UDK 512.44

H. Heineken (Math. Inst. Univ. Am Hubland, Würzbung, Germany)

SECTIONS OF ANGLES AND n-TH ROOTS OF NUMBERS

СЕГМЕНТИ КУТІВ І n-ТІ КОРЕНІ З ЧИСЕЛ

It is known since Galois that an algebraic equation can be solved using suitable n-th roots whenever the corresponding Galois group is soluble. The object of this note is the construction of real numbers by the use of n-th parts of suitable angles, and to state the necessary and sufficient condition for this to be possible.

Від Галуа відомо, що алгебраїчне рівняння можна розв'язати за допомогою n-х коренів щоразу, коли відповідна група Галуа є розв'язною. Метою даної статті є побудова дійсних чисел за допомогою n-х частин відповідних кутів та встановлення необхідної і достатньої умови, коли це можливо.

1. Introduction. Geometric constructions by ruler and compass have a long tradition; also the algebraic condition for a (finite) construction to be possible is well known for a long time. The restriction to these two tools has its reason in their simplicity and therefore in their reliability. A tool that allows the division of every angle into n equal parts can — in theory — be constructed as a mechanical device. Of course, every division of an angle into n equal parts can be executed by giving the cosine function of the new angle by an algebraic equation referring to the cosine function of the original angle, and for every n there is a polynomial P_n of degree n and with integers as coefficients such that $P_n(2\cos(\alpha)) = \cos(n\alpha)$. In this form the polynomial P_n will always have leading coefficient 1. The question, put in "geometric" terms, then has this form: *Which real algebraic numbers can be constructed by ruler, compass and divider of angles starting from a given real field F?* On the other hand, the "algebraic" form of this question is: *Which numbers can be reached by iterated extensions of K of the form $K[x]$ where $P_n(x) = k$ for $k \in K$ and some natural numbers n?*

First answers in this direction are known: If the Galois group is a 2-group, ruler and compass suffice; for the case that ruler, compass, and trisector (a device allowing the division of any angle into three parts) are at our disposal, the Galois group must be a $\{2, 3\}$-group with a condition on the subgroup which is the image of the real subfield of the splitting field. It will be seen that this is in fact the only condition needed in the general case.

In order to find a comparatively short formulation for our result, we use the following notation: An extension L of a field K is called a *subnormal* extension of K, if there is a sequence of fields

$$K = T_0 \subseteq T_1 \subseteq T_2 \subseteq \ldots \subseteq T_s = L$$

such that T_{i+1} is a normal extension of T_i for $0 \le i < s$. (By an obvious induction argument on the length of the series the following can be shown: If M is a normal extension of K and L is a subnormal extension of K such that $K \subseteq L \subseteq M$, then $\mathrm{Fix}_L \subseteq \mathrm{Gal}(M, K)$ is a subnormal subgroup of $\mathrm{Gal}(M, K)$. This may explain thai wording.) We will prove the following theorem.

Main Theorem. *Let K be a field of real numbers and a a real number which is algebraic over K, and let N be the smallest normal extension of K that contains a. Then a can be constructed by a succession of forming (real) square roots and division of angles if and only if the following two statements are true*:

(i) $\mathrm{Gal}(N, K)$ *is soluble*;

(ii) *there is a field L of real numbers such that $\langle K, a\rangle \subseteq L \subseteq N$ and L is a subnormal extension of K.*

The procedure follows mostly the steps taken in the case of roots, looking at the case of cyclic Galois groups first and proceeding by suitable iteration.

2. The primary step. We may restrict ourselves to the case of a normal extension N of degree p, an odd prime, of the real field F. We begin with a situation most similar to the division of an angle into p parts. In particular, we use the identity

$$\cos(\beta + \gamma) + \cos(\beta - \gamma) = 2\cos(\beta)\cos(\gamma).$$

We consider first a similar situation.

Lemma 1. *Assume that F is a field of real numbers and N is a normal extension of F of degree p. Assume further the existence of an element $a \in N\setminus F$ with minimal polynomial $Q(x)$. Denote the zeros of $Q(x)$ by $a_0 = a, a_1, a_2, \ldots, a_{p-1}$ in such a way that for some $\sigma \in \mathrm{Gal}(N, F)$ we have $\sigma(a_j) = a_{j+1}$, where the indices are taken modulo p. If $2\cos(2\pi/p) = c \in F$ and*

$$a_j - ca_{j+1} + a_{j+2} = 0,$$

then the zeros a_j are of the form $t\cos(\alpha + 2i\pi/p)$, where $2t\cos(p\alpha)$ and t^2 belong to F.

