Algebraic Numbers

Antonio Caminha M. Neto

December 13, 2017

Estas notas são um extrato dos capítulos 19 e 20 de [2].

1 Algebraic numbers over $\mathbb{Q}$

A complex number α is said to be **algebraic** over $\mathbb{Q}$ if there exists a polynomial $f \in \mathbb{Q}[X] \setminus \{0\}$ such that $f(\alpha) = 0$. A complex number which is not algebraic over $\mathbb{Q}$ is said to be **transcendental** over $\mathbb{Q}$. In this section and the next one we stick to the case of algebraic numbers.

Obviously, every rational number r, being a root of the polynomial $X - r \in \mathbb{Q}[X] \setminus \{0\}$, is algebraic over $\mathbb{Q}$. In turn, the coming example collects less trivial instances of algebraic numbers over $\mathbb{Q}$.

Example 1.1. *Let $r \in \mathbb{Q}_+^*$ and $n \in \mathbb{N}$. If ω is an $n-$th root of unity, then $\sqrt[n]{r}\omega$ is algebraic over $\mathbb{Q}$, for such a number is a root of the nonzero polynomial with rational coefficients $X^n - r$.*

Example 1.2. *If $\alpha \neq 0$ is algebraic, then so are α^{-1} and α^2.*

If a complex number α is algebraic, the set

$$\mathcal{A}_\alpha = \{f \in \mathbb{Q}[X] \setminus \{0\};\, f(\alpha) = 0\}$$

is nonempty by definition. Then, it is also nonempty the set of nonnegative integers $\{\partial f;\, f \in \mathcal{A}_\alpha\}$, so that there exists $p_\alpha \in \mathcal{A}_\alpha$, monic and of minimum degree. We thus have the following

Definition 1.3. *Given a complex number α algebraic over $\mathbb{Q}$, a polynomial $p_\alpha \in \mathbb{Q}[X] \setminus \{0\}$, monic, of minimum degree and having α as a root is called a* **minimal polynomial** *for α.*

The coming proposition and its corollaries collect the most important properties of minimal polynomials of algebraic numbers.

Proposition 1.4. *If $\alpha \in \mathbb{C}$ is algebraic over $\mathbb{Q}$ and p_α is the minimal polynomial of α, then:*

(a) p_α is irreducible over $\mathbb{Q}$.

(b) If $f \in \mathbb{Q}[X]$ is such that $f(\alpha) = 0$, then $p_\alpha \mid f$ in $\mathbb{Q}[X]$.

In particular, p_α is uniquely determined by α.

Proof.
(a) If we had $p_\alpha = fg$, with f and g being nonconstant and of rational coefficients, then the degrees of f and g would be less than that of p_α and at least one of them would have α as a root. In turn, this would contradict the minimality of the degree of p_α. Therefore, p_α is irreducible over $\mathbb{Q}$.

(b) By the division algorithm, there exist polynomials $q, r \in \mathbb{Q}[X]$ such that

$$f(X) = p_\alpha(X)q(X) + r(X),$$

with $r = 0$ or $0 \leq \partial r < \partial p_\alpha$. If $r \neq 0$, then

$$r(\alpha) = f(\alpha) - p_\alpha(\alpha)q(\alpha) = 0,$$

with $\partial r < \partial p_\alpha$, and this would again be a contradiction to the minimality of the degree of p_α. Thus, $r = 0$ and, hence, $p_\alpha \mid f$ in $\mathbb{Q}[X]$.

Finally, if p_α and q_α were minimal polynomials for α, then item (b) would give $p_\alpha \mid q_\alpha$ in $\mathbb{Q}[X]$. However, since p_α and q_α are both monic and of the same degree, it would come that $p_\alpha = q_\alpha$. □

Thanks to the former proposition, given $\alpha \in \mathbb{C}$ algebraic, we can refer to p_α as being *the* minimal polynomial of α.

Corollary 1.5. *If $\alpha \in \mathbb{C}$ is algebraic and $f \in \mathbb{Q}[X] \setminus \{0\}$ is a monic, irreducible polynomial such that $f(\alpha) = 0$, then $f = p_\alpha$.*

Proof. By the previous result, p_α divides f in $\mathbb{Q}[X]$. However, since f is irreducible, there must exist a nonzero rational number c such that $f = cp_\alpha$. Finally, since f and p_α are both monic, we must have $c = 1$. □

Corollary 1.6. *If $f \in \mathbb{Q}[X] \setminus \mathbb{Q}$ is irreducible, then f has no multiple roots.*

Proof. We can assume, without any loss of generality, that f is monic. If some $\alpha \in \mathbb{C}$ is a multiple root of f, then α is also a root of the derivative f' of f. However, since $f \in \mathbb{Q}[X] \setminus \{0\}$ is monic and irreducible, Corollary 1.5 assures that it is the minimal polynomial of α. Therefore, Proposition 1.4 gives $f \mid f'$ in $\mathbb{Q}[X]$, which is a contradiction to the inequality $\partial f > \partial f'$. □

Example 1.7 (IMO shortlist)**.** *Let f be a nonconstant polynomial of rational coefficients and α a real number such that $\alpha^3 - 3\alpha = f(\alpha)^3 - 3f(\alpha) = -1$. Prove that, for every positive integer n, one has*

$$f^{(n)}(\alpha)^3 - 3f^{(n)}(\alpha) = -1,$$

where $f^{(n)}$ stands for the composite of f with itself, n times.

In the next example we shall use the fact (to be proved later) that if p is prime and $\omega = \operatorname{cis}\frac{2\pi}{p}$, then the minimal polynomial of ω is

$$p_\omega(X) = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

Example 1.8 (IMO)**.** *Let p be an odd prime. Compute how many are the $p-$element subsets of the set $\{1, 2, \ldots, 2p\}$ such that the sum of its elements is divisible by p.*

Example 1.9 (Romania)**.** *Let $f \in \mathbb{Z}[X]$ be a monic polynomial, of odd degree greater than 1 and irreducible over $\mathbb{Q}$. Suppose also that:*

(a) $f(0)$ is square-free.

(b) The complex roots of f have modulus greater than or equal to 1.

Prove that the polynomial $F \in \mathbb{Z}[X]$, given by $F(X) = f(X^3)$, is also irreducible over $\mathbb{Q}$.

