A *binary operator* on a set S is a function from $S \times S$ to S, such as addition, subtraction, multiplication, or division. Usually binary operators are written in infix notation: $a \oplus b = c$. A *unary operator* on S is a function from S to S, such as negation or inversion

A binary operation $\oplus$ is *associative* if $(a \oplus b) \oplus c = a \oplus (b \oplus c)$, for all $a, b, c \in S$ A binary operation is *commutative* if $(a \oplus b) = b \oplus a$, for all $a, b \in S$ An element $i \in S$ is an *identity* for the binary operation $\oplus$ if $a \oplus i = a = i \oplus a$, for all $a \in S$. A unary operation $\ominus$ is an inverse function for a binary operation $\oplus$ and itentity i. if $a \oplus (\ominus a) = i = (\ominus a) \oplus a$, for all $a \in S$. Binary operation $\otimes$ distributes over binop $\oplus$ if $a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$ and $(b \oplus c) \otimes a = (b \otimes a) \oplus (b \otimes c)$.

Categories of algebraic domain

Semigroup: $(S, +)$, a set S with associative binary operation $+$,
Monoid: $(S, +, i)$, a semigroup with identity i.
Group: $(S, +, i, -)$, a monoid with inverse function $-$.
When the binary operation is commutative the word commutative is prefixed on the category name. In the case of groups, a commutative group is often called an *Abelian* group.

$(\mathsf{Z}, +, 0, a \rightarrow -a)$ is an Abelian group, as is $(\mathsf{N}, *, 1, a \rightarrow 1/a)$,

Ring: $(S, +, 0, -, *)$ such that $(S, +, 0, -)$ is an Abelian group, $(S, *)$ is a semigroup, and $*$ distributes over $+$. In other words, $+$ is associative, commutative, has identity 0 and inversion $-$ (unary negation), $*$ is associative and distributes over $+$.

CR1 (Commutative ring with 1): $(S, +, 0, -, *, 1)$. An important category of ring.

Let R be a CR1. An element $x \in R$ is a unit if $\exists y \in R$ such that $x * y = 1$. For each x, such a y, if it exists, is unique and is denoted x^{-1}. The set U consisting of the units of R forms a multiplicative Abelian group $(U, *, 1, x \rightarrow x^{-1}$.

An *ideal* of R is a subset $I \subset R$ which is closed under addition and under multiplication by R: $a, b \in I$, $r \in R$ implies $a + rb \in I$.

An ideal of R is *principal* if there exists an element $a \in I$ such that $I = \{a * r : r \in R\}$.

An ideal is *prime* if $a * b \in I$ implies $a \in I$ or $b \in I$. An ideal is *maximal* if for any ideal J, $I \subseteq J \subseteq R$ implies $J = I$ or $J = R$.

An nonzero element $x \in R$ is a *zero divisor* if $\exists y \in R, y \neq 0$, such that $x * y = 0$. The set of zero divisors of R forms an ideal of R.

ID (Integral domain): A CR1 with no non-zero zero-divisors. A cancellation law is equivalent: If $a \neq 0, b, c \in R$ and $a * b = a * c$, then $b = c$.

An element $a \in R$ is irreducible if for all $b, c \in R, a = b * c$ implies b or c is a unit.

We say that a *divides* b, written $a|b$, to mean that there $\exists c \in R$ such that $a * c = b$.

An element $a \in R$ is *prime* if for all $b, c \in R$, $a|b * c$ implies $a|b$ or $a|c$.

Elements a and b are *associates* if there is unit $u \in R$ such that $a = u * b$.

UFD (Unique Factorization Domain): an ID with the unique factorization property, which is: For all $a \in R$ there exists non-negative integer k and primes $p_1, \ldots, p_k \in R$ such that
1. $a = p_1 * \ldots * p_k$,
2. If $\exists j$ and primes $q_1, \ldots, q_j$, with $a = q_1 * \ldots * q_j$, then $j = k$, and (after some reordering) q_i p_i, for $i = 1$ to k.

Theorem: In a UFD, greatest common divisors are well defined and unique up to associate.

Definition: $\gcd(a, b) = g$ such that $g|a$ and $g|b$ and $\forall d$, if $d|a$ and $d|b$ then $d|g$.

PIR (Principal Ideal Ring): A CR1 in which every ideal is principal.

PID (Principal Ideal Domain): An ID which is also a PIR.

Theorem: In a PID, extended gcd is defined, ie., $\forall a, b, \exists g, u, v$ such that $g = \gcd(a, b)$ and $g = u * a + v * b$

ED (Euclidean Domain): A PID with Euclidean valuation and quotient/remainder theorem: $\forall a, b \neq 0 \in R, \exists q, r \in R$ such that $a = q * b + r$, and $r = 0$ or valuation(r) ¡ valuation(b).
Examples: integers under abs value, univariate polynomials over a field under degree.

Field: A CR1 in which every nonzero element is a unit.

Theorem: Field $\subset$ ED $\subset$ PID $\subset$ UFD $\subset$ ID $\subset$ CR1 $\subset$ Ring

Theorem: PID $\subset$ PIR $\subset$ CR1.

Functors

Univariate Polynomial: from a ring R form $R[x]$ the set consisting of zero and all finite sequences over R whose last element is nonzero. $R[x]$ is a ring when the sequences are understood as coefficient sequences, and the operations are the familiar ones.

In a natural way, R is a subring of $R[x]$.

Theorem: If R is a field, $R[x]$ is an ED.

Theorem: If R is a UFD, $R[x]$ is a UFD. Hence $R[x, y, \ldots, z]$ is a UFD.

Ring of Quotients: For a multiplictaively closed subset M of R with $0 \notin M$, $Q_{R,M}$ is $\{r/m : r \in R, m \in M\}$ modulo the relation $r/m = s/n$ if $r * n = s * m$.

Let Q_R denote Q_{R,R^*}, where $R^* = R$ $\{0\}$. In a natural way, R is a subring of $Q_{R,M}$.

Theorem: If R is an ID, Q_R is a Field.

Homomorphic image: IF I is an ideal of R, R/I denotes the ring $\{I + a : a \in R\}$.

The operations on R/I are defined by taking coset representatives and defining the result of an operator to be the coset containing the result of the corresponding operation on the representative(s) in R. For example, The zero is $I = I + 0$. The negation of $I + a$ is $I - a$. The product $(I + a) * (I + b)$ is $I + ab$.

Theorem: If I is prime R/I is an ID. If I is maximal R/I is a field.