Introduction

This book is an attempt to cover most of the results on reducibility of polynomials over fairly large classes of fields; results valid only over finite fields, local fields or the rational field have not been included. On the other hand, included are many topics of interest to the author that are not directly related to reducibility, e.g. Ritt's theory of composition of polynomials.

Here is a brief summary of the six chapters.

Chapter 1 (Arbitrary polynomials over an arbitrary field) begins with Lüroth's theorem (Sections 1 and 2). This theorem is nowadays usually presented with a short non-constructive proof, due to Steinitz. We give a constructive proof and present the consequences Lüroth's theorem has for subfields of transcendence degree 1 of fields of rational functions in several variables. The much more difficult problem of the minimal number of generators for subfields of transcendence degree greater than 1 belongs properly to algebraic geometry and here only references are given.

The next topic to be considered (Sections 3 and 4) originated with Ritt. Ritt 1922 gave a complete analysis of the behaviour of polynomials in one variable over $\mathbb{C}$ under composition. He called a polynomial prime if it is not the composition of two polynomials of lower degree and proved the two main results:

(i) In every representation of a polynomial as the composition of prime polynomials the number of factors is the same and their degrees coincide up to a permutation.

(ii) If A, H and B, G are polynomials of relatively prime degrees m and n, respectively, and

$$A(G) = B(H), \tag{1}$$

then A, B, G, H can be given explicitly.

Ritt showed also how every representation of a polynomial as the composition of prime polynomials can be obtained from a given one by solving several equations of the form (1), where A and B are prime.

We present an extension of Ritt's result to polynomials over an arbitrary field, for (ii) obtained only recently by Zannier 1993. Ritt's term 'prime' is replaced by 'indecomposable'.

Indecomposability plays an essential role in the next topic: reducibility of polynomials of the form $(f(x) - f(y))/(x - y)$ (Section 5). A necessary and sufficient condition for reducibility over fields of characteristic 0 was proved by Fried 1970. We give a proof of Fried's theorem published recently by Turnwald 1995 and summarize the more recent progress on this topic and the state of knowledge on reducibility of $f(x) - g(y)$, where g, h are polynomials. Section 6 contains results of Kronecker on factorization of polynomials. They include properties of the Kronecker substitution, a theorem of Kronecker once called fundamental and now nearly forgotten, that will be used later, and the theorem of Kronecker and A. Kneser. The latter describes a connection between reducibility of a polynomial $f \in \boldsymbol{k}[x]$ over $\boldsymbol{k}(\eta)$ and that of a polynomial $g \in \boldsymbol{k}[x]$ over $\boldsymbol{k}(\xi)$, where $f(\xi) = g(\eta) = 0$. Section 7 takes again the study of reducibility of polynomials with separated variables. H. Davenport and the author proved in 1963 that a polynomial of the form $F(x, y) + G(z)$ is reducible over a field $\boldsymbol{k}$ of characteristic 0 if and only if $F = H(A(x, y))$, $A, H \in \boldsymbol{k}[t]$ and $H(t) + G(z)$ is reducible over $\boldsymbol{k}$. Section 7 contains a natural generalization of this result and a discussion of the related results of Tverberg and Geyer. After some auxiliary results have been established in Section 8, a connection between irreducibility of a polynomial and of its substitution value after a specialization of some of the variables is treated in Section 9. This topic, connected with the names of Bertini and Hilbert, will be considered again in Chapter 3, Section 3 and Chapter 4, Section 4. The last Section 10 deals with the properties of the Newton polytope of a polynomial in many variables, a natural generalization of the Newton polygon.

Chapter 2 (Lacunary polynomials over an arbitrary field) begins with theorems of Capelli and M. Kneser. Capelli 1898 gave a simple necessary and sufficient condition for reducibility of a binomial $x^n - a$ over a subfield of $\mathbb{C}$. The case of positive characteristic was settled by Rédei 1967. The theorem can also be viewed as a necessary and sufficient condition for an element of a field $\boldsymbol{k}$ to satisfy the equality $[\boldsymbol{k}(\sqrt[n]{a}) : \boldsymbol{k}] = n$. In this aspect the theorem is open to generalization, specifically, one can study the degree $[\boldsymbol{k}(\sqrt[n_1]{a_1}, \sqrt[n_2]{a_2}, \ldots, \sqrt[n_l]{a_l}) : \boldsymbol{k}]$. An all encompassing result in this direction for separable extensions has been found by M. Kneser 1975. It is reproduced in Section 1 together with a more immediate extension of Capelli's theorem.