Problems – Section 1

1. Given $k, n \in \mathbb{N}$, prove that $\cos\frac{2k\pi}{n}$ and $\sin\frac{2k\pi}{n}$ are algebraic.
2. Let $\alpha \in \mathbb{C}$ be algebraic. If there exists $f \in \mathbb{Z}[X] \setminus \mathbb{Z}$ monic and such that $f(\alpha) = 0$, prove that $p_\alpha \in \mathbb{Z}[X]$.
3. (Brazil) Prove that the polynomial $f(X) = X^5 - X^4 - 4X^3 + 4X^2 + 2$ does not admit any roots of the form $\sqrt[n]{r}$, with $r \in \mathbb{Q}$ and $n \in \mathbb{N}$, $n > 1$.
4. Let $\alpha \in \mathbb{C}$ be algebraic, with $\partial p_\alpha = n$, and define

$$\begin{aligned}\mathbb{Q}(\alpha) &= \{a_0 + a_1\alpha + \cdots + a_{n-1}\alpha^{n-1};\ a_0, a_1, \ldots, a_{n-1} \in \mathbb{Q}\}\\ &= \{f(\alpha);\ f \in \mathbb{Q}[X],\ \text{with } f = 0 \text{ or } \partial f \leq n-1\}.\end{aligned}$$

   The purpose of this problem is to show that $\mathbb{Q}(\alpha)$ is a subfield of $\mathbb{C}$. To this end, do the following items:

   (a) Show that $\mathbb{Q}(\alpha)$ is closed for addition, subtraction and multiplication.
   (b) Given $\beta \in \mathbb{Q}(\alpha)$, show that there exists a single $f \in \mathbb{Q}[X]$ such that $\beta = f(\alpha)$, with $f = 0$ or $\partial f \leq n-1$.
   (c) For $\beta = f(\alpha) \in \mathbb{Q}(\alpha) \setminus \{0\}$, with $f \in \mathbb{Q}[X]$ such that $\partial f \leq n-1$, show that $\gcd(f, p_\alpha) = 1$. Then, conclude that $\frac{1}{\beta} \in \mathbb{Q}(\alpha)$.

5. Given $a, b, c \in \mathbb{Q}$ such that $a + b\sqrt[3]{2} + c\sqrt[3]{4} \neq 0$, show that there exist $x, y, z \in \mathbb{Q}$ for which

$$\frac{1}{a + b\sqrt[3]{2} + c\sqrt[3]{4}} = x + y\sqrt[3]{2} + z\sqrt[3]{4}.$$

   Then, find x, y and z if $a = b = 1$, $c = 2$.

6. Let $\alpha \in \mathbb{C}$ be algebraic, with $\partial p_\alpha = n$, and $\mathbb{Q}(\alpha)$ be as in problem 4. Find all functions $\phi : \mathbb{Q}(\alpha) \to \mathbb{C}$ satisfying the following conditions, for all $u, v \in \mathbb{Q}(\alpha)$:

   (i) $\phi(u+v) = \phi(u) + \phi(v)$.

   (ii) $\phi(uv) = \phi(u)\phi(v)$.

7. If r is a nonzero rational and $\alpha \in \mathbb{C} \setminus \{0\}$ is algebraic, prove that $r\alpha$ is also algebraic.

8. If $\alpha, \beta \in \mathbb{C} \setminus \{0\}$ are algebraic, prove that so are $\alpha + \beta$, $\alpha\beta$ and α/β.

9. Let a_1, a_2, ..., a_n be natural numbers, and $\alpha = \sqrt{a_1} + \sqrt{a_2} + \cdots + \sqrt{a_n}$. If $\alpha \notin \mathbb{Z}$, prove that it is irrational.

2 Polynomials over $\mathbb{Z}_p$

It is a well known fact that for a prime $p \in \mathbb{Z}$, the set $\mathbb{Z}_p$ of congruence classes modulo p can be furnished with operations of addition, subtraction, multiplication and division quite similar to those of $\mathbb{C}$. In turn, thanks to such a resemblance, essentially all of the concepts and results on polynomials studied so far remain true within the set $\mathbb{Z}_p[X]$ of polynomials with coefficients in $\mathbb{Z}_p$. Our purpose here is to make explicit comments on some similarities and differences between polynomials over $\mathbb{Z}_p$ and over $\mathbb{K}$, with $\mathbb{K} = \mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$.

Given $f(X) = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{Z}[X]$, we define $\mathbb{Z}_p[X]$ to be the set of formal expressions $\overline{f}$ of the form

$$\overline{f}(X) = \overline{a}_n X^n + \cdots + \overline{a}_1 X + \overline{a}_0, \tag{1}$$

where $\overline{a}_0, \overline{a}_1, \ldots, \overline{a}_n$ respectively denote the congruence classes of a_0, a_1, ..., a_n modulo p. As before, such an $\overline{f}$ is called a **polynomial** over $\mathbb{Z}_p$.

The correspondence $f \mapsto \overline{f}$ defines a map

$$\begin{array}{rccc} \pi_p : & \mathbb{Z}[X] & \longrightarrow & \mathbb{Z}_p[X] \\ & f & \longmapsto & \overline{f} \end{array}$$

which is obviously surjective and is called the **canonical projection** of $\mathbb{Z}[X]$ onto $\mathbb{Z}_p[X]$. For $f, g \in \mathbb{Z}[X]$, it is immediate to verify that

$$\begin{array}{c} \overline{f}(X) = \overline{g}(X) \text{ in } \mathbb{Z}_p[X] \\ \Updownarrow \\ \exists h \in \mathbb{Z}[X];\ f(X) = g(X) + ph(X) \text{ in } \mathbb{Z}[X]. \end{array}$$

Equivalently, letting

$$p\,\mathbb{Z}[X] = \{ph;\ h \in \mathbb{Z}[X]\},$$

we have

$$\overline{f} = \overline{0} \Leftrightarrow f \in p\mathbb{Z}[X].$$

We extend the operations of addition and multiplication in $\mathbb{Z}_p$ to homonymous operations $+, \cdot : \mathbb{Z}_p[X] \times \mathbb{Z}_p[X] \to \mathbb{Z}_p[X]$ by setting, for $f, g \in \mathbb{Z}[X]$,

$$\overline{f} + \overline{g} = \overline{f+g} \text{ and } \overline{f} \cdot \overline{g} = \overline{fg}.$$

As in $\mathbb{Z}[X]$, we say that a polynomial $\overline{f} \in \mathbb{Z}_p[X] \setminus \{\overline{0}\}$ as in (1) has **degree** n if $\overline{a}_n \neq \overline{0}$, i.e., if $p \nmid a_n$. More generally, if $f \in \mathbb{Z}[X] \setminus p\mathbb{Z}[X]$, then $\overline{f} \neq \overline{0}$ and $\partial\overline{f} \leq \partial f$.

