LECTURE 15

Basic Properties of Rings

THEOREM 15.1. *For any element a in a ring R, the equation $a + x = 0_R$ has a unique solution.*

Proof.

We know that $a + x = 0_R$ has at least one solution $u \in R$ by Axiom (5) in the definition of a ring. If v is also a solution then, $a + u = 0_R$ and $a + v = 0_R$, so

$$\begin{aligned} u &= u + 0_R \\ &= u + (a + v) \\ &= (u + a) + v \\ &= 0_R + v \\ &= v \quad . \end{aligned}$$

Therefore, $a + x = 0_R$ has only one solution. □

We can now define negatives and subtraction in any ring R. Let $a \in R$. By Theorem 3.2, $a + x = 0_R$ has a unique solution in R. We shall denote this unique solution by $-a$.

DEFINITION 15.2. *If R is a ring and $a \in R$, then $-a$ is the unique solution of $a + x = 0_R$.*

DEFINITION 15.3. *If $a, b \in R$, then*

$$a - b \equiv a + (-b) \quad .$$

The following example shows how these familiar concepts can take an unusual form.

Example: In $\mathbb{Z}_6$,

$$\begin{aligned} -0 &= 0 \\ -1 &= 5 \\ -2 &= 4 \\ -3 &= 3 \\ -4 &= 2 \\ -5 &= 1 \quad . \end{aligned}$$

Note that not only is $0 = -0$, but $3 = -3$.

While we're at it, let us also define for any ring R and any $a \in R$ and any positive integer $n \in \mathbb{Z}$

$$\begin{aligned} a^n &\equiv aaa \cdots a \quad (n \text{ factors}) \\ na &\equiv a + a + a + \cdots + a \quad (n \text{ summands}). \end{aligned}$$

THEOREM 15.4. *If $a + b = a + c$ in a ring R, then $b = c$.*

Proof. Adding $-a$ to both sides of $a+b=a+c$ produces

$$\begin{aligned} -a+(a+b) &= -a+(a+c) \\ (-a+a)+b &= (-a+a)+c \\ 0_R+b &= 0_R+c \\ b &= c \quad . \end{aligned}$$

□

THEOREM 15.5. *For any elements a, b of a ring R:*

(a) $a \cdot 0_R = 0_R = 0_R \cdot a$
(b) $a(-b) = -(ab) = (-a)b$
(c) $-(-a) = a$
(d) $-(a+b) = -a+(-b)$
(e) $-(a-b) = -a+b$
(f) $(-a)(-b) = ab$
(g) *If R has an identity 1_R, then $(-1_R)a = -a$*

Proof.

(a) We have

$$\begin{aligned} 0_R+0_R &= 0_R \\ \Rightarrow \quad a\cdot(0_R+0_R) &= a\cdot 0_R \\ &= (a+0_R)+0_R \\ \Rightarrow \quad (a\cdot 0_R)+(a\cdot 0_R) &= (a+0_R)+0_R \end{aligned}$$

Theorem 3.3 then implies $a \cdot 0_R = 0_R$. The proof that $0_R \cdot a = 0_R$ is similar.

(b) By definition $-(ab)$ is the unique solution of $ab + x = 0_R$, so any other solution of this equation must be equal to $-(ab)$. But $x = a(-b)$ is also a solution, since by the distributive law and (a)

$$ab + a(-b) = a\,(b+(-b)) = a \cdot 0_R = 0_R \quad .$$

Therefore $-(ab) = a(-b)$. The other parts are proven similiarly.

(c) By definition, $-(-a)$ is the unique solution of $(-a)+x = 0_R$. But $x = a$ is also a solution, so $a = -(-a)$.

(d) By definition, $-(a+b)$ is the unique solution of $(a+b)+x = 0_R$. But $(-a)+(-b)$ is also a solution, since

$$(a+b)+((-a)+(-b)) = (a+(-a))+(b+(-b)) = 0_R+0_R = 0_R \quad .$$

So, by uniqueness, $a+b = (-a)+(-b)$.

(e) By the definition of subtraction and (c) and (d),

$$-(a+b) = -\,(a-(-b)) = (-a)+(-(-b)) = -a+b \quad .$$

(f) By (c) and the repeated use of (b)

$$(-a)(-b) = -\,(a(-b)) = -\,(-(ab)) = ab \quad .$$

(g) By (b)

$$(-1_R)a = -\,(1_R a) = -(a) = -a \quad .$$

$\square$

THEOREM 15.6. *Let R be a ring and let $a, b \in R$. Then the equation $a + x = b$ has the unique solution $x = b - a$.*

Proof. $x = b - a$ is a solution because

$$a + (b - a) = a + (b + (-a)) = a + (-a) + b = 0_R + b = b \quad .$$

It is unique since, if w is any other solution then

$$a + w = b = a + (b - a)$$

hence $w = b - a$ by Theorem 3.3. Hence $x = b - a$ is the only solution.

Remark: Remember that, in general, a multiplicative equation

$$ax = b$$

need not have a solution in R. For example,

$$3x = 2$$

has no solution in $\mathbb{Z}$. Yet there is one special case when solutions of equations of the form $ax = b$ always exist. This is when R is a division ring. For in this case, by definition, for any $a \neq 0_R$ in R we have a solution of $ax' = 1_R$. Multiplying this equation (from the right by b yields

$$(ax')b = 1_R b$$

or

$$a(x'b) = b \quad .$$

Hence, if R is a division ring, a solution of $ax = b$ always exists (namely, $x = ax'$, where x' is the solution of $ax' = 1_R$).

