DIVISIBILITY IN COMMUTATIVE MONOIDS

PAVEL RŮŽIČKA

Abstract. We recall some properties of quasi-ordered sets and we define suprema, infima, and the order quotient of an quasi-ordered set. We will study the relation of divisibility in commutative cancellative monoids, focusing on the existence and the uniqueness of decompositions into products of irreducible elements. We apply our results to characterize unique factorization monoids.

1.1. **Quasi-order, induced equivalence, suprema and infima.** Recall that a *quasi-order* on a set M is a reflexive and transitive binary relation on M. A quasi-order $\mid$ on M induces an equivalence relation $\sim$ defined by

$$a \sim b \iff a \mid b \text{ and } b \mid a.$$

We denote by $\boldsymbol{a}$ the block of the equivalence relation $\sim$ containing a and we set

$$M/_{\sim} := \{\boldsymbol{a} \mid a \in M\}.$$

Observe that if $a \sim a'$ and $b \sim b'$, then $a \sim b \iff a' \sim b'$. Therefore we can define a binary relation $\mid$ on the set $M/_{\sim}$ so that

$$\boldsymbol{a} \mid \boldsymbol{b} \iff a \mid b.$$

It is straightforward that $\mid$ forms a partial order on $M/_{\sim}$. We will call the set $M/_{\sim}$ the *order-quotient* of the quasi-ordered set M. A *canonical projection* is the map

$$p_{\sim} \colon M \to M/_{\sim}$$
$$a \mapsto \boldsymbol{a}.$$

A *lower bound* of a subset X of a quasi-ordered set M is an element $l \in M$ such that $l \mid x$ for all $x \in X$. An *infimum* of the set X is $i \in M$ such that

- i is a lower bound of X,
- $l \mid i$ for all lower bounds l of X.

The infimum of the set X is not unique, but if j is another infimum of X, then $i \mid j$ (since i is a lower bound of X and j is an infimum of X) and, similarly, $j \mid i$ (since j is a lower bound and i is an infimum). Therefore $j \sim i$. On the other hand, if i is an infimum of X and $j \sim i$, then it is readily seen from the transitivity of $\mid$ that j is an infimum of X as well. Therefore all infima of the set X form a block of $\sim$. In the order-quotient

March 1 and March 8, 2019.

$M/_{\sim}$ the block of all infima of X corresponds to a least lower bound of the set $\{\boldsymbol{x} \mid x \in X\}$. Dually we define greatest upper bounds and *suprema* of subsets of M.

1.2. **Divisibility.** Let $\boldsymbol{M} = (M, \cdot, 1)$ be a commutative monoid and $a, b \in M$. We say that a *divides* b (and we write $a \mid b$) if there is $c \in M$ such that $b = a \cdot c$. It is straightforward that the binary relation $\mid$ of divisibility is reflexive and transitive. Therefore $\mid$ is a quasi-order on M.

The quasi-order of divisibility induces an equivalence relation $\sim$ on M (given by $a \sim b$ if $a \mid b$ and $b \mid a$). When $a \sim b$, we say that the elements a and b are *associated*. We say that a *properly divides* b if $a \mid b$ and $b \nmid a$ (or, equivalently, if $a \mid b$ and $a \nsim b$).

Observe that if $a \mid a'$ and $b \mid b'$, then $a \cdot b \mid a' \cdot b'$ and, consequently, $a \sim a'$ and $b \sim b'$ implies that $a \cdot b \sim a' \cdot b'$. It follows that the multiplication on $\boldsymbol{M}$ induces an associative operation on $M/_{\sim}$ and $\mathbf{1}$ is a unit element. We will call the monoid $\boldsymbol{M}/_{\sim} = (M_{\sim}, \cdot, \mathbf{1})$ the *order-quotient* of $\boldsymbol{M}$. Clearly, the monoid $\boldsymbol{M}/_{\sim}$ is partially ordered by the relation of divisibility.

