Polynomials in one Variable.

Any linear algebra can be used as a ring of scalars; we are mostly concerned with a ring $\mathbb{K}$in general but the polynomial algebra $\mathbb{K}_\theta$ is also needed when the subject develops.We provide a discussion here. Recall that for any ring $\mathbb{K}$' two algebras $\mathbb{K}_\theta$ of polynomials as polynomial arise: one in which we write polynomial as $a(\theta) = \theta^n a_n + \ldots + \theta a_1 + a_0, a_i \varepsilon \mathbb{K}, a_n$ and the other in which we write polynomial as$a(\theta) = a_n\theta^n + \ldots a_1 theta + a_0, a_i \varepsilon \mathbb{K}, a_n \neq 0,$

As modules, one of them is a right module and the other is a left modules and the development run in parallel.As rings they can be regarded as isomorphic via $f(a_n\theta^n) = \theta^n a_n$ the element $a_n \varepsilon \mathbb{K}$ is called the 'leading coefficient' of $a(\theta)$

(i) We take a ring $\mathbb{K}[\theta]$ of polynomial writing its elements as $a = a(\theta) = a_0 + \ldots + a_n\theta^n,\ a_n \neq 0$ and recall that it obey the following relations:

(a) If $a(\theta) = a_0 + a_1\theta + \ldots + a_n\theta^n, a_n \neq 0$

$b(\theta) = b_0 + b_1\theta + \ldots + b_m\theta^m, b_m \neq 0$ and

$c(\theta) = (a(\theta))(b(\theta)) = c_0 + c_1\theta + \ldots +$

$= (ab)_0 + (ab)_1\theta + \ldots$ then while this multiplication in $\mathbb{K}[\theta]$ is in general noncommutative $[c_n = (ab)_n = \sum_{n=p+q} a_p b_q \neq \sum_{n=p+q} b_p a_q = (ba)_n$ in general]we have $deg[b(\theta)a(\theta)] = deg[a(\theta)b(\theta)]$ $[= deg(a(\theta)) + deg(b(\theta)) = n + m$if "either a_n or b_n is not a zero divisor in $\mathbb{K} i.e.$ if we do not get $a_n b_m = 0 \varepsilon \mathbb{K}$ although $a_n \neq 0, b_m \neq 0$

note that this may happen if $\mathbb{K}$ is a matrix ring $Mat_n(\mathbb{L})$ for some ring $\mathbb{L}$]

(b) $deg[a(\theta) + b(\theta)] \leq max\{dega(\theta), degb(\theta)\} = max\{n, m\}$

(c) $dega(\theta) = 0 iff a(\theta) = a_0 \varepsilon \mathbb{K}$, we say that $a = a(\theta)$ is a constant.

(d) We set $deg(0) = -\infty$ for the zero polynomial $o\varepsilon\mathbb{K}[\theta]$.

(e) $\theta\ \varepsilon\mathbb{K}[\theta]$ [i.e.$\theta a(\theta) = a(\theta)\theta$ for all $a(\theta)\varepsilon\mathbb{K}\ [\theta]$] and thus each monomial $\{\theta^k\ \ /k\varepsilon\mathbb{N}$ is in *cen* $\mathbb{K}[\theta]\}$.

(ii) (a) **Proposition** If $\mu(\theta)$ has an invertible leading coefficient and $deg a(\theta) \geq deg \mu(\theta)$, we can find some $b(\theta)$ with $deg[a(\theta) - \mu(\theta)b(\theta)] < deg a(\theta)$.

Proof : Say $a(\theta) = a_0 + \ldots + a_{n+m}\theta^{n+m}, \mu(\theta) = \mu_0 + \ldots + \mu_m\theta^m$ then with $b(\theta) = \mu_m^{-1}a_{m+n}\theta^n$, we have $a(\theta) - \mu(\theta)b(\theta) = a_0 + \ldots + a_{n+m}\theta^{n+m} - \mu_m\mu_m^{-1}a_{n+m}\theta^{n+m} - \mu_{m-1}\mu_m^{-1}a_{n+m}\theta^{n+m-1} - \ldots - \mu_0\mu_m^{-1}a_{n+m}\theta^n$ which has degree $< n + m = deg a(\theta)$ since the coefficient of θ^{n+m} is 0.

