Definition of a ring

A **ring** is a set R with binary operations $+$ and $\cdot$ (multiplication) such that:

(+ assoc) For any $a, b, c \in R$, $(a + b) + c = a + (b + c)$.

(+ comm) For any $a, b \in R$, $a + b = b + a$.

(Zero) There exists some $0 \in R$ such that for all $a \in R$, $0 + a = a = a + 0$.

(Negatives) For every $a \in R$, there exists some $-a \in R$ such that $(-a) + a = 0 = a + (-a)$.

($\cdot$ assoc) For any $a, b, c \in R$, $(ab)c = a(bc)$.

($\cdot$ comm) For any $a, b \in R$, $ab = ba$.

(One) There exists some $1 \in R$ such that for all $a \in R$, $1a = a = a1$.

(Distrib) For any $a, b, c \in R$, $a(b + c) = ab + ac$ and $(a + b)c = ac + bc$.

First observations

- With one exception, the axioms of a ring allow us to recover high school algebra, e.g., the FOIL formula holds in any ring:

$$(a+b)(c+d) = a(c+d) + b(c+d) = ac + ad + bc + bd.$$

- The one exception is division, i.e., reciprocals. You can only take reciprocals of *units*, i.e., ring elements that have multiplicative inverses in the ring.
- Other authors do not assume that multiplication is commutative or that there exists a multiplicative identity $1 \in R$; in their language, what we call a ring is a "commutative ring with unity."

Special kinds of rings

Definition

To say a ring R is a *domain* means that it has the zero factor property, i.e., for $a, b \in R$, if $ab = 0$, then $a = 0$ or $b = 0$.

Definition

To say that a ring R is a *field* means that $1 \neq 0$ in R and every nonzero element of R is a unit, i.e., has a multiplicative inverse.

Note: Every field is always a domain, but not vice versa (exercise).

Divisibility in an arbitrary domain

Definition

Let R be a domain and $a, b, d \in R$. To say that d *divides* a means that $a = qd$ for some $q \in R$. To say that d is a *common divisor* of a and b means that d divides both a and b.

Definition

Let R be a domain and $a, b \in R$. To say that d is a *greatest common divisor* of a and b means that two things hold:

- d is a common divisor of a and b; and
- If e is a common divisor of a and b, then e divides d.

Associates and irreducibles

Definition

To say that $a, b \in R$ are *associates* means that $a = ub$ for some unit $u \in R$.

Definition

Let R be a domain. To say that $r \in R$ is *irreducible* means that r is not a unit and that if $r = ab$ for $a, b \in R$, then one of a and b must be a unit.

Note: We use the name irreducible and not the name prime because that name is reserved for a related concept that actually turns out to be distinct in rings where factorization is not unique.

Euclidean domains

Definition

Let R be a domain. A *size function* on R is a function $\sigma : R \to \mathbf{Z} \cup \{-\infty\}$ such that for all nonzero $r \in R$, $\sigma(r) \geq 0$ and $\sigma(r) > \sigma(0)$. In other words, a size function σ takes elements of R as its inputs, outputs nonnegative integers for nonzero inputs, and has $\sigma(0)$ strictly smaller than any other output.

Definition

A *Euclidean domain* is a domain R with a size function σ that satisfies the following axiom: For $a, d \in R$, $d \neq 0$, there exist $q, r \in R$ such that

$$a = qd + r \qquad \text{with } \sigma(r) < \sigma(d).$$

In other words, a Euclidean domain is a domain where some version of the Division Theorem holds.

Euclidean algorithm for an arbitrary Euclidean domain

To find $\gcd(a, b)$, let $r_{-1} = a$, $r_0 = b$. Then:

$$
\begin{aligned}
r_{-1} &= q_1 r_0 + r_1 && [\sigma(r_1) < \sigma(r_0)] \\
r_0 &= q_2 r_1 + r_2 && [\sigma(r_2) < \sigma(r_1)] \\
r_1 &= q_3 r_2 + r_3 && [\sigma(r_3) < \sigma(r_2)] \\
&\vdots \\
r_{N-3} &= q_{N-1} r_{N-2} + r_{N-1} && [\sigma(r_{N-1}) < \sigma(r_{N-2})] \\
r_{N-2} &= q_N r_{N-1}
\end{aligned}
$$

Theorem

Everything works the same as it does with $\mathbf{Z}$ *and* $F[x]$.

Proof.

Same proof! □

Factorization in Euclidean domains

Works the same with common divisors and gcd, and again, with the same proofs.

Also true that factorization is unique, but we'll get back to that later.