MONOIDS

Notes by Walter Noll (1992)

1 Invertible Elements, Pure Monoids

We assume that a monoid M, described with multiplicative notation and terminology and with unit u, is given.

Proposition 1: *For every $a \in M$, the problem*

$$? \ x \in M \qquad ax = xa = u \tag{P_a}$$

has at most one solution.

Definition 1: *We say that $a \in M$ is* **invertible** *if* (P_a) *has a solution and we denote this solution by a^{-1} and call it the* **inverse** *of a. The set of all invertible elements of M will be denoted by* Inv M.

Proposition 2: Inv M *is a groupable submonoid of M. We have $a^{-1} \in$* Inv M *for all $a \in$* Inv M *and the mapping $(a \mapsto a^{-1})$*: Inv $M \to$ Inv M, *taken to be the inversion, endows* Inv M *with the structure of a group, which we call the* **group of invertibles** *of M.*

Of course, M is groupable if and only if Inv $M = M$.

Definition 2: *We say that M is a* **pure monoid** *if* Inv $M = \{u\}$.

The multiplicative monoids $\mathbb{N}$ and $\mathbb{N}^\times$ are pure. the additive monoid $\mathbb{N}$ is also pure. Let a set S be given. Then Sub S is a pure monoid both relative to union and to intersection. We have Inv (Map (S, S)) = Perm S if Map (S, S) is regarded as a monoid relative to composition. We have Inv $\mathbb{Z} = \{1, -1\}$ when $\mathbb{Z}$ is regarded as a multiplicative monoid.

Theorem: *Put $U :=$* Inv M *and assume that*

$$aU = Ua \ \text{ for all } a \in M. \tag{1}$$

Then

$$\mathcal{P} := \{aU \mid a \in M\} \tag{2}$$

is a partition of M. Moreover, we have $U \in \mathcal{P}$ and

$$PQ \in \mathcal{P} \ \text{ for all } P, Q \in \mathcal{P}. \tag{3}$$

$\mathcal{P}$ acquires the structure of a pure monoid if we define its multiplication by $(P,Q) \mapsto PQ$ and its unity by U. We call $\mathcal{P}$ the **pure monoid associated with** *M. The partition mapping*

$$\pi_M : M \to \mathcal{P} \tag{4}$$

characterized by $x \in \pi_M(x)$ for all $x \in M$ is a surjective monoid homomorphism. If M is cancellative, so is $\mathcal{P}$.

Of course, if M is commutative, the condition (1) is satisfied and one can always construct the associated pure monoid $\mathcal{P}$.

2 Divisibility, Prime Elements

We now assume that a *commutative* monoid M is given.

Defnition: *Given $a, b \in M$. we say that a is a* **divisor** *and that b is a* **multiple** *of a, and we write a* div *b, if $b \in aM$, i.e., if*

$$ax = b \text{ for some } x \in M. \tag{5}$$

For a given subset S of M we define the set of all **common divisors** *of S by*

$$Cd\ S := \{a \in M \mid a \text{ div } b \text{ for all } b \in S\} \tag{6}$$

and the set of all **common multiples** *of S by*

$$Cm\ S := \{b \in M \mid a \text{ div } b \text{ for all } a \in S\}. \tag{7}$$

We have $u \in Cd\ S$ for every $S \in \text{Sub } M$. If $a, b \in M$ is given, then $ab \in Cm\{a, b\}$.

Proposition 1: *The relation* div *in M defined above is reflexive and transitive. If M is cancellative and pure then* div *is also antisymmetric and hence an order.*

Definition 2: *Assume that M is cancellative and pure, so that* div *is an order in M.*

A given $p \in M$ is called a **prime element** *if*

$$a \text{ div } p \Rightarrow a = u \text{ or } a = p \text{ for all } a \in M, \tag{8}$$

which is equivalent to saying that p is a minimal element of $M \backslash \{u\}$. The set of all prime elements M will be denoted by PrM.

Let S be a subset of M. If S has an infimum [supremum] relative to the div*-order, we call this infimum [supremum] the* **greatest common divisor [least common multiple]** *of S and denote it by* gcd S [lcm S].

Proposition 2: *Assume that M is cancellative and pure and let $S \in \mathrm{Sub}\ M$ be given. If both S and aS have a greatest common divisor [least common multiple] then*

$$\gcd(aS) = a(\gcd\ S)\ \ [\mathrm{lcm}(aS) = a(\mathrm{lcm}\ S)]. \tag{9}$$

Now assume that M is cancellative but not necessarily pure. We then consider the associated pure monoid $\mathcal{P}$, which is also cancellative (see the Theorem of Sect. 1). We say that $p \in M$ is a **prime element** of M if $\pi_M(p)$ is a prime element of $\mathcal{P}$.