(b) We note that the same argument works to prove that we can find $c(\theta)$ with $deg[a(\theta) - c(\theta)\mu(\theta)] < deg a(\theta)$

The left division algorithm :

Given $a(\theta)\varepsilon\mathbb{K}[\theta]$, and $\mu(\theta)\varepsilon\mathbb{K}[\theta]$ with an invertible leading coefficient, there exists exactly one $q(\theta)\varepsilon K[\theta]$ such that $a(\theta) = \mu(\theta) + r(\theta)$,deg$r(\theta) < deg\mu(\theta)$ and then $r(\theta)$ is also uniquely determined we say q is the 'quotient' and r is the remainder.

Proof : If there are two polynomials $q(\theta), q'(\theta)$ satisfying the requirement so that $a(\theta) = \mu(\theta)q(\theta) + r(\theta) = \mu(\theta)q'(\theta) + r'(\theta)$, we have

$$\mu(\theta)[q(\theta) - q'(\theta)] = r(\theta) - r'(\theta) \qquad (1)$$

Assume $deg[q(\theta) - q'(\theta)] = n$, $deg\ \mu(\theta) = m$ so that LHS of (1) has degree $n + m$ [$\because \mu(\theta)$ has invertible coefficient μ_m and thus if] λ is non zero we do not have $\mu_m\lambda = 0$ since $\lambda = \mu_m^{-1}(\mu_m\lambda)$

But $deg(r(\theta)) < deg\mu(\theta), deg(r'(\theta)) < deg\mu(\theta)$ and $deg[r'(\theta) - deg r(\theta)] \leq max\{deg r'(\theta), deg r(\theta)\} < deg\mu(\theta)$ and so we have $n + m < m$ which forces $n = -\infty$ and thus $q(\theta) = q'(\theta)$ which then forces $r'(\theta) = r(\theta)$ and consequently uniqueness is established for $q(\theta)$ and then for $r(\theta) = a(\theta) - \mu(\theta)q(\theta)$. For existence, we note that the set $S = \{deg[a(\theta) - \mu(\theta)b(\theta)] | b(\theta) \in k[\theta]\}$ will have a least element; let $q(\theta)$ correspond to that i.e., let $q(\theta)$ be such that $deg[a(\theta) - \mu(\theta)q\theta)]$. We record $r(\theta) = a(\theta) - \mu(\theta)q(\theta)$; thus $deg r(\theta)$ is the least element of S. If $deg r(\theta) \geq deg\mu(\theta)$ then [(iii)(a) on preceding page 11] we know there is some $b(\theta)$ with $deg[r(\theta) - \mu(\theta)b(\theta)] < deg r(\theta)$ so that with $q_1 = q(\theta) + b(\theta)$, we have $deg[a(\theta) - \mu(\theta)q_1(\theta)] < deg r(\theta)$ which contradicts the choice of $q(\theta)$ that had assumed $deg(a(\theta) - \mu(\theta)q_1(\theta))$ as the least element of S. Therefore, we must have $deg(r(\theta)) < deg(\mu(\theta))$ and we have found our $q(\theta)$ with $a(\theta) = \mu(\theta)q(\theta) + r(\theta), deg r(\theta) < deg\mu(\theta)$ as required.

[this argument works for $deg a(\theta\theta) \geq deg\mu(\theta)$;if $deg a(\theta) < deg\mu(\theta)$ put$q(\theta) = 0, r(\theta) = a(\theta)$. Further,note that if $dega(\theta)=0$, then $deg\mu(\theta)=0$ is forced since $deg\mu(\theta)=\infty$ is not permissible with invertible leading coefficient; then $a(\theta)=a_0, \mu(\theta)=\mu_0$ and μ_0 is invertible, take $q=\mu_0^{-1}a_0$].

