



planetmath.org

Math for the people, by the people.

motivation for Euclidean domains

Canonical name	MotivationForEuclideanDomains
Date of creation	2013-03-22 12:52:05
Last modified on	2013-03-22 12:52:05
Owner	Wkbj79 (1863)
Last modified by	Wkbj79 (1863)
Numerical id	8
Author	Wkbj79 (1863)
Entry type	Topic
Classification	msc 13G05
Related topic	EuclideanRing
Related topic	PID
Related topic	UFD
Related topic	IntegralDomain

UFDs, PIDs, and Euclidean domains are ways of building successively more of standard number into a domain.

First, observe that the units are numbers that behave in a manner similar to 1. Obvious examples, besides 1 itself, are  $-1$  in  $\mathbb{Z}$  or  $i$  and  $-i$  in the Gaussian integers.

Ideals behave something like the set of products of an element; in  $\mathbb{Z}$  those are the ideals (together with the zero ideal), and ideals in other rings have some similar behavior.

In commutative rings, prime ideals have one property similar to the prime numbers. Specifically, a product of two elements is in the ideal exactly when one of those elements is already in the ideal. For example, in  $\mathbb{Z}$ , if  $a \cdot b$  is even, we know that either  $a$  or  $b$  is even, but if  $a \cdot b$  is a multiple of four, we do not know that  $a$  or  $b$  is a multiple of four, since they could both be even numbers that are not multiples of four.

The other property most associated with prime numbers is their irreducibility: The only way to factor an irreducible element is to use a unit, and since units are “1-like”, that does not really break the element into smaller pieces. (Specifically, the non-unit factor can always be broken into another unit times the original irreducible element.)

In a UFD, these two properties of prime numbers coincide for nonzero numbers. All prime elements (generators of prime ideals) are irreducible, and all irreducibles are prime elements. Also, all numbers can be factored into prime elements the same way integers can be factored into primes.

A PID behaves even more like the integers by adding the concept of a greatest common divisor. Formally, this holds because, for any two ideals in any ring, we can find a minimal ideal which contains both of them, and in a PID we have the guarantee that the new ideal is generated by a particular element—the greatest common divisor. The Dedekind-Hasse valuation on the ring encodes this property by requiring that, if  $a$  is not a multiple of  $b$  (that is, in  $\langle b \rangle$ ), then there is a common divisor which is simpler than  $b$ . (The formal definition is that the element be of the form  $ax + by$ , but there is, in general, a between linear combinations of elements and their greatest common divisor.)

Being a Euclidean domain is an even stronger requirement, the most important effect of which is to provide Euclid’s algorithm for finding gcd’s. The key property is that division with remainders can be performed akin to the way it is done in the integers. A Euclidean valuation again encodes this property by ensuring that remainders are limited (specifically, requiring

that the norm of the remainder be less than the norm of the divisor). This the remainders to get successively smaller, guaranteeing that the process eventually terminates.