Polynomials, field extensions, and Euclidean constructions

In the following, F, G, H, K are fields, often assumed to be subfields of a larger field U (universe); typically $U = \mathbb{R}$ or $U = \mathbb{C}$. For the geometric constructions discussed below, we start with the field $F = \mathbb{Q}$ and extend it further and further finitely many times. All obtained fields will be subfields of $\mathbb{C}$.

Definitions

- We say that a polynomial $p(x) = c_n x^n + c_{n-1}x^{n-1} + \ldots + c_1 x + c_0$, $c_n \neq 0$, is a polynomial *over* F [or p is an F-polynomial] if all coefficients c_i are in F; the coefficient c_n is called the **leading coefficient**; p is **monic** if $c_n = 1$; the **degree** of p is n and is denoted by $deg(p)$. The 0 polynomial is considered to be an F-polynomial with no degree. The set of all F-polynomials is denoted by $F[x]$.

- Let $\alpha \in U$. We say that α is a **root** of p if $p(\alpha) = 0$. We say that α is **algebraic** over F [or α is F-algebraic] if there is a nonzero F-polynomial with root α. Note that α might be in F, but it might not. If α is F-algebraic, then among all nonzero F-polynomials with root α there is a *unique* monic polynomial of smallest possible degree; this is called the **minimal** polynomial of α over F. The **degree of α over F** is defined to be the degree of its minimum polynomial over F and is denoted by $deg_F(\alpha)$. [Note that the minimal polynomial cannot be a constant, so the degree of α is at least 1.]

- Let $a(x)$ and $b(x)$ be F-polynomials. We say that $b(x)$ **divides** $a(x)$ [or $a(x)$ is **divisible** by $b(x)$] if there exists an F-polynomial $q(x)$ such that $a(x) = q(x)b(x)$. An F-polynomial p is said to be **irreducible** over F if the only F-polynomials that divide p are constants and constant multiples of p itself [analogue of prime numbers]. We don't call constants irreducible [just as we don't call 1 a prime]. Hence, p is **reducible** means that there exist F-polynomials a and b both of degree at least 1 such that $p = ab$.

Theorem 1. *Let p be a polynomial over F, and let $\alpha \in F$. Then α is a root of p if and only if $p(x)$ is divisible by $(x - \alpha)$ (in which case the ratio q will automatically be over F). Consequently, a polynomial of degree n can have at most n roots (even with multiplicity).*

Theorem 2 (Polynomial Division). *Let $a, b \in F[x]$, $b \neq 0$. Then there are (unique) polynomials $q, r \in F[x]$ such that $a(x) = b(x)q(x) + r(x)$ and either r is 0 [the zero polynomial] or $deg(r) < deg(b)$.*

Theorem 3. *Let α be F-algebraic with minimal polynomial $m(x)$. If $f(x)$ is* any *F-polynomial with $f(\alpha) = 0$, then m divides f, that is, there is a $q \in F[x]$ such that $f = qm$. Consequently, if a monic polynomial $p \in F[x]$ is irreducible over F and $p(\alpha) = 0$, then p is the minimal polynomial of α.*

[Sketch of proof: divide f by m and substitute α for x.]

Corollary 4. *Since a cubic polynomial with rational coefficients but without rational roots is irreducible over $\mathbb{Q}$, hence all its roots are of degree 3 over $\mathbb{Q}$.*

Definition. *If F and K are fields and F is a subfield of K, then we write $F \leq K$ and say that K is an* **extension** *of F. It can then be seen that K is a vector space over F; the dimension (finite or infinite) of that vector space is called the* **degree** *of the extension and is denoted by $[K : F]$. We say that K is a finite extension of F if the degree $[K : F]$ is finite.*

Definition. *Given a field K and a set $S \subseteq K$, the field* **generated by** *S is the* **smallest** *subfield of K containing S, that is, the (unique) field $G \leq K$ with the following properties: (1) $S \subseteq G$, and (2) if $H \leq K$ is* any *field containing S then $G \leq H$.*

Theorem 5. *The field G described in the previous definition exists, and it is equal to the intersection of all subfields of K that contain S.*