(v) In this preceding, q is the left quotient and r is the left remainder on left division by $\mu(\theta)$;we say $\mu(\theta)$ is a left divisor of a iff r=0. we similarly have

The right division algorithm:

Given $a(\theta)\ \varepsilon\ \mathbb{K}\ [\theta]$, and $\mu(\theta)\varepsilon\mathbb{K}[\theta]$ with invertible leading coefficient, there is exactly one $q(\theta)\varepsilon\mathbb{K}[\theta]$ such that $a(\theta)=q(\theta)\mu(\theta)+r(\theta)$ with $degr(\theta)<deg\mu(\theta)$ and then $r(\theta)$ is also uniquely determined. Further, we say $q(\theta)$is the right quotient, $r(\theta)$ is the right remainder on right division by $\mu(\theta)$.

[The proof will use (iii) b on pase 11 preceding].

Example 0.1. If $a_3=\begin{pmatrix}1 & 2\\ 0 & 0\end{pmatrix}$, $\begin{pmatrix}-1 & 0\\ 1 & 3\end{pmatrix}$ $a_1=\begin{pmatrix}2 & 3\\ -2 & 0\end{pmatrix}$,$a_0=\begin{pmatrix}0 & -1\\ 1 & 2\end{pmatrix}$ and $\mu_1=\begin{pmatrix}2 & 1\\ 1 & 1\end{pmatrix}$,$\mu_0=\begin{pmatrix}1 & -1\\ 0 & 2\end{pmatrix}$ where $a(\theta)=a_0+a_1\theta+a_2\theta^2+a_3\theta^3$
$\mu(\theta)=\mu_0+\mu_1\theta$. The right quotient and remainder are $q(\theta)=q_0+q_1\theta+q_2\theta^2, r(\theta)=r_0$ with $q_2=\begin{pmatrix}-1 & 3\\ 0 & 0\end{pmatrix}$,$q_1=\begin{pmatrix}7 & -14\\ -2 & 5\end{pmatrix}$,$q_0=\begin{pmatrix}-43 & 81\\ 12 & -24\end{pmatrix}$ and $r_0=\begin{pmatrix}43 & -206\\ -11 & 62\end{pmatrix}$ while the left quotient is $q(\theta)=q_0+q_1\theta+q_2\theta^2$ and the left remainder is $r_0=\begin{pmatrix}-94 & -169\\ 115 & 206\end{pmatrix}$ on left and right division of $a(\theta)$ by $\mu(\theta)$ respectively.[Please verify this].

Proposition For a ring $\mathbb{K}$ and $\alpha,\beta\varepsilon\mathbb{K}$, the following are equivalent:

1. There is an invertible $y\varepsilon\mathbb{K}$ such that $\beta=\gamma\alpha\gamma^{-1}$

2. There are invertibles $p(\theta), q(\theta)\varepsilon\mathbb{K}[\theta]$ with $\theta-\beta=p(\theta)(\theta-\alpha)q(\theta)$

Proof : (1) $\Rightarrow$ (2) Since $\theta\varepsilon cen\mathbb{K}[\theta]$ and the constants $\gamma,\gamma^{-1}\varepsilon\mathbb{K}[\theta]$, we find $\theta-\beta=\theta\gamma\gamma^{-1}-\gamma\alpha\gamma^{-1}=\gamma\theta\gamma^{-1}-\gamma\alpha\gamma^{-1}=\gamma(\theta-\alpha)\gamma^{-1}$ which prove (2).

