§ 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 their 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 $\underbrace{(t-c_1)\cdots(t-c_n)}_{= a_0 + a_1 t + \cdots + a_{n-1} t^{n-1} + t^n}$ 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 $a_i = 0$ for $i > n$) uniquely by definition. 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.

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

The multiplication two polynomials

$$PQ := \sum_{i\in\mathbb{N}} c_i X^i \quad \text{with} \quad c_i := \sum_{j=0}^{i} a_j b_{i-j} = a_0b_i + \cdots + a_ib_0$$

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 constant polynomials. 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 degree of P and a_n is called the leading coefficient of P. If the leading coefficient of a polynomial P is 1, then P is called monic. The degree of the zero polynomial is by definition $-\infty$. The polynomials of degree 0 are precisely non-zero constant polynomials. The degree of a polynomial P is denoted by $\deg P$.
The n-dimensional K-subspace of the polynomials in $K[X]$ of degrees $< n$ is denoted by $K[X]_n$; $1, X, \cdots, X^{n-1}$ is a K-basis of $K[X]_n$.

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

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

Proof 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 $i > \operatorname{Max}(m,n)$ and hence $\deg(P+Q) \leq \operatorname{Max}(m,n)$. 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

$$F := 3X^4 + \tfrac{3}{2}X^3 + \tfrac{7}{2}X^2 + 2X + 2, \quad G := 2X^2 + X + 1 \in \mathbb{Q}[X]$$

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

$$(3X^4 + \tfrac{3}{2}X^3 + \tfrac{7}{2}X^2 + 2X + 2) : (2X^2 + X + 1) = \tfrac{3}{2}X^2 + 1$$

$$-(3X^4 + \tfrac{3}{2}X^3 + \tfrac{3}{2}X^2)$$

$$2X^2 + 2X + 2$$

$$-\ 2X^2 + X + 1$$

$$X + 1$$

$Q := \tfrac{3}{2}X^2 + 1$ quotient

$R = X + 1$ remainder.

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

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 $\gcd(R_k, R_{k+1}) = R_{k+1}$.

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:

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

$$S_{i+1} = S_{i-1} - Q_i S_i,\ T_{i+1} = T_{i-1} - Q_i T_i,\ i=1,\cdots,k.$$

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

10.A.5 Lemma of Bezout For $F, G \in K[X]$, there exist polynomials $S, T \in K[X]$ such that $\gcd(F,G) = SF + TG$. In particular, if F and G are relatively prime polynomials in $K[X]$, then there exist polynomials $S, T \in K[X]$ such that $1 = SF + TG$.

10.A.6 Example For $F := X^4 - X^3 - 3X^2 - X + 4$ and $G := X^3 + X^2 + X - 3$ in $\mathbb{Q}[X]$, we have

$$X^4 - X^3 - 3X^2 - X + 4 = (X-2)(X^3 + X^2 + X - 3) + (-2X^2 + 4X - 2)$$

$$X^3 + X^2 + X - 3 = \left(-\frac{1}{2}X - \frac{3}{2}\right)(-2X^2 + 4X - 2) + (6X - 6)$$

$$-2X^2 + 4X - 2 = \left(-\frac{1}{3}X + \frac{1}{3}\right)(6X - 6).$$

Therefore $\gcd(F,G) = X - 1$.

Further, the polynomials S_i, T_i, $i = 0, \cdots, 3$ are given in the following table:

i	0	1	2	3
Q_i		$X-2$	$-\frac{1}{2}X - \frac{3}{2}$	
S_i	1	0	1	$\frac{1}{2}X + \frac{3}{2}$
T_i	0	1	$-X+2$	$-\frac{1}{2}X^2 - \frac{1}{2}X + 4$

Therefore $\gcd(F,G) = X - 1 = \frac{1}{6}(6X - 6)$

$$= \left(\frac{1}{12}X + \frac{1}{4}\right)F + \left(-\frac{1}{12}X^2 - \frac{1}{12}X + \frac{2}{3}\right)G$$

$R_0 = F, \quad R_1 = G$

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

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

$R_{k-1} = Q_k R_k + R_{k+1} \quad 0 \le \deg R_{k+1} < \deg R_k$

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

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

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

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

$R_{k+2} = 0$

$\mathfrak{Q}_i$

$\mathfrak{Q}_i^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -Q_i \end{pmatrix}$

$\mathfrak{Q}_{k+1} \cdots \mathfrak{Q}_1 \begin{pmatrix} R_1 \\ R_2 \end{pmatrix}$

$=: \mathfrak{Q}$

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

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

$= \begin{pmatrix} S_i \\ S_{i+1} \end{pmatrix}$

$= \begin{pmatrix} S R_0 + T R_1 \\ U R_0 + V R_1 \end{pmatrix}$

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 $\deg F \geq 1$ 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 existence 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 uniqueness, 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 $a_i \in K^*$, $i = 1, \cdots, r$. Clearly $r \geq 1$. 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 $Q_1, \cdots, Q_s$, say Q_1. Now since Q_1 is prime, necessarily $Q_1 = a_1 P_1$ with $a_1 \in K^\times$. 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 same prime factors we obtain prime polynomial powers to get the <u>canonical prime factorisation</u>:

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

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

The element a is necessarily the leading coefficient of F. The exponent α_P is called the <u>multiplicity</u> of $P \in \mathfrak{P}$ in F.

In the monic prime polynomials $P \in \mathfrak{P}$, there are in particular, the <u>linear factors</u> $X - c$, $c \in K$

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
$(F+G)(t) = F(t) + G(t)$, $(FG)(t) = F(t)G(t)$ 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

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

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 multiplicity 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 $n \geq 0$ 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

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

Proof The polynomial $F - G$ has degree $\leq n$ and $t_1, \dots, t_{n+1}$ 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 not 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 not 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 $\mathbb{Q}[X]$, 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 $\mathbb{Q}$, it is very troublesome to decide whether it is prime or not. The polynomials X^2-2 and X^3-2 are prime in $\mathbb{Q}[X]$. It is less trivial to prove that the polynomial X^k-2 for $k>3$ is also prime in $\mathbb{Q}[X]$. In the following we will present some elementary results which will help to solve the above problem.

