by E and the roots $a_1, \ldots, a_n$ of P, which one writes as $F = E(a_1, \ldots, a_n)$.

Example 30.6: Let $E_1 = \mathbb{Q}$ and $E_2 = \mathbb{Q}[\sqrt{2}]$, so that $[E_2 : E_1] = 2$. One wants to add $\sqrt{3}$, so that one wonders if $E_3 = E_2[\sqrt{3}]$ coincides with E_2 or if it has degree 2 over E_2, hence degree 4 over E_1. Of course $E_3 = E_2[\sqrt{3}]$ means $E_3 = E_2[x]/(x^2-3)$, so that the question can be reformulated as: is $x^2 - 3$ irreducible in $\mathbb{Q}[\sqrt{2}]$? It is equivalent to wondering if there is an element of $\mathbb{Q}[\sqrt{2}]$ whose square is 3: since $(a + b\sqrt{2})^2 = a^2 + 2b^2 + 2ab\sqrt{2}$, it means $a^2 + 2b^2 = 3$ and $ab = 0$, so that one has to solve either $a^2 = 3$ or $2b^2 = 3$, which have no rational solution. E_3 is then a field extension of $\mathbb{Q}$ of degree 4, which one denotes $\mathbb{Q}[\sqrt{2}, \sqrt{3}]$, and it is characterized as $\{a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6} \mid a, b, c, d \in \mathbb{Q}\}$. Of course, E_2 is a splitting field extension for $x^2 - 2$ over E_1, and E_3 is a splitting field extension for $x^2 - 3$ over E_2, but also a splitting field extension for $(x^2-2)(x^2-3)$ over E_1.

Example 30.7: Let $E_1 = \mathbb{Q}$ and $E_2 = \mathbb{Q}[\sqrt[3]{2}]$, so that $[E_2 : E_1] = 3$. Since $P_0 = x^3 - 2$ which is irreducible in $\mathbb{Q}[x]$ is equal to $(x - \sqrt[3]{2})\,P_1$ with $P_1 = x^2 + \sqrt[3]{2}\,x + \sqrt[3]{4}$, one must check that P_1 is irreducible in $E_2[x]$, and there are different ways to prove this.

One way is to observe that if $a = \sqrt[3]{2}$ and $b \in E_2$ is different from a and also solves $b^3 = 2$ (which is the case if $b^2 + ab + a^2 = 0$, since a is not a solution), then $z = a^{-1}b \in E_2$ solves $z^3 = 1$ and $z \neq 1$, so that $z^2 + z + 1 = 0$, but $x^2 + x + 1 \in \mathbb{Q}[x]$ is irreducible because it can be written as $\left(x + \frac{1}{2}\right)^2 + \frac{3}{4}$ and -3 is not a square in $\mathbb{Q}$, hence z generates a field extension K with $[K : E_1] = 2$, but since $K \subset E_2$ it contradicts Lemma 29.5.

Another way is to invoke the fact that squares are non-negative in $\mathbb{R}$, so that P_1 has no root in $\mathbb{R}$, because $P_1 = \left(x + \frac{\sqrt[3]{2}}{2}\right)^2 + \frac{3\sqrt[3]{4}}{4}$ is > 0 for all $x \in \mathbb{R}$. Of course, it does not seem necessary to construct $\mathbb{R}$ and put an order on it, in order to prove an algebraic result, and the first argument is a way to avoid that.

If $E_3 = E_2[x]/(P_1)$, one has $[E_3 : E_2] = 2$, so that $[E_3 : E_1] = 6$. Since one has observed that the problem for defining E_3 is to find a square root of -3, one actually has $E_3 = \mathbb{Q}[\sqrt[3]{2}, \sqrt{-3}]$. Of course, E_3 is a splitting field extension for $x^3 - 1$ over E_1.

Definition 30.8: For a field extension F of E, the *Galois group* of F over E is the group (for composition) of all (ring-) automorphisms σ of F which fix E, i.e. $\sigma(e) = e$ for all $e \in E$, and it is denoted $Aut_E(F)$.

Remark 30.9: In defining the field extension $\mathbb{Q}[\sqrt{2}]$ it was mentioned that one cannot really distinguish between $\sqrt{2}$ and $-\sqrt{2}$, so that there is a natural automorphism ψ from $\mathbb{Q}[\sqrt{2}]$ onto itself, which fixes $\mathbb{Q}$

[11] The result is not true if one is given a circle without being given its center, but one can still do the constructions if only an arc of a circle is given (together with the center of the circle).

[12] Jakob STEINER, Swiss-born mathematician, 1796–1863. He worked in Berlin, Germany.

(i.e. the restriction of ψ to $\mathbb{Q}$ is identity) and changes $\sqrt{2}$ into $-\sqrt{2}$, namely, $\psi(a+b\sqrt{2}) = a - b\sqrt{2}$ for all $a, b \in \mathbb{Q}$. It means that $Aut_{\mathbb{Q}}(\mathbb{Q}[\sqrt{2}]) = \{id, \psi\}$, so that it is isomorphic to the symmetric group S_2.[13]

A first general observation is that if $P \in E_1[x]$, any automorphism $\psi \in Aut_{E_1}(E_2)$ transforms a root of P belonging to E_2 into another root of P belonging to E_2. A second observation is that if $b_1, \ldots, b_n$ is a basis of E_2 as an E_1-vector space, then $\psi\big(\sum_i \lambda_i b_i\big) = \sum_i \lambda_i \psi(b_i)$ for all $\lambda_1, \ldots, \lambda_n \in E_1$, so that defining ψ on the basis characterizes what ψ is on E_2, but for ψ to be an automorphism of E_2, one must check that $\psi(b_i b_j) = \psi(b_i)\,\psi(b_j)$ for all i, j, and a good choice for a basis may render this verification easy.

For $E_1 = \mathbb{Q}$ and $E_2 = \mathbb{Q}[\sqrt[3]{2}]$, there is only one root in E_2 for $P = x^3 - 2$, so that $\psi(\sqrt[3]{2}) = \sqrt[3]{2}$, which implies $\psi = id$ on E_2, hence the Galois group is trivial, i.e. $Aut_{\mathbb{Q}}(\mathbb{Q}[\sqrt[3]{2}]) = \{id\}$.

For $E_1 = \mathbb{Q}$ and $E_2 = \mathbb{Q}[\sqrt{2}]$, using $P = x^2 - 2$ gives $\psi(\sqrt{2}) = \varepsilon\sqrt{2}$ with $\varepsilon = \pm 1$, which implies $\psi(a+b\sqrt{2}) = a+\varepsilon\, b\sqrt{2}$ for all $a, b \in \mathbb{Q}$, and since composing two such ψ means multiplying the corresponding ε, the Galois group is like the multiplicative group $\{+1, -1\}$, or $Aut_{\mathbb{Q}}(\mathbb{Q}[\sqrt{2}]) \simeq S_2$.

For $E_1 = \mathbb{Q}$ and $E_2 = \mathbb{Q}[\sqrt{2}, \sqrt{3}]$, using $P = x^2 - 2$ and then $P = x^2 - 3$ give $\psi(\sqrt{2}) = \varepsilon_2\sqrt{2}$ and $\psi(\sqrt{3}) = \varepsilon_3\sqrt{3}$ with $\varepsilon_2, \varepsilon_3 \in \{+1, -1\}$, so that $\psi(a + b\sqrt{2} + c\sqrt{3} + d\sqrt{6}) = a + b\,\varepsilon_2\sqrt{2} + c\,\varepsilon_3\sqrt{3} + d\,\varepsilon_2\varepsilon_3\sqrt{6}$ for all $a, b, c, d \in \mathbb{Q}$, hence $Aut_{\mathbb{Q}}(\mathbb{Q}[\sqrt{2}, \sqrt{3}]) \simeq S_2 \times S_2$.

[13] It is isomorphic to $\mathbb{Z}_2$, but one should think about such a group with the operation being composition.

31- Wednesday November 16, 2011.

Remark 31.1: If $E_1 = \mathbb{Q}$, $E_2 = \mathbb{Q}[\sqrt[3]{2}]$ and $E_3 = E_2[\sqrt{-3}]$, then E_3 contains $\omega = \frac{-1+\sqrt{-3}}{2}$ and $\omega^2 = \frac{-1-\sqrt{-3}}{2}$, so that it contains the three roots of $x^3 - 2$; E_3 is generated by E_1 and the three roots, because E_1 and $\sqrt[3]{2}$ generate E_2, and since any field containing the three roots must contain the ratio of two distinct roots, which is either ω or ω^2, so that the field contains $\sqrt{-3}$, and then E_2 and $\sqrt{-3}$ generate E_3, and it means that E_3 is a splitting field extension for $x^3 - 2$ over $\mathbb{Q}$.

Since an element of the Galois group $Aut_{E_1}(E_3)$ must permute the three roots of $x^3 - 2$, the Galois group is a subgroup of the symmetric group S_3 of permutations of these three roots, and for showing that it is isomorphic to S_3, one exhibits a transposition τ and a cyclic permutation σ (and then the group generated by τ and ω is S_3).

$E_3 = \mathbb{Q}[\sqrt[3]{2}, \sqrt{-3}]$ may be considered as $\{z = a + b\,\sqrt[3]{2} + c\,\sqrt[3]{4} + (d + e\,\sqrt[3]{2} + f\,\sqrt[3]{4})\,\sqrt{3}\,i \mid a, b, c, d, e, f \in \mathbb{Q}\} \subset \mathbb{C}$, in which case τ is complex conjugation, defined by $\tau(\sqrt[3]{2}) = \sqrt[3]{2}$ and $\tau(\sqrt{-3}) = -\sqrt{-3}$, i.e. , and $\tau(z) = a + b\,\sqrt[3]{2} + c\,\sqrt[3]{4} - (d + e\,\sqrt[3]{2} + f\,\sqrt[3]{4})\,\sqrt{3}\,i$, so that $\tau \neq id$ and $\tau \circ \tau = id$.

For defining a cyclic permutation σ, one defines it so that $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}\,\omega$, $\sigma(\sqrt[3]{2}\,\omega) = \sqrt[3]{2}\,\omega^2$, and $\sigma(\sqrt[3]{2}\,\omega^2) = \sqrt[3]{2}$, which means $\sigma(\omega) = \omega$ (and $\sigma(\sqrt[3]{2}) = \sqrt[3]{2}\,\omega$): one writes $E_3 = \mathbb{Q}[\sqrt[3]{2}, \omega] = \{z = a + b\,\sqrt[3]{2} + c\,\sqrt[3]{4} + (d + e\,\sqrt[3]{2} + f\,\sqrt[3]{4})\,\omega \mid a, b, c, d, e, f \in \mathbb{Q}\}$, and then $\sigma(z) = a + b\,\sqrt[3]{2}\,\omega + c\,\sqrt[3]{4}\,\omega^2 + (d + e\,\sqrt[3]{2}\,\omega + f\,\sqrt[3]{4}\omega^2)\,\omega$, gives $\sigma \neq id$ and $\sigma \circ \sigma \circ \sigma = id$.

