de Gruyter Expositions in Mathematics 45

Editors

V. P. Maslov, Academy of Sciences, Moscow
W. D. Neumann, Columbia University, New York
R. O. Wells, Jr., International University, Bremen
More recently, it has been found that there are profound relations between Nevanlinna theory and Diophantine approximation. C. F. Osgood first noticed a similarity between the number 2 in the Nevanlinna’s defect relation and the number 2 in Roth’s theorem. S. Lang pointed to the existence of a structure to the error term in Nevanlinna’s second main theorem, conjectured what could be essentially the best possible form of this error term in general based on his conjecture on the error term in Roth’s theorem. P. M. Wong used a method of Ahlfors to prove Lang’s conjecture in one dimensional case. As for higher dimension, this problem was studied by S. Lang and W. Cherry, A. Hinkkanen, and was finally completed by Z. Ye. Lately, P. Vojta gave a much deeper analysis of the situation, and compared the theory of heights in number theory with the characteristic functions of Nevanlinna theory. In his dictionary, the second main theorem due to H. Cartan corresponds to the Schmidt’s subspace theorem. Further, he proposed the general conjecture in number theory by comparing the second main theorem in Carlson–Griffiths–King’s theory. Along this route, the Shiffman’s conjecture on hypersurface targets in value distribution theory corresponds to a subspace theorem for homogeneous polynomial forms in Diophantine approximation. Vojta’s \((1, 1)\)-form conjecture is an analogue of an inequality of characteristic functions of holomorphic curves for line bundles. Being influenced by Mason’s theorem, Oesterlé and Masser formulated the \(abc\)-conjecture. The generalized \(abc\)-conjectures for integers are counterparts of Nevanlinna’s third main theorem and its variations in value distribution theory, and so on.

In this book, we will introduce the analogues of Nevanlinna theory in Diophantine approximation, which are named “distribution theory of algebraic numbers” corresponded to another name “value distribution theory” of Nevanlinna theory. In other words, we will introduce some qualitative and quantitative relations of algebraic numbers distributed in spaces. The book consists of nine chapters: In Chapter 1, we introduce some basic notations, terminologies and propositions on groups, ideals in rings, fields, field extensions, valuations and absolute values, which are often used in this book. In particular, we hope to explain clearly the corresponding relation between prime ideals and places in Dedekind domains. It will help us to understand well some contents related to absolute values, say, product formula and its derivatives.

Some foundational properties of algebraic numbers will be discussed in Chapter 2, which contains factorizations and norms of ideals, product formula and discriminants on number fields, and Minkowski’s geometry of numbers.

In Chapter 3, we introduce basic notations and facts in algebraic geometry. This is
of spaces carrying algebraic numbers in this book. First of all, we discuss carefully operations, norms and some properties in projective spaces which play important role in this book, and then we introduce varieties, divisors, linear systems, algebraic curves, sheaves, vector bundles, schemes and Kobayashi hyperbolicity.

We will discuss height functions in Chapter 4. This is the part of quantitative tools studying distribution of algebraic numbers in this book. Height functions share many general character with Nevanlinna’s order functions, say, they all satisfy first main theorem of Nevanlinna type, which establishes an important connection among height, proximity and valence (or counting by some authors) functions. This chapter also contains some introduction on Weil functions, Aralelov theory and canonical heights over Abelian varieties.

In Chapter 5, we introduce the abc-conjecture and its generalizations in detail. To understand these conjectures well, we also introduce their analogues for polynomials.

In Chapter 6, we discuss the Roth’s theorem and its generations. The Roth’s theorem is corresponding to Nevanlinna’s second main theorem on meromorphic functions on \( \mathbb{C} \). In order to make reader convenience, we also introduce its proof and connection with the abc-conjecture.

In Chapter 7, we introduce the Schmidt subspace theorem and its generalization. Schmidt subspace theorem is corresponding to Cartan’s second main theorem in value distribution of holomorphic curves into complex projective spaces. We also give a subspace theorem on hypersurfaces which is regarded as an analogue of Shiffman conjecture (proved by Hu and Yang for non-Archimedean cases and Ru for complex cases) in value distribution.

In Chapter 8, we introduce Mordell–Faltings theorem, Bombieri–Lang’s conjecture related to pseudo canonical varieties, and Vojta’s conjectures on height inequalities.

In Chapter 9, we introduce a few of \( L \)-functions. Hopefully, the methods proving prime number theorem by using the Riemann zeta-function and Dirichlet \( L \)-functions can be applied to study similar problems of other \( L \)-functions derived from number fields, modular forms, geometric analysis and so on.

