• 6.17 (a) Describe the synchronised transducer which realises the recognisable relation $K \times L$ starting with the automata $\mathcal{A}$ and $\mathcal{B}$ over A^* and B^* that recognise K and L respectively.

(b) Construct this automaton in the case where $A = B = \{a, b\}$ and where

$$K = \{f \mid |f|_b \equiv 1 \bmod 2\} \quad \text{and} \quad L = \{g \mid |g|_a \equiv 2 \bmod 3\} \ .$$

6.18 Write out the proof of Proposition 6.20 based on that of Theorem 5.1.

• 6.19 Prove:

Proposition 6.21 *A synchronous rational relation is a deterministic rational relation.*

6.20 Verify that a recognisable relation is synchronous with a synchronisation ratio equal to r, for any rational number r.

7 Malcev–Neumann series

The purpose of this section is to present a proof of:

Theorem 4.5 *The semiring* $\mathbb{N}\mathrm{Rat}\, B^*$ *is a sub-semiring of a skew field and so is, more generally, the semiring* $\mathbb{N}\mathrm{Rat}\,(A_2^* \times \cdots \times A_k^*)$.

cf. Sec. 4.3, p. 574

We have already said that this result is based on two theorems of algebra, whose statement and the definitions they require are repeated below:

Definition 4.1 *A total order relation* $\leqslant$ *on a group* G *makes* G *an* ordered group *if it is compatible, left and right, with multiplication in* G*; that is, if the following holds:*

$$\forall a, b, c \in G \qquad a \leqslant b \quad \Longrightarrow \quad a\,c \leqslant b\,c \quad \textit{and} \quad c\,a \leqslant c\,b \ . \qquad \square$$

Theorem 4.6 [**Birkhoff–Tarski–Neumann–Iwazawa**] *A finite direct product of free groups is an ordered group.*

Definition 4.2 [**Hahn–Malcev–Neumann**] *Let* $\mathbb{K}$ *be a semiring and* G *an ordered group. We write*[30] $\mathbb{K}_{\mathsf{wo}}\langle\langle G \rangle\rangle$ *for the set of series on* G *with coefficients in* $\mathbb{K}$ *whose support is a well ordered subset of* G. □

cf. Sec. III.1.1 and Note III.11, p. 381

If there is no ambiguity we call $\mathbb{K}_{\mathsf{wo}}\langle\langle G \rangle\rangle$ simply the set *of series on* G *with coefficients in* $\mathbb{K}$ or the set of $\mathbb{K}$-series on G, in contrast with the general definition, because they are the only series which we can reasonably consider on G if $\mathbb{K}$ is not a continuous semiring.

Theorem 4.7 [**Malcev–Neumann**] *If* $\mathbb{K}$ *is a skew field and* G *an ordered group, then* $\mathbb{K}_{\mathsf{wo}}\langle\langle G \rangle\rangle$ *is a skew field.*

[30] The notation $\mathbb{K}_{\mathsf{m}}\langle\langle G \rangle\rangle$ is used by some authors, in homage to Malcev.

7.1 Order on the free group

We seek here to attain and reconcile two distinct and almost contradictory objectives: on one hand to prove in the most elementary possible way (that is, using the simplest notions and most direct reasoning) that the free group can be ordered, and on the other to describe and understand the nature of the order with which we shall equip it.[31]

We start with some elementary properties on ordered groups, then we introduce the Magnus representation of the free group, which is vital to the achievement of our two objectives. We then prove Theorem 4.6 by making a detour via ordered rings, a detour which turns out to be a fiendish shortcut. In the fourth paragraph, we return to the description of the order we have thus constructed, which brings into play the central descending series of the free group, which we shall also define with the aid of the Magnus representation.

7.1.1 On ordered groups

We begin by showing that the definition of a total order on a group is equivalent to finding sets of *positive* and *negative* elements; that is, of elements respectively greater than and less than the neutral element of the group.

Proposition 7.1 *A group G is ordered if and only if there exist two subsets P and N of G which satisfy the following[32] conditions:*
(i) $G = P \oplus N \oplus 1_G$; (ii) $P^2 \subseteq P$ *and* $N^2 \subseteq N$; (iii) $\forall t \in G \quad t^{-1}P\,t \subseteq P$.

