A Remark on Subsemigroups (DICKSONs Lemma)

Klaus Pommerening

April 1975 – english version November 2011

We consider semigroups S that are commutative and contain 0. If $H \leq \mathbb{N}^n$ is a subsemigroup, then $\langle H \rangle$ denotes the subgroup of $\mathbb{Z}^n$ it generates. It consists of all differences $x - y$ with $x, y \in H$. We assume $\mathbb{Z}^n$ is equipped with the ordering $x \geq y \iff x - y \in \mathbb{N}^n$.

Proposition 1 *For a subsemigroup $H \leq \mathbb{N}^n$ the following statements are equivalent:*

(i) *If $x, y \in H$ with $x \geq y$, then also $x - y \in H$.*

(ii) $\langle H \rangle \cap \mathbb{N}^n = H$.

(iii) *There is a homorphism $\alpha\colon \mathbb{N}^n \longrightarrow S$ of semigroups with $H = \ker \alpha$.*

Proof. "(i) $\Longrightarrow$ (ii)": Take $x \in \langle H \rangle$. Then there are $y, z \in H$ such that $x = y - z$. If also $x \in \mathbb{N}^n$, then $y \geq z$. Therefore $x \in H$.

"(ii) $\Longrightarrow$ (iii)": Consider the natural homomorphism $\nu\colon \mathbb{Z}^n \longrightarrow \mathbb{Z}^n/\langle H \rangle$ and restrict it to $\mathbb{N}^n$. For $x \in \mathbb{N}^n$ we have the equivalences $x \in \ker \nu \iff \nu(x) = 0 \iff x \in \langle H \rangle \cap \mathbb{N}^n = H$.

"(iii) $\Longrightarrow$ (i)": Let $x, y \in H = \ker \alpha$, $x \geq y$. Then

$$\alpha(x - y) = \alpha(x - y) + \alpha(y) = \alpha(x - y + y) = \alpha(x) = 0,$$

whence $x - y \in \ker \alpha = H$. $\diamond$

Definition (HOCHSTER[3]) A subsemigroup $H \leq \mathbb{N}^n$ is called **full**, if it fulfills the the equivalent conditions of Proposition 1.

As a motivation for the following result note that not every subsemigroup of $\mathbb{N}^n$ is finitely generated. As an example take

$$H = \{(x, y) \mid y \geq 1\} \cup \{(0, 0)\} \subseteq \mathbb{N}^2,$$

see Figure 1.

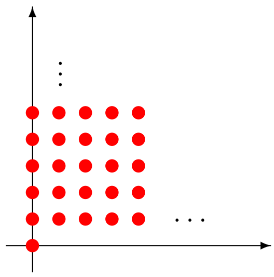

Figure 1: A non-full sub-semigroup

Theorem 1 *Let $H \le \mathbb{N}^n$ be a full subsemigroup. Then H is finitely generated.*

Proof. Let $E \subseteq H$ be the set of minimal elements > 0. Then

- E generates H: Otherwise take a minimal $h \in H$ such that $h \notin \langle E \rangle$. There is an $e \in E$ such that $e < h$. Then $h - e \in H$ and $h - e < h$, whence $h - e \in \langle E \rangle$ and $h \in \langle E \rangle$, contradiction.
- E is completely unordered, that means no two elements of E are comparable: This is immediate from minimality.

Now the assertion is an immediate consequence of the following lemma. $\diamond$

Lemma 1 (Dickson[1]) *Every completely unordered subset $E \subseteq \mathbb{N}^n$ is finite.*

Proof. Induction on n. We may assume $E \neq \emptyset$. If $n = 1$, then necessarily $\#E = 1$.

Now let $n \ge 2$. Fix $x = (x_1, \ldots, x_n) \in E$. For $1 \le i \le n$ and $0 \le j < x_i$ consider the sets

$$M_{ij} := \{y \in \mathbb{N}^n \mid y_i = j\}.$$

By omitting the fixed coordinate j each set $M_{ij} \cap E$ bijectively projects onto a completely unordered subset of $\mathbb{N}^{n-1}$, hence is finite by induction. Now

$$\mathbb{N}^n = \left(\bigcup_{i=1}^{n} \bigcup_{j=0}^{x_i - 1} M_{ij} \right) \cup (x + \mathbb{N}^n).$$

Intersection with E and noting $(x + \mathbb{N}^n) \cap E = \{x\}$ gives

$$E = \left(\bigcup_{i=1}^{n} \bigcup_{j=0}^{x_i - 1} E \cap M_{ij} \right) \cup \{x\},$$

a finite set. $\diamond$

We apply this result to two finiteness problems in elementary number theory.

Theorem 2 (GORDAN[2]) *Let*

$$\sum_{j=1}^{n} a_{ij}x_j = 0 \quad \textit{for } i = 1, \dots q \quad \textit{with } a_{ij} \in \mathbb{Z} \textit{ for all } i, j$$

be a system of linear diophantine equations. Then the semigroup of non-negative solutions (i. e. solution vectors in $\mathbb{N}^n$) is finitely generated.

Proof. The solutions are the elements of the kernel of a semigroup homorphism $\mathbb{N}^n \longrightarrow \mathbb{Z}^q$, hence form a full subsemigroup of $\mathbb{N}^n$. $\diamond$

Theorem 3 *Let*

$$\sum_{j=1}^{n} a_{ij}x_j \equiv 0 \pmod{m} \quad \textit{for } i = 1, \dots q \quad \textit{with } a_{ij} \in \mathbb{Z} \textit{ for all } i, j$$

be a system of linear congruences modulo a natural number $m \geq 2$. Then the semigroup of non-negative solutions (i. e. solution vectors in $\mathbb{N}^n$) is finitely generated.

Proof. As before; this time we consider the semigroup homorphism $\mathbb{N}^n \longrightarrow (\mathbb{Z}/m\mathbb{Z})^q$. $\diamond$

References

[1] L. E. Dickson: Finiteness of the odd perfect and primitive abundant numbers with n distinct prime factors. Amer. J. Math. 35 (1913), 413–422.

[2] P. Gordan: Beweis, dass jede Covariante und Invariante einer binären Form eine ganze Function mit numerischen Coeffizienten einer endlichen Anzahl solcher Formen ist. J. reine angew. Math. 69 (1868), 323–354.

[3] M. Hochster: Rings of invariants of tori, Cohen-Macaulay rings generated by monomials, and polytopes. Annals of Math. 96 (1972), 318–337.