

MTHSC 412 SECTION 3.2 – BASIC PROPERTIES OF RINGS

Kevin James

THEOREM

For R a ring and $a \in R$, the equation $a + x = 0_R$ has a unique solution.

PROOF.

Suppose that w and z are two solutions.

Then $w = w + 0 = w + (a + z) = (a + w) + z = 0 + z = z$. $\square$

DEFINITION

- 1 Given R , a ring and $a \in R$. We define $-a$ to be the unique solution in R to the equation $a + x = 0$.
- 2 In a ring R we define subtraction as $a - b = a + (-b)$.

EXAMPLE

Suppose that $R = \mathbb{Z}_6$.

- 1 Since $2 + 4 = 0$, $-2 = 4$.
- 2 So, $5 - 2 = 5 + 4 = 3$ in $\mathbb{Z}_6$.

NOTE

If R is a ring then we know that addition and multiplication are well-defined. It follows that

$$x = y \Rightarrow x + a = y + a \text{ and}$$

$$x = y \Rightarrow xa = ya.$$

THEOREM

Suppose that R is a ring and $a, b \in R$. Then

$$a + x = a + y \Rightarrow x = y.$$

PROOF.

$$\begin{aligned} x &= 0 + x = (-a + a) + x = -a + (a + x) = -a + (a + y) = \\ &(-a + a) + y = y. \end{aligned}$$



THEOREM

Suppose that R is a ring and $a, b \in R$. Then,

- ① $a \cdot 0_R = 0_R \cdot a = 0_R$.
- ② $a(-b) = -ab = (-a)b$.
- ③ $-(-a) = a$.
- ④ $-(a + b) = (-a) + (-b)$.
- ⑤ $-(a - b) = -a + b = b - a$.
- ⑥ $(-a)(-b) = ab$.
- ⑦ *If R is a ring with identity then we also have $(-1_R)a = -a$.*

THEOREM

Let R be a ring and let $\emptyset \neq S \subseteq R$ such that

- 1 S is closed under subtraction.
- 2 S is closed under multiplication.

Then S is a subring of R .

DEFINITION

Let R be a ring.

- ① For any $a \in R$ we define *nonnegative integral multiples* by

$$0a = 0_R, \quad 1a = a, \quad (n+1)a = na + a \quad (n > 0).$$

Negative integral multiples are defined by

$$(-n)a = n(-a) \quad n > 0.$$

- ② For any $a \in R$ we define *nonnegative integral exponents* as follows. If R has an identity then $a^0 = 1_R$. In any case,

$$a^1 = a, \quad a^{n+1} = a^n a \quad n > 0.$$

If a has a multiplicative inverse, negative integral exponents are defined by

$$a^{-n} = (a^{-1})^n \quad n > 0.$$

THEOREM (LAWS OF MULTIPLES)

Suppose that R is a ring and that $a, b \in R$, and $m, n \in \mathbb{Z}$. Then,

- ① $na + (-n)a = 0$,
- ② $ma + na = (m + n)a$,
- ③ $n(ma) = (nm)a$, and
- ④ $n(a + b) = na + nb$.

THEOREM (LAWS OF EXPONENTS)

Suppose that R is a ring $a, b \in R$, and $m, n \in \mathbb{Z}$. Then,

- ① If a is invertible, then $a^n \cdot a^{-n} = e$,
- ② $a^m \cdot a^n = a^{m+n}$,
- ③ $(a^m)^n = a^{mn}$, and
- ④ If R is commutative then $(ab)^n = a^n b^n$.

THEOREM

Let R be a ring and let $a, b \in R$. The equation $a + x = b$ has the unique solution $x = b - a$.

PROOF.

(Existence): We note that

$$a + (b - a) = a + ((-a) + b) = (a + (-a)) + b = 0 + b = b.$$

Thus $x = b - a$ is a solution.

(Uniqueness): Suppose that w is another solution.