Lemma 31.2: $Aut_{\mathbb{Q}}(\mathbb{R}) = \{id\}$, and $Aut_{\mathbb{R}}(\mathbb{C}) = \{id, \bar{\cdot}\} \simeq S_2$.
Proof: Let $\sigma \in Aut_{\mathbb{Q}}(\mathbb{R})$, i.e. $\sigma(a + b) = \sigma(a) + \sigma(b)$ and $\sigma(a\,b) = \sigma(a)\,\sigma(b)$ for all $a, b \in \mathbb{R}$, and $\sigma(q) = q$ for all $q \in \mathbb{Q}$, and σ is a bijection of $\mathbb{R}$ onto itself. Then, if $x \in \mathbb{R}$ with $x \geq 0$, one has $x = y^2$ for $y = \sqrt{x}$, and $\sigma(x) = \big(\sigma(y)\big)^2 \geq 0$, which implies that σ is non-decreasing (and it must be increasing since it is a bijection), and since $\sigma(q) = q$ for all $q \in \mathbb{Q}$ one deduces that $\sigma(r) = r$ for all $r \in \mathbb{R}$.[1]

Since $\big(\sigma(i)\big)^2 = \sigma(i^2) = \sigma(-1) = -1$, one deduces that $\sigma(i) = \pm i$. Then, for $a, b \in \mathbb{R}$ one has $\sigma(a + b\,i) = \sigma(a) + \sigma(b)\,\sigma(i) = a + b\,\sigma(i)$, so that σ is identity if $\sigma(i) = +i$, and σ is complex conjugation if $\sigma(i) = -i$.

Lemma 31.3: Let $P \in E[x]$ have degree n. Then, there exists a splitting field extension F for P over E satisfying $[F\!:\!E] \leq n!$ (it will be shown that two splitting field extensions for P over E are isomorphic).
Proof: By induction on n. If $n = 1$, take $F = E$. If $n > 1$, let $Q \in E[x]$ be irreducible and divide P, and let $E_1 = E(\alpha)$ with $Q(\alpha) = 0$, i.e. $E_1 = E[x]/(Q)$ and $\alpha = x$, so that $[E_1\!:\!E] = deg(Q) \leq n$. Then, $P \in E_1[x]$ and $P(\alpha) = 0$, so that $P = (x - \alpha)\,R$ with $R \in E_1[x]$, and by the induction hypothesis, there exists a splitting field extension F for R over E_1 satisfying $[F\!:\!E_1] \leq (n-1)!$. One checks easily that F is a splitting field extension for P over E,[2] and it satisfies $[F\!:\!E] = [F\!:\!E_1]\,[E_1\!:\!E] \leq n!$.

Remark 31.4: The proof of Lemma 31.3 shows that if $P = c\,P_1^{m_1} \cdots P_k^{m_k}$ where $c \in E^*$, $m_1, \ldots, m_k \geq 1$, and $P_1, \ldots, P_k \in E[x]$ are distinct monic irreducible polynomials, then one constructs a splitting field extension F for P over E by constructing a splitting field extension for $Q = P_1 \cdots P_k$. Then, instead of the bound $\big(deg(Q)\big)! = \big(deg(P_1) + \ldots + deg(P_k)\big)!$ for $[F\!:\!E]$ given by Lemma 31.3, one obtains a better bound $[F : E] \leq deg(P_1)! \cdots deg(P_k)!$ by successively constructing a splitting field extension F_1 for P_1 over E, a

[1] Notice that there is no hypothesis of continuity on σ, since the notion of automorphism is purely algebraic. Actually, the order structure of $\mathbb{R}$ implies that there are only two ring-homomorphisms from $\mathbb{R}$ into itself, 0 and *id*: indeed, if σ is a ring-homomorphism, then it is non-decreasing since $x \geq 0$ implies $x = y^2$ so that $\sigma(x) = \big(\sigma(y)\big)^2 \geq 0$; then, $\sigma(1) = \sigma(1^2) = \big(\sigma(1)\big)^2$ implies that $\sigma(1)$ is 0 or 1; finally, for $n \in \mathbb{Z}$ one then has $\sigma(n) = n\,\sigma(1)$, and for $q = \frac{a}{b} \in \mathbb{Q}$ one has $b\,\sigma(q) = \sigma(b\,q) = \sigma(a) = a\,\sigma(1)$, so that $\sigma(q) = q\,\sigma(1)$ for all $q \in \mathbb{Q}$; then, since σ is non-decreasing on $\mathbb{R}$, one deduces that $\sigma(r) = r\,\sigma(1)$ for all $r \in \mathbb{R}$.

[2] Since P splits over F, and the field generated by E and the roots of P must contain α, so that it contains $E_1 = E(\alpha)$, then it must contain E_1 and the roots of R, i.e. it must contain F, since F is a splitting field extension for R over E_1.

splitting field extension F_2 for P_2 over F_1, and so on. In particular, for $E = \mathbb{R}$ (where irreducible polynomials have degree 1 or 2), if $deg(P) = 2m$ or $2m+1$, then $[F:E] \leq 2^m$ (instead of $(2m)!$ or $(2m+1)!$).

Remark 31.5: A first step before proving that two splitting field extensions for $P \in E[x]$ over E are isomorphic, is to observe that when one adds to a field E a root of an irreducible polynomial $P \in E[x]$, it does not matter which root one adds. It might be counter-intuitive in the case of $P = x^3 - 2 \in \mathbb{Q}[x]$, which is irreducible, since one tends to think in terms of complex numbers and make a difference between the root $a = \sqrt[3]{2}$ which is real so that $F_1 = \mathbb{Q}[\sqrt[3]{2}] = \{z = a + b\sqrt[3]{2} \mid a, b \in \mathbb{Q}\} \subset \mathbb{R}$, and the other two roots, $a\,\omega$ and $a\,\omega^2$ with $\omega = \frac{-1+\sqrt{3}\,i}{2}$, which are not real, so that $F_2 = \mathbb{Q}[\sqrt[3]{2}\,\omega] = \{z = a + b\sqrt[3]{2}\,\omega \mid a, b \in \mathbb{Q}\} \subset \mathbb{C}$ and $\not\subset \mathbb{R}$; however, F_1 and F_2 are isomorphic, and defining ψ by $\psi(a + b\sqrt[3]{2}) = a + b\sqrt[3]{2}\,\omega$ for all $a, b \in \mathbb{Q}$ obviously gives an isomorphism ψ from F_1 onto F_2. Lemma 32.2 will imply the natural generalization, that two splitting field extensions for a polynomial $P \in E[x]$ over E are isomorphic, and it will be useful for proving that (up to isomorphism) there is only one field of size $q = p^k$ for each prime p and each integer $k \geq 1$.

Remark 31.6: In his work on constructing a regular polygon with n sides with straightedge and compass, GAUSS had already seen the importance of having a tower of field extensions of $\mathbb{Q}$ on one side, and a corresponding family of subgroups on the other side, but GALOIS went much further since he considered a more general question, because in the question of solvability one is led to introduce the splitting field extensions (over various fields) for polynomials $x^k - a$ for any $k \geq 2$, and not just for quadratic polynomials $x^2 - a$.

GALOIS must have realized that if a formula for giving the root of a polynomial exists, then it must apply to all the roots, since one should not be able to distinguish between the roots which one has to add. Certainly, one should add all the roots, hence the notion of a splitting field extension, which appears a crucial notion for the correspondence between an *intermediate field* K (i.e. such that $E \subset K \subset F$) and a subgroup of the Galois group $Aut_E(F)$: given K, the corresponding Galois group $Aut_K(F)$ is a subgroup of $Aut_E(F)$, but is every subgroup obtained?

In the question of adding a root of an irreducible polynomial, GAUSS had already considered the case of the polynomial $1 + x + \ldots + x^{p-1}$ for a prime p (a particular case of a *cyclotomic polynomial*), but his proof of irreducibility did not have the elegance of using "Eisenstein's criterion" after the change $x = 1 + y$;[3] actually, this criterion had actually been introduced before EISENSTEIN by SCHÖNEMANN.[4]

[3] Since $1 + x + \ldots + x^{p-1} = \frac{x^p-1}{x-1} = \frac{(y+1)^p-1}{y} = \sum_{k=1}^{p} \binom{p}{k} y^{k-1}$, for which "Eisenstein's criterion" applies.

[4] Theodor SCHÖNEMANN, German mathematician, (1812–1868). He proved "Hensel's lemma" before HENSEL, and "Eisenstein's criterion" before EISENSTEIN.

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

32- Friday November 18, 2011.

Lemma 32.1: If E is a field, if F is a field extension of E, and if $a \in F$ is algebraic over E, there is a unique irreducible monic (in the sense that the coefficient of highest degree is 1) polynomial $P_a \in E[x]$ such that $P_a(a) = 0$, and one calls it the *minimal polynomial* for a over E.[1] One has $E(a) = E[a]$, which is isomorphic to $E[x]/(P_a)$, and a basis of $E(a)$ (as an E-vector space) is $\{1, a, \ldots, a^{d-1}\}$ with $d = deg(P_a)$, so that $[E(a):E] = d$.
Proof: Let J be the ideal of polynomials $P \in E[x]$ such that $P(a) = 0$. One has $J \neq \{0\}$, since a is algebraic over E, and J is generated by a polynomial of minimum degree $d \geq 1$, and choosing it to be monic defines P_a. If $d = 1$, then $a \in E$, P_a is the polynomial $x - a$, and $E(a) = E[a] = E$. If $d \geq 2$, P_a must be irreducible, since if $P_a = Q_1 Q_2$ with $deg(Q_1), deg(Q_2) \geq 1$, then either $Q_1(a) = 0$ or $Q_2(a) = 0$ (since $0 = P_a(a) = Q_1(a)\, Q_2(a)$), contradicting the definition of d.

That P_a is unique comes from the fact that $Q(a) = 0$ implies that Q is a multiple of P_a, and if Q is irreducible it must then be $c\, P_a$ with $c \in F^*$, and if Q is monic, it implies $c = 1$.

Then, $1, a, \ldots, a^{d-1}$ are E-linearly independent, again because of the definition of d, and $E[a] = \{f(a) \mid f \in E[x], deg(f) \leq d-1\}$ is actually a field (so that it is $E(a)$): indeed if $f \in E[x]$ with $f \neq 0$ and $deg(f) \leq d-1$, then the *gcd* of f and P_a is 1, so that there exist $g, h \in E[x]$ with $1 = g\, f + h\, P_a$ (since $E[x]$ is a PID, and the *gcd* is well defined), which implies $f(a)\, g(a) = 1$, and every non-zero element in $E[a]$ then has a multiplicative inverse in $E[a]$ (since one may assume that $deg(g) \leq d-1$ by replacing g by its remainder in the Euclidean division by P_a, and changing accordingly what h is).

Remark 32.2: The notation P_a may be misleading, since it does not mention what E is, so let us use the notation P_a^E for the sake of this observation. If K is an intermediate field, i.e. $E \subset K \subset F$, and if $a \in F$ is algebraic over E, then it is algebraic over K, since $P_a^E \in E[x]$ implies $P_a^E \in K[x]$, but P_a^E may be reducible in $K[x]$, in which case P_a^K will be a divisor of P_a^E, hence $deg(P_a^K) \leq deg(P_a^E)$ in general.

Notation 32.3: If R_1, R_2 are two rings, then if σ is a ring-homomorphism from R_1 into R_2, one also denotes σ the corresponding ring-homomorphism from $R_1[x]$ into $R_2[x]$, which sends $P = \sum_j c_j x^j$ to $\sigma P = \sum_j \sigma(c_j)\, x^j$. Of course, if σ is an isomorphism from R_1 onto R_2, it induces an isomorphism from $R_1[x]$ onto $R_2[x]$.