It is an almost immediate consequence of Capelli's theorem that for $a \neq 0$ the polynomial $x^m + y^n + a$ is irreducible over every field of characteristic 0 containing a. This observation is generalized in Section 2 to an easily applicable irreducibility criterion for polynomials in many variables.

Following the work of Ritt 1927, Gourin 1933 proved that for a polynomial $F(x_1, \dots, x_s)$ with more than two terms, irreducible over $\mathbb{C}$, and for arbitrary positive integers $t_1, \dots, t_s$, the factorization of $F(x_1^{t_1}, \dots, x_s^{t_s})$ into irreducible factors can be derived from the factorization of $F(x_1^{t_1}, \dots, x_s^{t_s})$, where $\langle t_1, \dots, t_s \rangle$ belongs to a finite set of integral vectors depending only on F. Gourin's proof applies with small modifications to polynomials over an arbitrary algebraically closed field and to integers $t_1, \dots, t_s$ non-divisible by the characteristic of the field. An extension of the theorem to polynomials over fields no longer algebraically closed is given in Section 3. The only polynomials to which this extension does not apply apart from cx_i are of the form

$$F_0\left(\prod_{i=1}^{s} x_i^{\delta_i}\right) \prod_{i=1}^{s} x_i^{-d \min(0,\delta_i)}, \tag{2}$$

where $F_0(x)$ is a polynomial of degree d and $\delta_1, \dots, \delta_s$ are integers, possibly negative.

The long Section 4 deals with reducibility of trinomials over any rational function field $\boldsymbol{k}(\boldsymbol{y})$. A necessary and sufficient condition for reducibility is given for any trinomial $x^n + Ax^m + B$ $(n > m > 0)$ such that $A^{-n}B^{n-m} \notin \boldsymbol{k}$ and $nm(n-m)$ is not divisible by the characteristic of $\boldsymbol{k}$. The cases $A \in \boldsymbol{k}$ and $B \in \boldsymbol{k}$ are given special attention. These results are used in Section 5 to characterize reducible quadrinomials depending essentially on at least two variables and such that the exponent vectors are all different modulo the characteristic of the ground field.

Section 6 presents a lower estimate for the number of non-zero coefficients of f^l in terms of l and of the number of non-zero coefficients of a polynomial f in one variable. An upper estimate is also given, valid in infinitely many essentially different cases.

Chapter 3 (Polynomials over an algebraically closed field) begins with the result of E. Noether, according to which a form of degree d in n variables is reducible over an algebraically closed field if and only if its coefficients satisfy a system of algebraic equations depending only on d and n (Section 1). Section 2 presents a theorem of Ruppert in which for $n = 3$ and characteristic 0 a system of equations with the above property is explicitly constructed. Section 3 is devoted to Bertini's theorem on reducibility. This theorem in its

original formulation characterizes forms

$$f_0(\boldsymbol{x}) + \lambda_1 f_1(\boldsymbol{x}) + \cdots + \lambda_n f_n(\boldsymbol{x})$$

defined over $\mathbb{C}$ that become reducible over $\mathbb{C}$ for every choice of parameters $\lambda_1, \ldots, \lambda_n$. We present an extension of this result to all algebraically closed fields with a proof due to Krull 1937.

Section 4 differs definitely from the former three in that it concerns exclusively polynomials over $\mathbb{C}$. For such polynomials, in any number of variables, Mahler has introduced a measure M, that is multiplicative, i.e. $M(fg) = M(f)M(g)$. This measure has many interesting properties itself and also helps to describe the behaviour at the multiplication of other measures, e.g. of the length, defined for a polynomial as the sum of the absolute values of its coefficients. Section 4 presents several theorems on the Mahler measure of polynomials over $\mathbb{C}$, some of them quite recent.

Chapter 4 (Polynomials over a finitely generated field) begins with an extension of Gourin's theorem (discussed in Chapter 2, Section 3) to polynomials of the form (2), which is possible for every finitely generated ground field $\boldsymbol{K}$, provided the polynomial F_0 is irreducible over $\boldsymbol{K}$ and has neither 0 nor roots of unity as zeros (Section 1). Section 2 presents the best known lower bound in terms of the degree for the Mahler measure of an irreducible non-cyclotomic polynomial with integer coefficients. This bound is used in Section 3 to the study of the following problem.