For polynomial $F \in \mathbb{Q}[X]$, $F \neq 0$, we recommend 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 $\mathbb{Q}[X]$ 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 $I(F) \in \mathbb{Q}^*$ 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 $p \mid b_0, \cdots, p \mid b_{r-1}, p \nmid b_r$; $p \mid c_0, \cdots, p \mid c_{s-1}$, $p \nmid c_s$. 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 $F \in \mathbb{Z}[X] \setminus \{0\}$ 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 $F = I(F)\, F^* = I(F)\, G^* H^*$

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 $2 \mid b_0$, but $2 \nmid c_0$ and $2 \mid b_0, \dots, 2 \mid b_{r-1}$, but $2 \nmid b_r$. Then by 10.A.17 $2 \nmid a_r$, where $a_0, a_1, \dots$ 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 $p \mid a_0, \cdots, p \mid a_{k-1}$, $p \nmid a_k$, $p^2 \nmid a_0$. 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 $c_1, \cdots, c_q$. 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 generating 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 $ab = 0$, it 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 $a = qb \in Ab$.

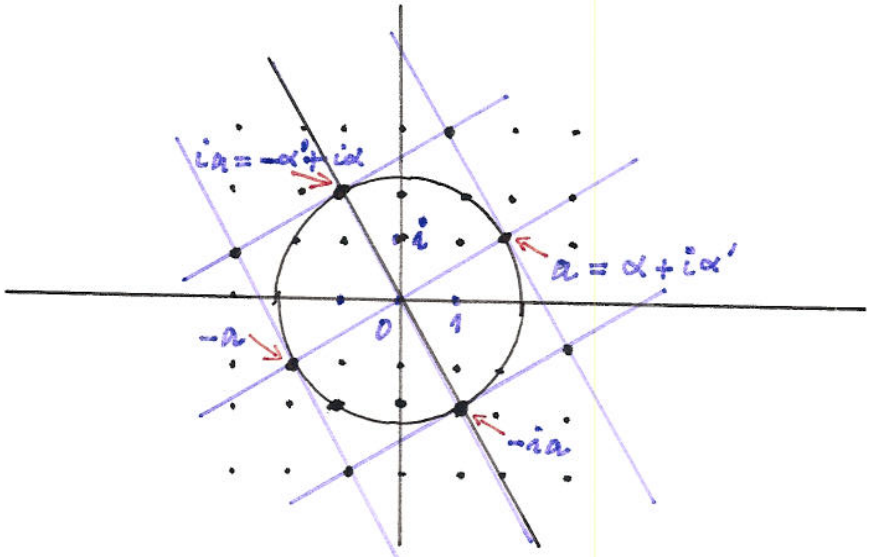
As we have remarked in the beginning, the ring $\mathbb{Z}$ of integers (with the absolute-value function as Euclidean function) and the polynomial ring $K[X]$ in one

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:

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



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) quadrant: $\mathrm{Re}\, z > 0$, $\mathrm{Im}\, z \geq 0$, as the natural representative.

In an arbitrary principal ideal domain (in particular, in every Euclidean domain), there exists a unique prime factorisation which exists 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 $X \overset{x}{\longmapsto} x$. 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 $\varphi_x : K[X] \longrightarrow A$ 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 $\underset{K}{\operatorname{Dim}}\, K[x]$ 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 $1, x, \dots, x^{n-1}$ is a K-vector space basis of $K[x] \subseteq A$.*

Proof The powers $1, x, \dots, x^{n-1}$ 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 $1, x, \dots, x^{n-1}$.

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 dimensional 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 particular, $\operatorname{Dim}_K K[X]/(\mu) = n = \deg \mu$ and $1, x, \dots, x^{n-1}$ 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 isomorphic 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 $p \equiv 3 \bmod 4$.

Proof If $p \equiv 3 \bmod 4$ and $x^2 = -1$ in $\mathbb{K}_p$, then x is an element of order 4 in $\mathbb{K}_p^\times$. But $\#\mathbb{K}_p^\times = p-1 \equiv 2 \bmod 4$ and 4 does not divide $p-1$.
Conversely, suppose that $p \equiv 1 \bmod 4$. 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 $x := \left(\frac{p-1}{2}\right)!$. By Wilson's theorem for this x, we have $x^2 = (p-1)! = -1$ 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 $\operatorname{Dim}_K L' = \deg \mu$ such that μ and hence F has a zero x in L'. Then $F = (X-x)G$ in $L'[X]$ and by induction hypothesis there exists a field extension L of L' with $\operatorname{Dim}_{L'} L < \infty$ such that G splits into linear factors in $L[X]$. Then F also splits into linear factors in $L[X]$. Further, since $\operatorname{Dim}_K L = \operatorname{Dim}_K L' \cdot \operatorname{Dim}_{L'} L$, we have $\operatorname{Dim}_K L < \infty$. This completes the proof.

The proof of 10.A.30 shows that one can choose L such that $\operatorname{Dim}_K L \leq n!$, 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 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 $x \in K$.

Nor conversely (by 10.A30) 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 upto 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 $K = \mathbb{K}_p[x] \cong \mathbb{K}_p[X]/(p_x) \cong \mathbb{K}_p[x'] = K'$.

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 Galois-Field.

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:
If $K = \mathbb{K}_q$ is a finite field of cardinality q, then the monic prime divisors of the polynomial $X^q - X$ are precisely the monic prime polynomials 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

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

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

$$F_1/G_1 + F_2/G_2 = \frac{F_1 G_2 + G_1 F_2}{G_1 G_2} \quad \text{and} \quad F_1/G_1 \cdot F_2/G_2 = \frac{F_1 F_2}{G_1 G_2}$$

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 representation

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

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

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

($\mathfrak{R}$ 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 A be a matrix with coefficients in $K[X]$, i.e. $A \in M_{m,n}(K[X])$, consider this as matrix in $M_{m,n}(K(X))$ of rank r. Then there exist elementary matrices $S_1, \ldots, S_p \in GL_m(K[X])$ and $T_1, \ldots, T_q \in GL_n(K[X])$ such that

$\mathcal{L}_1 \dots \mathcal{L}_p$ or $\tau_1 \cdots \tau_q$ is a diagonal matrix $\mathcal{D} = \mathrm{Diag}(E_1, \dots, E_r, 0, \dots, 0) \in M_{m,n}(K[X])$, where the non-zero polynomials $E_1, \dots, E_r \in K[X]$ satisfy the divisibility conditions $E_1 | E_2 | \dots | E_r$.