Lemma 32.4: Let E_1, E_2 be two (isomorphic) fields, and σ an isomorphism from E_1 onto E_2. If F_1 is a field extension of E_1 and $a_1 \in F_1$ is algebraic over E_1 with minimal polynomial P_{a_1}, if F_2 is a field extension of E_2 and $a_2 \in F_2$ is algebraic over E_2, with minimal polynomial P_{a_2}, and if $\sigma\, P_{a_1} = P_{a_2}$, then there is a unique isomorphism τ from $E_1(a_1)$ onto $E_2(a_2)$ extending σ and satisfying $\tau(a_1) = a_2$.
Proof: Remark that if $a_1 \in E_1$, then $P_{a_1} = x - a_1$, so that $\sigma\, P_{a_1} = x - \sigma(a_1)$, and the hypothesis is that $a_2 = \sigma(a_1)$, and then $E_1(a_1) = E_1$, $E_2(a_2) = E_2$ and $\tau = \sigma$.

Assume that $a_1 \notin E_1$, so that P_{a_1} has degree $d > 1$. If $f = c_0 + c_1 x + \ldots + c_n x^n \in E_1[x]$, then $\sigma\, f = \sigma(c_0) + \sigma(c_1)x + \ldots + \sigma(c_n)x^n \in E_2[x]$. Since the desired isomorphism τ must satisfy $\tau(c) = \sigma(c)$ for all $c \in E_1$, and $\tau(a_1) = a_2$, it must satisfy $\tau\big(f(a_1)\big) = \sigma\, f(a_2)$ for all $f \in E_1[x]$, and one observes that this definition makes sense, i.e. if $b \in E_1(a_1)$ can be written as $b = f(a_1) = g(a_1)$ for two polynomials $f, g \in E_1[x]$, the two definitions of $\tau(b)$ using either f or g are equal: indeed, $f - g$ must be a multiple of P_{a_1}, but $f - g = P_{a_1} Q$ implies $\sigma\, f - \sigma\, g = \sigma\, (f - g) = \sigma\, P_{a_1}\, \sigma\, Q = P_{a_2}\, \sigma\, Q$, so that $\sigma\, f - \sigma\, g$ being a multiple of P_{a_2}, their values at a_2 coincide, i.e. $\sigma\, f(a_2) = \sigma\, g(a_2)$.

[1] In linear algebra, the term minimal polynomial is used with a slightly different meaning: for a field K one considers the (non-commutative) ring of $n \times n$ matrices A with entries in K (or the endomorphisms of a K-vector space V of dimension n), and for such a matrix A one considers the polynomials $P \in K[x]$ satisfying $P(A) = 0$; they form an ideal, generated by a monic polynomial P_{min} of minimal degree, called the minimal polynomial of A, which has no reason to be irreducible (since the ring of matrices has zero-divisors). The Cayley–Hamilton theorem asserts that $P_{char}(A) = 0$, where the characteristic polynomial is defined by $P_{char}(\lambda) = det(A - \lambda\, I)$, so that the minimal polynomial divides P_{char}, hence has degree $\leq n$.

Remark 32.5: The application mentioned in Remark 31.5 consists in taking $E' = E$ and $\sigma = id$, so that it says that if a_1 and a_2 belong to two (possibly different) field extensions F_1, F_2 of E, and have the same minimal polynomial P, then $E(a_1) \subset F_1$ and $E(a_2) \subset F_2$ are isomorphic by an isomorphism τ whose restriction to E is identity.

Lemma 32.6: If E is a field, if F is any field extension of E, and if A is any (non-empty) finite subset of elements of F which are algebraic over E, then $E(A)$ is a finite field extension of E.
Proof: By induction on $n = |A|$. If $K = E(a_1, \ldots, a_{n-1})$ is a finite field extension of E, then a_n being algebraic over E is also algebraic over K, so that $K(a) = K[a]$, and one has $[K(a_n) : K] \leq d_n$, the degree of the minimal polynomial for a_n in E (which is the order of a_n as an algebraic element over E), because the degree of the minimal polynomial for a_n over K is $\leq d_n$; since $E(a_1, \ldots, a_n) = K(a_n)$, one deduces that $[E(a_1, \ldots, a_n) : E(a_1, \ldots, a_{n-1})] \leq d_n$, hence $[E(a_1, \ldots, a_n) : E]$ is $\leq$ the product of the orders of the elements of A.

Lemma 32.7: If D is a field, if E is an algebraic extension of D, and if F is an algebraic extension of E, then F is an algebraic extension of D.
Proof: If $z \in F$, it is algebraic over E, so that $P(z) = 0$ for a monic irreducible polynomial $P = c_0 + c_1 x + \ldots + x^n$, with $c_0, \ldots, c_{n-1} \in E$. Since $c_0, \ldots, c_{n-1}$ are algebraic over D, $E_0 = D(c_0, \ldots, c_{n-1}) \subset E$ is a finite field extension of D by Lemma 32.6, and then z is algebraic over E_0 because P has its coefficients in E_0, and P is irreducible over E_0, so that adding the root z to E_0 gives a field E_1 with $[E_1 : E_0] = n$, and one deduces that $[E_1 : D] = n\,[E_0 : D] < +\infty$, so that z is algebraic over D.

Lemma 32.8: If E is a field and F is any field extension field of E, then $\mathcal{A}_E(F) = \{z \in F \mid z \text{ algebraic over } E\}$ is a subfield of F.
Proof: For $a, b \in F$ algebraic over E, $E(a, b)$ is a finite field extension of E by Lemma 32.6, hence an algebraic extension of E. In consequence, $a + b$ and $a\,b$ are algebraic over E, as well as a^{-1} if $a \neq 0$, since they belong to $E(a, b)$.

Remark 32.9: Directly, all powers of a are E-linear combinations of $1, \ldots, a^{\alpha-1}$ with $\alpha = order(a)$, and all powers of b are E-linear combinations of $1, \ldots, b^{\beta-1}$ with $\beta = order(b)$, so that all powers of $a+b$ and of $a\,b$ are E-linear combinations of $a^i b^j$ with $0 \leq i \leq \alpha - 1, 0 \leq j \leq \beta - 1$, showing that $a + b$ and $a\,b$ are algebraic over E, because $1, a+b, \ldots, (a+b)^{\alpha\,\beta}$ are E-linearly dependent, as well as $1, a\,b, \ldots, (a\,b)^{\alpha\,\beta}$, since they are $\alpha\,\beta + 1$ elements in an E-vector space generated by $\alpha\,\beta$ elements. This shows that $order(a + b) \leq order(a)\,order(b)$, and $order(a\,b) \leq order(a)\,order(b)$.

Furthermore, if $a \neq 0$ is algebraic over E, then $c_0 + c_1 a + \ldots + c_{\alpha-1} a^{\alpha-1} + a^\alpha = 0$, with $c_0 \neq 0$, and multiplying by $c_0^{-1} a^{-\alpha}$ one has $c_0^{-1} + c_0^{-1} c_{\alpha-1} a^{-1} + \ldots + c_0^{-1} c_1 (a^{-1})^{\alpha-1} + (a^{-1})^\alpha = 0$, showing that a^{-1} is algebraic over E, with $order(a^{-1}) \leq order(a)$, hence $order(a^{-1}) = order(a)$.

Remark 32.10: Since $\mathbb{Q} \subset \mathbb{C}$, and $\mathbb{C}$ is algebraically closed, every polynomial $P \in \mathbb{Q}[x]$ has roots in $\mathbb{C}$, which are algebraic over $\mathbb{Q}$, and by Lemma 32.8, the set of all (complex) algebraic numbers $K = \mathcal{A}_{\mathbb{Q}}(\mathbb{C})$ is a field, which is an algebraic extension of $\mathbb{Q}$ by definition of K; this field is algebraically closed, since if $P \in K[x]$ had no root in K it would have a root in a finite extension of K, which would be an algebraic extension of $\mathbb{Q}$ by Lemma 32.7, i.e. it would be a root of $P_1 \in \mathbb{Q}[x]$, so that it would belong to K by definition of K.

It is true that for any field E there exists an algebraic extension F of E which is algebraically closed, but one difficulty for proving this result is that one cannot define the "set" of all "algebraic elements over E", since one can only say which elements of a *given* field extension F are algebraic over E.

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

33- Monday November 21, 2011.

Lemma 33.1: Splitting fields are unique up to isomorphism. More precisely, if σ is an isomorphism from E_1 onto E_2, if F_1 is a splitting field extension for $P_1 \in E_1[x]$ over E_1, and F_2 is a splitting field extension for $P_2 = \sigma P_1 \in E_2[x]$ over E_2, then there exists an isomorphism τ from F_1 onto F_2 extending σ.[1] It follows that $[F_1 : E_1] = [F_2 : E_2]$. If $E_2 = E_1$ and $\sigma = id_{E_1}$, then the isomorphism τ fixes E_1. If $F_2 = F_1$, τ is an automorphism of F_1 which moves E_1 to E_2.
Proof: By induction on the dimension $[F_1 : E_1]$.[2] If $[F_1 : E_1] = 1$, then $F_1 = E_1$ and P_1 splits over E_1, i.e. $P_1 = c \prod_{i=1}^{d} (x - a_i)$ with $c \in E_1^*$, $a_1, \ldots, a_d \in E_1$, so that $P_2 = \sigma P_1 = \sigma(c) \prod_{i=1}^{d} \big(x - \sigma(a_i)\big)$ with $\sigma(c) \in E_2^*$, $\sigma(a_1), \ldots, \sigma(a_d) \in E_2$, i.e. P_2 splits over E_2, hence $F_2 = E_2$.

If $[F_1 : E_1] > 1$, let $a \in F_1 \setminus E_1$ be a root of P_1 (which exists, since F_1 is generated by these roots), so that a is algebraic over E_1 (since $P_1(a) = 0$), and let $P \in E_1[x]$ be the monic irreducible polynomial with $P(a) = 0$, so that P divides P_1; one then defines $Q = \sigma P$. Since P divides P_1, one deduces that Q divides P_2, so that Q splits over F_2, and there exists $a' \in F_2$ (among the roots of P_2) such that $Q(a') = 0$, hence the monic irreducible polynomial in $E_2[x]$ associated to a' divides Q; then, there exists an isomorphism ρ from $E_1(a)$ onto $E_2(a')$ extending σ and such that $\rho(a) = a'$ by Lemma 32.2. Then, if $P_1 = (x - a)\, Q_1$ and $P_2 = (x - a')\, Q_2$, one has $Q_2 = \sigma Q_1$, and one checks easily that F_1 is a splitting field extension for Q_1 over $E_1(a)$,[3] and that F_2 is a splitting field extension for P_2 over $E_2(a')$, and one applies the induction hypothesis for constructing an isomorphism τ, since $[F_1 : E_1] = [F_1 : E_1(a)]\, [E_1(a) : E_1]$ and $[E_1(a) : E_1] > 1$ gives $[F_1 : E_1(a)] < [F_1 : E_1]$.

