divisibility in rings

Canonical name	DivisibilityInRings
Date of creation	2015-05-06 15:18:14
Last modified on	2015-05-06 15:18:14
Owner	pahio (2872)
Last modified by	pahio (2872)
Numerical id	24
Author	pahio (2872)
Entry type	Definition
Classification	msc 13A05
Classification	msc 11A51
Related topic	PrimeElement
Related topic	Irreducible
Related topic	GroupOfUnits
Related topic	DivisibilityByPrimeNumber
Related topic	GcdDomain
Related topic	CorollaryOfBezoutsLemma
Related topic	ExistenceAndUniquenessOfTheGcdOfTwoIntegers
Related topic	MultiplicationRing
Related topic	IdealDecompositionInDedekindDomain
Related topic	IdealMultiplicationLaws
Related topic	UnityPlusNilpotentIsUnit
Defines	divisible
Defines	divisibility
Defines	divisibility of ideals

Let $(A, +, \cdot)$ be a commutative ring with a non-zero unity 1. If a and b are two elements of A and if there is an element q of A such that $b = qa$, then b is said to be *divisible* by a; it may be denoted by $a \mid b$. (If A has no zero divisors and $a \neq 0$, then q is uniquely determined.)

When b is divisible by a, a is said to be a *divisor* or http://planetmath.org/DivisibilityInR of b. On the other hand, b is not said to be a *multiple* of a except in the case that A is the ring $\mathbb{Z}$ of the integers. In some languages, e.g. in the Finnish, b has a name which could be approximately be translated as '*containant*': b is a *containant* of a ("b on a:n *sisältäjä*").

- $a \mid b$ iff $(b) \subseteq (a)$ [see the principal ideals].
- Divisibility is a reflexive and transitive relation in A.
- 0 is divisible by all elements of A.
- $a \mid 1$ iff a is a unit of A.
- All elements of A are divisible by every unit of A.
- If $a \mid b$ then $a^n \mid b^n$ $(n = 1, 2, \ldots)$.
- If $a \mid b$ then $a \mid bc$ and $ac \mid bc$.
- If $a \mid b$ and $a \mid c$ then $a \mid b+c$.
- If $a \mid b$ and $a \nmid c$ then $a \nmid b+c$.

Note. The divisibility can be similarly defined if $(A, +, \cdot)$ is only a semiring; then it also has the above properties except the first. This concerns especially the case that we have a ring R with non-zero unity and A is the set of the ideals of R (see the ideal multiplication laws). Thus one may speak of the *divisibility of ideals* in R: $\mathfrak{a} \mid \mathfrak{b} \Leftrightarrow (\exists \mathfrak{q})\,(\mathfrak{b} = \mathfrak{q}\mathfrak{a})$. Cf. multiplication ring.