Further linear algebra. Chapter II. Polynomials.

Andrei Yafaev

1 Definitions.

In this chapter we consider a field k. Recall that examples of felds include $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_p$ where p is prime.

A polynomial is an expression of the form

$$f(x) = a_0 + a_1 x + \cdots + a_d x^d = \sum a_n x^n, \quad a_0, \ldots, a_d \in k$$

The elements a_is are called **coefficients** of f. If all a_is are zero, then f is called a **zero** polynomial (notation: $f = 0$).

If $f \neq 0$, then the **degree** of f (notation $\deg(f)$) is by definition the largest integer $n \geq 0$ such that $a_n \neq 0$.

If $f = 0$, then, by convention, $\deg(f) = -\infty$.

Addition and multiplication are defined as one expects: if $f(x) = \sum a_n x^n$ and $g(x) = \sum b_n x^n$ then we define

$$(f+g)(x) = \sum (a_n + b_n) x^n,$$

$$(fg)(x) = \sum c_n x^n,$$

where

$$c_n = \sum_{i=0}^{n} a_i b_{n-i}.$$

Notice that we always have:

$$\deg(f \times g) = \deg(f) + deg(g).$$

(we are using the convention that $-\infty + n = -\infty$). Notice also that

$$\deg(f + g) \leq \max\{\deg(f), \deg(g)\}$$

If $f = \sum a_n X^n \neq 0$ has degree d, the the coefficient a_d is called the **leading coefficient** of f. If f has leading coefficient 1 then f is called **monic**.

Two polynomials are **equal** if all their coefficients are equal.

Example 1.1 $f(x) = x^3 + x + 2$ *has degree 3, and is monic.*

The set of all polynomials with coefficients in k is denoted by $k[x]$.

The polynomials of the form $f(x) = a_0$ are called **constant** and a constant polynomial of the form $f(x) = a_0 \neq 0$ is called a **unit** in $k[x]$. In other words, units are precisely non-zero constant polynomials. Another way to put it: units are precisely polynomials of degree zero. Units are analogous to $\pm 1 \in \mathbb{Z}$. Notice that a unit is monic if it is just 1.

Given $f, g \in k[x]$, we say that g **divides** f is there exists a polynomial $h \in k[x]$ such that

$$f = gh$$

Clearly, a unit divides any polynomial. Also for any polynomial f, f divides f.

A non-zero polynomial is called **irreducible** is it is not a unit and whenever $f = gh$ with $g, h \in k[x]$, either g or h must be a unit. In other words, the only polynomials that divide f are units and f itself. Irreducible polynomials are analogues of prime numbers from Chapter I.

If f divides g i.e. $f = gh$, then

$$\deg(f) = \deg(g) + \deg(h) \leq \deg(g)$$

We prove the following:

Proposition 1.2 *Let* $f \in k[x]$. *If* $\deg(f) = 1$ *then* f *is irreducible.*

Proof. Suppose $f = gh$. Then $\deg(g) + \deg(h) = 1$. Therefore the degrees of g and h are 0 and 1, so one of them is a unit. $\square$

The property of being irreducible depends on the field k!

For example, the polynomial $f(x) = x$ is irreducible no matter what k is. If $k = \mathbb{R}$, then $f(x) = x^2 + 1$ is irreducible. However, if $k = \mathbb{C}$, then $x^2 + 1 = (x + i)(x - i)$ is reducible.

Similarly $x^2 - 2$ factorises in $\mathbb{R}[X]$ as $(x+\sqrt{2})(x-\sqrt{2})$, but is irreducible in $\mathbb{Q}[X]$ (since $\sqrt{2}$ is irrational).

We have the following theorem:

Theorem 1.3 (Fundamental Theorem of Algebra) *Let $f \in \mathbb{C}[x]$ be a non-zero polynomial. Then f factorises as a product of linear factors (i.e polynomials of degree one):*

$$f(X) = c(x - \lambda_1) \cdots (x - \lambda_d)$$

where c is the leading coefficient of f.

The proof of this uses complex analysis and is omitted here.

The theorem means the in $\mathbb{C}[x]$ the irreducible polynomials are exactly the polynomials of degree 1, with no exceptions. In $\mathbb{R}[x]$ the description of the irreducible polynomials is a little more complicated (we'll do it later). In $\mathbb{Q}[x]$ things are much more complicated and it can take some time to determine whether a polynomial is irreducible or not.