Example 2.1. *If $p \in \mathbb{Z}$ is a prime number and $k \in \mathbb{N}$, prove that $\binom{p^k}{j}$ is a multiple of p, for every integer $1 \leq j < p^k$.*

Example 2.2 (Romania)**.** *Prove that the number of odd binomial coefficients in the $n-$th line of Pascal's triangle is a power of 2.*

In order to define the polynomial function associated to a polynomial $\overline{f} \in \mathbb{Z}_p[X]$, we have to take some care. Firstly, note that if $f \in \mathbb{Z}[X]$ and $a, b \in \mathbb{Z}$ satisfy $a \equiv b \,(\mathrm{mod}\, p)$, then

$$f(a) \equiv f(b) \,(\mathrm{mod}\, p);$$

on the other hand, if $\overline{f} = \overline{g}$ in $\mathbb{Z}_p[X]$, we saw above that there exists $h \in \mathbb{Z}[X]$ such that $f(X) = g(X) + ph(X)$. Hence, for $a \in \mathbb{Z}$ we have

$$f(a) = g(a) + ph(a) \equiv g(a) \,(\mathrm{mod}\, p).$$

Given $\overline{f} \in \mathbb{Z}_p[X]$, the above comments allow us to define the **polynomial function** associated to $\tilde{f} : \mathbb{Z}_p \to \mathbb{Z}_p$ by setting, for $a \in \mathbb{Z}$,

$$\tilde{f}(\overline{a}) = \overline{g(a)}, \tag{2}$$

where $g \in \mathbb{Z}[X]$ is any polynomial for which $\overline{f} = \overline{g}$. Obviously, the image of $\tilde{f}$ is a finite set, for $\mathbb{Z}_p$ itself is finite. From now on, whenever there is no danger of confusion, we shall write (2) simply as

$$\overline{f}(\overline{a}) = \overline{f(a)}.$$

The coming example shows that, contrary to what happens with polynomials over $\mathbb{Q}$, $\mathbb{R}$ or $\mathbb{C}$, the polynomial function associated to a nonzero polynomial over $\mathbb{Z}_p[X]$ can vanish identically. In other words, *it is no longer valid* that two distinct polynomials over $\mathbb{Z}_p$ have distinct polynomial functions.

Example 2.3. *The polynomial $f(X) = X^p - X \in \mathbb{Z}_p[X]$ is clearly a nonzero element of $\mathbb{Z}_p[X]$. On the other hand, letting $\overline{f} : \mathbb{Z}_p \to \mathbb{Z}_p$ denote its associated polynomial function, Fermat's little theorem gives*

$$\overline{f}(\overline{a}) = \overline{a}^p - \overline{a} = \overline{a^p - a} = \overline{0}$$

for every $\overline{a} \in \mathbb{Z}_p$. Thus, $\overline{f}$ vanishes identically.

Let $f \in \mathbb{Z}[X]$ and $a \in \mathbb{Z}$ be given. We say that $\overline{a} \in \mathbb{Z}_p$ is a root of $\overline{f}$ provided $\overline{f}(\overline{a}) = \overline{0}$. An easy review of the proof of the root test shows that it continues to hold in $\mathbb{Z}_p[X]$. In particular, from the above example we obtain the following important result.

Proposition 2.4. *In $\mathbb{Z}_p[X]$, we have*

$$X^{p-1} - \overline{1} = (X - \overline{1})(X - \overline{2}) \dots (X - \overline{(p-1)}).$$

Proof. Since $\overline{1}, \overline{2}, \dots, \overline{p-1}$ are roots of $X^{p-1} - \overline{1}$ in $\mathbb{Z}_p$ (from the last example), we conclude that the polynomial $X^{p-1} - \overline{1}$ is divisible by $(X - \overline{1})(X - \overline{2}) \dots (X - \overline{(p-1)})$ in $\mathbb{Z}_p[X]$. However, since both such polynomials are monic and have degree $p - 1$, they are actually equal. □

In $\mathbb{Z}_p[X]$ the following theorem is valid.

Teorema 2.5. *If $p \in \mathbb{Z}$ is prime, then every polynomial $\overline{f} \in \mathbb{Z}_p[X] \setminus \mathbb{Z}_p$ can be written as a product of a finite number of irreducible polynomials over $\mathbb{Z}_p$. Moreover, such a decomposition of $\overline{f}$ is unique up to association and reordering of the irreducible factors.*

Example 2.6. *If $p \in \mathbb{Z}$ is an odd prime and d is a positive divisor of $p - 1$, then the algebraic congruence*

$$x^{p-1} - 1 \equiv 0 \,(\mathrm{mod}\, p) \tag{3}$$

has exactly $\varphi(d)$ roots of order d, pairwise incongruent modulo p. In particular, p has exactly $\varphi(p-1)$ primitive roots pairwise incongruent modulo p.

Example 2.7 (Miklós-Schweitzer)**.** *If $p > 3$ is a prime number satisfying $p \equiv 3 \,(\mathrm{mod}\, 4)$, prove that*

$$\prod_{1 \leq x \neq y \leq \frac{p-1}{2}} (x^2 + y^2) \equiv 1 \,(\mathrm{mod}\, p).$$

Problems – Section 2

1. Let $p > 2$ be a given prime. Find, if any, the roots of $X^{p-1} + \overline{1} \in \mathbb{Z}_p[X]$.
2. Given $f \in \mathbb{Z}[X]$ and an integer root a of f, prove that $\overline{a} \in \mathbb{Z}_p$ is a root of $\overline{f} \in \mathbb{Z}_p[X]$. In particular, conclude that if $\overline{a}_1, \dots, \overline{a}_k \in \mathbb{Z}_p$ are the roots of $\overline{f}$, then there exists $1 \leq j \leq k$ such that $a \equiv a_j \,(\mathrm{mod}\, p)$.
3. Show that $f(X) = X^3 - 15X^2 + 10X - 84 \in \mathbb{Z}[X]$ has no rational roots.
4. If $p \in \mathbb{Z}$ is prime and $f \in \mathbb{Z}[X]$, prove that $\overline{f}(X^p) = \overline{f}(X)^p$.