Each chapter of this book is self-contained and this book is appended with a comprehensive and up-dated list of references. The book will provide not just some new research results and directions but challenging open problems in studying Diophantine approximation. One of the aims of this book is to make timely surveys on these new results and their related developments; some of which are newly obtained by the authors and have not been published yet. It is hoped that the publication of this book will stimulate, among the peers, further the researches on Diophantine approximation and their applications.

We gratefully acknowledge the supports of the related research and writing of the present book from Natural Science Fund of China (NSFC) and Research Grant Council of Hong Kong during the past years.

Pei-Chu Hu
Chung-Chun Yang
## Contents

Preface .................................................. v  

1 Field extensions ........................................ 1  
   1.1 Groups .......................................... 1  
   1.1.1 Abelian groups ................................ 1  
   1.1.2 Galois cohomology............................... 7  
   1.2 Rings and ideals .................................... 9  
   1.2.1 Ideals ......................................... 9  
   1.2.2 Completion of topological groups ............... 16  
   1.2.3 Fractional ideals ............................... 18  
   1.2.4 Relative differentials .......................... 19  
   1.3 Integral elements and valuations ................. 21  
   1.3.1 Integral elements ............................. 21  
   1.3.2 Valuation rings ................................ 23  
   1.3.3 Discrete valuation rings ........................ 27  
   1.4 Polynomials ...................................... 32  
   1.5 Algebraic extension fields ....................... 36  
   1.6 Separable extension fields ....................... 41  
   1.6.1 Separable algebraic extensions ............... 41  
   1.6.2 Ramification indices .......................... 45  
   1.7 Norm and trace .................................... 47  
   1.8 Discriminant of field extensions .................. 52  
   1.9 Absolute values on fields ....................... 55  
   1.9.1 Absolute values .............................. 55  
   1.9.2 Extensions of absolute values ............... 58  
   1.9.3 Extensions of valuations ..................... 60  
   1.10 Divisor groups .................................. 71  
   1.10.1 Valuation properties of Dedekind domains .... 71  
   1.10.2 Local degrees in field extensions ............ 78  
   1.11 Different ........................................ 84  

2 Algebraic numbers ....................................... 91  
   2.1 Integral ideals .................................... 91  
   2.1.1 Factorization of ideals ........................ 91  
   2.1.2 The norm of an ideal .......................... 99
## Contents

2.2 Absolute values on number fields ........................................ 101
  2.2.1 Archimedean absolute values ........................................ 102
  2.2.2 Product formula ...................................................... 103
  2.2.3 Galois extensions of number fields .............................. 108
2.3 Discriminant of number fields ........................................... 109
2.4 Minkowski’s geometry of numbers ...................................... 112
  2.4.1 Minkowski’s first theorem ........................................ 112
  2.4.2 Minkowski’s bound ................................................. 116
  2.4.3 Dirichlet’s unit theorem ......................................... 120
  2.4.4 Minkowski’s second theorem ..................................... 123
2.5 Different of number fields ............................................... 124

3 Algebraic geometry .......................................................... 130
  3.1 Hermitian geometry ..................................................... 130
    3.1.1 Exterior product ................................................ 130
    3.1.2 Norms of vector spaces ....................................... 132
    3.1.3 Schwarz inequalities ........................................... 136
    3.1.4 General position ............................................... 140
    3.1.5 Hypersurfaces .................................................... 144
  3.2 Varieties .................................................................. 150
    3.2.1 Affine varieties ................................................. 150
    3.2.2 Projective varieties ............................................ 154
    3.2.3 Local rings of varieties ...................................... 156
    3.2.4 Dimensions ....................................................... 160
    3.2.5 Differential forms ............................................. 162
    3.2.6 Abelian varieties ............................................... 165
  3.3 Divisors .................................................................. 167
  3.4 Linear systems ........................................................... 173
  3.5 Algebraic curves .......................................................... 177
    3.5.1 Bézout’s theorem ................................................ 177
    3.5.2 Riemann–Roch theorem ....................................... 181
    3.5.3 Rational curves .................................................. 184
    3.5.4 Elliptic curves .................................................... 186
    3.5.5 Hyperelliptic curves ........................................... 194
    3.5.6 Jacobian of curves ............................................. 196
  3.6 Sheaves and vector bundles ............................................ 197
    3.6.1 Sheaves ............................................................. 197
    3.6.2 Vector bundles ................................................... 202
    3.6.3 Line bundles ....................................................... 206
    3.6.4 Intersection multiplicity ..................................... 209
  3.7 Schemes ................................................................ 212
    3.7.1 Schemes ............................................................ 212
3.7.2 Basic properties of schemes ........................................ 219
3.7.3 Sheaves of modules ................................................. 224
3.7.4 Differentials over schemes .......................................... 224
3.7.5 Ramification divisors ............................................... 226
3.8 Kobayashi hyperbolicity ................................................. 229
3.8.1 Hyperbolicity ....................................................... 229
3.8.2 Measure hyperbolicity ............................................... 232
3.8.3 Open problems ...................................................... 237

