

**Last Time:**

A *field* is a set  $\mathbb{F}$  with two operations, addition and multiplication, such that

(i)  $\alpha + (\beta + \gamma) = (\alpha + \beta) + \gamma$  and  $\alpha(\beta\gamma) = (\alpha\beta)\gamma \quad \forall \alpha, \beta, \gamma \in \mathbb{F}$ ,

(ii) There are elements  $0 \in \mathbb{F}$  and  $1 \in \mathbb{F}$  satisfying

$$\alpha + 0 = \alpha = 0 + \alpha \quad \text{and} \quad \alpha 1 = \alpha = 1\alpha \quad \forall \alpha \in \mathbb{F},$$

(iii) For every  $\alpha \in \mathbb{F}$  there exists a  $-\alpha \in \mathbb{F}$  and for every  $\beta \neq 0 \in \mathbb{F}$  there exists a  $\beta^{-1} \in \mathbb{F}$  satisfying

$$\alpha + -\alpha = 0 = -\alpha + \alpha \quad \text{and} \quad \beta\beta^{-1} = 1 = \beta^{-1}\beta,$$

(iv)  $\alpha + \beta = \beta + \alpha$  and  $\alpha\beta = \beta\alpha \quad \forall \alpha, \beta \in \mathbb{F}$ , and

(v)  $\alpha(\beta + \gamma) = \alpha\beta + \alpha\gamma$  and  $(\alpha + \beta)\gamma = \alpha\gamma + \beta\gamma \quad \forall \alpha, \beta, \gamma \in \mathbb{F}$ .

By identifying the field axioms, we can now use them to prove theorems about fields. Specifically, if we're careful to use only the field axioms and basic logic in our proofs, then the results we prove will have to be true for *every* field. For instance, we have

**Theorem:** (Additive cancellation law) If  $\mathbb{F}$  is a field and  $\alpha, \beta, \gamma \in \mathbb{F}$  satisfy  $\alpha + \beta = \alpha + \gamma$ , then  $\beta = \gamma$ .

**Proof:** Consider  $-\alpha + (\alpha + \beta)$ . Since  $\alpha + \beta = \alpha + \gamma$ , we have

$$-\alpha + (\alpha + \beta) = -\alpha + (\alpha + \gamma).$$

Now, the fact that addition is associative (axiom (i)) says

$$(-\alpha + \alpha) + \beta = (-\alpha + \alpha) + \gamma$$

and axiom (iii) then says

$$0 + \beta = 0 + \gamma$$

which then by axiom (ii) says

$$\beta = \gamma,$$

as required. □

Once we've proved a result, we can use it to prove other results. For example,

**Theorem:** For any  $\alpha \in \mathbb{F}$ ,  $0\alpha = 0$ .

**Proof:** By axiom (ii),  $0 = 0 + 0$ . Then  $0\alpha = (0 + 0)\alpha = 0\alpha + 0\alpha$  by axiom (v); on the other hand, axiom (ii) says  $0\alpha + 0 = 0\alpha$ . Then by additive cancellation we have  $0 = 0\alpha$ . □

**Theorem:** If  $\mathbb{F}$  is a field in which  $0$  has a multiplicative inverse, then every element of  $\mathbb{F}$  equals zero.

**Proof:** Let  $\mathbb{F}$  be a field in which  $0$  has a multiplicative inverse  $0^{-1}$ . Then for any  $\alpha \in \mathbb{F}$  we have

$$\alpha = 1\alpha = (00^{-1})\alpha = 0(0^{-1}\alpha) = 0.$$

□

Note that this explains why we can't just declare  $\infty = \frac{1}{0}$  and make math much simpler – any field in which zero has a multiplicative inverse contains only one element, namely zero. Thus, we have to either give up the field axioms, give up on zero having a multiplicative inverse, or settle for a number system with only one number.

