1

Basics of constructive algebraic number theory

1.1. Introduction

Algebraic numbers are defined as complex numbers x satisfying an *algebraic equation* of the form

$$a_0x^n + a_1x^{n-1} + \cdots + a_n = 0 \ (n\in\mathbb{N}; a_i\in\mathbb{Z} \ (0 \leqslant i \leqslant n), a_0 \neq 0). \qquad (1.1)$$

We are not satisfied merely with the existence of algebraic numbers such as, for instance,

the natural numbers $1, 2, 3, \ldots (\mathbb{N})$,
rational integers $0, \pm 1, \pm 2, \ldots (\mathbb{Z})$,
rational numbers $0, \pm 1, \pm \frac{1}{2}, \pm 2, \pm \frac{1}{3}, \pm \frac{2}{3}, \pm 3, \ldots (\mathbb{Q})$,
surds $r^{1/n}$ $(r\in\mathbb{Q}, n\in\mathbb{N}, n \geqslant 2)$;

we also inspect the means of constructing them. For this purpose we employ *algorithms*.

We shall not endeavour to give a definition of algorithms in terms of mathematical logics. Our algorithms consist of a stated input, a stated output and a finite number of well-defined steps. The input and output will usually be rational integers and quantities (such as fractions, algebraic integers, integral matrices) derived from rational integers by stated rules. The steps are numbered from 1 to n $(n\in\mathbb{N})$. They consist of statements which use the known data (from the input, or already calculated) to obtain new data by unique mathematical rules. The steps are usually carried out one after the other. But there can also be a jump from step i to step k $(k \neq i+1)$ depending on the value of some data. The mathematical rules for the computation of new data and for the decision, whether a jump occurs, are fixed throughout the whole algorithm. During the execution of the algorithm a certain step i $(1 \leqslant i \leqslant n)$ may be carried out several times, say $N(i)$ times, depending on the input data. However, all numbers $N(i)$ $(1 \leqslant i \leqslant n)$ must be finite.

The rational integers occuring in the algorithm usually signify what they stand for. Sometimes they denote algebraic numbers, sometimes they signify a decision of questions such as: is this real algebraic number r positive, zero, or negative?

$$\operatorname{sign}(r) = \begin{cases} 1 \text{ if } r > 0 \text{ (i.e. } r \text{ is positive)} \\ 0 \text{ if } r = 0 \\ -1 \text{ if } r < 0 \text{ (i.e. } r \text{ is negative).} \end{cases} \tag{1.2}$$

As an introductory but very instructive example for an algorithm, we present *Euclid's algorithm for rational integers*. For a better understanding of algorithms it is useful to present the underlying ideas in advance. The theory of Euclid's algorithm in $\mathbb{Z}$ is easily explained. For two natural numbers a, b with $a \geqslant b$ there exists a third natural number c subject to

$$bc \leqslant a,\ b(c+1) > a. \tag{1.3}$$

Hence, there exists a non-negative integer d such that

$$a = bc + d \quad \text{and} \quad 0 \leqslant d < b. \tag{1.4}$$

The process (1.4) is called *division with remainder* or, simply, *long division*. The numbers c, d are uniquely determined by a, b. The same procedure for $a, b \in \mathbb{Z}$ instead of a, $b \in \mathbb{N}$ is a little more complicated. One possibility of generalizing (1.3), (1.4) for arbitrary integers a, b, $b \neq 0$, is to stipulate

$$a = bc + d \quad \text{with} \quad 0 \leqslant d < |b|, \quad \operatorname{sign}(c) = \operatorname{sign}(a)\operatorname{sign}(b) \quad \text{for} \quad c, d \in \mathbb{Z}. \tag{1.5}$$

For a number theorist, however, the following generalization is more 'natural' and more useful:

$$a = bc + d \quad \text{and} \quad 0 \leqslant |d| \leqslant \left|\frac{b}{2}\right| \quad (c, d \in \mathbb{Z}). \tag{1.6}$$

It makes the remainder as small as possible in absolute value. On the other hand, IBM chose still another solution for its 360 computer series. Their way of long division for a, b yields c, $d \in \mathbb{Z}$ subject to

$$a = bc + d, \quad 0 \leqslant |d| < |b|, \quad \operatorname{sign}(b) = \operatorname{sign}(d). \tag{1.7}$$

Let us finally remark that there are other computers, such as the CDC Cyber 70 series, without any hardware instruction for integer division.

