CHAPTER 1

Words

1.0. Introduction

This chapter contains the main definitions used in the rest of the book. It also presents some basic results about words that are of constant use in the sequel. In the first section are defined words, free monoids, and some terms about words, such as length and factors.

Section 1.2 is devoted to submonoids and to morphism of free monoids, one of the basic tools for words. Many of the proofs of properties of words involve a substitution from the alphabet into words over another alphabet, which is just the definition of a morphism of free monoids. A nontrivial result called the *defect theorem* is proved. The theorem asserts that if a relation exists among words in a set, those words can be written on a smaller alphabet. This is a weak counterpart for free monoids of the Nielsen-Schreier theorem for subgroups of a free group.

In Section 1.3 the definition of conjugate words is given, together with some equivalent characterizations. Also defined are *primitive words*, or words that are not a repetition of another word. A very useful result, due to Fine and Wilf, is proved that concerns the possibility of multiple repetitions. The last section introduces the notation of formal series that deal with linear combinations of words, which will be used in Chapters ??-?? and ??.

A list of problems, some of them difficult, is collected at the end. Two of them (1.1.2 and 1.2.1) deal with free groups; their object is to point out the existence of a combinatorial theory of words in free groups, although the theory is not developed in the present book (see Lyndon and Schupp 1977). Two others (1.1.3 and 1.3.5) deal with the analysis of algorithms on words.

1.1. Free Monoids and Words

Let A be a set that we shall call an *alphabet*. Its elements will be called *letters*. (In the development of this book, it will often be necessary to suppose that the alphabet A is finite. Because this assumption is not always necessary, however, it will be mentioned explicitly whenever it is used.)

A word over the alphabet A is a finite sequence of elements of A:

$$(a_1, a_2, \ldots, a_n), \qquad a_i \in A.$$

The set of all words over alphabet A is denoted by A^*. It is equipped with a binary operation obtained by concatenating two sequences.

$$(a_1, a_2, \ldots, a_n)(b_1, b_2, \ldots, b_m) = (a_1, a_2, \ldots, a_n, b_1, b_2, \ldots, b_m).$$

This binary operation is obviously associative, which allows writing a word as

$$a_1 a_2 \cdots a_n$$

instead of

$$(a_1, a_2, \ldots, a_n),$$

by identifying a letter $a \in A$ with the sequence (a).

The empty sequence, called the *empty word*, is a neutral element for the operation of concatenation. It is denoted by 1; hence, for any word w

$$1w = w1 = w\,.$$

A *monoid* is a set M with a binary operation that is associative and has a neutral element denoted by 1_M. Hence, what has been defined on the set A^* is a monoid structure.

A *morphism* of a monoid M into a monoid N is a mapping φ of M into N compatible with operations of M and N:

$$\varphi(mm') = \varphi(m)\varphi(m'), \qquad m, m' \in M,$$

and such that $\varphi(1_M) = 1_N$.

Proposition 1.1.1. *For any mapping α of A into a monoid M, there exists a unique morphism φ of monoids from A^* into M such that the following diagram is commutative:*

$$\begin{tikzcd} A \arrow[r, "i"] \arrow[dr, "\alpha"'] & A^* \arrow[d, "\varphi"] \\ & M \end{tikzcd}$$

where i is the natural injection of A into A^*.

Proof. Left to the reader. ■

Because of this property (called a *universal property*), the set A^* of all words over the alphabet A is called the *free monoid* over the set A.

The set of all nonempty words over A will be denoted by A^+:

$$A^+ = A^* - 1.$$

It is called the *free semigroup* over A (recall that a semigroup is a set with an associative binary operation). It may be readily verified that Proposition 1.1.1 can be stated for A^+ instead of A^* by replacing the term "monoids" by "semigroups".

As for any monoid the binary operation of A^* may be extended to the subsets of A^* by defining for $X, Y \subset A^*$.

$$XY = \{xy \mid x \in X, y \in Y\}\,.$$

We shall come back to this extension in Section 1.4. Consider now some terminology about words.

The *length* of the word $w = a_1 a_2 \cdots a_n$, $a_i \in A$ is the number n of the letters w is a product of. It will be denoted by $|w|$:

$$|w| = n\,.$$

The length of the empty word is 0 and the mapping $w \mapsto |w|$ is a morphism of the free monoid A^* onto the additive monoid $\mathbb{N}$ of positive integers.

For a subset B of the alphabet A, we denote by $|w|_B$ the number of letters of w that belong to B. Therefore,

$$|w| = \sum_{a \in A} |w|_a\,.$$

Denoted by $\mathrm{alph}(w)$ is the subset of the alphabet formed by the letters actually occurring in w. Therefore $a \in A$ belongs to $\mathrm{alph}(w)$ iff

$$|w|_a \geq 1\,.$$

A word $v \in A^*$ is said to be a *factor* of a word $x \in A^*$ if there exist words $u, w \in A^*$ such that

$$x = uvw\,.$$

The relation "v is factor of x" is an order on A^*. A factor v of $x \in A^*$ is said to be *proper* if $v \neq x$.

