Notations: we write $\mathbb{Z}^+ = \{0, 1, 2, \ldots\}$, $\mathbb{N} = \{1, 2, 3, \ldots\}$, $2\mathbb{N} := \{2n; n \in \mathbb{N}\} = \{2, 4, 6, \ldots\}$, and $2\mathbb{N} - 1 := \{2n - 1; n \in \mathbb{N}\} = \{1, 3, 5, \ldots\}$.

Properties

In the following, $\circ : S \times S \to S$ is a binary operation on a nonempty set S. We write $a \circ b$ instead of the too formal $\circ(a, b)$.

We say that $\circ$ is **associative** if $(a \circ b) \circ c = a \circ (b \circ c)$ for all $a, b, c \in S$. This is the most important property, and all our operations below will share that.

Definition. *Let $\circ$ be an associative binary operation on a nonempty set S. Then the pair $(S, \circ)$ is a called a* **semigroup.** *(When the operation $\circ$ is clear from the context, we often just say that S is a semigroup.)*

Remark. Implicit in the word "binary operation" is the following property - often called *closure*: for all $a, b \in S$, $a \circ b \in S$.

We say that $\circ$ is **commutative** if $a \circ b = b \circ a$ for all $a, b \in S$. [Warning: our operations are not assumed to be commutative unless explicitly stated so!]

We say that $(S, \circ)$ has an **identity** (or "S has an identity" for short) if there is an element $e \in S$ such that $e \circ x = x$ and $x \circ e = x$ for all $x \in S$. An identity is also called a neutral element. It is easy to see that when exists, the identity is unique. [Indeed, if e and e' are identities, then $e = e \circ e' = e'$.] A semigroup with identity is sometimes called a monoid.

When a semigroup $(S, \circ)$ has an identity e, we say that an element $a \in S$ has an **inverse** (or "a is invertible", or "a is a unit") if there is a $b \in S$ such that $a \circ b = e$ and $b \circ a = e$; it is easy to see that if exists, such an element b is unique; we usually write a^{-1} for this b and call it the inverse of a. [Indeed, if b and b' are two such elements, then $b = b \circ (a \circ b') = (b \circ a) \circ b' = b'$.] The set of all invertible elements of S is denoted by S^*.

Given two binary operations $+$ and $\cdot$ on the same set S, we say that $\cdot$ distributes over $+$ if $a \cdot (b + c) = a \cdot b + a \cdot c$ and $(b + c) \cdot a = b \cdot a + c \cdot a$ for all $a, b, c \in S$.

Examples. $(\mathbb{R}, +)$, $(\mathbb{Z}, +)$, $(\mathbb{Z}^+, +)$, $(\mathbb{N}, \cdot)$, $(2\mathbb{N} - 1, \cdot)$, $(\mathbb{Z}_n, +)$, $(\mathbb{Z}_n, \cdot)$, as well as the set of $n \times n$ real matrices with respect to matrix-multiplication are semigroups with identity. $(\mathbb{N}, +)$ and $(2\mathbb{N}, \cdot)$ are semigroups without identity.

Structures

Definition. *Let $\circ$ be an associative binary operation on a nonempty set G. The pair $(G, \circ)$ is a called a* **group** *if G has an identity and each element of G has an inverse. The number of elements in G is called the* **order** *of the group. When $\circ$ is commutative, we say that the group $(G, \circ)$ is commutative or* **Abelian.**

Remark. We often use $\cdot$ to denote the group operation and call it multiplication. Then we may just write ab for $a \cdot b$, and sometimes we write 1 to denote the identity. For commutative groups, we often use $+$ to denote the operation and call it addition, write 0 for the identity, and $(-a)$ for the inverse of a.

Theorem. *Let $(S, \circ)$ be a semigroup with identity (a monoid). Then $(S^*, \circ)$ is a group.*

Examples. Of the above semigroup examples, the only ones that are groups are $(\mathbb{R}, +)$, $(\mathbb{Z}, +)$ and $(\mathbb{Z}_n, +)$. Here are a few more standard Abelian groups: $(\mathbb{Q}, +)$, $(\mathbb{C}, +)$, $(\mathbb{Q} \setminus \{0\}, \cdot)$, $(\mathbb{R} \setminus \{0\}, \cdot)$, $(\mathbb{C} \setminus \{0\}, \cdot)$. The set of all $k \times k$ non-singular real matrices forms a non-Abelian group with respect to matrix-multiplication; so does the set of all symmetries of an equilateral triangle under composition.