We just pointed out that long division for rational integers is not unique. However, all possibilities have the following properties in common: for given $a, b \in \mathbb{Z}$, $b \neq 0$, they determine a *quotient* $c = Q(a, b)$ and a *remainder* $d = R(a, b)$ satisfying

$$a = Q(a,b)b + R(a,b) \quad \text{and} \quad 0 \leqslant |R(a,b)| < |b|. \tag{1.8}$$

If we repeat long division in case $R(a, b) \neq 0$ with b, $R(a, b)$ in place of a, b we obtain a remainder $R(b, R(a, b))$ which is smaller in absolute value than

$R(a, b)$. Going on we get a sequence of remainders becoming smaller and smaller in absolute value. Hence, this process must come to a halt after finitely many steps, the last remainder being zero.

For example, let $a_1 = a$, $a_2 = b \neq 0$, then there are integers $k \in \mathbb{N}$, $a_i \in \mathbb{Z}$ $(1 \leqslant i \leqslant k+2)$, $q_i \in \mathbb{Z}$ $(2 \leqslant i \leqslant k+1)$, subject to

$$a_i = q_{i+1} a_{i+1} + a_{i+2} \tag{1.9}$$

and

$$0 < |a_{i+1}| < |a_i| \quad (2 \leqslant i < k+1), \quad a_{k+2} = 0. \tag{1.10}$$

It is clear that we can specify the a_i $(2 \leqslant i \leqslant k+1)$ analogous to (1.5) or (1.6) or (1.7). For each case, however, we obtain

$$|a_{k+1}| = \gcd(a_1, a_2), \tag{1.11}$$

i.e. $|a_{k+1}|$ is the greatest common divisor of a_1 and a_2 $(\gcd(a_1, a_2))$. Namely, each divisor e of a_1 and a_2 divides a_3 because of (1.9). Inductively we conclude $e | a_{k+1}$. On the other hand, a_{k+1} is a divisor of a_k because of (1.9) and $a_{k+2} = 0$. Applying (1.9) repeatedly it follows that a_{k+1} also divides $a_{k-1}, a_{k-2}, \ldots, a_2$, a_1. Both results together prove $|a_{k+1}| = \gcd(a_1, a_2)$.

Sometimes it does not suffice to compute the greatest common divisor c of two integers a, b but one also needs to determine integers $x = x(a, b)$, $y = y(a, b)$ for its presentation

$$c = xa + yb \tag{1.12}$$

by a and b. (Such a presentation exists since $\mathbb{Z}$ is a principal ideal ring.) This task can be easily incorporated into (1.9), (1.10). At the beginning we have $a_1 = x_1 a_1 + y_1 a_2$, $a_2 = x_2 a_1 + y_2 a_2$ for $x_1 = y_2 = 1$, $x_2 = y_1 = 0$. We show that there exists a presentation $a_i = x_i a_1 + y_i a_2$ at each level i. Namely, after the computation of a_{i+2} from a_{i+1}, a_i according to (1.9) we obtain

$$a_{i+2} = a_i - q_{i+1} a_{i+1} = (x_i - q_{i+1} x_{i+1}) a_1 + (y_i - q_{i+1} y_{i+1}) a_2 \quad \text{for } 1 \leqslant i \leqslant k-1.$$

Therefore the x_i, y_i satisfy the recurrence relations

$$x_{i+2} = x_i - q_{i+1} x_{i+1}, \quad y_{i+2} = y_i - q_{i+1} y_{i+1} \quad (1 \leqslant i \leqslant k-1). \tag{1.13}$$

With these explanations it is easy to write down the following algorithm. We note that $\gcd(0, 0) = 0$ by definition.

Euclid's algorithm with presentation of the gcd (1.14)

Input. $a, b \in \mathbb{Z}$.