4 Height functions ............................................................. 239
4.1 Heights on projective spaces ............................................. 239
4.1.1 Basic properties ..................................................... 239
4.1.2 Heights on number fields .......................................... 242
4.1.3 Functional properties of heights ................................... 247
4.2 Heights of polynomials .................................................. 250
4.2.1 Coefficients for polynomials ....................................... 250
4.2.2 Gelfand's inequality ................................................. 255
4.2.3 Finiteness theorems ................................................ 259
4.3 Heights on varieties ..................................................... 264
4.4 Heights and Weil functions .............................................. 274
4.4.1 Weil functions ....................................................... 274
4.4.2 Heights expand Weil functions .................................... 278
4.4.3 Proximity functions ................................................ 280
4.5 Arakelov theory ............................................................ 283
4.5.1 Function fields ....................................................... 283
4.5.2 Number fields ....................................................... 286
4.6 Canonical heights on Abelian varieties ............................... 294
4.6.1 Periodic points ....................................................... 294
4.6.2 Canonical heights .................................................... 297
4.6.3 Tate–Shafarevich groups ........................................... 299
4.6.4 Mordell–Weil theorem .............................................. 301

5 The abc-conjecture ............................................................ 304
5.1 The abc-theorem for function fields .................................. 304
5.2 The abc-conjecture for integers ....................................... 306
5.3 Equivalent abc-conjecture .............................................. 308
5.4 Generalized abc-conjecture ............................................. 312
5.5 Generalized Hall’s conjecture ......................................... 315
5.6 The abc-conjecture for number fields ................................ 318
5.6.1 Generalizations of the abc-conjecture ............................ 318
5.6.2 Further formulations of the abc-conjecture ...................... 321
5.7 Fermat equations .......................................................... 323
## Contents

### 6 Roth’s theorem
- 6.1 Statement of the theorem ........................................... 328
- 6.2 Siegel’s lemma ......................................................... 331
- 6.3 Indices of polynomials .............................................. 335
- 6.4 Roth’s lemma .......................................................... 340
- 6.5 Proof of Roth’s theorem ............................................ 346
- 6.6 Formulation of Roth’s theorem .................................... 351
  - 6.6.1 A generalization .................................................. 351
  - 6.6.2 Approach infinity ................................................ 352
  - 6.6.3 Ramification term .............................................. 354
  - 6.6.4 Roth’s theorem and abc-conjecture ........................... 358

### 7 Subspace theorems
- 7.1 $p$-adic Minkowski’s second theorem ............................ 360
- 7.2 Adelic Minkowski’s second theorem .............................. 366
  - 7.2.1 Haar measures ................................................... 366
  - 7.2.2 Adèle rings ...................................................... 368
  - 7.2.3 Minkowski’s second theorem ................................ 371
- 7.3 Successive minima of a length function ....................... 379
- 7.4 Vojta’s estimate ...................................................... 386
- 7.5 Schmidt subspace theorem ........................................ 392
  - 7.5.1 Subspace theorem ............................................... 392
  - 7.5.2 Proof of subspace theorem .................................. 395
- 7.6 Cartan’s method ..................................................... 399
- 7.7 Subspace theorems on hypersurfaces ........................... 403
  - 7.7.1 Statements of theorems ....................................... 404
  - 7.7.2 Proof of Theorem 7.35 ....................................... 406

### 8 Vojta’s conjectures
- 8.1 Mordellic varieties .................................................. 415
- 8.2 Main conjecture ...................................................... 420
- 8.3 General conjecture .................................................. 424
- 8.4 Vojta’s $(1, 1)$-form conjecture ................................. 429
- 8.5 abc-conjecture implies Vojta’s height inequality ............ 432