A word v is said to be a *left factor* of $x \in A^*$ if there exists a word $w \in A^*$ such that

$$x = vw\,,$$

and it is said to be a *proper left factor* if $v \neq x$. The relation "v is a left factor of x" is again an order on A^*; it will be denoted by

$$v \leq x\,.$$

This order has the fundamental property that if

$$v \leq x, \qquad v' \leq x,$$

then v and v' are comparable: $v \leq v'$ or $v' \leq v$.

More precisely, if

$$vw = v'w',$$

either there exists $s \in A^*$ such that $v = v's$ (and then $sw = w'$) or there exists $t \in A^*$ such that $v' = vt$ (and then $w = tw'$). This will be referred to as the property of *equidivisibility* of the free monoid.

The definition of a *right factor* is symmetrical to that of a left factor. The *reversal* of a word $w = a_1 a_2 \cdots a_n$, $a_i \in A$, is the word

$$\tilde{w} = a_n \cdots a_2 a_1 .$$

Hence v is a left factor of x iff $\tilde{v}$ is a right factor of $\tilde{x}$. We shall also use the notation $w^\sim$ instead of $\tilde{w}$; we may then write or all $u, v \in A^+$,

$$(uv)^\sim = \tilde{v}\tilde{u} .$$

A word w is palindrome if $w = \tilde{w}$.

A word $v \in A^*$ is said to be a *subword* of a word $x \in A^*$ if

$$v = a_1 a_2 \cdots a_n , \qquad a_i \in A, n \geq 0,$$

and there exist $y_0, y_1, \ldots, y_n \in A^*$ such that

$$x = y_0 a_1 y_1 a_2 \cdots a_n y_n .$$

Therefore v is a subword of x if it is a sub-sequence of x.

1.2. Submonoids and Morphisms

A submonoid of a monoid M is a subset N of M containing the neutral element of M and closed under the operation of M : $NN \subset N$. Given a subset X of the free monoid A^*, we denote by X^* the submonoid of A^* generated by X. Conversely, given a submonoid P of A^*, there exists a unique set X that generates P and is minimal for set-inclusion. In fact, X is the set

$$X = (P - 1) - (P - 1)^2$$

of the nonempty words of P that cannot be written as the product of two nonempty words of P. It is a straightforward verification that X generates P and that it is contained in any set $Y \subset A^*$ generating P. The set X will be referred to as the *minimal generating set* of P.

A monoid M is said to be *free* if there exist an alphabet B and an isomorphism of the free monoid B^* onto M. For instance, for any word $w \in A^+$ the submonoid generated by w, written w^* instead of $\{w\}^*$, is free. It is very important to observe that not all the submonoids of a free monoid are themselves free (see Example 1.2.2).

Proposition 1.2.1. *Let P be a submonoid of A^* and X be its minimal generating set. Then P is free iff any equality*

$$x_1x_2\cdots x_n = y_1y_2\cdots y_m, \qquad n, m \geq 0, \quad x_i, y_j \in X$$

implies $n = m$ and $x_i = y_i$, $1 \leq i \leq n$.

The proof is again left to the reader. The minimal generating set of a free submonoid P of A^* is called a *code*; it is referred to as the *basis* of P.

A set $X \subset A^*$ is called a *prefix* if for $x, y \in X$

$$x \leq y$$

implies $x = y$; it can easily be verified that any prefix $X \subset A^+$ is a code.

Example 1.2.2. Let $A = \{a, b\}$; the set $X = \{a, b, ab\}$ is not a code since it is not the minimal generating set of X^*. The set $Y = \{a, ab, ba\}$ is the minimal generating set of Y^*; yet it is not a code because

$$a(ba) = (ab)a$$

is a nontrivial equality between products of elements of Y. The set $Z = \{aa, ba, baa, bb, bba\}$ can be verified to be a code.

The following characterization of free submonoids of A^* is useful:

Proposition 1.2.3. *A submonoid P of A^* is free iff for any word $w \in A^*$, one has $w \in P$ whenever there exist $p, q \in P$ such that*

$$pw, wq \in P\,.$$

Proof. Let P be a submonoid of A^* and denote by X its minimal generating set. First suppose that the preceding condition holds for P. Then if

$$x_1x_2\cdots x_n = y_1y_2\cdots y_m, \quad x_i \in X,\ y_j \in X\,, \tag{1.2.1}$$

we may suppose that $x_1 \leq y_1$ and let $y_1 = x_1w$, $w \in A^*$. Then

$$x_2\cdots x_n = wy_2\cdots y_m\,,$$

and therefore x_1w, $wy_2\cdots y_m \in P$; this implies by hypothesis $w \in P$. Since X is the minimal generating set of P, we have $w = 1$, and this proves that eq. (1.2.1) is trivial by induction on $n + m$. Therefore P is free.

