CHAPTER 5

Idempotents and Hindman's theorem

In the last chapter, we proved an abstract version (4.9) of Schur's theorem: for every colouring of a semigroup $(S, \cdot)$ with finitely many colours, there are elements v, w of S such that v, w, and vw have the same colour. The proof heavily used the existence of an idempotent ultrafilter on S . In this chapter, we will prove a vast generalization of this result: for every colouring $S = A_1 \cup \cdots \cup A_r$ of S with finitely many colours, at least one of the colours A_j includes an IP-set, i.e. a (usually infinite) set with strong combinatorial structure.
In Section 1, we define the notion of an IP-set, state the main result Theorem 5.2, and point out some obvious reformulations resp. consequences. In Section 2, we prove the theorem – in fact, we show how IP-subsets of S are intimately connected to idempotent elements and to closed subsemigroups of βS. Section 3 extends this connection to some extent.

1. Statement of Hindman's theorem

For the definition of an IP-subset in a semigroup S, and later for the proof of the main theorem 5.5, we put up some notation. This looks quite technical, but is easily understood.

5.1. Definition (a) For any set X, we denote by $\mathcal{P}_f(X)$ the set of all non-empty finite subsets of X, as in 1.4.
(b) Assume that $(S, \cdot)$ is a semigroup, $\bar{x} = (x_i)_{i\in\omega}$ is an infinite sequence in S, and $e \in \mathcal{P}_f(\omega)$. We denote by p_e the product of the elements x_i, $i \in e$. More exactly, if $e = \{i_1, \ldots, i_k\}$ where $i_1 < \cdots < i_k$, we put $p_e = x_{i_1} \ldots x_{i_k}$. I.e. the elements x_i, $i \in e$, are multiplied from left to right in the order of their appearance in the sequence $\bar{x}$. (The order of multiplication is, of course, irrelevant in a commutative semigroup.)
(c) Given a sequence $\bar{x}$ as in (b), the subset $FP(\bar{x})$ of S (the set of *f*inite *p*roducts over $\bar{x}$) is defined by

$$FP(\bar{x}) = \{p_e : e \in \mathcal{P}_f(\omega)\}.$$

I.e. $FP(\bar{x}) = \{x_0, x_1, x_0x_1, x_2, x_0x_2, x_1x_2, x_0x_1x_2, x_3, \ldots\}$.
Similarly, for any subsequence $\bar{y} = (x_i)_{i\in I}$ of $\bar{x}$, where the index set I is a subset of ω, $FP(\bar{y})$ denotes the set $\{p_e : e \in \mathcal{P}_f(I)\}$.
(d) A subset A of S is called an *IP-set* if $FP(\bar{x}) \subseteq A$, for some infinite sequence $\bar{x} = (x_i)_{i\in\omega}$ in S.
(e) For $(S, +)$ a commutative semigroup in additive notation, we will write $s_e = \Sigma_{i\in e} x_i$ instead of p_e and similarly $FS(\bar{x})$ (the set of *f*inite *s*ums over $\bar{x}$) instead of $FP(\bar{x})$. We call $A \subseteq S$ an *IS-set* if $FS(\bar{x}) \subseteq A$, for some infinite sequence $\bar{x}$ in S.

In older literature, an IP-set is defined to be the set $FP(\bar{x})$, for some sequence $\bar{x} = (x_i)_{i\in\omega}$ in S, rather than an arbitrary superset of $FP(\bar{x})$. The denomination

"IP-set" for the set of all p_e, $e \in \mathcal{P}_f(\omega)$, comes from the following example. Assume that V is a vector space over an arbitrary field; its additive group $(V, +)$ is a commutative (semi-) group. Assume that $\bar{x} = (x_i)_{i\in\omega}$ is a sequence of linearly independent vectors in V. Then the set $FS(\bar{x}) = \{x_0, x_1, x_0 + x_1, x_2, x_0 + x_2, x_1 + x_2, x_0 + x_1 + x_2, x_3, \dots\}$, together with the zero vector, constitutes the set of edges of an $i$nfinite-dimensional $p$arallel epiped.

