§ 10 Polynomial Algebras

10.A Polynomials in one variable

Let K be a field. It is often useful and convenient to distinguish between polynomials and the ~~Polynomial~~ functions defined by it. A __polynomial function__ $K \longrightarrow K$ is a function of the form $t \longmapsto a_0 + a_1 t + \cdots + a_n t^n$ with coefficients $a_0, \cdots, a_n \in K$. If K has infinitely many elements, then the polynomial function determines its coefficients uniquely. If K has only finitely many elements, then this is not the case: for example, if $c_1, \cdots, c_n$ are all the elements of K then the polynomial function $\underbrace{(t-c_1) \cdots (t-c_n)}_{= a_0 + a_1 t + \cdots + a_{n-1} t^{n-1} + t}$ is the constant function zero, but all of its coefficients are not zero.

A __polynomial__ $a_0 + a_1 X + \cdots + a_n X^n = \sum a_i X^i$ over K determines the coefficient tuple $(a_i) \in K^{(\mathbb{N})}$ (where $\underset{\text{by definition}}{a_i = 0}$ for $i > n$) uniquely. Therefore, we identify a polynomial with its coefficient tuple.

Two polynomials $P = \sum_{i \in \mathbb{N}} a_i X^i$ and $Q = \sum_{i \in \mathbb{N}} b_i X^i$ will be added coefficientwise, like in $K^{(\mathbb{N})}$, i.e.

$$P + Q := \sum_{i \in \mathbb{N}} (a_i + b_i) X^i.$$ Further, multiplied

by scalar $a \in K$ also by coefficient-wise, i.e.

$$aP = \sum_{i \in \mathbb{N}} (a \, a_i) X^i.$$

The multiplication two polynomials

$$PQ := \sum_{i \in \mathbb{N}} c_i X^i \text{ with } c_i := \sum_{j=0}^{i} a_j \cdot b_{i-j} = a_0 b_i + \cdots + a_i b_0$$

An easy calculation shows that: the set of polynomials with this K-vector space structure and the above multiplication is a commutative K-algebra. We denote this K-algebra by $K[X]$. It is called the polynomial algebra (in one variable) over K. By definition X^m, $m \in \mathbb{N}$, is a K-basis of $K[X]$, this corresponds to the standard basis e_m, $m \in \mathbb{N}$, of $K^{(\mathbb{N})}$. Further, X^m is the m-th power of X in the K-algebra $K[X]$ and hence the m-fold product of $X = e_1$ with itself. For the indeterminate or variable X, occasionally we also use another Capital-letter, e.g. Y or Z etc. The unit element in $K[X]$ is the polynomial $1 + 0 \cdot X + \cdots$, we shall identify this with the unit element in K. Similarly, we shall identify the multiples $a \cdot 1 = a + 0 \cdot X + \cdots$, $a \in K$, with the elements $a \in K$. These elements

a in $K \subseteq K[X]$ are called the <u>constant</u> <u>polynomials</u>. If $P = \sum_{i \in \mathbb{N}} a_i X^i$ is a non-zero polynomial in $K[X]$ and if $a_n \neq 0$, but $a_m = 0$ for all $m > n$, then $P = a_0 + a_1 X + \cdots + a_n X^n$, $a_n \neq 0$, and hence n is called the <u>degree</u> of P and a_n is called the <u>leading coefficient</u> of P. If the leading coefficient of a polynomial P is 1, then P is called <u>monic</u>. The degree of the zero polynomial is $\overset{by}{\vee}$ definition $-\infty$. The poly-nomials of degree 0 are precisely non-zero constant polynomials. The degree of a polyno-mial P is denoted by $\deg P$.

The n-dimensional K-subspace of the poly-nomials in $K[X]$ of degrees $< n$ is denoted by $K[X]_n$; $1, X, \cdots, X^{n-1}$ is a K-basis of $K[X]_n$.

<u>10.A.1</u> For polynomials $P, Q \in K[X]$, we have

$$\deg (P+Q) \leq \text{Max} (\deg P, \deg Q) \quad \text{and}$$
$$\deg (PQ) = \deg P + \deg Q$$

<u>Proof</u> The assertions are trivial if any one of the polynomial P or Q is the zero-polynomial. Assume that $P = a_0 + a_1 X + \cdots + a_n X^n$, $Q = b_0 + b_1 X + \cdots + b_m X^m$, with $a_n \neq 0$, $b_m \neq 0$. Then $a_i + b_i = 0$ for all $i > \text{Max}(m, n)$ and hence $\deg (P+Q) \leq \text{Max}(m, n)$. Further, $PQ = a_0 b_0 + (a_0 b_1 + a_1 b_0) X + \cdots + a_n b_m X^{n+m}$, $a_n b_m \neq 0$, and hence $\deg PQ = n + m$.

Note that 10.A.1 in particular implies that the product PQ of two polynomials $P, Q \in K[X]$ is 0 if and only if one of its factor is 0. From this the _cancellation law_ follows: from $PR = QR$ and $R \neq 0$, it follows that $P = Q$ for P, Q, R in $K[X]$. Since $PR = QR$ implies $(P-Q)R = 0$ and hence $P - Q = 0$ because $R \neq 0$.

One can prove the theorem on division with remainder in $K[X]$ exactly similar to that of $\mathbb{Z}$.

10.A.2 Division with remainder Let F, G be two polynomials in $K[X]$, $G \neq 0$. Then there exist unique polynomials Q and R in $K[X]$ such that $F = QG + R$ and $\deg R < \deg G$.

The polynomial Q is called the _quotient_ and the polynomial R is called the _remainder_ of the division of F by G.

10.A.3 Example Let
$$F := 3X^4 + \frac{3}{2}X^3 + \frac{7}{2}X^2 + 2X + 2, \quad G := 2X^2 + X + 1 \in \mathbb{Q}[X]$$

Then the following computation scheme gives division of F by G:

$$(3X^4 + \frac{3}{2}X^3 + \frac{7}{2}X^2 + 2X + 2) : (2X^2 + X + 1) = \frac{3}{2}X^2 + 1$$
$$-(3X^4 + \frac{3}{2}X^3 + \frac{3}{2}X^2)$$
$$\underline{ 2X^2 + 2X + 2}$$
$$- 2X^2 + X + 1$$
$$\overline{ X + 1}$$

$Q :=$ quotient

$R = X + 1$, remainder.

$F = (\frac{3}{2}X^2 + 1) G + (X + 1)$.

If the remainder of the division of F by G is equal to 0, i.e. $F = QG$, then F is said to be __divisible__ by G or F is a __multiple__ of G and denote it by $G|F$.