### 9 $L$-functions
- 9.1 Dirichlet series ..................................................... 434
  - 9.1.1 Abscissa of convergence .................................... 434
  - 9.1.2 Riemann’s $\zeta$-function .................................. 436
  - 9.1.3 Dirichlet’s characters ........................................ 443
  - 9.1.4 Dirichlet’s $L$-functions .................................... 446
  - 9.1.5 Zeros of Dirichlet’s $L$-functions ......................... 449
- 9.2 The Dedekind zeta-function ..................................... 454
9.2.1 The $\zeta$-functions of number fields .......................... 454
9.2.2 Selberg class ........................................ 456
9.3 Special linear groups ........................................ 459
  9.3.1 General linear groups .................................. 459
  9.3.2 Modular groups ....................................... 461
9.4 Modular functions ........................................... 464
  9.4.1 Automorphic forms ................................... 464
  9.4.2 Weierstrass $\wp$ function .......................... 466
  9.4.3 Elliptic modular functions ............................ 468
  9.4.4 Hecke’s theorem ..................................... 470
9.5 Modular forms ............................................. 475
  9.5.1 Modular forms for $\text{SL}(2,\mathbb{Z})$ .................. 475
  9.5.2 Modular forms for congruence subgroups ............... 478
  9.5.3 Hecke operator ....................................... 480
  9.5.4 Hecke’s $L$-series .................................. 483
  9.5.5 Modular representations ............................... 484
9.6 Hasse–Weil $L$-functions ................................... 485
9.7 $L$-functions of varieties .................................. 490
  9.7.1 $L$-functions of $\mathbb{P}^N$ ............................ 492
  9.7.2 $L$-functions of Abelian varieties .................... 493

Bibliography .................................................. 495

Symbols ....................................................... 511

Index .......................................................... 515
Chapter 1

Field extensions

In this chapter, we will introduce some basic notations, terminologies and theorems about fields and algebraic geometry, which will be used in this book.

1.1 Groups

We denote the fields of complex, real, and rational numbers by $\mathbb{C}$, $\mathbb{R}$, and $\mathbb{Q}$, respectively, and let $\mathbb{Z}$ be the ring of integers. If $\kappa$ is a set, we write

$$\kappa^n = \{(x_1, \ldots, x_n) \mid x_i \in \kappa\} = \kappa \times \cdots \times \kappa \ (n \text{ times}).$$

If $\kappa$ is partially ordered, denote

$$\kappa(s, r) = \{x \in \kappa \mid s < x < r\}, \quad \kappa(s, r] = \{x \in \kappa \mid s < x \leq r\},$$

$$\kappa[s, r) = \{x \in \kappa \mid s \leq x < r\}, \quad \kappa[s, r] = \{x \in \kappa \mid s \leq x \leq r\},$$

$$\kappa_+ = \kappa[0, \infty), \quad \kappa^+ = \kappa(0, \infty).$$

For example, $\mathbb{Z}[s, r]$ means the set of integers $i$ satisfying $s \leq i \leq r$, $\mathbb{R}^+$ is the set of positive real numbers, and so on.

1.1.1 Abelian groups

Let $G$ be an Abelian group with a rule of composition by multiplication. If the group contains infinitely many different elements it is called an infinite group; otherwise it is called a finite group of order $h$, where $h$ is the number of its elements. Now in case $G$ is a finite group of order $h$, then the order $N$ of a subgroup $H$ is also finite and then the number of different cosets $gH$ for each $g \in G$ is also finite, say $= j$. Since each element of $G$ occurs in exactly one coset and exactly $N$ different elements are contained in each coset, we have $h = jN$, and thus we have shown

**Proposition 1.1.** In a finite group of order $h$, the order $N$ of each subgroup is a divisor of $h$. 

The quotient \( h/N = j \) is called the index of the subgroup relative to \( G \). In case \( G \) is an infinite group, then the order of \( H \) as well as the number of different cosets can be infinite and at least one of these cases must obviously occur. Furthermore, the number of different cosets in a group \( G \) determined by a subgroup \( H \) of \( G \) is called the index of \( H \) in \( G \) whether this index is finite or not.

If \( G \) is a finite group of order \( h \), all powers of an element \( g \) with a positive exponent always form a subgroup of \( G \). These powers cannot all be different. From \( g^m = g^n \) it follows that \( g^{m-n} = 1 \) (unit of \( G \)). Hence a certain power of \( g \) with exponent different from zero is always \( = 1 \), say \( g^l = 1 \). These \( l \) are identical with all multiples of an integer \( t \) \((> 0)\). This exponent \( t \), uniquely determined by \( g \), is called the order of \( g \). Consequently among the powers of \( g \) there are only \( t \) different ones, say, \( g^0 = 1, g^1, \ldots, g^{t-1} \), and by the above these form a subgroup of \( G \) of order \( t \). Moreover from Proposition 1.1 we obtain

**Theorem 1.2.** The order \( a \) of each element of a finite group \( G \) is a divisor of the order \( h \) of \( G \) and hence \( g^h = 1 \) for each element \( g \in G \).

