Basic Algebraic Number Theory

Uwe Kraeft

2006

Berichte aus der Mathematik

Uwe Kraeft

Basic Algebraic Number Theory

Shaker Verlag
Aachen 2006

Bibliographic information published by Die Deutsche Bibliothek
Die Deutsche Bibliothek lists this publication in the Deutsche Nationalbibliografie; detailed bibliographic data is available in the internet at http://dnb.ddb.de.

Printed in Germany.

ISBN 3-8322-4951-6
ISSN 0945-0882

Shaker Verlag GmbH • P.O. BOX 101818 • D-52018 Aachen
Phone: 0049/2407/9596-0 • Telefax: 0049/2407/9596-9
Internet: www.shaker.de • eMail: info@shaker.de

Preface

Today, algebra is an own discipline of pure mathematics. Algebraic number theory comprises great parts of algebra, algebraic geometry, and algebraic topology; the two latter are, in simplified way, the disciplines where one original has different maps, like f.e. in curves. Algebra with its branches is perhaps the most growing part of mathematics because other disciplines, like f.e. infinitesimal calculus, have got less importance by the use of computers for numerical approximations. In number theory and algebra, exact theorems, algorithms, and solutions are needed. While theorems are most powerful, the algorithms to find solutions have greatest importance in applications. For proofs, also here, computers can be used, what is discussed in our days because in this case the program itself is the proof and you have to verify that all possible ways are checked.

The most important and fundamental result of modern algebra is the new definition of old and new numbers. In former times, these were developed step by step for practical use. Later, the characteristics were found which led to axioms for the different types of natural numbers, integers, rational numbers, real number symbols and algorithms, complex numbers, quaternions, hypercomplex numbers, vectors, tensors, matrices, and others. Once these axioms have been available, you could characterize new numbers in combining different axioms.

This text is a summary of basic algebraic methods which are used in number theory. It is neither a textbook of algebra nor of number theory; otherwise, a great part of algebra is treated here.

I would appreciate discussions, remarks, and hints if there are mistakes.

Leimen, in January 2006 Uwe Kraeft

Choice of symbols

$\Rightarrow$, $\Leftarrow$, $\Leftrightarrow$	by this follows (in the given directions)
$\forall$	for all
$\exists$	there is/are
$\in$	is element of (is contained in)
$\cap$, $\cup$, $\subset$	intersection, union, is contained in = is subset of
$A=\{a,b,c\}$	an example of a set A with elements a, b, and c
$-a$, b^{-1}	inverse elements
N	set of natural numbers 1, 2, 3, ... or any natural number
P	primes of N 2, 3, 5, ...
N^0	$N \cup \{0\}$
N^-	$\{-n; n \in N\}$, set of negative integers -1, -2, -3, ...
Z	$=N \cup \{N^-\} \cup \{0\}$, set of integers
Q	set of rational numbers a/b with $a \in Z$, $b \in N$
R	set of real number algorithms
Q(R,C)	Q or R or C (C complex numbers a+bi with $a,b \in Z(Q,R)$)
Q(t)	adjunction of element t to Q
$\underset{\sim}{x}$, $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$	vector $\underset{\sim}{x}$, matrix **A**
$A(+,*)$	$=(A^{+,*})$ algebraic structure with two operations (see below)
$GL_2(R)$	general linear group (see below)
$SL_2(R)$	special linear group (see below)
Γ	full modular group
$\Gamma_0(N)$	example of a congruence subgroup of Γ (see below)
$M_k(\Gamma)$	modular forms of weight k for Γ (see below)
$S_k(\Gamma)$	cusp-forms of weight k for Γ (see below)
E, E_l	elliptic curve, elliptic curve modulo l
=	equal (identical) by axioms or definitions
$\cong$	so near as you want but not identical
$\approx$	about, rounded, can f.e. be approximated for great n
$\equiv$	$a \equiv b \pmod{c} \Leftrightarrow a \equiv b_c \Leftrightarrow (a-b)/c \in Z$ for $a,b \in Z$, $c \in N$
im	image
PT	Pythagorean Triple
FLT	Fermat's Last Theorem
gcd	greatest common divisor
lcm	least common multiple
det	determinant

Basic mappings used in this text (see chapter 2)

mapping: $F: a\in A \rightarrow \alpha\in\Omega$
surjection: $\forall\ \alpha\in\Omega\ \ \exists a\in A$ with $F(a)=\alpha$
injection: $F(a)=F(b) \Rightarrow a=b$
bijection: F is injective and surjective

morphisms (for one or more operations)
homomorphism: Hom: surjective mapping with $\varphi(a+b)=\varphi(a)\oplus\varphi(b)$
endomorphism: Hom: $A \rightarrow A$
isomorphism: Iso: bijective Hom
automorphism: Iso: $A \rightarrow A$
kernel of Hom: $\ker(\varphi)=\{a\in A$ with $\varphi(a)=0\}$

operation: O: $a_1,a_2,\ldots\in A \rightarrow \alpha\in\Omega$ or $b\in A$
number: element of a set with operation