Lemma 33.2: For any prime p and any $k \geq 1$, two fields of size $q = p^k$ are isomorphic.
Proof: If F is a finite field of characteristic p, and F_0 is its prime subfield, isomorphic to $\mathbb{Z}_p$, then $|F| = q = p^k$ means $[F : F_0] = k$. Since F^* is a finite multiplicative group of order $q - 1$, one has $a^{q-1} = 1$ for all $a \in F^*$, so that $a^q = a$ for all $a \in F$. Since $x^q - x$ is a monic polynomial of degree q and one knows q distinct roots, one has $x^q - x = \prod_{a \in F} (x - a)$, and F is then a splitting field extension for $x^q - x$ over F_0, since the polynomial splits over F and its roots certainly generate F, because every element of F is a root. Since splitting field extensions are unique up to isomorphism by Lemma 33.1, two such fields are isomorphic.

Lemma 33.3: Let D be any field of characteristic p, with D_0 as prime subfield ($\simeq \mathbb{Z}_p$). Then, the mapping φ_p, defined by $\varphi_p(a) = a^p$ for all $a \in D$, is an *injective* ring-homomorphism from D into itself. If D is finite, it is an automorphism, the *Frobenius automorphism*,[4] with *fixed field* D_0.[5]
Proof: Since $\varphi_p(a + b) = (a + b)^p = a^p + \big(\sum_{j=1}^{p-1} \binom{p}{j} a^j b^{p-j}\big) + b^p$ and the binomial coefficient $\binom{p}{i}$ is a multiple of p except for $i = 0$ and $i = p$ because p is prime, the right side is $a^p + b^p$, i.e. $\varphi_p(a) + \varphi_p(b)$; then $\varphi_p(a\, b) = (a\, b)^p = a^p b^p = \varphi_p(a)\, \varphi_p(b)$, so that φ_p is a ring-homomorphism.

If $\varphi_p(a) = \varphi_p(b)$, then $\varphi_p(b - a) = \varphi_p(b) + \varphi_p(-1)\, \varphi_p(a) = \varphi_p(b) - \varphi_p(a) = 0$ (since $p = 2$ implies $+1 = -1$), and $(b - a)^p = 0$ implies $b = a$. If D is finite, any injective mapping from D into itself is also surjective. By Fermat's theorem, $j^{p-1} = 1 \pmod p$ for $j = 1, \ldots, p - 1$, so that $a^{p-1} = 1$ for all $a \in D_0^*$, hence $a^p = a$ for all $a \in D_0$, i.e. $\varphi_p(a) = a$; since $x^p - x$ has degree p and one already knows p distinct roots, one knows them all, and $\varphi_p(x) = x$ implies $x \in D_0$.

---

[1] This isomorphism τ is not unique in general, as seen from the proof, where one chooses a root of Q.

[2] One has $[F_1 : E_1] < \infty$: if $a_1, \ldots, a_d$ are the roots of P_1 in F_1, then each a_j is algebraic over E_1 with an order $\leq d$, so that $[F_1 : E_1]$ is at most the product of the orders, giving an upper bound d^d. Once the result is proved, it is at most $d!$ since a splitting field extension was constructed satisfying such a bound.

[3] Because Q_1 splits over F_1, and the smallest field containing $E_1(a)$ and all the roots of Q_1 contains E_1 and all the roots of P_1, and is then F_1.

[4] Ferdinand Georg FROBENIUS, German mathematician, 1949–1918. He worked in Berlin, Germany.

[5] The fixed points of an endomorphism ψ of a ring R is a subring of R, since $\psi(x) = x$ and $\psi(y) = y$ imply $\psi(x + y) = \psi(x) + \psi(y) = x + y$, so that $\psi(0) = 0$ and $\psi(-x) = -\psi(x)$, and $\psi(x\, y) = \psi(x)\, \psi(y) = x\, y$. The fixed points of an automorphism ψ of a field K is a subfield of K, since $\psi(x) = \psi(x)\, \psi(1)$ for all $x \in K$ implies $\psi(1) = 1$, and $x^{-1}\, x = 1$ for $x \neq 0$ implies $\big(\psi(x)\big)^{-1} \psi(x) = 1$, so that $\psi(x) = x \neq 0$ implies $\psi(x^{-1}) = x^{-1}$.

Lemma 33.4: Let $E = \mathbb{Z}_p$, and for $k \geq 1$ let F be a splitting field extension for $Q = x^{p^k} - x$ over E. Then $|F| = p^k$.
Proof: Since $Q' = -1$, there are no multiple roots in F, and since $[F:E] < \infty$, F is finite and the Frobenius mapping φ_p is an automorphism by Lemma 33.3, fixing E by Fermat's theorem, i.e. $\varphi_p \in Aut_E(F)$, hence $\varphi_p^k \in Aut_E(F)$, and $\varphi_p^k(x) = x^{p^k}$ for all x (because product means composition), the fixed field of φ_p^k is then exactly the roots of Q, which is then the smallest field containing E and the roots of Q, i.e. F, and this shows that $|F| = p^k$.

Remark 33.5: It is common to call F_q a field of order q, with q a power of a prime p, so that F_p is then isomorphic to $\mathbb{Z}_p$.

This is a third different meaning for the notation F_n, but it denotes now a finite field (only used if $n = p^k$ for a prime p), while the first two denoted integers, the nth Fibonacci number (with $F_0 = F_1 = 1$ and $F_{n+2} = F_n + F_{n+1}$ for all $n \geq 0$), or the nth Fermat "prime" ($F_n = 2^{2^n} + 1$, which is only known to be prime for $0 \leq n \leq 4$).

Lemma 33.6: If E is any field, and G is a *finite* subgroup of the multiplicative group $E^* = E \setminus \{0\}$, then G is cyclic.
Proof: Because G is finite, every element has a finite order; let ℓ be the *lcm* (least common multiple) of the orders of the elements of G, so that $g^\ell = 1$ for all $g \in G$. By the structure theorem for finite Abelian groups, there is an element g_0 of order ℓ,[6] so that G has at least ℓ elements, but on the other hand $x^\ell = 1$ has at most ℓ roots, so that G has exactly ℓ elements and is generated by g_0.

Definition 33.7: If E is a field and F is a finite field extension of E, with $[F:E] = k$, a *power basis* is a basis of F (as an E-vector space) which has the form $\{1, a, \ldots, a^{k-1}\}$ for an element $a \in F$.

Remark 33.8: Using Lemma 33.6, we shall prove that a power basis exists for any finite field F_q (if E is its prime subfield, isomorphic to $\mathbb{Z}_p$ if $q = p^k$).

From a practical point of view, finite fields are important in coding theory and in cryptography, and a power basis is often used, but implicitly as a root of an irreducible polynomial, so that one encounters the question of irreducible polynomial in $\mathbb{Z}_p[x]$, for example. In case of $\mathbb{Z}_2$, I found written that the irreducible polynomials are $x^2 + x + 1$ if $k = 2$, $x^3 + x + 1$ or $x^3 + x^2 + 1$ if $k = 3$, $x^4 + x + 1$ or $x^4 + x^3 + 1$ if $k = 4$, and that some irreducible polynomials for $k \geq 5$ are $x^5 + x^2 + 1$ if $k = 5$, $x^6 + x + 1$ if $k = 6$, $x^7 + x + 1$ if $k = 7$, $x^8 + x^4 + x^3 + x^2 + 1$ if $k = 8$, so that there are various practical aspects to consider, like how to check that any of these given polynomials is indeed irreducible, or how to find an irreducible polynomial in a situation which is not listed in the books.

The values used in coding theory are reasonable low for p and for k, and the study of *cyclotomic polynomials* will be of great help, but the values of p used in cryptography have a few hundred digits, and the questions for such cases are then quite different.

[6] Directly, using additive notation, if in an Abelian group H an element a of order n, and if m divides n, then $b = \frac{n}{m}\, a$ has order m. If $(q, r) = 1$ and an element g has order q and another element h has order r, then the cyclic group generated by g and the cyclic group generated by h only intersect at 0, and $g + h$ has order $q\, r$.

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

34- Monday November 28, 2011.

Definition 34.1: If E is a field, a *primitive* mth root of unity is an element $a \in E^*$ which generates a (cyclic) group of order m consisting of the m roots of $x^m - 1 = 0$.

Remark 34.2: If a primitive mth root of unity a exists, then there are $\varphi(m)$ primitive mth roots of unity, of the form a^k with $(k, m) = 1$.

For $E = \mathbb{C}$ (or any algebraically closed field) a primitive mth root of unity exists for every $m \geq 1$. For $E = \mathbb{R}$ or $E = \mathbb{Q}$, a primitive mth root of unity exists only for $m = 1, 2$.

Lemma 34.3: If E is a finite field with q elements (and $q = p^k$, where p is the characteristic of E and $k \geq 1$), then a primitive mth root of unity exists if and only if m divides $q - 1$.
Proof: Since the multiplicative group E^* is cyclic, it is generated by an element a, which has order $q - 1$. If an mth root $b \neq 1$ exists, it means $b^m = 1$, and one writes $b = a^j$ for some j which is unique modulo $q - 1$, so that one may choose $j \in \{1, \dots, q - 2\}$, and one defines $d = (m, q - 1)$. Since $a^{m\,j} = b^m = 1$, $m\,j$ is a multiple of $q - 1$, and if one writes $m = d\,n$, $q - 1 = d\,r$ with $(n, r) = 1$, one deduces that $n\,j$ is a multiple of r, so that j is a multiple of r since n and r are relatively prime; because a^r has order d, and the powers of b are among the powers of a^r, one deduces that there are at most d distinct powers of b. One deduces that if a primitive mth root $b \neq 1$ exists, then $m = d$ is a divisor of $q - 1$. Conversely, if $q - 1 = m\,r$, then a^r is a primitive mth root.

Definition 34.4: A field extension F of E is called *simple* if $F = E(\theta)$ for some $\theta \in F$.

Lemma 34.5: If E is a finite field, then for any finite extension F of E with $[F : E] = \ell$, there exists $a \in F$ such that $\{1, a, \dots, a^{\ell-1}\}$ is a power basis (of F as an E-vector space), hence $F = E(a)$.
Proof: Let a be any of the $\varphi(q - 1)$ generators of the multiplicative group E^* (with $q = |E|$), and l Let P_a be the minimal polynomial of a (i.e. the monic irreducible polynomial satisfying $P_a(a) = 0$). One wants to show that P_a has degree ℓ. The $\ell + 1$ elements $1, a, \dots, a^\ell$ are E-linearly dependent, since they belong to an E-vector space of dimension ℓ, and the non-zero E-linear combination which is 0 gives a polynomial Q of degree $\leq \ell$ such that $Q(a) = 0$, but Q is then a multiple of P_a, whose degree is then $\leq \ell$. If P_a had degree $d < \ell$, all the powers of a would be E-linear combinations of $1, a, \dots, a^{d-1}$, and since these powers form all of E^*, one would deduce that the dimension of F over E is $\leq d$.

Lemma 34.6: If E is a finite field with q elements, and F is a field extension of E, then for every $a \in F$ which is algebraic over E, $\varphi_q(a)$ has the same minimal polynomial than a.
Proof: Since E is isomorphic to a splitting field extension for $x^q - x$ over $\mathbb{Z}_p$, one deduces that $\varphi_q(e) = e$ for all $e \in E$. If $a \in F$ is algebraic over E, it has a minimal polynomial $P \in E[x]$, but since the coefficients of P are fixed by φ_q which is a ring-homomorphism from F into itself, one finds that $P\big(\varphi_q(a)\big) = \varphi_q\big(P(a)\big) = 0$. Of course, this is just using the fact that $\varphi_q \in Aut_E(F)$.