DEFINITION 15.7. *A element a in a ring R with identity 1_R is called a* ***unit*** *if there exists an element $b \in R$ such that $ab = 1_R = ba$. In this case, the element b is called the multiplicative inverse of a and is denoted by a^{-1}.*

Note that in a division ring every non-zero element a is a unit (since if R is a division ring, the equation $ax = 1_R = xa$ always has a solution if $a \neq 0_R$). Indeed, in a division ring R we are by definition guaranteed solutions of $ax = 1_R$ and $ya = 1_R$. So suppose $au = 1_R$ and $va = 1_R$. Then

$$u = 1_R u = (va)u = v(au) = v1_R = v \quad .$$

Example: The only units in $\mathbb{Z}$ are 1 and -1.

Example: Recall that $M_2(\mathbb{R})$ is the non-commutative ring with identity defined

$$M_2(\mathbb{R}) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbb{R} \right\}$$

with

$$\begin{aligned} \begin{pmatrix} a & b \\ c & d \end{pmatrix} + \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} &= \begin{pmatrix} a + a' & b + b' \\ c + c' & d + d' \end{pmatrix} \\ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a' & b' \\ c' & d' \end{pmatrix} &= \begin{pmatrix} aa' + bc' & ab' + bd' \\ ca' + dc' & ab' + fd' \end{pmatrix} \\ O_R &= \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix} \\ 1_R &= \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} \quad . \end{aligned}$$

Every element $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ such that $ad - bc \neq 0$ is a unit in $M_2(\mathbb{R})$; for

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \equiv \begin{pmatrix} \frac{d}{ad-bc} & \frac{-b}{ad-bc} \\ \frac{-c}{ad-bc} & \frac{a}{ad-bc} \end{pmatrix}$$

satisfies

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & b \\ c & d \end{pmatrix}^{-1} \begin{pmatrix} a & b \\ c & d \end{pmatrix} \quad .$$

DEFINITION 15.8. *A nonzero element a in a commutative ring R is called a* ***zero divisor*** *if there exists a nonzero element $b \in R$ such that $ab = 0_R$.*

THEOREM 15.9. *Let R be a ring with identity and $a, b \in R$. If a is a unit, then each of the equations*

$$\begin{aligned} ax &= b \\ ya &= b \end{aligned}$$

has a unique solution in R.

Proof. Since a is a unit, it has an inverse $a^{-1} \in R$. But then $x = a^{-1}b$ and $y = ba^{-1}$ are solutions of the equations above since

$$\begin{aligned} a(a^{-1}b) = (aa^{-1})b = 1_R b = b \quad , \\ (ba^{-1})a = b(a^{-1}a) = b1_R = b \quad . \end{aligned}$$

If c is another solution of $ax = b$, then $ac = b$ and

$$c = 1_R c = (a^{-1}a)c = a^{-1}(ac) = a^{-1}b \quad .$$

Similarly, if d is another solution of $ya = b$, then $dc = b$ and

$$d = d1_R = d(aa^{-1}) = (da)a^{-1} = ba^{-1} \quad .$$

Therefore, $x = a^{-1}b$ and $y = ba^{-1}$ are the only solutions. □

THEOREM 15.10. *Let R be a commutative ring with identity. Then R is an integral domain if and only if R has this cancellation property:*

$$ab = ac \quad \Longrightarrow \quad b = c \qquad \textit{whenever } a \neq 0_R$$

Proof.

⇒ Assume R is an integral domain. If $ab = ac$ then $ab - ac = 0_R$, so $a(b - c) = 0_R$. Since R is an integral domain, if $a \neq 0_R$, then we must necessarily have $b - c = 0_R$, or $b = c$.

⇐ Assume that the cancellation property holds in R and that R is not an integral domain. Then there exists $a, b \in R$ such that $ab = 0_R$ and $a, b \neq 0_R$. But then

$$a \cdot 0_R = 0_R = ab$$

and so the cancellation property implies $b = 0_R$; but this is a contraction. □

COROLLARY 15.11. *Every field R is a an integral domain.*

Proof. We first note that by definition(s) every non-zero element a of a field R is a unit. Also, every field is a commutative ring with identity. Now suppose $ab = ac$ and $a \neq 0_R$. Multiplying both sides of $ab = ac$ by a^{-1} yields $b = c$. Therefore, R is an integral domain by Theorem 3.7. □

THEOREM 15.12. *Every finite integral domain R is a field.*

Proof. Since R is a commutative ring with identity, we need only show that for each $a \neq 0_R$, the equation $ax = 1_R$ has a solution. Let $a_1, a_2, \ldots, a_n$ be the distinct elements of R, and suppose $a_t \neq 0_R$. To show that $a_t x = 1_R$ has a solution, consider the products $a_t a_1, a_t a_2, \ldots, a_t a_n$. If $a_i \neq a_j$ we must have $a_t a_i \neq a_t a_j$ since otherwise the cancellation property coming from Theorem 3.7 would imply $a_i = a_j$, i.e., we would have a contradiction. Therefore, the $a_t a_1, a_t a_2, \ldots, a_t a_n$ are all distinct elements of R. However, R has exactly n elements, one of which is 1_R. Therefore, there must be some a_j such that $a_t a_j = 1_R$. Therefore, every equation $ax = 1_R$, with $a \neq 0_R$ has a solution in R. Hence, R is a field. $\square$

COROLLARY 15.13. *Every $\mathbb{Z}_p$ with p prime is a (finite) field.*