2 Euclid's algorithm in $k[x]$.

The rings $\mathbb{Z}$ and $k[x]$ are very similar. This is because in both rings we a able to divide with remainder in such a way that the remainder is smaller than the element we divided by. In $\mathbb{Z}$ if we divide a by b we find:

$$a = qb + r, \quad 0 \leq r < b.$$

In $k[x]$, we have something identical:

Theorem 2.1 *Euclidean division Given $f, g \in k[X]$ with $g \neq 0$ and $\deg(f) \geq \deg(g)$ there exist unique $q, r \in k[x]$ such that*

$$f = qg + r \quad \textit{and} \quad \deg(r) < \deg(b).$$

Proof. The proof is **IDENTICAL** to the one for integers.

Existence:

Choose q so that $\deg(f - qg)$ is minimal. Write

$$(f - qg)(x) = c_k x^k + \cdots + c_0,$$

$c_k \neq 0$.

If g has degree $m \leq k$ say

$$g(x) = b_m x^m + \cdots + b_0,$$

where $b_m \neq 0$. Let us subtract $c_k b_m^{-1} x^{k-m} g$ from $(f - qg)$ to give

$$q' = q + c_k b_m^{-1} x^{k-m}.$$

Then

$$f - q'g = f - qg - c_k b_m^{-1} x^{k-m} g = c_k x^k - c_k x^k + \text{terms of order at most } k - 1.$$

This contradicts the minimality of $\deg(f - qg)$. Hence we can choose q such that $\deg(f - qg) < \deg(g)$ and then set $r = f - qg$.

Uniqueness:

Suppose we have $f = q_1 g + r_1 = q_2 g + r_2$. Then

$$g(q_1 - q_2) = r_2 - r_1.$$

So if $q_1 \neq q_2$ then $\deg(q_1 - q_2) \geq 0$ so $\deg(g(q_1 - q_2)) \geq \deg(g)$. But then

$$\deg(r_2 - r_1) \leq \max\{\deg(r_2), \deg(r_1)\} < \deg(g) \leq \deg(g(q_1 - q_2)) = \deg(r_2 - r_1),$$

a contradiction. So $q_1 = q_2$ and $r_1 = r_2$. $\square$

The procedure for finding q and r is the following. Write:

$$f = a_0 + a_1 x + \cdots + a_m x^m$$

where $a_m \neq 0$ and

$$g = b_0 + b_1 x + \cdots + b_n x^n$$

with $b_n \neq 0$ and $m \geq n$.

We calculate

$$r_1 = f - \frac{a_m}{b_n} x^{m-n} g$$

if $\deg(r_1) < \deg(g)$ then we are done; if not, we continue until we found $\deg(r_i) < \deg(g)$.

For example: in $\mathbb{Q}[x]$:

$$f(x) = x^3 + x^2 - 3x - 3, \quad g(x) = x^2 + 3x + 2$$

Then

$$f - xg = -2x^2 - 5x - 3$$
$$(f - xg) + 2g = x + 1$$

Hence

$$f = (x-2)g + x + 1$$

hence $q = x - 2, r = x + 1$.

Another example: still in $\mathbb{Q}[x]$

$$f(x) = 3x^4 + 2x^3 + x^2 - 4x + 1, \quad g(x) = x^2 + x + 1$$

Then

$$f - 3x^2 g = -x^3 - 2x^2 - 4x + 1$$
$$(f - 3x^2 g) + xg = -x^2 - 3x + 1$$
$$(f - 3x^2 g) + xg + g = -2x + 2$$

Hence

$$f = (3x^2 - x - 1)g + (-2x + 2)$$

hence $q = 3x^2 - x - 1, r = -2x + 2$.

We now define the **greatest common divisor** of two polynomials:

Definition 2.1 *Let f and g be two polynomials in $k[x]$ with one of them non-zero. The* **greatest common divisor** *of f and g is the unique* **monic** *polynomial $d = \gcd(f,g)$ with the following properties:*

1. *d divides f and g*

2. *c divides f and g implies c divides d*

Why is it unique? Suppose we had two gcd's d_1 and d_2, then d_1 divides d_2 i.e. $d_1 = hd_2$. Similarly d_2 divides d_1: $d_2 = kd_1$. It follows that

$$\deg(h) + \deg(k) = 0$$

therefore $h, k \in k\backslash\{0\}$. As polynomials d_1 and d_2 are monic, we have $h = k = 1$ hence $d_1 = d_2$.