Remark 34.7: Consider $E = \mathbb{Z}_2$ and F ($\simeq F_8$), so that $[F : E] = 3$, and since $\varphi(7) = 6$, all the non-zero elements except 1 generate F^*, and there are then two irreducible polynomials of degree 3 over $\mathbb{Z}_2$. Let ξ be any of these generators, so that the minimal polynomial of ξ is $P = (x - \xi)\,(x - \xi^2)\,(x - \xi^4)$, which has the form $x^3 + a\,x^2 + b\,x + 1$ (since $\xi^7 = 1$ and $-1 = 1$), and the minimal polynomial of ξ^3 is $Q = (x - \xi^3)\,(x - \xi^6)\,(x - \xi^{12})$, but since ξ^3 is the inverse of ξ^4, ξ^6 is the inverse of ξ, and $\xi^{12} = \xi^5$ is the inverse of ξ^2, one has $Q = x^3 P\big(\frac{1}{x}\big) = x^3 + b\,x^2 + a\,x + 1$. Then, since $x^7 - 1 = (x - 1)\,P\,Q$, one has $P\,Q = x^6 + x^5 + x^4 + x^3 + x^2 + x + 1$, but the coefficient of x^5 in $P\,Q$ is then $a + b$, and $a + b = 1$ has the symmetric solutions $a = 1, b = 0$ or $a = 0, b = 1$, so that one finds that the two irreducible polynomials of degree 3 over $\mathbb{Z}_2$ are $x^3 + x^2 + 1$ and $x^3 + x + 1$.

Remark 34.8: Consider $E = \mathbb{Z}_2$ and F ($\simeq F_{16}$), so that $[F : E] = 4$, and since $\varphi(15) = \varphi(3)\varphi(5) = 2 \cdot 4 = 8$, there are 8 generators. Let ξ be any of these generators, so that the minimal polynomial of ξ is $P = (x - \xi)\,(x - \xi^2)\,(x - \xi^4)\,(x - \xi^8)$, which has the form $x^4 + a\,x^3 + b\,x^2 + c\,x + 1$ (since $\xi^{15} = 1$); the minimal polynomial of ξ^3 is $Q = (x - \xi^3)\,(x - \xi^6)\,(x - \xi^{12})\,(x - \xi^{24})$, but since $\xi^{24} = \xi^9$ and $\eta = \xi^3$ is a fifth

root of unity different from 1, one has $Q = (x-\eta)\,(x-\eta^2)\,(x-\eta^3)\,(x-\eta^4) = \frac{x^5-1}{x-1} = x^4+x^3+x^2+x+1$; the minimal polynomial of ξ^5 is $R = (x-\xi^5)\,(x-\xi^{10})$ since $\xi^{20} = \xi^5$, and because $\zeta = \xi^5$ is a third root of unity different from 1, one has $R = (x-\zeta)\,(x-\zeta^2) = \frac{x^3-1}{x-1} = x^2+x+1$; the minimal polynomial of ξ^7 is $S = (x-\xi^7)\,(x-\xi^{14})\,(x-\xi^{28})\,(x-\xi^{56})$, but since ξ^7 is the inverse of ξ^8, ξ^{14} is the inverse of ξ, $\xi^{28} = \xi^{13}$ is the inverse of ξ^2, and $\xi^{56} = \xi^{11}$ is the inverse of ξ^4, one has $S = x^3 P\big(\frac{1}{x}\big) = x^4 + c\,x^3 + b\,x^2 + a\,x + 1$. There are then three irreducible polynomials of degree 4 over $\mathbb{Z}_2$.

One has $x^{15}-1 = (x-1)\,P\,Q\,R\,S$, and $(x-1)\,Q = x^5-1$, so that $P\,R\,S = \frac{x^{15}-1}{x^5-1} = x^{10}+x^5+1$ (by using $x^5 = y$), hence $P\,S = \frac{x^{10}+x^5+1}{x^2+x+1}$, and in $\mathbb{Z}_2[x]$ this quotient is $x^8+x^7+x^5+x^4+x^3+x+1$; identifying then the coefficients of powers x^7, x^6, x^5, x^4 (since those of x^3, x^2, x coincide then with those of x^5, x^6, x^7), one obtains $1 = a+c$, $0 = 2b+a\,c$, $1 = (a+c)\,(1+b)$, and $1 = a^2+b^2+c^2$ which gives the symmetric solutions $a = 1, b = 0, c = 0$ and $a = 0, b = 0, c = 1$, so that, besides $x^4+x^3+x^2+x+1$, the two other irreducible polynomials of degree 4 over $\mathbb{Z}_2$ are x^4+x^3+1 and x^4+x+1.

Remark 34.9: Using the monic irreducible polynomial $P = x^4+x+1 \in \mathbb{Z}_2[x]$ just obtained, one lets ξ be any of its four roots, and one uses the basis $1, \xi, \xi^2, \xi^3$ for F ($\simeq F_{16}$) over F_2, and since $\xi^4 = 1+\xi$ one constructs easily by induction the formula expressing ξ^j:

$$\begin{array}{ccc} \xi^4 = 1+\xi & \xi^8 = 1+\xi^2 & \xi^{12} = 1+\xi+\xi^2+\xi^3 \\ \xi^5 = \xi+\xi^2 & \xi^9 = \xi+\xi^3 & \xi^{13} = 1+\xi^2+\xi^3 \\ \xi^6 = \xi^2+\xi^3 & \xi^{10} = 1+\xi+\xi^2 & \xi^{14} = 1+\xi^3 \\ \xi^7 = 1+\xi+\xi^3 & \xi^{11} = \xi+\xi^2+\xi^3 & \xi^{15} = 1 \end{array} .$$

Remark 34.10: The preceding remarks show that all the irreducible polynomials of degree d over $\mathbb{Z}_p$ are obtained by considering a field extension F ($\simeq F_q$ with $q = p^d$) of $\mathbb{Z}_p$ with $[F:\mathbb{Z}_p] = d$, and considering the $\varphi(q-1)$ generators, which will correspond to $\frac{\varphi(q-1)}{d}$ such irreducible polynomials of degree d, but that some others may be associated to a non-zero element different from 1 which is not a generator, as in the case $q = 16$. Also, the product of these polynomials divide $x^{q-1}-1$, so that considering the factorization of x^n-1 for a general n is a natural question, which will be considered over $\mathbb{Z}[x]$.

Definition 34.11: The *cyclotomic field* of nth roots of unity over $\mathbb{Q}$ is the splitting field extension for x^n-1 over $\mathbb{Q}$, i.e. $\mathbb{Q}\big(e^{2i\,\pi/n}\big)$ $(= \mathbb{Q}\big[e^{2i\,\pi/n}\big])$.

The nth *cyclotomic polynomial* Φ_n is defined by $\Phi_n(x) = \prod_{primitive}(x-\xi_k)$, where the product is taken over the primitive nth roots of unity ξ_k, so that the degree of Φ_n is $\varphi(n)$, where φ is the Euler function.

Lemma 34.12: For all $n \geq 1$, $x^n-1 = \prod_{d|n}\Phi_d(x)$, Φ_n is monic, and $\Phi_n \in \mathbb{Z}[x]$.

Proof: If $1 \leq k \leq n-1$, then $(k,n) = \delta$ and $d = \frac{n}{\delta}$ are divisors of n, and $e^{2i\,\pi\,k/n}$ is a primitive dth root of unity. Since $x^n-1 = \prod_{0\leq k\leq n}(x-e^{2i\,\pi\,k/n})$, and $\Phi_1 = x-1$, by grouping the terms $(x-e^{2i\,\pi\,k/n})$ for k a dth root of unity, which must be a divisor of n, one obtains the formula $x^n-1 = \prod_{d|n}\Phi_d(x)$, a consequence of which is $n = \sum_{d|n}\varphi(d)$ by comparing degrees.[1] That the coefficients are integers is easily derived from the formula by induction on n, observing first that it is true for Φ_1 and for $\Phi_p = x^{p-1}+\ldots+1$ when p is a prime; then, one has $x^n-1 = \Psi_n\Phi_n$ and Ψ_n is the product of Φ_d for $d < n$ a divisor of n, so that by induction $\Psi_n \in \mathbb{Z}[x]$, and then since Ψ_n is monic, the Euclidean division of x^n-1 by Ψ_n gives a quotient and a remainder (here 0) in $\mathbb{Z}[x]$.

Remark 34.13: For p prime $\Phi_p = x^{p-1}+\ldots+1$, and for the first composite n, the formula gives $\Phi_4 = x^2+1$, $\Phi_6 = x^2-x+1$, $\Phi_8 = x^4+1$, $\Phi_9 = x^6+x^3+1$, $\Phi_{10} = x^4-x^3+x^2-x+1$, $\Phi_{12} = x^4-x^2+1$, $\Phi_{14} = x^6-x^5+x^4-x^3+x^2-x+1$, $\Phi_{15} = x^8-x^7+x^5-x^4+x^3-x+1$, $\Phi_{16} = x^8+1$, and one observes some simple properties, which will be proved later to be general.

One may think that the coefficients are always -1, 0, or $+1$, but it is not the case: the smallest value of n for which it is not true is $n = 105$, and Φ_{105} has a coefficient equal to -2; $105 = 3\cdot 5\cdot 7$ is the smallest odd integer with three distinct prime factors, and if n has at most two distinct odd prime factors, then one can show that the coefficients of Φ_n belong to $\{-1, 0, +1\}$.

[1] A consequence of this formula is $\sum_n \frac{n}{n^s} = \sum_n \frac{\varphi(n)}{n^s}\,\sum_n \frac{1}{n^s}$, i.e. $\sum_n \frac{\varphi(n)}{n^s} = \frac{\zeta(s-1)}{\zeta(s)}$, valid for $\Re(s) > 2$.

35- Wednesday November 30, 2011.

Lemma 35.1: Φ_n is irreducible in $\mathbb{Q}[x]$, so that $[\mathbb{Q}(e^{2i\,\pi/n}):\mathbb{Q}] = \varphi(n)$.
Proof: If n is a prime p, one can use Eisenstein criterion after a translation: $\Phi_p(x+1) = \frac{(x+1)^p-1}{x} = x^{p-1} + \sum_{j=1}^{p-1} \binom{p}{j} x^{j-1}$ so that all coefficients but the first are multiple of p, and the constant coefficient is p, hence not a multiple of p^2.

By Gauss's lemma, Φ_n is irreducible in $\mathbb{Q}[x]$ if and only if it is irreducible in $\mathbb{Z}[x]$ (since the content of a monic polynomial is 1). If Φ_n is reducible in $\mathbb{Z}[x]$, then $\Phi_n = f\,g$, with $f, g \in \mathbb{Z}[x]$ monic, and one may assume that f is irreducible. Let ξ be a primitive nth root of 1 which is a root of f, and let p be any prime not dividing n, so that ξ^p is another primitive nth root of 1, hence either a root of f or a root of g; one assumes that $g(\xi^p) = 0$ in order to arrive at a contradiction, and deduce then that $f(\xi^p) = 0$. Since $g(x^p)$ has ξ as a root, it must be a multiple of f, hence $g(x^p) = f(x)\,h(x)$ for some $h \in \mathbb{Z}[x]$, since one deals with monic polynomials and Euclidean division works. Reducing this equation modulo p, one obtains $\overline{g}(x^p) = \overline{f}(x)\,\overline{h}(x)$ in $\mathbb{Z}_p[x]$, but in $\mathbb{Z}_p[x]$ one has $\overline{g}(x^p) = \big(\overline{g}(x)\big)^p$, so that $\overline{g}^p = \overline{f}\,\overline{h}$, and since $\mathbb{Z}_p[x]$ is a PID hence a UFD, $\overline{f}$ and $\overline{g}$ have a common factor, and using $\overline{\Phi_n} = \overline{f}\,\overline{g}$, one deduces that $\overline{\Phi_n} \in \mathbb{Z}_p[x]$ has a repeated factor; the same is then true of $x^n - 1$, which is a multiple of $\overline{\Phi_n}$, but it is a contradiction since its derivative $n\,x^{n-1}$ is not 0 (since n is not a multiple of p), and the gcd of $x^n - 1$ and $n\,x^{n-1}$ in $\mathbb{Z}_p[x]$ is then 1.