(2) $\Rightarrow$ (1)Let invertibles $p(\theta), q(\theta)\varepsilon\mathbb{K}[\theta]$ be given with $\theta-\beta=p(\theta)(\theta-\alpha)q(\theta)$.Since $\theta-\alpha$ has leading coefficient $1\neq 0$ the division algorithm assume the existence of uniquely given $a(\theta)$and $u(\theta)$such that

$(p(\theta)^{-1})\varepsilon\mathbb{K}[\theta]$ can be written as $(p(\theta)^{-1}) = (\theta-\alpha)a(\theta)+u(\theta), deg u(\theta) < deg(\theta-\alpha) = 1$ which forces $u = u(\theta)\varepsilon\mathbb{K}$. then $u(\theta-\beta) = [p(\theta)^{-1} - (\theta-\alpha)a(\theta)](\theta-\beta) = (p(\theta))^{-1}(\theta-\beta) - (\theta-\alpha)a(\theta)(\theta-\beta) = (p(\theta))p(\theta)(\theta-\alpha)q(\theta) - (\theta-\alpha)a(\theta)(\theta-\beta) = (\theta-\alpha)[q(\theta)-a(\theta)(\theta-\beta)]$

comparing the highest degree terms on both sides, we get $q(\theta) - a(\theta)(\theta-\beta)u$ The equation is thus $u(\theta-\beta) = (\theta-\alpha)u$ which has forces $u\beta = \alpha u$. Dividing $p(\theta)$ by $(\theta-\beta)$ [which has leading coefficent $1 \neq 0$] we get $p(\theta) = (\theta-\beta)b(\theta)+r(\theta)$, with $deg r(\theta) < deg(\theta-\alpha) = 1$ forcing $r(\theta) = r\varepsilon\mathbb{K}$.

We have $1 = p(\theta)[p(\theta)]^{-1} = p(\theta)[(\theta-\alpha)a(\theta)+u] = p(\theta)(\theta-\alpha)a(\theta)+p(\theta)u = (\theta-\beta)[q(\theta)]^{-1}a(\theta) + [(\theta-\beta)p(\theta+r)]u = (\theta-\beta)[q(\theta)a(\theta)+b(\theta)u]+ru$ so that $1-ru = (\theta-\beta)[q(\theta)a(\theta)+b(\theta)u]$ comparing the coefficient if on both sides,we get RHS=0 hence $1-ru = 0$ which forces $ru = 1$. Further,we have $1 = [p(\theta)]^{-1}p(\theta) = [(\theta-\alpha)a(\theta)+u]p(\theta) = [(\theta-\alpha)a(\theta)+u][(\theta-\beta)b(\theta)+r] = (\theta-\alpha)a(\theta)(\theta-\beta)b(\theta)+(\theta-\alpha)a(\theta)r+u(\theta-\beta)b(\theta)+ur$ so that $1-ur = (\theta-\alpha)a(\theta)(\theta-\beta)b(\theta)+(\theta-\alpha)a(\theta)r+u(\theta-\beta)b(\theta)$Comparing the coefficients of θ on both sides, we get RHS=0 which forces $1-ur = 0$. Therefore, u is invertible with inverse r.

Euclidean domain :

We say a ring is an entire ring iff $\lambda\mu = 0 \Rightarrow$ either $\lambda = 0$ or $\mu = 0$; a commutative entire ring is also called integral domain.[Some text books use 'integral domain' for 'entire ring' also]. An integral domain $\mathbb{K}$ is called a Euclidean domain iff there is an 'Euclidean function'$\mathbb{K}|\{0\} \rightarrow^{g} \mathbb{N}$ satisfying