We can now state the abstract version of Hindman's theorem.

5.2. Theorem *Assume $(S, \cdot)$ is a semigroup and $S = A_1 \cup \dots \cup A_r$ is a colouring of S with r colours. Then at least one of the sets A_j, $j \in \{1, \dots, r\}$, is an IP-set.*

The abstract version of Schur's theorem 4.9 turns out to be an extreme special case of 5.2: if A_j is an IP-set, i.e. if there is some sequence $\bar{x}$ in S satisfying $FP(\bar{x}) \subseteq A_j$, then, for example, x_0, x_1 and x_0x_1 are all in A_j.

Hindman's theorem is the following special case of 5.2.

5.3. Corollary *(Hindman's finite sums theorem) Assume $\mathbb{N} = A_1 \cup \dots \cup A_r$ is a colouring of $\mathbb{N}$ with r colours. Then at least one of the sets A_j, $j \in \{1, \dots, r\}$, is an IS-set, in $(\mathbb{N}, +)$.*
Moreover the sequence $\bar{x} = (x_i)_{i\in\omega}$ proving this can be taken strictly increasing, i.e. such that $x_0 < x_1 < \dots$.

Just as for 4.9 and 4.10 , 5.2 can be deduced from its special case 5.3; see Exercise 1. Let us finally state a consequence of 5.3 which was proved much earlier.

5.4. Corollary *(Hilbert's theorem) Assume that $\mathbb{N} = A_1 \cup \dots \cup A_r$ is a colouring of $\mathbb{N}$ with r colours and that $m \in \mathbb{N}$. Then there are a sequence $\bar{y} = (x_1, \dots, x_m)$ in $\mathbb{N}$, an infinite subset B of $\mathbb{N}$ and some $j \in \{1, \dots, r\}$ such that $FS(\bar{y}) + B \subseteq A_j$.*

Proof. Take $j \in \{1, \dots, r\}$ and a strictly increasing sequence $\bar{x} = (x_i)_{i\in\mathbb{N}}$ such that $FS(\bar{x}) \subseteq A_j$. Then put $\bar{y} = (x_1, \dots, x_m)$ and $B = \{x_i : i \geq m + 1\}$. □

2. Proof of Hindman's theorem

The abstract version 5.2 of Hindman's theorem is the most interesting part of the following equivalence. We will define the notion of a multiplicative family, and other ones still missing, later in this section at the places where they are required.

5.5. Theorem *For any subset A of an arbitrary semigroup $(S, \cdot)$, the following are equivalent.*
(a) A is contained in an idempotent ultrafilter on S (i.e. $\hat{A}$ contains an idempotent of βS)
(b) A is an IP-set
(c) the power set $\mathcal{P}(A)$ of A includes a multiplicative family
(d) $\hat{A}$ includes a closed subsemigroup of βS.

Let us first note how Theorem 5.2 follows from 5.5, more exactly from the implication from (a) to (b): by 1.21, pick an idempotent p in βS; then pick $j \in \{1, \dots, r\}$ such that $A_j \in p$. By 5.5, A_j is an IP-set. In fact, this proof gives the following corollary which, in turn, implies, 5.2.

5.6. Corollary *If an IP-set $A \subseteq S$ is the union of finitely many subsets $A_1, \dots, A_r$, then at least one A_j is an IP-set.*

In 5.5 , the implication from (a) to (d) in 5.5 is trivial, because for any idempotent p in βS, $\{p\}$ is a closed subsemigroup of βS. But this observation is not too helpful, because we want to prove the chain (a) $\Rightarrow$ (b) $\Rightarrow$ (c) $\Rightarrow$ (d) $\Rightarrow$ (a) of implications. We handle the easiest one of these implications - (d) implies (a) - first and the least trivial one - (a) implies (b) - last.

