Theorem (Euclidean algorithm) Let $g(x)$ be a nonzero polynomial over a field $\mathbb{F}$. For every polynomial $f(x) \in \mathbb{F}[x]$, there exists a unique pair of polynomials $q(x)$ and $r(x)$ in $\mathbb{F}[x]$ such that $f(x) = q(x)g(x) + r(x)$, with $\deg g > \deg r$ or $r(x) = 0$.

Proof: If $f(x) = 0$, then let $q(x) = r(x) = 0$. In the following assume that $f(x) \neq 0$. write $f(x) = a_n x^n + \cdots + a_0$ and $g(x) = b_m x^m + \cdots + b_0$, with $a_n \neq 0$, $b_m \neq 0$. We use induction on n. If $n < m$, then set $q(x) = 0$ and $r(x) = f(x)$. It left to consider the case $n \geq m$. ~~If $n = m = 0$, then set $q(x) = a_0 b_0^{-1}$ and $r(x) = 0$;~~

~~If Now suppose that the theorem is true for all polynomials of degree~~

If $n = m$, then we have

$$f(x) = a_n b_m^{-1} g(x) + (f(x) - a_n b_m^{-1} g(x)),$$

where $f(x) - a_n b_m^{-1} g(x) = 0$ or $\deg(f(x) - a_n b_m^{-1} g(x)) < \deg f(x)$. Hence,

$$q(x) = a_n b_m^{-1}, \quad r(x) = f(x) - a_n b_m^{-1} g(x),$$

as required.

Now suppose that the theorem is true for all polynomials of degree $< n$ (where $n > m$). With this assumption, we write

$$f(x) = a_n b_m^{-1} x^{n-m} g(x) + f_1(x) \qquad (*)$$

where $f_1(x) = 0$ or $\deg f_1(x) < \deg f(x)$. By the induction assumption, we find $q_1(x)$ and $r(x)$ for which

$$f_1(x) = q_1(x) g(x) + r(x), \quad \deg r(x) < \deg g(x) \text{ or } r(x) = 0.$$

Substituting this into $(*)$ gives

$$f(x) = (q_1(x) + a_n b_m^{-1} x^{n-m}) g(x) + r(x).$$

~~Hence~~ Set $q(x) = q_1(x) + a_n b_m^{-1} x^{n-m}$. Hence we obtain a pair of polynomials $q(x)$ and $r(x)$ with the required properties.

It remains to prove that $q(x)$ and $r(x)$ are unique. (The same as we have talked in class). □

$f(x)g(x)=0$ if and only if $f(x)=0$ or $g(x)=0$. (No zero-divisors)

Proposition 2. Let $\mathbb{F}$ be a field. The addition and multiplication operations on $\mathbb{F}[x]$ satisfy the following properties:

(1) The addition is commutative, i.e., $f(x)+g(x)=g(x)+f(x)$

(2) The addition is associative, i.e., $(f(x)+g(x))+h(x)=f(x)+(g(x)+h(x))$

(3) The multiplication is commutative, i.e., $f(x)g(x)=g(x)f(x)$

(4) The multiplication is associative, i.e., $(f(x)g(x))h(x)=f(x)(g(x)h(x))$

(5) The multiplication is distributive, i.e. (with respect to addition).
$$f(x)(g(x)+h(x))=f(x)g(x)+f(x)h(x)$$
$$(f(x)+g(x))h(x)=f(x)h(x)+g(x)h(x)$$

(6) Cancellation law.

If $f(x)g(x)=f(x)h(x)$ and $f(x)\neq 0$, then $g(x)=h(x)$.

Proof of (4):

The coefficient of the sth term of $f(x)g(x)$ is $\sum_{i+j=s} a_i b_j$. Thus the coefficient of the tth term of $(f(x)g(x))h(x)$ is

$$\sum_{s+k=t}\left(\sum_{i+j=s} a_i b_j\right)c_k=\sum_{i+j+k=t} a_i b_j c_k.$$

The coefficient of the rth term of $g(x)h(x)$ is $\sum_{j+k=r} b_j c_k$. Hence the coefficient of the tth term of $f(x)(g(x)h(x))$ is

$$\sum_{i+h=t} a_i\left(\sum_{j+k=r} b_j c_k\right)=\sum_{i+j+k=t} a_i b_j c_k.$$

□.

Def 3. We call $\mathbb{F}[x]$ is the ring of polynomials over the field $\mathbb{F}$.

Def 4. A polynomial $f(x)$ in $\mathbb{F}[x]$ is called a unit if there exists a polynomial $g(x)\in\mathbb{F}[x]$ such that $f(x)g(x)=1$.

Every unit of $F[x]$ is a nonzero constant.

Fact: The units of $F[x]$ coincides with the units of F.

Proof: It is clear that every unit of F is a unit of $F[x]$. Conversely, if $f(x)g(x)=1$, then both $f(x)$ and $g(x)$ must be of degree 0, i.e., $f(x)=a_0\neq 0$, $g(x)=b_0\neq 0$, and $a_0b_0=1$. So that a_0 and b_0 are units in F.

Example. Compute the product of $f(x)$ and $g(x)$, with

$$f(x)=x^4+3x^3-x^2-4x-6,$$
$$g(x)=3x^4+x^2+5.$$

Solution.