Suppose that P, Q are coprime polynomials over a field $\boldsymbol{K}$. Then there exists a number $c(P, Q)$ with the following property. If $P(\xi^{n_1}, \ldots, \xi^{n_k}) = Q(\xi^{n_1}, \ldots, \xi^{n_k}) = 0$ for some integers $n_1, \ldots, n_k$ and some $\xi \neq 0$ in the algebraic closure of $\boldsymbol{K}$ then either $\xi^q = 1$ for a positive integer q or there exist integers $\gamma_1, \ldots, \gamma_k$ such that

$$\sum_{i=1}^{k} \gamma_i n_i = 0 \quad \text{and} \quad 0 < \max_{1 \le i \le k} |\gamma_i| \le c(P, Q).$$

This is established in Section 3 only for $k \le 3$, $\boldsymbol{K}$ arbitrary and for k arbitrary, $\boldsymbol{K}$ of positive characteristic. The result is placed in Chapter 4 rather than in Chapter 2 since the decisive role is played by the field generated over the prime field of $\boldsymbol{K}$ by the coefficients of P and Q.

For $k > 3$, $\boldsymbol{K}$ of zero characteristic, the assertion is established in the appendix written by Umberto Zannier, entitled Proof of Conjecture 1. Indeed, in the first version of Section 3 the assertion in full generality was only conjectured and the name Conjecture has been retained.

Section 4 is devoted to Hilbert's irreducibility theorem. The simplest case of this theorem asserts that if a polynomial $F(x, t)$ is irreducible over $\mathbb{Q}$ as a

polynomial in two variables then $F(x, t^*)$ is irreducible over $\mathbb{Q}$ for infinitely many integers t^*. Section 4 presents a much more general form of the theorem, in which in particular $\mathbb{Q}$ is replaced by an arbitrary finitely generated field. In order to prove the theorem in such generality we use a method of Eichler based on some deep properties of equations over finite fields, rather than the more elementary approach sufficient to establish the theorem for number fields.

Hilbert's theorem in its simplest form stated above is closely related to the following property of diophantine equations. If an algebraic equation $F(x, t) = 0$ is soluble in rational or integer x for a sufficiently large set of integers t, then it is soluble for x in $\mathbb{Q}(t)$ or $\mathbb{Q}[t]$, respectively. A question suggests itself, whether a similar statement holds for equations with a greater number of unknowns and parameters and with $\mathbb{Q}$ replaced by a number field $\boldsymbol{K}$. The bulk (Sections 1–8) of Chapter 5 (Polynomials over a number field) is devoted to the study of this question. Section 1 constitutes an introduction to Sections 2–8, therefore here we only explain the fact that many theorems proved in this section concern polynomials over $\mathbb{C}$ rather than over a number field. Specifically, in every such case the main difficulty lies in proving the theorem for polynomials over $\boldsymbol{K}$ and then the general statement follows by linear algebra.

The result of Section 9 is tantamount to the following theorem. Let $F \in \boldsymbol{K}[x_1, \dots, x_s]$, where $\boldsymbol{K}$ is a number field, be irreducible over $\boldsymbol{K}$, not a scalar multiple of x_i and not of the form (2), where F_0 has roots of unity as zeros. Then there exists a number $c_0(\boldsymbol{K}, F)$ with the following property. If for some integers $n_1, \dots, n_s$ the only zeros of $F(x^{n_1}, \dots, x^{n_s})$ are 0 and roots of unity, then there exist integers $\gamma_1, \dots, \gamma_k$ such that

$$\sum_{i=1}^{s} \gamma_i n_i = 0 \quad \text{and} \quad 0 < \max |\gamma_i| \le c_0(\boldsymbol{K}, F).$$

The title of the last chapter 'Polynomials over a Kroneckerian field' itself requires an explanation. By a Kroneckerian field (a term due to K. Győry) we mean a totally real number field or a totally complex quadratic extension of such a field. Among polynomials defined over a Kroneckerian field and prime to the product of the variables, exceptional in several respects are polynomials called self-inversive, i.e. polynomials F that satisfy an identity

$$F(x_1^{-1}, \dots, x_k^{-1}) \prod_{i=1}^{k} x_i^{d_i} = c\overline{F}(x_1, \dots, x_k),$$

where d_i is the degree of F with respect to x_i, $c \in \mathbb{C}$ and the bar denotes complex conjugation.

Section 1 presents estimates for the Mahler measure of non-self-inversive polynomials. They are far better than the estimates true in general.