Conversely, if P is free, let φ be an isomorphism of a free monoid B^* onto P, with $X = \varphi(B)$. Then if for $p, q \in P$, one has $pw, wq \in P$, let $\varphi(x) = p$, $\varphi(y) = wq$, $\varphi(z) = pw$, $\varphi(t) = q$. Since $\varphi(xy) = \varphi(zt)$ we have $xy = zt$, and this implies that $z = xu$, $u \in B^*$. Therefore $w = \varphi(u) \in P$. ■

Corollary 1.2.4. *An intersection of free submonoids of A^* is free.*

Proof. If the submonoids P_i, $i \in I$ are free, and if there exists

$$p, q \in P = \bigcap_{i \in I} P_i$$

such that $pw, wq \in P$, then by Proposition 1.2.3, $w \in P_i$ for each $i \in I$ and therefore $w \in P$. By 1.2.2, this shows that P is free. ∎

If X is any subset of A^*, the set $\mathcal{F}$ of free submonoids of A^* containing X is not empty (it contains A^*) and, by Corollary 1.2.4, it is closed under intersection. Therefore the intersection of all elements of $\mathcal{F}$ is the smallest free submonoid containing X; the code generating this submonoid is called the *free hull* of X.

THEOREM 1.2.5 (Defect theorem). *The free hull Y of a finite subset $X \subset A^*$, which is not a code, satisfies the inequality*

$$\mathrm{Card}(Y) \leq \mathrm{Card}(X) - 1.$$

Proof. Consider the mapping α of X into Y associating to $x \in X$ the word $y \in Y$ such that $x \in yY^*$; since Y is a code, the mapping α is well defined.

As X is not a code, there exists an equality

$$x_1 x_2 \cdots x_n = y_1 y_2 \cdots y_n$$

with $x_i, y_j \in X$ and $x_1 \neq y_1$. Therefore, $\alpha(x_1) = \alpha(y_1)$ and α cannot be injective.

The following shows that α is surjective: if it were not, let $z \in Y$ be such that $z \notin \alpha(X)$; consider the set

$$Z = (Y - z)z^* .$$

The set Z is a code since an equality

$$z_1 z_2 \cdots z_n = z'_1 z'_2 \cdots z'_{n'}, \qquad z_i, z'_j \in Z \tag{1.2.2}$$

can be rewritten

$$y_1 z^{k_1} y_2 z^{k_2} \cdots y_n z^{k_n} = y'_1 z^{k'_1} y'_2 z^{k'_2} \cdots y'_{n'} z^{k'_{n'}} \tag{1.2.3}$$

with $z_i = y_i z^{k_i}$, $z'_j = y'_j z^{k'_j}$, $y_i, y'_j \in Y - Z$, $k_i, k'_j \geq 0$. Since Y is a code Eq. (1.2.3) is trivial. This implies $y_1 = {y'}_1$, $k_1 = k'_1$, $y_2 = y'_2, \ldots$ and finally $n = n'$ and $z_i = z'_i$.

But we have $X \subset Z^*$ and $Z^* \subset Y^*$, which contradicts the minimality of the submonoid Y^*. Hence α is surjective, which implies that Y has fewer elements than X. ∎

As an immediate consequence, of Theorem 1.2.5, there is the following corollary.

Corollary 1.2.6. *Each pair of words $\{x, y\}$ $(x, y \in A^*)$ is a code unless x and y are powers of a single word $z \in A^*$.*

Morphisms of free monoids play an essential role in the sequel. Let

$$\varphi : B^* \to A^*$$

be a morphism of free monoids. Clearly it is completely characterized by the images $\varphi(b) \in A^*$ of the letters $b \in B$. It is an isomorphism of B^* into A^* iff its restriction to B is injective and if the submonoid $\varphi(B^*)$ is a free submonoid of A^*.

A morphism $\varphi : B^* \to A^*$ is called *nonerasing* if $\varphi(B^+) \subset A^+$. If φ is nonerasing, then for all $w \in B^*$,

$$|\varphi(w)| \geq |w|.$$

1.3. Conjugacy

A word $x \in A^*$ is said to be *primitive* if it is not a power of another word; that is, if $x \neq 1$ and $x \in z^*$ for $z \in A^*$ implies $x = z$.

Proposition 1.3.1. *If*

$$x^n = y^m, \qquad x, y \in A^*,\ n, m \geq 0,$$

there exists a word z such that $x, y \in z^*$.

In particular, for each word $w \in A^+$, there exists a unique primitive word x such that $w \in x^*$.