Output. c, $x = x(a, b)$, $y = y(a, b) \in \mathbb{Z}$, $c \geqslant 0$ satisfying
$\gcd(a, b) = c = xa + yb$.

Step 1. (Initialization).
For $b = 0$ set $x \leftarrow \operatorname{sign}(a)$, $c \leftarrow xa$, $y \leftarrow 0$ and terminate. Else set $m \leftarrow a$, $n \leftarrow b$, $\tilde{x} \leftarrow 1$, $\tilde{y} \leftarrow 0$, $x \leftarrow 0$, $y \leftarrow 1$.

Step 2. (Long division).
Compute $Q(m,n)$, $R(m,n)$ according to (1.8).

Step 3. (Done?).
For $R(m,n)=0$ set $c \leftarrow \text{sign}(n)\cdot n$, $x \leftarrow \text{sign}(n)\cdot x$, $y \leftarrow \text{sign}(n)\cdot y$ and terminate. Else set $\tilde{\tilde{x}} \leftarrow \tilde{x} - Q(m,n)x$, $\tilde{\tilde{y}} \leftarrow \tilde{y} - Q(m,n)y$ and then $m \leftarrow n$, $n \leftarrow R(m,n)$, $\tilde{x} \leftarrow x$, $\tilde{y} \leftarrow y$, $x \leftarrow \tilde{\tilde{x}}$, $y \leftarrow \tilde{\tilde{y}}$ and go to 2.

For a detailed discussion of Euclid's algorithm we refer to Knuth [1].

We note that the greatest common divisor of two rational integers a, b is unique by definition if it exists. As already stated algorithm (1.14) comes to halt since each decreasing sequence of non-negative integers becomes constant after finitely many terms. *Thus the algorithm actually proves the existence of the gcd.* This observation is one of the guiding principles of our exposition.

Exercises

1. Show by using (1.14): $a = bc$ and $\gcd(a,b)=1 \Rightarrow a|c$ for any $a, b, c \in \mathbb{Z}$.
2. Show that any rational number r can be presented in precisely one way in the 'reduced form' $r = a/b (a \in \mathbb{Z}, b \in \mathbb{Z}^{>0}, \gcd(a,b)=1)$. Write an algorithm which transforms $r = \tilde{a}/\tilde{b} (\tilde{a}, \tilde{b} \in \mathbb{Z}, \tilde{b} \neq 0)$ into its reduced form.
3. Let $n \in \mathbb{Z}$ and $a_i \in \mathbb{Z}$ $(1 \leqslant i \leqslant n+1)$. Show that the greatest common divisor of $a_1, \ldots, a_{n+1}$ satisfies the recursive law
$$\gcd(a_1, \ldots, a_{n+1}) = \gcd(\gcd(a_1, \ldots, a_n), a_{n+1}), \tag{1.15}$$
where $\gcd(0, \ldots, 0) = 0$ by definition. Use (1.14) to write an algorithm which computes $\gcd(a_1, \ldots, a_{n+1})$.
4. Let $n \in \mathbb{N}$ and $a_i \in \mathbb{Z}$ $(1 \leqslant i \leqslant n+1)$. Prove the existence of a relation
$$\gcd(a_1, \ldots, a_{n+1}) = \sum_{i=1}^{n+1} x_i a_i \quad (x_i \in \mathbb{Z}, 1 \leqslant i \leqslant n+1). \tag{1.16}$$
Use (1.14) to write an algorithm for determining $x_i = x_i(a_1, \ldots, a_{n+1})$ $(1 \leqslant i \leqslant n+1)$ satisfying (1.16).

1.2. The main task of constructive algebra

Diophantine analysis begins with the problem of solving (1.1) by a rational integer. Constructively speaking: find an algorithm deciding, whether (1.1) has a rational integral solution and if the answer is 'yes' to exhibit a solution $x \in \mathbb{Z}$. For the calculation of x we now interpret the left-hand side of (1.1) as the 'value' of the polynomial
$$f(t) = a_0 t^n + a_1 t^{n-1} + \cdots + a_n \in \mathbb{Z}[t] \tag{2.1}$$
for a fixed ring element (in that case x). Then (1.1) is shortly written as
$$f(x) = 0 \tag{2.2}$$
and x is called *a zero of* $f(t)$ in that case. For $a \in \mathbb{Z}$ we compute $f(a)$ in n steps

by Horner's method. At step j we assume that we have already calculated $S_j = \sum_{i=0}^{j} a_i t^{j-i}$, and for $j < n$ we proceed to S_{j+1} via $S_{j+1} = S_j \cdot a + a_{j+1}$.