Note that $\mathcal{L} := \mathcal{L}_1 \dots \mathcal{L}_p \in GL_m(K[X])$ and $\tau := \tau_1 \cdots \tau_q \in GL_n(K[X])$, since $\mathcal{L}^{-1} = \mathcal{L}_p^{-1} \dots \mathcal{L}_1^{-1}$ and $\tau^{-1} = \tau_q^{-1} \cdots \tau_1^{-1}$ and the coefficients of these inverses are again in $K[X]$.

The polynomials $E_1, \dots, E_r$ in the diagonal of $\mathcal{D} = \mathcal{L} M \tau$ are uniquely determined by the matrix M 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

$$\mathfrak{d}_s(\mathcal{D}) = (E_1 \cdots E_s), \text{ i.e. } D_s(\mathcal{D}) = E_1 \cdots E_s$$

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

$$\mathfrak{d}_s(\mathcal{A}) = \mathfrak{d}_s(\mathcal{D}) \text{ for all } s \leq \operatorname{Min}(m,n).$$

Then $D_s(\mathcal{A}) = E_1 \cdots E_s$ and E_s (upto constant factor) is the quotient $D_s(\mathcal{A}) / D_{s-1}(\mathcal{A})$ for all $s = 1, \cdots, r$. For the proof of equality $\mathfrak{d}_s(\mathcal{A}) = \mathfrak{d}_s(\mathcal{D})$, it is enough to show that the ideal $\mathfrak{d}_s$ 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 $D_s = D_s(\mathcal{A})$ of the matrix $\mathcal{A}$ and hence is equal to the greatest common divisor of the s-minors of $\mathcal{A}$.*

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 $\mathcal{A}$.

[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 $\mathfrak{A} \in M_{m,n}(K[X])$. We shall also denote by $\mathfrak{A}$ the K-linear map defined by $\mathfrak{A}$, $K[X]^n \longrightarrow K[X]^m$, $\underline{f} \mapsto \mathfrak{A}\underline{f}$. Then for the matrices $\mathfrak{L} = \mathfrak{L}_1 \cdots \mathfrak{L}_p$, $\mathfrak{T} = \mathfrak{T}_1 \cdots \mathfrak{T}_q$ and the diagonal matrix $\mathfrak{D}$ as in 10.A.31, we have $\mathfrak{L}.\mathfrak{A} = \mathfrak{D}\mathfrak{T}^{-1}$, i.e. the diagram

$$\begin{array}{ccc} K[X]^n & \xrightarrow{\mathfrak{A}} & K[X]^m \\ \mathfrak{T}^{-1}\downarrow\wr & & \wr\downarrow\mathfrak{L} \\ K[X]^n & \xrightarrow{\mathfrak{D}} & K[X]^m \end{array}$$

Since $\mathfrak{L}$ and $\mathfrak{T}^{-1}$ are isomorphisms, the cokernals $\operatorname{Coker}\mathfrak{A}$ and $\operatorname{Coker}\mathfrak{D}$ are also isomorphic. Clearly,

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

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

We have the following:

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

the cokernal of the map $\mathcal{A}: K[X]^n \longrightarrow K[X]^n$ is finite dimensional over K if and only if $\operatorname{Det}\mathcal{A} \neq 0$. Moreover, in this case

$$\dim_K \operatorname{Coker}\mathcal{A} = \deg(\operatorname{Det}\mathcal{A}).$$

10.A.35 Remark An analogous theorem to 10.A.32 is self-evident also for integral-matrices. Therefore:

10.A.36 Theorem Let $\mathcal{A} \in M_{m,n}(\mathbb{Z})$ be an integral matrix of rank r and $\mathcal{S}_1, \dots, \mathcal{S}_p \in GL_m(\mathbb{Z})$ and $\mathcal{T}_1, \dots, \mathcal{T}_q \in GL_n(\mathbb{Z})$ be elementary matrices as in 8.C.11. If $\mathcal{S}_1 \cdots \mathcal{S}_p \mathcal{A} \mathcal{T}_1 \cdots \mathcal{T}_q$ is a diagonal matrix $\mathcal{D} = \operatorname{Diag}(e_1, \dots, e_r, 0, \dots, 0) \in M_{m,n}(\mathbb{Z})$, then $d_s = e_1 \cdots e_s$ for all $s \leq r$ (up to the sign) is the greatest common divisor $d_s(\mathcal{A})$ of the s-minors of $\mathcal{A}$.

The analog of 10.A.34 is:

10.A.37 Theorem Let $\mathcal{A} \in M_{m,n}(\mathbb{Z})$. Then the cokernal of the group homomorphism $\mathcal{A}: \mathbb{Z}^n \longrightarrow \mathbb{Z}^m$ is finite if and only if $\operatorname{rank}\mathcal{A} = m$. Moreover, in this case the order of this cokernal is equal to the greatest common divisor $d_m(\mathcal{A})$ of the m-minors of $\mathcal{A}$. – In particular, for an $n \times n$ matrix $\mathcal{A} \in M_n(\mathbb{Z})$ the cokernal of the endomorphism $\mathcal{A}: \mathbb{Z}^n \longrightarrow \mathbb{Z}^n$ is finite if and only if $\operatorname{Det}\mathcal{A} \neq 0$. Moreover, in this case

$$|\operatorname{Coker}\mathcal{A}| = |\operatorname{Det}\mathcal{A}|.$$

10.A EXERCISES

(Polynomials in One variable)

In the following exercises K denote a field.

1 Let K be a field of $\operatorname{char} K \neq 2$. A polynomial $F = X^2 + pX + q$ is irreducible in $K[X]$ if and only if $p^2 - 4q$ is not a square in K.

2 For the following polynomials find the monic prime-factorisation in $\mathbb{Q}[X]$, $\mathbb{R}[X]$ and $\mathbb{C}[X]$.

a) $X^4 - 5$ b) $X^4 + 5$ c) $X^4 + 4$ d) $X^4 + X^2 + 1$

e) $X^3 - 2X^2 + 2X - 1$ f) $X^5 + 2X^4 + 2X^3 + 4X^2 + X + 1$

(The decomposition $(X^4 + 4) = (X^2 + 2X + 2)(X^2 - 2X + 2)$ is a good observation!)