Many results in linear algebra are proved using a method known as *proof by mathematical induction*, which should really be called “recursive deduction.” Here’s the idea: let  $\phi(n)$  be a statement involving a variable  $n$  and let  $X$  be the set of all numbers  $n \in \mathbb{Z}$  for which  $\phi(n)$  is true. Suppose we know that

- (1)  $1 \in X$  and
- (2) If  $n \in X$  then  $n + 1 \in X$ .

Then since  $1 \in X$ , (2) says that  $2 \in X$ . But then  $2 \in X$  says  $3 \in X$ , and then  $3 \in X$  says  $4 \in X$ , and so on... Indeed, (1) and (2) together imply that  $X = \{1, 2, 3, \dots\}$ . To do a proof by induction then, we must prove the *initial case* which is analogous to (1) and the *induction step* which is analogous to (2). We usually prove the initial case (typically  $n = 1$  or  $n = 0$ ) directly, i.e. by substituting in the initial value for  $n$  and verifying that the statement holds. To do the induction step, we *suppose* (which in mathematics really means “temporarily pretend”) that the statement is true for a generic  $n$  and use this to prove that the result must then hold for  $n + 1$ .

**Theorem:** (Little Gauss) For every integer  $n \geq 1$ , the sum of the integers from 1 to  $n$ , i.e.  $1 + 2 + 3 + \dots + n = \sum_{k=1}^n k$ , equals  $\frac{n(n+1)}{2}$ . That is,

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

**Proof:** (By induction on  $n$ )

Case  $n = 1$ :

$$\sum_{k=1}^1 k = 1 = \frac{2}{2} = \frac{1(1+1)}{2}.$$

Induction step:

Now suppose that  $\sum_{k=1}^n k = \frac{n(n+1)}{2}$ ; we must use this to show that  $\sum_{k=1}^{n+1} k = \frac{(n+1)((n+1)+1)}{2}$ . Well,

$$\begin{aligned} \sum_{k=1}^{n+1} k &= \sum_{k=1}^n k + (n+1) \\ &= \frac{n(n+1)}{2} + (n+1) \\ &= \frac{n(n+1)}{2} + \frac{2(n+1)}{2} \\ &= \frac{n(n+1) + 2(n+1)}{2} \\ &= \frac{(n+1)(n+2)}{2} \end{aligned}$$

as required. □

Here’s another example:

**Theorem:** The sum of the odd numbers from 1 to  $2n - 1$  equals  $n^2$ .

**Proof:** We must show that for all  $n = 1, 2, \dots$ , the sum  $\sum_{k=1}^n 2k - 1 = n^2$ .

Case  $n = 1$ : If  $n = 1$ , we have

$$\sum_{k=1}^1 2k - 1 = 2(1) - 1 = 1 = 1^2$$

as required.

Induction step:

Let us suppose that  $\sum_{k=1}^n (2k - 1) = n^2$  for a generic  $n$ ; we must use this to show that  $\sum_{k=1}^{n+1} (2k - 1) = (n + 1)^2$ .  
Well,

$$\begin{aligned}\sum_{k=1}^{n+1} (2k - 1) &= \sum_{k=1}^n 2k - 1 + (2(n + 1) - 1) \\ &= n^2 + 2n + 2 - 1 \\ &= n^2 + 2n + 1 \\ &= (n + 1)^2\end{aligned}$$

as required. □

A variant form of proof by induction is called *strong induction*; in strong induction, instead of assuming  $\phi(n)$  and using it to prove  $\phi(n + 1)$ , we assume  $\phi(1), \phi(2), \dots, \phi(n - 1)$  and use these to prove  $\phi(n)$ . Thus, the induction step consists of breaking down  $\phi(n)$  into parts that depend on  $\phi(k)$  for values of  $k$  less than  $n$ . Rephrasing the last example as a strong induction proof, we have

Induction step:

We can write

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

Then our strong induction hypothesis says  $(n - 1)^2 = \sum_{k=1}^{n-1} (2k - 1)$ , so we have

$$n^2 = (n - 1)^2 + 2(n - 1) + 1 = \sum_{k=1}^{n-1} (2k - 1) + 2(n - 1) + 1 = \sum_{k=1}^n (2k - 1)$$

as required. □