Basic algebraic structures used in this text (see chapter 2)

Axioms of sets S with operations addition A „+“ (or multiplication M „*“)
$\forall a,b,c,x\in S$

A1/M1 $a+b\in S$ (set S closed with operation)
A2/M2 $(a+b)+c=a+(b+c)$ (associative law of operation)
A3/M3 $a+b=b+a$ (commutative law of operation)
A4a $\exists 0\in S$ such that $0+a=a$ (existence of a left neutral element: zero)
A4b $\exists x=-a\in S$ such that $x+a=0$ (existence of left inverses)
A4c $\exists x\in S$ with $a+x=b$ ($\Rightarrow$ **A4a, A4b**)
A4d $\exists x\in S$ with $x+a=b$ ($\Rightarrow$ **A4a, A4b**)
A4 $a,b\in S'$, $-b\in S$, $a+(-b)\in S'\subset$(S with **A4a, A4b**) ($\Rightarrow$ S′: **A4a, A4b**)
M4a $\exists 1\in S$ such that $1*a=a$ (existence of a left neutral element: unity)
M4b $\forall a\neq 0\ \exists x=a^{-1}\neq 0\in S$ such that $a^{-1}*a=1$ (existence of left inverses)
M4c $\forall a\neq 0\ \exists x\in S$ with $a*x=b$ ($\Rightarrow$ **M4a, M4b**)
M4d $\forall a\neq 0\ \exists x\in S$ with $x*a=b$ ($\Rightarrow$ **M4a, M4b**)
M4 $a,b\neq 0\in S'$, $b^{-1}\in S$, $a*b^{-1}\in S'\subset$(S with **M4a, M4b**) ($\Rightarrow$ S′: **M4a, M4b**)

D	**D1** $a*(b+c)=a*b+a*c$, **D2** $(b+c)*a=b*a+c*a$ (distributive laws)
Z	from $a*b=0$ follows at least $a=0$ or $b=0$ (zero divisor free)
U	$1\neq 0$

one inner operation + (or * in **M1**, ...)

groupoid:	**A1**	
semigroup:	**A1, A2**	
monoid:	**A1, A2,**	**A4a**
module:	**A1,**	**A4a, A4b**
group *G*:	**A1, A2,**	**A4a, A4b**
Abelian group *AG*:	**A1, A2, A3,**	**A4a, A4b**

subgroup *B* of *A*	$B\subset A$ and A, B are groups
normal subgroup *N* (normal divisor *N*)	N is a subgroup of a group A; $\forall\ n\in N$ and $a\in A$, it is $a^{-1}na\in N$
coset of *B* in *A*:	aB $(Ba)=\{a*b\ (b*a);\ (\text{given})\ a\in A,\ b\in B\}$
quotient group	$A/N=\{aN\colon a\in A\}$ (A modulo N)
chain complex	sequence of Abelian groups or modules A_0, A_1, A_2, ... which are connected by homomorphisms $d_n\colon A_n\rightarrow A_{n-1}$ such that the composition of two consecutive maps is zero
cochain complex	sequence of Abelian groups or modules A_0, A_1, A_2, ... which are connected by homomorphisms $d_n\colon A_n\rightarrow A_{n+1}$ such that the composition of two consecutive maps is zero

general linear group: $GL_2(R)=\{g=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $\det g=ad-bc\in R^*\}$ (R^* is the multiplicative group of „invertible" elements from the commutative ring R with unity, f.e. Z, Q, C, all without zero)

special linear group: $SL_2(R)=\{g=\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with $\det g=ad-bc=1\}$

two inner operations + and *

ring *R*:	***AG*, M1, M2,**		**D**
commutative ring:	***AG*, M1, M2, M3,**		**D**
ring with unity :	***AG*, M1, M2,**	**M4a,**	**D**
zero div. free ring:	***AG*, M1, M2,**	**M4a,**	**D, Z**
integral domain:	***AG*, M1, M2, M3,**	**M4a,**	**D, Z, U**
skew field:	***AG*, M1, M2,**	**M4a, M4b,**	**D, Z, U**
field *K,F*:	***AG*, M1, M2, M3,**	**M4a, M4b,**	**D, Z, U**

polynomial over *R,K*: $\sum_{i=0}^{n} a_i x^i = a_0x^0+a_1x^1+a_2x^2+ \ldots +a_nx^n$, $a_i \in R,K$, $i,n \in N^0$

ideal *I* over a ring *R*: *AG*, from $a \in I \subset R$ and $r \in R$ follows $a*r \in I$ ($r*a \in I$)

extension field *K*(t): $t, t*t, t*t*t*\ldots = t^n \in K(t)$, $t \in K(t)$, $t \notin K$

residue class $[a]_m$: $a=n*m+r$ or $(a+(-r))*m^{-1}=n$ or $a \equiv r_m$
for $a,n,(m \neq 0),m^{-1},r \in K$

