MATHEMATICS AROUND US - TUTORIAL AND HOMEWORK 2

Please submit all exercises below in hard copy (either in English or in Hebrew) next Thursday, November 16^{th}, in the tutorial. Sections marked as bonus are not mandatory.

1. Polynomials (reminder)

Definition: Let $P(x) = a_0 + a_1x + a_2x^2 + a_3x^3 + ... + a_nx^n$ be a polynomial such that $a_n \neq 0$. We define the degree of $P(x)$ to be n and we write $deg(P) = n$. Note that the degree of the zero polynomial ($P(x) = 0$) is not defined.

Easy facts: Let $P(x), Q(x)$ be two non zero polynomials, then $deg(P + Q) \leq max\{deg(P), deg(Q)\}$ (unless $P = -Q$, in that case $deg(P + Q)$ is not defined), $deg(P \cdot Q) = deg(P) + deg(Q)$.

1.1. Exercise: Give an example of a polynomial of degree 3 with roots 1, 2, 3 (write the coefficients explicitly).

1.2. Exercise: Let $P(x), Q(x)$ be two polynomials such that the sum of the coefficients of $P(x)$ is 14, and the sum of coefficients of $Q(x)$ is 7. What would be the sum of coefficients of each of the following polynomials?

(1) $P(x) + Q(x)$
(2) $P(x) \cdot Q(x)$

(hint: what value of x should you substitute in a polynomial in order to get the sum of its coefficients?)

1.3. Exercise: Is there a polynomial $P(x)$, of degree at most 2, such that

$$P(0) = 2, P(1) = 7, P(2) = 0, P(3) = -19 \ ?$$

If the answer in no prove it, if the answer is yes prove whether this polynomial is unique and find all such polynomials.

1.4. Exercise: Let $P(x)$ be a polynomial and define $Q(x) = P(x) \cdot (x-1)$. It is known that all the non-zero coefficients of $Q(x)$ are positive. What can you say about the coefficients of $P(x)$?

2. Division with remainder

2.1. Theorem: Let $P(x), Q(x)$ be two polynomials such that $Q(x) \neq 0$. There exist unique polynomials $R(x), D(x)$ such that $P(x) = D(x)Q(x) + R(x)$ and either $deg(R) < deg(Q)$ or $R(x) = 0$.

Definition: $D(x)$ and $R(x)$ as above are called the quotient and the remainder of $P(x)$ divided by $Q(x)$ respectively. If $R(x) = 0$ we sy that $Q(x)$ divides $P(x)$, and $P(x)$ is divisible by $Q(x)$, and we write $Q(x)|P(x)$.

Proof of the Theorem: we prove by giving an explicit iterative algorithm for finding $D(x)$ and $R(x)$. Define $P_0(x) = P(x)$ and $C_0(x) = 0$.

Date: November 9^{th} 2017.

Step k: If either $P_{k-1}(x) = 0$ of $deg(P_{k-1}(x)) < deg(Q(x))$ we define

$$R(x) = P_{k-1}(x) \text{ and } D(x) = C_0(x) + C_1(x) + C_2(x) + C_3(x) + ... + C_{k-1}(x).$$

Otherwise we define

$$l_k = deg(P_{k-1}(x)) - deg(Q(x)), \alpha_k = \frac{P_{k-1}(x)\text{'s leading coefficient}}{Q(x)\text{'s leading coefficient}},$$

$$C_k(x) = \alpha_k \cdot x^{l_k}, P_k(x) = P_{k-1}(x) - C_k(x) \cdot Q(x),$$

and proceed to step $k+1$.

In order to prove the theorem it is enough to prove the following three claims:

Claim 1: The algorithm stops after a finite number of steps.

Claim 2: $D(x)$ and $R(x)$ obtained in the algorithm indeed satisfy $P(x) = D(x)Q(x) + R(x)$ and either $deg(R) < deg(Q)$ or $R(x) = 0$.

Claim 3: $D(x)$ and $R(x)$ are unique, i.e. if $P(x) = D(x)Q(x) + R(x)$ and either $deg(R) < deg(Q)$ or $R(x) = 0$, and in addition $P(x) = D_1(x)Q(x) + R_1(x)$ and either $deg(R_1) < deg(Q)$ or $R_1(x) = 0$, then $D_1(x) = D(x)$ and $R_1(x) = R(x)$.

Proof of Claim 1: The series of numbers $\{deg(P_k(x))\}_{k\geq 0}$ is a strictly descending series of non-negative integers (as by defining $P_k(x) = P_{k-1}(x) - C_k(x) \cdot Q(x)$ the leading power of x in $P_{k-1}(x)$ is cancelled out), thus it must reach $\{0, 1, 2, ..., deg(Q) - 1\}$ or stop as $P_k(x) = 0$ for some k.