Section 2 shows, for arbitrary integers $n_1, \dots, n_k$, how all non-self-inversive factors of a polynomial $F(x^{n_1}, \dots, x^{n_k})$ irreducible over a Kroneckerian field $\boldsymbol{K}$ can be obtained together with their multiplicities from the factorization of finitely many polynomials

$$F\left(\prod_{i=1}^{r} y_i^{v_{i1}}, \dots, \prod_{i=1}^{r} y_i^{v_{ik}}\right), \text{ where } \max|v_{ij}| \le c(\boldsymbol{K}, F).$$

For $k = 1$ this is a consequence of the result of Chapter 4, Section 1. For $k > 1$ there is an analogy between the two results, but the above result lies much deeper, concerning reducibility of polynomials in one variable. Probably a similar result is true for all factors of $F(x^{n_1}, \dots, x^{n_k})$ irreducible over $\boldsymbol{K}$ that have neither 0 nor roots of unity as zeros, however this is far from being proved and Section 3 presents only some steps in this direction. As a consequence one obtains for a given algebraic number $a \neq 0, \pm 1$ and a given polynomial $f(x)$ with algebraic coefficients the existence of a polynomial

$$x^n + ax^m + f(x) \text{ irreducible over } \boldsymbol{K}(a, \boldsymbol{f}),$$

where $\boldsymbol{f}$ is the coefficient vector of f. Unfortunately, there is a very restrictive condition that the field $\boldsymbol{K}(a, \boldsymbol{f})$ should be linearly disjoint with all cyclotomic fields.

Section 4, the last one, gives an exposition of the work of Győry on reducibility over Kroneckerian fields of composite polynomials $F(G(x))$.

The choice of material has been dictated by the personal taste of the author; out of 82 theorems, 37 belong to him and out of these 23 (Theorems 23, 24, 52, 54, 56, 58–66, 72, 74–81) have not been published before with the same degree of generality. Also Theorems 17, 29, 43, 50, 51, 55, 57, 67–71 are technically new, although their crucial special cases have been published before. In particular, Theorem 43 is taken from an unpublished and now lost manuscript of the late J. Wójcik.

Theorems proved in the sequel, conjectures and definitions are numbered successively for the whole book except the appendices; lemmas, conventions, remarks, examples and formulae are numbered separately for each section.

The book is not self-contained, the reader is often referred to the following five books:

E. Hecke, *Lectures on the theory of algebraic numbers*,
S. Lang, *Algebra*,
H. Mann, *Introduction to algebraic number theory*,

W. Rudin, *Principles of mathematical analysis*,
W. Rudin, *Real and complex analysis*,

abbreviated as [H], [L], [M], [P], [R]. The definitions and the results needed to follow the exposition, not found in the above books, are collected in 10 appendices: A, B, C, D, E, F, G, I, J, K. The reference Theorem E5, say, means Theorem 5 of Appendix E, the reference Theorem [L] 10.1 means Theorem 10.1 of Lang's book.

At the end of the book there are an index of theorems and an index of definitions and conjectures covering the main part of the book, not the appendices. The index of terms covers the whole book. There is no index of names, but in the bibliography for each reference, except ones listed as standard, there are indicated pages, where this reference is cited.

Notation

The letters $\boldsymbol{k}$ and $\boldsymbol{K}$ are reserved for fields, in Chapters 4–6 the letter $\boldsymbol{K}$ denotes a finitely generated field.

