group of units

Canonical name	GroupOfUnits
Date of creation	2013-03-22 14:41:32
Last modified on	2013-03-22 14:41:32
Owner	pahio (2872)
Last modified by	pahio (2872)
Numerical id	24
Author	pahio (2872)
Entry type	Theorem
Classification	msc 16U60
Classification	msc 13A05
Synonym	unit group
Related topic	CommutativeRing
Related topic	DivisibilityInRings
Related topic	NonZeroDivisorsOfFiniteRing
Related topic	PrimeResidueClass
Defines	group of units of ring
Defines	multiplicative group of field

Theorem. The set E of units of a ring R forms a group with respect to ring multiplication.

Proof. If u and v are two units, then there are the elements r and s of R such that $ru = ur = 1$ and $sv = vs = 1$. Then we get that $(sr)(uv) = s(r(uv)) = s((ru)v) = s(1v) = sv = 1$, similarly $(uv)(sr) = 1$. Thus also uv is a unit, which means that E is closed under multiplication. Because $1 \in E$ and along with u also its inverse r belongs to E, the set E is a group.

Corollary. In a commutative ring, a ring product is a unit iff all are units.

The group E of the units of the ring R is called the *group of units of the ring*. If R is a field, E is said to be the *multiplicative group of the field*.

Examples

1. When $R = \mathbb{Z}$, then $E = \{1,\, -1\}$.
2. When $R = \mathbb{Z}[i]$, the ring of Gaussian integers, then $E = \{1,\, i,\, -1,\, -i\}$.
3. When $R = \mathbb{Z}[\sqrt{3}]$, `http://planetmath.org/UnitsOfQuadraticFields`then $E = \{\pm(2+\sqrt{3})^n \vdots\ n \in \mathbb{Z}\}$.
4. When $R = K[X]$ where K is a field, then $E = K \smallsetminus \{0\}$.
5. When $R = \{0+\mathbb{Z},\, 1+\mathbb{Z},\, \ldots,\, m-1+\mathbb{Z}\}$ is the residue class ring modulo m, then E consists of the prime classes modulo m, i.e. the residue classes $l+\mathbb{Z}$ satisfying $\gcd(l, m) = 1$.