Example 1.1. *Let $\mathbb{Z}^*$ denote the multiplicative monoid of all non-zero integers. Observe that $\boldsymbol{a} = \{a, -a\}$ for every non-zero integer a. The map $[a]_{\sim} \mapsto |a|$ defines an izomorphism $(\mathbb{Z}^*/_{\sim}, \cdot) \overset{\cong}{\to} (\mathbb{N}, \cdot)$ onto the monoid $\mathbb{N}$ of all positive integers.*

Lemma 1.2. *Let $\boldsymbol{M}$ be a commutative cancellative monoid, let $a, b \in M$. Then $a \sim b$ if and only if there is an invertible element $u \in M$ such that $b = a \cdot u$.*

Proof. ($\Rightarrow$) Suppose that $a \sim b$. Then $a \mid b$ and $b \mid a$, that is, there are $u, v \in M$ satisfying $b = a \cdot u$ and $a = b \cdot v$. It follows that $a = a \cdot u \cdot v$ and from the cancellativity we get that $1 = u \cdot v$. Since $\boldsymbol{M}$ is commutative, we conclude that u is invertible. ($\Leftarrow$) Suppose that there is an invertible element $u \in M$ such that $b = a \cdot u$. Let v be an inverse of u. Then $1 = u \cdot v$, and so $a = a \cdot 1 = a \cdot u \cdot v = b \cdot v$. Therefore $a \mid b$ and $b \mid a$, hence $a \sim b$. $\square$

Corollary 1.3. *Let $\boldsymbol{M}$ be a commutative cancellative monoid. Then*

$$\boldsymbol{a} = a \cdot \mathbf{1} = \{a \cdot u \mid u \sim 1\},$$

for all $a \in M$.

Definition 1.4. Let $\boldsymbol{M}$ be a commutative monoid. We say that an element $p \in M$ is *prime* provided that p is not invertible and

$$p \mid a \cdot b \implies p \mid a \text{ or } p \mid b,$$

for all $a, b \in M$.

An element $q \in M$ is *irreducible* provided that q is not invertible and

$$q \sim a \cdot b \implies q \sim a \text{ or } q \sim b,$$

for all $a, b \in M$.

By induction we prove that

Lemma 1.5. *Let $\boldsymbol{M}$ be a commutative monoid. An element $p \in M$ is prime if and only if*

$$p \mid a_1 \cdots a_n \implies p \mid a_i \text{ for some } i \in \{1, 2, \dots, n\},$$

for all $n \in \mathbb{N}$ and all $a_1, \dots, a_n \in M$.

An element $q \in M$ is irreducible if and only if

$$q \sim a_1 \cdots a_n \implies q \sim a_i \text{ for some } i \in \{1, 2, \dots, n\},$$

for all $n \in \mathbb{N}$ and all $a_1, \dots, a_n \in M$.

Lemma 1.6. *Every prime element of a commutative monoid $\boldsymbol{M}$ is irreducible.*

Proof. Let $p \in M$ be a prime element and $p \sim a \cdot b$ for some $a, b \in M$. Then either $p \mid a$ or $p \mid b$. Since both $a \mid p$ and $b \mid p$, we conclude that either $p \sim a$ or $p \sim b$. It follows that p is irreducible. □

In general not every irreducible element is prime. We will have a closer look at this phenomenon later.

1.3. The uniqueness of decompositions.

Lemma 1.7. *Let $\boldsymbol{M}$ be a commutative cancellative monoid. If*

$$p_1 \cdot p_2 \cdots p_m \mid q_1 \cdot q_2 \cdots q_n, \tag{1.1}$$

where all $p_1, \dots, p_m$ are primes and all $q_1, \dots, q_n$ are irreducible. Then $m \leq n$ and there is a permutation σ of the set $\{1, 2, \dots, n\}$ such that $p_i \sim q_{\sigma(i)}$ for all $i = 1, 2, \dots, m$.

