The integers.

If S is a set then an *order* on S is a binary relation $a < b$ that has two properties:

I (Transitivity)If $a, b, c \in S$ and $a < b$ and $b < c$ then $a < c$.

2.(Trichotomy)If $a, b \in S$ then exactly one of $a < b$, $a = b$ or $b < a$ is true.

Examples of orders are the usual orderings on $\mathbb{Z}$ (the integers), $\mathbb{Q}$ (the rational numbers) and $\mathbb{R}$ (the real numbers). The following exercise defines a different sort of order.

Exercise 1. If (a, b) and (c, d) are in $\mathbb{R}^2$ (the plane) then we say that $(a, b) < (c, d)$ if $a < c$ or if $a = c$ and $b < d$. Show this definition defines an order. It is called the *lexicographic order* since it mimics a dictionary.

We note that if T is a subset of S then if we have an order on S then if $a, b \in S$ then $a < b$ in the order on S defines an order on T.

If S is an order on a set S then it is called a *well order* if whenever T is a non-empty subset of S such that there exists $s \in S$ such that $s \leq t$ for all $t \in S$ (i.e. the set S is *bounded below*) then there is an element $m \in T$ such that $m \leq t$ for every $t \in T$ (here $a \leq b$ means $a = b$ or $a < b$). This element is called a *minimal element of* T.

Exercise 2. Show that of S is well ordered then for each $T \neq \emptyset$ (empty set) that is bounded blow there is a unique minimal element.

Examples. If S is $\mathbb{R}$ with the usual order then every subset non-empty $T \subset \mathbb{R}$ that is bounded below has a greatest lower bound in $\mathbb{R}$ but not necessarily in T. For example the set $\mathbb{R}_{>0} = \{x \in \mathbb{R} | x > 0\}$. If S is $\mathbb{Q}$ then the set $T = \{x \in \mathbb{Q} | x > 0 \text{ and } x^2 > 2\}$ has no greatest lower bound in $\mathbb{Q}$.

A set S is called a *ring with identity* if it contains elements 0 and 1 and there are two binary operations on S, denoted $a + b$ and $a \cdot b$ or ab for $a, b \in S$ that satisfy the following rules:

R-1.(Commutativity) If $a, b \in S$ then $a + b = b + a$ and $ab = ba$.

R-2. (Associativity) If $a, b, c \in S$ then $a + (b + c) = (a + b) + c$ and $a(bc) = (ab)c$. This rule allows us to drop parentheses.

R-3 (Distributive Law) If $a, b, c \in S$ then $a(b + c) = ab + ac$.

R-4 (Identity) If $a \in S$ then $a + 0 = a$ and $1a = a$.

R-5 (Negative) If $a \in S$ then there exists an element $b \in S$ such that $a + b = 0$.

We note **R**-1-5 are the familiar rules of arithmetic and are satisfied by $\mathbb{Z}$,$\mathbb{Q}$ and $\mathbb{R}$ with the usual addition and multiplication. We we will now prove that if $1' \in S$ has the property that $1'a = a$ for all $a \in S$ then $1' = 1$. To see

this we note that $1 \cdot 1' = 1'$ and (this is a trick– if you don't think of such a trick you can't go on with the argument) **R**-1 implies that $1 \cdot 1' = 1' \cdot 1$. Since $1' \cdot a = a$ for all $a \in S$ we see that in particular $1' \cdot 1 = 1$. Thus $1' = 1' \cdot 1 = 1' \cdot 1 = 1$.

Lemma 1. If $0' \in S$ is such that $0' + a = a$ for some $a \in S$ then $0' = 0$.

Proof. We have $a = 0' + a$. Thus $(-a) + a = (0' + a) - a$. Thus $0 = 0' + (a - a) = 0' + 0 = 0'$. (Another trick.)

Exercise 3. Prove that the element b in R-5 is unique.

Thus if we have a ring then we also have subtraction. if $a \in S$ and b is the element such that $a + b = 0$ then we will write $b = -a$. Also, we write $c - a$ for $c + (-a)$ (subtraction).

Exercise 4. On $\mathbb{Z}$ we change addition to subtraction but leave multiplication as is. Are rules R-1-5 satisfied?

Exercise 5. Let S be a set consisting of one element which we call 0. Then show that if $S = \{0\}$ then the only possible way to define multiplication and addition on S is $0 \cdot 0 = 0$ and $0 + 0 = 0$. Show that with these choices R-1-5 are satisfied.

Exercise 6. Let S be a set with 2 elements which we denote 0 and 1. We assume that these elements satisfy R-4. Write out the only possible multiplication and addition tables and show that all of R-1 through R-5 are satisfied.

Exercises 5 and 6 say that the rules of arithmetic are satsified in many ways.

Lemma 2. If S is a ring and $a \in S$ then $0 \cdot a = 0$ and $-a = (-1)a$

Proof. We have $a + 0.a = 1 \cdot a + 0 \cdot a = (1 + 0) \cdot a = 1 \cdot a = a$. Thus Lemma 1 implies $0 \cdot a = 0$. We now calculate $a + (-1)a = 1 \cdot a + (-1) \cdot a = (1 + -1) \cdot a = 0 \cdot a = 0$. Thus Exercise 3 implies that $(-1)a = -a$.