char $\boldsymbol{k}$ is the characteristic of $\boldsymbol{k}$,
$\boldsymbol{k}^*$ is the multiplicative group of the field $\boldsymbol{k}$,
$\overline{\boldsymbol{k}}$ is the algebraic closure of $\boldsymbol{k}$,$\boldsymbol{k}^{\text{sep}}$ the maximal subfield of $\overline{\boldsymbol{k}}$ separable over $\boldsymbol{k}$.
$O_{\boldsymbol{K}}$ is the ring of integers of a number field $\boldsymbol{K}$, disc $\boldsymbol{K}$ is its discriminant, $O_{\boldsymbol{K}}^*$ the group of units. For an extension $\boldsymbol{K}/\boldsymbol{k}$, tr.deg. $\boldsymbol{K}/\boldsymbol{k}$ is the transcendence degree of $\boldsymbol{K}$ over $\boldsymbol{k}$. For a finite extension $\boldsymbol{K}/\boldsymbol{k}$ the symbols $N_{\boldsymbol{K}/\boldsymbol{k}}$ and $\mathrm{Tr}_{\boldsymbol{K}/\boldsymbol{k}}$ denote the norm and the trace, respectively, from $\boldsymbol{K}$ to $\boldsymbol{k}$ or from $\boldsymbol{K}(x_1, \dots, x_n)$ to $\boldsymbol{k}(x_1, \dots, x_n)$, where $x_1, \dots, x_n$ are variables.
$\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ are the fields of rational, real and complex numbers, respectively,
$\mathbb{F}_q$ is the finite field of q elements,
$\mathbb{Z}$ is the ring of rational integers,
$\mathbb{N}$, $\mathbb{N}_0$, $\mathbb{R}_+$ are the sets of positive integers, non-negative integers and non-negative real numbers, respectively,
$\mathfrak{M}_{k,l}(S)$ is the set of all matrices with k rows and l columns and with entries from the set S, ${}^tM$, and rank M are the transpose and the rank of a matrix M, ${}^aM$ and $\det M$ the adjoint and the determinant of a square matrix M, respectively. Vectors are treated as matrices with one row. For a set S of vectors rank S is the number of linearly independent vectors in S.
$GL(\mathbb{Z}, n)$ is the multiplicative group formed by all elements of $\mathfrak{M}_{n,n}(\mathbb{Z})$ with determinant ± 1,
I_n is the identity matrix of order n.

Bold face letters denote fields or vectors; which of the two should be clear from the context; in addition $\boldsymbol{C}(F)$ and $\boldsymbol{M}(F)$ have a special meaning explained in Chapter 1, Section 10 and bold face letters are freely used in Chapter 4,

Section 3. If $\boldsymbol{a}$ is a vector, a_i is its ith coordinate; for two vectors $\boldsymbol{a}$ and $\boldsymbol{b}$, $\boldsymbol{ab}$ and $\boldsymbol{a} \wedge \boldsymbol{b}$ denote the inner and the external product, respectively. German letters, except $\mathfrak{M}$ with subscripts, denote prime divisors and prime ideals, script letters usually denote groups.

If distinct bold face letters occur as arguments of a polynomial, it is assumed that the coordinates of the relevant vectors are independent variables. For a polynomial $F(\boldsymbol{x}_1, \boldsymbol{x}_2, \ldots, \boldsymbol{x}_n)$ over an integral domain D or a field $\boldsymbol{k}$:

$\partial_{\boldsymbol{x}_i} F$ is the maximum degree of F with respect to x, where x runs over all variables occurring in $\boldsymbol{x}_i$, if $n = 1$, $\partial_{\boldsymbol{x}_1} F =: \partial F$, however $\frac{\partial F}{\partial x}$ is the partial derivative of F with respect to x;

$\deg_{\boldsymbol{x}_i} F$ is the degree of F viewed as a polynomial in $\boldsymbol{x}_i$, if $n = 1$, $\deg_{\boldsymbol{x}_1} F =: \deg F$.

If $f = \frac{F}{G}$, where F, G are coprime polynomials, then $\deg f := \max\{\deg F, \deg G\}$.

If $f, g \in \boldsymbol{k}(\boldsymbol{x})$, $f \underset{\boldsymbol{k}}{\cong} g$ means that $fg^{-1} \in \boldsymbol{k} \setminus \{0\}$ (f, g are scalar multiples of each other) and $f \underset{\boldsymbol{k}}{\ncong} g$ means that the above relation does not hold. Further

$$F(\boldsymbol{x}) \underset{D}{\overset{\text{can}}{=}} \text{const} \prod_{\sigma=1}^{s} F_\sigma(\boldsymbol{x})^{e_\sigma}$$

means that

$$F(\boldsymbol{x}) \prod_{\sigma=1}^{s} F_\sigma(\boldsymbol{x})^{-e_\sigma} \in D \setminus \{0\},$$

the polynomials $F_\sigma \in D[\boldsymbol{x}]$ $(1 \le \sigma \le s)$ are irreducible over the quotient field of D and pairwise relatively prime, $e_\sigma \in \mathbb{N}$.