As in the case of integers we have the __Euclidean algorithm__ :

Let F and G be polynomials in $K[X]$, $G \neq 0$. We put $R_0 := F$ and $R_1 := G$ and define polynomials $R_2, \cdots, R_{k+1}$ through the recursion :

$$R_0 = Q_1 R_1 + R_2, \quad 0 \leq \deg R_2 < \deg R_1$$
$$R_1 = Q_2 R_2 + R_3, \quad 0 \leq \deg R_3 < \deg R_2$$
$$\cdots\cdots$$
$$R_{k-1} = Q_k R_k + R_{k+1}, \quad 0 \leq \deg R_{k+1} < \deg R_k$$
$$R_k = Q_{k+1} R_{k+1}$$

R_{k+1} is the last non-zero remainder

$$\begin{pmatrix} Q_i & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} R_i \\ R_{i+1} \end{pmatrix} = \begin{pmatrix} R_{i-1} \\ R_i \end{pmatrix}$$

$$i = 1, \cdots, k+1$$

(put $R_{k+2} = 0$)

As in the case $\mathbb{Z}$ we also have :

__10.A.4__   We have $R_{k+1} = \gcd(F, G)$.

Where $\gcd(F, G)$ denote a __greatest common divisor__ of F and G, this is a common divisor of F and G which is divisible by every other common divisor. Two greatest common divisors of F and G divide each other and hence on the degree-argument they differ by a non-zero constant. The greatest common divisor of F and G (the polynomials)

(at least one of which is $\neq 0$; otherwise $\gcd(F,G)=0$) is therefore only, upto a non-zero constant, uniquely determined). Choose a greatest common divisor which is a _monic_ polynomial, so that it is uniquely determined.

Two polynomials F and G are called relatively prime if $\gcd(F,G)=1$.

The _proof_ of 10.A.4 follows easily from the scheme of Euclidean algorithm, the polynomials R_i, R_{i+1} and R_{i-1}, R_i have the same greatest common divisors for all $i=1,\cdots,k$, i.e.

$$\gcd(R_i, R_{i+1}) = \gcd(R_{i-1}, R_i)$$
and $\quad\gcd(R_k, R_{k+1}) = R_{k+1}.$

The Euclidean algorithm implies much more, with its help we get a prepresentation
$$\gcd(F,G) = SF + TG$$
i.e. the greatest common divisor $\gcd(F,G)$ is a linear combination of F and G with coefficients $S, T \in K[X]$. For this we define recursively:

$S_0 = 1, T_0 = 0; \quad S_1 = 0, T_1 = 1;$
$$\begin{pmatrix} 0 & 1 \\ 1 & -Q_i \end{pmatrix}\begin{pmatrix} S_{i-1} \\ S_i \end{pmatrix} = \begin{pmatrix} S_i \\ S_{i+1} \end{pmatrix}$$
$S_{i+1} = S_{i-1} - Q_i S_i, \quad T_{i+1} = T_{i-1} - Q_i T_i, \quad i=1,\cdots,k.$

Then $R_{i+1} = S_{i+1}F + T_{i+1}G$ for $i=0,\cdots,k$ and in particular, $\gcd(F,G) = R_{k+1} = S_{k+1}F + T_{k+1}G$

$$R_0 = F, \quad R_1 = G$$

$$R_0 = Q_1 R_1 + R_2 \,, \quad 0 \leq \deg R_2 < \deg R_1$$

$$R_1 = Q_2 R_2 + R_3 \,, \quad 0 \leq \deg R_3 < \deg R_2$$

$$R_{k-1} = Q_k R_k + R_{k+1} \qquad 0 \leq \deg R_{k+1} < \deg R_k$$

$$R_k = Q_{k+1} R_{k+1} . \qquad \text{Put } R_{k+2} = 0$$

1) $\quad \gcd(R_0, R_1) = \gcd(R_1, R_2) = \cdots = \gcd(R_k, R_{k+1})$
$$= R_{k+1}$$

2) $\quad \begin{pmatrix} Q_1 & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} R_1 \\ R_2 \end{pmatrix} = \begin{pmatrix} R_0 \\ R_1 \end{pmatrix}$

$$\begin{pmatrix} Q_i & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} R_i \\ R_{i+1} \end{pmatrix} = \begin{pmatrix} R_{i-1} \\ R_i \end{pmatrix} , \quad i = 1, \ldots, k, k+1 \qquad \boxed{R_{k+2} = 0}$$

$$\underbrace{\phantom{\begin{pmatrix} Q_i & 1 \\ 1 & 0 \end{pmatrix}}}_{\mathcal{D}_i}$$

$$\bar{\alpha}_i^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -Q_i \end{pmatrix}$$

$$\underbrace{\begin{pmatrix} \mathcal{D}_{k+1} & \mathcal{D}_k & \cdots & \mathcal{D}_1 \end{pmatrix}}_{=: \, \mathcal{D}} \begin{pmatrix} R_1 \\ R_2 \end{pmatrix}$$

$$\begin{pmatrix} \mathcal{D}_1 & \cdots & \mathcal{D}_{k-1} & \mathcal{D}_k \end{pmatrix} \begin{pmatrix} R_{k+1} \\ 0 \end{pmatrix} = \begin{pmatrix} R_0 \\ R_1 \end{pmatrix}$$

$$\begin{pmatrix} 0 & 1 \\ 1 & -Q_i \end{pmatrix} \begin{pmatrix} S_{i-1} \\ S_i \end{pmatrix} \begin{pmatrix} R_{k+1} \\ 0 \end{pmatrix} = \mathcal{D}^{-1} \begin{pmatrix} R_0 \\ R_1 \end{pmatrix} = \begin{pmatrix} S & T \\ U & V \end{pmatrix} \begin{pmatrix} R_0 \\ R_1 \end{pmatrix}$$

$$= \begin{pmatrix} S_i \\ S_{i+1} \end{pmatrix} \qquad = \begin{pmatrix} S R_0 + T R_1 \\ U R_0 + V R_1 \end{pmatrix}$$

The fundamental theorem of the elementary number theory on the uniqueness of the prime decomposition of integers also has analog in $K[X]$. For this first we must define the polynomials which correspond to the prime numbers:

10.A.7 Definition A polynomial $P \in K[X]$ is called a _prime polynomial_ or _prime_, if $\deg P \geq 1$ and every divisor of P is constant or a multiple aP, $a \in K^\times$ of P.

Clearly a polynomial $P \in K[X]$ of degree ≥ 1 is prime if and only if there is no decomposition $P = FG$ of P as a product of polynomials $F, G \in K[X]$ of degrees $< \deg P$. Prime polynomials are therefore also _indecomposable_ or _irreducible_.

If P is a prime polynomial which does not divide the polynomial $F \in K[X]$, then $\gcd(F, P) = 1$. From the Lemma of Bezout it follows that:

10.A.8 Lemma of Euclid _If a prime polynomial $P \in K[X]$ divide a product $F_1 \cdots F_r$ of polynomials $F_1, \cdots, F_r \in K[X]$, then P divides at least one of the factor $F_1, \cdots, F_r$._

Proof Without loss of generality, we may assume that $r = 2$ and P is not a divisor of F_1.

Then $\gcd(P, F_1) = 1$ and hence there exist polynomials $S, T \in K[X]$ with $1 = SP + TF_1$. Therefore $F_2 = SPF_2 + TF_1F_2$. Now, since P divides F_1F_2, P also divides F_2.

10.A.9 Theorem on the uniqueness of prime factorisation in $K[X]$

Every polynomial $F \in K[X]$ with $\deg F \geqslant 1$ can be written as a product of prime polynomials. Moreover, the prime factors are uniquely determined, upto permutation and upto multiplication by constants, by F.

Proof We shall first prove the <u>existence</u> of the prime factorisation by induction on $\deg F$. If $\deg F = 1$, then F is irreducible. Now, assume that $\deg F > 1$. If F is not irreducible, then F has a representation $F = F_1F_2$ with the degrees of F_1 and F_2 are strictly smaller than $\deg F$. Therefore by induction hypothesis F_1 and F_2 are product of prime polynomials and hence F is also a product of prime polynomials.