Now we state the fundamental theorem of Abelian groups which gives us full information about the structure of the finite Abelian group (cf. [95]).

**Theorem 1.3.** In each Abelian group \( G \) of order \( h \) \((> 1)\) there are certain elements \( w_1, \ldots, w_n \) with orders \( h_1, \ldots, h_n \) respectively \((h_i > 1)\) such that each element of \( G \) is obtained in exactly one way in the form

\[
v = w_1^{k_1} w_2^{k_2} \cdots w_n^{k_n},
\]

where the integers \( k_i \) each run through a complete system of residue \( \mod h_i \) independently of one another. Moreover the \( h_i = p_1^{l_i} \) are prime powers and \( h = h_1 h_2 \cdots h_n \).

The \( n \) elements of this kind are called a basis of \( G \). To prove next theorem, we need a fact from number theory. A system \( S \) of integers is a module if it contains at least one number different from 0 and if among with \( m \) and \( n \), \( m + n \) and \( m - n \) also always belong to \( S \). A general theorem about modules states that the numbers in a module \( S \) are identical with the multiples of certain number \( d \). The number \( d \) is determined by \( S \) up to the factor \( \pm 1 \).

**Theorem 1.4.** If an infinite Abelian group \( G \) has a finite basis, then each subgroup of \( G \) also has a finite basis.

**Proof.** Let \( w_1, w_2, \ldots, w_n \) be a basis of \( G \) where \( w_1, \ldots, w_m \) are the elements of infinite order and \( w_{m+1}, \ldots, w_n \) are those of order \( h_1, \ldots, h_{n-m} \). We consider the set \( I \) of exponents \((k_1, \ldots, k_n)\) of all products of powers

\[
v = w_1^{k_1} \cdots w_n^{k_n}
\]
which belong to a subgroup $H$ of $G$, where, in addition, the last $k_{m+1}, \ldots, k_n$ are to run through all numbers, not just the numbers which are distinct mod $h_i$, as long as the product belongs to $H$. By the group property of $H$, however, we obviously have that for exponents $(k_1, \ldots, k_n)$ and $(k'_1, \ldots, k'_n)$ in $I$, the exponents $(k_1 + k'_1, \ldots, k_n + k'_n)$ and $(k_1 - k'_1, \ldots, k_n - k'_n)$ also correspond to elements $v$ in $H$. In particular, we keep in mind the elements

$$v = w_i^{k_i} w_{i+1}^{k_{i+1}} \cdots w_n^{k_n} \quad (1 \leq i \leq n)$$  \hspace{1cm} (1.1)$$

belonging to $H$ for a definite $i$, thus for which $k_1 = \cdots = k_{i-1} = 0$. There are such elements, since if all $k_i = 0$ the unit element of $H$ is obtained. The totality of possible first exponents $k_i$ in (1.1) forms a module of integers, as long as we do not always have $k_i = 0$. However, all numbers of this module are identical with the multiples of a certain integer; consequently, if we do not always have $k_i = 0$, there is an element $v_i$ in $H$ with one such $r_{ii} \neq 0$,

$$v_i = w_i^{r_{ii}} w_{i+1}^{r_{i,i+1}} \cdots w_n^{r_{in}},$$

such that $k_i$ in (1.1) is a multiple of this $r_{ii}$. From the $v_i$ with this $r_{ii}$ (possibly infinite in number), we pick out a definite one for each $i = 1, \ldots, n$, where we set $v_i = 1$ and $r_{ii} = 0$ in case we always have $k_i = 0$ for this $i$ in (1.1).

We show that each element in $H$ is representable as a product of these elements $v_1, \ldots, v_n$. Let $v = w_1^{k_1} \cdots w_n^{k_n}$ be an element of $H$. By the preceding discussion, $k_1$ is a multiple of $r_{11}$, $k_1 = j_1 r_{11}$, and hence

$$v v_1^{-j_1} = w_2^{k_2'} w_3^{k_3'} \cdots w_n^{k_n'}$$  \hspace{1cm} (1.2)$$

is a product only of powers of $w_2, \ldots, w_n$, which also belongs to $H$ by the group property. If we should have $r_{11} = 0$ and $v_1 = 1$, then we should take $j_1 = 0$. Likewise, in (1.2), $k'_2$ must be a multiple of $r_{22}$ in case this element is $\neq 0$, $k'_2 = j_2 r_{22}$. Moreover if $r_{22} = 0$ then $k'_2$ must be $0$ and we take $j_2 = 0$. In any case then $v v_1^{-j_1} v_2^{-j_2}$ is an element of $H$ and representable as product of powers only of $w_3, \ldots, w_n$ etc. until we arrive at the unit element and obtain a representation

$$v = v_1^{j_1} v_2^{j_2} \cdots v_n^{j_n}.$$  

The $v_1, \ldots, v_m$ are of infinite order if they are $\neq 1$, the other $v$’s are of finite order.

