MATH 295. HANDOUT ON INDUCTION

The purpose of this handout is to explain some issues related to induction and to construct "copies" of the natural numbers, integers, and rational numbers inside of any ordered field whatsoever. Let F be an ordered field. We say that a subset $N \subseteq F$ is *inductive* if $1 \in N$ and for all $n \in N$ we have $n + 1 \in N$.

Lemma 0.1. *There exists a unique inductive set $\mathbb{N}_F \subseteq F$ contained in all inductive sets in F.*

Proof. Note that F is an inductive set, so such sets *do* exist. Let $\mathbb{N}_F$ denote the set of all $x \in F$ which lie in *all* inductive subsets of F. Since 1 lies in every inductive subset of F, certainly $1 \in \mathbb{N}_F$. We just have to prove that $\mathbb{N}_F$ is itself inductive (by construction the rest is then clear). Well, since we just noted that $1 \in \mathbb{N}_F$, it remains to check that for all $n \in \mathbb{N}_F$, we have $n + 1 \in \mathbb{N}_F$. That is, if n lies in every inductive set in F, the same should hold true for $n + 1$. But whenever an inductive subset $S \subseteq F$ contains some n then by *definition* of the concept of "inductive set" it follows that $n + 1 \in S$. Thus, if n lies in every such S then indeed $n + 1$ lies in every such S, which is to say $n \in \mathbb{N}_F \Rightarrow n + 1 \in \mathbb{N}_F$. ∎

Note that since $\mathbb{N}_F$ is inductive, by definition of "inductive set" we see that $\mathbb{N}_F$ is stable under the operation $x \mapsto x + 1$ performed within F on elements $x \in \mathbb{N}_F$. Also, $\mathbb{N}_F$ satisfies the so-called weak induction property: if $S \subseteq \mathbb{N}_F$ is a subset such that $1 \in S$ and $n+1 \in S$ whenever $n \in S$, then $S = \mathbb{N}_F$. Indeed, any such $S \subseteq \mathbb{N}_F$ is an inductive set and hence (by the property of $\mathbb{N}_F$ in Lemma 0.1!) $\mathbb{N}_F \subseteq S$ so in fact $S = \mathbb{N}_F$.

Lemma 0.2. *If $n \in \mathbb{N}_F$ then $n \geq 1$. Moreover, if $n, m \in \mathbb{N}_F$ then $n < m$ if and only if $m = n + r$ for some $r \in \mathbb{N}_F$. In particular, if $n, m \in \mathbb{N}_F$ then $m > n$ if and only if $m \geq n + 1$ (and so $m \leq n$ if and only if $m < n + 1$).*

Note that it follows from this lemma that if $n, m \in \mathbb{N}_F$ and $n < m \leq n + 1$ then necessarily $m = n + 1$. Indeed, if not then $m < n + 1$, which the lemma shows is equivalent to $m \leq n$, contradicting our assumption that $n < m$!

Proof. Let $T = \{x \in \mathbb{N}_F \,|\, x \geq 1\} \subseteq \mathbb{N}_F$. We will show that T is an inductive set, from which it follows that $T = \mathbb{N}_F$ (so $n \geq 1$ for all $n \in \mathbb{N}_F = T$). Certainly $1 \in T$. Meanwhile, if $n \in T$ then $n \geq 1$ and so $n + 1 \in \mathbb{N}_F$ and $n + 1 \geq 1 + 1 > 1$, so $n + 1 \in T$. This says exactly that T is an inductive set, as desired. Thus, we have proven the first part.

It remains to show that if $n, m \in \mathbb{N}_F$ with $n < m$ then $m = n + r$ for some $r \in \mathbb{N}_F$ (the converse is easy: if the latter condition holds then certainly $m \geq n + 1$, so $m > n$, since we just showed that any element of $\mathbb{N}_F$ (such as r) is ≥ 1; from this the final assertion in the lemma is immediate). We will argue via "double induction" on n and m. To be precise, we *fix* n and consider

$$T_n = \{m \in \mathbb{N}_F \,|\, m \leq n \text{ or } m = n + r \text{ for some } r \in \mathbb{N}_F\}.$$

We want to show that $T_n = \mathbb{N}_F$ (so then if $m \in \mathbb{N}_F = T_n$ with $m > n$ we must have $m = n + r$ for some $r \in \mathbb{N}_F$). Consider the set

$$T = \{n \in \mathbb{N}_F \,|\, T_n = \mathbb{N}_F\}.$$

Our goal is to prove that $T = \mathbb{N}_F$. We have to show that $1 \in T$ (i.e., $T_1 = \mathbb{N}_F$) and that *if* $n \in T$ (i.e., $T_n = \mathbb{N}_F$) then $n + 1 \in T$ (i.e., $T_{n+1} = \mathbb{N}_F$).