For the proof of <u>uniqueness</u>, suppose that $F = P_1 \cdots P_r = Q_1 \cdots Q_s$ are two representations of F as product of prime polynomials. By induction on r we shall show that $r = s$ and after renumbering $Q_i = a_i P_i$ with $a_i \in K^{\times}$, $i = 1, \cdots, r$. Clearly $r \geqslant 1$. Since the prime polynomial P_1 divides the product $Q_1 \cdots Q_s$ from 10.A.8 it follows

that P_1 divides one of the factors $Q_1, \ldots, Q_s$, say Q_1. Now, since Q_1 is prime, necessarily $Q_1 = a_1 P_1$ with $a_1 \in K^x$. Cancelling P_1 on both sides, we get $G := P_2 \cdots P_r = (a_1 Q_2) \cdots Q_s$. Applying induction hypothesis to G, the assertion is immediate.

Collecting together some prime factors we obtain prime polynomial powers to get the Cannonical prime factorisation :

Let $\mathcal{P}$ be the set of monic prime polynomials in $K[X]$. For every polynomial $F \in K[X]$, $F \neq 0$, there exist unique element $a \in K^x$ and unique natural numbers α_P, $P \in \mathcal{P}$, (almost all of which are 0) such that

$$F = a \prod_{P \in \mathcal{P}} P^{\alpha_P}.$$

The element a is necessarily the leading coefficient of F. The exponent α_P is called the multiplicity of $P \in \mathcal{P}$ in F.

In the monic prime polynomials $P \in \mathcal{P}$, there are in particular, the linear factors $X - c$, $c \in K$.

Let $F = a_0 + a_1 X + \cdots + a_n X^n \in K[X]$. Then F defines the K-valued function $K \longrightarrow K$, $t \longmapsto F(t) := a_0 + a_1 t + \cdots + a_n t^n$ by substitution.

This function is called the _polynomial function_ corresponding to F. For all $F, G \in K[X]$ and all $a, t \in K$, we have

$$(F+G)(t) = F(t) + G(t), \quad (FG)(t) = F(t)G(t) \text{ and}$$
$$(aF)(t) = aF(t).$$

This means that the map $K[X] \longrightarrow K^K$ which assigns every polynomial F to corresponding polynomial function, is a K-algebra homomorphism from the polynomial algebra $K[X]$ in the K-algebra K^K of K-valued functions on K.

If $F(c) = 0$ for $F \in K[X]$ and $c \in K$, then c is called a _zero_ of the polynomial F.

10.A.10 Theorem Let $c \in K$. Then c is a zero of $F \in K[X]$ if and only if $X-c$ is a factor of F.

Proof The division of F by $X-c$ gives a representation $F = Q \cdot (X-c) + r$, $Q \in K[X]$, $r \in K$. Then $F(c) = Q(c)(c-c) + r = r$ and hence the assertion follows.

Now, if $F \in K[X]$, $F \neq 0$ and

$$F = a \prod_{\in K} (X-c)^{\alpha_c} \prod_{\deg P \geq 2} P^{\alpha_P}$$

is the canonical prime factorisation of F, then by 10.A.10 for an element $c \in K$ the multiplicity

α_c of the linear factors $X-c$ is bigger than
0 if and only if c is a zero of F. For $c \in K$,
the multiplicity α_c is also called the multi-
plicity of the zero c. (Therefore $\alpha_c = 0$ means
that c is not a zero of F). It is clear that

$$\sum_{c \in K} \alpha_c \leq \deg F$$

Where the equality holds if and only if F has
no prime factor of degree ≥ 2. Therefore:

10.A.11 Theorem A polynomial $F \in K[X]$
of degree $n > 0$ has at most n zeros in K,
even if these zeros are counted with their
multiplicities.

For example, all non-zero elements in K_p are zeros of
the polynomial $X^{p-1} - 1$
$\in K_p[X]$ by Fermat's little theorem. Therefore

$$X^{p-1} - 1 = \prod_{k=1}^{p-1} (X-k)$$

In this identity putting $X = 0$, we get the
well-known __Wilson's formula__:

$$-1 \equiv (p-1)! \mod p.$$

Further, as a corollary to 10.A.11 we note:

10.A.12 Identity Theorem Let $F, G \in K[X]$
be polynomials of degree $\leq n$. If the values
of F and G are equal at $n+1$ distinct elements

$t_1, \cdots, t_{n+1} \in K$, then $F = G$.

Proof The polynomial $F - G$ has degree $\leq n$ and $t_1, \cdots, t_{n+1}$ are zeros of $F - G$ and hence by 10.A.11 necessarily $F - G$ is the zero polynomial.

From 10.A.12 in particular it follows that if K is an infinite field, then distinct polynomials define distinct polynomial functions. Therefore, in this case identification of the polynomials with the corresponding polynomial functions is possible.

If there is no prime polynomial in $K[X]$ of degree ≥ 2, then every polynomial $F \in K[X]$, $F \neq 0$, has the prime factorisation

$$F = a \prod_{c \in K} (X-c)^{\alpha_c}$$

into only linear factors. This is exactly the case if every polynomial of degree ≥ 1 in $K[X]$ has at least one zero in K (since a prime polynomial of degree ≥ 2 cannot have a zero)

10.A.13 Definition A field K is called algebraically closed if every non-constant polynomial $F \in K[X]$ has a zero in K.

Now, we can formulate the fundamental theorem of algebra as follows:

10.A.14 Theorem

The field $\mathbb{C}$ of complex numbers is algebraically closed.

The field $\mathbb{R}$ of real numbers is <u>not</u> algebraically closed. The polynomial X^2+1 has no zero in $\mathbb{R}$ and hence it is a prime polynomial in $\mathbb{R}[X]$. As a corollary to the fundamental theorem of algebra we note that:

10.A.15 Theorem

The monic prime polynomials in $\mathbb{R}[X]$ are precisely the polynomials

$X-c$, $c \in \mathbb{R}$ and X^2+pX+q, $p,q \in \mathbb{R}$ with $p^2-4q<0$.

In particular, the prime factorisation of every real polynomial $F \in \mathbb{R}[X]$, $F \neq 0$, contains only linear and quadratic factors.

10.A.16 Example (Polynomials with rational coefficients)

Let K be a field. A polynomial $F \in K[X]$ of degree 3, which is <u>not</u> prime has a factorisation $F=GH$ with $\deg G$, $\deg H < 3$ and hence one of the factor G or H is linear. It follows that: A polynomial $F \in K[X]$ of degree 3 is prime if and only if F has no zero in K. For a polynomial $F \in \mathbb{Q}[X]$ it is easy[1] to decide whether or not F has a zero in $\mathbb{Q}$ and so for a polynomial of degree 3 in $\mathbb{Q}[X]$, it is easy to decide whether it is prime or not. For example,

1 PTO↷ Lemma of Gauss (On page 10A/14a)

the polynomial $P = X^3 + 4X + 2$ is prime in $Q[X]$, since $\pm 1, \pm 2$ are not zeros of P and hence P has no rational zeros.