Proof. Suppose that G is ordered; we take

$$P = \{g \in G \mid 1_G \lneq g\} \qquad \text{and} \qquad N = \{g \in G \mid g \lneq 1_G\} \ .$$

This choice implies (i). The definition of the order on G implies

$$1_G \lneq g \quad \text{and} \quad 1_G \lneq h \quad \Longrightarrow \quad 1_G \lneq g\,h \ ,$$

that is, (ii), and

$$1_G \lneq g \quad \Longrightarrow \quad t \lneq g\,t \quad \Longrightarrow \quad 1_G \lneq t^{-1}g\,t \ ,$$

that is, (iii).

Suppose conversely that there exist P and N which verify (i), (ii) and (iii); we define a relation $\lneq$ on G by

$$g \lneq h \quad \text{if and only if} \quad g^{-1}h \in P \ ;$$

Hypothesis (i) implies that $\lneq$ is total and anti-symmetric; (ii) implies the transitivity of $\lneq$ and (iii) ensures its compatibility with multiplication in the group. ∎

---

[31]The result of this contradiction is long-windedness.

[32]The $\oplus$ denotes here the *disjoint* union.

Proposition 7.2 *A subgroup of an ordered group is ordered.* ■

Proposition 7.3 *If G and H are ordered groups, the group $G \times H$ is ordered.*

cf. Sec. II.7.2, p. 326

Proof. We define the *lexicographic order*[33] on $G \times H$ by

$$(g,h) \lneqq (g',h') \qquad \text{if and only if} \qquad \begin{cases} g \lneqq g' \\ \quad \text{or} \\ g = g' \quad \text{and} \quad h \lneqq h' \end{cases} .$$

We verify immediately that this order makes $G \times H$ an ordered group. ■

Remark 7.1 The result is actually much more general and extends to infinite products (on a set of well-ordered indices). □

Corollary 7.4 *The free commutative group $\mathbb{Z}^k$ is ordered.* ■

7.1.2 Representation of the free group

Let $\mathbb{Z}\langle A^*\rangle$ be the algebra of polynomials on A^* with coefficients in $\mathbb{Z}$, and $\mathbb{Z}\langle\langle A^*\rangle\rangle$ the algebra of series on A^* with coefficients in $\mathbb{Z}$ (also called the (large) algebra of the free monoid). The representation of the free group $\mathrm{F}(A)$ described in the following theorem is known as the *Magnus representation.*

Theorem 7.1 *The morphism $\mu\colon A^* \to \mathbb{Z}\langle A^*\rangle$ defined by $a\mu = 1 + a$ extends to an* injective morphism

$$\mu\colon \mathrm{F}(A) \longrightarrow \mathbb{Z}\langle\langle A^*\rangle\rangle \ ,$$

by taking $a^{-1}\mu = 1 - a + a^2 - \cdots + (-1)^n a^n + \cdots$.

Proof. Since $(1+a)(1-a+a^2-\cdots) = (1-a+a^2-\cdots)(1+a) = 1$, the choice of $a^{-1}\mu$ indeed makes μ a morphism. It suffices to show that $1_{\mathbb{Z}\langle\langle A^*\rangle\rangle}\mu^{-1} = 1_{\mathrm{F}(A)}$ and for that that $w\mu \neq 1$ if $w \neq 1_{\mathrm{F}(A)}$. We identify $\mathrm{F}(A)$ with the set of reduced words: an element w in $\mathrm{F}(A)$ other than $1_{\mathrm{F}(A)}$ is written (uniquely) in the form

$$w = a_1^{i_1} a_2^{i_2} \cdots a_n^{i_n} \ ,$$

with a_j in A, i_j in $\mathbb{Z} \setminus 0$, and $a_j \neq a_{j+1}$ for all $j \in [n]$. We shall show that the support of $w\mu$ contains $a_1 a_2 \cdots a_n$. We write

$$a_j^{i_j}\mu = 1 + i_j\, a_j + {a_j}^2\, S_{i_j}(a_j) \ , \tag{7.1}$$

where $S_{i_j}(a_j)$ is a series of $\mathbb{Z}\langle\langle A^*\rangle\rangle$. By assumption, the word $a_1 a_2 \cdots a_n$ contains no factor of the form ${a_j}^2$ and the only way to obtain $a_1 a_2 \cdots a_n$ in the product

$$w\mu = \big(1 + i_1\, a_1 + {a_1}^2\, S_{i_1}(a_1)\big) \cdots \big(1 + i_n\, a_n + {a_n}^2\, S_{i_n}(a_n)\big)$$

is to form the product of the terms $i_j\, a_{i_j}$, and its coefficient is the product of the i_j , all different from 0. ■