Then we have $a + x = a + w \Rightarrow x = w$. □

NOTE

Suppose that R is a ring with identity and that $a \in R$. If $ax = 1$ and $ya = 1$ both have solutions, say u and v respectively, then we have

$$u = 1 \cdot u = (va)u = v(au) = v \cdot 1 = v.$$

DEFINITION

Suppose that R is a ring with identity and that $a \in R$. If there exists $u \in R$ such that $au = 1_R = ua$ then we say that a is a unit and that u is the multiplicative inverse of a and we write $u = a^{-1}$.

EXAMPLE

- 1 In $\mathbb{Z}_{10}$, 7 is a unit and in fact $7^{-1} = 3$.
- 2 In $\mathbb{Z}_{10}$, 2 is not a unit.

THEOREM

Suppose that R is a ring with identity and that $a, b \in R$ with a a unit. Then the equations $ax = b$ and $ya = b$ have a unique solution in R .

PROOF.

(Existence): Since a is a unit, there is an element $c \in R$ such that $ac = ca = 1$.

Thus, $a(cb) = (ac)b = 1 \cdot b = b$. and $(bc)a = b(ca) = b \cdot 1 = b$.
Thus $x = cb$ and $y = bc$ are solutions.

(Uniqueness): Suppose that u and v are both solutions to $ax = b$.
Then $au = av \Rightarrow c(au) = c(av) \Rightarrow (ca)u = (ca)v \Rightarrow u = v$.

The proof in the other case is similar. □

FIELDS ARE INTEGRAL DOMAINS

THEOREM

Every field F is an integral domain.

PROOF.

Suppose that F is a field and that $a, b \in F$ with $ab = 0$ and $a \neq 0$. Since, $0 \neq a \in F$, a is a unit.

So, $b = 1 \cdot b = (a^{-1}a)b = a^{-1}(ab) = a^{-1} \cdot 0 = 0$. □

THEOREM

Suppose that R is an integral domain and that $0 \neq a \in R$. Then $ax = ay \Rightarrow x = y$.

PROOF.

Suppose that $0 \neq a \in R$ and that R is an integral domain.

Then we have $ax = ay \Rightarrow ax - ay = 0 \Rightarrow a(x - y) = 0$.

Since $a \neq 0$ and R is an integral domain, we conclude that $x = y$. □

LEMMA

If R is an integral domain and $0 \neq a \in R$ and $0 < k \in \mathbb{Z}$ then $a^k \neq 0$.

PROOF.

Suppose that $0 \neq a \in R$.

Let $S = \{k \in \mathbb{Z} \mid k > 0; a^k = 0\}$.

Assume for the sake of contradiction that $S \neq \emptyset$.

If this is true then by the well ordering principle, there is a smallest element, say $j \in S$.

Note that $0 \neq a = a^1$. Thus $j \geq 2$.

Now we have $0 = a^j = a \cdot a^{j-1}$.

Since $1 \leq j-1 < j$, we have that $a^{j-1} \neq 0$ and we were given that $a \neq 0$.

Thus we have reached a contradiction to our hypothesis that R was an integral domain.

Thus $S = \emptyset$ and the lemma holds. □

THEOREM

Every finite integral domain is a field.

PROOF.

Suppose that R is a finite integral domain and $0 \neq a \in R$.

Consider the infinite sequence $\{a^k\}_{k \geq 1}$

Since R is finite the above sequence must repeat.

Thus there exists $i, j \in \mathbb{Z}$ with $i > j$ such that $a^i = a^j$.

Since $(i - j) > 0$, we have $0 = a^i - a^j = a^j(a^{i-j} - 1)$.

Since R is an integral domain and $a^j \neq 0$ by our lemma, we can conclude that $a^{i-j} = 1$

Thus, we have $a \cdot a^{i-j-1} = 1$. (**Note:** $i > j \Rightarrow i - j - 1 \geq 0$.)

Thus, $a^{i-j-1} = a^{-1}$.

So, we have shown that if $a \neq 0$, then a is a unit. Thus R is a field. □

DEFINITION

Suppose that R is a ring. A zero divisor in R is an element a satisfying:

- 1 $a \neq 0$.
- 2 There is an element $0 \neq b \in R$ such that either $ab = 0$ or $ba = 0$.