In general for polynomials of higher degrees over Q, it is very troublesome to decide whether it is prime or not. The polynomials $X^2 - 2$ and $X^3 - 2$ are prime in $Q[X]$. It is less trivial to prove that the polynomial $X^k - 2$ for $k > 3$ is also prime in $Q[X]$. In the following we will present some elementary results which will help to solve the above problem.

For polynomial $F \in Q[X]$, $F \neq 0$, we recommed to use a canonical representation: With the help of common denominator for the coefficients of F, we may write F in the form $F = \frac{1}{q} \tilde{F}$ with $q \in \mathbb{Z} \setminus \{0\}$ and $\tilde{F} \in \mathbb{Z}[X]$ with positive leading coefficient; where $\mathbb{Z}[X]$ denote the subring of $Q[X]$ consisting of polynomials with coefficients in $\mathbb{Z}$. Now, taking out the greatest common divisor of the coefficients of $\tilde{F}$, we get a unique representation $F = I(F) F^*$ with a rational number $I(F) \in Q^*$ and a polynomial $F^* \in \mathbb{Z}[X]$ having relatively prime coefficients and positive leading coefficient. $I(F)$ is called the content[1] of F and F^* is called the primitive part of F. First we prove:

---

[1] Clearly $I(F)$ (upto a sign) the greatest common divisor of the coefficients of F in the following sense: See Exercise on Page

10.A.17 Lemma Let $G = b_0 + b_1 X + \cdots + b_m X^m$ and $H = c_0 + c_1 X + \cdots + c_n X^n$ be polynomials with coefficients in $\mathbb{Z}$ and let $F = GH = a_0 + a_1 X + \cdots + a_{m+n} X^{m+n}$ be their product. For the prime number p, suppose that $p | b_0, \cdots, p | b_{r-1}, p \nmid b_r; p | c_0, \cdots, p | c_{s-1}$ $p \nmid c_s$. Then p divides the coefficient $a_0, \cdots, a_{r+s-1}$, but p does not divide a_{r+s}.

Proof For $j < r+s$, i.e. $j-r < s$, every summand of the sum

$$a_j = b_0 c_j + b_1 c_{j-1} + \cdots + b_{r-1} c_{j-r+1} + b_r c_{j-r} + \cdots + b_j c_0$$

one of factor is divisible by p. In the sum

$$a_{r+s} = b_0 c_{r+s} + \cdots + b_{r-1} c_{s+1} + b_r c_s + b_{r+1} c_{s-1} + \cdots + b_{r+s} c_0$$

every summand other than $b_r c_s$ is divisible by p.

Now, it follows that:

10.A.18 Lemma of Gauss For polynomials G, $H \in \mathbb{Q}[X] \setminus \{0\}$ and their product $F = GH$, we have $F^* = G^* H^*$ and $I(F) = I(G) I(H)$.

Proof Since $F = GH = I(G) I(H) G^* H^*$ it is enough to show that $G^* H^* \in \mathbb{Z}[X]$ is equal to its primitive part. Since leading coefficients of G^* and H^* are positive, the leading coefficient of their product $G^* H^*$ is also positive. Further, the coefficients of G^* and H^* does not have a common prime factor and hence by 10.A.17 the coefficients

of $G^* H^*$ are also does not have such a common factor.

10.A.19 **Corollary** If the polynomial $F \in \mathbb{Z}[X] \backslash \{0\}$ has a decomposition $F = GH$ with non-constant polynomials $G, H \in \mathbb{Q}[X]$, then F has also such a decomposition in $\mathbb{Z}[X]$.

Proof By 10.A.18 $\quad F = I(F) F^* = I(F) G^* H^*$

10.A.20 **Corollary** Let $G, H \in \mathbb{Q}[X]$ be monic polynomials. If the product $F = GH$ belongs to $\mathbb{Z}[X]$, then already G and H belong to $\mathbb{Z}[X]$.

Proof We have $F = F^* = G^* H^*$ by 10.A.18 and since G^* and H^* are monic, it follows that $G^* = G$ and $H^* = H$.

Now, we can easily show that the polynomials $F := X^k - 2 \in \mathbb{Q}[X]$ are prime in $\mathbb{Q}[X]$ for all $k \in \mathbb{N}^*$. By 10.A.19 it is enough to show that: if $F = GH$ with polynomials $G = b_0 + \cdots + b_m X^m$, $H = c_0 + \cdots + c_n X^n \in \mathbb{Z}[X]$, then either G or H must be constant. Since $2 = b_0 c_0$, both b_0 and c_0 are not divisible by 2. Suppose that $2 | b_0$, but $2 \nmid c_0$ and $2 | b_0, \cdots, 2 | b_{r-1}$, but $2 \nmid b_r$. Then by 10.A.17 $2 \nmid a_r$, where $a_0, a_1, \cdots$ are the coefficients of $F = X^k - 2$. Therefore $r = k$ and so $\deg G \geq k$ and H is constant.

An obvious generalisation is the following result:

10.A.21 Lemma of Eisenstein Let

$F = a_0 + \cdots + a_k X^k \in \mathbb{Z}[X]$ and let P be a prime number such that $p | a_0, \ldots, p | a_{k-1}, p \nmid a_k, p^2 \nmid a_0$.

Then F is prime in $\mathbb{Q}[X]$.

With 10.A.21 we get plenty prime polynomials of arbitrary high degree in $\mathbb{Q}[X]$. For example, $X^n - p$, $X^n - pq$, $n \in \mathbb{N}^*$, p, q prime numbers, $p \neq q$ are prime in $\mathbb{Q}[X]$.

10.A.22 Example Let K be a finite field with q elements $c_1, \ldots, c_q$. The monic polynomials of degree 2 which are not prime in $K[X]$ are precisely the $\binom{q+1}{2}$ polynomials $(X - c_i)(X - c_j)$, $1 \leq i \leq j \leq q$. Since there are exactly q^2 monic polynomials of degree 2 in $K[X]$, there are precisely $q^2 - \binom{q+1}{2} = \binom{q}{2}$ monic prime polynomials of degree 2 in $K[X]$. In particular, K is not algebraically closed. The only prime polynomial of degree 2 over the field of 2 elements is $X^2 + X + 1$.

In a polynomial $F \in K[X]$, for the indeterminate we can substitute any element in K; more generally we can also substitute any element from an arbitrary K-algebra.

Let $F = a_0 + a_1 X + \cdots + a_n X^n \in K[X]$. For the element x in the K-algebra A, we get

$F(x) := a_0 + a_1 x + \cdots + a_n x^n$ (note that in $F(x)$ $a_0 = a_0 \cdot 1_A \in A$). For a fixed $x \in A$, the map

$$\varphi_x : K[X] \longrightarrow A, \quad F \longmapsto F(x)$$

is clearly a K-algebra homomorphism from $K[X]$ into A; this is called the __substitution homomorphism__ $X \longmapsto x$. Two essentially distinct cases occur:

(1) The substitution homomorphism φ_x is injective. This is the case if and only if the powers $x^n, n \in \mathbb{N}$, of x in A are linearly independent. In this case x is called __transcendental over A__.

