11.1. **Rings.** A *ring* $R$ consists of a set, $R$, and a pair of binary operations $+$ and $\cdot$ respectively of addition and multiplication such that

(i) $(R,+)$ is an Abelian group,
(ii) $(R,\cdot)$ is a monoid,
(iii) the *distributive law* holds true, that is,

\[(a + b) \cdot c = a \cdot c + b \cdot c \quad \text{and} \quad c \cdot (a + b) = c \cdot a + c \cdot b,\]

for all $a,b,c \in R$.

The unit of the Abelian group $(R,+)$ is usually denoted by 0 and called the zero of the ring $R$ while the unit of the monoid $(R,\cdot)$ is usually denote by 1 and it is called the unit of $R$. We will often write $a - b$ instead of $a + (-b)$.

**Exercise 11.1.** Let $R = (R,+,\cdot)$ be a ring. Prove that

(i) $a \cdot 0 = 0 \cdot a = 0$, for all $a \in R$.
(ii) $(-a) \cdot b = a \cdot (-b) = -a \cdot b$, for all $a,b \in R$.

A ring $R$ is *commutative* provided that

\[a \cdot b = b \cdot a,\]

for all $a,b \in R$, i.e, the monoid $(R,\cdot)$ is commutative.

A commutative ring $F = (F,+,\cdot)$ such that $(F \setminus \{0\},\cdot)$ is an (Abelian) group is called a *field*, i.e, a field is a commutative ring whose every non-zero element has a multiplicative inverse.

**Example 11.1.** Let us recall some well known examples of fields.

1. The sets of all rational, real, or complex numbers respectively form fields that are usually denoted by $\mathbb{Q}$, $\mathbb{R}$, and $\mathbb{C}$.
2. For each prime number $p$, the set $\mathbb{Z}_p = \{0,1,\ldots,p-1\}$ with the operations $+_p$ and $\cdot_p$ of addition and multiplication modulo $p$, respectively, is an example of a finite field. We will denote this field by $\mathbb{Z}_p$.

**Example 11.2.** Let us list a few examples of rings:
1. The ring $\mathbb{Z} = (\mathbb{Z}, +, \cdot)$ of all integers.

2. Let $\mathbf{F}$ be a field. All polynomials in a single variable $x$ with coefficients from the field $\mathbf{F}$ form a ring which we denote by $\mathbf{F}[x]$.

3. Let $\mathbf{F}$ be a field and $n$ a positive integer. All $n \times n$ matrices with entries from $\mathbf{F}$ form a ring. We will denote this ring by $M_n(\mathbf{F})$.

11.2. Ideals and factor-rings. An ideal of a ring $R = (R, +, \cdot)$ is a subset $I \subseteq R$ such that

(i) $a, b \in I \implies a + b \in I$,

(ii) $b \in I \implies a \cdot b \cdot c \in I$,

for all $a, b, c \in R$.

Observe that $(I, +)$ is a subgroup of the Abelian group $(R, +)$, indeed, if $a \in I$, then $-a = (-1) \cdot a \in I$, due to (ii). We can form a factor-group $R/I$, elements of the factor-group are cosets, $a + I$, of $I$.

Let $a, b \in R$. We have that

$$(a + I) \cdot (b + I) = a \cdot b + a \cdot I + b + I \cdot I \subseteq a \cdot b + I.$$ And so $R/I$ is a ring which will be called a factor-ring of $R$ over the ideal $I$.

11.3. Ring homomorphisms and their kernels. Let $R$ and $S$ be rings. A map $\varphi : R \to S$ is a (ring) homomorphism provided that

(i) $\varphi(a + b) = \varphi(a) + \varphi(b)$, for all $a, b \in R$,

(ii) $\varphi(a \cdot b) = \varphi(a) \cdot \varphi(b)$, for all $a, b \in R$,

(iii) $\varphi(1) = 1$.

Note that a map $\varphi : R \to S$ is a ring homomorphism if and only if it is at the same a homomorphism $(R, +) \to (S, +)$ of Abelian groups and $(R, \cdot) \to (S, \cdot)$ of monoids.

Let $\varphi : R \to S$ be a ring homomorphism. The kernel of $\varphi$ is the set

$$\ker \varphi := \{a \in R \mid \varphi(a) = 0\}.$$  

Lemma 11.3. Let $\varphi : R \to S$ be a ring homomorphism. Then $\ker \varphi$ is an ideal of $R$.

Proof. Let $a, b \in \ker \varphi$. Then

$$\varphi(a + b) = \varphi(a) + \varphi(b) = 0,$$ hence $a + b \in \ker \varphi$. If $b \in \ker \varphi$ and $a, c \in R$, then

$$\varphi(a \cdot b \cdot c) = \varphi(a) \cdot \varphi(b) \cdot \varphi(c) = \varphi(a) \cdot 0 \cdot \varphi(c) = 0,$$ hence $a \cdot b \cdot c \in \ker \varphi$. We conclude that $\ker \varphi$ is an ideal of $R$.  \[\square\]
On the other hand, if $I$ is an ideal of the ring $R$, we define a map $\pi_{R/I}: R \to R/I$ by $a \mapsto a + I$, for all $a \in R$. One readily sees that $\pi_{R/I}: R \to R/I$ is a ring homomorphism and that $I = \ker \pi_{R/I}$. Therefore, ideals correspond to kernels of rings homomorphisms.

11.4. Divisibility in commutative monoids. Let $M = (M, \cdot, 1)$ 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 $\mid$ defined on the set $M$ is reflexive and transitive, that is, it is a quasi-order on $M$.