Proof. **(d) implies (a), in 5.5** A straightforward application of Theorem 1.21: a closed subsemigroup T of βS included in $\hat{A}$ is a compact right topological semigroup, and 1.21 gives the existence of an idempotent in T and hence in $\hat{A}$. □

The implications from (c) to (d) and from (b) to (c) in 5.5 work smoothly with the following notion and lemma.

5.7. Definition A family $\mathcal{C}$ of subsets of a semigroup $(S, \cdot)$ is called *multiplicative* if it is nonempty, has the finite intersection property, and for every $C \in \mathcal{C}$ and every $c \in C$, there is some $D \in \mathcal{C}$ such that $c \cdot D \subseteq C$.

Multiplicative families are a standard tool for constructing closed subsemigroups of βS.

5.8. Lemma *Assume that $\mathcal{C} \subseteq \mathcal{P}(S)$ is a multiplicative family. Then $T = \bigcap_{C \in \mathcal{C}} \hat{C} = \{p \in \beta S : \mathcal{C} \subseteq p\}$ is a closed subsemigroup of βS.*

Proof. The set T is closed, being the intersection of closed sets; it is non-empty since $\mathcal{C}$ has the finite intersection property. So let p and q be elements of T with the aim of proving that $pq \in T$. Let C be any element of $\mathcal{C}$; we have to show that $C \in pq$.
By the multiplicative property of $\mathcal{C}$, we pick for every $c \in C$ some $D_c \in \mathcal{C}$ such that $c \cdot D_c \subseteq C$. Thus $\bigcup_{c \in C} c \cdot D_c \subseteq C$; since $C \in p$ and $D_c \in q$ holds for all $c \in C$, we see that $C \in pq$. □

Proof. **(c) implies (d), in 5.5** Assume $\mathcal{C}$ is a multiplicative family and $D \subseteq A$ holds for some $D \in \mathcal{C}$. The closed subsemigroup $T = \bigcap_{C \in \mathcal{C}} \hat{C}$ of βS is included in $\hat{D}$ and hence in $\hat{A}$. □

Proof. **(b) implies (c), in 5.5** Let $\bar{x} = (x_i)_{i \in \omega}$ be a sequence in S certifying that A is an IP-set, i.e. such that $FP(\bar{x}) \subseteq A$. For every $n \in \omega$, we consider the subsequence $(x_i)_{n \leq i < \omega}$ of $\bar{x}$ and define

$$C_n = FP((x_i)_{n \leq i < \omega}),$$

the subset of A containing the products p_e where e is a finite nonempty subset of $\{n, n+1, n+2, \dots\}$. So

$$\mathcal{C} = \{C_n : n \in \omega\}$$

is a subfamily of $\mathcal{P}(A)$; it has the finite intersection property because $C_{n+1} \subseteq C_n$ holds for all n.

To check that $\mathcal{C}$ is multiplicative, consider some $n \in \omega$ and some $c \in C_n$, say $c = p_e$ where $e \subseteq \{n, n+1, n+2, \dots\}$ is finite and nonempty. Then pick some $m \in \omega$ greater than every element of e and consider $D = C_m \in \mathcal{C}$; we show that $c \cdot D \subseteq C_n$. For any $d \in D$, say $d = p_\varepsilon$ where $\varepsilon \subseteq \{m, m+1, \dots\}$ is finite and nonempty, we have $c \cdot d = p_e \cdot p_\varepsilon = p_{e \cup \varepsilon}$; the last equality holds because every element of e is less than every element of ε. □

For the remaining implication from (a) to (b) in 5.5, we develop some additional notation and technical lemmas. Recall from 4.5 that, for $A \subseteq S$, $s \in S$ and $q \in \beta S$, the subsets $s^{-1}A$ and A^{-q} of S were defined by $s^{-1}A = \{x \in S : sx \in A\}$ and $A^{-q} = \{s \in S : s^{-1}A \in q\} = \{s \in S : A \in sq\}$. There are a few simple rules for computing with these sets.