Proof. We proceed by induction on m. The statement holds trivially when $m = 0$. Suppose that $0 < m$ and the statement holds whenever we have less than m primes on the left hand side of (1.2). Since $p_1 \mid q_1 \cdot q_2 \cdots q_n$ and p_1 is a prime, $p_1 \mid q_j$ for some $1 \leq j \leq n$. After suitably permuting the indices $1, 2, \dots, n$ we get that $p_1 \mid q_1$. Since q_1 is irreducible, we infer that $p_1 \sim q_1$. Finally, since the monoid $\boldsymbol{M}$ is cancellative, we have that

$$p_2 \cdots p_m \mid q_2 \cdots q_n,$$

and we can apply the induction hypothesis. □

Since every prime element of a commutative cancellative monoid is irreducible, we get that

Corollary 1.8. *Let $\boldsymbol{M}$ be a commutative cancellative monoid. If*

$$p_1 \cdot p_2 \cdots p_m \sim q_1 \cdot q_2 \cdots q_n,$$

where all $p_1, \dots, p_m$, $q_1, \dots, q_n$ are primes, then $m = n$, and there is a permutation σ of the set $\{1, 2, \dots, m\}$ such that $p_i \sim q_{\sigma(i)}$ for all $i = 1, 2, \dots, m$.

In particular, if an element of an order quotient $\boldsymbol{M}/_{\sim}$ decomposes into a product of primes, then the decomposition is unique up a permutation of the primes.

1.4. **The minimal property and the existence of decompositions.** Let $(Q, \leq)$ be a quasi-ordered set. For elements $a, b \in Q$ we denote by $a < b$ that $a \leq b$ and $a \nsim b$. A *minimal element* of a non-empty subset X of Q is $x \in X$ such that $y \nless x$ for all $y \in X$ (i.e., there is no strictly smaller element than x in X). Dually we define *maximal* elements of non-empty subsets of quasi-ordered sets.

Definition 1.9. We say that a quasi-ordered set Q satisfies the *minimal property* (resp. the *maximal property*) provided that every non-empty subset of Q has a minimal (resp. maximal) element.

Lemma 1.10. *A quasi-oredered set Q has the minimal property if and only if Q does not contain an infinite strictly decreasing chain $a_1 > a_2 > \dots$.*

Proof. ($\Rightarrow$) The elements of a strictly decreasing chain $a_1 > a_2 > \dots$ form a subset $\{a_1, a_2, \dots\}$ without a minimal element. ($\Leftarrow$) Suppose that there is a non-empty subset X of Q without a minimal element. We construct inductively a strictly decreasing chain from its elements. We pick $a_1 \in X$ arbitrary and having constructed a finite chain $a_1 > a_2 > \dots > a_n$ we pick $a_{n+1} \in X$ so that $a_n > a_{n+1}$. Such a_{n+1} exists since otherwise a_n would be a minimal element of X. □

Lemma 1.11. *In a commutative cancellative monoid, if*

$$a \mid p_1 \cdot p_2 \cdots p_n,$$

where $p_1, p_2, \dots, p_n$ are primes, then there are $1 \leq i_1 < i_2 < \dots < i_m \leq n$ such that

$$a \sim p_{i_1} \cdot p_{i_2} \cdots p_{i_m}.$$

Proof. We will prove the lemma by induction on the number of primes n. If $n = 0$, then a is invertible and the statement trivially holds true. Suppose that it holds whenever the number of primes is less than n. Let b be such that $a \cdot b = p_1 \cdot p_2 \cdots p_n$.

If $p_n \mid b$, there is b' such that $b = b' \cdot p_n$. Canceling p_n, we get that $a \cdot b' = p_1 \cdot p_2 \cdots p_{n-1}$. By the induction hypothesis , there are $1 \leq i_1 < \dots < i_m \leq n - 1$ such that $a \sim p_{i_1} \cdot p_{i_2} \cdots p_{i_m}$.