			1	3	-1	-4	-6	
			3	0	1	0	5	
			5	15	-5	-20	-30	
		0	0	0	0	0		
	1	3	-1	-4	-6			
0	0	0	0	0				
3	9	-3	-12	-18				
3	9	-2	-9	-14	11	-11	-20	-30

Thus,

$$f(x)g(x)=3x^8+9x^7-2x^6-9x^5-14x^4+11x^3-11x^2-20x-30.$$

§3. Divisibility

Def 1. Let F be a field. A polynomial $g(x)$ in $F[x]$ divides a polynomial $f(x)$ in $P[x]$ if there is a polynomial $h(x)$ in $F[x]$ such that

$$f(x) = g(x)h(x).$$

In this case, we also say that $g(x)$ is a divisor of $f(x)$, and $f(x)$ is a multiple of $g(x)$.

~~In the following~~, We use $g(x) \mid f(x)$ to denote that $g(x)$ divides $f(x)$, and use $g(x) \nmid f(x)$ to denote that $g(x)$ cannot divide $f(x)$.

Theorem 1. The following divisibility facts hold:

(1) The zero polynomial is divisible by every polynomial.

(2) Every polynomial is divisible by itself.

(3) Every polynomial is divisible by a polynomial of degree 0, i.e., non-zero constant.

(4) If $f(x) \mid g(x)$ and $g(x) \mid f(x)$, then $f(x) = cg(x)$, where c is a non-zero constant. In the case, we say that $f(x)$ and $g(x)$ are associates of each other.

(5) If $f(x) \mid g(x)$ and $g(x) \mid h(x)$, then $f(x) \mid h(x)$.

(6) If $f(x) \mid a(x)$ and $g(x) \mid b(x)$, then $f(x) \mid a(x)+b(x)$ and $f(x) \mid a(x)-b(x)$. More generally, for every polynomials $r(x)$ and $s(x)$, we have

$$f(x) \mid r(x)a(x) + s(x)b(x),$$

where $r(x)a(x) + s(x)b(x)$ is called a combination of $a(x)$ and $b(x)$.

Example: $f(x)=3x^3+4x^2-5x+6$, $g(x)=x^2-3x+1$, we have

$$\begin{array}{r|l} & 3x+13 \quad \to \text{Quotient} \\ \hline x^2-3x+1 & 3x^3+4x^2-5x+6 \quad \to \text{Dividend} \\ & 3x^3-9x^2+3x \\ \hline & 13x^2-8x+6 \\ & 13x^2-39x+13 \\ \hline & 31x-7 \quad \to \text{Remainder} \end{array}$$

Divisor $\leftarrow$

"Long Division"

And thus $f(x)=(3x+13)g(x)+31x-7$.

Theorem 2. (Euclidean algorithm). Let $\mathbb{F}$ be a field, and let $g(x)$ be a nonzero polynomial in $\mathbb{F}[x]$. Then for every polynomial $f(x)\in\mathbb{F}[x]$, there exists a unique pair of polynomials $q(x)$, $r(x)\in\mathbb{F}[x]$ for which

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

where $\deg r(x)<\deg g(x)$, or $r(x)=0$.

Proof: If $f(x)=0$, then $q(x)=r(x)=0$, as required. We assume $n=\deg f(x)\geq 0$ and $m=\deg g(x)\geq 0$. Write

$$f(x)=a_nx^n+\cdots+a_0$$
$$g(x)=b_mx^m+\cdots+b_0$$

If $n<m$, let $q(x)=0$ and $r(x)=f(x)$. If $n\geq m$, let

$$f_1(x)=f(x)-a_nb_m^{-1}x^{n-m}g(x).$$

If $f_1(x)=0$, then $f(x)=a_nb_m^{-1}x^{n-m}g(x)$. In this case, $q(x)=a_nb_m^{-1}x^{n-m}$, $r(x)=0$.

otherwise, $\deg f_1(x)<\deg f(x)$. Continuing in this way, or more formally by induction on n, we can find polynomials $q_1(x)$ and $r(x)$ such that

$$f_1(x)=q_1(x)g(x)+r(x)$$

with $\deg r(x)<\deg g(x)$ or $r(x)=0$. Then

$$f(x)=f_1(x)+a_nb_m^{-1}x^{n-m}g(x)=q_1(x)g(x)+r(x)+a_nb_m^{-1}x^{n-m}g(x)$$
$$=(q_1(x)+a_nb_m^{-1}x^{n-m})g(x)+r(x)$$

Hence we have consequently expressed our polynomial in the desired form.

To prove the uniqueness, suppose that

$$f(x)=q_1(x)g(x)+r_1(x)=q_2(x)g(x)+r_2(x)$$

with $\deg r_1(x) < \deg g(x)$ or $r_1(x)=0$;

$\deg r_2(x) < \deg g(x)$ or $r_2(x)=0$

Then

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

Either the degree of the left-hand side is $\geq \deg g(x)$ or the left-hand side is equal to 0. Either the degree of the right-hand side is $< \deg g(x)$, or the right-hand side is equal to 0. Hence, the only possibility is that they are both 0, whence

$$q_1(x)=q_2(x) \quad \text{and} \quad r_1(x)=r_2(x),$$

as was to be shown. □.

Excercise: (1) For $f(x)=5x^3-6x^2-28x-2$, $g(x)=x+2$, write $f=qg+r$ with

$\deg g > \deg r$ or $r=0$

Solution: $f(x)=g(x)(5x^2-16x+4)+(-10)$.

(2) In $\mathbb{Q}[x]$, divide x^4+1 by x^3-2x^2+x-2 using long division. Determine the quotient and the remainder.

Solution: $x^4+1=(x+2)(x^3-2x^2+x-2)+(3x^2+3)$

quotient, remainder

Caution. To avoid errors, use 0 as coefficient for any missing terms, including a missing constant, when setting up the long division.

Notice that in Theorem 2 $f(x)$ is divisible by $g(x)$ if and only if $r(x)=0$.