Proof. Let ξ be the p-th root of unity such that $\xi + \xi^{-1} = c$. The system of linear equations given is solved by the requirement $a_j = \lambda\xi^j + \mu\xi^{-j}$, and the fact that a_0 and a_1 are real numbers yield that μ is the complex number which is conjugate to λ. If t is the absolute value of λ, then $\lambda = te^{\alpha_i}$ for suitable α. But then $a_j = 2t\cos(\alpha + 2j\pi/p)$, and if $P_p(2\cos(\rho)) = 2\cos(p\rho)$, then $t^p(P_p(t^{-1}x) - 2\cos(p\rho))$ has the zeros a_j. The coefficients of this polynomial have to be contained in F, and only the constant term and the coefficients of odd powers are different from zero. Further, the coefficients of P_p are integers. So t^2 and $2t^p\cos(p\alpha)$ belong to F, the result follows.

We will now generalize Lemma 1 by deleting the linear relation among the zeros of the minimal polynomial. We want to show the following lemma.

Lemma 2. *Let p be an odd prime. If N is a normal extension of degree p of the field F of real numbers containing $\cos(2\pi/p)$. For every $b \in N\setminus F$, there is a linear combination a of the zeros of the minimal polynomial of b over F such that a and its images under powers of $\sigma \in \mathrm{Gal}(N, F)$ satisfy the equation of Lemma* 1.

Proof. Let $b_0 = b, b_1, \ldots, b_{p-1}$ be the zeros of the minimal polynomial of b, and assume that they are ordered such that $\sigma b_j = b_{j+1}$, where indices are taken modulo p. We have the identity

$$\sin(\beta + \gamma) + \sin(\beta - \gamma) = 2\cos(\gamma)\sin(\beta).$$

We will use this for $\gamma = 2\pi/p$ and for multiplies β of γ. Let $c_j = (\sin(j\gamma))(\sin(\gamma))^{-1}$. Notice that $c_0 = 0$ and that c_j is a polynomial in $\cos(\gamma)$ of degree $j-1$ for $j = 1, \ldots, (p-1)/2$, further $c_j = -c_{p-j}$. With these identities it can be shown that

$$a_k = \sum_{j=0}^{p-1} c_{j-k}b_j$$

is a collection of elements of the desired nature.

The attentive reader may have noticed that the element a constructed in Lemma 2 is not said to belong to $N \setminus F$. If $a \in F$, this element clearly would not help for our construction. The following observation allows us to overcome this.

Lemma 3. (A) *Lemma* 1 *and Lemma* 2 *remain true if* $\cos(2j\pi/p)$ *is taken for* $\cos(2\pi/p)$, *where* $j \in \{1, \ldots, (p-1)/2\}$.

(B) *Not all elements constructed in this way in Lemma* 2 *belong to* F.

Proof. Part (A) is true because the proofs given are correspondingly valid for these cases.

For part (B) we assume the contrary. We aim to show that the element b defined in Lemma 2 will belong to F already. We define $c(j, k)$ to be $(\sin(jk\pi/p))(\sin(k\pi/p))^{-1}$. Now we have the following equations, with $k = (p - 1)/2$:

$$\sum_{j=0}^{p-1} b_j = u_0,$$

$$\sum_{j=1}^{k} c(j,1)(b_j - b_{p-j}) = u_1,$$

$$\sum_{j=1}^{k} c(j,2)(b_j - b_{p-j}) = u_2,$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$\sum_{j=1}^{k} c(j,k)(b_j - b_{p-j}) = u_k,$$

so that we have $k + 1$ linear equations over F. Obviously $u_0 \in F$, all other u_j belong to F by our assumption. For given $m = 1, \ldots, k$ the factor $c(j, m)$ differs from $c(j, 1)$ by substitution of $\cos(2\pi/p)$ with $\cos(2m\pi/p)$, and the latter is a polynomial of degree m of the first. We consider the system of equations for $k \neq 0$. Arguing as for the Vaudermonde determinant we find that the coefficients on the left-hand of the equations form a linearly independent set, so all $b_j - b_{p-j}$ belong to F, and, using the element of $\mathrm{Gal}(N, F)$ we find that $b_k - b_{k+1} = b_{k+1} - b_{k+2} = \ldots = b_0 - b_1 = b_{k-1} - b_k$. Now using the first equation we have that $pb_0 \in F$, a contradiction to our construction. So not all u_m belong to F; Lemma 2 is proved.

***Corollary* 1.** *Assume that the following is true*:

(i) N *is a field of real numbers,*

(ii) N *is a normal extension of field* F *and* $|N : F| = p$, *where* p *is an odd prime,*

(iii) $\cos(2\pi/p) \in F$.