3 Let F and G be non-zero polynomials in $K[X]$ with the monic prime-decomposition

$$F = a \prod_{P \in \mathcal{P}} P^{\alpha_P} \quad , \quad G = b \prod_{P \in \mathcal{P}} P^{\beta_P}$$

a) $$\operatorname{GCD}(F, G) = \prod_{P \in \mathcal{P}} P^{\operatorname{Min}(\alpha_P, \beta_P)}$$

b) Define the least common multiple $\operatorname{LCM}(F, G)$ and prove the formula

$$\operatorname{LCM}(F, G) = \prod_{P \in \mathcal{P}} P^{\operatorname{Max}(\alpha_P, \beta_P)}$$

c) Show that $LCM(F,G) \cdot GCD(F,G) = FG$. (Up to a factor $c \in K^*$)

d) In $K[X]$ prove the following equalities of ideals:
$K[X] \cdot F + K[X] \cdot G = K[X]\, GCD(F,G)$ and
$K[X] \cdot F \cap K[X] \cdot G = K[X] \cdot LCM(F,G)$.

4. Let K be a subfield of the field L and let $F, G \in K[X]$.

a) F divides G in $K[X]$ if and only if F divides G in $L[X]$.

b) $GCD_{K[X]}(F,G) = GCD_{L[X]}(F,G)$.

5. Let K be a field. Show that there are infinitely many monic prime-polynomials in $K[X]$. (Only in the case of a finite field K the assertion is non-trivial)

6. (Formal Differentiation) Let K be a field. For a polynomial $F = \sum_{\nu \in \mathbb{N}} a_\nu X^\nu \in K[X]$, the derivative of F is defined by $F' := \sum_{\nu \in \mathbb{N}} \nu a_\nu X^{\nu-1} \in K[X]$.

a) The map $K[X] \longrightarrow K[X]$, $F \longmapsto F'$ is K-linear

b) Product-rule: $(FG)' = F'G + FG'$ for all $F, G \in K[X]$

c) Let $a \in K$. Then a is a multiple zero of F if and only if $F(a) = F'(a) = 0$.

d) On the rational function field $K(X)$ the quotient rule

$$\left(\frac{F}{G}\right)' = \frac{GF' - G'F}{G^2}, \quad F, G \in K[X], \ G \neq 0$$

defines a well-defined map $K(X) \longrightarrow K(X)$ which is K-linear and satisfies the product-rule

7. Let $F \in K[X]$ be a non-zero polynomial.

a) The following statements are equivalent:

(i) $GCD(F, F') = 1$.

(ii) All prime factors P of F are simple and $P' \neq 0$ (see Exercise 6 -- If F fullfill these conditions, then F is called separable)

b) Suppose that F splits into linear factors in $K[X]$. Then all zeros of F are simple if and only if F and F' are relatively prime. Further, if $\operatorname{char} K = 0$, then the quotient $F/GCD(F, F')$ have the same zeros as F, but all of them are simple. (This is an algorithmic process to construct a polynomial with the same zeros as F all simple without knowing the zeros of F)

8. Let $K = \mathbb{K}_q$ be a field with q elements. Then there are exactly $2\binom{q+1}{3}$ monic prime polynomials of degree 3 over K (see Example 10.A.22 Let $s_q(m)$ denote the number of monic prime-

polynomials of degree m in $K[X]$. Then by the remark at the end of Example 10.A.8, we have the equation $q^m = \sum_{d|m} s_q(d)\cdot d$. Now use Möbius inversion formula to deduce the Gauss-formula:

$$s_q(m) = \frac{1}{m}\sum_{d|m} \mu\left(\frac{m}{d}\right)\cdot q^d \quad \text{and in particular,}$$

$$s_q(p) = q\left(q^{p-1}-1\right)/p \quad \text{for an arbitrary prime number } p.$$

9. (Partial fractions decomposition) Let $F/G \in K(X)$ be a rational function over K with $\deg F < \deg G$. Suppose that the denominator polynomial G is monic and have the prime-decomposition $G = P_1^{n_1}\cdots P_r^{n_r}$ with pairwise distinct monic prime polynomials $P_1,\cdots,P_r$. Then there exists a representation

$$\frac{F}{G} = \frac{A_{11}}{P_1} + \cdots + \frac{A_{1n_1}}{P_1^{n_1}} + \cdots + \frac{A_{r1}}{P_r} + \cdots + \frac{A_{rn_r}}{P_r^{n_r}}$$

with uniquely determined polynomials $A_{ij}\in K[X]$ and $\deg A_{ij} < \deg P_i$ for all $1\le j\le n_i$, $1\le i\le r$

(Remark The result of this Exercise says that the rational functions

$$X^\nu,\ \nu\in\mathbb{N};\quad \frac{X^\mu}{P^n},\ (\mu,P,n)\in \mathbb{N}\times\mathcal{P}\times\mathbb{N}^*,\ \mu<\deg P$$

together form a K-basis of $K(X)$, where $\mathcal{P}$ denote the set of monic prime polynomials in $K[X]$. In particular, $\dim_K K(X) > \aleph_0$ if $\#K > \aleph_0$, while $\dim_K K[X] = \aleph_0 = \#\mathbb{N}$.)

10. a) (Chinese-remainder theorem) Let $\mu_1, \dots, \mu_r$ be monic and pairwise relatively prime polynomials in $K[X]$, i.e. $GCD(\mu_i, \mu_j) = 1$ for all $i \neq j$. Let $\mu = \mu_1 \cdots \mu_r$. Then the canonical K-algebrahomomorphism

$$K[X]/(\mu) \xrightarrow{\varphi} K[X]/(\mu_1) \times \cdots \times K[X]/(\mu_r)$$

is an isomorphism. (The surjectivity can also be deduced from injectivity by using dimension-argument.)

b) (Hermite-Interpolation) Let $a_1, \dots, a_r$ be distinct elements in a field K and $n_1, \dots, n_r \in \mathbb{N}^*$. For arbitrary given elements $c_1^{(0)}, \dots, c_1^{(n_1-1)}, \dots, c_r^{(0)}, \dots, c_r^{(n_r-1)}$ in K, there exists unique polynomial $f \in K[X]$ of degree $< n_1 + \cdots + n_r$ with the Taylor-expansion at a_s is

$$f = c_s^{(0)} + c_s^{(1)}(X-a_s) + \cdots + c_s^{(n_s-1)}(X-a_s)^{n_s-1} + \dots$$

for all $s = 1, \dots, r$. (Hint Apply part a) to $\mu_s := (X-a_s)^{n_s}$, $s = 1, \dots, r$. For the concept of the Taylors-expansion over an arbitrary field see Exercise 14)

11. Let K be a field and let A be a non-zero K-algebra. Further, let $x \in A$ and let $M \subseteq K[X]$ be the set of all polynomials $G \in K[X]$ with $G(x) \in A^\times$.