If $p_n \mid a$, there is a' such that $a = a' \cdot p_n$. Canceling p_n, we get that $a' \cdot b = p_1 \cdot p_2 \cdots p_{n-1}$. By the induction hypothesis , there are $1 \leq i_1 < \dots < i_{m-1} \leq n - 1$ such that $a' \sim p_{i_1} \cdot p_{i_2} \cdots p_{i_{m-1}}$. With $i_m := n$, we get that $i_{m-1} < i_m \leq n$ and $a \sim p_{i_1} \cdot p_{i_2} \cdots p_{i_m}$. □

Clearly, in the previous lemma, $m = n$ if and only if $a \sim p_1 \cdot p_2 \cdots p_n$. We conclude that

Corollary 1.12. *Let a, b be elements of a commutative cancellative monoid. If b is a product of n primes and a properly divides b, then a is a product of less than n primes.*

Lemma 1.13. *Let $\boldsymbol{M}$ be a commutative cancellative monoid.*

(1) *If every element of $\boldsymbol{M}$ is a product of primes, then $(M, |)$ satisfies the minimal property.*

(2) *If $(M, |)$ satisfies the minimal property, then every element of $\boldsymbol{M}$ is a product of irreducible elements.*

Proof. (1) It follows from Corollary 1.12 that if $a \in M$ is a product of n primes, then the sequence $a = a_1, a_2, \dots$ such that a_{i+1} properly divides a_i for all $1 \leq i$ has length at most $n + 1$. Therefore, if every element of $\boldsymbol{M}$ is a product of primes, then there is not an infinite sequence $a_1, a_2, \dots$ such that a_{i+1} properly divides a_i for all $1 \leq i$. According to Lemma 1.10, $(M, |)$ satisfies the minimal property. (2) Suppose that the quasi-ordered set $(M, |)$ satisfies the minimal property. Let us denote by $\mathcal{I}$ the set of all elements of M that are not product of irreducible elements. Suppose that the set $\mathcal{I}$ is non-empty. Then it contains a minimal element, say a. The element a is clearly neither irreducible nor invertible, and so it decomposes into a product $a = b \cdot c$ of proper divisors. It follows from the minimality of a that none of the elements b, c belongs to $\mathcal{I}$, hence they are product of primes. But then a is a product of primes as well, which contradicts that $a \in \mathcal{I}$. □

1.5. **Greates common divisors.**

Definition 1.14. A *greatest common divisor* of elements $a_1, \dots, a_n \in M$ is an infimum of the set $\{a_1, \dots, a_n\}$ with respect to the quasi-order $|$. The greatest common divisor is unique up to associativity. In fact, all the greatest common divisors of the given elements form a block of $\sim$. We will denote this block by $(a_1, \dots, a_n)$. Similarly we define a *least common multiple* of elements $a_1, \dots, a_n \in M$ as a supremum of the set $\{a_1, \dots, a_n\}$.

Remark 1.15. We will slightly abuse our notation denoting by

$$(a_1, \dots, a_n, X_1, \dots, X_m)$$

the greatest common divisor of the union $a_1, \dots, a_n \cup X_1 \cup \cdots \cup X_m$.

Lemma 1.16. *Let $\boldsymbol{M}$ be a commutative monoid, $a, b, c \in M$. Then*

$$(a, (b, c)) = ((a, b), c). \tag{1.1}$$

Proof. Let $\boldsymbol{d} = (a, (b, c))$ and $\boldsymbol{e} = ((a, b), c)$. We prove that $d \sim e$. Furthermore, let $\boldsymbol{f} := (b, c)$ and $\boldsymbol{g} := (a, b)$. Then $d \mid a$ and $d \mid f$. Since $d \mid f$, we have that $d \mid b$ and $d \mid c$. From $d \mid a$ and $d \mid b$ we infer that $d \mid g$ and, since $d \mid c$, we conclude that $d \mid e$. Similarly we prove that $e \mid d$. □