(2) The substitution homomorphism φ_x is not injective; in this case x is called __algebraic over K__. The kernel of φ_x is a non-zero ideal in $K[X]$ and hence is of the form $K[X]\mu_x = \{F\mu_x \mid F \in K[X]\}$ with a uniquely determined monic polynomial $(0 \neq) \mu_x \in K[X]$. This follows from the following important theorem:

__10.A.23 Theorem__ Let $\mathfrak{a}$ be a non-zero ideal in the polynomial algebra $K[X]$, i.e. $\mathfrak{a} \subseteq K[X]$

is a non-zero subgroup such that for each $G \in \mathfrak{a}$ all multiples FG, $F \in K[X]$ also belong to $\mathfrak{a}$. Then there exists a unique monic polynomial $\mu \in \mathfrak{a}$ with $\mathfrak{a} = K[X]\mu$.

Proof Let $\mu \in \mathfrak{a}$ be a non-zero polynomial in $\mathfrak{a}$ of minimal degree. By multiplying the inverse of the leading coefficient of μ, we may assume that μ is monic. Since $\mu \in \mathfrak{a}$ we have $K[X]\mu \subseteq \mathfrak{a}$. Conversely, for $F \in \mathfrak{a}$, using division with remainder, F has a representation $F = Q\mu + R$ with $\deg R < \deg \mu$. Now, since $R = F - Q\mu \in \mathfrak{a}$, we must have $R = 0$ by the choice of μ, i.e. $F = Q\mu \in K[X]\mu$. – The uniqueness of μ is trivial.

The element μ in 10.A.23 is called a **genera-** **ting element** of the ideal $\mathfrak{a} = K[X]\mu$. We usually write (μ) for $K[X]\mu$.

10.A.24 Remark (Euclidean-domains) The proof of Theorem 10.A.23 is analogous to the corresponding theorem on the (identical with the subgroups of $\mathbb{Z}$) ideals of $\mathbb{Z}$.

To axiomatise this conclusion, we use the following notation: A commutative ring A is called an **integral domain** if $A \neq 0$ and if A is free-from zero-divisors, i.e. for all $a, b \in A$, from $ab = 0$, if follows that either $a = 0$ or $b = 0$.

An integral domain A is called Euclidean if there is a so-called Euclidean function $\varphi: A \setminus \{0\} \longrightarrow \mathbb{N}$ such that for all $a, b \in A$, $b \neq 0$, there exist $q, r \in A$ with $a = qb + r$, where either $r = 0$ or $\varphi(r) < \varphi(b)$. It makes possible a division with remainder in A with the remainder r is "smaller" than the divisor b in the case remainder is non-zero. However, the quotient and the remainder r need not be uniquely determined by a and b.

An ideal $Ab = \{rb \mid r \in A\} = (b)$ in a commutative ring A, generated by the element $b \in A$ is called a principal ideal. A is called a principal ideal ring if every ideal in A is a principal ideal and called a principal ideal domain (PID) if in addition A is an integral domain. With these definitions we have:

Every Euclidean domain A is a principal ideal domain

Proof If $\mathfrak{a}$ is a non-zero ideal in A, then every element $b \in \mathfrak{a}$, $b \neq 0$ whose value under the Euclidean function $\varphi(b)$ is minimal, generates $\mathfrak{a}$. For, if $a \in \mathfrak{a}$, then using division with remainder write $a = qb + r$, with either $r = 0$ or $\varphi(r) < \varphi(b)$. Since $r = a - qb \in \mathfrak{a}$, $r = 0$ by the minimality of $\varphi(b)$ and hence $a = qb \in Ab$.

As we have remarked in the begining, the ring $\mathbb{Z}$ of integers (with the absolute-value function as Euclidean function) and the polynomial ring $K[X]$ in one
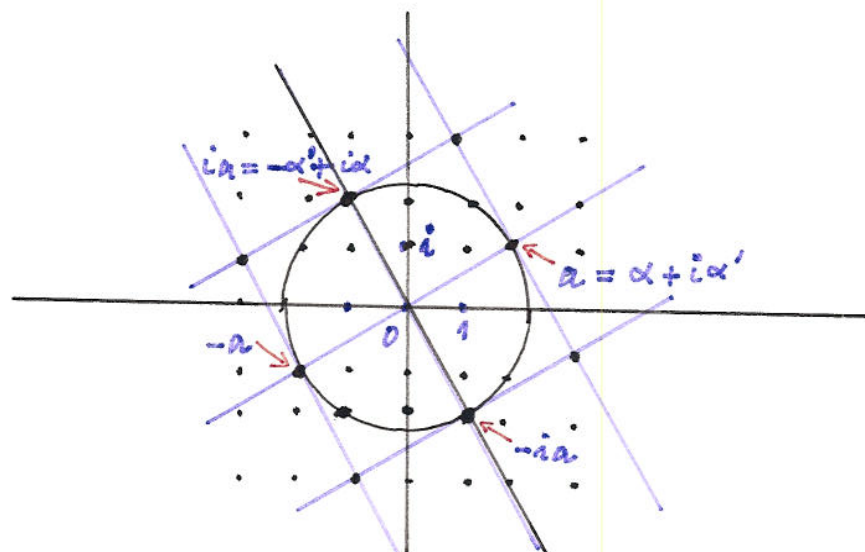
variable X over a field (with the degree as Euclidean function) are Euclidean domains and hence are principal ideal domains. Further an important example is the subring $\mathbb{Z}[i] := \{\alpha + i\alpha' \mid \alpha, \alpha' \in \mathbb{Z}\}$ of $\mathbb{C}$, called the ring of Gaussian integers. The ring $\mathbb{Z}[i]$ is an Euclidean domain with the square of an absolute-value as Euclidean function.

Proof Let $a = \alpha + i\alpha'$ and $b = \beta + i\beta' \neq 0$ in $\mathbb{Z}[i]$, $\alpha, \alpha', \beta, \beta' \in \mathbb{Z}$. Division in $\mathbb{C}$ (without remainder) gives $z = \gamma + i\gamma'$ with $\gamma, \gamma' \in \mathbb{R}$ and $a = zb$. For $\gamma, \gamma' \in \mathbb{R}$, there exist $c, c' \in \mathbb{Z}$ with $|\gamma - c| \leq \frac{1}{2}$ and $|\gamma' - c'| \leq \frac{1}{2}$. Then for $q := c + ic' \in \mathbb{Z}[i]$ and $r = a - qb \in \mathbb{Z}[i]$, we have $a = qb + r$ and $|r|^2 = |z - q|^2 |b|^2 = \left(|\gamma - c|^2 + |\gamma' - c'|^2\right)|b|^2 \leq \frac{1}{2}|b|^2 < |b|^2$.