Then $K[X]_M := \{F/G \mid F \in K[X],\ G \in M\}$ is a K-subalgebra of $K(X)$ and the map

$$F/G \longmapsto F(x)/G(x) := F(x)G(x)^{-1} = G(x)^{-1}F(x),$$

($F \in K[X],\ G \in M$,)

is a well-defined K-algebra homomorphism from $K[X]_M \longrightarrow A$. (Therefore one can substitute x not only in a polynomial, but also in such a rational function (in $K[X]_M$) for which the denominator is a unit in A at the place x.) If x is algebraic over K with minimal polynomial μ_x, then M is the set of all polynomials in $K[X]$ which are relatively prime to μ_x. (If $G \in K[X]$ is relatively prime to μ_x and $SG + T\mu_x = 1$, $S, T \in K[X]$, then $S(x) \cdot G(x) = 1 = G(x) \cdot S(x)$. If H is a common divisor of positive degree of G and μ_x and if $F := \mu_x/H$, then $G(x)F(x) = 0$, but $F(x) \neq 0$.)

12. Let F and G be non-zero polynomials over the field K. Then $\deg F(G) = \deg F \cdot \deg G$.

13. Let K be a field and let A be a K-algebra. Every K-algebra homomorphism $K[X] \longrightarrow A$ is a substitution homomorphism $X \longmapsto x \in A$.

14 Let K be a field. The K-algebra automorphisms are precisely the substitution homomorphisms $X \longmapsto bX - a$, $a, b \in K$, $b \neq 0$. Some consequences of this are:

(1) The group $\mathrm{Aut}_{K\text{-alg}}\, K[X]$ of the K-algebra automorphisms of $K[X]$ is isomorphic to the affine group[1] $A_1(K) = K \rtimes K^\times$.

(2) For $a \in K$, the substitution homomorphism $X \longmapsto X - a$ is an automorphism of $K[X]$ and hence $(X-a)^\nu$, $\nu \in \mathbb{N}$, is a K-basis of $K[X]$. (The representation $F = \sum_{\nu \in \mathbb{N}} c_\nu (X-a)^\nu$ of a polynomial $F \in K[X]$ in this basis is called the Taylor-expansion of F at a.)

15. Every rational function $R \in K(X)$, $R \notin K$, is transcendental over K.

16. Let K be a field and let A be a K-algebra. Suppose that the element $x \in A$ is algebraic over K of degree n with the minimal polynomial $\mu_x = X^n + a_{n-1}X^{n-1} + \cdots + a_1 X + a_0$.

a) x is a unit in A if and only if the constant term a_0 of μ_x is non-zero; moreover, in this case $x^{-1} = \frac{1}{a_0}\left(x^{n-1} + a_{n-1}x^{n-2} + \cdots + a_1\right)$.

---

[1] The automorphism group $\mathrm{Aut}_K K^n$ acts naturally on K^n (the additive group) and the semi-direct product $K^n \rtimes \mathrm{Aut}_K K^n$ is called the affine group of K^n; usually denoted by $A_n(K)$.

b) If x is a unit in A, then the minimal polynomial $\mu_{x^{-1}}$ of x^{-1} is:

$$\mu_{x^{-1}} = \frac{1}{a_0} X^n \mu_x\left(\frac{1}{X}\right) = X^n + \frac{a_1}{a_0} X^{n-1} + \cdots + \frac{a_{n-1}}{a_0} X + \frac{1}{a_0}.$$

c) For $a \in K$, the minimal polynomial of $x+a$ is $\mu_x(X-a)$, i.e. $\mu_{x+a} = \mu_x(X-a)$.

17. Let K be a field and let A be a K-algebra.

a) If $x \in A$ is algebraic over K of degree n, then every element $y \in K[x]$ is algebraic over K of degree $\leq n$. Moreover, y is of degree n if and only if $K[y] = K[x]$.

b) Let $x \in A$ be nilpotent. Then x is algebraic over K and the degree of x is equal to the nilpotent-degree of x. What is the degree of $(a+x)^m$ for $a \in K$ and $m \in \mathbb{N}^*$? (Hint Treat the cases $a=0$ and $a \neq 0$ separately and consider them. In particular also if $\operatorname{char} K = 0$, then always $m = m \cdot 1_K \neq 0$ in these cases.)

18. Compute the minimal polynomial of a complex number $a+bi$, $a, b \in \mathbb{R}$, over $\mathbb{R}$. For every quadratic prime polynomial $\mu \in \mathbb{R}[X]$ we have $\mathbb{R}[X]/(\mu) \cong \mathbb{C}$ (as $\mathbb{R}$-algebras).

19. Let x and y be commuting algebraic elements in a K-algebra A of degrees m and n, respectively.

Then $x \pm y$ and xy are also algebraic and of degree $\leq mn$. ($x \pm y$ and xy are elements of the smallest K-subalgebra $K[x,y]$ of A containing x and y and $K[x,y]$ is generated as a K-vector space by the elements $x^\mu y^\nu$, $0 \leq \mu < m$, $0 \leq \nu < n$ and hence has dimension $\leq mn$.)

b) Let A be a commutative K-algebra. The elements $x \in A$ which are algebraic over K form a K-subalgebra A' of A. (Hint: Use the part a) above. -- The algebra A' is called the algebraic closure of K in A.) If K is a field, then A' is also a field.