Corollary 1.17. *Let $\boldsymbol{M}$ be a commutative monoid. If a greatest common divisor exists for each pair of elements of $\boldsymbol{M}$, then a greatest common divisor exists for every non-empty finite subset $\{a_1, \dots, a_n\}$ of $\boldsymbol{M}$ and it can be computed inductively as*

$$(a_1, a_2, \dots, a_n) = ((a_1, \dots, a_{n-1}), a_n).$$

Lemma 1.18. *Let $\boldsymbol{M}$ be a commutative cancellative monoid. Let $a, b, c \in M$ be such that both (a, b) and $(a \cdot c, b \cdot c)$ exist. Then*

$$(a \cdot c, b \cdot c) = (a, b) \cdot c.$$

Proof. Let $\boldsymbol{d} = (a, b)$ and $\boldsymbol{e} = (a \cdot c, b \cdot c)$. From $d \mid a$ we get that $d \cdot c \mid a \cdot c$. Similarly, $d \mid b$ implies that $d \cdot c \mid a \cdot c$. We conclude that $d \cdot c \mid e$. It follows that there is $x \in M$ such that

$$e = d \cdot c \cdot x.$$

Since $e \mid a \cdot c$ and $e \mid b \cdot c$, there are $y, z \in M$ such that

$$a \cdot c = e \cdot y = d \cdot c \cdot x \cdot y,$$
$$b \cdot c = e \cdot z = d \cdot c \cdot x \cdot z.$$

Since the monoid $\boldsymbol{M}$ is cancellative, we infer that

$$a = d \cdot x \cdot y \quad \text{and} \quad b = d \cdot x \cdot z.$$

Therefore $d \cdot x$ is a common divisor of a, b, and so $d \cdot x \mid d$. It follows that x is invertible, hence $e \sim d \cdot c$, whence $\boldsymbol{e} = \boldsymbol{d}$. □

We say that $a, b \in M$ are *relatively prime* if $(a, b) = \mathbf{1}$.

Lemma 1.19. *Let $\boldsymbol{M}$ be a commutative cancellative monoid such that the greatest common divisor exists for each pair of elements of M. Let $a, b, c \in M$. If $(a, b) = \mathbf{1}$ and $(a, c) = \mathbf{1}$, then $(a, b \cdot c) = \mathbf{1}$.*

Proof. Applying Lemma 1.18, we get from $(a, b) =\sim 1$, that $(a \cdot c, b \cdot c) = \mathbf{1} \cdot c = \boldsymbol{c}$. Similarly, we infer from $(1, c) = \mathbf{1}$, that $(a, a \cdot c) = \boldsymbol{a}$. It follows from Lemma 1.16 that

$$(a, b \cdot c) = ((a, a \cdot c), b \cdot c) = (a, (a \cdot c, b \cdot c)) = (a, c) = \mathbf{1}.$$

□

Observe that from Lemma 1.19 it follows that

Corollary 1.20. *Let $\boldsymbol{M}$ be a commutative cancellative monoid such that the greatest common divisor exists for each pair of elements of M, $a \in M$. Then the set of all elements of $\boldsymbol{M}$ that are relatively prime to the element a forms a submonoid of $\boldsymbol{M}$.*

Theorem 1.21. *Let $\boldsymbol{M}$ be a commutative cancellative monoid. If every pair of elements of $\boldsymbol{M}$ has a greatest common divisor, then every irreducible element of $\boldsymbol{M}$ is prime.*

Proof. Suppose that the assumptions of the theorem hold true and let q be an irreducible element of $\boldsymbol{M}$. Let $a, b \in M$. Since q is irreducible either $q \mid a$, in which case $(q, a) = \boldsymbol{a}$ or $(q, a) = \mathbf{1}$. It follows that if $q \nmid a$ and $q \nmid b$, then $(q, a) = (q, b) = \mathbf{1}$. From Lemma 1.19 we infer that $(q, a \cdot b) = \mathbf{1}$, hence $q \nmid a \cdot b$. Therefore q is a prime element of $\boldsymbol{M}$. □

Corollary 1.22. *Let $\boldsymbol{M}$ be a commutative cancellative monoid such that every pair of elements of $\boldsymbol{M}$ has a greatest common divisor. If*

$$p_1 \cdot p_2 \cdots p_m \sim q_1 \cdot q_2 \cdots q_n, \tag{1.2}$$

where all $p_1, \dots, p_m$ and $q_1, \dots, q_n$ are irreducible elements, then $m = n$ and there is a permutation σ of the set $\{1, 2, \dots, n\}$ such that $p_i \sim q_{\sigma(i)}$ for all $i = 1, 2, \dots, n$.