5. A polynomial $f \in \mathbb{Z}[X] \setminus \{0\}$ is **primitive** if the gcd of its nonzero coefficients is equal to 1. Prove that if $f, g \in \mathbb{Z}[X] \setminus \mathbb{Z}$ are primitive polynomials, then so is fg.

6. Let $p > 2$ be a prime number and $1 \leq d \leq p-1$ be an integer.
   (a) If $d \nmid (p-1)$, show that $X^d - \overline{1}$ has no roots in $\mathbb{Z}_p[X]$.
   (b) If $d \mid (p-1)$, factorise $X^d - \overline{1}$ in $\mathbb{Z}_p[X]$.

7. Let $p \geq 3$ be a prime number and, for $1 \leq j \leq p-1$, let $s_j(1, 2, \ldots, p-1)$ denote the $j-$th elementary symmetric sum of the natural numbers $1, 2, \ldots, p-1$. Prove that:
   (a) For $1 \leq j \leq p-2$, we have $s_j(1, 2, \ldots, p-1) \equiv 0 \,(\mathrm{mod}\, p)$.
   (b) $s_{p-1}(1, 2, \ldots, p-1) \equiv -1 \,(\mathrm{mod}\, p)$.

8. If a, b and c are the complex roots of the polynomial $X^3 - 3X^2 + 1$, show that $a^n + b^n + c^n \in \mathbb{Z}$ for every $n \in \mathbb{N}$, and that such a sum is always congruent to 1 modulo 17.

9. (France) For a given $n \in \mathbb{N}$, let I_n denote the number of odd coefficients of the polynomial $(X^2 + X + 1)^n$.
   (a) Compute I_{2^m}, for $m \in \mathbb{Z}_+$.
   (b) Show that, for $m \in \mathbb{N}$, we have
   $$I_{2^m - 1} = \frac{2^{m+1} + (-1)^{m+1}}{3}.$$

10. Prove **Lucas' theorem**: given natural numbers $m \geq n$ and a prime number p, if
    $$m = \sum_{j=0}^{k} m_j p^j \quad \text{and} \quad \sum_{j=0}^{k} n_j p^j$$
    are the representations of m and n in base p, then
    $$\binom{m}{n} \equiv \prod_{j=0}^{k} \binom{m_j}{n_j} \,(\mathrm{mod}\, p).$$
    In particular, conclude that:
    (a) $p \mid \binom{m}{n}$ if and only if $m_j < n_j$ for some $0 \leq j \leq k$.
    (b) Exactly $(m_0 + 1)(m_1 + 1) \ldots (m_k + 1)$ binomial numbers of the form $\binom{m}{n}$ are not divisible by p.
    (c) No binomial number of the form $\binom{p^{k+1}-1}{n}$ is divisible by p.

11. Let p be a prime number and $k \in \mathbb{N}$. Prove that
    $$\binom{p^k(p-1)}{l} \equiv \begin{cases} (-1)^q \,(\mathrm{mod}\, p), \text{ if } l = p^k q;\ 0 \leq q \leq p-1,\ q \in \mathbb{Z} \\ 0 \,(\mathrm{mod}\, p), \text{ otherwise.} \end{cases}.$$

3 Cyclotomic polynomials

The theory of polynomials over $\mathbb{Z}_p$, p prime, allows us to present some of the most elementary properties of the so-called *cyclotomic polynomials*; in particular, we will show that such polynomials are precisely the minimal polynomials of the complex roots of unity. As a byproduct of our study, we will use cyclotomic polynomials to prove a particular case of Dirichlet's theorem on primes in arithmetic progressions.

Given $n \in \mathbb{N}$, recall that the *primitive $n-$th roots of unity* are the complex numbers of the form ω_n^k, with $\omega_n = \text{cis}\,\frac{2\pi}{n}$ and $1 \leq k \leq n$ being relatively prime with n. In particular, there are exactly $\varphi(n)$ primitive $n-$th roots of unity, where $\varphi : \mathbb{N} \to \mathbb{N}$ stands for the Euler function. Given $m, n \in \mathbb{N}$, whenever there is no danger of confusion we shall write simply (m, n) to denote the gcd of m and n.

Definition 3.1. *For $n \in \mathbb{N}$, the* **$n-$th cyclotomic polynomial** *is the polynomial*

$$\Phi_n(X) = \prod_{\substack{1 \leq k \leq n \\ (k,n)=1}} (X - \omega_n^k). \tag{4}$$

It follows from the above definition that Φ_n is monic with degree $\partial\Phi_n = \varphi(n)$. The coming proposition collects other elementary properties of Φ_n.

Proposition 3.2. *For $n \in \mathbb{N}$, we have:*

(a) $X^n - 1 = \prod_{0<d|n} \Phi_d(X)$.

(b) $\Phi_n \in \mathbb{Z}[X]$.

(c) $\Phi_n(0) = 1$ *for* $n > 1$.

Proof.
(a) First of all, we have

$$\prod_{0<d|n} \Phi_d(X) = \prod_{0<d|n} \Phi_{n/d}(X) = \prod_{0<d|n} \prod_{\substack{1 \leq k \leq n/d \\ (k,n/d)=1}} (X - \omega_{n/d}^k)$$

$$= \prod_{0<d|n} \prod_{\substack{1 \leq k \leq n/d \\ (k,n/d)=1}} (X - \omega_n^{dk}).$$

Now, note that each integer $1 \leq m \leq n$ can be uniquely written as $m = dk$, with $d, k \in \mathbb{N}$ such that $0 < d \mid n$ and $\left(k, \frac{n}{d}\right) = 1$ (d is exactly $d = \gcd(m, n)$). Therefore, the last sum above is clearly equal to

$$\prod_{j=1}^{n} (X - \omega_n^j) = X^n - 1.$$

(b) Let us make induction on $n \in \mathbb{N}$, beginning with $\Phi_1(X) = X - 1 \in \mathbb{Z}[X]$. Given a natural number $n > 1$, assume, by induction hypothesis, that $\Phi_m \in \mathbb{Z}[X]$ for every integer $1 \leq m < n$. Then, if

$$g(X) = \prod_{\substack{1 \leq d < n \\ d|n}} \Phi_d(X),$$

we have $g \in \mathbb{Z}[X]$ and, by (a), $X^n - 1 = \Phi_n(X)g(X)$. Since g is monic (for we already know that each Φ_m is monic), the division algorithm guarantees that $\Phi_n \in \mathbb{Z}[X]$.