5.9. Lemma *For $A, B \subseteq S$, $s, t \in S$ and $p, q \in \beta S$, the following hold.*
(a) $s^{-1}(A \cap B) = s^{-1}A \cap s^{-1}B$
(b) $t^{-1}s^{-1}A = (st)^{-1}A$
(c) $(A \cap B)^{-q} = A^{-q} \cap B^{-q}$
(d) $A^{-pq} = (A^{-q})^{-p}$.

Proof. (a) is obvious because $s^{-1}A$ is the preimage of A under the left multiplication $\lambda_s : S \to S$ with s and (b) because $\lambda_{st} = \lambda_s \circ \lambda_t$. (c) follows from (a) and the very definition of $s^{-1}A$. For (d), we have to show that, for any $s \in S$, $s \in A^{-pq}$ iff $s \in (A^{-q})^{-p}$. But $s \in A^{-pq}$ holds iff $s^{-1}A \in pq$ iff $A \in s(pq)$, and $s \in (A^{-q})^{-p}$ iff $A^{-q} \in sp$ iff (by 4.7) $A \in (sp)q$. □

5.10. Definition For $A \subseteq S$ and $p \in \beta S$, we define the subset A^* of S by

$$A^* = A \cap A^{-p}.$$

(A more exact notation would be A^{*p}, pointing out the dependence from p.)

The set A^* and its properties given by the next lemma are the key ingredients for the remaining implication from (a) to (b) in 5.5.

5.11. Lemma *Assume A^* is defined with respect to an idempotent ultrafilter p. Then the following hold.*
(a) $A \in p$ iff $A^{-p} \in p$ iff $A^* \in p$.
(b) $A^{**} = A^*$.
(c)AssumethatA $\in p$ and L is a finite subset of A^*. Then there is some $W \in p$ such that $W \subseteq A^*$ and $L \cdot W \subseteq A^*$.

Proof. (a) By 4.7, $A \in p = p \cdot p$ is equivalent to $A^{-p} \in p$.
(b) Writing $B = A^*$, we obtain from **??** that $A^{**} = B \cap B^{-p} = (A \cap A^{-p}) \cap (A^{-p} \cap (A^{-p})^{-p}) = A \cap A^{-p} = A^*$ – note that $A^{-p})^{-p} = A^{-p}$ because p is idempotent.
(c) We know from (a) and (b) that $A^{**} = A^*$ is an element of p. For every $x \in L$, $x \in A^{**}$ implies that there is some $W_x \in p$ such that $xW_x \subseteq A^*$. So $W = A^* \cap \bigcap_{x \in L} W_x$ works for the assertion. □

PROOF. **(a) implies (b), in 5.5** Assume that p is an idempotent ultrafilter on S and $A \in p$. Using the set $A^* \in p$, defined from p, we construct by induction elements $x_i, i \geq 1$ of S such that, for every $n \in \mathbb{N}$, the sequence $(x_i)_{1 \leq i \leq n}$ satisfies the inductive assertion

$$FP(x_i)_{1 \leq i \leq n} \subseteq A^*.$$

This shows that A^* and hence A is an IP-set.
To begin with, pick an arbitrary element x_1 of A^*; so the inductive assertion is satisfied for $n = 1$. Given $x_1, \ldots, x_n$ satisfying the inductive assertion for n, we apply 5.11 to the finite subset $L = FP(x_i)_{1 \leq i \leq n}$ of A^* and obtain a set $W \subseteq A^*$ such that $W \in p$ and $L \cdot W \subseteq A^*$. Let x_{n+1} be an arbitrary element of W.
To show the inductive assertion for $n+1$, consider a non-empty subset e of $\{1, \ldots, n+1\}$ with the aim of showing $p_e \in A^*$, where p_e is the product defined in 5.1. Now if $e \subseteq \{1, \ldots, n\}$, then $p_e \in A^*$ holds by the inductive assumption for n. If $e = \{n+1\}$, then $p_e = x_{n+1} \in W \subseteq A^*$. Otherwise, $p_e = p_\varepsilon \cdot x_{n+1}$ where ε is a non-empty subset of $\{1, \ldots, n\}$; in this case, $p_e \in L \cdot W \subseteq A^*$. □