Proof. If $w = x^n = y^m$ with $x \neq y$ the set $\{x, y\}$ is not a code and, by the defect theorem (1.2.5) there exists a word $z \in A^*$ such that $x, y \in z^*$. If $w = x^n = y^m$ with x and y primitive, then there exists a word $z \in A^*$ such that $x = z^i$, $y = z^j$, $i, j \geq 0$. This implies $x = y = z$. ∎

Proposition 1.3.2. *Two words $x, y \in A^+$ commute iff they are powers of the same word. More precisely the set of words commuting with a word $x \in A^+$ is a monoid generated by a single primitive word.*

Proof. Let z be the unique primitive word such that $x \in z^*$. Then if $xy = yx$ for $y \in A^+$, the set $\{x, y\}$ is not a code and there exists $t \in A^+$ such that $x, y \in t^*$. Then by Proposition 1.3.1, $t \in z^*$. Therefore the set of words commuting with x is generated by z. ∎

Two words x and y are said to be *conjugate* if there exist words $u, v \in A^*$ such that

$$x = uv, \qquad y = vu. \tag{1.3.1}$$

This is an equivalence relation on A^* since x is conjugate to y iff y can be obtained by a cyclic permutation of the letters of x. More precisely, let γ be the permutation of A^+ defined by

$$\gamma(ax) = xa, \qquad a \in A, \qquad x \in A^*;$$

then the classes of conjugate elements are the orbits of γ.

Proposition 1.3.3. *Let $x, y \in A^*$ and z, t be the primitive words such that $x \in z^*$, $y \in t^*$. Then x and y are conjugate iff z and t are also conjugate; in this case, there exists a unique pair $(u, v) \in A^* \times A^+$ such that $z = uv$, $t = vu$.*

Proof. Let $x = z^k$. If $x = rs$, there exists $u, v \in A^*$ such that $z = uv$, $r = z^{k_1}u$, $s = vz^{k_2}$ and $k_1 + k_2 + 1 = k$. Then the conjugate $y = sr$ of x can be written $y = t^k$ with $t = vu$. Moreover the pair (u, v) such that $z = uv$, $t = vu$ is unique since by Proposition 1.3.2 z has $|z|$ distinct conjugates. ■

Proposition 1.3.4. *Two words $x, y \in A^+$ are conjugate iff there exists a $z \in A^*$ such that*

$$xz = zy. \tag{1.3.2}$$

More precisely, equality (1.3.2) holds iff there exist $u, v \in A^*$ such that

$$x = uv, \qquad y = vu, \qquad z \in u(vu)^*. \tag{1.3.3}$$

Proof. If Eq. (1.3.3) holds, then (1.3.2) also holds. Conversely, if $xz = zy$, for $x, y \in A^+$, $z \in A^*$, we have for each $n \geq 1$

$$x^n z = zy^n \tag{1.3.4}$$

Let n be such that $n|x| \geq |z| \geq (n-1)|x|$. Then we deduce from Eq. (1.3.4) that

$$z = x^{n-1}u, \qquad x = uv, \qquad vz = y^n. \tag{1.3.5}$$

Finally $y^n = vz = vx^{n-1}u$ is also equal to $(vu)^n$ and since $|y| = |x|$, we obtain $y = vu$, proving that Eq. (1.3.3) holds. ■

It may be observed that, in accordance with the defect theorem, the equality $xz = zy$ implies $x, y, z \in \{u, v\}^*$, a submonoid with two generators.

The properties of conjugacy in A^* proved thus far can be viewed as particular cases of the properties of conjugacy in the free group on A (see Problem 1.3.1).

If $\mathrm{Card}(A) = k$ is finite, let us denote by $\psi_k(n)$ the number of classes of conjugates of primitive words of length n on the alphabet A. If w is a word of length n and if $w = z^q$ with z primitive and $n = qd$, then the number of conjugates of w is exactly d. Hence

$$k^n = \sum_{d|n} d\psi_k(d), \tag{1.3.6}$$

the sum running over the divisors of n. By Möbius inversion formula (see Problem 1.3.2) this is equivalent to:

$$\psi_k(n) = \frac{1}{n}\sum_{d|n}\mu(d)k^{n/d} \tag{1.3.7}$$

where μ is the *Möbius function* defined on $\mathbb{N} - 0$ as follows:

$$\begin{aligned} \mu(1) &= 1, \\ \mu(n) &= (-1)^i \end{aligned}$$

if n is the product of i distinct primes and

$$\mu(n) = 0$$

if n is divisible by a square.