The greatest common divisor of f and g is also the unique monic polynomial d such that:

1. d divides f and g

2. if c divides f and g, then $\deg(c) \leq \deg(d)$

Let us see that this definition is equivalent to the previous one. Let $d_1 = \gcd(f, g)$ and d_2 the monic polynomial satisfying

1. d_2 divides f and g

2. if c divides f and g, then $\deg(c) \leq \deg(d_2)$

We need to show that $d_1 = d_2$.
As $d_1|f$ and $d_1|g$, we have

$$\deg(d_1) \leq \deg(d_2)$$

by definition of d_2.
Now, $d_2|f$ and $d_2|g$ hence $d_2|d_1$ by defition of d_1. In particular $\deg(d_2) \leq \deg(d_1)$.
It follows that $\deg(d_2) = \deg(d_1)$ and $d_2|d_1$.
Hence $d_1 = \alpha d_2$ with $\deg(\alpha) = 0$ i.e. α is a unit. As both d_1 and d_2 are monic, it follows that

$$d_1 = d_2$$

From Euclidean division, just like in the case of integers, we derive a Euclidean algorithm for calculating the gcd.
The Eucledian division gives $f = qg + r, \quad \deg(r) < \deg(g)$; then

$$\gcd(f, g) = \deg(g, r)$$

To see this, just like in the case of integers, let $A := \gcd(f, g)$ and $B := \gcd(g, r)$. We have $f = qg + r$. As A divides f and g, A divides r. Therefore A divides g and r. As B is the greatest common divisor of g and r, $A|B$.
Similarly, B divides g and r, hence $B|f$. It follows that $B|A$.
The same argument we used to show that the gcd is unique now shows that $A = B$.
Running the algorithm backwards, we get the **Bézout's identity**: there exist two polynomials h and k such that

$$\gcd(f, g) = hf + kg$$

Just like in the case of integers, it follows that

1. f and g are coprime iff there exist polynomials h and k such that

$$hf + gk = 1$$

2. If $f|gh$ and f and g are coprime, then $f|h$

We say that f and g are coprime if $\gcd(f,g) = 1$ and, using Bézout's identity, one sees that f and g are coprime if and only if there exist (h,k), polynomials, such that

$$1 = hf + kg$$

Let's do an example : Calculate $\gcd(f,g)$ and find h,k such that $\gcd(f,g) = hf + kg$ with $f = x^4 + 1$ and $g = x^2 + x$.

We write: $f - x^2 g = -x^3 + 1$, then $f - x^2 g + xg = x^2 + 1$ and $f - x^2 g + xg - g = 1 - x$ and we are finished.

We find:

$$f = (x^2 - x + 1)g + 1 - x$$

And then

$$x^2 + x = (-x + 1)(-x - 2) + 2$$

As 2 is invertible, we find that the gcd is one !

Now, we do it backwards:

$$\begin{aligned} 2 = g - (1-x)(-x-2) = \\ g + (1-x)(x+2) = \\ g + (x+2)(f - (x^2 - x + 1)g) = \\ g[1 - (x+2)(x^2 - x + 1)] + (x+2)f = \\ g[-1 - x^3 - x^2 + x] + (x+2)f \end{aligned}$$

hence $h = (1/2)(x+2)$ and $k = (1/2)(-x^3 - x^2 + x - 1)$.

Now, suppose we considered the same example in $\mathbb{F}_2[x]$. In $\mathbb{F}_2[x]$,

$$f = x^4 + 1 = x^4 - 1 = (x-1)^4$$

and

$$g = x(x+1) = x(x-1)$$

Clearly in $\mathbb{F}_2[x]$, $\gcd(f,g) = x - 1$ and the Bézout's identity is

$$x - 1 = (x^2 - x + 1)g - f$$

An element $a \in k$ is called a **root** of a polynomial $f \in k[x]$ if $f(a) = 0$.