(c) For $n = 2$ this is a direct computation. For $n > 2$, arguing once more by induction, start by noticing that

$$X^2 - 1 = \Phi_1(X)\Phi_2(X) = (X - 1)\Phi_2(X);$$

hence, $\Phi_2(X) = X + 1$ and $\Phi_2(0) = 1$. Let $n > 1$ and suppose, as induction hypothesis, that $\Phi_m(0) = 1$ for every integer $2 \leq m < n$. Then, in the notations of the proof of (b), we have

$$g(0) = \Phi_1(0) \prod_{\substack{1 < d < n \\ d|n}} \Phi_d(0) = (-1) \prod_{\substack{1 < d < n \\ d|n}} \Phi_d(0) = -1,$$

and it follows from $X^n - 1 = \Phi_n(X)g(X)$ that

$$-1 = \Phi_n(0)g(0) = -\Phi_n(0),$$

as wished. □

Corollary 3.3. *If $p \in \mathbb{Z}$ is prime, then*

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

Proof. Item (a) of the previous proposition gives

$$X^p - 1 = \Phi_1(X)\Phi_p(X) = (X - 1)\Phi_p(X),$$

so that

$$\Phi_p(X) = X^{p-1} + X^{p-2} + \cdots + X + 1.$$

□

We now need to establish a simple auxiliary result.

Lemma 3.4. *Let $f, g \in \mathbb{Z}[X]$ and $p \in \mathbb{Z}$ be a prime number. If $\overline{g} \in \mathbb{Z}_p[X] \setminus \mathbb{Z}_p$ and $\overline{g}^2 \mid \overline{f}$ in $\mathbb{Z}_p[X]$, then $\overline{g} \mid \overline{f'}$ in $\mathbb{Z}_p[X]$.*

Proof. If $h \in \mathbb{Z}[X]$ is such that $\overline{f} = \overline{g}^2\overline{h}$ in $\mathbb{Z}_p[X]$, we know that there exists a polynomial $l \in \mathbb{Z}[X]$ such that

$$f(X) = g(X)^2 h(X) + pl(X)$$

in $\mathbb{Z}[X]$. Computing derivatives at both sides of this equality, we obtain

$$f'(X) = 2g(X)g'(X)h(X) + g(X)^2 h'(X) + pl'(X)$$

in $\mathbb{Z}[X]$, and hence

$$\overline{f'}(X) = \overline{g}(X)\big(\overline{2}\,\overline{g'}(X)\overline{h}(X) + \overline{g}(X)\overline{h'}(X)\big)$$

in $\mathbb{Z}_p[X]$. Therefore, $\overline{g} \mid \overline{f'}$ in $\mathbb{Z}_p[X]$. □

For our next result, recall that if ω is an $n-$th root of unity, then Proposition 1.4 guarantees that its minimal polynomial p_ω divides $X^n - 1$ in $\mathbb{Q}[X]$. Then, problem 2, page 3, assures that $p_\omega \in \mathbb{Z}[X]$.

Proposition 3.5. *Let $n, p \in \mathbb{N}$ be such that p is prime and $p \nmid n$. If ω is an $n-$th root of unity, then $p_\omega(X) = p_{\omega^p}(X)$.*

Proof. Let $\zeta = \omega^p$. Since both ω and ζ are roots of $X^n - 1$, item (b) of Proposition 1.4 shows that both p_ω and p_ζ divide $X^n - 1$. By contradiction, assume that $p_\omega \neq p_\zeta$. Then, the irreducibility of these polynomials assures, via Gauss' theorem, that $p_\omega p_\zeta$ divides $X^n - 1$ in $\mathbb{Z}[X]$, say

$$X^n - 1 = p_\omega(X)p_\zeta(X)u(X) \tag{5}$$

for some $u \in \mathbb{Z}[X]$.

If $g(X) = p_\zeta(X^p)$, then

$$g(w) = p_\zeta(\omega^p) = p_\zeta(\zeta) = 0$$

so that (once more by Proposition 1.4) p_ω divides g in $\mathbb{Z}[X]$. Let $v \in \mathbb{Z}[X]$ be such that $p_\omega v = g$. In $\mathbb{Z}_p[X]$, problem 4, page 6 gives

$$\overline{p}_\omega(X)\overline{v}(X) = \overline{g}(X) = \overline{p}_\zeta(X^p) = \big(\overline{p}_\zeta(X)\big)^p,$$

and Theorem 2.5 guarantees the existence of a monic and irreducible polynomial $\overline{h} \in \mathbb{Z}_p[X]$ such that $\overline{h} \mid \overline{p}_\omega, \overline{p}_\zeta$ in $\mathbb{Z}_p[X]$. It follows from (5) that $\overline{h}(X)^2 \mid (X^n - \overline{1})$ in $\mathbb{Z}_p[X]$, and the previous lemma gives that $\overline{h}(X) \mid \overline{n}X^{n-1}$ in $\mathbb{Z}_p[X]$. However, since $\overline{h}$ is monic and $\overline{n} \neq \overline{0}$, by applying once again Theorem 2.5 we obtain $1 \leq l \leq n-1$ such that $\overline{h}(X) = X^l$ in $\mathbb{Z}_p[X]$. Hence, $\overline{h}(X) \nmid (X^n - \overline{1})$ in $\mathbb{Z}_p[X]$, which is a contradiction. □

We can finally state and prove the desired result.