In particular, if an element of the order quotient $\boldsymbol{M}/_{\sim}$ decomposes into a product of irreducible elements, then the elements are determined uniquelly up to permutation.

Proof. Apply Lemma 1.7, Corollary 1.8, and the previous theorem. □

1.6. Unique factorization monoids.

Definition 1.23. A commutative cancellative monoid $\boldsymbol{M}$ is said to be *unique factorization* provided that every non-invertible element $a \in M$ has a factorization $a = q_1 \cdots q_n$ into a product of irreducible elements and the elements $\boldsymbol{q}_1, \dots, \boldsymbol{q}_n$ are uniquely determined up to permutation.

The *height* of an element $a = q_1^{\alpha_1} \cdots q_n^{\alpha_n}$ of a unique factorization monoid is the number $h(a) := n$ of irreducible elements in its decomposition. Note that elements of height 0 are exactly irreducible ones. Observe also that

$$c = a \cdot b \implies h(c) = h(a) + h(b). \tag{1.1}$$

Indeed, if $a := q_1 \cdot q_2 \cdots q_n$ and $b = r_1 \cdot r_2 \cdots r_m$ are decompositions of the elements a and b, respectively, into products of irreducible elements, then $c := q_1 \cdots q_n \cdot r_1 \cdots r_m$ is the unique decomposition of c. From (1.1) we infer that

Lemma 1.24. *Let a, b be elements of a unique factorization monoid. If $a \mid b$, then $h(a) \leq h(b)$. Moreover $a \mid b$ and $h(a) = h(b)$ if and only if $a \sim b$.*

Lemma 1.25. *Let $\boldsymbol{M}$ be a unique factorization monoid. Let a, b in M and*

$$b = q_1^{\beta_1} \cdots q_n^{\beta_n},$$

where $q_1, \dots, q_n$ are pairwise non-associated irreducible elements and $\beta_1, \dots, \beta_n$ are non-negative integers. Then $a \mid b$ if and only if

$$\boldsymbol{a} = \boldsymbol{q}_1^{\alpha_1} \cdots \boldsymbol{q}_n^{\alpha_n}, \tag{1.2}$$

where $0 \leq \alpha_i \leq \beta_i$, for all $i = 1, \dots, n$.

Proof. ($\Leftarrow$) There is an invertible u such that $a = u \cdot q_1^{\alpha_1} \cdots q_n^{\alpha_n}$. Therefore

$$b = q_n^{\beta_n - \alpha_n} \cdots q_1^{\beta_1 - \alpha_1} \cdot u^{-1} \cdot a,$$

and so $a \mid b$. ($\Rightarrow$) Since $a \mid b$, there is $c \in M$ such that $b = a \cdot c$. We prove that a is of the form (1.2) by induction on the height of a. If $h(a) = 0$, then a is invertible and the statement trivially holds true. Suppose that a is not invertible and let q be an irreducible element dividing a; with a' such that

$a = q \cdot a'$. Clearly $a' \mid b$ and $h(a') = h(a) - 1$. By the induction hypothesis $\boldsymbol{a'} = \boldsymbol{q}_1^{\alpha'_1} \cdots \boldsymbol{q}_n^{\alpha'_n}$ for some $0 \leq \alpha'_i \leq \beta_i$, $i = 1, \dots, n$.