E_1 if λ divides $\mu[\neq 0]$ then $g(\lambda) \leq g(\mu)$

E_2 For every pair of elements α, β of $\mathbb{K}$,$\alpha \neq 0$

there exists elements $\gamma, \delta\varepsilon\mathbb{K}$ with $\beta = \alpha\gamma+\delta$ with $\delta = 0$ or $g(\delta) < g(\alpha)$.[thus in a domain, it is called 'Euclidean algorithm']. In the preceding section, we proved that if $\mathbb{F}$ is a field, $\mathbb{F}[\theta]$ is a Euclidean domain $[g(a(\theta)) = deg a(\theta)]$ The ring of integers $\mathbb{Z}$ is also an integral domain [This is the reason for 'integral' domain'] with $g(a) = |a|, a\varepsilon\mathbb{Z}$. Indeed, if $b = ac \neq 0$ then $|c| \geq 1$ and hence $|b| = |c||a| \geq |a|$. Further, for any two integers $a, b, a \neq 0$ the division algorithm in $\mathbb{Z}$ ensures $b = |a|q + r = a(\pm q) + r$ with $r = 0$ or $0 < r < |a|$. These two examples of Euclidean domains are the ones we shall use in this course .However, there are other Euclidean domains: let $d \neq 1$ be a square free integer [in the sense that its prime factorization has no square] and let $\theta = \{ \frac{\frac{1+\sqrt{d}}{2}}{\sqrt{d}} \ \frac{if \quad d \equiv 1 mod 4}{otherwise}$

Consider $\mathbb{Q}[\sqrt{d}]$ [we met this on pase 8 preceding] which is a field; for $\alpha = p + q\sqrt{d}$ we write$p^2 - q^2 d$ as $N(\alpha)$. Then for $d = -1, -2, -3, -7, -11, 2, 3, 5, 6, 7, 13, 17, 21, 29$, the function $g(\alpha) = |N(\alpha)|$ is a

Euclidean function; we shall not prove this here.

Proposition The *gcd* of any two elements α, β not both zero, of Euclidean domain $\mathbb{E}$ exists and can be expressed as $\alpha\lambda + \beta\mu$ with $\lambda, \mu \varepsilon \mathbb{E}$.

Proof : Suppose g is the Euclidean function, $g(\alpha) \geq g(\beta)$. Then by the property of g [the 'Euclidean algorithm',also called 'division algorithm'] we have $\alpha = \beta\gamma_1 + \delta_1, g(\delta_1) < g(\beta)$; $\beta = \delta_1\gamma_2 + \delta_2, g(\delta_2) < g(\delta_1)$

$\ldots \qquad \ldots \qquad \ldots$

Thus $g(\beta) > g(\delta_1) > g(\delta_2) \ldots$ is a decreasing sequence of nonnegative integers which must stop and after some time, we have $\delta_{n-2} = \delta_{n-1}\gamma_n + \delta_n$, $\delta_{n-1} = \delta_n\gamma_{n+1} + \delta_{n+1}$ with $\delta_{n+1} = 0 = \delta_k$ for any $k > n+1$ now $\delta_1 = \alpha - \beta\gamma_1$ so δ_1 has the form $\alpha\lambda + \beta\mu$ with $\lambda = 1, \mu = -\gamma_1$. In general, if $\delta_{i-1} = \alpha\lambda_{i-1} + \beta\mu_{i-1}$ and $\delta_{i-2} = \alpha\lambda_{i-2} + \beta\mu_{i-2}$