The products of powers of the $v_{m+1}, \ldots, v_n$ form a finite Abelian group and can hence be represented by a basis $u_1, \ldots, u_q$, by Theorem 1.3. We assert that $v_1, \ldots, v_m, u_1, \ldots, u_q$ form a basis for $H$ if we omit the elements $v_i = 1$. First, each element can be represented by the $v_1, \ldots, v_n$, hence also by the $v_1, \ldots, v_m, u_1, \ldots, u_q$. Now if

$$v_1^{a_1} v_2^{a_2} \cdots v_m^{a_m} u_1^{b_1} \cdots u_q^{b_q} = 1$$  \hspace{1cm} (1.3)$$
is a representation of the unit element where \( a_i = 0 \) is assumed for \( v_i = 1 \) (i.e., \( r_{ii} = 0 \)), then by substitution of the \( w_i \) in place of the \( v_i \) and \( u_j \), it follows that \( a_1 r_{11} = 0 \); hence either \( a_1 = 0 \) or \( r_{11} = 0 \). However, in the latter case we also have \( a_1 = 0 \) as a consequence of our convention. Likewise \( a_2 = 0, \ldots, a_m = 0 \).

Furthermore, since the \( u_j \) form a basis of the finite group, then in (1.3) each \( b_j \) must be a multiple of the order of \( u_j \). Now since each element is represented the same number of times by the \( v_i \) as by the \( u_i \), hence the same number of times as the unit element, these elements actually form a basis for \( H \) as was to be proved.

Those infinite Abelian groups in which no element of finite order except the unit 1 appears are of chief interest. We call such groups torsion-free groups, the others mixed groups. Along with a torsion-free group \( G \), each subgroup of \( G \) is also torsion-free. In particular, let \( H \) be a subgroup of \( G \) of finite index. Then a certain power of each element of \( G \) with exponent different from zero must always belong to \( H \). For if \( g \) is an element of \( G \), then the cosets

\[ gH, \ g^2H, \ldots, \ g^mH, \ldots \]

are not all distinct, since the index is assumed to be finite. Thus for some \( n \), \( g^nH = g^mH \), that is, \( g^{n-m} \in H \) with \( n - m \neq 0 \). Hence in the proof of Theorem 1.4 applied to \( G \) and \( H \), the case \( r_{ii} = 0, v_i = 1 \) can obviously never occur, since, in fact, a system of values \( k_i \neq 0, k_{i+1} = \cdots = k_n = 0 \) always exists, so that \( v_i = w_i^{k_i} \in H \). From this we have immediately

**Theorem 1.5.** If \( G \) is a torsion-free Abelian group with finite basis \( w_1, \ldots, w_n \), then every subgroup \( H \) of \( G \) with finite index has a basis \( v_1, \ldots, v_n \) of the form

\[ v_i = \prod_{j=i}^{n} w_j^{r_{ij}}, \]

with \( r_{ii} \neq 0 \) for \( i = 1, 2, \ldots, n \).

It is not difficult to show that the index of \( H \) in \( G \) is just \( j = |r_{11}r_{22} \cdots r_{nn}| \) (see [95], Theorem 36).

**Theorem 1.6.** If a torsion-free Abelian group \( G \) has a finite basis of \( n \) elements \( w_1, \ldots, w_n \), then \( n \) is the maximal number of independent elements of \( G \), independent of the choice of basis.

**Proof.** Since the \( w_1, \ldots, w_n \) are independent in any case, there are \( n \) independent elements in \( G \) and thus we need only show that \( n + 1 \) elements in \( G \) are not independent. In fact, between \( n + 1 \) arbitrary elements

\[ v_i = w_1^{a_{i1}} w_2^{a_{i2}} \cdots w_n^{a_{in}} \quad (i = 1, 2, \ldots, n + 1), \]
there is the relation
\[ v_1^{x_1}v_2^{x_2}\cdots v_{n+1}^{x_{n+1}} = 1, \]
if we choose the \( n + 1 \) integers \( x_i \) so that they satisfy the \( n \) linear homogeneous equations
\[
\sum_{i=1}^{n+1} a_{ij} x_i = 0 \quad (j = 1, 2, \ldots, n).
\]
As is known this is always possible since the coefficients \( a_{ij} \) are integers. \( \square \)

**Theorem 1.7.** From a basis \( w_1, \ldots, w_n \) of a torsion-free Abelian group \( G \) one can obtain all systems of bases \( w_1', \ldots, w_n' \) of \( G \) in the form
\[
w_i' = \prod_{j=1}^{n} w_j'^{a_{ij}}, \quad i = 1, 2, \ldots, n
\]
where the system of the exponents are arbitrary integers \( a_{ij} \) with determinant \( \pm 1 \).

