group of units*

pahio†

2013-03-21 18:03:46

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 factors 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 $R=\mathbb{Z}[\sqrt{3}]$, 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 $\gcd(l,m)=1$.

*⟨GroupOfUnits⟩ created: ⟨2013-03-21⟩ by: ⟨pahio⟩ version: ⟨36301⟩ Privacy setting: ⟨1⟩ ⟨Theorem⟩ ⟨16U60⟩ ⟨13A05⟩