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 $a^d=c_0+c_1a+\ldots+c_{d-1}a^{d-1}$, 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. $\sum_{j=0}^m\lambda_ja^j=0$ with $\lambda_0,\ldots,\lambda_m\in E$ not all 0, which means that the non-zero polynomial $P=\lambda_0+\lambda_1x+\ldots+\lambda_mx^m\in E[x]$ 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 $n^dP\big(\frac{a}{n}\big)$ is a non-zero integer, one has $1\leq\big|n^dP\big(\frac{a}{n}\big)\big|\leq C_1n^d\big|\xi-\frac{a}{n}\big|$ 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 $\cos 20^\circ$ 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 $4\cos^3 20^\circ - 3\cos 20^\circ = \frac{1}{2}$, 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 $8a^3 - 6a\,b^2 - b^3 = b^3 P\big(\frac{a}{b}\big) = 0$, so that a divides 1 and b^2 divides 8, but $a = 1$ and $b = \pm1, \pm2$ 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 $\cos 40^\circ$, their equation was $8x^3 - 6x + 1 = 0$.