5.12. Remark If, in the implication from (a) to (b) of 5.5, the idempotent ultrafilter p is free, then we can construct a witness $(x_i)_{i \geq 1}$ for the IP-set property of A in such a way that the x_i are pairweise distinct; in the case that the underlying set of S is $\mathbb{N}$, we can even guarantee that $x_1 < x_2 < x_3 < \ldots$. This is because, in the above construction of x_{n+1}, the set W is in p, hence infinite, and we can pick $x_{n+1} \in W \setminus \{x_1, \ldots, x_n\}$ or $x_{n+1} \in W \setminus \{1, \ldots, x_n\}$.

3. More on idempotent ultrafilters and IP-sets

Theorem 5.5 says that the sets contained in some idempotent ultrafilter on S are exactly the IP-sets. Conversely, if p is an ultrafilter on S consisting of IP-sets, does it follow that p is idempotent? Not quite, but a weaker statement holds: p belongs to the topological closure of the set $E(\beta S)$ of idempotent elements of βS. It seems worth while to state a simple topological fact on the space βS connected with this situation.

5.13. Lemma *Assume that M is a subset of βS and $p \in \beta S$. Then p belongs to the closure of M (in βS) iff $p \subseteq \bigcup M$, i.e. iff every set in p is contained in some $m \in M$.*

PROOF. The following assertions are clearly equivalent: $p \in \mathrm{cl}_{\beta S} M$; every neighbourhood of p intersects M; for every $A \in p$, there is some $m \in M$ such that $m \in \hat{A}$; for every $A \in p$, there is some $m \in M$ such that $A \in m$. □

We introduce the standard notation for the set of all idempotent elements of a semigroup and conclude which ultrafilters on a semigroup S have only IP-sets as their elements.

5.14. Definition For any semigroup $(S, \cdot)$, we denote by $E(S)$ the set of all idempotent elements of S:

$$E(S) = \{e \in S : e \cdot e = e\}.$$

5.15. Proposition *Let p be any ultrafilter on a discrete semigroup S. Then every set in p is an IP-set iff $p \in \mathrm{cl}_{\beta S} E(\beta S)$.*

Proof. We apply 5.13 to the set $M = E(\beta S)$ and note that by 5.5, $\bigcup M$ is the family of all IP-subsets of S. □

The set $\mathbb{N}$ of natural numbers is a semigroup both under addition and under multiplication, and we can apply the theory developed in this chapter both to $(\mathbb{N}, +)$ and to $(\mathbb{N}, \cdot)$. Here we have to distinguish the sets $E(\beta\mathbb{N}, +)$ and $E(\beta\mathbb{N}, \cdot)$ of idempotents in $\beta\mathbb{N}$ with respect to addition and to multiplication, and similarly IP-subsets of $\mathbb{N}$ with respect to addition and to multiplication, i.e. IS-sets and IP-sets, in the notation of 5.1. This suggests, among others, questions like whether there is an ultrafilter p on $\mathbb{N}$ such that $p = p + p = p \cdot p$, or whether there exists a sequence $\bar{x} = (x_i)_{i \in \omega}$ in $\mathbb{N}$ such that $FS(\bar{x}) = FP(\bar{x})$. The answer to both questions is negative - a result which we do not prove here. However, Proposition 5.16 states a nontrivial result connecting IS- and IP-subsets of $\mathbb{N}$.