We have the following consequence of the Euclidean division:

Theorem 2.2 (The Remainder Theorem) *If $f \in k[x]$ and $a \in k$ then*

$$f(a) = 0 \iff (x-a)|f.$$

Proof. If $(x-a)|f$ then there exists $g \in k[x]$ such that $f(x) = (x-a)g(x)$. Then $f(a) = (a-a)g(a) = 0g(a) = 0$.

Conversely by Eucledian division we have $q, r \in k[x]$ with $\deg(r) < \deg(x-a) = 1$ such that $f(x) = q(x)(x-a) + r(x)$. So $r(x) \in k$. Then

$$r(a) = f(a) - q(x)(a-a) = 0 + 0 = 0.$$

Hence $(x-a)|f$. □

A consequence of this theorem is the following:

Lemma 2.3 *A polynomial $f \in k[x]$ of degree 2 is reducible if and only if f has a root in k.*

Proof. If f has a root a in k, then the above theorem shows that $(x-a)$ divides f and as $\deg(f) > 1$, f is reducile. Conversely, suppose that f is reducible i.e.

$$f = gh$$

where neither g nor h is a unit.

Therefore, we have $\deg(g) = \deg(h) = 1$ Dividing by the leading coefficient of g, we may assume that $g = x - a$ for some a in k, hence $f(a) = 0$, a is a root of f. □

For example, $x^2 + 1$ in $\mathbb{R}[x]$ is of degree two and has no roots in $\mathbb{R}$, hence it is irreducible in $\mathbb{R}[x]$.

The polynomial x^2+1 is also irreducible in $\mathbb{F}_3[x]$: it suffices to check that $0, 1$ and 2 are not roots in $\mathbb{F}_3$.

We have the following corollary of the fundamental theorem of algebra and euclidean division.

Proposition 2.4 *No polynomial $f(x)$ in $\mathbb{R}[x]$ of degree > 2 is irreducible in $\mathbb{R}[x]$.*

Proof. Let $f \in \mathbb{R}[x]$ be a polynomial of degree > 2. By fundamental theorem f has a root in $\mathbb{C}$, call it α. Then $\overline{\alpha}$ (complex conjugate) is another root (because $f \in \mathbb{R}[x]$). Let

$$p(x) = (x - \alpha)(x - \overline{\alpha}) = x^2 - (\alpha + \overline{\alpha})x + \alpha\overline{\alpha}$$

The polynomial p is in $\mathbb{R}[x]$ and is irreducible (if it was reducible it would have a real root).

Divide f by p.

$$f(x) = p(x)q(x) + r(x)$$

with $\deg(r) \leq 1$. We can write $r = sx + r$ with $s, r \in \mathbb{R}$. But $f(\alpha) = p(\alpha)q(\alpha) + r(\alpha) = 0 = r(\alpha)$. As α not real we must have $r = s = 0$. This implies that p divides f but $\deg(p) = 2 < \deg(f)$. It follows that f is not irreducible. $\square$

Notice that the proof above shows that any polynomial of degree three in $\mathbb{R}[x]$ has a root in $\mathbb{R}$. This is not true for polynomials of degree > 3. For example $x^4 + 1$ is not irreducible in $\mathbb{R}[x]$:

$$x^4 + 1 = (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1)$$

However, the polynomial $x^4 + 1$ has no roots in $\mathbb{R}$. The proposition above does not hold for $\mathbb{Q}[x]$. For example, it can be shown that x^4+1 is irreducible in $\mathbb{Q}[x]$. The reason why the proof does not work is that although $\alpha + \overline{\alpha}$ and $\alpha\overline{\alpha}$ are in $\mathbb{R}$, they have no reason to be in $\mathbb{Q}$.

Lemma 2.5 *Suppose f in $k[x]$ is irreducible. Then $f | g_1 \cdots g_r$ implies $f = g_i$ for some i.*

Proof. Copy the proof for integers. $\square$

Theorem 2.6 (Unique Factorisation Theorem) *Let $f \in k[x]$ be monic. Then there exist $p_1, p_2, \ldots, p_n \in k[x]$ monic irreducibles such that*

$$f = p_1 p_2 \cdots p_n.$$

If $q_1, \ldots, q_s$ are monic and irreducible and $f = q_1 \ldots q_s$ then $r = s$ and (after reordering) $p_1 = q_2$, ... , $p_r = q_r$.