Given $S \in \mathrm{Sub}\ M$ we define

$$\mathrm{Gcd}\ S := \{d \in Cd\ S \mid d' \text{ div } d \ \text{ for all } d' \in Cd\ S\} \tag{10}$$

$$\mathrm{Lcm}\ S := \{m \in Cm\ S \mid m \text{ div } m' \ \text{ for all } m' \in Cm\ S\} \tag{11}$$

Proposition 3: *Let $S \in \mathrm{Sub}\ M$ be given. Then* Gcd $S \neq \emptyset$ [Lcm $S \neq \emptyset$] *if and only if $(\pi_M)_>(S)$ has a greatest common divisor [least common multiple] in $\mathcal{P}$ as defined in Def. 2. If this is the case, then*

$$\mathrm{Gcd}\ S = \gcd(\pi_M)_>(S).\ \ [\mathrm{Lcm}\ =\ \mathrm{lcm}(\pi_M)_>(S).] \tag{12}$$

Proposition 4: *An element $p \in M$ is prime if and only if*

$$a \text{ div } p \Rightarrow a \in\ \mathrm{Inv}(M) \text{ or } a \in p\ \mathrm{Inv}(M). \tag{13}$$

3 Prime-Decompositions, Factorial Monoids.

Let a set I be given. Then the set $\mathbb{N}^{(I)}$ of all families in $\mathbb{N}$ indexed on I and with finite support has the natural structure of an additive monoid, the addition being defined by termwise addition. It is clear that this monoid is cancellative and pure. The set $\mathbb{N}^{(I)}$ has also a natural order structure $\leq$, defined by using the order $\leq$ in $\mathbb{N}$ termwise.

Proposition 1: *The natural order $\leq$ in $\mathbb{N}^{(I)}$ coincides with the* div*-order in $\mathbb{N}^{(I)}$ determined by the additive monoid structure of $\mathbb{N}^{(I)}$ according to Prop. 1 of Section 2.*

We recall that an order relation on a set S is said to be *inductive* if every non-empty subset of S has at least one minimal element.

Proposition 2: *The order* $\leq$ *in* $\mathbb{N}^{(I)}$ *is an inductive lattice-order. More precisely, every non-empty subset* S *of* $\mathbb{N}^{(I)}$ *has a minimal element and, given* $\delta, \rho \in \mathbb{N}^{(I)}$, *we have*

$$\sup\{\delta, \rho\} = (\max\{\delta_i, \rho_i\} \mid i \in I) \in \mathbb{N}^{(I)} \tag{14}$$

and

$$\inf\{\delta, \rho\} = \{\min\{\delta_i, \rho_i\} \mid i \in I) \in \mathbb{N}^{(I)}. \tag{15}$$

We now assume that a commutative, cancellative, and pure monoid M is given and we consider the mapping

$$\Phi : \mathbb{N}^{(PrM)} \to M \tag{16}$$

defined by

$$\Phi(\delta) := \prod_{p \in PrM} p^{\delta_\pi} \quad \text{for all } \delta \in \mathbb{N}^{(PrM)}. \tag{17}$$

Proposition 3: *The mapping* Φ *is a monoid-homomorphism from the additive monoid* $\mathbb{N}^{(PrM)}$ *into* M *and is also strictly isotone when* $\mathbb{N}^{(PrM)}$ *is ordered by* $\leq$ *and* M *by* div.

Definition 2: *We say that* M *is a* **factorial monoid** *if the mapping* Φ *defined by* (17) *is invertible. If this is the case we write* $Pd := \Phi^{\leftarrow}$ *and, given* $a \in M$, *we call* $Pd(a) \in \mathbb{N}^{(PrM)}$ *the* **prime-decomposition** *of* a.

Proposition 4: *If* M *is factorial then the mapping* Φ *defined by* (17) *is a monoid-isomorphism and an order-isomorphism; also, the order* div *in* M *is an inductive lattice-order.*

Proposition 5: *Assume that* div *is a lattice-order and let* $p \in PrM\ M$ *be given. Then*

$$p \text{ div } ab \Rightarrow (p \text{ div } a \quad \text{or} \quad p \text{ div } b) \text{ for all } a, b \in M \tag{18}$$

Proposition 6: *The mapping* Φ *definted by* (17) *is injective if and only if the order* div *in* M *is lattice-order.*

Proposition 7: *The mapping* Φ *defined by* (17) *is surjective if and only if the order* div *in* M *is inductive.*

Theorem: *The monoid M is factorial if (and only if) the order* div *in M is an inductive lattice-order.*

Now let a commutative and cancellative, but not necessarily pure, monoid M be given. We say that M if **factorial** if the associated pure monoid $\mathcal{P}$ is factorial. Assume that this is the case and let $a \in M$ be given. We can then determine $\delta \in \mathbb{N}^{Pr\mathcal{P}}$ such that, for every family $(q_P \mid P \in \text{ Supt } \delta)$ such that $q_P \in P$ for all $P \in \text{ Supt } \delta$, there is $c \in \text{Inv } M$ such that

$$a = c \prod_{P \in \text{ Supt } \delta} q_P \tag{19}$$

Example: The multiplicative monoid $\mathbb{N}^x$ is cancellative and pure, and so is the multiplicative monoid $\text{Mpol}_{\mathbb{F}}$ of all monic polynomials over a field $\mathbb{F}$. It is easy to see that the div order is an inductive lattice order in both cases. Hence, both monoids are factorial. In the past literature, the prime decomposition theorems in these cases are treated separately.