In order to prove that $1 \in T$, we have to show that if $m \in \mathbb{N}_F$ and $m > 1$ then $m = 1 + r$ for some $r \in \mathbb{N}_F$. That is, we want to prove

$$\mathbb{N}_F = \{1\} \cup \{x \in \mathbb{N}_F \,|\, x = y + 1 \text{ for some } y \in \mathbb{N}_F\}$$

(so any element $m \in \mathbb{N}_F$ distinct from 1 must have the form $1+y$ for some $y \in \mathbb{N}_F$). But the right side of this alleged equality is certainly a subset of $\mathbb{N}_F$ which contains 1 and whenever it contains some $y \in \mathbb{N}_F$ it definitely contains $y+1$. That is, this right side is an inductive subset of $\mathbb{N}_F$ and thus must coincide with all of $\mathbb{N}_F$, as desired. This completes the verification that $T_1 = \mathbb{N}_F$, which is to say $1 \in T$.

Our hypothesis on n says exactly that if $m \in \mathbb{N}_F$ and $m > n$ then $m = n + r$ for some $r \in \mathbb{N}_F$. We want to prove that $n+1 \in T$, which is to say that if $m \in \mathbb{N}_F$ and $m > n+1$ then $m = (n+1)+r$ for some $r \in \mathbb{N}_F$. Certainly $m > n+1$ at least gives $m-1 > n$ and $m > 1$. Since $m \in \mathbb{N}_F = T_1$ and $m > 1$, we know $m = 1 + m'$ for some $m' \in \mathbb{N}_F$. That is, $m - 1 \in \mathbb{N}_F$. But $m-1 > n$ so by our hypothesis on n that $T_n = \mathbb{N}_F$, we have $m-1 \in T_n$ with $m-1 > n$, so $m-1 = n+r$ for some $r \in \mathbb{N}_F$. Thus, $m = (n+1)+r$ for this very same $r \in \mathbb{N}_F$. This completes the inductive step: $n \in T$ implies $n+1 \in T$.

■

Lemma 0.3. *If $a, b \in \mathbb{N}_F$ then $a+b, ab \in \mathbb{N}_F$. If we also have $a > b$ then $a - b \in \mathbb{N}_F$.*

Proof. The final part follows from the preceding lemma. To prove the stability of $\mathbb{N}_F$ under formation of sums and products, we *fix* $a \in \mathbb{N}_F$ and induct on b. Since $\mathbb{N}_F$ is inductive, certainly $a+1 \in \mathbb{N}_F$. Also, by hypothesis $a \cdot 1 = a \in \mathbb{N}_F$. Now let

$$T_a = \{b \in \mathbb{N}_F \,|\, a+b \in \mathbb{N}_F\},\ T'_a = \{b \in \mathbb{N}_F \,|\, ab \in \mathbb{N}_F\}.$$

Our goal is to show that $T_a = \mathbb{N}_F$ and $T'_a = \mathbb{N}_F$ and we just noted that $1 \in T_a$ and $1 \in T'_a$. We just have to check that if $b \in T_a$ then $b+1 \in T_a$ and likewise if $b \in T'_a$ then $b+1 \in T'_a$.

We first handle the case of T_a (i.e., proving $T_a = \mathbb{N}_F$). If $b \in T_a$ then $a+b \in \mathbb{N}_F$ so certainly $a+(b+1) = (a+b)+1 \in \mathbb{N}_F$. That is, $b+1 \in T_a$. This proves that $T_a = \mathbb{N}_F$. We now *use* this fact to handle the case of products. Suppose that $b \in T'_a$. Then $ab \in \mathbb{N}_F$ and $a(b+1) = ab + a \in \mathbb{N}_F$ since $ab \in \mathbb{N}_F = T_a$! This completes the proof that $T'_a = T_a = \mathbb{N}_F$ for all $a \in \mathbb{N}_F$, which says exactly that $\mathbb{N}_F$ is stable under the formation of sums and products.