Example. The algebraic numbers $z \in \mathbb{C}$ are precisely the ones which are algebraic over $\mathbb{Q}$, they form a subfield $\overline{\mathbb{Q}}$ of $\mathbb{C}$. The field $\overline{\mathbb{Q}}$ is algebraically closed field (like the field $\mathbb{C}$), but $\overline{\mathbb{Q}}$ has only countably many elements. For the proof of $\overline{\mathbb{Q}}$ is algebraically closed, more generally show that: If $K \subseteq L$ is an algebraic field extension, i.e. $L = L'$ and if B is an arbitrary L-algebra, then an element $y \in B$ is algebraic over L if and only if y is algebraic over K.)

c) Give an example of a K-algebra A with algebraic elements $x, y \in A$ such that $x+y$ and xy are transcendental over K. (For example, try $A := \operatorname{End}_K V$, where V is infinite dimensional K-vector space, e.g. $V = K^{(\mathbb{N})}$)

20. Find the minimal polynomials of the following algebraic numbers over $\mathbb{Q}$:

a) $\sqrt[n]{p}$, $n \in \mathbb{N}^*$, p prime

b) $\sqrt{2}+\sqrt{3}$ c) $\sqrt{2}+\sqrt[3]{3}$ d) $\sqrt[3]{2}+\sqrt[3]{3}$ (cf 10.A.21)

21. Let $p \in \mathbb{N}^*$ be a prime number. For a polynomial $F \in \mathbb{Z}[X]$ with integer coefficients, denote $\overline{F}$ the polynomial in $\mathbb{Z}/\mathbb{Z}p[X]$ obtained by taking the images of the coefficients of F in the field $\mathbb{Z}/\mathbb{Z}p$. Clearly the map $F \longmapsto \overline{F}$ is a ring homomorphism. Show that: if $\deg F = \deg \overline{F}$ and if $\overline{F}$ is prime in $\mathbb{Z}/\mathbb{Z}_p[X]$, then F is prime in $\mathbb{Q}[X]$. (Hint: Use 10.A.19. -- Use this result to test (very easily) the irreducibility of a polynomial in $\mathbb{Q}[X]$. For example, the polynomial X^4+X^3+1 is prime in $(\mathbb{Z}/\mathbb{Z}\cdot 2)[X]$; for even a_1 and a_2 and odd a_0, a_3, a_4, all polynomials $a_4X^4+a_3X^3+a_2X^2+a_1X+a_0 \in \mathbb{Z}[X]$ are prime in $\mathbb{Q}[X]$. But there exists a monic irreducible polynomial F in $\mathbb{Z}[X]$ such that $\overline{F}$ is irreducible for all prime numbers $p \in \mathbb{N}^*$, e.g. $F := X^4+1 = /\!/_8$, $\zeta_8 = e^{2\pi i/8} = (1+i)/\sqrt{2}$, proof!)

22 (Polynomials with coefficients in $k(Z)$) Let k be a field. Consider the polynomial algebra $K[X] = k(Z)[X]$ with the ground field $K := k(Z)$ the rational function field in one variable Z. Analogous to Example 10.A.16 for every polynomial $F \in K[X]$, $F \neq 0$, there exists a unique representation

$F = I(F)\,F^*$, where $I(F) \in k(z)$ is a rational function and $F^* \in k[z][x] = k[z,x]$ whose coefficients are relatively prime polynomials in $k[z]$. and the leading coefficient of F is monic in $k[z]$. $I(F)$ is called the content and F^* is called the primitive part of F. Formulate and prove the analogous statements 10.A.17 and 10.A.21 for the polynomials in $k(z)[x]$ and $k[z,x]$. -- For the investigation of $F^* \in k[z,x]$ we can interchange the roles of z and x, i.e. consider F^* as a polynomial in $k[x][z] \subseteq k(x)[z]$ (see also section 10.B on polynomials in several variables) The (monic in x) polynomial $F = F^* = (x-1)^2(x^2+z^2)-x^2$ in $k(z)[x]$ is prime if $\operatorname{char} k \neq 2$, since $F = (x-1)^2 z^2 + x^3(x-2)$ and since $z^2 + x^3(x-2)/(x-1)^2 \in k(x)[z]$ is prime by Exercise 1.

Another simple example: if $R \in k(z)$, $R \notin k$, $R = F/G$ with relatively prime polynomials $F, G \in k[z]$, then R is transcendental over k (see Exercise 15) and $k(z)$ is algebraic over $k(R)$. The minimal polynomial of z over $k(R)$ is upto normalising (in the case R is linear) the polynomial $F(x) - G(x)\,R \in k(R)[x]$. In particular, we have $[k(z) : k(R)] = \operatorname{Max}(\deg F, \deg G)$ and $k(R) = k(z)$ if and only if R is a fractional linear function $R = \dfrac{a+bz}{c+dz}$ with $a,b,c,d \in k$, $ad-bc \neq 0$.

Therefore $\mathrm{Aut}_{k\text{-alg}}\, k(z) \cong PGL_2(k)$. More generally: If $\pi = \pi(X) \in k[X]$ is prime and if $F_0, F_1 \in k[z]$, $F_1 \neq 0$, F_0 and F_1 are not both constants, then $\pi(X)$ and $\pi(F_1 X + F_0)$ are prime in $k(z)[X]$ and it is $I(\pi(F_1 X + F_0)) = 1$, i.e. $\pi(F_1 X + F_0) \notin k(X)$ is also prime in $k[z, X]$ and $k(X)[z]$ if and only if $GCD(\pi(F_0), F_1) = 1$.

23. Let A be an Euclidean integral domain with the Euclidean function φ. Then every element $a \neq 0$ in A with $\varphi(a)$ minimal in $\varphi(A \setminus \{0\})$ is a unit in A.

24. Let A be an Euclidean integral domain with the Euclidean function φ. Further, assume that for all $a, b \in A \setminus \{0\}$, we have $\varphi(a+b) \leq \mathrm{Max}\{\varphi(a), \varphi(b)\}$ and $\varphi(ab) = \varphi(a) + \varphi(b)$

a) The division with remainder in A is unique, i.e. the elements $q, r \in A$ with $a = qb + r$ and either $r = 0$ or $\varphi(r) < \varphi(b)$, are uniquely determined (in A) by a and $b \neq 0$.

b) A is either a field or is isomorphic to the polynomial ring $k[X]$ over a field k.
(Hint: By Exercise 23, $k := \{a \in A \setminus \{0\} \mid \varphi(a) = 0\} \cup \{0\}$ is a field (subfield of A). If $k \neq A$, then choose $x \in A \setminus k$ such that $\varphi(x)$ is minimal in $\varphi(A \setminus k)$. Then $k[x] = A$.)