Teorema 3.6. *If $\omega_n = \operatorname{cis}\frac{2\pi}{n}$, then $p_{\omega_n} = \Phi_n$. In particular, $\Phi_n \in \mathbb{Z}[X]$ is irreducible in $\mathbb{Q}[X]$.*

Proof. Take $k \in \mathbb{N}$ such that $k > 1$ and $\gcd(k, n) = 1$, and let $k = p_1 \dots p_l$, with $p_1, \dots, p_l$ being primes not dividing n. Repeated applications of the previous proposition give us

$$p_{\omega_n} = p_{\omega_n^{p_1}} = p_{\omega_n^{p_1 p_2}} = \cdots = p_{\omega_n^{p_1 \cdots p_l}} = p_{\omega_n^k}.$$

In particular, the $\varphi(n)$ complex numbers ω_n^k, with $1 \leq k \leq n$ and $\gcd(k, n) = 1$, are distinct roots of p_{ω_n}, so that

$$\partial p_{\omega_n} \geq \varphi(n) = \partial \Phi_n.$$

However, since Φ_n is monic, has integer (thus rational) coefficients and ω_n as a root, the definition of minimal polynomial assures that $p_{\omega_n} = \Phi_n$. □

Example 3.7 (Dirichlet)**.** *If $n \in \mathbb{N}$, then the arithmetic progression $1, 1+n, 1+2n, \dots$ contains infinitely many primes.*

Example 3.8. *For each prime number p, let $g(p) \in \mathbb{N}$ denote the least positive prime root modulo p. Then, the function $p \mapsto g(p)$ is unbounded.*

Problems – Section 3

1. Let $p, k \in \mathbb{N}$ be given, with p being prime. Compute Φ_{p^k} explicitly.
2. If m and n are distinct naturals, prove that Φ_m and Φ_n have no nonconstant common factors in $\mathbb{C}[X]$. In particular, $\Phi_m \neq \Phi_n$.
3. Let $n > 1$ be a natural number and d be the product of the distinct prime factors of n. Show that $\Phi_n(X) = \Phi_d\left(X^{n/d}\right)$.
4. (England) The set $\left\{1, \frac{1}{2}, \frac{1}{3}, \frac{1}{4}, \dots\right\}$ contains several arithmetic progressions. Given an integer $k > 2$, prove that it contains an arithmetic progression of k terms which is not contained in any arithmetic progression of $k + 1$ terms of the same set.
5. Let $a, n \in \mathbb{N}$, with $a > 1$ and n odd. Prove that the algebraic congruence $x^n \equiv a \pmod{p}$ has a solution for infinitely many primes p.
6. Let a be a natural number which is not a perfect square. Prove that there are infinitely many prime numbers p for which a is a non-quadratic residue modulo p.
7. Let $a, b \in \mathbb{Z}$ be such that for each $n \in \mathbb{N}$ there exists $c \in \mathbb{Z}$ for which $n \mid (c^2 + ac + b)$. Prove that the equation $x^2 + ax + b = 0$ has integer roots.

4 Algebraic numbers over $\mathbb{Z}_p$

This section is somewhat more abstract that the previous ones, for we extend the concept of algebraic number to consider algebraic numbers over $\mathbb{Z}_p$, for some prime number p. However, the payoff will be worth the effort, for, given $n \in \mathbb{N}$, we will be able to compute the exact number of irreducible polynomials over $\mathbb{Z}_p$ and having degree n.

We depart from a naive though profitable idea, namely, that there exists a *number set* Ω_p containing $\mathbb{Z}_p$ that plays, for $\mathbb{Z}_p$, the same role as $\mathbb{C}$ plays for $\mathbb{Q}$. We start by formalizing the concept of *field*.

Definition 4.1. *A* **field** *is a nonempty set $\mathbb{K}$, furnished with operations $+, \cdot : \mathbb{K} \times \mathbb{K} \to \mathbb{K}$ having the following properties:*

(a) $+$ and $\cdot$ are commutative and associative, and $\cdot$ is distributive with respect to $+$.

(b) There exist elements $0, 1 \in \mathbb{K}$, with $0 \neq 1$, such that $a + 0 = a$ and $a \cdot 1 = a$, for every $a \in \mathbb{K}$.

(c) For every $a \in \mathbb{K}$, there exists an element $-a \in \mathbb{K}$ such that $a + (-a) = 0$.

(d) For every $a \in \mathbb{K} \setminus \{0\}$, there exists an element $a^{-1} \in \mathbb{K}$ such that $a \cdot a^{-1} = 1$.

The reader has certainly realized what we mean by *commutative*, *associative* and *distributive* from his/her previous experience. Nevertheless, let us explain all that from first principles. Commutativity in item (a) means that

$$a + b = b + a \quad \text{and} \quad a \cdot b = b \cdot a,$$

whereas associativity stands for

$$(a + b) + c = a + (b + c) \quad \text{and} \quad (a \cdot b) \cdot c = a \cdot (b \cdot c),$$

for all $a, b, c \in \mathbb{K}$. In turn, the distributivity of $\cdot$ with respect to $+$ is exactly what one expects:

$$a \cdot (b + c) = a \cdot b + a \cdot c,$$

with the right hand side being a shorthand for the more precise (though somewhat cumbersome) expression $(a \cdot b) + (a \cdot c)$.

Thus, we surely have that $\mathbb{Q}$, $\mathbb{R}$ and $\mathbb{C}$ are fields, and problem 4, page 3 shows that so is $\mathbb{Q}(\alpha)$, for every $\alpha \in \mathbb{C}$ algebraic over $\mathbb{C}$. Moreover, in all of these cases, the elements 0 and 1 of item (b) in the above definition are the usual complex numbers 0 and 1, and this is the reason why, for a general field $\mathbb{K}$, we also denote them by 0 and 1. A similar remark holds for $-a$ and a^{-1}, i.e., we are simply adopting the same notation we use for the additive (resp. multiplicative) inverses of elements of $\mathbb{C}$ (resp. of $\mathbb{C} \setminus \{0\}$).

Another class of examples of fields we have been dealing with is that of the finite fields $\mathbb{Z}_p$, with $p \in \mathbb{Z}$ prime. In this case, however, we shall stick to the

usage of writing $\overline{0}$ and $\overline{1}$ whenever convenient, in order to avoid any possibility of confusion with $0, 1 \in \mathbb{Z}$.

Back to a general field $\mathbb{K}$, the *cancellation laws* for addition and multiplication hold:

$$a + c = b + c \Rightarrow a = b \text{ and } a \cdot c = b \cdot c,\ c \neq 0 \Rightarrow a = b.$$

Indeed,

$$\begin{aligned} a + c = b + c &\Rightarrow (a + c) + (-c) = (b + c) + (-c) \\ &\Rightarrow a + (c + (-c)) = b + (c + (-c)) \\ &\Rightarrow a + 0 = b + 0 \Rightarrow a = b, \end{aligned}$$

and likewise for the multiplication.

As it happens within $\mathbb{C}$, whenever there is no danger of confusion we shall write ab instead of $a \cdot b$, to denote the product of elements a and b of a general field $\mathbb{K}$.