[33] N.B. this is not the *product order* on $G \times H$, that is, the order obtained as the product of the orders on G and H.

7.1.3 A detour via ordered rings

Definition 7.1 A total order $\leqslant$ on a ring R makes R an *ordered ring* if it is compatible with addition in R and left and right multiplication by the 'positive' elements of R; that is, if the following holds:

$$\forall a, b, c \in R\,,\ \forall d \in R\,,\ 0_R \leqslant d \qquad a \leqslant b \quad \Longrightarrow \quad \begin{cases} a + c \leqslant b + c\ , \\ a\,d \leqslant b\,d \quad \text{and} \quad d\,a \leqslant d\,b\ . \end{cases} \qquad \square$$

We then have the equivalent of Proposition 7.1.

Proposition 7.5 *A ring R is ordered if and only if there exists a subset C of R which satisfies the following conditions:*
(i) $R = C \oplus 0_R \oplus -C$ *;* (ii) C *is closed for* $+$ *and* $\times$.

Proof. Suppose that R is ordered; we take

$$C = \{x \in R \mid 0_R \lneq x\}\ .$$

The definition of the order on R implies directly

$$0_R \lneq x \quad \text{and} \quad 0_R \lneq y \quad \Longrightarrow \quad 0_R \lneq x + y \quad \text{and} \quad 0_R \lneq x\,y\ .$$

Conversely, suppose that the subset C verifies (i) and (ii); we define the ordering relation $\lneq$ on R by

$$x \lneq y \qquad \text{if and only if} \qquad y - x \in C\ .$$

Condition (i) implies that $\lneq$ is total and antisymmetric; (ii) implies the transitivity of $\lneq$ as shown by the following:

$$y - x \in C \quad \text{and} \quad z - y \in C \quad \Longrightarrow \quad z - x = (z - y) + (y - x) \in C\ ,$$

and, together with the distributivity of $\times$ over $+$, it also implies compatibility with multiplication in R. ■

Let $\mathsf{U}_+(R)$ be the intersection of the group of units of R with C:

$$\mathsf{U}_+(R) = \{x \in R \mid 0_R \lneq x \quad \text{and} \quad x \text{ invertible}\}\ .$$

It is a simple exercise to verify:

Lemma 7.6 *Let R be an ordered ring. The subset $\mathsf{U}_+(R)$ is a group and the restriction of the order on R to $\mathsf{U}_+(R)$ makes $\mathsf{U}_+(R)$ an ordered group.* ■

Proof of Theorem 4.6. We choose a total order on A^* which is a well ordering and is compatible with multiplication; that is,

$$a \leqslant b \quad \text{and} \quad c \leqslant d \quad \Longrightarrow \quad a\,c \leqslant b\,d\ ,$$

for example, the radix order. We then order $\mathbb{Z}\langle\langle A^*\rangle\rangle$ by choosing as the positive cone the set of series such that the coefficient of the smallest monomial with a non-zero coefficient is positive.

The group $\mathsf{U}_+(\mathbb{Z}\langle\langle A^*\rangle\rangle)$ is thus the set of series whose constant term is equal to 1. The free group $\mathrm{F}(A)$ is a subgroup of $\mathsf{U}_+(\mathbb{Z}\langle\langle A^*\rangle\rangle)$, ordered by Proposition 7.2. A finite direct product of free groups is ordered by Proposition 7.3. ■