Therefore in any case $\mathbb{Z}[i]$ is a principal ideal domain. The ideals in $\mathbb{Z}[i]$ are clearly precisely the subgroups $\mathfrak{a} \subseteq \mathbb{Z}^2 = \mathbb{Z} \oplus i\mathbb{Z}$ which are invariant under the multiplication by i, i.e. are invariant under the rotation of the complex-plane by the angle $\pi/2$ (and hence mapped onto itself). These non-zero subgroups are exactly the square-lattices as proved below:

$$\mathbb{Z}(\alpha + i\alpha') \oplus \mathbb{Z}i(\alpha + i\alpha') = \mathbb{Z}(\alpha + i\alpha') \oplus \mathbb{Z}(-\alpha' + i\alpha),$$
$$(\alpha, \alpha') \in \mathbb{Z}^2 \setminus \{(0,0)\}$$

An element $z \in \mathbb{Z}[i]$ is a unit in $\mathbb{Z}[i]$ if and
only if $z \cdot \bar{z} = 1$, i.e. if and only if z is one of the
fourth-root $1, i, -1, -i$ of unity. The four elements
$a := \alpha + i\alpha'$, ia, $-a$, $-ia$ are the generators of the
principal ideal $\mathfrak{a} = Aa = (a)$. Note that using
this observation and elementary geometry, it is easy
to prove that an arbitrary ideal $\mathfrak{a} \neq 0$ in $\mathbb{Z}[i]$ is
principal and hence $\mathbb{Z}[i]$ is a principal ideal domain.
Among the four generators of the ideal $0 \neq \mathfrak{a} \subseteq \mathbb{Z}[i]$,
as a rule we choose the element in the first) qua-
drant : $\mathrm{Re}\, z > 0$, $\mathrm{Im}\, z \geqslant 0$, as the natural represen-
tative.

In an arbitrary principal ideal domain (in particular,
in every Euclidean domain), there exists a unique
                                which exist
prime factorisation the analogous to the one in $\mathbb{Z}$,
resp. in the polynomial ring $K[X]$ over a field K, see
also Exercise 27.

10.A.25 __Definition__ Let x be an algebraic element of the K-algebra A and let $\varphi : K[X] \to A$ be the substitution homomorphism $X \xmapsto{x} x$. The uniquely determined monic polynomial $\mu_x \in K[X]$ with $\operatorname{Ker} \varphi_x = K[X]\mu_x$ is called the __minimal polynomial of x__ (over K) and its degree is called the __degree of x__ (over K). If $x \in A$ is transcendental over K, then the zero polynomial is (by definition) the minimal polynomial of the element x.

The image of the substitution homomorphism $\varphi_x : K[X] \to A$ is the smallest K-subalgebra $K[x]$ of A which contains x. The elements of $K[x]$ are also called __polynomials in x__; they are K-linear combinations of the powers x^ν, $\nu \in \mathbb{N}$. If x is transcendental (over K), then $K[x] \cong K[X]$ (as K-algebras). If $x \in A$ is algebraic over K, then by the isomorphism theorem $K[x] \cong K[X]/(\mu_x)$ and hence the degree of x, i.e. the degree of μ_x is the K-vector space dimension $\operatorname{Dim}_K K[x]$ of $K[x]$.

Therefore we have the following theorem:

10.A.26 __Theorem__ Let x be an algebraic element in the K-algebra A of degree $n \in \mathbb{N}$. Then $1, x, \ldots, x^{n-1}$ is a K-vector space basis of $K[x] \subseteq A$.

__Proof__ The powers $1, x, \ldots, x^{n-1}$ are linearly independent over K, since otherwise there will be a non-

zero polynomial in $\operatorname{Ker} \varphi_x$ of degree $< n$.
Conversely, if $F(x) \in K[x]$ and $F = Q\mu_x + R$
with $Q, R \in K[X]$, $\deg R < \deg \mu_x = n$, then
$F(x) = R(x)$ is a K-linear combination of $1, x, \cdots, x^{n-1}$.

10.A.27 Examples

(1) If the K-algebra A is finite
dimensional, then every element of A is algebraic
over K with a degree $\leq \operatorname{Dim}_K A$. For example, if
A is the endomorphism algebra of a finite dimen-
sional K-vector space or equivalently a matrix
algebra $M_n(K)$, then $\operatorname{Dim}_K A = n^2$.

(2) If $\mathfrak{a} = (\mu) \subseteq K[X]$ is a non-zero ideal
which is generated by the monic polynomial $\mu \in$
$K[X]$ of degree n, then $\mu = \mu_x$ is the minimal
polynomial of the residue class x of X in the
residue-class algebra $K[X]/\mathfrak{a} = K[x]$. In par-
ticular, $\operatorname{Dim}_K K[X]/(\mu) = n = \deg \mu$ and
$1, x, \cdots, x^{n-1}$ is a K-basis of this K-algebra.

(3) The minimal polynomial of $i = \sqrt{-1}$ in the $\mathbb{R}$-
algebra $\mathbb{C} = \mathbb{R}[i]$ is $X^2 + 1$ and hence $\mathbb{C}$ is iso-
morphic to the residue-class algebra $\mathbb{R}[X]/(X^2+1)$.

10.A.28 Example

Let x be an element of the
K-algebra A. Then the following theorem gives a
characterisation for the K-subalgebra $K[x] \subseteq A$
generated by x to be a field:

10.A.29 Theorem For an element x in a K-algebra A, the following statements are equivalent:

(1) The K-subalgebra $K[x]$ of A is a field.

(2) x is algebraic over K and the minimal polynomial μ_x of x over K is prime in $K[X]$.

Proof (1) $\Rightarrow$ (2): If x is not algebraic over K, then $K[x] \cong K[X]$ which is not a field, since x (and every non-constant polynomial in x) has no inverse in $K[x]$. Therefore, suppose that $\mu_x \neq 0$ is the minimal polynomial of x. If μ_x is not prime, then there is a representation $\mu_x = FG$ with polynomials $F, G \in K[X]$ of degrees smaller than the degree of μ_x. Then $0 = \mu_x(x) = F(x)G(x)$, but $F(x) \neq 0 \neq G(x)$.

(2) $\Rightarrow$ (1) Suppose that μ_x is prime in $K[X]$ and $F(x) \in K[x]$, $F(x) \neq 0$, $F \in K[X]$. Then F is not a multiple of μ_x and hence $\gcd(F, \mu_x) = 1$. By the Lemma 10.A.5 of Bezout there exist polynomials $S, T \in K[X]$ such that $SF + T\mu_x = 1$. Therefore $S(x)F(x) = 1$ and $S(x) \in K[x]$ is the inverse of $F(x)$ in $K[x]$.

For a (another) proof of 10.A.29, see also Exercise 28.

By 10.A.29 a residue-class algebra $L = K[X]/{}_{K[X]\mu}$ $= K[x]$, x is the residue-class of X, is a field if and only if μ is a prime polynomial in $K[X]$.

This allows us to construct field extensions L of K which have finite dimension over K. For example,

the field $\mathbb{C} \cong \mathbb{R}[X]/(X^2+1)$ is a 2-dimensional $\mathbb{R}$-algebra.

More generally, $K[X]/(X^2+1)$ is a field if and only if X^2+1 has no zero in K. For $K = \mathbb{K}_p = \mathbb{Z}/\mathbb{Z}_p$ this is exactly the case if and only if $p \equiv 3 \mod 4$.

Proof If $p \equiv 3 \mod 4$ and $x^2 = -1$ in $\mathbb{K}_p$, x is an element of order 4 in $\mathbb{K}_p^\times$. But $\# K_p^\times = p-1 \equiv 2 \mod 4$ and 4 does not divide $p-1$.
Conversely, suppose that $p \equiv 1 \mod 4$. Since $\mathbb{K}_p^\times$ is cyclic and $\# \mathbb{K}_p^\times = (p-1) \equiv 0 \pmod 4$, there is an element $x \in \mathbb{K}_p^\times$ of order 4. Then x^2 is an element of order 2, but -1 is the only element of order 2 in $\mathbb{K}_p^\times$ and hence $x^2 = -1$ (in fact, one can explicitly give the element $x := ((p-1)/2)!$.
By Wilson's theorem for this x, we have
$$x^2 = (p-1)! = -1 \text{ in } \mathbb{K}_p.$$

In general, for a polynomial $\mu \in K[X]$ of degree 2 or 3 which has no zero in K, the K-algebra $L := K[X]/(\mu)$ is a field extension of K of dimension 2 or 3. If $K = \mathbb{K}_2$ is a field with 2 elements, then $\mathbb{K}_2[X]/(X^2+X+1)$ is a field with 4 elements and $\mathbb{K}_2[X]/(X^3+X+1)$ is a field with 8 elements.