5.16. Proposition *Assume $\mathbb{N} = A_1 \cup \cdots \cup A_r$ is a colouring of $\mathbb{N}$ with finitely many colours. Then at least one of the sets A_i is both an IS-set and an IP-set. I.e. there are $j \in \{1, \ldots, r\}$ and sequences $\bar{x} = (x_i)_{i \in \omega}$, $\bar{y} = (y_i)_{i \in \omega}$ in $\mathbb{N}$ such that $FS(\bar{x}) \subseteq A_j$ and $FP(\bar{y}) \subseteq A_j$.*

Proof. We first note that, for W an IS-subset of $\mathbb{N}$ and an arbitrary $v \in \mathbb{N}$, the set $vW = \{vw : w \in W\}$ is an IS-set, too. Because if $\bar{x} = (x_i)_{i \in \omega}$ witnesses the IS-property of W, i.e. $FS(\bar{x}) \subseteq W$, then $(vx_i)_{i \in \omega}$ witnesses the IS-property of vW. In $\beta\mathbb{N}$, denote by E the set $E(\beta\mathbb{N}, +) = \{p \in \beta\mathbb{N} : p + p = p\}$ of all additive idempotents and by P its closure in the space $\beta\mathbb{N}$. We claim that P is a multiplicative subsemigroup of $\beta\mathbb{N}$ – in fact, more holds true: for any $p \in \beta\mathbb{N}$ and $q \in P$, we have $pq \in P$. Because of 5.15, applied to $(\beta\mathbb{N}, +)$, we have to show that every $A \in pq$ is an IS-set. By 4.7, pick $V \in p$ and, for every $v \in V$, some $W_v \in q$ such that $\bigcup_{v \in V} vW_v \subseteq A$. Fix any $v \in V$; then $vW_v \subseteq A$ shows that A is an IS-set.
To prove the proposition, we pick an idempotent element p of the closed subsemigroup P of $(\beta\mathbb{N}, \cdot)$, and then $j \in \{1, \ldots, r\}$ such that $A_j \in p$. Then A_j is an IP-set by 5.5 and an IS-set by 5.15, because $p \in \mathrm{cl}_{\beta\mathbb{N}} E$. □

Exercises

(1) Deduce Theorem 5.2 from its special case 5.3.
(2) Assume that $\mathcal{C}$ is a family of subsets of a discrete semigroup S which satisfies the following assumption slightly weaker than multiplicativeness: for any $C \in \mathcal{C}$, there are $E \in \mathcal{C}$ and $D_e \in \mathcal{C}$, for $e \in E$, such that $\bigcup_{e \in E} eD_e \subseteq C$. Prove that $\bigcap_{C \in \mathcal{C}} \hat{C}$ is a (closed) subsemigroup of βS.
(3) Generalize the implication from (a) to (b) in 5.5 as follows. Assume that p is an idempotent of βS and $(A_n)_{n \in \omega}$ is a countable sequence of elements of p. Prove that there is a sequence $(x_i)_{i \in \omega}$ in S such that $FP(x_i)_{i \geq n} \subseteq A_n$ holds for every $n \in \omega$.
(4) In the additive semigroup of natural numbers, find infinitely many pairwise disjoint IS-subsets $A_n, n \in \omega$.
(5) Find disjoint subsets A and B of $\mathbb{N}$ such that A is an IS-set and B is an IP-set, with respect to the operations of addition and multiplication on $\mathbb{N}$.
(6) A family $\mathcal{A}$ of subsets of S is called *upward closed* if for $A \in \mathcal{A}$ and $A \subseteq B \subseteq S$, also $B \in \mathcal{A}$. It is *partition regular* if for $A \in \mathcal{A}$ and $A = A_1 \cup \cdots \cup A_r$, some A_j is in $\mathcal{A}$. E.g., for a semigroup S, the family of IP-subsets of S is partition

regular, by 5.6.
Prove that $\mathcal{A}$ is partition regular iff $\mathcal{A} = \bigcup M$ for some subset M of βS. And in this case, the closure of M in βS is the set of ultrafilters p satisfying $p \subseteq \mathcal{A}$, by 5.13.