Proposition 1.3.1 admits the following refinement (Fine and Wilf 1965):

Proposition 1.3.5. *Let $x, y \in A^*$, $n = |x|$, $m = |y|$, $d = gcd(n, m)$. If two powers x^p and y^q of x and y have a common left factor of length at least equal to $n + m - d$, then x and y are powers of the same word.*

Proof. Let u be the common left factor of length $n + m - d$ of x^p, y^q. We first suppose that $d = 1$ and show that x and y are powers of a single letter. We may assume that $n \leq m - 1$. It will be enough to show that the first $n - 1$ letters of u are equal. Denote by $u(i)$ the ith letter of u. By hypothesis, we have

$$u(i) = u(i + n), \qquad 1 \leq i \leq m - 1, \tag{1.3.8}$$

$$u(j) = u(j + m), \qquad 1 \leq j \leq n - 1. \tag{1.3.9}$$

Let $1 \leq i, j \leq m - 1$ and $j \equiv i + n \bmod m$. Then either $j = i + n$ or $j = i + n - m$. In the first case $u(i) = u(j)$ by (1.3.8). In the second case $u(j) = u(j + m)$ by (1.3.9) since $j = i + n - m \leq n - 1$. Therefore

$$u(i) = u(i + n) = u(j + m) = u(j)\,.$$

Hence $u(i) = u(j)$ whenever $1 \leq i, j \leq m - 1$ and $j - i \equiv n \bmod m$. But since m, n are supposed to be relatively prime, any element of the set $\{1, 2, \ldots, m - 1\}$ is equal modulo m to a multiple of n. This shows that the first $m - 1$ letters of u are equal. In the general case, we consider the alphabet $B = A^d$ and, by the foregoing argument, x and y are powers of a single word of length d. ■

Example 1.3.6. Consider the sequence of words on $A = \{a, b\}$ defined as follows: $f_1 = b$, $f_2 = a$ and

$$f_{n+1} = f_n f_{n-1}\,, \quad n \geq 2.$$

The sequence of the lengths $\lambda_n =| f_n |$ is the Fibonacci sequence. Two consecutive elements λ_n and λ_{n+1} for $n \geq 3$ are relatively prime. Let g_n be the left factor of f_n of length $\lambda_n - 2$ for $n \geq 3$. Then

$$g_{n+1} = f_{n-1}^2 g_{n-2}$$

for $n \geq 5$, as it may be verified by induction. We then have simultaneously

$$f_{n+1} \leq f_n^2, \quad g_{n+1} \leq f_{n-1}^3 \,.$$

Therefore, for each $n \geq 5$, f_n^2 and f_{n-1}^3 have a common left factor of length $\lambda_n + \lambda_{n-1} - 2$. This shows that the bound given by Proposition 1.3.5 is optimal. For instance,

$$g_7 = \mathrlap{\overbrace{}^{f_6}}\underbrace{a\,b\,a\,a\,b}_{f_5}\,\underbrace{a\,b\,a\,a\,b}_{f_5}\,a$$

1.4. Formal Series

Enumeration problems on words often lead to considering mappings of the free monoid into a ring. Such mappings may be viewed (and usefully handled) as finite or infinite linear combinations of words (see for instance Problem 1.4.2). This is the motivation for introducing the concept of a formal series.

Let K be a ring with unit; in the sequel K will be generally be the ring $\mathbb{Z}$ of all integers. A *formal series* (or series) with coefficients in K and variables in A is just a mapping of the free monoid A^* into K. The set of these series is denoted by $K\langle\langle A\rangle\rangle$.

For a series $\sigma \in K\langle\langle A\rangle\rangle$ and a word $w \in A^*$, the value of σ on w is denoted by $\langle \sigma, w\rangle$ and called the *coefficient* of w in σ; it is an element of K. For a set $X \subset A^*$, we denote by $\mathbf{X}$ the *characteristic series* of X, defined by

$$\begin{aligned} \langle \mathbf{X}, x\rangle &= 1 \quad \text{if } x \in X, \\ \langle \mathbf{X}, x\rangle &= 0 \quad \text{if } x \notin X. \end{aligned}$$

The operations of sum and product of two series $\sigma, \tau \in K\langle\langle A\rangle\rangle$ are defined by:

$$\begin{aligned} \langle \sigma + \tau, w\rangle &= \langle \sigma, w\rangle + \langle \tau, w\rangle \,, \\ \langle \sigma\tau, w\rangle &= \sum_{w=uv} \langle \sigma, u\rangle\langle \sigma, v\rangle \,, \end{aligned}$$

for any $w \in A^*$. These operations turn the set $K\langle\langle A\rangle\rangle$ into a ring. This ring has a unit that is the series $\mathbf{1}$, where 1 is the empty word.

A formal series $\sigma \in K\langle\langle A\rangle\rangle$ such that all but a finite number of its coefficients are zero is called a *polynomial.* The set $K\langle A\rangle$ of these polynomials is a subring of the ring $K\langle\langle A\rangle\rangle$. It is called the free (associative) K-algebra over A (see Problem 1.4.1). For each $\sigma \in K\langle\langle A\rangle\rangle$ and $\tau \in K\langle A\rangle$, we define

$$\langle \sigma, \tau\rangle = \sum_w \langle \sigma, w\rangle\langle \tau, w\rangle \ .$$

This is a bilinear map of $K\langle\langle A\rangle\rangle \times K\langle A\rangle$ in K.