Proof of claim 2: It is clear from the algorithm that the condition either $deg(R) < deg(Q)$ or $R(x) = 0$ holds. Assume the algorithm stopped at step $n+1$, then:

$$P(x) = P_0(x) = P_1(x) + C_1(x) \cdot Q(x) = P_2(x) + C_2(x) \cdot Q(x) + C_1(x) \cdot Q(x) = ...$$

$$... = P_n(x) + (C_n(x) + C_{n-1}(x) + C_1(x)) \cdot Q(x) = R(x) + D(x) \cdot Q(x)$$

as desired.

The proof of claim 3 is left as an exercise.

Thus we proved Theorem 2.1. □

2.2. Exercise: Prove claim 3 above.

2.3. Example: Let us divide with remainder the polynomial $3x^5 + 4x^3 + 2$ in the polynomial $x^2 + 1$.

Step 0: define $C_0(x) = 0, P_0(x) = 3x^5 + 4x^3 + 2$, and proceed to step 1.

Step 1: define $l_1 = 3, \alpha_1 = 3$ and $C_1(x) = 3x^3, P_1(x) = x^3 + 2$, and proceed to step 2.

Step 2: define $l_2 = 1, \alpha_2 = 1$ and $C_2(x) = x, P_2(x) = -x + 2$. Here the algorithm stops as $1 = deg(P_2(x)) < deg(Q(x)) = 2$, and we have $D(x) = C_0(x) + C_1(x) + C_2(x) = 3x^3 + x, R(X) = P_2(x) = -x + 2$.

One can verify that indeed $3x^5 + 4x^3 + 2 = (3x^3 + x)(x^2 + 1) + (-x + 2)$.

2.4. Exercise: Divide with remainder the polynomial $x^7 + 1$ in the polynomial $x^2 + 3$ (show all the steps).

2.5. Exercise: Let $P(x), Q(x)$ be two polynomials, $D(x)$ be the quotient of the division of $P(x)$ by $Q(x)$, and $R(x)$ be the remainder. Assume $deg(P(x)) = 100$, $deg(Q(x)) = 43$. What could be the degrees of $D(x)$ and $R(x)$ (list all the possibilities)? Prove your answer!

2.6. Exercise: Show that when dividing with remainder a polynomial $P(x)$ by the linear polynomial $x - a$ (a being a complex number), the remainder is the constant polynomial $P(a)$. This result is called Little Bezout's Theorem.

It follows from Little Bezout's Theorem that a number a is the root of the polynomial $P(x)$ if and only if the polynomial $P(x)$ is divisible by the linear polynomial $x - a$.

2.7. Exercise: (bonus) For which positive integers n, k the polynomial $x^k - 1$ divides the polynomial $x^n - 1$?

3. Greatest Common Divisor of polynomials and Euclid's algorithm

Definition: let P, Q be two polynomials, we call a polynomial D a common divisor of P and Q if both $D|P$ and $D|Q$.

Definition: the greatest common divisor of two polynomials P and Q, where at least one of them is not zero, is the common divisor D satisfying the following two conditions: the degree of D is maximal out of all of the common divisors of P and Q, and D is a monic polynomial (i.e. a polynomial with leading coefficient 1). We denote such D by $gcd(P, Q)$.

One can show that such polynomial always exists and it is unique. It follows from the following fact:

Let P, Q be two polynomials, where at least one of them is not zero, then for any common divisor D of P and Q: $D|gcd(P, Q)$.

This fact is also true for numbers:

Let a, b be two integers, where at least one of them is not zero, then for any common divisor d of a and b: $d|gcd(a, b)$.

In fact, these facts can be taken to be the definition of the greatest common divisor, and it turns out this will be equivalent to the definition we gave, up to the sign in the numbers case and the monic requirement in the polynomial case.

One can define Euclid's algorithm for polynomials in the same way we did for integers, and prove it gives us the greatest common divisor after dividing the last non zero remainder in the algorithm by the leading coefficient (i.e. after making it monic).

3.1. Exercise: (bonus) Calculate $gcd(2x^4 + 5x^2 - 7, x^3 + 3x^2 - x - 3)$. (instructions: follow carefully the steps of Euclid's algorithm for numbers, it is not difficult!).

4. Using modular arithmetic for polynomials

4.1. Example: does the polynomial $f(x) = x^2 - 117x + 31$ has an integer root?

Let us show that the answer is no by looking at $f(x)$ modulo 2. Assume a is an integer such that $f(a) = 0$, then $a^2 - 117a + 31 = 0$. Note that $a^2 - 117a + 31 \equiv a^2 + a + 1 \ (mod\ 2)$. However, if a is even (i.e. $a \equiv 0 \ (mod\ 2)$) then $a^2 + a + 1 \equiv 0 + 0 + 1 \equiv 1 \ (mod\ 2)$ and if a is odd (i.e. $a \equiv 1 \ (mod\ 2)$) then $a^2 + a + 1 \equiv 1 + 1 + 1 \equiv 1 \ (mod\ 2)$. Thus we got a contradiction and so the polynomial $f(x) = x^2 - 117x + 31$ has no integer roots. □

4.2. Exercise: Is there a polynomial $P(x)$ with integer coefficients such that $P(7) = 5$ and $P(11) = 7$?

5. Complex Numbers (reminder)

Recall that any complex number can be written either in the form $a + bi$ (with a, b being two real numbers), or $re^{i\theta} = r(\cos(\theta) + i\sin(\theta))$. Also recall that complex numbers can be represented as points on the plane $\mathbb{R}^2$: $z = a + ib$ is represented by the point whose Cartesian coordinates are (a, b), or $z = re^{i\theta}$ is represented by the point whose distance from the origin is r and the angle from the positive side of the "real" axis is θ.