7.1.4 Order on the free group

We shall now describe more explicitly this order on the free group whose existence we have just proved. To this end we shall use the Magnus representation to define a sequence of normal subgroups of the free group. For all u and v in $\mathrm{F}(A)$, we write $[u,v] = u^{-1}v^{-1}uv$ for the *commutator* of u and v and, if D and E are subsets of $\mathrm{F}(A)$,

$$[D,E] = \{[u,v] \bigm| u \in D\,, \quad v \in E\} \ .$$

Theorem 7.2 *Let D_n be the subset of $\mathrm{F}(A)$ defined by*

$$D_n = \{w \in \mathrm{F}(A) \bigm| w\mu = 1 + S_w \quad \textit{and} \quad \mathbf{v}(S_w) \geqslant n\} \ ,$$

cf. Rem. III.1.5, p. 387 *where $\mathbf{v}(S_w)$ is the valuation of the series S_w. Then, for all n in $\mathbb{N}_*$,*

(i) *D_n is a normal subgroup of $\mathrm{F}(A)$ ($D_1 = \mathrm{F}(A)$);*

(ii) $\displaystyle\bigcap_{n\in\mathbb{N}} D_n = 1_{\mathrm{F}(A)}$ *;*

(iii) *D_n/D_{n+1} is a finitely generated free commutative group; more precisely, for $n = 1$, we have: $D_1/D_2 = \mathbb{Z}^{\|A\|}$;*

(iv) $[D_n,D_1] \subseteq D_{n+1}$ *.*

Proof. (i) Since $\mathbf{v}(st) = \mathbf{v}(s) + \mathbf{v}(t)$ for all s and t in $\mathbb{Z}\langle\langle A^*\rangle\rangle$, D_n is a subgroup of $\mathrm{F}(A)$, indeed, a normal subgroup, for all n in $\mathbb{N}_*$.
(ii) By definition, $1_{\mathrm{F}(A)}$ belongs to the intersection of all the D_n and we saw with Theorem 7.1 that $w\mu$ is different from 1 for all w in $\mathrm{F}(A)$ other than $1_{\mathrm{F}(A)}$.
(iii) For all w in D_n, we write $w\mu$ in the form

$$w\mu = 1 + Q_w + S'_w \ , \tag{7.2}$$

where Q_w is a homogeneous polynomial of degree n of $\mathbb{Z}\langle A^*\rangle$ and $\mathbf{v}(S'_w)$ is greater than or equal to $n+1$. If w and w' are in D_n, we have

$$(w\,w')\mu = 1 + Q_w + Q_{w'} + S'_{w\,w'}$$

and the map $\pi_n \colon w \mapsto Q_w$ is a morphism from D_n to the *additive group* H_n of homogeneous polynomials of degree n over $\mathbb{Z}\langle A^*\rangle$. The kernel of π_n is D_{n+1} and D_n/D_{n+1} is isomorphic to $(D_n)\pi_n$, a subgroup of H_n.

Of course H_1, the group of homogeneous polynomials *of degree* 1, is isomorphic to $\mathbb{Z}^{\|A\|}$ and it is again the proof of Theorem 7.1, Equation (7.1), which ensures the surjectivity of π_1 onto H_1.
(iv) Let w be in D_n and t in $D_1 = \mathrm{F}(A)$; we write

$$t\mu = 1 + U_t + T_t \ ,$$

where U_t is a polynomial whose monomials are of degree between 1 and n (inclusive) and T_t is a series with valuation greater than or equal to $n+1$. By writing $w\mu$ in the form of (7.2), we obtain

$$(w\,t)\mu = 1 + U_t + Q_w + T_{w\,t} \qquad \text{and} \qquad (t\,w)\mu = 1 + U_t + Q_w + T_{t\,w} \ .$$

Thus, $(wt)\mu$ and $(tw)\mu$ are two series that are equal modulo A^{n+1}, hence so are $((wt)\mu)^{-1}$ and $((tw)\mu)^{-1}$. It follows that $((tw)\mu)^{-1}(wt)\mu = ([w,t])\mu$ is equal to 1 modulo A^{n+1}; that is, $[w,t]$ belongs to D_{n+1}. ■

Remark 7.2 We have not really proved (iii), but only that D_n/D_{n+1} is a *subgroup* of a finitely generated commutative group. It is a classic result in algebra that such a subgroup is itself a finitely generated free commutative group. Formally, though, we do not need to prove more than we already have in order to prove Theorem 4.6 (or Theorem 7.3). *cf. Exer. 7.4*