Since this argument applies to every root of f, one may repeat the argument and one finds that ξ^m is a root of f for any integer $m = p_1 \cdots p_k$ for (not necessarily distinct) primes not dividing n, i.e. for any m relatively prime with n, and that means that ξ^m can be any of the $\varphi(n)$ primitive roots of 1, i.e. $f = \Phi_n$.

Remark 35.2: GAUSS had showed that if $n = 2^{2^k} + 1$ is a (Fermat) prime, one can construct a regular polygon with n sides by straightedge and compass, so that one can do it if $n = 2^\ell p_1 \cdots p_m$ if $p_1, \ldots, p_m$ are distinct Fermat primes. It was WANTZEL who proved that it is necessary, and this follows from Lemma 35.1, since it is necessary that the dimension of the cyclotomic extension over $\mathbb{Q}$ be a power of 2 for the construction of $e^{2i\,\pi/n}$ to be possible with straightedge and compass. Suppose that $n = 2^k q_1^{\alpha_1} \cdots q_\ell^{\alpha_\ell}$ (with $q_1, \ldots, q_\ell$ distinct primes and $\alpha_1, \ldots, \alpha_\ell \geq 1$) has the property that $\varphi(n)$ is a power of 2; then, since $\varphi(2^k q_1^{\alpha_1} \cdots q_\ell^{\alpha_\ell}) = \varphi(2^k)\,\varphi(q_1^{\alpha_1}) \cdots \varphi(q_\ell^{\alpha_\ell})$ and $\varphi(2^k) = 2^{k-1}$, it is necessary that $\varphi(q_i^{\alpha_i})$ is a power of 2 for $i = 1, \ldots, \ell$; since $\varphi(q_i^{\alpha_i}) = (q_i - 1)\,q_i^{\alpha_i - 1}$, it is a power of 2 if $q_i - 1$ is a power of 2, and $\alpha_i - 1 = 0$; then one notices that if $2^m + 1$ is prime, then m is a power of 2 (since $2^{a\,b} + 1$ is divisible by $2^b + 1$ if a is odd), i.e. each q_i is a Fermat prime, and it appears with power 1.

Lemma 35.3: If n is odd ≥ 3, then $\Phi_{2n}(x) = \Phi_n(-x)$, and $\Phi_2(x) = x + 1 = -\Phi_1(-x)$.
Proof: The formula for Φ_{2n} is true for $n = 3$ (and $n = 5, 7$ from the list in Remark 34.13), and one uses an induction upon n. Since n is odd, the divisors of $2n$ are the divisors d of n, and $2d$ for the divisors d of n, so that by Lemma 34.12 one has $\prod_{d|n} \Phi_d(x) = x^n - 1$ and $\prod_{d|n} \Phi_d(x)\,\Phi_{2d}(x) = x^{2n} - 1$, from which one deduces that $\prod_{d|n} \Phi_{2d}(x) = \frac{x^{2n}-1}{x^n-1} = x^n + 1$. Since $\prod_{d|n} \Phi_d(-x) = -x^n - 1$ (as n is odd), one deduces that $\prod_{d|n} \frac{\Phi_{2d}(x)}{\Phi_d(-x)} = -1$; for $d = 1$, the ratio $\frac{\Phi_2(x)}{\Phi_1(-x)}$ is -1, and then by the induction hypothesis the ratio $\frac{\Phi_{2d}(x)}{\Phi_d(-x)}$ is $+1$ for $1 < d < n$, so that the ratio $\frac{\Phi_{2n}(x)}{\Phi_n(-x)}$ is $+1$.

Lemma 35.4: (Möbius inversion formula) If $a_1, a_2, \ldots, a_n, \ldots \in E^*$ for a field E, and one defines the sequence $b_1, b_2, \ldots, b_m, \ldots \in E^*$ by $b_m = \prod_{d|m} a_d$ for all $m \geq 1$, then $a_n = \prod_{d|n} b_{n/d}^{\mu(d)}$ for all $n \geq 1$, where μ is the Möbius function.[1]
Proof: In the product $\prod_{d|n} b_{n/d}^{\mu(d)}$, if one replaces each $b_{n/d}$ by its definition as a product, one only finds values of a_j for j dividing n, and the exponent of a_j is $\sum_d \mu(d)$ for the values of d such that j divides $\frac{n}{d}$, i.e. d

[1] The Möbius function is defined by $\mu(1) = 1$ and if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ for distinct primes $p_1, \ldots, p_k$, with $\alpha_1, \ldots, \alpha_k \geq 1$, by $\mu(n) = (-1)^k$ if $\alpha_j = 1$ for all j, and $\mu(n) = 0$ if $\alpha_j \geq 2$ for some j. It is used for inverting $g = 1 \star f$ by $f = \mu \star g$, so that $1 \star \mu = \delta$ the identity for convolution, i.e. $\delta(1) = 1$ and $\delta(m) = 0$ for $m \geq 2$.

divides $\frac{n}{j}$, so that the sum is $(1 \star \mu)\big(\frac{n}{j}\big)$, and then one uses $1 \star \mu = \delta$ defined by $\delta(1) = 1$ and $\delta(m) = 0$ for $m \geq 2$.

Lemma 35.5: If n is odd ≥ 1, $\Phi_{2^k n}(x) = \Phi_{2n}\big(x^{2^{k-1}}\big)$ for all $k \geq 1$, and more generally, if $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ for distinct primes $p_1, \ldots, p_k$, with $\alpha_1, \ldots, \alpha_k \geq 1$, and if r is the radical of n, i.e. $r = p_1 \cdots p_k$, then $\Phi_n(x) = \Phi_r(x^{n/r})$.

Proof: One applies Lemma 35.4 to Lemma 34.12, with $E = \mathbb{Q}(x)$, and $a_n = \Phi_n$ for all $n \geq 1$, so that $b_m = x^m - 1$ for all $m \geq 1$, and one obtains $\Phi_n(x) = \prod_{d|n}(x^{n/d} - 1)^{\mu(d)}$. Then one notices that $\mu(d) \neq 0$ imposes that no prime factor from $\{p_1, \ldots, p_k\}$ appears with exponent ≥ 2 in d, so that it means that d divides r, and it gives $\Phi_n(x) = \prod_{d|r}(x^{n/d} - 1)^{\mu(d)} = \prod_{d|r}(y^{r/d} - 1)^{\mu(d)}$ with $y = x^{n/r}$, i.e. $\Phi_n(x) = \Phi_r(y)$.

36- Friday December 2, 2011.

Remark 36.1: The argument of EUCLID that there are infinitely many primes consists in assuming that there are only finitely many primes $p_1, \ldots, p_k$, and to consider $N = 1 + p_1 \cdots p_k$, which certainly has a prime factor (possibly itself) which is not in the list, since $N = 1 \pmod{p_j}$ for $j = 1, \ldots, k$.

There are simple variants for showing that in a particular arithmetic progression $a\,n + b$ with $a \geq 3$ and $(a, b) = 1$ there are infinitely many primes, but it is limited to $\varphi(a) \leq 2$, i.e. $a = 3, 4, 6$ for the value of $b \neq 1$; there is an improvement using quadratic residue theory, but it is limited to $\varphi(a) \leq 4$; then, using cyclotomic polynomials will give the case $b = 1$.

It is useful to know that DIRICHLET proved the result for all cases, that for $a \geq 3$ and b relatively prime with a, there are infinitely many values of n for which $a\,n + b$ is prime;[1] however, his proof belongs to *analytic* number theory, and not to *algebraic* number theory. Since there are $\varphi(a)$ families, it is natural to wonder in which of these families the primes fall, and each family has "asymptotic density" $\frac{1}{\varphi(a)}$ by a result of DE LA VALLÉE POUSSIN,[2] who improved a previous result of DIRICHLET for another notion of density, related to Dirichlet series.

Lemma 36.2: There are infinitely many primes of the form $6n - 1$ (hence infinitely many primes of the form $3n - 1$), and there are infinitely many primes of the form $4n - 1$. More generally, for each $a \geq 3$ there are infinitely many primes of the form $a\,n + b$ for *some* $b \neq 1$, i.e. which are *not* of the form $a\,n + 1$.
Proof: If there was only finitely many primes $q_1 < \ldots < q_k$ not of the form $a\,n + 1$, then $N = a\,q_1 \cdots q_k - 1$ would be of the form $a\,n - 1$, so that the prime factors of N could not prime divisors of a, but they could not be all of the form $a\,n + 1$ since the product would also have this form (and $-1 \neq 1 \pmod{a}$ since $a = 2$ is excluded), so that N would have a prime divisor not of the form $a\,n + 1$, but it could not be any q_j, giving a contradiction.

If $\varphi(a) = 2$, i.e. $a \in \{3, 4, 6\}$, then it tells the form of the family in which these primes fall, i.e. $3n - 1$, $4n - 1$, $6n - 1$.

Lemma 36.3: There are infinitely many primes of the form $4n + 1$.
Proof: One has seen that -1 is a quadratic residue modulo an odd prime p if and only if p is of the form $4m + 1$, and one deduces that (whatever N is) all the (necessarily odd) prime divisors of $4N^2 + 1$ are of the form $4m + 1$, since if p is such a prime divisor one has $(2N)^2 = -1 \pmod{p}$, hence -1 is a quadratic residue modulo p. If the only primes of the form $4n + 1$ were $5 = p_1, \ldots, p_k$, then one would take $N = p_1 \cdots p_k$, and obtain a contradiction.

Remark 36.4: If a prime p has the form $4n + 1$, one can deduce that -1 is a quadratic residue by using a primitive root ξ modulo p: ξ has order $4n$ in $\mathbb{Z}_p^*$, so that $(\xi^{2n})^2 = 1$ and $\xi^{2n} \neq 1$ imply $\xi^{2n} = -1$, hence the solutions of $a^2 = -1 \pmod{p}$ are $a = \pm\xi^n \pmod{p}$.

Similarly, if a prime q is $4n + 3$, one can deduce that -1 is not a quadratic residue modulo q: one chooses a primitive root η modulo q, and if -1 was the square of b, b would be η^j for some j, so that $-1 = \eta^{2j}$, hence $1 = \eta^{4j}$, which implies that $4j$ would a multiple of $q - 1$ but $2j$ would not be a multiple of $q - 1$, and this is contradictory, since $4j = k\,(q - 1)$ implies k even (because $2j = k\,(2n + 1)$), so that $k = 2\ell$, hence $2j = \ell\,(q - 1)$.