Definition. *Let $F \leq K$ be fields, and let $\alpha \in K$. We obtain an extension of F by* **adjoining** *α to F: the extension $F(\alpha)$ is defined to be the smallest subfield of K containing F* and *α. In general, given a set $S \subseteq K$, the extension field $F(S)$ is the field generated by $F \cup S$. Clearly [by definition], $F \leq F(S) \leq K$.*

It is easy to see that if F is a subfield of K, then for any $\alpha \in K$, the extension field $F(\alpha)$ is

$$F(\alpha) = \{p(\alpha)/q(\alpha) \colon\ p(x), q(x) \in F[x],\ q(\alpha) \neq 0\}.$$

The following theorem is harder; it describes the extension field for F-algebraic numbers.

Theorem 6. *Let F be a subfield of a field K, and let $\alpha \in K$ be F-algebraic with degree d. Then $F(\alpha)$ is a finite extension of F and the degree of the extension $[F(\alpha) : F]$ equals d. The extension field has the explicit form $F(\alpha) = \{c_0 + c_1\alpha + \ldots + c_{d-1}\alpha^{d-1} : c_i \in F\}$.*

Theorem 7 (Product Rule). *Let $F \leq G \leq K$ be fields. If $[K : F]$ is finite then so are $[K : G]$ and $[G : F]$, and*

$$[K : F] = [K : G] \cdot [G : F]$$

Proof. K as a vector space over F was assumed to be finite-dimensional; let B be a basis there. Hence, by definition, $[K : F] = |B|$. Now B is a spanning set (though not necessarily a basis) in K even if K is considered as a vector space over G (since the "set of scalars" $F \subseteq G$); hence $[K : G] \leq |B| = [K : F] < \infty$. Also, G as a vector space over F is a subspace of K as a vector space over F, so its dimension $[G : F] \leq [K : F] < \infty$. It remains to prove the product formula. Let $g_1, \ldots, g_\ell$ be a basis of G over F, and let $k_1, \ldots, k_m$ be a basis of K over G. **Claim.** The set $S := \{g_i k_j : 1 \leq i \leq \ell,\ 1 \leq j \leq m\}$ is a basis of K over F. Proof: Step 1: S is spanning [easy]. Step 2: S is independent [easy].

The following theorem is the key to the Main Theorem (Gauss) about constructibility.

Corollary 8 (Divisibility Theorem). *Let $F \leq K$ be fields such that $[K : F] < \infty$. Let $\alpha \in K$ be arbitrary. Then α is algebraic over F, and $\deg_F(\alpha)$ divides $[K : F]$.*

Proof. Indeed, the fields $F \leq F(\alpha) \leq K$ satisfy the conditions of the Product Rule. Hence, the Product Rule and Theorem 6 together yield the Divisibility Theorem.

The above discussion leads to various constructibility criteria.

In the course of any specific Euclidean construction, only finitely many numbers are actually constructed. (We may consider a constructed point on the plane as a pair of real numbers or, alternatively, as one single complex number.) The field that these numbers generate (the smallest field which contains all of them) will be called "the field of the construction". Since every construction starts with 0 and 1, this field always contains $\mathbb{Q}$ as a subfield.

Theorem 9. *The order over $\mathbb{Q}$ of the field of any geometric construction is finite and is a power of 2.*

This, together with the Divisibility Theorem above imply the following *necessary* condition.

Corollary 10 (Main Theorem – Gauss). *Every constructible number (real or complex) is algebraic over $\mathbb{Q}$ and its degree is a power of 2.*

Corollary 11. *If a cubic polynomial with rational coefficients has no rational roots, then (by Corollary 4) its roots are of degree 3 over $\mathbb{Q}$ and hence they are not constructible.*

Corollary 12. *Doubling the cube (constructing $\sqrt[3]{2}$) and trisecting a 60° angle (constructing $\cos 20^\circ$) are both impossible using only straightedge and compass.*

Definition. *A prime number p is a* **Fermat prime** *if it is of the form $p = 2^k + 1$. It is easy to see that all Fermat primes are of the form $2^{2^i} + 1$. (The only known Fermat primes are: 3,5,17,257, and 65537.)*