Furthermore, it is standard, but rather more difficult to prove, that we have not just the inclusion of $[D_n, D_1]$ in D_{n+1} but also equality of the two, and thus that D_n is *the nth term of the central descending series* of $\mathrm{F}(A)$. We shall not need this beautiful result either. □

Theorem 7.3 *Let A be a finite alphabet of cardinal k. For all group orders on $\mathbb{Z}^k$, we can choose on $\mathrm{F}(A)$ an order which makes $\mathrm{F}(A)$ an ordered group such that the canonical morphism $\gamma\colon \mathrm{F}(A) \to \mathbb{Z}^k$ is a morphism of ordered groups.*

Proof. We use the notation of Theorem 7.2 (and sketch the construction in Figure 7.1); for each n, H_n is a free commutative group (of rank k^n), hence ordered, and $E_n = (D_n)\pi_n$ is an ordered group (Proposition 7.2). Let $E_n = X_n \oplus Y_n \oplus 1_{E_n}$ be the partition constructed on this order (Proposition 7.1). Set $P_n = (X_n){\pi_n}^{-1}$ and $N_n = (Y_n){\pi_n}^{-1}$ (we have $D_{n+1} = (1_{E_n}){\pi_n}^{-1}$) and

$$P = \bigcup_{n\in\mathbb{N}_*} P_n \qquad \text{and} \qquad N = \bigcup_{n\in\mathbb{N}_*} N_n \ .$$

It remains to show that P and N satisfy the three conditions of Proposition 7.1 and hence define an order on $\mathrm{F}(A)$.

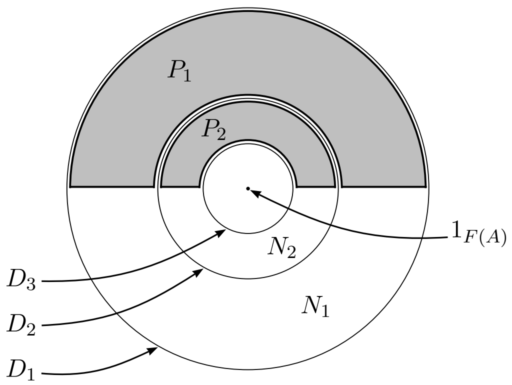

Figure 7.1: Construction of an order on $\mathrm{F}(A)$

From Theorem 7.2 (ii), we deduce that $P \cup N = \mathrm{F}(A) \setminus 1_{\mathrm{F}(A)}$.

Let u and v be in P, u be in D_n, hence in P_n, and v be in D_m, hence in P_m. If $n = m$, $(uv)\pi_n = u\pi_n v\pi_n$ and uv is in P_n by the property of X_n. If $n \lneq m$, then uv is equivalent to u modulo D_{n+1} hence belongs to P_n.

Let u be in P, hence in P_n for some n, and t be in D_1. Since $t^{-1}ut = u[u,t]$, and $[u,t]$ is in D_{n+1} (Theorem 7.2 (iv)), u and $t^{-1}ut$ are equivalent modulo D_{n+1} and $t^{-1}ut$ is in P_n, hence in P.

By definition, the canonical morphism $\gamma\colon \mathrm{F}(A) \to \mathbb{Z}^k$ is equal to π_1, and the order on $D_1 \setminus D_2$, hence on $\mathrm{F}(A)$, is constructed in such a way that π_1 is a morphism for the order. ∎

Exercises

7.1 Verify Proposition 7.2 and that the lexicographic order indeed makes the product of two ordered groups an ordered group.

7.2 Show that we can order $\mathbb{Z}^n$ other than by the lexicographic order, by projection on to a line of 'completely' irrational gradient.

7.3 Verify Lemma 7.6.

7.4 Show that a subgroup of a free commutative group of rank k (that is, generated by k elements) is a free commutative group of rank $r \leqslant k$.