■

We say that $S \subseteq \mathbb{N}_F$ is *weakly inductive* if, for all $n \in \mathbb{N}_F$, $n+1 \in S$ whenever $n \in S$. We have seen above (and have used quite a lot) the weak induction property of $\mathbb{N}_F$: a weakly inductive subset of $\mathbb{N}_F$ which contains 1 *must* coincide with $\mathbb{N}_F$. We say that $S \subseteq \mathbb{N}_F$ is *strongly inductive* if, for all $n \in \mathbb{N}_F$, $n \in S$ whenever $\{k \in \mathbb{N}_F \,|\, k < n\} \subseteq S$.

Theorem 0.4. *The only strongly inductive subset of $\mathbb{N}_F$ is $\mathbb{N}_F$, and every non-empty subset of $\mathbb{N}_F$ has a minimal element.*

That is, we claim that $\mathbb{N}_F$ satisfies the strong induction property and the well-ordering principle.

Proof. We begin by deducing the well-ordering principle from the weak induction property (whose validity for $\mathbb{N}_F$ was noted right after Lemma 0.1). Let $S \subseteq \mathbb{N}_F$ be a non-empty subset. We wish to prove that there exists $s_0 \in S$ with $s_0 \le s$ for all $s \in S$. Observe, for example, that if $1 \in S$ taking $s_0 = 1$ would certainly give a minimal element (as Lemma 0.2 shows that every element in $\mathbb{N}_F$ is ≥ 1). So we just have to consider the case $1 \notin S$. Consider the set

$$T = \{n \in \mathbb{N}_F \,|\, k \notin S \text{ for all } k \in \mathbb{N}_F \text{ with } k \le n\}.$$

Since we have reduced ourselves to considering just the case $1 \notin S$, we certainly have $1 \in T$ (thanks to the first part of Lemma 0.2!). Also, T is disjoint from S, since if $n \in T \subseteq \mathbb{N}_F$ then $n \le n$ forces $n \notin S$, and we just noted that we may assume $1 \in T$ (since we just have to consider the case $1 \notin S$). Since S is non-empty, there is *some* $s \in S$, so $s \notin T$. Hence, $T \neq \mathbb{N}_F$. But $1 \in T$, so by the weak induction property of $\mathbb{N}_F$ there must exist *some* $n_0 \in T$ with $n_0 + 1 \notin T$ (for if there were no such n_0, then *weak induction* would force $T = \mathbb{N}_F$, which is false). I claim that the magical $n_0 + 1$ is our sought-after least element of S. Since $n_0 \in T \subseteq \mathbb{N}_F$, we know that $k \notin S$ for all $k \in \mathbb{N}_F$ with $k \leq n_0$. But $n_0 + 1 \in \mathbb{N}_F$ (since $n_0 \in \mathbb{N}_F$) and $n_0 + 1 \notin T$, so *some* $k_0 \in \mathbb{N}_F$ satisfying $k_0 \leq n_0 + 1$ must lie in S. We just noted that the condition $k \leq n_0$ for $k \in \mathbb{N}_F$ forces $k \notin S$, so $n_0 < k_0 \leq n_0 + 1$. By the remark following Lemma 0.2 we conclude that $k_0 = n_0 + 1$. That is, $n_0 + 1 \in S$ and (since $n_0 \in T$) for all $k \in \mathbb{N}_F$ with $k < n_0 + 1$ (i.e., $k \leq n_0$, by Lemma 0.2!!) we have $k \notin S$. This says exactly that $n_0 + 1 \in S$ is a minimal element, and so completes the deduction of the well-ordering principle from the weak induction axiom.