Note that in the field extension $L = K[X]/(\mu)$, $\mu \in K[X]$ prime, the residue-class x of X in L is

a zero of the polynomial $\mu \in K[X] \subseteq L[X]$.
Therefore in $L[X]$ we have $\mu = (X-x)\alpha$ with
a polynomial $\alpha \in L[X]$. One can iterate this
process to prove the following:

10.A.30 Theorem of Kronecker Let K be a field
and let $F \in K[X]$ be a non-zero polynomial.
Then there exists an overfield L of K such that
F splits into linear factors in $L[X]$. Further,
we can choose L such that L has a finite
dimension (as a K-algebra).

Proof We prove the assertion by induction on
$\deg F$. Suppose that $\deg F \geq 2$ and μ is a
prime factor of F. By the last remark there
exists a field extension L' of K with $\text{Dim}_K L' = \deg \mu$ such that μ and hence F has a zero x
in L'. Then $F = (X-x) G$ in $L'[X]$ and by ind-
uction hypothesis there exists a field extension L
of L' with $\text{Dim}_{L'} L < \infty$ such that G splits into
linear factors in $L[X]$. Then F also splits into linear
factors in $L[X]$. Further, since $\text{Dim}_K L = \text{Dim}_K L' \cdot \text{Dim}_{L'} L$,
we have $\text{Dim}_K L < \infty$. This completes the proof.

The proof of 10.A.30 shows that one can choose
L such that $\text{Dim}_K L \leq n!$, where $n = \deg F$.

From 10.A.30 it follows immediately that: for
every prime-power p^m, p prime, $m \in \mathbb{N}^*$, there
exists a field of cardinality p^m.

Proof If K is such a field, then the characteristic of K must be p and if the degree of K over its prime field $\mathbb{K}_p \cong \mathbb{Z}/\mathbb{Z}p$ is m. Since the multiplicative group $K^\times$ of K is cyclic of order $p^m - 1$, $x^{p^m - 1} = 1$ for every $x \in K^\times$ and so $x^{p^m} = x$ for all $x \in K$.

Now conversely $\overset{by\ 10.A30}{\text{Consider}}$ an over field L of $\mathbb{K}_p$ such that the polynomial $F := X^{p^m} - X$ splits into linear factors in $L[X]$. Let $K \subseteq L$ be the set of zeros of F (in L). Since $(x+y)^{p^m} = x^{p^m} + y^{p^m}$ for all $x, y \in L$, the subset K is a subfield of L. To show $\#K = p^m$, it is enough to show that the zeros of F are simple. This follows from the equality $F' = -1$ and $F'(a) = -1 \neq 0$ for all zeros a of F, see also Exercise 7)-c).

The field K of cardinality p^m is uniquely determined up to an isomorphism.

Proof Let $x \in K$ be a generator of the cyclic multiplicative group $K^\times$ and let $\mu_x \in \mathbb{K}_p[X]$ be the minimal polynomial of x over the prime field $\mathbb{K}_p \subseteq K$. Then $K = \mathbb{K}_p[x] \cong \mathbb{K}_p[X]/(\mu_x)$ and μ_x is a prime divisor of $X^{p^m - 1} - 1$, since $X^{p^m - 1} - 1 = \prod_{a \in K^\times} (X - a)$ in $K[X]$. If K' is another field of cardinality p^m, then $X^{p^m - 1} - 1$ also splits into linear factors in $K'[X]$, in particular, μ_x has a zero $x' \in K'$ and hence $\mathbb{K}_p[X]/(\mu_x) \cong \mathbb{K}_p[x'] \subseteq K'$; moreover, the equality must hold, since $\#\mathbb{K}_p[x'] = \#K' = p^m$.

Therefore $\overset{K=}{\mathbb{K}_p [x]} \cong \mathbb{K}_p[X] / {(\mu_x)} \cong \mathbb{K}_p[x'] = K'$.

The uniquely determined (upto isomorphism) field of cardinality p^m is denoted by $\mathbb{K}_{p^m}$; it is often also denoted by $GF(p^m)$ in the honour of E. Galois. GF is a short-form of $\underline{Galois-Feld}$.

The last proof shows that the monic prime divisors of the polynomial $X^{p^m} - X \in \mathbb{K}_p[X]$ are precisely the monic prime polynomials in $\mathbb{K}_p[X]$, of degree a divisor of m.

Clearly we can generalize this to a proof of the following more general result:

$\underline{If \;\; K = \mathbb{K}_q \; is \; a \; finite \; field \; of \; cardinality \; q, \; then}$ $\underline{the \; monic \; prime \; divisors \; of \; the \; polynomial}$ $\underline{X^q - X \; are \; precisely \; the \; monic \; prime \; polynomials}$ $\underline{in \; \mathbb{K}_q[X] \; whose \; degrees \; are \; divisors \; of \; m.}$

Rational function field (in one variable) over a field K.

Exactly like the construction of rational numbers as fractions of the integers, from the polynomial algebra $K[X]$ we construct a field of fractions

$$F/G, \quad F, G \in K[X], \quad G \neq 0.$$

Two such fractions F_1/G_1 and F_2/G_2 are equal[1] if and only if $F_1 G_2 = G_1 F_2$.

On the set of fractions the operations
$$\frac{F_1}{G_1} + \frac{F_2}{G_2} = \frac{F_1 G_2 + G_1 F_2}{G_1 G_2} \quad \text{and} \quad \frac{F_1}{G_1} \cdot \frac{F_2}{G_2} = \frac{F_1 F_2}{G_1 G_2}$$
of an addition and multiplication are well-defined. With respect to these binary operations the set of fractions form a field, which is called the rational function field (in one variable) over the field K and is denoted by $K(X)$.

In the K-algebra $K(X)$, the polynomial algebra $K[X]$ is a K-subalgebra as the set of fractions $F/1$, $F \in K[X]$. Further, from the canonical prime factorisation in $K[X]$, for every rational function

---

[1] More precisely, the fraction F/G is the equivalence class of the pairs (F, G) in the set of all pairs (R, S), $R, S \in K[X]$ $S \neq 0$ under the equivalence relation $(R_1, S_1) \sim (R_2, S_2)$ iff $R_1 S_2 = S_1 R_2$.

$R \in K(X)$, $R \neq 0$, we get a normalized repre-
sentation

$$R = a \prod_{P \in \mathcal{R}} P^{\alpha_P} \quad , \quad a \in K^{\times}, \quad \alpha_P \in \mathbb{Z},$$

with integral multiplicities α_P, $P \in \mathcal{R}$, which
are zero for almost all $P \in \mathcal{R}$. Therefore we
get the lowest fraction representation

$$R = F/G \quad , \quad F := a \prod_{\alpha_P \geq 0} P^{\alpha_P} \quad , \quad G := \prod_{\alpha_P < 0} P^{-\alpha_P}$$

($\mathcal{R}$ denote the set of monic prime polynomials
in $K[X]$.)