7.2 Series on an ordered group

We now come to the proof of Theorem 4.7. It relies on the notion of a *well partial ordering* and on Higman's Theorem, which we saw in Section II.5. Hence, we freely use the definitions and results proved in that section for *well quasi-orderings* and which hold identically for well partial orderings. Recall in particular:

Th. II.5.2, p. 295

cf. p. 293

Theorem II.5.2 [**Higman**] *If X is a set equipped with a well partial ordering, then division is a well partial ordering on $\mathrm{V}(X)$.*

Properties II.5.2 *Let E be a set equipped with a well partial ordering $\leqslant$.*

(i) *The trace of $\leqslant$ on every subset of E is a well partial ordering.*

(ii) *Every image of E under a morphism is equipped with a well partial ordering.*

7.2.1 The semiring $\mathbb{K}_{\mathsf{wo}}\langle\langle G\rangle\rangle$

cf. Def. II.5.3, p. 298

Recall that if E and F are partially ordered sets, a map $\alpha\colon E \to F$ is a *morphism* (we understand 'for the order') if

$$a \leqslant b \Rightarrow a\alpha \leqslant b\alpha \ .$$

The morphism α is called *strict* if, in addition,

$$a \lneqq b \Rightarrow a\alpha \lneqq b\alpha \ .$$

In other words, the morphism α is strict if $a \leqslant b$ and $a\alpha = b\alpha$ imply $a = b$.

Lemma 7.7 *Let $\alpha\colon E \to F$ be a strict morphism between two ordered sets. If the order on E is a well partial ordering, then, for all f in F, $f\alpha^{-1}$ is a finite set.*

Proof. By definition of a strict morphism, the elements of $f\alpha^{-1}$ are *pairwise incomparable*, and hence finite in number. ■

cf. Th. II.5.1 (vi), p. 294

We now know enough to show that the series on an ordered group form a semiring. We first prove a small lemma.

Lemma 7.8 *Let G be an ordered group. The map $\pi\colon G \times G \to G$ defined by $(g,h)\pi = g\,h$ is a strict morphism (of (partially) ordered sets).*[34]

Proof. That π is a morphism is a direct consequence of the definitions: $(g,h) \leqslant (g',h')$ implies $g \leqslant g'$ and $h \leqslant h'$, from which $g\,g' \leqslant h\,h'$.

Since $(g,h) \leqslant (g',h) \leqslant (g',h')$, $g\,h = g'\,h'$ implies $g\,h = g'\,h = g'\,h'$ and hence $g = g'$ and $h = h'$, since G is a group. ■

Proposition 7.9 *If $\mathbb{K}$ is a semiring (resp. a ring) and G a (totally) ordered group, $\mathbb{K}_{\mathsf{wo}}\langle\!\langle G\rangle\!\rangle$ is a semiring (resp. a ring).*

Proof. We need to show that $\mathbb{K}_{\mathsf{wo}}\langle\!\langle G\rangle\!\rangle$ is closed under product. Therefore, let s and t be series on G (with coefficients in $\mathbb{K}$) whose supports, respectively S and T, are two well ordered subsets of G. For each $g\,h$ in $S\,T$, the set $(S \times T) \cap (g\,h)\pi^{-1}$ is finite (Lemma 7.7) and the Cauchy product of s and t is well defined. The support of $s\,t$ is contained in $(S \times T)\pi$ and is hence a well ordered set. ■

cf. Propty II.5.2 (i) and (ii), p. 298

7.2.2 Ordered semigroups

The last step is to define *ordered semigroups*, which will be an essential ingredient of the proof of Theorem 4.7.

Definition 7.2 A semigroup P is called *ordered* if there exists a *total* order $\leqslant$ on P such that, for all r, s and t in P we have

(i) $r \leqslant s \implies r\,t \leqslant s\,t$ and $t\,r \leqslant t\,s$; (ii) $r \lneqq r^2$. □

Condition (i) expresses the regularity of the order relation for multiplication. It entails, as for a congruence, that

$$r \leqslant r' \quad\text{and}\quad s \leqslant s' \implies r\,s \leqslant r'\,s \leqslant r'\,s' \ .$$

From condition (ii) we deduce:

Lemma 7.10 *In an ordered* simplifiable *semigroup a product is strictly greater than each of its factors.*

Proof. Let r and s be elements of P, an ordered semigroup, such that $r \lneqq s$. From (ii) and (i), we obtain $r \lneqq r^2 \leqslant r\,s$.

[34] But not at all a morphism of groups.