inner and outer operations

vector $\underline{a} \in V$ over *R,K*: *AG* with addition for $\underline{a} \in V$ (vector space)
M1′ $h*\underline{a} \in V$
M2′ $(hk)*\underline{a} = h*(k*\underline{a})$
M4a′ $e*\underline{a} = \underline{a}$
D′ $h*(\underline{a}+\underline{b}) = h*\underline{a}+h*\underline{b}$, $(h+k)*\underline{a} = h*\underline{a}+k*\underline{a}$
for $\underline{a},\underline{b} \in V$ and $h,k,e \in R,K$

linear combination: $\sum_{i} h_i * \underline{a}_i$ for $\underline{a}_i \in V$ and $h_i \in R,K$, $i \in N$

linear form *L*: $V \rightarrow K$
D′ $L(\underline{a}+\underline{b}) = L(\underline{a})+L(\underline{b})$
D″ $L(h*\underline{a}) = hL(\underline{a})$ for $\underline{a},\underline{b} \in V$ and $h \in K$

matrix *M*: *V* $(a_{hkl\ldots})$ with $a_{hkl\ldots} \in R,K$

algebra *A* over *K*: *R* with inner addition and inner multiplicat.
V with inner addition and outer multiplicat.
M1′ $h*a \in A$
M2′ $h*(ab) = (h*a)b = a(h*b)$
for $a,b \in A$ and $h \in K$

Simplified basic definitions of function theory and algebraic geometry (see chapter 15)

holomorphic (analytic) function

function f(z) defined on an open subset of complex numbers C with values in C which are complex differentiable at every point z_0 by existing $f'(z_0)=\lim_{z\to z_0}\frac{f(z)-f(z_0)}{z-z_0}$

meromorphic function

function f(z) defined on an open subset D of complex numbers C with values in C which is holomorphic on all points of D without one or more isolated points which are poles of the function = ratio of two holomorphic functions with a denominator which is not always zero; the poles are given by the zeros of the denominator

fractional linear transformation of the Riemann sphere $\tilde{C}=C\cup\{\infty\}$

$gz=\frac{az+b}{cz+d}$; $g\infty=a/c=\lim_{z\to\infty}gz$; $g=\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in SL_2(R)$, $z\in C$

full modular group

$\Gamma=\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in SL_2(Z)\}$

congruence subgroups of Γ of level N

principal congruence subgroup of level N:

$\Gamma(N)=\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in\Gamma,|\ a\equiv d\equiv 1_N,\ b\equiv c\equiv 0_N\}$,

$\Gamma_0(N)=\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in\Gamma,|\ c\equiv 0_N\}$, $\Gamma_1(N)=\{\begin{pmatrix} a & b \\ c & d \end{pmatrix}\in\Gamma_0(N)|\ a\equiv 1_N\}$

modular function of weight $k \in N$ for Γ
meromorphic function f(z) of complex numbers on the upper half-plane $H \subset C$ with $g=\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(Z)$, b,d>0, and $f(gz)=(cz+d)^k f(z)$; with Fourier series $f(z) \cong \sum_{n \in Z} a_n e^{2\pi i n z}$ and a finite number of $a_n \neq 0$ for $n<0$

modular forms of weight $k \in N$ for Γ: $M_k(\Gamma)$
holomorphic function f(z) (also for $z \to i\infty$) of complex numbers on the upper half-plane $H \subset C$ with $g=\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(Z)$, b,d>0, and $f(gz)=(cz+d)^k f(z)$; with Fourier series $f(z) \cong \sum_{n \in Z} a_n e^{2\pi i n z}$ and $a_n=0$ for $n<0$; if $a_0=0$, f(z) is called cusp-form of weight k for Γ: $S_k(\Gamma)$

modular form of weight $k \in N$ of level group $\Gamma_0(N)$
holomorphic function f(z) (also for $z \to i\infty$) of complex numbers in the upper half-plane $H \subset C$ with $g=\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N)$, b,d>0, and $f(gz)=(cz+d)^k f(z)$; with Fourier series $f(z) \cong \sum_{n=0}^{\infty} a_n e^{2\pi i n z}$

general modular forms
generalizations allow numbers k other than integers and factors ε of the map: $\varepsilon(cz+d)^k f(z)$

Basic definition of algebraic topology (see also [Kr8 p. 53])

homology	method to associate a sequence of Abelian groups or modules with an algebraic structure
n^{th} homology group	$H_n(X)=\ker(d_n)/\mathrm{im}(d_{n+1})$
cohomology	sequence of Abelian groups from a cochain complex
group cohomology	study of groups by a sequence of functors H^n
Galois cohomology	group cohomology of Galois modules

homotopic, homotopy
the maps of two continuous mappings $f,g: X \rightarrow Y$ are called homotopic (f to g) if there exists a continuous mapping $\Phi_t: X * I \rightarrow Y$ $(t \in I=[0,1] \subset Q)$ such that $\Phi_0=f$ and $\Phi_1=g$: Φ is called the homotopy between f and g

f.e.	for example (e.g.)

Content