Next, we show that the just-proven well-ordering principle implies the strong induction axiom. Let $S \subseteq \mathbb{N}_F$ be strongly inductive. We want $S = \mathbb{N}_F$. Assume otherwise, so the complement $T = \mathbb{N}_F - S$ is *non-empty*. By the *well-ordering principle*, there is a least element $t_0 \in T$. I claim that any $x \in \mathbb{N}_F$ with $x < t_0$ necessarily lies in S. Indeed, since $t_0 \in \mathbb{N}_F$ is the *least* element of T, any $x \in \mathbb{N}_F$ satisfying $x < t_0$ *cannot* lie in $T = \mathbb{N}_F - S$. This forces any such x to be in S, as desired. Now recall that we assumed S is a strongly inductive set. Since we just showed that $x \in S$ for all $x \in \mathbb{N}_F$ satisfying $x < t_0$, the strongly inductive set $S \subseteq \mathbb{N}_F$ must contain t_0. This is a contradiction (since $t_0 \in T = \mathbb{N}_F - S$), so our original hypothesis that $S \neq \mathbb{N}_F$ (i.e., $T = \mathbb{N}_F - S \neq \emptyset$) is false. In other words, from the well-ordering principle we have deduced that a strongly inductive subset of $\mathbb{N}_F$ must equal $\mathbb{N}_F$.

■

We conclude by making some other auxiliary definitions and remarks. We define

$$\mathbb{Z}_F = \{x \in F \mid x \in \mathbb{N}_F \text{ or } x = 0 \text{ or } -x \in \mathbb{N}_F\},$$
$$\mathbb{Q}_F = \{x \in F \mid x = m/n \text{ for some } m, n \in \mathbb{Z}_F \text{ with } n \neq 0\}.$$

We claim that $\mathbb{Z}_F \subseteq F$ is stable under formation of sums, products, and additive inverses, while $\mathbb{Q}_F - \{0\}$ is also stable under multiplicative inversion within F (so $\mathbb{Q}_F$ is a *field*). By its definition $\mathbb{Z}_F$ is preserved under formation of additive inverses. Thus, the stability of $\mathbb{Z}_F$ under products immediately reduces to the already-proven stability of $\mathbb{N}_F$ under products (multiplication by 0 is trivially handled separately). For sums, since $-a + -b = -(a + b)$ and we already know that $\mathbb{N}_F$ is stable under sums, we just have to check $-a + b \in \mathbb{Z}_F$ for $a, b \in \mathbb{N}_F$ (the case of adding 0 is trivial). If $b = a$ then $-a + b = 0 \in \mathbb{Z}_F$. If $b > a$ then $-a + b = b - a \in \mathbb{N}_F \subseteq \mathbb{Z}_F$ by Lemma 0.1. Finally, if $b < a$ then $-a + b = -(a - b) \in \mathbb{Z}_F$ since $a - b \in \mathbb{N}_F$.

Using the formulas for how to add and multiply a/b and c/d in a field, it follows from the just-proven stability properties of $\mathbb{Z}_F$ that $\mathbb{Q}_F$ is stable under formation of sums and products. The stability of $\mathbb{Q}_F$ under formation of inverses is similar.

Finally, if we let F^+ denote the positive elements of F, then we claim that $\mathbb{Q}_F \cap F^+$ is *exactly* the set of $q = m/n$ with $m, n \in \mathbb{N}_F$, and that this defines an order structure on $\mathbb{Q}_F$. We have shown $n \geq 1 > 0$ for all $n \in \mathbb{N}_F$, and so we certainly have $n^{-1} > 0$ for any $n \in \mathbb{N}_F$. Thus, if $m, n \in \mathbb{N}_F$ then $m/n = m \cdot n^{-1} > 0$. This proves that

$$\{q \in \mathbb{Q}_F \mid q = m/n \text{ for some } m, n \in \mathbb{N}_F\} \subseteq \mathbb{Q}_F \cap F^+.$$

Since $a/b = (-a)/(-b)$, any $q \in \mathbb{Q}$ can be expressed in the form $q = m/n$ with $m \in \mathbb{Z}_F$ and $n \in \mathbb{N}_F$. If $m \notin \mathbb{N}_F$ then either $m = 0$ (in which case $q = 0$) or $-m \in \mathbb{N}_F$ (in which case $q = -((-m)/n)$ with $(-m)/n \in F^+$ since $-m, n \in \mathbb{N}_F$). Since both of these latter options rule out the possibility $q \in F^+$, we conclude that *if* $q \in \mathbb{Q} \cap F^+$ then necessarily $q = m/n$ with $n, m \in \mathbb{N}_F$. That is, the above displayed inclusion of sets must be an equality. It is easy to check that $\mathbb{Q}_F \cap F^+$ satisfies the properties to define an order structure on $\mathbb{Q}_F$ (since F^+ is an order structure on F).