The sum may be extended to an infinite number of elements with the following restriction: A family $(\sigma_i)_{i\in I}$ of series is said to be *locally finite* if for each $w \in A^*$, all but finitely many of the coefficients $\langle\sigma_i, w\rangle$ are zero.

If $(\sigma_i)_{i\in I}$ is a locally finite family of series, the sum

$$\sigma = \sum_{i\in I} \sigma_i$$

is well defined since for each $w \in A^*$, the coefficient $\langle\sigma, w\rangle$ is the sum of a finite set of nonzero coefficients $\langle\sigma_i, w\rangle$.

In particular, the family $(\mathbf{w})_{w\in A^*}$ is locally finite, and this allows to write for any $\sigma \in K\langle\langle A\rangle\rangle$

$$\sigma = \sum_{w\in A^*} \langle\sigma, w\rangle \mathbf{w},$$

or, by identifying w with $\mathbf{w}$,

$$\sigma = \sum_{w\in A^*} \langle\sigma, w\rangle w,$$

This is the usual notation for formal series in one variable:

$$\sigma = \sum_{n\geq 0} \sigma_n a^n$$

with $\sigma_n = \langle\sigma, a^n\rangle$.

Let σ be a series such that $\langle\sigma, 1\rangle = 0$; the family $(\sigma^i)_{i\geq 0}$ is then locally finite since $\langle\sigma^i, w\rangle = 0$ for $i \geq |w| + 1$. This allows us to define the new series

$$\sigma^* = 1 + \sigma + \sigma^2 + \cdots$$

which is called the *star* of σ. It is easy to verify the following:

Proposition 1.4.1. *Let $\sigma \in K\langle\langle A\rangle\rangle$ be such that $\langle\sigma, 1\rangle = 0$. The series σ^* is the unique series such that:*

$$\sigma^*(1-\sigma) = (1-\sigma)\sigma^* = 1.$$

Following is a list of statements relating the operations in $K\langle\langle A\rangle\rangle$ with the operations on the subsets of A^* when K is assumed to be of characteristic zero.

Proposition 1.4.2. *For two subsets X, Y of A^*, one has*

(i) *let $Z = X \cup Y$. Then $\mathbf{Z} = \mathbf{X} + \mathbf{Y}$ iff $X \cap Y = \emptyset$,*

(ii) *let $Z = XY$. Then $\mathbf{Z} = \mathbf{XY}$ iff $xy = x'y' \Rightarrow x = x', y = y'$, for $x, x' \in X$, $y, y' \in Y$,*

(iii) *let $X \subset A^+$, and $P = X^*$. Then $\mathbf{P} = \mathbf{X}$ iff X is a code.*

The proof is left to the reader as an exercise.

Notes

The terminology used for words presents some variations in the literature. Some authors call *subword* what is called here *factor* the term *subword* is reserved for another use (see Chapter 6). Some call *prefix* or *initial segment* what we call a *left factor*. Also, the *empty word* is often denoted by ϵ instead of 1.

General references concerning free submonoids are Eilenberg 1974 and Lallement 1979; Proposition 1.2.3 was known to Schützenberger (1956) and to Cohn (1962). The defect theorem (Theorem 1.2.5) is virtually folklore; it has been proved under various forms by several authors (see Lentin 1972; Makanin 1976; Ehrenfeucht and Rozenberg 1978). The proof given here is from Berstel et al. 1979, where some generalizations are discussed.

The results of Section 1.3 are also mainly common knowledge. For further references see Chapters 8 and 9.

The standard reference for Section 1.4 is Eilenberg 1974.

Problems

Section 1.1

1.1.1 (Levi's lemma). A monoid M is free iff there exists a morphism λ of M into the monoid $\mathbb{N}$ of additive integers such that $\lambda^{-1}(0) = 1_M$ and if for any $x, y, z, t \in M$

$$xy = zt$$

implies the existence of a $u \in M$ such that either $x = zu$, $uy = t$ or $xu = z$, $y = ut$.

1.1.2 Let A be an alphabet and $\bar{A} = \{\bar{a} \mid a \in A\}$ be a copy of A. Consider in the free monoid over the set $A \cup \bar{A}$ the congruence generated by the relations

$$a\bar{a} = \bar{a}a = 1, \qquad a \in A\,.$$

a. Show that each word has a unique representative of minimal length, called a *reduced word*.

b. Show that the quotient of $(A \cup \bar{A})^*$ by this congruence is a group F; the inverse of the reduced word w is denoted by $\bar{w}$.

c. Show that for any mapping α of A into a group G, there exists a unique morphism φ of F onto G making the following diagram commutative:

$$\begin{tikzcd} A \arrow[r] \arrow[dr, "\alpha"'] & F \arrow[d, "\varphi"] \\ & G \end{tikzcd}$$

F is called the *free group* over A (see Magnus, Karass, and Solitar 1976 or Hall 1959 or Lyndon and Schupp 1977). Henceforth in problems about free groups,

$$\rho : F \to (A \cup \bar{A})^*,$$

denotes the mapping associating to each element of F the unique reduced word representing it.