Lemma 36.5: (Gauss's lemma)[3] Let $p = 2m + 1$ be an odd prime. For a not a multiple of p, and for $j \in \{1, \ldots, m\}$ one writes $j\,a = \alpha_j \pmod{p}$ with $\alpha_j \in \{1, \ldots, 2m\}$, and one defines $g(a)$ as the number of α_j which belong to $\{m + 1, \ldots, 2m\}$. Then, one has $\left(\frac{a}{p}\right) = (-1)^{g(a)}$.

[1] Of course, in an arithmetic progression $a\,n + b$ where n varies, all the terms are multiple of $d = (a, b)$, so that if a and b are not relatively prime one finds at most one prime in the arithmetic progression, if d is prime.

[2] Charles Jean Gustave Nicolas DE LA VALLÉE POUSSIN, Belgian mathematician, 1866–1962. He was made baron in 1928. He worked in Louvain, Belgium.

[3] This is a different lemma of GAUSS than the one on irreducibility in $\mathbb{Z}[x]$.

Proof: Since a is invertible modulo p, the elements $j\,a$ are distinct modulo p, so that the α_j are distinct. For $j = 1, \ldots, m$, one defines β_j as $\min\{\alpha_j, p - \alpha_j\}$ (so that $1 \leq \beta_j \leq m$), and the number of indices j such that $\beta_j = p - \alpha_j$ is $g(a)$, hence $\prod_j \beta_j = (-1)^{g(a)} \prod_j \alpha_j = (-1)^{g(a)} \prod_j (j\,a) = (-1)^{g(a)} a^m m! \pmod p$. The elements $\{\beta_j \mid j = 1, \ldots, m\}$ are distinct, since one cannot have $\alpha_j = p - \alpha_k$, because one has $2 \leq \alpha_j + \alpha_k \leq 2m = p - 1$ for all $j, k \in \{1, \ldots, m\}$, so that $\{\beta_1, \ldots, \beta_m\}$ is a permutation of $\{1, \ldots, m\}$, and $\prod_j \beta_j = m!$, hence $(-1)^{g(a)} a^m m! = m! \pmod p$. Since $m!$ is invertible modulo p, one deduces that $a^m = (-1)^{g(a)} \pmod p$, giving $\left(\frac{a}{p}\right) = (-1)^{g(a)}$.

Lemma 36.6: For p an odd prime, one has $\left(\frac{2}{p}\right) = +1$ if and only if p has the form $8n \pm 1$, and $\left(\frac{2}{p}\right) = -1$ if and only if p has the form $8n \pm 3$, which analytically means that $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$.

As a consequence, one has $\left(\frac{-2}{p}\right) = +1$ if and only if p has the form $8n + 1$ or $8n + 3$, and $\left(\frac{-2}{p}\right) = -1$ if and only if p has the form $8n + 5$ or $8n + 7$.

Proof: One applies Gauss's lemma (Lemma 36.5) to $a = 2$, so that if $p = 2m + 1$ one has $\alpha_j = 2j$ for $j = 1, \ldots, m$, and $\alpha_j \geq m + 1$ means $j \geq \frac{m+1}{2}$: if $m = 2r$, it means $j \geq r + 1$, so that $g(a) = r$ and $g(a)$ is even if and only if p has the form $8n + 1$, while if $m = 2r + 1$, it also means $j \geq r + 1$, but $g(a) = r + 1$, so that $g(a)$ is even if r is odd, i.e. m has the form $4n + 3$ and p has the form $8n + 7$ (which is the same as the form $8n - 1$).

Then, one uses $\left(\frac{-2}{p}\right) = \left(\frac{2}{p}\right)\left(\frac{-1}{p}\right)$, together with the fact that -1 is a quadratic residue modulo p if and only if p has the form $4n + 1$.

Lemma 36.7: There are infinitely many primes of the form $8n + 7$, and there are infinitely many primes of the form $8n + 3$.[4]

Proof: If there were only a finite number of primes $7 = p_1 < \ldots < p_k$ of the form $8n+7$, then for $N = p_1 \cdots p_k$ any prime factor s of $8N^2 - 1$ would be either of the form $8n + 1$ or of the form $8n + 7$ by Lemma 36.6, since 2 is a quadratic residue modulo s, because $2(8N^2 - 1) = 0 \pmod s$ means $2 = (4N)^2 \pmod s$; since $8N^2 - 1$ is odd and its prime factors cannot all be of the form $8n + 1$, because their product would have this form, there would be at least one prime factor s of the form $8n + 7$, which could not belong to the list $\{p_1, \ldots, p_k\}$, made of divisors of N.

If there were only a finite number of primes $3 = q_1 < \ldots < q_k$ of the form $8n + 3$, then for $M = q_1 \cdots q_k$ any prime factor t of $2M^2 + 1$ would be either of the form $8n + 1$ or of the form $8n + 3$ by Lemma 36.6, since -2 is a quadratic residue modulo t, because $2(M^2 + 1) = 0 \pmod t$ means $(2M)^2 = -2 \pmod t$; since $2M^2 + 1$ is odd and its prime factors cannot all be of the form $8n + 1$, because their product would have this form (and M being odd implies $2M^2 + 1 = 3 \pmod 8$), there would be at least one prime factor t of the form $8n + 3$, which could not belong to the list $\{q_1, \ldots, q_k\}$, made of divisors of M.

Remark 36.8: One may expect the preceding idea to work for proving that there are infinitely many primes in some family of the form $a\,n + b$ if $\varphi(a) = 4$, by finding a quadratic residue which only occurs for the form $a\,n + 1$ or $a\,n + \beta$ for a particular value of β (and not for the other two families). One has $\varphi(a) = 4$ for $a \in \{5, 8, 12\}$, and the argument does work for $a = 5$ and for $a = 12$, but it uses the law of quadratic reciprocity, which is then a more technical step: recall that it was conjectured by LEGENDRE, who could not prove it, and EULER could not prove it either, but GAUSS published six different proofs.

Lemma 36.9: If $P \in \mathbb{Z}[x]$ is a (non-constant) monic polynomial, then there are infinitely many prime divisors of the sequence $P(1), P(2) \ldots, P(n), \ldots$.

Proof: Suppose that $p_1, \ldots, p_k$ are the only prime divisors of the sequence, and let $N = p_1 \cdots p_k$. Since P has at most $deg(P)$ zeros, there exists $m \geq 1$ such that $P(m) = a \neq 0$, and then the Taylor expansion of $P(m + a\,N\,x)$ at m has all its coefficients multiple of a, since it is $\sum_j c_j x^j$ with $c_0 = P(m) = a \in \mathbb{Z}$, and $c_j = \frac{P^{(j)}(m)}{j!}\, a^j N^j$ for $j \geq 1$, which is a multiple of a since $\frac{P^{(j)}(m)}{j!} \in \mathbb{Z}$.[5] One deduces that $Q(x) = \frac{P(m+a\,N\,x)}{a} \in \mathbb{Z}[x]$, but also that $Q(n) = 1 + \sum_{j \geq 1} \frac{P^{(j)}(m)}{j!}\, a^{j-1} N^j n^j = 1 \pmod N$ for all $n \geq 1$, and

[4] This is more precise than the part of Lemma 36.2 which says that there are infinitely many primes of the form $4n + 3$.

[5] For $P = \sum_{i \geq 0} \alpha_i x^i \in \mathbb{Z}[x]$, one has $\frac{P^{(j)}}{j!} = \sum_{i \geq j} \alpha_i \binom{i}{j} x^{i-j} \in \mathbb{Z}[x]$.

since there are only a finite number of n for which $Q(n) = 1$, there exists n with $Q(n) > 1$ and $Q(n) = 1 \pmod N$, so that $Q(n)$ must have a prime factor not in the list $\{p_1, \ldots, p_k\}$, hence $P(m + a\,N\,n) = a\,Q(n)$ has a prime factor not in the list $\{p_1, \ldots, p_k\}$.

Lemma 36.10: For $m \geq 3$, let p be an odd prime not dividing m, and such that the cyclotomic polynomial Φ_m satisfies $\Phi_m(a) = 0 \pmod p$ for some $a \in \mathbb{Z}$. Then, a is not a multiple of p, and the order of a in $\mathbb{Z}_p^*$ is exactly m, so that m divides $p - 1$, i.e. $p = 1 \pmod m$.
Proof: Since $x^m - 1 = \Phi_m \prod_{d|m, d \neq m} \Phi_d$, $a^m - 1$ is a multiple of $\Phi_m(a)$, so that $a^m - 1 = 0 \pmod p$, hence a is not a multiple of p. If the order of a in $\mathbb{Z}_p^*$ was $d < m$, d would be a divisor of m, and from $a^d = 1 \pmod p$ one would deduce that $\Phi_\delta(a) = 0 \pmod p$ for a divisor δ of d, hence a divisor of m (different from m), so that $x^m - 1$ would have a as a (non-zero) repeated root in $\mathbb{Z}_p$ (since Φ_m and Φ_δ would be divisible by $(x - a)$), contradicting the fact that $m\,x^{m-1}$, the derivative of $x^m - 1$, is $\neq 0$ on $\mathbb{Z}_p^*$ (because p is not a divisor of m). The order of a is then m, and since $a^{p-1} = 1 \pmod p$ by Fermat's theorem, one deduces that $p - 1$ is a multiple of m.

Lemma 36.11: For any integer $m \geq 3$, there are infinitely many primes equal to 1 modulo m.
Proof: By Lemma 36.10, if p is a prime factor of $\Phi_m(a)$, then either p divides m or $p = 1 \pmod m$, but by Lemma 36.9 there are infinitely many prime divisors of $\Phi_m(1), \Phi_m(2), \ldots$, and one deduces that infinitely many of these primes are equal to 1 modulo m, since there are only a finite number of prime divisors of m.

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

37- Monday December 5, 2011.

Remark 37.1: The next step in the theory of quadratic residues is to prove the *law of quadratic reciprocity*, Lemma 37.3. It was conjectured by EULER, and by LEGENDRE, who could not prove it. GAUSS published six different proofs, and two more were found in his papers after he died.[1]

Lemma 37.2: Let p and q be distinct odd primes, and a a positive integer not a multiple of p or q. If $q = p \pmod{4a}$ or $q = -p \pmod{4a}$, then $\left(\frac{a}{p}\right) = \left(\frac{a}{q}\right)$.[2]
Proof: For $p = 2m+1$ let $S = \{a, 2a, \ldots, m\,a\}$, so that by Gauss's lemma $\left(\frac{a}{p}\right) = (-1)^M$ where M is the number of elements of S which fall into one of the open intervals $\left(\frac{p}{2}, p\right), \left(\frac{3p}{2}, 2p\right), \ldots, \left(\frac{(2c-1)\,p}{2}, c\,p\right)$,[3] and one wants the value c to be optimal, so that $\frac{(2c-1)\,p}{2} < j\,a < c\,p$ implies $j \leq m$ and $\frac{(2c+1)\,p}{2} < j\,a < (c+1)\,p$ implies $j > m$: the answer is $c = \frac{a}{2}$ if a is even,[4] and $c = \frac{a-1}{2}$ if a is odd,[5] and it is important that c does not depend upon p, since one will use the same value of c after replacing p by q. By dividing by a, one finds that M is the number of positive integers which fall into one of the open intervals $\left(\frac{p}{2a}, \frac{p}{a}\right), \left(\frac{3p}{2a}, \frac{2p}{a}\right), \ldots, \left(\frac{(2c-1)\,p}{2a}, \frac{c\,p}{a}\right)$. Similarly, $\left(\frac{a}{q}\right) = (-1)^N$ where N is the number of positive integers which fall into one of the open intervals $\left(\frac{q}{2a}, \frac{q}{a}\right), \left(\frac{3q}{2a}, \frac{2q}{a}\right), \ldots, \left(\frac{(2c-1)\,q}{2a}, \frac{c\,q}{a}\right)$.