**Proof.** Note that the \( w_i' \) always form a basis. To see this we need only show that the \( w_i \) can be represented through the \( w_i' \). The equation
\[
w_j = w_1^{x_{j1}}w_2^{x_{j2}}\cdots w_n^{x_{jn}}
\]
is satisfied if the integers \( x_{jk} \) are chosen so that the \( n \) equations
\[
\sum_{j=1}^{n} a_{ij} x_{jk} = \begin{cases} 
0, & \text{if } i \neq k, \\
1, & \text{if } i = k 
\end{cases}
\]
hold. Since the determinant of the (integral) coefficients is \( \pm 1 \) and the right side is also integral, the \( x_{jk} \) are uniquely determined integers.

Secondly, if \( n \) elements
\[
w_i' = \prod_{j=1}^{n} w_j'^{a_{ij}}, \quad i = 1, 2, \ldots, n
\]
form a basis, then \( w_j \) must be represented through the \( w_i' \),
\[
w_j = w_1^{b_{j1}}w_2^{b_{j2}}\cdots w_n^{b_{jn}}, \quad j = 1, 2, \ldots, n,
\]
if the \( w_j \) are substituted for the \( w_i' \), then the \( n^2 \) equations
\[
\sum_{j=1}^{n} a_{ij} b_{jk} = \begin{cases} 
0, & \text{if } i \neq k, \\
1, & \text{if } i = k 
\end{cases}
\]
are obtained, by the basis property of the $w'_i$. The determinant of this array is thus $= 1$; on the other hand, however, by the multiplication theorem of determinant theory, the determinant is equal to the product of the two determinant $\det(a_{ij})$ and $\det(b_{jk})$. Hence each of these integers must divide 1, and therefore each integer is itself $= \pm 1$; thus $\det(a_{ij}) = \pm 1$.

By Theorem 1.7 and the remark after Theorem 1.5, we obtain

**Theorem 1.8.** If $G$ is a torsion-free Abelian group with a finite basis $w_1, \ldots, w_n$, then every subgroup $H$ of $G$ with finite index $j$ has a basis $v_1, \ldots, v_n$, and the determinant $\det(a_{ij})$ in the $n$ equations

$$v_i = \prod_{j=1}^{n} w_j^{a_{ij}}, \quad i = 1, 2, \ldots, n$$

is always equal to $j$ in absolute value.

**Theorem 1.9.** If $G$ is a group with a finite basis $w_1, \ldots, w_n$, then a subgroup $H$ is of finite index if and only if a power of each element of $G$ belongs to $H$.

**Proof.** If the $h_i$-th power ($h_i > 0$) of $w_i$ belongs to $H$ and if we set

$$h = h_1 h_2 \cdots h_n,$$

then $w_i^h$ also belongs to $H$ and consequently the $h$-th power of each element likewise belongs to $H$. Hence each element of $G$ differs from some $w_1^{x_1} w_2^{x_2} \cdots w_n^{x_n}$ ($0 \leq x_i < h$) by a factor in $H$; therefore there are at most $h^n$ different cosets, represented by the above elements. Thus the index of $H$ is finite.

Conversely, in the case of a finite index the infinitely many cosets $gH, g^2H, g^3H, \ldots$ cannot all be distinct for each $g \in G$, thus a power of $g$ must belong to $H$.  

Let $\Gamma = (\Gamma, +, \leq)$ be a totally ordered Abelian additive group. This means that the order relation $\leq$ on $\Gamma$ satisfies:

1. $\alpha \leq \beta$ implies $\alpha + \gamma \leq \beta + \gamma$ for any $\alpha, \beta, \gamma \in \Gamma$.
2. For each $\alpha, \beta \in \Gamma$ either $\alpha \leq \beta$ or $\beta \leq \alpha$.

Special cases occur when $\Gamma$ is a subgroup of $\mathbb{R}$. This happens if and only if the Archimedean property holds:

3. If $\alpha > 0$, for every $\beta \in \Gamma$ there exists a natural number $n$ such that $n\alpha > \beta$. 

Lemma 1.10. If $\Gamma$ is a totally ordered Abelian additive group satisfying the Archimedean property, then it is order-isomorphic to a subgroup of the ordered additive group $\mathbb{R}$.

