Lecture 20, Oct. 18

20.1 Axiom.

$$\forall x\, \forall y\, \forall z\ (x+y)+z = x+(y+z)$$

20.2 Axiom.

$$\forall x\, \forall y\ x+y = y+x$$

20.3 Axiom.

$$\forall x\ x+0 = x$$

20.4 Axiom.

$$\forall x\, \exists y\ x+y = 0$$

20.5 Axiom.

$$\forall x\, \forall y\, \forall z\ (xy)z = x(yz)$$

20.6 Axiom.

$$\forall x\ 1x = x1 = x$$

20.7 Axiom.

$$\forall x\, \forall y\, \forall z\ x(y+z) = xy+xz \wedge (x+y)z = xz+yz$$

R is commutative when

20.8 Axiom.

$$\forall x\, \forall y\ xy = yx$$

R is a field when

20.9 Axiom.

$$\forall x\ (\neg x = 0 \rightarrow \exists y\ (xy = 1 \wedge yx = 1))$$

20.10 Definition. Let R be a ring. Let $a, b \in R$. If $ab = 1$ we sat that a is a **left inverse** of b and b is a **right inverse** of a

If $ab = ba = 1$, then we say that a and b are (2-sided) inverses of each other. We say that $a \in R$ is **invertible** or that a is a **unit** when a has a (2-sided) inverse b.

If $a \neq 0$ and $b \neq 0$ and $ab = 0$ then a and b are called **zero divisors**.

20.11 Theorem. Uniqueness of Identities and Inverses. *Let R be a ring.*

1. *The zero element is unique:*
   for all $e \in R$, if for all $x \in R$, $x + e = x$, then $e = 0$
2. *For all $a \in R$ the additive inverse of a is unique (which we denote by $-a$):*
   for all $a \in R$, for all $b, c \in R$, if $a + b = 0$ and $a + c = 0$ then $b = c$
3. *The identity element is unique.*
   for all $u \in R$, if for all $x \in R$ we have $x \cdot u = x$ and $u \cdot x = x$ then $u = 1$

4. *For every invertible $a \in R$, the multiplicative inverse of a is unique:*
   for all $a \in R$, for all $b, c \in R$, if $ab = ba = 1$ and $ac = ca = 1$, then $b = c$

Proof. 1. Let $e \in R$ be arbitrary. Suppose that for all $x \in R$, $x + e = x$. Then, in particular, $0 + e = 0$. Thus

$$\begin{aligned} e =& e + 0 \text{ by 20.3} \\ =& 0 + e \text{ by 20.2} \\ =& 0 \text{ as shown above} \end{aligned}$$

□

20.12 Exercise. Make a derivation to show that

$$\{20.2, 20.3\} \models \forall e \; (\forall x \; x + e = x \to e = 0)$$

20.13 Theorem. Some Additive Cancellation Properties. *Let R be a ring. Let $a, b, c \in R$ Then*

1. *if $a + b = a + c$ then $b = c$*
2. *if $a + b = a$ then $b = 0$*
3. *if $a + b = 0$ then $b = -a$*

Proof. 1. Suppose that $a + b = b + c$. Choose $d \in R$ so that $a + d = 0$ (by 20.4). Then

$$\begin{aligned} b =& b + 0 \text{ by 20.3} \\ =& b + (a + d) \text{ since } a + d = 0 \\ =& (b + a) + d \text{ by 20.1} \\ =& (a + b) + d \text{ by 20.2} \\ =& (a + c) + d \text{ since } a + b = a + c \\ =& (c + a) + d \text{ by 20.2} \\ =& c + (a + d) \text{ by 20.1} \\ =& c + 0 \text{ since } a + d = 0 \\ =& c \text{ by 20.3} \end{aligned}$$

□

20.14 Exercise. Make a derivation

20.15 Theorem. Some More basic Properties *Let R be a ring. Let $a, b \in R$ then,*

1. $0 \cdot a = 0$
2. $-(-a) = a$
3. $(-a)b = -(ab) = a(-b)$

4. $(-a)(-b) = ab$
5. $(-1)a = -a$
6. $a(b-c) = ab - ac$ *and* $(a-b)c = ac - bc$ *where* $x - y = x + (-y)$

Proof. 1. Choose $b \in R$ so that $0a + b = 0$

$$\begin{aligned} 0a =& (0+0)a \text{ by 20.3} \\ =& 0a + 0a \text{ by 20.3} \end{aligned}$$

$$\begin{aligned} 0a + b =& (0a + 0a) + b \text{ as shown above} \\ =& 0a + (0a + b) \text{ by 20.1} \end{aligned}$$

$$\begin{aligned} 0 =& 0a + 0 \text{ since } 0a + b = 0 \\ =& 0a \text{ by 20.3} \end{aligned}$$

□

20.16 Theorem. Multiplicative Cancellation *Let R be a ring. Let $a, b, c \in R$. Then if $ab = ac$ (or if $ba = ca$) then $a = o$ or a is a zero-divisor or $b = c$.*

Proof. Suppose $ab = ac$

Then $ab - ac = 0$, then $a(b-c) = 0$.

So either $a = 0$ or $b - c = 0$ or ($a \neq 0$ and $b - c \neq 0$) a is a zero-divisor ($b - c$ is a zero-divisor) □