5.1. Exercise: Write the following numbers in the form $a+bi$, where a, b are real numbers:

(1) i^{10}
(2) $\frac{1}{1+i}$
(3) $(\sqrt{3} + i)^{30}$
(4) $1 + i + ... + i^{100}$
(5) $\frac{1+i}{1-i}$

5.2. Exercise: In each of the following cases, describe the set of points on the plane for which the corresponding complex numbers z satisfy the equation:

(1) $z + \bar{z} = 1$
(2) $z \cdot \bar{z} = 1$

(the description should include both a description of the set in terms of Cartesian coordinates, and a geometrc description).

5.3. Exercise: Let z, w be two complex numbers. Prove the inequality:

$$|z| + |w| \geq |z + w| .$$

When does equality occurs (hint: use the representation of complex numbers as points on the plane)?

Recall the function of complex conjugation taking a complex number $z = a + bi = re^{i\theta}$ and sending it to $\bar{z} = a - bi = re^{-i\theta}$.

5.4. Exercise: Prove that for any complex number z both $z \cdot \bar{z}$ and $z + \bar{z}$ are real numbers. Express these two numbers in terms of a and b. Express those two numbers in terms of r and θ.

5.5. Example: let us find all complex z's such that $z^3 = 1$. First, in order not to lose solutions we write $z = re^{i(\theta+2\pi k)}$, and then $z^3 = r^3(e^{i(\theta+2\pi k)})^3 = r^3 e^{3i(\theta+2\pi k)} = 1 = 1e^{i0}$. It is easy to see that $r = 1$ and then taking 3^{rd} root we get $\theta = \frac{0}{3} + \frac{2\pi k}{3}$, i.e. $\theta \in \{0, \frac{2\pi}{3}, \frac{4\pi}{3}\}$.

6. Reducibility of polynomials

Definition: Let $P(x)$ be a non constant polynomial with coefficients in a field $\mathbb{F}$ (e.g. the real numbers). We call $P(x)$ irreducible over $\mathbb{F}$ if it there are no two non constant polynomials $Q(x), R(x)$ with coefficients in the field $\mathbb{F}$ such that $P(x) = Q(x) \cdot R(x)$.

Example: $x^2 + 1$ is irreducible over the field of real numbers but is not over the field of complex numbers (as $x^2 + 1 = (x + i)(x - i)$).

Recall the fundamental theorem of algebra: any polynomial with complex coefficients decomposes into a product of linear polynomials. That is, given a polynomial $P(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$, where $a_n, a_{n-1}, ..., a_1, a_0$ are complex numbers and $a_n \neq 0$, there exist complex numbers $\alpha_1, ..., \alpha_n$ (not necessarily different) such that $P(x) = a_n(x - \alpha_1)(x - \alpha_2)....(x - \alpha_n)$.

The aim of the following two exercises is to understand how to present a polynomial $P(x)$ with real coefficients (i.e. $P(x) = a_n x^n + a_{n-1} x^{n-1} + ... + a_1 x + a_0$, where $a_n, a_{n-1}, ..., a_1, a_0$ are real numbers) as a product of polynomials, each having real coefficients, which have the smallest possible degrees. That is, we want $P(x)$ to be a product of polynomials with real coefficients and which are irreducible over the real numbers.

6.1. Exercise: Let $P(x)$ be a polynomial with real coefficients, and z (a complex number) a root of $P(x)$. Prove that $\bar{z}$ is a root of $P(x)$ as well (hint: recall that the complex conjugate of a sum of numbers equals the sum of the complex conjugates of those numbers, e.g. $\overline{z_1 + z_2 + z_3} = \bar{z_1} + \bar{z_2} + \bar{z_3}$).

6.2. Exercise: Use the above result, together with the fundamental theorem of algebra and exercise 5.4, to prove the following statement:

Any non-zero polynomial with real coefficients can be presented as a product of polynomials with real coefficients which are irreducible over the real numbers, such that each of these polynomial has degree at most 2.

6.3. Exercise: (bonus) Use the above statement to show that any real polynomial of odd degree has a real root. Do not use the intermediate value theorem (MISHPAT ERECH HABEINAIM).

6.4. Exercise: Decompose the polynomial $x^4 + 1$ and present it as a product of polynomials with real coefficients, each having degree at most 2 (hint: use the example 5.5).

E-mail address: ary.shaviv@weizmann.ac.il