

## Why Everything Interesting Factors

**Proposition:** Every non-zero integer not equal to 1 or -1 factors into a product of “irreducible” integers.

**Proof:** Suppose not. Then there is an integer which does not factor. Further, amongst all such integers is one of smallest absolute value. Call it  $a$ .

Now  $a$  can't be irreducible itself, so we can write  $a = bc$  where neither  $b$  nor  $c$  are  $\pm 1$ . This implies that  $|b|$  and  $|c|$  are both smaller than  $|a|$ . But this would mean both  $b$  and  $c$  factor, so that  $a$  factors as well.

**Proposition:** Every non-zero polynomial which doesn't divide 1 factors into a product of irreducible polynomials.

**Proof:** Suppose not. Then there is a polynomial which does not factor. Further, amongst all such polynomials is one of smallest degree. Call it  $a$ .

Now  $a$  can't be irreducible itself, so we can write  $a = bc$  where neither  $b$  nor  $c$  divide 1. This implies that  $b$  and  $c$  both have degree less than the degree of  $a$ . But this would mean both  $b$  and  $c$  factor, so that  $a$  factors as well.

Note that we did use a tiny result about polynomials above; namely, if a polynomial divides 1, then its degree is 0. This is pretty straightforward, since if  $ab = 1$ , then

$$\deg a + \deg b = \deg ab = \deg 1 = 0.$$

**Size Doesn't Matter**  
**(But Theorem 1.1.4 Does)**

The proofs for integers and polynomials used a “size” (absolute value or degree) which is a non-negative integer. In fact, there is a way to prove this using only the notions from Theorem 1.1.4.

Let's say we have a set of “things” which satisfy our usual axioms for addition and multiplication, the product of two non-zero “things” is never zero, and where an analogue of Theorem 1.1.4 is also true. (Remember that Theorem 1.1.4 was a consequence of the division algorithm when our “things” were integers or polynomials.)

**Generically Applicable Proof:** Suppose there are non-zero  $a$  which don't divide 1 and don't factor. Pick any such  $a_0$ . This  $a_0$  can't be irreducible itself, so write it as  $a_0 = bc$  where neither  $b$  nor  $c$  divide 1. Now  $a_0$  doesn't factor, and is the product of  $b$  and  $c$ . So at least one of  $b$  and  $c$  doesn't factor. Pick one which doesn't and call it  $a_1$ . Then  $a_0$  and  $a_1$  are both non-zero, don't divide 1, and don't factor. Further,  $a_1|a_0$  and  $a_0 \nmid a_1$ .

Now repeat the whole process, getting a non-zero  $a_2$  which doesn't divide 1 and doesn't factor into a product of irreducibles. Further,  $a_2|a_1|a_0$  and  $a_0 \nmid a_1 \nmid a_2$ .

We can continue on, getting a whole unending chain of non-zero “things”  $a_i$  which don't divide 1, don't factor,  $a_{i+1}|a_i$  and  $a_i \nmid a_{i+1}$ .

Let  $I$  be the collection of “things” of the form  $a_i \times z$  for some index  $i$  and “thing”  $z$ . We claim that this collection is an ideal. First,  $I$  is clearly not empty;  $a_0 \in I$ , for example. Next, if  $a$  and  $b$  are elements of  $I$ , then  $a = a_i z_1$  and  $b = a_j z_2$  for some indices  $i$  and  $j$  and “things”  $z_1$  and  $z_2$ . We may suppose without loss of generality that  $i \leq j$ . Then by our hypotheses (and exercise #7b from section 1.1),  $a_j|a_i$ . This implies (via exercise #7b) that  $a_j|a$ ; let's write  $a = a_j z_3$  for some “thing”  $z_3$ . Then via exercise #7c,  $a_j|a + b$ , so  $a + b$  is an element of  $I$ . Finally, if  $z$  is any “thing,” then  $az = a_i z_1 z$ , which is an element of  $I$ , too.

Since  $I$  is an ideal, it consists solely of multiples of some “thing”  $a$ . In particular  $a = a \times 1$  is in  $I$ , so must be of the form  $a_i \times z$  for some index  $i$  and “thing”  $z$ . In other words,  $a_i|a$ . But  $a_{i+1}$

is also in  $I$ , so it must be true that  $a|a_{i+1}$ . By a exercise #7b yet again, we have  $a_i|a_{i+1}$ , which contradicts our construction.

Since our construction just couldn't be, we are forced to conclude that there is no non-factorizable  $a_0$  to start the process. In other words, all non-zero "things" which don't divide 1 must factor into a product of irreducible "things."

If you find this proof uncomfortable, try replacing every instance of "thing" with "integer" or "polynomial."

It's a very difficult exercise to find an example of a collection of "things" which satisfy the axioms for addition and multiplication together with an analogue of Theorem 1.1.4 and where the product of two non-zero "things" is never zero, but *don't* have a "division algorithm." Rest assured there are such collections, though.