Finite Rings

Theorem. *Let R be a finite ring with $1 \neq 0$, and let $a \in R$. Then exactly one of the following is true:*

(i). $a = 0$;
(ii). a *is a unit; or*
(iii). a *is a zero divisor.*

Examples. $\mathbb{Z}_n$ and $\mathbb{Z}$.

Finite Rings: Proof

Proof. If $a = 0$ then a is not a zero divisor, and it's also not a unit ($0 = 0 \cdot 0^{-1} = 1 \neq 0$, contradiction).

So suppose $a \neq 0$.

Define $\phi \colon R \to R$ by $\phi(x) = ax$.

We first consider what happens when ϕ is surjective (onto).

If it's surjective, then there is a $b \in R$ such that $\phi(b) = 1$, so that $ab = 1$. Then b is a **right multiplicative inverse** of a.

Conversely if a has a right multiplicative inverse b (so that $ab = 1$), then ϕ is onto. This is because, for all $y \in R$, $\phi(by) = aby = 1y = y$.

Now consider injectivity. If ϕ is *not* injective, then there are $b, c \in R$ such that $b \neq c$ and $\phi(b) = \phi(c)$. Then $ab = ac$, so $a(b - c) = 0$. Since $b - c \neq 0$ and $a \neq 0$, a is a zero divisor. Specifically, a is a **left zero divisor**.

Conversely, if a is a left zero divisor, say $ab = 0$ with $b \neq 0$, then ϕ is not injective, because $\phi(b) = ab = 0 = a0 = \phi(0)$ with $b \neq 0$.

Now, since R is *finite*, we have:

$$\begin{aligned} a \text{ has a right multiplicative inverse} &\iff \phi \text{ is surjective} \\ &\iff \phi \text{ is injective} \\ &\iff a \text{ is not a left zero divisor}. \end{aligned}$$

Similarly, letting $\psi \colon R \to R$ be the map $\psi(x) = xa$, we have:

$$\begin{aligned} a \text{ has a left multiplicative inverse} &\iff \psi \text{ is surjective} \\ &\iff \psi \text{ is injective} \\ &\iff a \text{ is not a right zero divisor}. \end{aligned}$$

Also, if a has both a left inverse b and a right inverse c, then $b = c$ because

$$b = b1 = bac = 1c = c.$$

So (assuming $a \neq 0$),

$$\begin{aligned} a \text{ is a unit} &\iff a \text{ has both a left inverse and a right inverse} \\ &\iff a \text{ is neither a left zero divisor nor a right zero divisor} \\ &\iff a \text{ is not a zero divisor}. \end{aligned}$$

□

[Revisit $\mathbb{Z}_n$ and $\mathbb{Z}$.]

Corollary. *Every finite integral domain is a field.*

Proof. It has no zero divisors, so every element is either 0 or a unit. $\square$

A Homomorphism $\gamma\colon \mathbb{Z} \to R$

Proposition. *Let R be a ring with unity 1, and let $\gamma\colon \mathbb{Z} \to R$ be the unique group homomorphism from $\mathbb{Z}$ to $\langle R, + \rangle$ for which $\gamma(1) = 1$. Then γ is a ring homomorphism.*

Proof. First, we have $\gamma(n+m) = \gamma(n) + \gamma(m)$ for all $n, m \in \mathbb{Z}$ (by assumption).

Now we show that

$$\gamma(nm) = \gamma(n)\gamma(m)$$

for all $n, m \in \mathbb{Z}$. If $n = 0$ then it's true because both sides are 0.

If $n > 0$ then we have

$$\begin{aligned}\gamma(nm) &= \gamma(m + \cdots + m) = \gamma(m) + \cdots + \gamma(m) = (1 + \cdots + 1)\gamma(m) \\ &= (\gamma(1) + \cdots + \gamma(1))\gamma(m) = \gamma(1 + \cdots + 1)\gamma(m) = \gamma(n)\gamma(m)\ .\end{aligned}$$

(Here all expressions $+\cdots+$ mean repeated addition n times.)

Finally, if $n < 0$ then

$$\gamma(nm) = -\gamma(-nm) = -\gamma(-n)\gamma(m) = \gamma(n)\gamma(m)\ . \qquad \square$$