Horner's algorithm (2.3)

Input. Coefficients $a_0, \ldots, a_n$ of an nth degree polynomial $f(t) = \sum_{i=0}^{n} a_i t^{n-i}$ $(n \geqslant 1)$ and a number a.
Output. $S = f(a)$.
Step 1. (Initialization). Set $S \leftarrow a_0$, $j \leftarrow 0$.
Step 2. (Computation of S_j). Set $j \leftarrow j+1$, $S \leftarrow S \cdot a + a_j$.
Step 3. (Done?). In case $j = n$ terminate, else go to 2.

We note that the algorithm remains valid, if $a, a_0, a_1, \ldots, a_n$ are elements of a commutative ring.

In case $f(t) \in \mathbb{Z}[t]$ Horner's algorithm is very useful in determining all zeros of $f(t)$ in $\mathbb{Z}$. As we saw it suffices to compute $f(a)$ for those $a \in \mathbb{Z}$ dividing a_n, i.e. we must check $f(\pm a)$ for $a \mid a_n$, $a > 0$. A fast computation of $f(\pm a)$ uses the even and odd part of $f(t)$:

$$\left.\begin{aligned} &f(t) = f_e(t) + f_o(t) \\ \text{defined by} \quad &f_e(t) = \sum_{\substack{i=0 \\ n-i \equiv 0 \bmod 2}}^{n} a_i t^{n-i}, \quad f_o(t) = \sum_{\substack{i=0 \\ n-i \equiv 1 \bmod 2}}^{n} a_i t^{n-i} \end{aligned}\right\} \tag{2.4}$$

We recommend it as an excercise to write an algorithm analogous to (2.3) for the computation of $f(\pm a)$ using $f_e(a)$ and $f_o(a)$.

Knowing Horner's method an algorithm for the computation of a solution x of (1.1) (if it exists) is immediate.

Algorithm Diophant (2.5)

Input. Coefficients $a_0, \ldots, a_n$ of $f(t) = \sum_{i=0}^{n} a_i t^{n-i} \in \mathbb{Z}[t]$.
Output. $\varnothing$ if $f(t)$ has no zero in $\mathbb{Z}$, or $a \in \mathbb{Z}$ for which $f(a) = 0$.
Step 1. (Initialization). For $a_n = 0$ set $a \leftarrow 0$ and terminate. Else set $a \leftarrow 1$.
Step 2. (Zero found?). Compute $Q(a_n, a)$, $R(a_n, a)$. For $R(a_n, a) \neq 0$ go to 3. Else calculate $f(\pm a)$, $f(\pm Q(a_n, a))$ by (2.3) and (2.4). If $f(x) = 0$ for $x \in \{\pm a, \pm Q(a_n, a)\}$ set $a \leftarrow x$ and terminate.
Step 3. (Increase a). Set $a \leftarrow a + 1$. For $a^2 \leqslant |a_n|$ go to 2, else print $\varnothing$ and terminate.

(Obviously (2.5) is useful only if $|a_n|$ is small.)

In case (1.1) has no rational integral solution the question is, whether one can find a solution in a larger number system. The number system $\mathbb{Z}$ formed by the rational integers uses two basic operations: addition and multiplication which are connected by certain basic rules of operation (associativity,

commutativity, distributivity, invertibility of addition), which, taken together, establish the axioms of a *commutative ring*. We observe that the commutative ring $\mathbb{Z}$ is *unital*, i.e. it contains a neutral element n with respect to multiplication:

$$nx = x = xn \text{ for all } x \in \mathbb{Z} \text{ is satisfied for } n = 1 \neq 0.$$

Not every ring is unital, for example the even integers form the ring $2\mathbb{Z}$ which is contained in $\mathbb{Z}$ as a subring (the operations in $2\mathbb{Z}$ are obtained by restricting the operations of $\mathbb{Z}$ to $2\mathbb{Z}$), but $2\mathbb{Z}$ has no neutral element of multiplication. Since number theory is just swarming with such non-unital rings (viz. the proper ideals of orders) we shall retain the distinction made between commutative unital rings and commutative rings contrary to the usage in S. Lang's algebra book.