We could have developed most of the theory of polynomials by considering the set $\mathbb{K}[X]$ of polynomials over (or with coefficients in) an arbitrary field $\mathbb{K}$, with operations $+, \cdot : \mathbb{K}[X] \times \mathbb{K}[X] \to \mathbb{K}[X]$ extending those of $\mathbb{K}$. Taking for granted the (harmless) assumption that we have done that, we now have at our disposal the following concepts and facts, whose validities the reader can easily check:

1. If $f, g \in \mathbb{K}[X]$ are such that $fg = 0$ (the identically zero polynomial), then $f = 0$ or $g = 0$.

2. The notions of degree (for nonzero polynomials) and roots for polynomials over $\mathbb{K}$ remain true, unchanged. Likewise, $\partial(fg) = \partial f + \partial g$ if $f, g \neq 0$ and $\partial(f + g) \leq \max\{\partial f, \partial g\}$ if $f + g \neq 0$.

3. The division algorithm, the root test and Lagrange's theorem on the number of distinct roots of a nonzero polynomial also continue to hold, with identical proofs.

4. The concept of greatest common divisor for nonzero polynomials over $\mathbb{K}$ is a direct extension from that for polynomials over $\mathbb{Q}$, and Bézout's theorem is also true, with exactly the same proof.

5. Another concept that extends in a likewise manner from $\mathbb{Q}[X]$ is that of irreducible polynomial $f \in \mathbb{K}[X]$. We also have unique factorisation.

A major gap on extending the theory for polynomials over arbitrary fields is fulfilled by the coming result, which will be assumed without proof (we refer the interested reader to [1] or [3]).

Teorema 4.2. *Given an arbitrary field $\mathbb{K}$, there exists another field Ω containing $\mathbb{K}$, whose operations extend those of $\mathbb{K}$ and such that every $f \in \mathbb{K}[X]$ has at least one root in Ω.*

The field Ω plays the role of $\mathbb{C}$ for $\mathbb{K}$. We refer to the property of Theorem 4.2 by saying that Ω is an **algebraically closed** field containing $\mathbb{K}$. Also as with $\mathbb{C}$, one now proves that if $f \in \mathbb{K}[X] \setminus \{0\}$ has degree n, then there exists $a \in \mathbb{K}$ (the leading coefficient of f) and $\alpha_1, \ldots, \alpha_n \in \Omega$ such that

$$f(X) = a(X - \alpha_1)(X - \alpha_2) \ldots (X - \alpha_n).$$

The equality above is the **factorised form** of f over Ω.

We can now define, exactly as was done in Section 1, what one means for an element $\alpha \in \Omega$ to be *algebraic* over $\mathbb{K}$, and consider its *minimal polynomial* $p_\alpha \in \mathbb{K}[X] \setminus \{0\}$ as was done for $\alpha \in \mathbb{C}$ algebraic over $\mathbb{Q}$. This way, Proposition 1.4 and Corollary 1.5 remain true, unchanged.

We now restrict our attention to $\mathbb{K} = \mathbb{Z}_p$, and write Ω_p to denote the field Ω of Theorem 4.2. We first recall the result of problem 4, page 6, which we write in the following form:

$$f(X^p) = f(X)^p, \ \forall \ f \in \mathbb{Z}_p[X]. \tag{6}$$

We shall also need the following auxiliary result.

Lemma 4.3. *Let $f \in \Omega_p[X] \setminus \{0\}$ be given. If $\alpha \in \Omega_p$ is a root of f, then:*

(a) α^p is also a root of f.

(b) There exists a natural number $m \leq \partial f$ such that α is a root of $X^{p^m} - X$.

Proof.
(a) It follows from (6) that $f(\alpha^p) = f(\alpha)^p = \overline{0}^p = \overline{0}$.

(b) Iterating the result of (a), we conclude that α, α^p, α^{p^2}, ... are roots of f. Since it has at most ∂f distinct roots, we conclude that there exist integers $0 \leq k < l \leq \partial f$ for which $\alpha^{p^k} = \alpha^{p^l}$. Therefore,

$$\overline{0} = \alpha^{p^l} - \alpha^{p^k} = \left(\alpha^{p^{l-k}}\right)^{p^k} - \alpha^{p^k} = \left(\alpha^{p^{l-k}} - \alpha\right)^{p^k},$$

where we have used the result of Example 2.1 in the last equality above. It comes that $\alpha^{p^{l-k}} - \alpha = 0$, and α is a root of $X^{p^m} - X$, with $m = l - k \leq \partial f$. □

We are now in position to prove the following

Proposition 4.4. *Let p be prime and $\alpha \in \Omega_p$ be algebraic over $\mathbb{Z}_p$. If $\partial p_\alpha = n$, then:*

(a) α is a root of $X^{p^n} - X$.

(b) α is not a root of $X^{p^m} - X$, for any positive integer $m < n$.

Proof. We already know, from the previous lemma, that α is a root of $X^{p^m}-X$, for any positive integer $m \leq n$. Now, let

$$\Phi : \underbrace{\mathbb{Z}_p \times \mathbb{Z}_p \times \ldots \times \mathbb{Z}_p}_{n \text{ times}} \longrightarrow \Omega_p$$

be defined by

$$\Phi(\overline{a}_0, \overline{a}_1, \ldots, \overline{a}_{n-1}) = \overline{a}_0 + \overline{a}_1\alpha + \cdots + \overline{a}_{n-1}\alpha^{n-1}.$$

We claim that Φ is injective and each $\beta \in \mathrm{Im}(\Phi)$ is a root of $X^{p^m} - X$. Indeed, if

$$\Phi(\overline{a}_0, \overline{a}_1, \ldots, \overline{a}_{n-1}) = \Phi(\overline{b}_0, \overline{b}_1, \ldots, \overline{b}_{n-1}),$$

for distinct $n-$tuples $(\overline{a}_0, \overline{a}_1, \ldots, \overline{a}_{n-1})$ and $(\overline{b}_0, \overline{b}_1, \ldots, \overline{b}_{n-1})$ in the domain of Φ, then

$$(\overline{a}_0 - \overline{b}_0) + (\overline{a}_1 - \overline{b}_1)\alpha + \cdots + (\overline{a}_{n-1} - \overline{b}_{n-1})\alpha^{n-1} = \overline{0},$$

so that α would be a root of the nonzero polynomial $(\overline{a}_0 - \overline{b}_0) + (\overline{a}_1 - \overline{b}_1)X + \cdots + (\overline{a}_{n-1} - \overline{b}_{n-1})X^{n-1}$ of $\mathbb{Z}_p[X]$. Since $\partial p_\alpha = n$, this is a contradiction.