Proof. (Existence): We prove the existence by induction on $\deg(f)$. If f is linear then it is irreducible and the result holds. So suppose the result holds for polynomials of smaller degree. Either f is irreducible and so the result holds or $f = gh$ for g, h non-constant polynomials of smaller degree. By our inductive hypothesis g and h can be factorized into irreducibles and hence so can f.

(Uniqueness): Factorization is obviously unique for linear polynomials (or even irreducible polynomials). For the inductive step, assume all polynomials of smaller degree than f have unique factorization. Let

$$f = g_1 \cdots g_s = h_1 \cdots h_t,$$

with g_i, h_j monic irreducible.

Now g_1 is irreducible and $g_1 | h_1 \cdots h_t$. By the Lemma, there is $1 \leq j \leq t$ such $g_1 | h_j$. This implies $g_1 = h_j$ since they are both monic irreducibles. After reordering, we can assume $j = 1$, so

$$g_2 \cdots g_s = h_2 \cdots h_t,$$

is a polynomial of smaller degree than f. By the inductive hypothesis, this has unique factorization. I.e. we can reorder things so that $s = t$ and

$$g_2 = h_2, \ldots, g_s = h_t.$$

$\square$

The fundamental theorem of algebra tells you exactly that any monic polynomial in $\mathbb{C}[x]$ is a product of irreducibles (recall that polynomials of degree one are irreducible).

A consequence of factorisation theorem and fundamental theorem of algebra is the following: any polynomial of **odd degree** has a root in $\mathbb{R}$. Indeed, in the decomposition we can have polynomials of degree one and two. Because the degree is odd, we have a factor of degree one, hence a root.

Another example : $x^2 + 2x + 1 = (x + 1)^2$ in $k[x]$.

Look at $x^2 + 1$. This is irreducible in $\mathbb{R}[x]$ but in $\mathbb{C}[x]$ it is reducible and decomposes as $(x + i)(x - i)$ and in $\mathbb{F}_2[x]$ it is also reducible : $x^2 + 1 = (x + 1)(x - 1) = (x + 1)^2$ in $\mathbb{F}_2[x]$. In $\mathbb{F}_5[x]$ we have $2^2 = 4 = -1$ hence $x^2 + 1 = (x + 2)(x - 2)$ (check : $(x - 2)(x + 2) = x^2 - 4 = x^2 + 5$).

In fact one can show that $x^2 + 1$ is reducible in $\mathbb{F}_p[x]$ is and only if $p \equiv 1 \bmod 4$.

In $\mathbb{F}_p[x]$, the polynomial $x^p - x$ decomposes as product of polynomials of degree one.

Suppose you want to decompose $x^4 + 1$ in $\mathbb{R}[x]$. It is not irreducible puisque degree est > 2. Also, $x^4 + 1$ does not have a root in $\mathbb{R}[x]$ but it does in $\mathbb{C}[x]$. The idea is to decompose into factors of the form $(x - a)$ in $\mathbb{C}[x]$ and then group the conjugate factors.

This is in general how you decompose a polynomial into irreducibles in $\mathbb{R}[x]$!

So here, the roots are

$$a_1 = e^{i\pi/4}, a_2 = e^{3i\pi/4}, a_3 = e^{5i\pi/4}, a_4 = e^{7i\pi/4}.$$

Now note that $a_4 = \overline{a_1}$ and the polynomial $(x - a_1)(x - a_4)$ is irreducible over $\mathbb{R}$. The middle coefficient is $-(a_1 + a_2) = -2\cos(\pi/4) = -\sqrt{2}$. Hence we find : $(x - a_1)(x - a_4) = x^2 - \sqrt{2}x + 1$.

Similarly $a_2 = \overline{a_3}$ and $(x - a_2)(x - a_3) = x^2 + \sqrt{2}x + 1$.

We get the decomposition into irreducibles over $\mathbb{R}$:

$$x^4 + 1 = (x^2 - \sqrt{2}x + 1)(x^2 + \sqrt{2}x + 1)$$

In $\mathbb{Q}[x]$ one can show that $x^4 + 1$ is irreducible.

In $\mathbb{F}_2[x]$ we can also decompose $x^4 + 1$ into irreducibles. Indeed :

$$x^4 + 1 = x^4 - 1 = (x^2 - 1)^2 = (x - 1)^4$$