

Let R be an integral domain.

Divisors Let $a, b \in R$ such that $a = bc$ for some $c \in R$. Then we say b is a *divisor* of a or that b *divides* a . This is denoted by $b \mid a$.

Associates Let $a, b \in R$ such that $a = ub$ for some $u \in U(R)$ (u is a unit of R). Then we say a is an *associate* of b . It is easy to show that the relation “is an associate of” is an equivalence relation. Therefore, R is partitioned into equivalence classes of associates. The equivalence class of 0 is just itself $\{0\}$ while the equivalence class of 1 is the set of all units $U(R)$.

Irreducible Let $a \in R$ such that $a \neq 0$ and $a \notin U(R)$ (i.e. a is a nonzero nonunit of R). We say that a is *irreducible* in R if the only divisors of a are units and associates. In other words, if $a = bc$ for some $b, c \in R$, then either b or c is an associate of a (and the other is a unit).

Prime Let $a \in R$ such that $a \neq 0$ and $a \notin U(R)$. We say that a is a *prime* of R if whenever $a \mid bc$ for some $b, c \in R$, then $a \mid b$ or $a \mid c$.

GCD Let $a_1, \dots, a_k \in R$ (not all zero). We say $d \in R$ is a *common divisor* of a_1, \dots, a_k if $d \mid a_i$ for all $i = 1, \dots, k$. Also, we say d is a *greatest common divisor* (or GCD for short) of a_1, \dots, a_k if d is a common divisor of a_1, \dots, a_k and whenever c is a common divisor of a_1, \dots, a_k we have that $c \mid d$.

Warning: First, note that there is no guarantee that the GCD of a set of elements exists! Next, notice that we say d is “a GCD” not “the GCD” since any associate of d is also a GCD of a_1, \dots, a_k . Thus to make the notion of GCD unique we need a way of picking out one representative among an equivalence class of associates. When $R = \mathbb{Z}$ we do this by requiring d to be positive. When $R = \mathbb{F}[x]$ we do this by requiring that $d(x)$ be monic.

Some basic facts

Let R be an integral domain and let $a, b \in R$.

- $(a) \subseteq (b) \iff b \mid a$.
- $(a) = (b) \iff b \mid a$ and $a \mid b \iff a$ is an associate of b .
- $(a) \subsetneq (b) \iff b \mid a$ and $a \nmid b \iff b \mid a$ and a is not an associate of b .
- Prime \implies Irreducible. Every prime $p \in R$ is irreducible.

[Warning: The converse does not always hold!]

Special Types of Rings

Euclidean Domain Let R be an integral domain equipped with a function δ from the non-zero elements of R to the set of non-negative integers $\mathbb{Z}_{\geq 0}$. In addition, assume that:

- If $a, b \in R_{\neq 0}$ (non-zero elements of R), then $\delta(ab) \geq \delta(a)$.
- If $a, b \in R$ and $b \neq 0$, then there exists $q, r \in R$ such that $a = bq + r$ where either $r = 0$ or $\delta(r) < \delta(b)$.

Then R is a *Euclidean domain*.

Principal Ideal Domain Let R be an integral domain in which all ideals are principal (i.e. if $I \triangleleft R$, there exists $a \in R$ such that $(a) = I$). Then R is called a *principal ideal domain* (or PID for short).

Unique Factorization Domain Let R be an integral domain. Then R is a *unique factorization domain* (or UFD for short) if for all $a \in R$ such that $a \neq 0$ and $a \notin U(R)$, there exists $b_1, b_2, \dots, b_k \in R$ such that $a = b_1 b_2 \cdots b_k$, each b_i is irreducible, and if $b_1 b_2 \cdots b_k = c_1 c_2 \cdots c_\ell$, then $k = \ell$ and there exists some reordering of the c_i 's, say $c_1 \cdots c_\ell = c'_1 \cdots c'_\ell$, such that b_i is an associate of c'_i for all $i = 1, \dots, k = \ell$.

More important facts

- Euclidean Domain \Rightarrow Principal Ideal Domain \Rightarrow Unique Factorization Domain.
- GCDs always exist in UFDs (thus GCDs always exist in Euclidean domains and PIDs).
- In a UFD, Irreducible \Leftrightarrow Prime (thus this holds in Euclidean domains and PIDs too).

Examples

- \mathbb{Z} is a Euclidean domain (thus a PID and UFD also). Use $\delta(n) = |n|$.
- $\mathbb{Z}[i]$ is a Euclidean domain (thus a PID and UFD also). Use $\delta(a + bi) = a^2 + b^2$.
- If \mathbb{F} is a field, then $\mathbb{F}[x]$ is a Euclidean domain (thus a PID and UFD also). Use $\delta = \deg$.
- If \mathbb{F} is a field, then \mathbb{F} is a Euclidean domain (thus a PID and UFD also). Use $\delta(a) = 1$ for all $a \neq 0$. [Note: \mathbb{F} has no primes or irreducibles!]
- If R is a UFD, but **not** a field, then $R[x]$ is a UFD, but $R[x]$ is neither a ED nor a PID.

[Why? “ R a UFD implies $R[x]$ a UFD” is Theorem 9.38 on page 326 (we will skip the proof).

On the other hand, if R is not a field, there exists some irreducible (and prime) element $p \in R$. Consider the ideal (x, p) in $R[x]$. If it were principal, say generated by $f(x)$, then $f(x)g(x) = p$ for some $g(x) \in R[x]$. Therefore, $f(x)$ has degree 0 (i.e. $f(x) = c \neq 0$). However, $x = f(x)h(x) = ch(x)$ for some $g(x) \in R[x]$. We must have $h(x) = bx$. Therefore, $bcx = x$, thus $bc = 1$, so c is a unit and thus $(x, p) = R[x]$. But notice $(x, p) = \{f(x)x + g(x)p \mid f(x), g(x) \in R[x]\} = \{a_n x^n + \cdots + a_1 x + a_0 \in R[x] \mid p \text{ divides } a_0\}$. But p does not divide 1 (it is irreducible). Thus $1 \notin (x, p) = R[x]$ (contradiction). Thus $R[x]$ is not a PID.]

- From the previous discussion, $\mathbb{R}[x, y]$ is a UFD but not a PID (or a Euclidean domain) because $\mathbb{R}[x]$ is a UFD but not a field. Also, $\mathbb{Z}[x]$ is a UFD but not a PID (or a Euclidean domain) because \mathbb{Z} is a UFD but not a field.
- $\mathbb{Z}[\sqrt{-3}]$ is an integral domain, but not a UFD (thus neither a Euclidean domain nor a PID).