$\delta_i = -\delta_{i-1}\gamma_i + \delta_{i-2} = -(\alpha\lambda_{i-1} + \beta\mu_{i-1})\gamma_i + \alpha\lambda_{i-2} + \beta\mu_{i-2} = \alpha[\lambda_{i-2} - \lambda_{i-1}] + \beta[\mu_{i-2} - \mu_{i-1}\gamma_i]$ also has this form $\alpha\lambda + \beta\mu$ [with $\lambda = \lambda_{i-2} - \lambda_{i-1}, \mu = \mu_{i-2} - \mu_{i-1}\gamma_i$]. Thus $\delta_n = \alpha\lambda_n + \beta\mu_n$ for some $\lambda_n, \mu_n \varepsilon \mathbb{E}$. Now $\delta_n = \delta_n.1{+}0$ so δ_n divides δ_n and $\delta_{n-1} = \delta_n\gamma_{n+1}{+}0$ so δ_n divides δ_{n-1}. But we have $\delta_{n-2} = \delta_{n-1}\gamma_n + \delta_n = \delta_n\gamma_{n+1}\gamma_n + \delta_n = \delta_n[\gamma_{n+1}\gamma_n + 1]$ so δ_n divides δ_{n-2}. Similarly, δ_n divides all the 'remainders'δ_i.Let $\delta_i = \delta_n p_i, p_i \varepsilon \mathbb{E}$. Then $\beta = \delta_1\gamma_2 + \delta_2 = \delta_n p_1\gamma_2 + \delta_n p_2 = \delta_n[p_1\gamma_2 + \beta_2]$ so that δ_n divides β and $\alpha = \beta\gamma_1 + \delta_1$ $= \delta_n[p_1\gamma_2 + \beta_2]\gamma_1 + \delta_n p_1 = \delta_n[p_1\gamma_2\gamma_1 + p_1]$

so that δ_n divides α.

Thus is a common divisor of α and β. If γ is any other divisor of α and β say $\alpha = \gamma p, \beta = \gamma q, p, q \varepsilon \mathbb{E}$ then $\delta_n = \alpha\lambda_n + \beta\mu_n = \gamma p\lambda_n + \gamma q\mu_n = \gamma[p\lambda_n + q\mu_n]$ so that γ divides δ_n.Thus δ_n is the greatest common divisor of α and β, and is of the form $\alpha\lambda + \beta\mu$ [with $\lambda = \lambda_n, \mu = \mu_n$]. This proves that advertized result.But there is a further piece of information.Suppose $\alpha = \delta_n a, \beta = \delta_n b$ then writing $\delta_n\ m = \alpha\beta$, we have $\delta_n\ m = \delta_n a\delta_n b = a\delta_n^2 b = \delta_n^2 ab$ [because of commutativity] i.e. $m = a\beta$ and $m = b\alpha$ [$\because \mathbb{E}$ is a integral domain ,$\delta_n \neq 0$] so that m is a common multiple. If m' is another common multiple, then $m' = \alpha c_1, m' = \beta c_2$ hence $\delta_n m' = (\alpha\lambda_n + \beta\mu_n)m' = \alpha m'\lambda_n + \beta m'\mu_n = \alpha\beta c_2\lambda_n + \beta\alpha c_1\mu_n = \alpha\beta[c_2\lambda_n + c_1\mu_n] = \delta_n m[c_2\lambda_n + c_1\mu_n]$ But then $\delta_n[m' - m(c_2\lambda_n + c_1\mu_n)] = 0$ and since $\delta_n \neq 0$, and $\mathbb{E}$ is an integral domain,we get $m' - m(c_2\lambda_n + c_1\mu_n) = 0$ which means $m' = m(c_2\lambda_n + c_1\mu_n)$ so that m is a divisor of m'.Thus m is the least common multiple of α, β.

To sum up: In a Euclidean domain, both the *LCM* and *GCD* exists.

[There are rings in which the *LCM* exists and the *GCD* dose not and vice versa; this is not the place to go in more detail] Now suppose A is an ideal in a Euclidean domain $\mathbb{E}$ [For 'ideal' see Modules, pase 14]. Pick $a \varepsilon A$ with $a = bq + r$ where $g(b)$ has the least value for element of A.Then since $a, b \varepsilon A$, we have $r = a - bq \varepsilon A$ with $g(r) < g(b)$ which is not possible since b has the least value $g(b)$ for elements of A.Thus $r = 0$ and we have '$A = (a) = \{a\lambda | \lambda \in \mathbb{E}\}'$.Such an ideal which is generated by a single element is called a principal ideal.To sum up: Every Euclidean domain $\mathbb{E}$ is a principal ideal domain in the sense that every ideal in $\mathbb{E}$ is a principal ideal.