For the second part, let $\beta = \overline{a}_0 + \overline{a}_1\alpha + \cdots + \overline{a}_{n-1}\alpha^{n-1}$. The result of Example 2.1 gives, together with Fermat's little theorem and $\alpha^{p^m} = \alpha$, gives

$$\begin{aligned}
\beta^{p^m} &= \left(\overline{a}_0 + \overline{a}_1\alpha + \cdots + \overline{a}_{n-1}\alpha^{n-1}\right)^{p^m} \\
&= \overline{a}_0^{p^m} + \overline{a}_1^{p^m}\alpha^{p^m} + \cdots + \overline{a}_{n-1}^{p^m}\alpha^{(n-1)p^m} \\
&= \overline{a}_0 + \overline{a}_1\alpha + \cdots + \overline{a}_{n-1}\alpha^{n-1} \\
&= \beta
\end{aligned}$$

Let $\mathcal{R}_m$ stand for the set of roots of $X^{p^m} - X$ in Ω_p. The above claims then assure that $|\mathcal{R}_m| \geq p^n$, so that $p^m \geq p^n$ and, hence, $m \geq n$. Since $m \leq n$, we then get $m = n$, and items (a) and (b) follow at once. □

A direct consequence of this proposition is the coming

Corollary 4.5. *Let p be prime and $\alpha \in \Omega_p$ be algebraic over $\mathbb{Z}_p$. If $\partial p_\alpha = n$, then $p_\alpha \mid \left(X^{p^n} - X\right)$ in $\mathbb{Z}_p[X]$.*

Proof. This follows from the previous result, together with the analogue of Proposition 1.4 in our setting. □

Another consequence is collected as the next result.

Lemma 4.6. *Let $f \in \mathbb{Z}_p[X]\backslash\mathbb{Z}_p$ be irreducible and of degree d. If $f \mid (X^{p^n} - X)$, then $d \mid n$.*

Proof. If $\alpha \in \Omega_p$ is a root of f, then $f = p_\alpha$, and the previous corollary guarantees that $f \mid (X^{p^d} - X)$ and $f \nmid (X^{p^k} - X)$, for every positive integer $k < d$. Since $f \mid (X^{p^n} - X)$, we conclude that $d \leq n$.

Now, let $n = d + t$ and write

$$\begin{aligned} X^{p^n} - X &= X^{p^{d+t}} - X = \left(X^{p^d}\right)^{p^t} - X^{p^t} + X^{p^t} - X \\ &= \left(X^{p^d} - X\right)^{p^t} + X^{p^t} - X. \end{aligned}$$

It readily follows from this equality that

$$\gcd\left(X^{p^n} - X, X^{p^d} - X\right) = \gcd\left(X^{p^t} - X, X^{p^d} - X\right).$$

Assume that $n = dq + r$, with $0 < r < d$. Iterating the gcd equality above, we get

$$\gcd\left(X^{p^n} - X, X^{p^d} - X\right) = \gcd\left(X^{p^r} - X, X^{p^d} - X\right). \tag{7}$$

Since f divides the left hand side, it also divides the right hand side. In particular, $f \mid (X^{p^r} - X)$, which is a contradiction. □

We can finally state and prove our main result, for which we let

$a_n = \#\{\text{monic, pairwise distinct irreducible polynomials of degree } n \text{ in } \mathbb{Z}_p[X]\}$.

Also, if $a_n > 0$, we write f_{n1}, f_{n2}, …, f_{na_n} to denote such polynomials.

Teorema 4.7. *Let p be prime and $n \in \mathbb{N}$. Then,*

$$X^{p^n} - X = \prod_{0<d|n} f_{d1}(X) \dots f_{da_d}(X), \tag{8}$$

with the product $f_{d1} \dots f_{da_d}$ taken as 1 if $a_d = 0$.

Proof. Unique factorisation assures that $X^{p^n} - X$ is the product of finitely many irreducible polynomials, which can all be assumed to be monic.

If f is one such polynomial, with $\partial f = d$, the previous lemma shows that $d \mid n$, so that f is one of the polynomials in the right hand side of (8). Conversely, if $0 < d \mid n$, $1 \leq j \leq a_d$ and $\alpha \in \Omega_p$ is a root of f_{dj}, then $f_{dj} = p_\alpha$, and Corollary 4.5 guarantees that $f_{dj} \mid \left(X^{p^d} - X\right)$ in $\mathbb{Z}_p[X]$. However, since $d \mid n$, the argument in the proof of the previous lemma leading to (7) shows that $\left(X^{p^d} - X\right) \mid \left(X^{p^n} - X\right)$ in $\mathbb{Z}_p[X]$. Therefore, $f_{dj} \mid \left(X^{p^n} - X\right)$ in $\mathbb{Z}_p[X]$. □

Example 4.8. *If p is prime and $n \in \mathbb{N}$, show that $a_n = \frac{1}{n}\sum_{0<d|n} \mu\left(\frac{n}{d}\right) p^d > 0$.*

Problems – Section 4

1. Let p be prime and $n \in \mathbb{N}$. If $0 < d \mid n$, then $X^{p^n} - X$ has an irreducible factor of degree d.

2. Let p be prime and, for $n \in \mathbb{N}$, let $\mathcal{R}_n$ denote the set of roots of $X^{p^n} - X$ in Ω_p. Show that $\mathcal{R}_n$ is a subfield of Ω_p containing $\mathbb{Z}_p$.

3. In the notations of the statement of Theorem 4.7, show that $a_2 = \binom{p}{2}$ and

$$f_{21}(X) \dots f_{2a_2}(X) = (X^p - X)^{p-1} + \overline{1}.$$

4. Let $\mathbb{K}$ be any field. Prove that $\mathbb{K}[X]$ has infinitely many irreducible polynomials.

References

[1] R. Ash. *Basic Abstract Algebra: for Graduate Students and Advances Undergraduates*. Mineola, Dover, 2006.

[2] A. Caminha. *An Excursion Through Elementary Mathematics III*. Springer Nature, Cham, 2018.

[3] C. R. Hadlock. *Field Theory and its Classical Problems*. Washington, MAA, 2000.