25: (Uniqueness of prime decomposition in Principal ideal domain) See Remark 10.A.24.

a) If a and b are non-zero elements in A and $Aa + Ab = Ad$, $d \in A$, then d is a greatest common divisor of a and b, i.e. a common divisor of a and b which is divisible by every other common divisor of a and b. If A is Euclidean domain, then GCD can be computed with the help of the Euclidean algorithm like in the cases $\mathbb{Z}$ and $K[X]$.

b) An element $a \in A \setminus \{0\}$, $a \notin A^\times$ is called irreducible in A if every divisor of a is either a unit in A or of the form εa with a unit $\varepsilon \in A^\times$. Prove the Lemma of Euclid: If $a \in A \setminus \{0\}$ irreducible and if a divides the product $a_1 \cdots a_r$, $a_1, \dots, a_r \in A$, then a divides at least one of the factor (see 10.A.8 Since Euclid's lemma holds for A, the irreducible elements in A are also prime in A.)

c) Every element $a \in A \setminus \{0\}$, $a \in A^\times$, is a product of finitely many prime elements. (Suppose that a has no such a decomposition, then there exists an infinite proper ascending chain $Aa = Aa_0 \subsetneq Aa_1 \subsetneq \cdots \subsetneq Aa_n \subsetneq \cdots$ of principal ideals in A. Then $\mathfrak{A} := \bigcup_{n \in \mathbb{N}} Aa_n$ is an ideal in A and hence principal ideal Ab. If $b \in Aa_{n_0}$, then $\mathfrak{A} = Ab = Aa_{n_0}$ a contradiction.)

d) The representation of a in the part c) is unique in the following sense: if $a = p_1 \cdots p_r = q_1 \cdots q_s$ with prime elements $p_1, \cdots, p_r; q_1, \cdots, q_s \in A$, then $r = s$ and there exists a permutation $\sigma \in \mathfrak{S}_r$ and units $\varepsilon_1, \cdots, \varepsilon_r \in A^\times$ such that $q_{\sigma(i)} = \varepsilon_i p_i$, $i = 1, \cdots, r$. (See the proof of uniqueness assertion in 10.A.9. – The representation $a = p_1 \cdots p_r$ is called the prime decomposition of a in A.)

26. Let A be a principal ideal domain but not a field. An element $a \in A$ is prime if and only if the principal ideal $\mathfrak{a} = Aa = (a)$ is a maximal ideal in A, i.e. if and only if the residue-class ring $A/\mathfrak{a}$ is a field. (10.A.29 is a special case of this assertion)

27. (Elementary divisor theorem for Euclidean domains) Let A be an Euclidean domain and let $\mathfrak{A}$ be an $m \times n$ matrix with coefficients in A of rank r. Then there exist elementary matrices $S_1, \cdots, S_p \in GL_m(A)$ and $T_1, \cdots, T_q \in GL_n(A)$ such that $S_1 \cdots S_p \mathfrak{A} T_1 \cdots T_q$ is a diagonal matrix $\mathfrak{D} = \mathrm{Diag}(e_1, \cdots, e_r, 0, \cdots, 0) \in M_{m,n}(A)$ where $e_1, \cdots, e_r \in A$ satisfy the divisibility-relations $e_1 | e_2 | \cdots | e_r$.
(The proof is analogous to the Elementary divisor theorem for $A = \mathbb{Z}$. – In this form the Elementary divisor theorem is not true for arbitrary principal ideal domain.)

28. a) The ring $\mathbb{K}[\![X]\!]$ and $\mathbb{K}\langle\langle X\rangle\rangle$ of the formal and the convergent power series rings over the field $\mathbb{K}$ are Euclidean domains (with the function which associates every power series $\sum_{n=n_0}^{\infty} a_n X^n$, $a_{n_0} \neq 0$, its order or under-degree n_0 as the Euclidean function). The only non-zero ideals in $\mathbb{K}[\![X]\!]$ and $\mathbb{K}\langle\langle X\rangle\rangle$ are the principal ideals (X^n), $n \in \mathbb{N}$. (The formal power series ring $\mathbb{K}[\![X]\!]$ is defined for any field K. It is always an Euclidean domain with the principal ideals (X^n), $n \in \mathbb{N}$ are the only non-zero ideals in it.)

b) Let A be an integral domain in which every element $a \in A \setminus \{0\}$, $a \notin A^\times$, can be written uniquely as a product $a = q_1 \cdots q_s$ of irreducible elements like in Exercise 25d) is called a factorial domain. Therefore every principal ideal domain is a factorial domain. Now, let A be a factorial domain in which there are only finitely many irreducible elements (upto multiplication by units) $p_1, \dots, p_r \in A$. Then every element $a \in A \setminus \{0\}$ can be uniquely represented in the form: $a = \varepsilon p_1^{\nu_1} \cdots p_r^{\nu_r}$ with $\varepsilon \in A^\times$, and $\nu_p =: v_p(a) \in \mathbb{N}$. (For $A = \mathbb{K}[\![X]\!]$ or $A = \mathbb{K}\langle\langle X\rangle\rangle$ we have $r = 1$.) Show that the function $\varphi : A \setminus \{0\} \to \mathbb{N}$ defined by $\varphi(a) := \sum_{j=1}^{r} v_j(a)$ is a Euclidean function in the sense of Remark 10.A.24. In particular, A is a principal ideal domain. (Hint: Let $a, b \in A \setminus \{0\}$.

For the existence of a $q \in A$ with $\varphi(a - qb) < \varphi(b)$ (if $\neq q$) one can assume that $a \neq qb$ for all $q \in A$. Then $v_{p_0}(b) > v_{p_0}(a)$ for at least one p_0 and for q one can choose $\prod_{p=1}^{r} p^{\alpha_p}$ with $\alpha_p = 0$ if $v_p(a) \neq v_p(b)$ and $\alpha_p = 1$ if $v_p(a) = v_p(b)$. Note that $v_p(x+y) = \min\{v_p(x), v_p(y)\}$ if $v_p(x) \neq v_p(y)$.)

29. The ring $\mathbb{Z}[\sqrt{-2}] = \{\alpha + i\beta\sqrt{2} \mid \alpha, \beta \in \mathbb{Z}\} \subseteq \mathbb{C}$ is an Euclidean domain with the square of the absolute value $\alpha^2 + 2\beta^2$ as Euclidean function and the ring $\mathbb{Z}[\sqrt{2}] = \{\alpha + \beta\sqrt{2} \mid \alpha, \beta \in \mathbb{Z}\} \subseteq \mathbb{R}$ is an Euclidean domains with the function $|\alpha^2 - 2\beta^2|$ as Euclidean function.

30. The integral domain $\mathbb{Z}[\sqrt{-5}] = \{\alpha + i\alpha'\sqrt{5} \mid \alpha, \alpha' \in \mathbb{Z}\} \subseteq \mathbb{C}$ is not principal ideal domain and hence also not Euclidean domain. (The ideal generated by 2 and $1 + i\sqrt{5}$ is not a principal ideal as one can see this with the calculation with the square of the absolute value. This is also the classical example for different representations of an element in $\mathbb{Z}[\sqrt{-5}]$ as a product of irreducible elements: $6 = 2 \cdot 3 = (1 + i\sqrt{5})(1 - i\sqrt{5})$.)