*1.1.3 Let $\varphi : A^* \to A^*$ be the mapping assigning to each word $w \in A^*$ the longest word that is both a proper left and a proper right factor of w.

a. Let $w = a_1 a_2 \cdots a_n$ and denote $\varphi(i) = j$ instead of $\varphi(a_1 \cdots a_i) = a_1 \cdots a_j$; show that the following algorithm allows computation of φ:

```
1.  $\varphi(1) \leftarrow 0$;
2.  for $i \leftarrow 2$ until $n$ do
          begin
3.        $j \leftarrow \varphi(i-1)$;
4.        while $j > 0$ and $a_i \neq a_{j+1}$ do $j \leftarrow \varphi(j)$;
5.        if $j = 0$ and $a_i \neq a_{j=1}$ then $\varphi(i) \leftarrow 0$
6.        else $\varphi(i) \leftarrow j + 1$;
          end
```

(For the notations concerning algorithms, see Aho, Hopcroft, and Ullman 1974.)

b. Show that the number of successive comparisons of two letters of the word w in performing the foregoing algorithm does not exceed $2n$. (*Hint* : Note that the variable j can be increased at most n times by one unit.)

c. Show that the foregoing algorithm can be used to test whether a word $u \in A^+$ is a factor of a word $v \in A^+$. (*Hint* : Apply the algorithm of (1) to the word $w = uv$.)

This is called a *string-matching algorithm* (see Knuth, Morris, and Pratt 1977).

Section 1.2

*1.2.1 Let F be the free group over the set A and H be a subgroup of F.

a. Show that it is possible to choose a set Q of representatives of the right cosets of H in F such that the set $\rho(Q)$ of reduced words representing Q contains all its left factors. Such a set Q is called a *Schreier system* for H.

b. Let Q be a Schreier system for H and

$$X = \{pa\bar{q} \mid p, q \in Q, a \in A, pa \in (H-1)q\};$$

Show that X generates H.

c. Show that each $pa\bar{q} \in X$ is reduced as written and that, in the product of two elements of $X \cup \bar{X}$ the letters a in the triple (p, a, q) never cancel unless the whole product does.

d. Deduce from (a), (b), and (c) that any subgroup H of a free group F is free and that if H is of finite index d in F, then it is isomorphic with a free group on r generators with

$$r - 1 = d(k - 1), \qquad k = \mathrm{Card}(A)$$

(Schreier's formula; see the references of Problem 1.1.2).

1.2.2 A submonoid N of A^* is generated by a prefix iff it satisfies:

$$m, mn \in N \Rightarrow n \in N$$

for all $m, n \in A^*$. Such a submonoid is called (right) *unitary.*

1.2.3 Let P be the set of words

$$P = \{w\tilde{w} \mid w \in A^*\}.$$

Then P is the set of *palindromes* (i.e., $u = \tilde{u}$) of even length. Show that the submonoid P^* is right and left unitary.
(*Hint* : Let Π be the basis of P^*; show that Π is prefix.) (See Knuth, Morris and Pratt 1977.)

1.2.4 Let $\theta : A^* \to B^*$ be a morphism and $P \subset B^*$ be a free submonoid of B^*. Show that $\theta^{-1}(P)$ is a free submonoid of A^*.

Section 1.3

1.3.1 Show that two words $x, y \in A^*$ are conjugate iff they are conjugate in the free group F over A —that is, iff there exists an element g of F such that

$$x = gyg^{-1},$$

(Identify A^* to a subset of F.)

1.3.2 (*Möbius inversion formula*) Let μ be the Möbius function; show that

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & \text{if } n = 1\,, \\ 0 & \text{if } n \geq 2\,. \end{cases}$$

Deduce from this that two functions φ, ψ of $\mathbb{N} - 0$ in $\mathbb{Z}$ are related by

$$\sum_{d|n} \psi(d) = \varphi(n)$$

iff

$$\sum_{d|n} \mu(d)\varphi(n/d) = \psi(n)\,.$$

1.3.3 Show directly (without using the defect theorem, that is) that if $\{x, y\}$ is not a code, then x and y are powers of a single word.