Let the decomposition of c into a product of irreducible elements be $r_1 \cdots r_m$. From $b = a \cdot c = q \cdot a' \cdot c$ we infer that

$$\boldsymbol{b} = \boldsymbol{q} \cdot \boldsymbol{q}_1^{\alpha'_1} \cdots \boldsymbol{q}_n^{\alpha'_n} \cdot \boldsymbol{r}_1 \cdots \boldsymbol{r}_m = \boldsymbol{q}_1^{\alpha_1} \cdots \boldsymbol{q}_n^{\alpha_n}$$

From the uniqueness of such a decomposition we get that $q \sim q_i$ for some $i = 1, \dots, n$. Without loss of generality we can assume that $i = 1$. Canceling $q_1$we get that $a' \mid q_1^{\beta_1 - 1} \cdots q_n^{\beta_n}$. Therefore $0 \leq \alpha'_1 \leq \beta_1 - 1$ and $0 \leq \alpha'_i \leq \beta$ for all $i = 2, \dots, n$. From $a = q \cdot a'$, $q \sim q_1$ and the uniqueness of the decomposition in unique factorization monoids we conclude that

$$\boldsymbol{a} = \boldsymbol{q}_1^{\alpha_1} \cdots \boldsymbol{q}_n^{\alpha_n},$$

where $0 \leq \alpha_1 = \alpha'_1 + 1 \leq \beta$ and $0 \leq \alpha_i = \alpha'_i \leq \beta$, for all $2 \leq i \leq n$. □

Lemma 1.26. *Every pair of elements of a unique factorization monoid has a greatest common divisor.*

Proof. Let $\boldsymbol{M}$ be a unique factorization monoid, and $a, b \in M$. There are pairwise non-associated irreducible elements $q_1, q_2, \dots, q_n$ in M and integers $0 \leq \alpha_i, \beta_i$, $i = 1, 2, \dots, n$, such that

$$a \sim q_1^{\alpha_1} \cdot q_2^{\alpha_2} \cdots q_n^{\alpha_n} \quad \text{and} \quad b \sim q_1^{\beta_1} \cdot q_2^{\beta_2} \cdots q_n^{\beta_n}.$$

It follows readily from Lemma 1.25 that

$$(a, b) = \boldsymbol{q}_1^{\min\{\alpha_1, \beta_1\}} \cdot \boldsymbol{q}_2^{\min\{\alpha_2, \beta_2\}} \cdots \boldsymbol{q}_n^{\min\{\alpha_n, \beta_n\}}.$$

□

Theorem 1.27. *Let $\boldsymbol{M}$ be a commutative cancellative monoid. The monoid $\boldsymbol{M}$ is a unique factorization monoid if and only if the quasi-ordered set $(M, |)$ satisfies the minimal property and every irreducible element of M is prime.*

Proof. ($\Rightarrow$) It follows from Lemma 1.26 that every pair of elements of a unique factorization monoid $\boldsymbol{M}$ has a greatest common divisor. According to Theorem 1.21 all irreducible elements of the monoid $\boldsymbol{M}$ are prime. It follows that every element of $\boldsymbol{M}$ is a product of primes, hence the quasi-ordered set $(M, |)$ satisfies the minimal property due to Lemma 1.13(1). ($\Leftarrow$) If the quasi-ordered set $(M, |)$ satisfies the minimal property, then every element $a \in M$ is a product of irreducible elements, say $a = q_1 \cdot q_2 \cdots q_n$, due to Lemma 1.13(1). If, moreover, every irreducible element of M is prime, then the elements $\boldsymbol{q}_1, \boldsymbol{q}_2, \dots, \boldsymbol{q}_n$ are unique up to permutations. Therefore $\boldsymbol{M}$ is a unique factorization domain. □

Applying Lemma 1.6, Corollary 1.8, and Lemma 1.13 we conclude that

Corollary 1.28. *Let $\boldsymbol{M}$ be a commutative cancellative monoid. Then $\boldsymbol{M}$ is a unique factorization monoid if and only if every element of $\boldsymbol{M}$ is a product of primes.*

It follow from Lemma 1.10 that the quasi-ordered set $(M, |)$ satisfies the minimal property if and only if there is not an infinite sequence $a_1, a_2, \dots$ of elements of M such that $a_{i+1} \mid a_i$ and $a_i \nmid a_{i+1}$ for all i. Applying Theorem 1.21 and Lemma 1.26, we get that