The division with remainder in $K[X]$ allows
to carry over the elementary divisor theorem
from $\mathbb{Z}$ to $K[X]$, where we replace the
absolute value on $\mathbb{Z}$ by the degree function
on $K[X]$. Therefore we have the following
important result:

10.A.31 **Elementary divisor theorem for
polynomial rings.** Let K be a field and let
$\mathcal{M}$ be a matrix with coefficients in $K[X]$, i.e.
$\mathcal{M} \in M_{m,n}(K[X])$, consider this as matrix in
$M_{m,n}(K(X))$ of rank r. Then there exist elemen-
tary matrices $\mathcal{L}_1, \ldots, \mathcal{L}_p \in GL_m(K[X])$ and
$\mathcal{L}_1, \ldots, \mathcal{L}_q \in GL_n(K[X])$ such that

$$\mathcal{L}_1 \cdots \mathcal{L}_p \; \mathcal{U} \; \mathcal{T}_1 \cdots \mathcal{T}_q$$

is a diagonal matrix $\mathcal{O} = \mathrm{Diag}(E_1, \cdots, E_r, 0, \cdots, 0)$ $\in M_{m,n}(K[X])$, where the non-zero polynomials $E_1, \cdots, E_r \in K[X]$ satisfy the divisibility conditions $E_1 \mid E_2 \mid \cdots \mid E_r$.

Note that $\mathcal{L} := \mathcal{L}_1 \cdots \mathcal{L}_p \in GL_m(K[X])$ and $\mathcal{T} := \mathcal{T}_1 \cdots \mathcal{T}_q \in GL_n(K[X])$, since $\mathcal{L}^{-1} = \mathcal{L}_p^{-1} \cdots \mathcal{L}_1^{-1}$ and $\mathcal{T}^{-1} = \mathcal{T}_q^{-1} \cdots \mathcal{T}_1^{-1}$ and the coefficients of these inverses are again in $K[X]$.

The polynomials $E_1, \cdots, E_r$ in the diagonal of $\mathcal{O} = \mathcal{L} \mathcal{U} \mathcal{T}$ are uniquely determined by the matrix $\mathcal{U}$ upto a factors in $K^\times$. For this we consider for an arbitrary matrix $M \in M_{m,n}(K[X])$ and for an arbitrary natural number $s \leq \mathrm{Min}(m,n)$, the ideal $\mathfrak{d}_s = \mathfrak{d}_s(M) \subseteq K[X]$ generated by s-minors of M. Then $\mathfrak{d}_s$ has greatest common divisor $D_s = D_s(M)$ of these minors is a generator[1] of the ideal $\mathfrak{d}_s$. $D_s(M)$ is called the s-th determinant divisor[2] of M.

---

[1] In $K[X]$ we have the equality for ideals
$$K[X]F + K[X]G = K[X]\gcd(F,G).$$

[2] We remark here that the ideals $\mathfrak{d}_s(M)$ and the determinant divisors are often numbered another way and then $\mathfrak{d}_{m-s}(M)$ is called the s-th determinantal ideal of M and the corresponding $D_{m-s}(M)$ is then s-th determinant divisor of M.

For the above diagonal matrix $\mathcal{D}$, obviously

$$\partial_s(\mathcal{D}) = (E_1 \cdots E_s), \quad \text{i.e.} \quad D_s(\mathcal{D}) = E_1 \cdots E_s$$

for all $s \leq r$ because of the divisibility conditions $E_1 | E_2 | \cdots | E_r$. Therefore it is enough to prove that

$$\partial_s(\mathcal{U}) = \partial_s(\mathcal{D}) \quad \text{for all} \quad s \leq \text{Min}(m, n).$$

Then $D_s(\mathcal{U}) = E_1 \cdots E_s$ and E_s (upto constant factor) is the quotient $D_s(\mathcal{U})/D_{s-1}(\mathcal{U})$ for all $s = 1, \cdots, r$. For the proof of equality $\partial_s(\mathcal{U}) = \partial_s(\mathcal{D})$, it is enough to show that the ideal ∂_s for a matrix M is same as if M is multiplied by left or right by an elementary matrix in $M_m(K[X])$ resp. $M_n(K[X])$, i.e. if to a row resp. column of M a multiple of another row resp. column is added. But this is trivial by the basic computation rules for determinants. Altogether we have the following:

10.A.32 Theorem
The assumptions and notations as in the Theorem 10.A.31. Then for $s \leq r$ the product $E_1 \cdots E_s$ (upto a constant factor) is the s-th determinant divisor $D_s = D_s(\mathcal{U})$ of the matrix $\mathcal{U}$ and hence is equal to the greatest common divisor of the s-minors of $\mathcal{U}$.

The polynomials $E_1, \cdots, E_r, E_{r+1} = E_{r+2} = \cdots = 0$ in 10.A.31 resp. 10.A.32 are called the elementary divisors[1] of $\mathcal{U}$.

[1] Often E_{m-s+1} is known as the s-th elementary divisor, $s = 1, \cdots, m$ and further put $E_s = 1$ for $s > m$. Cf. Footnote 2

10.A.33 Example Let $\alpha \in M_{m,n}(K[X])$.
We shall also denote by α, the K-linear map
defined by α, $K[X]^n \xrightarrow{\quad} K[X]^m$, $\underline{f} \mapsto \alpha\underline{f}$.
Then for the matrices $\Sigma = \Sigma_1 \cdots \Sigma_p$, $\tau = \tau_1 \cdots \tau_q$
and the diagonal matrix Δ as in 10.A.31,
we have $\Sigma \cdot \alpha = \Delta \bar{\tau}^{-1}$, i.e. the diagram

$$
\begin{array}{ccc}
K[X]^n & \xrightarrow{\ \alpha\ } & K[X]^m \\[4pt]
{\scriptstyle \bar{\tau}^{-1}}\downarrow{\scriptstyle\approx} & & \approx\downarrow{\scriptstyle \Sigma} \\[4pt]
K[X]^n & \xrightarrow{\ \Delta\ } & K[X]^m
\end{array}
$$

Since Σ and $\bar{\tau}^{-1}$ are isomorphisms, the coker-
nals Coker α and Coker Δ are also isomorphic.
Clearly,

$$
\text{Coker }\Delta \cong \frac{K[X]}{(E_1)} \oplus \cdots \oplus \frac{K[X]}{(E_r)} \oplus K[X]^{m-r}.
$$

Now, since $\operatorname{Dim}_K \dfrac{K[X]}{(E_s)} = \deg E_s$, $s = 1, \cdots, r$,

We have the following :

10.A.34 Theorem Let $\alpha \in M_{m,n}(K[X])$. Then
the Cokernal of the map $\alpha : K[X]^n \longrightarrow K[X]^n$
is a finite dimensional K-vector space if and
only if Rank $\alpha = m$. Moreover, in this case
the dimension of this cokernal is equal to the
degree of the m-th determinant divisor $D_m(\alpha)$ of
α and hence is equal to the degree of the great-
est common divisor of the m-minors of α.
— In particular, for an $n \times n$ matrix $\alpha \in M_n(K[X])$,