Theorem 13 (Theorem of Gauss – long version). *A regular n-gon is constructible if and only if $n = 2^k$ or $n = 2^k p_1 p_2 \cdots p_\ell$ for some k and some* different *Fermat primes $p_1, p_2, \ldots, p_\ell$.*

For $n \in \mathbb{N}$, we define the Euler's (totient) function $\varphi(n)$ to be the number of integers between 1 and n that are relatively prime to n: $\varphi(n) := |\{k : 1 \leq k < n,\ gcd(k,n) = 1\}|$ (where *gcd* stands for *g*reatest *c*ommon *d*ivisor). φ is multiplicative in the following sense: if $gcd(m,n) = 1$, then $\varphi(mn) = \varphi(m)\varphi(n)$. Hence the explicit formula: If $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ where p_i are distinct primes, then $\varphi(n) = \prod_{i=1}^{k}(p_i^{\alpha_i} - p_i^{\alpha_i - 1}) = n\prod_{i=1}^{k}(1 - 1/p_i)$.

Theorem 14 (Theorem of Gauss – short version). *A regular n-gon is constructible (that is, the number $\alpha = e^{2\pi i/n}$ is constructible) if and only if $\varphi(n)$ is a power of two.*

The proof of Theorem 13 is reduced to the following proposition.

Theorem 15. *Let p be a prime. Then the polynomial $\Phi_p(x) = 1 + x + x^2 + \ldots + x^{p-1}$ is irreducible over $\mathbb{Q}$, and hence it is the minimal polynomial of $e^{2\pi i/p}$ over $\mathbb{Q}$.*

Proof. The claim easily follows by applying the following so-called Eisenstein criterion to $f(x) = \Phi_p(x+1) = \sum_{1 \leq k \leq p} \binom{p}{k} x^{k-1}$:

> If for an integer polynomial f there is a prime p such that p divides all coefficients except the leading one, but p^2 does not divide the constant term, then f is irreducible over $\mathbb{Q}$.

Remark. The following lemma is often useful to prove irreducibility over $\mathbb{Q}$ of polynomials with integer coefficients.

Lemma (Gauss Lemma). *If an integer polynomial factors over $\mathbb{Q}$, then it already factors over $\mathbb{Z}$. That is, if a polynomial $P(x) \in \mathbb{Z}[x]$ can be written as $P(x) = F(x)G(x)$ with $F(x), G(x) \in \mathbb{Q}[x]$, then there are $f(x), g(x) \in \mathbb{Z}[x]$ such that $deg(f) = deg(F)$, $deg(g) = deg(G)$, and $P(x) = f(x)g(x)$.*

Remark. The polynomial Φ_p mentioned in Theorem 15 is called a cyclotomic polynomial. For a general $n \in \mathbb{N}$, the cyclotomic polynomial is defined as follows. Let $\alpha = e^{2\pi i/n}$. Then,

$$\Phi_n(x) := \prod_{\substack{0<k\leq n \\ gcd(k,n)=1}} (x - \alpha^k) = \prod_{\substack{0<k\leq n \\ gcd(k,n)=1}} (x - e^{2\pi ik/n})$$

The polynomial $\Phi_n(x)$ is monic and of order $\varphi(n)$; it can be shown to have integer coefficients and to be irreducible over $\mathbb{Q}$. Hence Φ_n is the minimal polynomial of $\alpha = e^{2\pi i/n}$ over $\mathbb{Q}$.

Remark. The following decomposition is not hard to show:

$$x^n - 1 = \prod_{d|n} \Phi_d(x)$$

Hence,

$$\sum_{d|n} \varphi(d) = n$$

(but this is also easy to show directly).

Here are a few related websites:

www.math.niu.edu/∼beachy/abstract_algebra/study_guide/85.html#8501

www.wikipedia.org/wiki/Euler's_phi_function

www.wikipedia.org/wiki/Cyclotomic_polynomial

mathworld.wolfram.com/CyclotomicPolynomial.html