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 $(a + b\sqrt{2})^2 = a^2 + 2b^2 + 2a\,b\sqrt{2}$, it means $a^2 + 2b^2 = 3$ and $a\,b = 0$, 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 $b^2 + a\,b + a^2 = 0$, 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 $\big(x + \frac{1}{2}\big)^2 + \frac{3}{4}$ 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 $P_1 = \big(x + \frac{\sqrt[3]{2}}{2}\big)^2 + \frac{3\sqrt[3]{4}}{4}$ 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.