A ring, S ,with identity that is ordered as a set is said to be and *ordered ring* if whenever $a.b.c \in S$ the relation $a < b$ implies $a + c < b + c$ and if $c > 0$ then $ac < bc$. Here are some properties of ordered rings,

Lemma 3. Let S be an ordered ring with $1 \neq 0$ then

a. $1 > 0$.

b. If $a < 0$ then $-a > 0$.

Proof. Trichotomy implies that $1 > 0$ or $1 < 0$ (but not both). If $1 < 0$ then if $a > 0$ then $a \cdot 1 < a \cdot 0 = 0$. Thus $a > 0$ implies $a < 0$ this contradicts Trichotomy.

If $a < 0$ then $a + (-a) < 0 + (-a)$. Thus $0 < -a$.

We note that if S is a ring with $0 = 1$ then $S = \{0\}$. This is the *trivial* ring.

Examples of ordered rings are $\mathbb{Z}, \mathbb{Q}$ and $\mathbb{R}$. Thus we still haven't characterized the integers. The basic difference is that $\mathbb{Z}$ is *well ordered*.

We have finally separated the integers from the rational numbers and the real numbers.

Theorem 1. $\mathbb{Z}$ is a well ordered ring.

Proof. For this we use the Archimedian property of the order on $\mathbb{Z}$. That is if $a, b \in \mathbb{Z}$ then then by progressively adding $1's$ to a we will eventually have a number greater than b. We also will use the fact that if $s \in \mathbb{Z}$ then there is no $t \in \mathbb{Z}$ such that $s+1 > t > s$. Now let $T \neq \emptyset$ be a subset of $\mathbb{Z}$ with lower bound $s \in \mathbb{Z}$. If we add 1 to s then either $s + 1$ is still a lower bound or there is a t in T such that $s + 1 > t$. The Archimedean property implies that since there exists $u \in T$ that if we progressively add 1 to s eventually we will have a number that is greater than u and hence not a lower bound for T. Thus we define $s_1 = s$ if $s_1 + 1$ is not a lower bound then there is $t \in T$ with $s + 1 > t$. Thus $s_1 + 1 > t \geq s_1$. We have observed that $s_1 + 1 > t > s_1$ is impossible so we must have $t = s_1$ so s_1 is a minimum. Otherwise $s_1 + 1$ is a lower bound. Set $s_2 = s_1 + 1$. If $s_2 + 1$ is not a lower bound then the argument above says s_2 is a minimum. If $s_2 + 1$ it is a lower bound then call it s_3. We continue in this way and find that either we have found a minimum or we will have a sequence defined by $s_{i+1} = s_i + 1$ and every element is a lower bound. This contradicts the Archimedian condition (Why?).

We can now lay out what we have about $A = \mathbb{Z}$, the integers.

I-1. The integers form a ring with 1.

I-2. The ring is an ordered ring with $1 \neq 0$.

I-3. The order is Archimedian. That is of $a, b \in A$ and if we progressively add 1 to a we will eventually have a number greater than b.

I-4. If $a \in A$ then there is no solution in A to $a < b < a + 1$.

We now observe that in the proof of Theorem 1 we only used these three properties.

Theorem 2. If A is a ring satisfying I-1 though I-4 then the elements of A are exactly $0, \pm 1, \pm(1 + 1), \pm(1 + 1 + 1), ..., \pm(1 + 1 + ... + 1), ...$

Proof. It is enough to show that the set gotten by progressively adding 1 to 1 exhausts $\{a \in A | a > 0\}$. So let $a \in A, a > 0$. Since we cannot solve $0 < a < 1$ by I-4, Trichotomy implies that $a \geq 1$. If $a = 1$ we are done. Otherwise we have $a > 1$. Since we cannot solve $1 < a < 1+1$ we have either $a = 1 + 1$ or $a > 1 + 1$. The Archimedian condition implies that the greater

than condition is eventually impossible. Thus a is a sum of $1's$.

Corollary.(The principle of mathematical induction). If $S \subset \mathbb{Z}_{>0} = \mathbb{N} - \{0\} = \{n \in \mathbb{Z} | n > 0\}$ satisfies the two conditions:

a) $1 \in S$.

b) If $s \in S$ then $s + 1 \in S$.

Then $S = \mathbb{Z}_{>0}$.

Example. If n is a positive integer then $1 + 2 + ... + n = \frac{n(n+1)}{2}$.

Proof. Let $S = \{n \in \mathbb{Z}_{>0} | 1 + 2 + ... + n = \frac{n(n+1)}{2}\}$. Then since $1 = \frac{1(1+1)}{2}$, $1 \in S$. Assume that $n \in S$ then

$$1 + 2 + ... + n + (n + 1) = (1 + 2 + ... + n) + (n + 1).$$

The assumption for n (the inductive hypothesis) implies

$$(1 + 2 + ... + n) + (n + 1) = \frac{n(n + 1)}{2} + n + 1.$$

The right hand side of this equation is $\frac{(n+1)(n+2)}{2}$. This implies that $n+1 \in S$. Thus $S = \mathbb{Z}_{>0}$ which is the assertion of the example.

In practice we will not mention the set S. We will just show that the formula is satisfied for 1 and can be derived for $n+1$ from the formula for n.

Exercise 7. Prove by induction that $1 + 2 + ... + 2^k = 2^{k+1} - 1$. *Give a proof of this without using the method of mathematical induction.

Exercise 8. Prove that every element n of $\mathbb{N}$ can be written in the form

$$n_0 + n_1 2 + n_2 2^2 + ... + n_k 2^k$$

for some k and $n_0, ..., n_k$ are each either 0 or 1.