However, every ring R (not necessarily commutative) can be embedded into the unital ring $R \oplus \mathbb{Z}$ formed by the couples $x \oplus \lambda$ ($x \in R, \lambda \in \mathbb{Z}$) with the following rules of operation:

$$\left.\begin{aligned} &x \oplus \lambda = y \oplus \mu \Leftrightarrow x = y, \lambda = \mu; \\ &x \oplus \lambda = y \Leftrightarrow x = y, \lambda = 0; \\ &x \oplus \lambda = \mu \Leftrightarrow x = 0, \lambda = \mu; \\ &(x \oplus \lambda) + (y \oplus \mu) = (x + y) \oplus (\lambda + \mu); \\ &(x \oplus \lambda)(y \oplus \mu) = (xy + \lambda y + \mu x) \oplus \lambda\mu \qquad \text{for all } x, y \in R, \lambda, \mu \in \mathbb{Z}. \end{aligned}\right\} \quad (2.6)$$

The *permanence principle* as established by Peacock and his British contemporaries implies that any number system should satisfy the axioms of a commutative ring.

In general terms the task of constructive algebra assumes the following form. Let a commutative ring R be given in such a way that for any two of its elements a, b

(i) there is a clearcut answer whether a is equal to b ($a = b$) or whether a, b are distinct ($a \neq b$);
(ii) there are elements $a + b$, $a - b$, ab of R explicitly known (viz. sum, difference, product of a, b) such that the axioms of a commutative ring are satisfied.

Then we say that the *commutative ring R is given constructively*. For example, the rational integer ring $\mathbb{Z}$ as introduced in customary high-school mathematics is constructively given.

Now let us consider an algebraic equation (1.1) with coefficients $a_0, a_1, \ldots, a_n$ in a commutative ring R. Can it be solved in a commutative overring Λ of R, i.e. in a commutative ring Λ containing R such that the operations of Λ restrict to the given operations on the elements of R?

Moreover, can we give Λ constructively in terms of R and exhibit a solution x of (1.1) in Λ? For example, the linear diophantine equation (1.1) for $n = 1$ has a solution in $\mathbb{Z}$ only if a_0 divides a_1. However, there is always a unique solution in terms of the rational number

$$x = \frac{-a_1}{a_0}. \tag{2.7}$$

As a matter of fact, the history of mathematics shows that the desire to solve (1.1) in case $n = 1$ has led to the creation of the rational number system $\mathbb{Q}$ as quotient ring of $\mathbb{Z}$: $\mathbb{Q} = \mathfrak{Q}(\mathbb{Z})$. (In the sequel we denote the *quotient ring* of a commutative ring R – relative to the semigroup formed by the non-zero divisors of R – by $\mathfrak{Q}(R)$.) Again the fractional calculus as taught by well-trained math teachers presents a constructive solution of the task.

Exercises

1. Develop an algorithm to determine all solutions of (1.1) in $\mathbb{Z}$.
2. Examine whether the embedding (2.6) of R into $R \oplus \mathbb{Z}$ is constructive.

1.3. On the construction of overmodules and overrings

The computation of overrings Λ of a given ring R involves the discussion of the additive structure of Λ relative to the multiplicative action of R as well as the multiplicative structure of Λ.

1. Modules

Speaking purely in terms of addition the operation $+$ on Λ satisfies the module axioms (commutativity, associativity and invertibility of addition) which are the additive version of the axioms of a commutative (abelian) group. We refer to the basic definitions and concepts of module theory as contained in chapter 3 of S. Lang, *Algebra*, pp. 74–93. Of course the admission of non-unital rings R leads to a slightly more general concept of (*left*) *R-modules* M:

M is an additive abelian group together with a left multiplication of R and M resulting in a mapping $(R, M) \to M$: $(a, x) \mapsto ax$ satisfying $a(x + y) = ax + ay$, $(a + b)x = ax + bx$, $(ab)x = a(bx)$ for all $a, b \in R$, $x, y \in M$. (3.1)

As an example of the more general definition let us mention the *null-modules* for which every product is defined to be zero.