Furthermore, by multiplying (ii) on the right by s, we have $r\,s \leqslant r^2\,s$. If $r\,s \leqslant s$, it follows, by multiplying on the left by r, that $r^2\,s \leqslant r\,s$ from which $r\,s = r^2\,s$ or $r = r^2$ since P is simplifiable; this is a contradiction, hence $s \nleqslant r\,s$. ■

Remark 7.3 Definition 7.2 is inconsistent in the sense that a group G is a semigroup but at the same time an order that makes G an ordered group does not make it an ordered semigroup, because of condition (ii). This does not matter: it is in fact simply taking liberties with language, but it does require that we take care to give separate statements for analogous properties of ordered groups and ordered semigroups (for example, Lemma 7.8 and Lemma 7.11).

On the other hand, if G is an ordered group, the trace of the order of G on the set P of 'positive' elements of G certainly makes P an ordered semigroup, and this is what we have in mind. □

With the same proof as that of Lemma 7.8 we have:

Lemma 7.11 *Let P be an ordered semigroup. The map $\pi\colon P \times P \to P$ defined by $(g,h)\pi = g\,h$ is a morphism (of (partially) ordered sets). If P is* simplifiable *the morphism π is strict.* ■

Lemma 7.12 *Let P be a simplifiable ordered semigroup. The canonical morphism (of semigroups) $\alpha\colon \mathrm{V}(P) \to P$ is a strict morphism (of ordered sets).*

Proof. Suppose $(s_1, s_2, \ldots, s_p) \trianglelefteq (t_1, t_2, \ldots, t_n)$; there then exists an ascending sequence of indices $i_1, i_2, \ldots, i_p$ such that, for all j, $s_j \leqslant t_{i_j}$. Thus

$$(s_1, s_2, \ldots, s_p)\alpha = s_1 s_2 \cdots s_p \leqslant t_{i_1} t_{i_2} \cdots t_{i_p} \quad .$$

Lemma 7.10 used $p+1$ times gives

$$t_{i_1} t_{i_2} \cdots t_{i_p} \leqslant t_1 t_2 \cdots t_n = (t_1, t_2, \ldots, t_n)\alpha \quad .$$

Lemma 7.11 and Lemma 7.10 ensure that we cannot have the equality

$$(s_1, s_2, \ldots, s_p)\alpha = (t_1, t_2, \ldots, t_n)\alpha$$

unless $p = n$ and $s_j = t_j$ for all j, hence α is strict. ■

7.2.3 The field $\mathbb{K}_{\mathsf{wo}}\langle\!\langle G \rangle\!\rangle$

From the above results we now easily deduce the crucial result for the embedding of $\mathrm{F}(A)$ in a field.

Proposition 7.13 [**Neumann**] *Let P be an ordered simplifiable semigroup and S a well ordered subset of P. Then*

(i) *The semigroup generated by S, S^+, is a well ordered subset of P.*

(ii) *The family $\{S^n\}_{n\in\mathbb{N}}$ is locally finite: every p in S^+ belongs to a finite number of the S^n.*

Proof [Higman]. We write, as in Lemma 7.12, $\alpha\colon \mathrm{V}(P) \to P$ for the canonical morphism.

(i) Since S is well ordered, $\mathrm{V}(S)$ is a well (partially) ordered set by Higman's Theorem; the semigroup $S^{+} = (\mathrm{V}(S))\alpha$ is well ordered by Lemma 7.12 and Properties II.5.2.

(ii) For all p in S^{+}, $(p)\alpha^{-1}$ is finite by Lemma 7.7 and since, under our assumptions, the morphism α is *strict*. *A fortiori*, $(p)\alpha^{-1} \cap \mathrm{V}(S)$ is finite, and this is exactly the property sought. ■

Proof of Theorem 4.7. We already know that $\mathbb{K}_{\mathsf{wo}}\langle\langle G\rangle\rangle$ is a ring; to prove that it is a skew field, we must show not only that every non-zero element is invertible but also that this inverse belongs to $\mathbb{K}_{\mathsf{wo}}\langle\langle G\rangle\rangle$. Let, as in Proposition 7.1, P be the set of 'positive' elements of G; as we have already noted, the trace on P of the order of G makes P an ordered semigroup (and P is *simplifiable* since it is a sub-semigroup of a group).