1.3.4 (Problem 1.1.3) Show that $\varphi(w) = u$ iff

$$w = (st)^{k+1}s, \; u = (st)^k s, \quad k \geq 0, \; s, t \in A^*$$

with $|s|$ minimal. Deduce that the algorithm of Problem 1.1.3 allows computation of the primitive word such that $w = v^n$, $n \geq 1$ (*Hint*: Use Proposition 1.3.5)

1.3.5 Let $w = a_1 a_2 \cdots a_n$, $n \geq 1$, $a_i \in A$. For $1 \leq i \leq n$, let $\psi(i)$ be the greatest integer $j \leq i - 1$ such that

$$a_1 a_2 \cdots a_{j-1} = a_{i-j+1} \cdots a_{i-1}, \quad a_i \neq a_j \,,$$

with $\psi(i) = 0$ if no such integer j exists.

a. Show that the following algorithm computes ψ:

```
1. $\psi(i) \leftarrow 0$;
2. $i \leftarrow 1; j \leftarrow 0$;
3. while $i < n$ do
       begin
4.         while $j > 0$ and $a_i \neq a_j$ do $j \leftarrow \psi(j)$;
5.         $i \leftarrow i + 1$;  $j \leftarrow j + 1$;
6.         if $a_i = a_j$ then $\psi(i) \leftarrow \psi(j)$ else $\psi(i) \leftarrow \psi(j)$;
       end
```

(*Hint*: Show that the value of the variable j at line 6 is $\varphi(i-1)+1$ wheres φ is as in Problem 1.1.3.)

b. Show that the algorithm of problem part (a) can be used to test whether a word u is a factor of a word v.

c. Show that the number of consecutive times the *while* loop of line 4 may be executed does not exceed the integer r such that

$$\lambda_{r+3} \leq n < \lambda_{r+4}$$

where λ_r is the rth term of the Fibonacci sequence. Show, using the sequence of Example 1.3.6 that this bound can be reached. (See Knuth, Morris and Pratt 1978; Duval 1981.)

Section 1.4

1.4.1 For any mapping α of A into an associative K-algebra R, there exists a unique morphism φ of $K\langle A\rangle$ into R such that the following diagram is commutative:

$$\begin{tikzcd}
A \arrow[rr] \arrow[dr, "\alpha"'] & & K\langle A\rangle \arrow[dl, "\varphi"] \\
& R &
\end{tikzcd}$$

1.4.2 Let $W \subset A^+$ and

$$P = A^* - A^* W A^*$$

be the set of words having no factor in W. Let for each $u \in W$,

$$X_u = A^*u - A^*WA^+$$

be the set of words having u as a right factor but no other factor in W. For each $u, v \in W$, let $R_{u,v}$ be the finite set

$$R_{u,v} = \{t \in A^+ - A^*v \mid ut \in A^*v\}.$$

a. Show that the following equalities hold in $\mathbb{Z}\langle\langle A\rangle\rangle$:

$$1 + \mathbf{PA} = \mathbf{P} + \sum_{u \in W} \mathbf{X}_u, \tag{a.1}$$

and for each $u \in W$,

$$\mathbf{P}u = \mathbf{X}u + \sum_{v \in W} \mathbf{X}\mathbf{R}_{v,u} \tag{a.2}$$

b. Show that the system of equalities (a.1) and (a.2), for $u \in W$, allows computation of P.

c. Show that the formal series

$$\lambda = \sum_{n \geq 0} \lambda_n z^n$$

with $\lambda_n = \mathrm{Card}(A^n \cap P)$, is rational. (*Hint*: Use the morphism of $\mathbb{Z}\langle\langle A\rangle\rangle$ onto $\mathbb{Z}\langle\langle z\rangle\rangle$ sending $a \in A$ on z.)

d. Apply the foregoing method to show that for $W = \{aba\}$ one has

$$\lambda_n = 2\lambda_{n-1} - \lambda_{n-2} + \lambda_{n-3}, \ n \geq 3.$$

(See Schützenberger 1964; for a general reference concerning linear equations in the ring $\mathbb{Z}\langle\langle A\rangle\rangle$, see Eilenberg 1974.)

Bibliography

Berstel, J., Perrin, D., Perrrot, J.-F., and Restivo, A. (1979). Sur le théorème du défaut, *J. Algebra*, *60*, 169–180.

Cohn, P. M. (1962). On subsemigroups of free semigroups, *Proc. Amer. Math. Soc.*, *13*, 347–351.

Ehrenfeucht, A. and Rozenberg, G. (1978). Elementary homomorphisms and a solution of the DOL sequence equivanlence problem, *Theoret. Comput. Sci.*, *7*, 169–183.

Eilenberg, S. (1974). *Automata, Languages and Machines*, Vol. A. Academic Press.

Lallement, G. (1979). *Semigroups and Combinatorial Applications.* J. Wiley and Sons.

Lentin, A. (1972). *Equations dans les monoïdes libres.* Gauthier–Villars, Paris.

Makanin, G. S. (1976). On the rank of equations in four unknowns in a free semigroup, *Mat. Sb.*, *100*, 285–311. (English trans. in *Math USSR Sb.*, *32*, 257–280).

Schützenberger, M. P. (1956). Une théorie algébrique du codage, *Séminaire Dubreil–Pisot*, *année 55–56.*