If R is unital and if

$$1x = x \quad \text{for all } x \in M, \tag{3.2}$$

then M is said to be a (*left*) *unital R-module*. The last, more special concept is the only one considered by S. Lang. We stipulate that in case R is unital the (left) R-modules considered are unital, too, if not otherwise stated. This convention leaves open the possibility of considering also R-modules over non-unital rings in which case there will be no restrictions.

Regarding direct sums, the direct sum of a family $\{M_i\}_{i\in I}$ of R-modules (I an index set) can be defined categorically as on p. 79 of S. Lang. From the constructive viewpoint it is more satisfactory to define the direct sum

$$M = \prod_{i\in I} M_i \tag{3.3}$$

of the R-module family $\{M_i\}_{i\in I}$ as the set of 'vectors' $(x_i)_{i\in I}$ with 'components' x_i in M_i such that $x_i = 0$ for almost all i, and the rules of vector calculus

$$a(x_i)_{i\in I} = (ax_i)_{i\in I}, \tag{3.4a}$$

$$(x_i)_{i\in I} + (y_i)_{i\in I} = (x_i + y_i)_{i\in I} \tag{3.4b}$$

are used to define the two basic operations.

If the given index set happens to be finite, say, I consists of $1, 2, \ldots, n$ ($n\in\mathbb{N}$), then we also write

$$M = M_1 \oplus M_2 \oplus \cdots \oplus M_n. \tag{3.5}$$

On the other hand, if one discovers that a given R-module M contains two R-submodules M_1, M_2 such that

$$M = M_1 + M_2, \quad M_1 \cap M_2 = \{0\} \tag{3.6}$$

then there is the R-module isomorphism

$$\alpha\colon M_1 \oplus M_2 \to M\colon m_1 \oplus m_2 \mapsto m_1 + m_2, \tag{3.7}$$

but of course it is imprecise and confusing to identify M with $M_1 \oplus M_2$. Therefore we introduce a new symbol $\dot{+}$ to describe the discovered relation (3.6) briefly as

$$M = M_1 \dot{+} M_2. \tag{3.8}$$

For example, the module $M = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ is a $\mathbb{Z}$-module of four elements with operation table

	n	b	c	d
n	n	b	c	d
b	b	n	d	c
c	c	d	n	b
d	d	c	b	n

for the elements $n = 0\oplus 0$ (neutral element).
$b = 1\oplus 0$
$c = 0\oplus 1$
$d = 1\oplus 1$

Using addition we have a module with n as zero element, using multiplication as operation we have the *Klein Four Group* with n as unit element. Adopting module language the only submodule of M other than M and $\{n\}$ and

the two direct summands $M_1 = \{n, b\}$, $M_2 = \{n, c\}$ is the submodule $M_3 = \{n, d\}$. It is easy to see that $M = M_1 + M_3$, $M_1 \cap M_3 = \{n\}$ so that $M = M_1 \dot{+} M_3$. However, $M_1 \oplus M_3$ is a construct which is isomorphic to M but it should not be confused with M.

2. Rings over commutative rings

For the rest of this section R always denotes a commutative ring. An *R-ring* is defined as a ring Λ which is also an R-module such that scalar multiplication and ring multiplication commute:

$$\lambda(ab) = (\lambda a)b = a(\lambda b) \quad \text{for all } \lambda \in R, a, b \in \Lambda. \tag{3.9}$$

Examples are the commutative overrings of R, where (3.9) is trivially satisfied.