31. (Prime elements in $\mathbb{Z}[i]$) Because of the unique prime factorisation in the principal ideal domain

it is enough to find prime elements, i.e. irreducible elements in this ring and describe their multiplicative structure.

a) Let $z \in \mathbb{Z}[i]$. If $z\cdot\bar{z}$ is a prime number in $\mathbb{N}$, then z is prime in $\mathbb{Z}[i]$. If z is prime in $\mathbb{Z}[i]$, then z divides the number $z\bar{z} > 1$ and hence by Euclid's Lemma z divides a prime factor $p \in \mathbb{N}^*$ of $z\bar{z}$.

b) Let $p \in \mathbb{N}$ be a prime number. If $p \equiv 3 \bmod 4$, then p is prime in $\mathbb{Z}[i]$. (Hint: For a proper divisor $z = \alpha+\beta i$, $\alpha, \beta \in \mathbb{Z}$, of p, $z\bar{z} = \alpha^2+\beta^2$ must be a proper divisor of p^2 in $\mathbb{N}$ and hence it must be p. Now by computing modulo 4, one can see that this is not possible.)

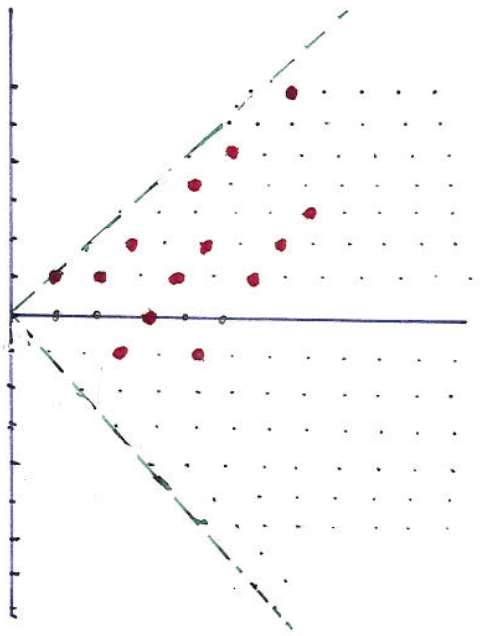
c) Let $p \in \mathbb{N}$ be a prime number. If $p \equiv 1 \bmod 4$, then the prime-factorisation of p in $\mathbb{Z}[i]$ is of the form $p = z\bar{z}$ with prime elements z and $\bar{z}$. (Since X^2+1 has a zero in $\mathbb{K}_p$ by the remark at the end of 10.A.29, there exists $x \in \mathbb{Z}$ such that $x^2 \equiv -1 \bmod p$. One can also use the argument: If $p = 4k+1$, then all $4k$ non-zero elements in $\mathbb{K}_p = \mathbb{Z}/\mathbb{Z}p$ are zeros of $X^{p-1}-1 = (X^{2k}-1)(X^{2k}+1)$ and $X^{2k}-1$ has atmost $2k$ zeros. Now, $(x+i)(x-i) = x^2+1 = tp$ for some $t \in \mathbb{Z}$. If p is prime in $\mathbb{Z}[i]$, then by the uniqueness

of the prime factorisation in $\mathbb{Z}[i]$ either p divides $x+i$ or p divides $x-i$, but this is not possible. This shows that p cannot be prime in $\mathbb{Z}[i]$. Let z be a prime element in the prime-factorisation of p in $\mathbb{Z}[i]$. Then $z\bar{z}$ is a proper divisor of p^2 in $\mathbb{Z}$ and hence $z \cdot \bar{z} = p$. Now, by the part a) $\bar{z}$ is also prime.)

d) The prime-factorisation of 2 in $\mathbb{Z}[i]$ is

$2 = (1+i)(1-i)$ (by part a) $1 \pm i$ are prime in $\mathbb{Z}[i]$.)

e) The prime elements $z = \alpha + \beta i$ in $\mathbb{Z}[i]$ with $\alpha > 0$ and $-\alpha < \beta \leq \alpha$ are exactly the following elements:
(1) $1+i$ (2) The prime numbers $p \in \mathbb{N}$ with $p \equiv 3 \bmod 4$ (3) The numbers of the form $\alpha \pm \beta i$, $0 < \beta < \alpha$ for which the $\alpha^2 + \beta^2$ is a prime number $p \in \mathbb{N}$ with $p \equiv 1 \bmod 4$. -- All other prime elements are obtained by rotation through $\pi/2$, π or $3\pi/2$, i.e. by multiplication with one of the units $i, -1, -i$ (other than the unit 1).



(As prime element z divides one of the prime numbers p from the prime factorisation of $z\bar{z} \in \mathbb{N}^*$. By parts b), c) and d) therefore there exist only the given prime elements. Given two from them, say $\alpha+\beta i$ and $\alpha'+\beta' i$ which are obtained from each other by multiplication of a unit, then $\alpha^2+\beta^2 = \alpha'^2+\beta'^2$.
-- It is not known whether there are infinitely many prime elements in $\mathbb{Z}[i]$ of the form $\alpha+i$, $\alpha \in \mathbb{N}^*$ i.e. whether there are infinitely many $\alpha \in \mathbb{N}^*$ such that α^2+1 is prime in $\mathbb{N}$. Since there are infinitely many prime numbers p with $p \equiv 3 \bmod 4$, it follows that there are infinitely many prime elements of $\mathbb{Z}[i]$ which lie on the real-axis.)

32. (Two-Square theorem of Fermat-Euler) A positive natural number n is the sum of two squares if and only if all of its prime divisors p with $p \equiv 3 \bmod 4$ have even multiplicity. Further, n is the sum of two relatively prime squares if and only if n is of the form $n = m$ or $n = 2m$, where the prime divisors of m are $\equiv 1 \bmod 4$.
(A number $n \in \mathbb{N}^*$ is the sum of two squares if and only if $n = z\bar{z}$ for a $z \in \mathbb{Z}[i]$. Now, use the uniqueness of prime-factorisation in $\mathbb{Z}[i]$ and the description of prime elements in Exercise 31 part e). -- Using similar arguments one can also easily obtain the formula for the number of possible representations of a number as sum of two squares.)