The quasi-order of divisibility induces an equivalence relation $\sim$ on $M$ given by $a \sim b$ provided that $a \mid b$ and $b \mid a$, for all $a, b \in M$. We say that the elements $a$ and $b$ are associated if $a \sim b$. We denote by $[a]_\sim$ the block of the equivalence relation $\sim$ containing $a \in M$.

**Lemma 11.4.** Assume that the monoid $M$ is cancellative. 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 $b = a \cdot u \cdot v$ and from the cancellativity we get that $1 = u \cdot v$. Since $M$ 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 $a \sim b$. \hfill $\square$

An element $p \in M$ is prime provided that $p$ is not invertible and $p \mid a \cdot b$ implies that $p \mid a$ 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 that either $q \sim a$ or $q \sim b$, for all $a, b \in M$.

By induction we prove that

**Lemma 11.5.** An element $p \in M$ is prime if and only if

$p \mid a_1 \cdots a_n \iff p \mid a_i$ for some $i \in \{1, 2, \ldots, n\}$,

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

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

$q \sim a_1 \cdots a_n \iff q \sim a_i$ for some $i \in \{1, 2, \ldots, n\}$,

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

**Lemma 11.6.** Every prime element of $M$ is irreducible.
Proof. Let \( p \in M \) be a prime element and \( p \sim a \ldots b \) 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 phenomena later.

A common divisor of elements \( a_1, \ldots, a_n \in M \) is \( b \in M \) such that \( b \mid a_i \) for all \( i \in \{1, 2, \ldots, n\} \). A greatest common divisor of elements \( a_1, \ldots, a_n \) is

- a common divisor of \( a_1, \ldots, a_n \),
- if \( c \) is a common divisor of \( a_1, \ldots, a_n \), then \( c \mid d \).

The greatest common divisor of \( a_1, \ldots, a_n \) may not be unique. However, it is easy to see that all the greatest common divisors are associated. On the other hand, if \( d \) is a greatest common divisor of the elements \( a_1, \ldots, a_n \) and \( c \sim d \) then \( c \) is a greatest common divisor of \( a_1, \ldots, a_n \) as well. Therefore, all greatest common divisors of \( a_1, \ldots, a_n \) form a block of the equivalence \( \sim \). We will denote the block by \( (a_1, \ldots, a_n) \).

Lemma 11.7. Let \( M \) be a commutative monoid, \( a, b, c \in M \). Then

\[
(a, (b, c)) = ((a, b), c).
\]

Proof. Pick \( d \in (a, (b, c)) \) and \( e \in ((a, b), c) \). We prove that \( d \sim e \). Pick \( f \in (b, c) \) and \( g \in (a, b) \). 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 11.8. Let \( M \) be a commutative monoid. If a greatest common divisor exists for each pair of elements of \( M \), then a greatest common divisor exists for every non-empty finite subset \( \{a_1, \ldots, a_n\} \) of \( M \) and it can be computed inductively as

\[
(a_1, a_2, \ldots, a_n) = (a_1, (a_2, \ldots, a_n)).
\]

Lemma 11.9. Let \( M \) 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. Pick \( d \in (a, b) \) and \( e \in (a \cdot c, b \cdot c) \). From \( d \cdot c \mid a \cdot c \) and \( d \cdot c \mid b \cdot c \) we infer that \( d \cdot c \mid e \), in particular, 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 $M$ 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 $d \cdot x \sim d$, hence $e = d \cdot x \cdot c \sim d \cdot c$. We conclude that $d \cdot c$ is a greatest common divisor of $a \cdot c$ and $b \cdot c$.

We say that $a, b \in M$ are \textit{relatively prime} if the only common divisors of $a$ and $b$ are the invertible elements of $M$. Clearly, elements $a, b \in M$ are relatively prime if and only if $(a, b) = [1]$. \hfill \Box

\textbf{Lemma 11.10.} Let $M$ 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 $(a, b) = [1]$ and $(a, c) = [1]$, then $(a, b \cdot c) = [1]$.

\textbf{Proof.} Applying Lemma 11.9, we get from $(a, b) = [1]$, that $(a \cdot c, b \cdot c) = [1] \cdot c = [c]$. Similarly, we infer from $(1, c) = [1]$, that $(a, a \cdot c) = [a]$. Applying Lemma 11.7 we conclude that
\[ (a, b \cdot c) = ((a, a \cdot c), b \cdot c) = (a, (a \cdot c, b \cdot c)) = (a, c) = [1]. \hfill \Box \]

Observe that from Lemma 11.10 it follows that

\textbf{Corollary 11.11.} Let $M$ 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 $M$ that are relatively prime to $a$ forms a submonoid of $M$.

\textbf{Theorem 11.12.} Let $M$ be a commutative cancellative monoid. If every pair of elements of $M$ has a greatest common divisor, then every irreducible element of $M$ is prime.

\textbf{Proof.} Suppose that the assumptions of the theorem hold true and let $q$ be an irreducible element of $M$. Let $a, b \in M$. Since $q$ is irreducible either $q \mid a$, in which case $(q, a) = [a]$, or $(q, a) = [1]$. It follows that if $q \nmid a$ and $q \nmid b$, then $(q, a) = (q, b) = [1]$. From Lemma 11.10 we infer that $(q, a \cdot b) = [1]$, hence $q \nmid a \cdot b$. Therefore $q$ is a prime element of $M$. \hfill \Box