Proof. See P. Ribenboim [215], Lemma 1 on page 60. \hfill $\square$

1.1.2 Galois cohomology

Let $G$ be a (finite or topological) group acting on another Abelian group $A$ (endowed with the discrete topology). Denote the action of $G$ on $A$ by

$$G \times A \longrightarrow A, \quad (\sigma, a) \longmapsto \sigma(a).$$

By the definition, we have the relations

$$(\sigma\tau)(a) = \sigma(\tau(a)), \quad 1(a) = a$$

for $\sigma, \tau \in G, a \in A$, where $1$ is the unit of $G$.

The cohomology groups of $G$ with coefficients in $A$ are defined with the help of the complex of cochains. Consider the following Abelian groups:

$$C^0(G, A) = A,$$

and for $n \geq 1$,

$$C^n(G, A) = \{ f : G^n \longrightarrow A \mid f \text{ is continuous} \},$$

where the continuity of $f \in C^n(G, A)$ means that the function $f(\sigma_1, \ldots, \sigma_n)$ depends only on a coset of $\sigma_i$ modulo some open subgroup of $G$. More precisely, if $f, g : G^n \longrightarrow A$ are two continuous mappings, we define their sum by the rule

$$(f + g)(\sigma_1, \ldots, \sigma_n) = f(\sigma_1, \ldots, \sigma_n) + g(\sigma_1, \ldots, \sigma_n).$$

It is clear from the commutativity of $A$ that $f + g$ is again an element of $C^n(G, A)$, so it forms a group.

We define a homomorphism $d_n : C^n(G, A) \longrightarrow C^{n+1}(G, A)$ by the formula

$$(d_nf)(\sigma_1, \ldots, \sigma_{n+1}) = \sigma_1(f(\sigma_2, \ldots, \sigma_{n+1})) + (-1)^{n+1}f(\sigma_1, \ldots, \sigma_n)$$

$$+ \sum_{i=1}^n (-1)^i f(\sigma_1, \ldots, \sigma_i \sigma_{i+1}, \ldots, \sigma_{n+1})$$

such that $d_{n+1} \circ d_n = 0$. The group

$$Z^n(G, A) = \text{Ker}(d_n)$$
is called the group of \( n \)-cocycles, and the group
\[
B^n(G, A) = \text{Im}(d_{n-1})
\]
is called the group of \( n \)-coboundaries. The property \( d_{n+1} \circ d_n = 0 \) implies that
\[
B^n(G, A) \subseteq Z^n(G, A).
\]
The \( n \)-th cohomology group of \( G \) acting on \( A \) is then defined by
\[
H^n(G, A) = Z^n(G, A) / B^n(G, A).
\]
If \( n = 0 \), the 0-th cohomology group of \( G \) is the group
\[
H^0(G, A) = \{ a \in A \mid \sigma(a) = a \text{ for all } \sigma \in G \}
\]
of elements of \( A \) that is fixed by every element of \( G \). For \( n = 1 \), we find that a continuous mapping \( f : G \to A \) is a 1-cocycle if and only if for all \( \sigma, \tau \in G \) one has
\[
f(\sigma \tau) = f(\sigma) + \sigma(f(\tau)).
\]
Obviously, we have
\[
B^1(G, A) = \text{Im}(d_0) = \{ d_0 a \mid a \in A \},
\]
where, by the definition,
\[
(d_0 a)(\sigma) = \sigma(a) - a, \quad \sigma \in G.
\]
Two 1-cocycles \( f, g \) from \( G \) to \( A \) are said to be cohomologous if there exists an \( a \in A \) such that each \( \sigma \in G \) satisfies
\[
g(\sigma) - f(\sigma) = \sigma(a) - a.
\]
This is an equivalence relation, and 1-th cohomology group \( H^1(G, A) \) of \( G \) acting on \( A \) is just the set of cohomology classes of 1-cocycles.

Let \( A' \) be other Abelian group on which \( G \) acts and let \( \varphi : A \to A' \) be a \( G \)-homomorphism, that is, a homomorphism that commutes with the action of \( G \). Then \( \varphi \) induces a natural homomorphism
\[
\varphi_* : H^1(G, A) \to H^1(G, A')
\]
defined by \( \varphi_*([f]) = [\varphi \circ f] \) for any \([f] \in H^1(G, A)\).

Let \( \Phi : G' \to G \) be a homomorphism. Then \( G' \) acts on \( A \) via \( \Phi \), and this induces a natural homomorphism
\[
\Phi^* : H^1(G, A) \to H^1(G', A)
\]
defined by \( \Phi^*([f]) = [f \circ \Phi] \) for any \([f] \in H^1(G, A)\).