Units

Definition: Unit

Let R be a ring with $1 \neq 0$. To say that $r \in R$ is a *unit* in R means that $\exists\, s \in R$ such that:

$$rs = sr = 1$$

In other words, r has a multiplicative inverse.

The set of all units in R is denoted by $R^{\times}$.

Theorem

Let R be a ring with $1 \neq 0$. $R^{\times}$ is a multiplicative group.

Proof

Clearly, $R^{\times} \subseteq R$
$1 \cdot 1 = 1$, so $1 \in R^{\times}$ and $R^{\times} \neq \emptyset$
Assume $r, s \in R^{\times}$
$(rs)(s^{-1}r^{-1}) = r(ss^{-1})r^{-1} = r1r^{-1} = rr^{-1} = 1$
$(s^{-1}r^{-1})(rs) = s^{-1}(r^{-1}r)s = s^{-1}1s = s^{-1}s = 1$
Thus, $rs \in R^{\times}$ and moreover, $(rs)^{-1} = s^{-1}r^{-1}$

Therefore, by the subgroup test, $R^{\times}$ is a group.

Example

1). $\mathbb{Z}^{\times} = \{\pm 1\}$

$mn = 1$
$|mn| = |m|\,|n| = |1| = 1$
$|m| = \frac{1}{|n|} \leq 1$
But $|m| \geq 1$
$\therefore |m| = 1$, or $m = \{\pm 1\}$

2). $\mathbb{Z}[i]^{\times} = \{\pm 1, \pm i\}$

$\frac{1}{a+bi} = \frac{a-bi}{a^2+b^2}$
So $a^2 + b^2 = 1$
Note that $a, b \leq 1$
When $a = 0, b = \pm 1$
When $a = \pm 1, b = 0$
$\therefore \mathbb{Z}[i]^{\times} = \{\pm 1, \pm i\}$

3). $\mathbb{Z}[\omega]^\times = \{\pm 1, \pm\omega, \pm\omega^2\}$

$\omega = \frac{-1+\sqrt{3}}{2} = e^{\frac{2\pm i}{3}}$
$\omega^3 = 1$
$1 \cdot 1 = 1$
$\omega \cdot \omega^2 = 1$
$\mathbb{Z}[\omega] = \{\pm 1, \pm\omega, \pm\omega^2\}$

4). $(\mathbb{Z}/n\mathbb{Z})^\times = \{a + n\mathbb{Z} \mid a \in \mathbb{Z}, (a,n) = 1\}$

$$\begin{aligned}
a + n\mathbb{Z} \in (Z/n\mathbb{Z})^\times \quad &\iff \quad \exists\, b + n\mathbb{Z} \in (Z/n\mathbb{Z})^\times, (a+nZ)(b+nZ) = 1 + nZ \\
&\iff \quad ab + n\mathbb{Z} = 1 + n\mathbb{Z} \\
&\iff \quad ab \equiv 1 \pmod{n} \\
&\iff \quad \exists\, k \in \mathbb{Z}, ab - 1 = kn \\
&\iff \quad ab + n(-k) = 1 \text{ has solutions} \\
&\iff \quad (a,n) = 1 \quad \text{(Bézout)}
\end{aligned}$$