Units

Definition

Let R be a ring with unity $1 \neq 0$ and $a \in R$. To say that $a^{-1} \in R$ is a *multiplicative inverse* of a means:

$$aa^{-1} = a^{-1}a = 1$$

Theorem

Let R be a ring with unity $1 \neq 0$. $0 \in R$ does not have a multiplicative inverse.

Proof

ABC: $0^{-1} \in R$
$00^{-1} = 1$
But $00^{-1} = 0$
$0 = 1$
CONTRADICTION!
$\therefore 0$ has no multiplicative inverse.

Definition

Let R be a ring with unity $1 \neq 0$. To say that $a \in R$ is a *unit* means that a has a multiplicative inverse $a^{-1} \in R$.

Theorem

Let R be a ring with unity $1 \neq 0$. $\forall\, a \in R, a$ is a unit $\implies a^{-1}$ is unique.

Proof

Assume a is a unit in R
Let b and b' be multiplicative inverses of a in R
$ab = ba = 1$
$ab' = b'a = 1$
$ab = ab'$
$b(ab) = b(ab')$
$(ba)b = (ba)b'$
$1b = 1b'$
$b = b'$

Theorem

Let R be a ring with unity $1 \neq 0$ and let $R^* = \{a \in R \mid a \text{ is a unit}\}$. $\langle R, \cdot \rangle$ is a group.

Proof

$(1)(1) = 1$, so $1 \in R^*$ and $R^* \neq \emptyset$

Assume $a, b \in R^*$
$\exists\, a^{-1}, b^{-1} \in R^*$
$(b^{-1}a^{-1})(ab) = b^{-1}(a^{-1}a)b = b^{-1}1b = b^{-1}b = 1$
$(ab)(b^{-1}a^{-1}) = a(bb^{-1})a^{-1} = a1a^{-1} = aa^{-1} = 1$
$b^{-1}a^{-1} = (ab)^{-1}$
$ab \in R^*$
$\therefore R^*$ is closed under the operation.

Assume $a \in R^*$
By definition, $a^{-1} \in R^*$
$\therefore R^*$ is closed under inverses.

$\therefore R^*$ is a group.

Example

$R = M_n(\mathbb{R})$
$R^* = LR_n(\mathbb{R})$

$R = \mathbb{Z}$
$R^* = \{-1, 1\}$

$R = \mathbb{Z}_n$
$R^* = \{a \in \mathbb{Z}_n \mid (a, n) = 1\}$

Theorem

$u \in \mathbb{Z}_n$ is a unit $\iff (u, n) = 1$

Proof

$\implies$ Assume $u \in \mathbb{Z}_n$ is a unit
$\exists\, v \in \mathbb{Z}_n, uv = 1$
$\exists\, k \in \mathbb{Z}, uv = kn + 1$
$uv - kn = 1$
Let $d = (u, n)$
$d \mid u$ and $d \mid n$
So $d \mid uv - kn$
Thus $d \mid 1$
$d = 1$
$\therefore (u, n) = 1.$

$\impliedby$ Assume $(u, n) = 1$
$uv - kn = 1$ has solutions in R
$uv = kn + 1$
$uv = 1$
But Z_n is commutative,
So $vu = 1$
Thus, u has multiplicative inverse v
$\therefore u$ is a unit.