A useful (counter)example: Let S be a set containing at least two elements. Define a binary operation $\cdot$ on S by $(\forall x, y \in S) x \cdot y = x$. How do the group axioms fare for S equipped with this operation? Firstly, $\cdot$ is clearly associative. Furthermore, the condition $|S| \geq 2$ implies that S has no left-identity (hence no identity), but every element of S is a right-identity. This example may be useful for discarding some hastily made conjectures about groups. One could add an identity e to S and still keep its weirdness.

Definition. *Let R be a set equipped with two binary operations $+$ and $\cdot$ such that*

(1) $(R, +)$ *is a commutative group (we will always write 0 for its neutral element)*

(2) $(R, \cdot)$ *is a semigroup*

(3) $\cdot$ *distributes over* $+$

Then $(R, +, \cdot)$ is called a **ring**. *(We often just say R is a ring.)*

Furthermore, if $\cdot$ is also commutative, then R is a commutative ring.
R is a ring with identity if R has a multiplicative identity.

Remark. It is easy to see that in a ring $(R, +, \cdot)$ one always has $0 \cdot a = 0$ and $a \cdot 0 = 0$ for all $a \in R$. [Indeed, for any $a \in R$, $0 \cdot a = (0 + 0) \cdot a = 0 \cdot a + 0 \cdot a$; use cancellation, and do the same from the left of 0.] Hence, if a ring has at least two elements and it has an identity, then the identity is different from 0. If in a ring there are non-zero elements a and b such that $a \cdot b = 0$, then such elements are called **zero divisors.**

Definition. *Let $(F, +, \cdot)$ be a commutative ring with an identity $1 \neq 0$. If all nonzero elements of F are invertible, then the ring is called a* **field.** *Hence in a field $(F, +, \cdot)$*

(i) $(F, +)$ *is a commutative group*

(ii) $(F \setminus \{0\}, \cdot)$ *is a commutative group*

(iii) $\cdot$ *distributes over* $+$

Remark. It is easy to see that (i)-(iii) are not only corollaries of the field definition but are equivalent to it.

Examples. The set of all $k \times k$ real matrices is a ring (under matrix addition and multiplication). It is a non-commutative ring with identity and it has zero divisors.

$(\mathbb{Z}, +, \cdot)$ is a *commutative ring with identity* and it has *no zero divisors.* In view of this example, such structures are called **integral domains**. Contrast this infinite example with the following fact:

Exercise. Prove that a finite integral domain $(D, +, \cdot)$ is a field. [Hint: Given a nonzero $a \in D$, prove the existence of a^{-1} by considering the set $aD := \{ax : x \in D\}$.]

Subgroups, subrings, subfields

Definition. *Let $(G, \circ)$ be a group. A subset H of G is a subgroup if H itself is a group with respect to the same operation $\circ$. We write $(H, \circ) \leq (G, \circ)$, or simply write $H \leq G$ when it is clear what the operation is. $H < G$ means $H \leq G$ and $H \neq G$ (proper subgroup).*

It is easy to see that $H \subseteq G$ forms a subgroup with respect to $\circ$ if and only if H is nonempty, H is closed under $\circ$, and H is closed under taking inverse (in $(G, \circ)$). The following test provides a more compact form:

Theorem (Closure Test). *Let $(G, \circ)$ be a group and let $H \subseteq G$ be nonempty. Then $(H, \circ)$ is a group if and only if $a^{-1} \circ b \in H$ for all $a, b \in H$.*

With a similar definition for subrings and subfields, one can show that a nonempty subset of a ring forms a subring if and only if it is closed under subtraction and multiplication, and a subset of a field forms a subfield if and only if it has at least two elements and is closed under subtraction and division (by nonzero elements). We use the same notation $H \leq G$ when it is clear from the context of whether it means subgroup or subring or subfield.

Examples: $(2\mathbb{Z}, +) < (\mathbb{Z}, +) < (\mathbb{Q}, +) < (\mathbb{R}, +) < (\mathbb{C}, +)$ and $(\mathbb{Q}^*, \cdot) < (\mathbb{R}^*, \cdot) < (\mathbb{C}^*, \cdot)$ are subgroup relations, $(\mathbb{Q}, +, \cdot) < (\mathbb{R}, +, \cdot) < (\mathbb{C}, +, \cdot)$ are subfield relations, while $(\mathbb{Z}, +, \cdot)$ is only a subring of the field (and hence ring) $(\mathbb{R}, +, \cdot)$.