Proposition 1.29. *Let $\boldsymbol{M}$ be a commutative cancellative monoid such that $(M, |)$ satisfies the minimal property. Then the following are equivalent:*

(i) *Every pair of elements of $\boldsymbol{M}$ has a greatest common divisor.*
(ii) *Every irreducible element of $\boldsymbol{M}$ is prime.*
(iii) *$\boldsymbol{M}$ is a unique factorization monoid.*

Exercises

Exercise 1.1. *Let $\mathbb{Z}^* := \mathbb{Z} \setminus \{0\}$ denote the set of all non-zero integers. Prove that $(\mathbb{Z}^*, \cdot, 1)$ is a unique factorization monoid. Compute the order quotient of $(\mathbb{Z}^*, |)$.*

Exercise 1.2. *Let $\boldsymbol{M}$ denote the monoid of all maps $\mathbb{N} \to (\mathbb{N}, \cdot, 1)$ from the set of all positive integers to the set of all positive integers with the multiplication defined by $f \cdot g(n) = f(n) \cdot g(n)$, for all $f, g \in M$ and all $n \in \mathbb{N}$.*

(i) *Prove that the monoid $\boldsymbol{M}$ is equal to its order quotient.*
(ii) *Prove that every irreducible element of $\boldsymbol{M}$ is prime.*
(iii) *Decide whether $\boldsymbol{M}$ is a unique factorization monoid.*

Exercise 1.3. *Let $\boldsymbol{M}$ be the monoid from Exercise 1.2. Put*

$$N := \{f \colon \mathbb{N} \to \mathbb{N} \mid f(n) = 1 \text{ for all but finitely many } n\}. \tag{1.3}$$

Prove that $\boldsymbol{N}$ is a submonoid of $\boldsymbol{M}$. Prove that $\boldsymbol{N}$ is a unique factorization monoid.

Exercise 1.4. *Let $(\mathbb{N}_0, +, 0)$ denote the monoid of all non-negative integers with the operation of addition. Show that $a \mid b$ if and only if $a \leq b$. Prove that the monoid is a unique factorization monoid and find its prime elements.*

Exercise 1.5. *Let $(\mathbb{Q}_0^+, +, 0)$ denote the monoid of all non-negative rational numbers with the operation of addition. Prove that the divisibility corresponds to the order relation. From this infer that the monoid does not satisfy the minimality property and that it has no irreducible elements.*

Exercise 1.6. *Let $\boldsymbol{A}$ be a group of all pairs $(a, b) \in \mathbb{Z}^2$ with the binary operation of addition computed coordinate-wise:*

$$(a, b) + (a', b') = (a + a', b + b').$$

Observe that

$$\boldsymbol{B} := \{(2a, -2a) \mid a \in \mathbb{Z}\}$$

is a sub-group of $\boldsymbol{A}$ *and put* $\boldsymbol{C} := \boldsymbol{A}/\boldsymbol{B}$ *and for every* $a \in A$ *let* $[\, a \,]_{\boldsymbol{B}} := a + B$ *denote the coset of* $\boldsymbol{B}$ *containing* a. *Finally let*

$$M := \{[\,(a,b)\,]_{\boldsymbol{B}} \mid 0 \leq a, b\}$$

denote the subset of $\boldsymbol{C}$ *of blocks of "positive tuples".*

(i) *Show that (*$\boldsymbol{M}$*,+,0) is a sub-monoid of the factor group* $\boldsymbol{C}$. *From this infer that* $\boldsymbol{M}$ *is commutative and cancellative.*

(ii) *Prove that* $(M, |)$ *satisfies the minimality property.*

(iii) *Find all irreducible elements of the monoid* $\boldsymbol{M}$.

(iv) *Prove that the monoid* $\boldsymbol{M}$ *has no primes.*

(v) *Find a pair of non-zero elements in* $\boldsymbol{M}$ *without a greatest common divisor.*