If $q = p \pmod{4a}$, then $q = p + 4a\,r$ for some $r \in \mathbb{Z}$, and one observes that for any j the number M_j of positive integers which fall into the interval $\left(\frac{(2j-1)\,p}{2a}, \frac{j\,p}{a}\right)$ has the same parity that the number N_j of positive integers which fall into the interval $\left(\frac{(2j-1)\,q}{2a}, \frac{j\,q}{a}\right)$, so that M and N have the same parity, implying the equality of the Legendre symbols. Indeed, one notices that $\left(\frac{(2j-1)\,q}{2a}, \frac{j\,q}{a}\right) = \left(2r + \frac{(2j-1)\,p}{2a}, 4r + \frac{j\,p}{a}\right)$, and that the number of integers in an open interval (x, y) and the number of integers in the open interval $(x + 2r_1, y + 2r_2)$ have the same parity if $x < y$ and $x + 2r_1 < y + 2r_2$, and $r_1, r_2 \in \mathbb{Z}$.[6]

If $q = -p \pmod{4a}$, then $q = -p + 4a\,s$ for some $s \in \mathbb{Z}$, and one observes that for any j the number M_j of positive integers in the interval $\left(\frac{(2j-1)\,p}{2a}, \frac{j\,p}{a}\right)$ has the same parity than the number N_j of positive integers in the interval $\left(\frac{(2j-1)\,q}{2a}, \frac{j\,q}{a}\right)$, so that M and N have the same parity, implying the equality of the Legendre symbols. Indeed, one notices that $\left(\frac{(2j-1)\,q}{2a}, \frac{j\,q}{a}\right) = \left(2s - \frac{(2j-1)\,p}{2a}, 4s - \frac{j\,p}{a}\right)$, and that if $x < y < x + 2k$ the number of integers in (x, y) and the number of integers in $(-x - 2k, -y)$ have the same parity if y is not an integer, since by symmetry $(-x - 2k, -y)$ and $(y, x + 2k)$ have the same number of integers, and that the number of integers in (x, y) plus the number of integers in $(y, x + 2k)$ is the number of integers in $(x, x + 2k)$, i.e. $2k$.

Lemma 37.3: (law of quadratic reciprocity) One has $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\,\frac{q-1}{2}}$ for p and q distinct odd primes, i.e. $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$ if p or q has the form $4n+1$, and $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$ if both p and q have the form $4n+3$. Analytically, it means that if p and q are distinct odd primes, one has $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\,\frac{q-1}{2}}$.

---

[1] It is worth pointing out that GAUSS did not know about the Legendre symbol, and that LEGENDRE and EULER did not know about congruences, introduced by GAUSS.

[2] Lemma 37.2 follows from the law of quadratic reciprocity, but it is here a step towards its proof, and it will be used for proving the law of quadratic reciprocity.

[3] The intervals are chosen to be open since $j\,a$ cannot be a multiple of $\frac{p}{2}$.

[4] If $a = 2\alpha$, then $c = \alpha$ is the right answer because $\frac{(2\alpha-1)\,p}{2} < 2\alpha\,j < \alpha\,p$ implies $2j < p = 2q+1$, i.e. $j \leq m$, and $\frac{(2\alpha+1)\,p}{2} < 2\alpha\,j < (\alpha+1)\,p$ implies $2j > p + \frac{1}{2\alpha\,p} > 2q+1$, so that $j \geq m+1$.

[5] If $a = 2\beta+1$, then $c = \beta$ is the right answer because $\frac{(2\beta-1)\,p}{2} < (2\beta+1)\,j < \beta\,p$ implies $j < \frac{\beta}{2\beta+1}\,p < \frac{p}{2} = m + \frac{1}{2}$, i.e. $j \leq m$, and $\frac{(2\beta+1)\,p}{2} < (2\beta+1)\,j < (\beta+1)\,p$ implies $j > \frac{p}{2} = m + \frac{1}{2}$, so that $j \geq m+1$.

[6] If $x < y$, and n is a positive integer, each of the open intervals $(x - n, y)$ and $(x, y + n)$ contain n more integers than the open interval (x, y); one deduces that if $x_1 < y_1$, $x_2 < y_2$ with $x_1 - x_2 \in \mathbb{Z}$ and $y_1 - y_2 \in \mathbb{Z}$, then the number of integers in the open interval (x_1, y_1) has the same parity than the number of integers in the open interval (x_2, y_2) if (and only if) $(x_1 - x_2) \pm (y_1 - y_2)$ is even.

Proof: If $q = p \pmod 4$, one has $q = p + 4r$, so that $\left(\frac{q}{p}\right) = \left(\frac{p+4r}{p}\right) = \left(\frac{4r}{p}\right) = \left(\frac{r}{p}\right)$, and $\left(\frac{p}{q}\right) = \left(\frac{q-4r}{q}\right) = \left(\frac{-4r}{q}\right) = \left(\frac{-r}{q}\right) = \left(\frac{-1}{q}\right)\left(\frac{r}{q}\right)$. By Lemma 37.2 one has $\left(\frac{r}{p}\right) = \left(\frac{r}{q}\right)$, and one concludes by noticing that $\left(\frac{-1}{q}\right) = +1$ if both p and q have the form $4n+1$, and $\left(\frac{-1}{q}\right) = -1$ if both p and q have the form $4n+3$.

If $q = -p \pmod 4$ (i.e. among p and q one has the form $4n+1$ and the other has the form $4n+3$), one has $q = -p + 4s$, and one deduces that $\left(\frac{q}{p}\right) = \left(\frac{s}{p}\right)$, and $\left(\frac{p}{q}\right) = \left(\frac{s}{q}\right)$, and by Lemma 37.2 one has $\left(\frac{s}{p}\right) = \left(\frac{s}{q}\right)$, hence $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$.

Lemma 37.4: For p an odd prime, one has $\left(\frac{3}{p}\right) = +1$ if and only if p has the form $12n \pm 1$, and $\left(\frac{3}{p}\right) = -1$ if and only if p has the form $12n \pm 5$, so that one has $\left(\frac{-3}{p}\right) = +1$ if and only if p has the form $12n+1$ or $12+7$, and $\left(\frac{-3}{p}\right) = -1$ if and only if p has the form $12n+5$ or $12n-1$.

Proof: If p has the form $4n+1$, then by the law of quadratic reciprocity (Lemma 37.3) $\left(\frac{3}{p}\right) = \left(\frac{p}{3}\right)$, which is $= +1$ if $p = 1 \pmod 3$ (i.e. p has the form $12n+1$) and which is $= -1$ if $p = 2 \pmod 3$ (i.e. p has the form $12n+5$); for those primes $\left(\frac{-3}{p}\right) = \left(\frac{3}{p}\right)$ since $\left(\frac{-1}{p}\right) = +1$.

If p has the form $4n+3$, then by the law of quadratic reciprocity $\left(\frac{3}{p}\right) = -\left(\frac{p}{3}\right)$, which is $= -1$ if $p = 1 \pmod 3$ (i.e. p has the form $12n+7$) and which is $= +1$ if $p = 2 \pmod 3$ (i.e. p has the form $12n-1$); for those primes $\left(\frac{-3}{p}\right) = -\left(\frac{3}{p}\right)$ since $\left(\frac{-1}{p}\right) = -1$.

Lemma 37.5: There are infinitely many primes of the form $12n-1$, and there are infinitely many primes of the form $6n+1$.

Proof: If there were only a finite number of primes $11 = p_1 < \ldots < p_k$ of the form $12n-1$, then for $N = p_1 \cdots p_k$ any prime factor s of $12N^2 - 1$ would be either of the form $12n+1$ or of the form $12n-1$ by Lemma 37.4, since 3 is a quadratic residue modulo s, because $3(12N^2 - 1) = 0 \pmod s$ means $(6N)^2 = 3 \pmod s$; since the prime factors of $12N^2 - 1$ cannot all be of the form $12n+1$, because their product would have this form, there would be at least one prime factor s of the form $12n-1$, which could not belong to the list $\{p_1, \ldots, p_k\}$ made of divisors of N.

If there were only a finite number of primes $7 = q_1 < \ldots < q_k$ of the form $6n+1$, then for $M = q_1 \cdots q_k$ any prime factor t of $12M^2 + 1$ would be either of the form $12n+1$ or of the form $12n+7$ by Lemma 37.4 (hence of the form $6n+1$), since -3 is a quadratic residue modulo t, because $3(12M^2 + 1) = 0 \pmod t$ means $(6N)^2 = -3 \pmod t$, and it would contradict the fact that all primes of the form $6n+1$ divide M.

Lemma 37.6: For p an odd prime, one has $\left(\frac{5}{p}\right) = +1$ if and only if p has the form $5n \pm 1$, and $\left(\frac{5}{p}\right) = -1$ if and only if p has the form $5n \pm 2$.

Proof: Since 5 has the form $4n+1$, the law of quadratic reciprocity (Lemma 37.3) gives $\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right)$, which is $+1$ if p has the form $5n \pm 1$, and is -1 if p has the form $5n \pm 2$.

Lemma 37.7: There are infinitely many primes of the form $5n-1$.

Proof: If there were only a finite number of primes $19 = p_1 < \ldots < p_k$ of the form $5n-1$, then for $N = p_1 \cdots p_k$ any prime factor s of $5N^2 - 1$ would be of the form $5n \pm 1$ since 5 is a quadratic residue modulo s, because $5N^2 - 1 = 0 \pmod s$ implies $(5N)^2 = 5 \pmod s$; not all prime factors s would be of the form $5n+1$ since it would imply that $5N^2 - 1$ has this form, and a prime factor of the form $5n-1$ could not be in the list $\{p_1, \ldots, p_k\}$, made of divisors of $5N^2$.

Remark 37.8: DIRICHLET's proof that the arithmetic progression $a\,n + b$ contains infinitely many primes whenever $a \geq 3$ and $(a, b) = 1$ uses a special type of Dirichlet series (called a Dirichlet L-series) associated to a completely multiplicative function (called a *Dirichlet character*).

Definition 37.9: A *representation* of a group G on a vector space V over a field F is a group homomorphism ρ from G to $GL(V)$, the general linear group on V (invertible F-linear mappings from V into V), i.e. satisfying $\rho(g_1 g_2) = \rho(g_1)\,\rho(g_2)$ for all $g_1, g_2 \in G$; the representation is *faithful* if ρ is injective; the representation has *dimension* (or degree) n if V has dimension n, and it $n = 1$ it is called a *multiplicative character* (or *linear character*, or character). A representation ρ is *irreducible* if there are non non-trivial invariant subspace, i.e. if a subspace W of V is such that $\rho(g)$ maps W into W for all $g \in G$, then either $W = \{0\}$ or $W = V$. The *character* of a representation ρ of finite dimension is the mapping $g \mapsto \chi_\rho(g) = Trace\big(\rho(g)\big)$.[7]

[7] It is not in general an homomorphism of G into F^*.