For constructive purposes the R-rings Λ with a *basis* (over R) are of importance. They are defined as unital R-rings which – considered as R-modules – have an R-basis B. In other words, the module theoretic structure underlying the ring Λ is a *free R-module*. $|B|$ is called the *rank* of the free R-module Λ. The ring structure of Λ is derived from the basis multiplication table:

$$bb' = \sum_{b'' \in B} \gamma_{b,b',b''} b'' \quad (b, b' \in B, \gamma_{b,b',b''} \in R), \tag{3.10a}$$

$$\gamma_{b,b',b''} = 0 \text{ for all but a finite number of } b'' \in B, \text{ if } b, b' \in B \text{ are fixed.} \tag{3.10b}$$

The associativity of ring multiplication implies the associativity relations

$$\sum_{d \in B} \gamma_{a,b,d}\gamma_{d,c,e} = \sum_{d \in B} \gamma_{a,d,e}\gamma_{b,c,d} \quad (a, b, c, e \in B). \tag{3.10c}$$

Conversely, if a set of elements $\gamma_{b,b',b''} (b, b', b'' \in B)$ of R is known for some subset B of Λ satisfying (3.10b) and (3.10c), then it can be interpreted as the set of multiplication constants of the R-ring RB formed by the formal linear combinations

$$\sum_{b \in B} \lambda(b)b, \tag{3.10d}$$

where $\lambda: B \to R$ is a restricted mapping of B into R (i.e. $\lambda(b) = 0$ for all but a finite number of $b \in B$) subject to the rules of operations of a free R-module and the multiplication rule

$$\left(\sum_{b \in B} \lambda(b)b\right)\left(\sum_{b' \in B} \mu(b')b'\right) = \sum_{b'' \in B}\left(\sum_{b,b' \in B} \lambda(b)\mu(b')\gamma_{b,b',b''}\right)b'', \tag{3.10e}$$

which is implied by (3.10a) and linearity.

Thus a very powerful tool for the construction of R-rings is obtained. However, it must be used with care, since the number of associativity relations to be satisfied is equal to the cube of the number of basis elements so that

it becomes impractical to verify them by direct means already for quite small R-dimensions.

It is clear that the commutativity of an R-ring with an R-basis is implied by the commutativity of the multiplication of basis elements, i.e. by the commutativity rules

$$\gamma_{b',b'',b} = \gamma_{b'',b',b} \tag{3.10f}$$

for the multiplication constants.

We shall very frequently consider unital commutative rings Λ containing a given unital commutative ring R such that $1_R = 1_\Lambda$. In such cases we simply speak of a *unital overring* Λ *of* R (but see exercise 7 for an example where $1_R \neq 1_\Lambda$).

3. Polynomial rings

For example, we interpret the polynomial ring $R[t]$ in one variable t over a unital commutative ring R as the R-ring with basis

$$t^0 = 1, t^1 = t, t^2, \ldots,$$

and basis multiplication law

$$t^i t^k = t^{i+k} \quad (i, k \in \mathbb{Z}^{\geq 0}),$$

which corresponds to the multiplication constants

$$\gamma_{i,k,m} = \delta_{i+k,m} \quad (i, k, m \in \mathbb{Z}^{\geq 0}).$$

(Here $\delta_{x,y}$ is the well-known *Kronecker symbol* which is 1 for $x = y$ and otherwise 0.)

Elementary properties of polynomials are explained in S. Lang, chapter V.3. We denote the images of elements of R under the canonical injection

$$\iota: R \to R[t]: a \mapsto at^0$$

as the *constant polynomials*. For a polynomial $A \in R[t]$ we denote its *degree* by $\deg(A)$ and – in case $A \neq 0$ – its *leading coefficient* by $l(A)$, i.e. $l(A)$ is the coefficient of $t^{\deg(A)}$, hence $l(A) \neq 0$. In case of $l(A) = 1$ the polynomial A is called *monic*.

4. Long division of polynomials

Though the quotient of two polynomials $A, B \in R[t]$ may not exist in $R[t]$, not even if both A and B are distinct from zero, there is a *division with remainder* in $R[t]$. It assumes its simplest form in case $B \neq 0$ and $l(B) = 1$. In that case the following equation holds:

$$A = Q(A, B)B + R(A, B) \tag{3.11a}$$

in $R[t]$ with $Q(A, B)$ a polynomial of degree $\deg(A) - \deg(B)$ in case $\deg(A) \geq \deg(B)$, otherwise $Q(A, B) = 0$, and with $R(A, B)$ a polynomial of degree less