Let t be an arbitrary non-zero element of $\mathbb{K}_{\mathsf{wo}}\langle\langle G\rangle\rangle$. Let $T = \mathsf{supp}\, t$ be the (non-empty) support of t, and $g_t = \mathsf{min}\, T$ the smallest element of T: this exists since, by definition of $\mathbb{K}_{\mathsf{wo}}\langle\langle G\rangle\rangle$, T is a well ordered set. We can then write

$$t = \langle t, g_t\rangle g_t\,(1 - s)\,, \qquad \text{that is, written otherwise,} \qquad s = 1_G - \frac{1}{\langle t, g_t\rangle} {g_t}^{-1} t \ ,$$

and the series s thus defined satisfies

$$\langle s, 1_G\rangle = 0_{\mathbb{K}} \qquad \text{and} \qquad \langle s, g\rangle = \frac{-1}{\langle t, g_t\rangle}\langle t, g_t\, g\rangle \ ,$$

for all g in G. Hence we deduce that $\langle s, g\rangle \neq 0_{\mathbb{K}}$ implies that $g_t \lneqq g_t\, g$, that is, $1_G \lneqq g$, and the support $S = g_t^{-1}T \setminus 1_G$ of s is hence contained in P.

The family $\{s^n\}_{n\in\mathbb{N}}$ is locally finite by Proposition 7.13 (ii); it is thus summable and the support of its sum s^* is a subset of S^* hence a well ordered subset of G: then s^* belongs to $\mathbb{K}_{\mathsf{wo}}\langle\langle G\rangle\rangle$ and so does

$$t^{-1} = s^* {g_t}^{-1} \frac{-1}{\langle t, g_t\rangle} \ . \qquad ■$$

7.2.4 A last inclusion

The theorem that we want to prove requires a final lemma on well ordered sets. *Th. 4.5, p. 616*

Lemma 7.14 *For each i in a finite set I, let F_i be a well ordered subset of a (totally) ordered set E_i. Then $\prod_{i\in I} F_i$ is a well ordered subset of $\prod_{i\in I} E_i$, ordered lexicographically.* ■

Note that this lemma is not redundant with respect to Property II.5.2 (recalled above) since the order considered here on $\prod_{i\in I} E_i$ is not the product order but the lexicographic order. We then deduce from Theorem 7.3:

Corollary 7.15 *Let A be a finite alphabet. We can choose an order on* $\mathrm{F}(A)$ *such that the canonical injection makes A^* a well ordered subset of* $\mathrm{F}(A)$.

Proof. Let $k = \|A\|$. Since $\mathbb{N}$ is a well ordered submonoid of $\mathbb{Z}$, we see $\mathbb{N}^k$ is a well ordered submonoid of $\mathbb{Z}^k$. We choose an order on $\mathrm{F}(A)$ such that $\gamma\colon \mathrm{F}(A) \to \mathbb{Z}^k$ is a morphism for the lexicographic order on $\mathbb{Z}^k$.

Let f_1, f_2, f_3,... be a sequence of words in A^*, strictly descending for the order of $\mathrm{F}(A)$. Its image under γ is a descending sequence of $\mathbb{N}^k$, hence eventually stationary. As the inverse image under γ *in* A^* of an arbitrary element of $\mathbb{N}^k$ is finite, the sequence f_i is also eventually stationary; we have a contradiction, and A^* is a well ordered subset of $\mathrm{F}(A)$. ■

Theorem 4.5 is then only a formality since we have

$$\mathbb{N}\mathrm{Rat}\, A^* \subseteq \mathbb{N}\langle\langle A^* \rangle\rangle \subseteq \mathbb{Q}\langle\langle A^* \rangle\rangle \subseteq \mathbb{Q}_{\mathsf{wo}}\langle\langle F(A) \rangle\rangle \ ,$$

the first three inclusions being obvious and Corollary 7.15 ensuring the last one. ■

Exercises

7.5 Verify Lemma 7.11.

7.6 Justify our assertion in Theorem 4.7 that S^* is a well ordered subset, since we have only proved the property for S^+ in Proposition 7.13.

7.7 Verify Lemma 7.14.