The leading coefficient of F is the coefficient of the first term of F in the antilexicographic order†. A polynomial with leading coefficient 1 is called monic, the greatest common divisor of non-zero polynomials is assumed to be monic,

$\operatorname{disc}_x F$ is the discriminant of F with respect to the variable x,

$\operatorname{cont} F$ is the content of F defined as the greatest common divisor of the coefficients of F, F is primitive if $\operatorname{cont} F = 1$. For rational functions f and g in one variable we set

$$f \circ g = f(g(x)).$$

For a rational function of the form

$$f(x_1, x_2, \ldots, x_n) = x_1^{\alpha_1} x_2^{\alpha_2} \ldots x_n^{\alpha_n} F(x_1, x_2, \ldots, x_n),$$

† i.e. such a term $a \prod_{i=1}^n x_i^{\alpha_i}$ $(a \neq 0)$ that for every other term $b \prod_{i=1}^n x_i^{\beta_i}$ $(b \neq 0)$ there is a $k \ge 0$ satisfying $\alpha_i = \beta_i$ $(i \le k)$, $\alpha_{k+1} > \beta_{k+1}$.

where F is a polynomial prime to $x_1x_2\dots x_n$ we set

$$Jf(x_1, x_2, \dots, x_n) = F(x_1, x_2, \dots, x_n)$$

and consider the leading coefficient and the content of F as those of f. A homogeneous polynomial is called a form. A form $F \in \boldsymbol{k}[x, y]$ is called singular if it has a multiple factor over $\overline{\boldsymbol{k}}$, and non-singular otherwise.

$\operatorname{res}\begin{pmatrix} H_1, \dots, H_s \\ x_1, \dots, x_s \end{pmatrix}$ is the resultant of forms $H_1, \dots, H_s$ with respect to variables $x_1, \dots, x_s$.

Braces denote sets, card S is the cardinality of S, S^n is usually the Cartesian nth power of S, but occasionally, when $\boldsymbol{k}$ is a field, $\boldsymbol{k}^n = \{x^n : x \in \boldsymbol{k}\}$ and similarly for groups or rings. For sets A and B : $A \setminus B = \{x \in A : x \notin B\}$, $A - B = \{a - b : a \in A,\ b \in B\}$.

Parenthesis is used as above to denote matrices, but $(abc\dots)$ denotes the cycle $a \to b \to c \dots \to a$;

$(a, b, c, \dots)$ denotes the greatest common divisor of $a, b, c, \dots$, but occasionally $(a, b) = \{x \in \mathbb{R} : a < x < b\}$;

$\boldsymbol{k}(S)$ denotes the least field containing the field $\boldsymbol{k}$ and the set S,

$\boldsymbol{k}((\boldsymbol{x}))$ is the field of Laurent series over $\boldsymbol{k}$ of the variable vector $\boldsymbol{x}$.

Brackets $[a, b, c, \dots]$ denote the least common multiple of $a, b, c, \dots$, but occasionally, $[a, b] = \{x \in \mathbb{R} : a \le x \le b\}$, $[a, b) = \{x \in \mathbb{R} : a \le x < b\}$;

$[\boldsymbol{L} : \boldsymbol{K}]$ or $[\mathcal{H} : \mathcal{G}]$ denotes the degree of extension $\boldsymbol{L}/\boldsymbol{K}$ or the index of the group $\mathcal{G}$ in $\mathcal{H}$, depending on the context;

$D[S]$ denotes the least ring containing the ring D and the set S,

$D[[\boldsymbol{x}]]$ is the ring of power series over D of the variable vector $\boldsymbol{x}$.

For an $x \in \mathbb{R}$: $\lfloor x \rfloor = \max\{n \in \mathbb{Z} : n \le x\}$, $\lceil x \rceil = \min\{n \in \mathbb{Z} : n \ge x\}$.

Brackets $\langle\ \rangle$ denote vectors, $\mathcal{G}\langle S\rangle$ denotes the least group containing the group $\mathcal{G}$ and the set S, also if S is a set of permutations, $\langle S\rangle$ denotes the least group of permutations containing S.

$|\cdot|$ denotes an absolute value or the Euclidean norm (except in Chapter 1, Section 9), but $|\mathcal{G}|$, where $\mathcal{G}$ is a group, denotes the order of $\mathcal{G}$.

For $z \in \mathbb{C}$, $\overline{z}$ is the complex conjugate of z, Re z and Im z are the real and the imaginary part of z, respectively. For $A = (a_{ij}) \in \mathfrak{M}_{k,l}(\mathbb{C})$: $\overline{A} = (\overline{a}_{ij})$, unless stated to the contrary. For $P \in \mathbb{C}[\boldsymbol{x}]$, $\overline{P}$ is the polynomial with the coefficients equal to the complex conjugates of the corresponding coefficients of P.

For $P \in \boldsymbol{k}[x]$, $P' = \dfrac{dP}{dx}$.

ζ_n is a primitive root of unity of order n,

μ is the Möbius function,