Then there is an extension G *of* F *such that* G *is a field of real numbers,* $|G : F| = 2^s$ *and* $N \subseteq G[\cos(\alpha_1), \cos(\alpha_2), \ldots, \cos(\alpha_r)]$ *with* $s \leq r \leq (p-1)/2$ *such that* $\cos(p\alpha_j) \in G$ *for all* j.

Proof. Let $N = F[b]$ for some element b and let $S(x)$ be the minimal polynomial of a over N. By Lemma 1 we have $k = (p - 1)/2$ many different constructions of linear combinations of the roots $b_0 = b, b_1, \ldots, b_{p-1}$, namely

$$u_i = \sum_{j=1}^{k} c(j,i)(b_j - b_{p-j}),$$

and we find by Lemma 1 that there is an element t_i for every i such that t_i^2 and $2t_i^p \cos(p\gamma_i)$ belong to F such that $u_i = t_i \cos(\gamma_i)$. The extension of F by means of all t_i just found leads to the extension G. Over G we have the equations on u_i as well as the given value

$$u_0 = \sum_{j=0}^{p-1} b_j$$

and the equations found from the above by the use of the galois automorphism:

$$v_i = \sum_{j=1}^{k} c(j,i)(b_{j-1} - b_{p-j-1}).$$

Now every b_j can be computed from these equations since the system of coefficients of the b_j is linearly independent. The numbers s, r will decrease whenever some u_i belongs to F. The proof is completed.

***Corollary* 2.** *If N is a real field and a normal extension of degree a prime p of the field F. Then the elements of N are contained in a field reached by almost $(p-1)/2$ steps of extensions, each describe by division of an angle into p equal parts.*

Remark. The construction given here may be considered the analogue of the use of iterated pure equations (extensions using polynomials $x^n - a$) for the solution by radicals (see [1, p. 177]).

3. The criterion.

Theorem 1. *Let x be a real number which is algebraic over the subfield F of R. The following statements are equivalent:*

(i) *x is contained in a subnormal extension S of F which is contained in R, and the Galois groups for the successive normal extensions taken are cyclic;*

(ii) *x is contained in a subnormal extension W of F which is contained in R, and in a subnormal extension W of F such that $\mathrm{Gal}(W, F)$ is soluble;*

(iii) *x can be reached by a series of steps explained in the Corollary.*

Proof. The equivalence of (i) and (iii) follows from Lemma 2 and Lemma 3. Assume now that (i) is satisfied, we want to show (ii). Let V be the minimal normal extension of F that contains S. Then the Galois duality connected with the Galois group $G = \mathrm{Gal}(V, F)$ will map S onto some subnormal subgroup K of G and, by minimality of V, the intersection of all conjugates of S will be trivial. Now the set $C(G, K)$ of all composition factors appearing in the normal chain from G to K coincides with the corresponding set $C(G, 1)$ by a classical theorem of Wielandt [2]. So (ii) is true with $W = V$. But also (i) follows from (ii) since $C(G, K) \subseteq C(G, 1)$ is always true.

Our Main Theorem now follows from Theorem 1.

4. Constructions with *p*-divider of angles. From now on a *p-divider* is supposed to mean a device to divide any given angle into p equal parts. We will use this for odd primes p only, and assume further to have ruler and compasses at our disposal. The use of compasses is equivalent to using a device dividing any angle into two equal parts. For instance, Theorem 1 yields the following proposition.

Proposition 1. *Let q be a prime such that $q - 1 = 2^m p^n$, where m, n are natural numbers and p is some odd prime. Then the regular q-gon can be constructed by ruler, compasses and p-divider.*

Proof. We obtain that $Q[\cos(2\pi/2)]$ is a normal extension of the rationals, of degree $(q-1)/2$ and consisting of real numbers. Furthermore the Galois group is cyclic. The result is therefore a consequence of Theorem 1.

Further Remarks.

1. The statement of Proposition 1 for $p = 3$ and $p = 5$ was shown in [3].

2. If $p \neq 2$ and the real root z of the polynomial $x^p - a$ with $a \in K$ is not contained in K, then this root is not constructible by use of a p-divider over K.

3. Allowing all intersections of definable conic sections leads to a wider variety than using only trisectors. The intersection of $xy = 2$ and of $x^2 - y = 0$ is not constructible by trisector by the previous remark (see also [3]).

1. *Van der Waerden B.* Algebra I: 4th edition. – Berlin etc., 1955.
2. *Wielandt H.* Eine Verallgemeinerung der invarianten Untergruppen // Math. Z. – 1939. – **45**. – S. 209 – 244.
3. *Heineken H.* Ruler, compass, and trisector // Ist. Lombardo (Rend. sci.). – 2000. – **A134**. – P. 87 – 98.

Received 28.02.2002