Theorem ($\mathbb{Z}$). *The only subgroups of $(\mathbb{Z}, +)$ are the sets $d\mathbb{Z} := \{dn : n \in \mathbb{Z}\}$, $d = 0, 1, 2, \ldots$*

[Hint for a proof: let $I \leq \mathbb{Z}$ and start with the smallest positive element of I (if any).]

Corollary. *Let $(G, \cdot)$ be a group with identity e, and let $a \in G$ be arbitrary. The set $\{k \in \mathbb{Z} : a^k = e\}$ is clearly a subgroup of $\mathbb{Z}$, and hence it is of the form $d\mathbb{Z}$ for some nonnegative integer d. When this d is positive, we say that the order of a is d, and we write $o(a) = d$. Thus, the order of a is the smallest positive integer d (if any) such that $a^d = e$.*

Theorem (Lagrange). *Let G be a finite group of order n with identity e. Then, $a^n = e$ for all $a \in G$. Hence, the order of any element of G is a divisor of n. More generally, the order of any subgroup of G divides n.*

Remark. One can get an easy proof for commutative groups by using the following lemma. (For non-commutative groups the standard proofs use the notion of cosets.)

Lemma. *Let $(G, \circ)$ be a group and let $a \in G$ be arbitrary. The map $f_a : G \to G : x \mapsto a \circ x$ is a bijection.*

Proof of Lagrange's theorem in the commutative case: Let $a \in G$. By the previous lemma,

$$\prod_{g \in G} g = \prod_{g \in G} (ag) = a^{|G|} \prod_{g \in G} g$$

and the claim follows. $\square$

Some number-theoretical consequences

The greatest common divisor of a and b is denoted by $gcd(a,b)$.

Theorem (Fermat's Little Theorem). *Let p be prime and let a be not divisible by p. Then,*

$$a^{p-1} \equiv 1 \ (\mathbf{mod}\ p).$$

This theorem is a special case of Euler's theorem (see below).

Definition. *For $m \in \mathbb{N}$, we define the Euler (totient) function $\varphi(m)$ as follows: $\varphi(m)$ is the number of integers between 1 and m that are relatively prime to m:*

$$\varphi(m) := |\{k : 1 \leq k < m,\ gcd(k,m) = 1\}|.$$

Theorem (Euler's Theorem). *Let $m \in \mathbb{N}$, $m \geq 2$, and let a be relatively prime to m. Then,*

$$a^{\varphi(m)} \equiv 1 \ (\mathbf{mod}\ m).$$

Proof. Indeed, the set $S := \{k : 1 \leq k < m,\ gcd(k,m) = 1\} = \mathbb{Z}_m^*$ (the set of invertible elements of $\mathbb{Z}_m$) forms a group under multiplication modulo m. Hence the claim follows from Lagrange's theorem (which we proved in the commutative case). $\square$

Remark. It is not hard to find the following explicit formula for $\varphi(m)$: If $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ where p_i are distinct primes, then

$$\varphi(m) = m \prod_{i=1}^{k} \left(1 - \frac{1}{p_i}\right).$$

The following theorem can be proved from Theorem ($\mathbb{Z}$) above.

Theorem (GCD Theorem). *Let a and b be non-zero integers. Then there are integers x and y such that $gcd(a,b) = ax + by$. In fact, writing $d = gcd(a,b)$, we have*

$$\{ax + by : x, y \in \mathbb{Z}\} = d\mathbb{Z} := \{dn : n \in \mathbb{Z}\}.$$

Remark. The Extended Euclidean Algorithm computes one such pair (x,y) as well as $gcd(a,b)$ — see www.millersv.edu/~bikenaga/absalg/exteuc/exteucth.html

Corollary. *The greatest common divisor of a and b is a multiple of all common divisors of a and b.*

Corollary. *The (Diophantine) equation $ax + by = c$ has a solution (in integers x, y) if and only if $gcd(a,b)$ divides c.*

In other words, the congruence $ax \equiv c\ (\mathbf{mod}\, m)$ has a solution x if and only if $gcd(a,m)$ divides c; and in that case there are exactly $gcd(a,m)$ different solutions modulo m.

Theorem. *If a divides $b \cdot c$, and a and b are relatively prime, then a divides c.*

Proof. By the GCD Theorem, there are x, y such that $1 = gcd(a,b) = ax + by$. Hence $c = acx + bcy$, and since both acx and bcy are divisible by a, so is c. $\square$

Corollary. *If a prime p divides $b \cdot c$, then either p divides b or p divides c.*

Corollary (The Fundamental Theorem of Arithmetic). *Any integer greater than 1 can be factored uniquely as a product of primes.*