# UNIQUE FACTORIZATION IN Z AND $F[T]$ 

KEITH CONRAD

## 1. Introduction

We call an integer $p>1$ prime when its only positive factors are 1 and $p$. Every integer $n>1$ has two obvious positive factors: 1 and itself. Primes are the numbers greater than 1 whose only positive factors are the obvious ones. The sequence of primes starts out as

$$
2,3,5,7,11,13,17,19,23,29,31,37,41,43,47,53, \ldots
$$

Prime numbers are the building blocks of the positive integers under multiplication, as codified in the following theorem.

Theorem 1.1 (Unique Factorization in Z). Every integer $n>1$ can be written as a product of primes. Moreover, the prime factorization of $n$ is unique: if $n=p_{1} \cdots p_{r}$ and $n=q_{1} \cdots q_{s}$ where the $p_{i}$ 's and $q_{j}$ 's are prime then $r=s$ and after relabeling the factors we have $p_{i}=q_{i}$ for all $i$.

Theorem 1.1 is really two statements about each $n>1$ : (i) a prime factorization of $n$ exists and (ii) there is only one prime factorization for $n$ up to the order of multiplication of the prime factors. To prove Theorem 1.1, we will prove these two statements separately.

When we talk about a product of primes in Theorem 1.1, we allow repeated factors, e.g., 45 is $3 \cdot 3 \cdot 5$. Also we allow a "product" with a single term in it, so a prime number is a product of primes using only itself in the product. If we didn't allow this, then we'd have to say every $n>1$ is a prime or a product of primes. By allowing a product with a single term, our language becomes simpler.

Polynomials can be factored, just like integers, and for historical reasons the name for building blocks of polynomials is irreducible instead of prime: in $F[T]$, where $F$ is a field, a nonconstant polynomial $p(T)$ is called irreducible if its only factors are nonzero constants and nonzero constant multiples of itself. Every nonconstant $f(T)$ in $F[T]$ is divisible by nonzero constants and nonzero constant multiples of $f(T)$, so the irreducible polynomials are the ones whose only factors are the obvious ones. Unique factorization in $F[T]$ has a statement very similar to unique factorization in $\mathbf{Z}$ :

Theorem 1.2 (Unique Factorization in $F[T]$ ). Let $F$ be a field. Every nonconstant $f(T)$ in $F[T]$ can be written as a product of irreducibles. Moreover, the irreducible factorization of $f(T)$ is unique: if $f(T)=p_{1}(T) \cdots p_{r}(T)$ and $f(T)=q_{1}(T) \cdots q_{s}(T)$ where the $p_{i}(T)$ 's and $q_{j}(T)$ 's are irreducible then $r=s$ and after relabeling the factors we have $p_{i}(T)=c_{i} q_{i}(T)$ for all $i$, where the $c_{i}$ 's are nonzero constants.

Like Theorem 1.1, there are two statements in Theorem 1.2: for every nonconstant polynomial in $F[T]$, (i) an irreducible factorization exists and (ii) it is unique up to the order of multiplication and up to scaling by nonzero constants. Also, we adopt the convention that an irreducible polynomial is a one-term product of irreducibles.

The ambiguity in irreducible factorizations is broader than just changing the order of multiplication: we have to allow scaling of irreducible factors by nonzero constants (which doesn't change their irreducibility). To illustrate this, consider in $\mathbf{R}[T]$ the following irreducible factorizations of $T^{2}-1$ :

$$
T^{2}-1=(T+1)(T-1)=(3 T+3)\left(\frac{1}{3} T-\frac{1}{3}\right)=\left(\frac{4}{5} T-\frac{4}{5}\right)\left(\frac{5}{4} T+\frac{5}{4}\right) .
$$

The second irreducible factorization scales the two factors $T+1$ and $T-1$ by 3 and $1 / 3$, while the third irreducible factorization scales these factors by $5 / 4$ and $4 / 5$ and changes the order of multiplication.

The proofs of Theorems 1.1 and 1.2 will be similar: induct on $n$ and induct on $\operatorname{deg} f$.

## 2. Proof of Theorem 1.1

Theorem 2.1. Every $n>1$ has a prime factorization: we can write $n=p_{1} \cdots p_{r}$, where the $p_{i}$ are prime numbers.
Proof. We will use induction, but more precisely strong induction: assuming every integer between 1 and $n$ has a prime factorization we will derive that $n$ has a prime factorization.

Our base case is $n=2$. This is a prime, so it is a product of primes by our convention that a prime is a product of primes with one term.

Now assume $n>2$ and (here comes the strong inductive hypothesis) for all $m$ with $1<m<n$ that $m$ is a product of primes. To show $n$ is a product of primes, we take cases depending on whether $m$ is prime or not.

Case 1: The number $n$ is prime.
In this case, $n$ is a product of primes with just one term. (This is the easy case.)
Case 2: The number $n$ is not prime.
Since $n>1$ and $n$ is not prime, there is some nontrivial factorization $n=a b$ where $1<a<n$ and $1<b<n$. By our strong inductive hypothesis, both $a$ and $b$ are products of primes. Since $n$ is the product of $a$ and $b$, and both $a$ and $b$ are products of primes, $n$ is a product of primes by stringing together the prime factorizations of $a$ and $b$. More explicitly, writing $a=p_{1} \cdots p_{k}$ and $b=p_{1}^{\prime} \cdots p_{\ell}^{\prime}$ where $p_{i}$ and $p_{j}^{\prime}$ are all prime, we have

$$
n=a b=p_{1} \cdots p_{k} p_{1}^{\prime} \cdots p_{\ell}^{\prime}
$$

which is a product of primes.
The key to proving uniqueness of prime factorization is the following property of primes.
Lemma 2.2. If $p$ is a prime number and $p \mid$ ab for some integers $a$ and $b$, then $p \mid a$ or $p \mid b$.

Proof. We will assume $p \mid a b$ and the conclusion is false: $p$ does not divide $a$ or $p$ does not divide $b$. If $p$ does not divide $a$ then $(p, a)=1$ because $p$ is prime. A basic consequence of Bezout's identity tells us that from $p \mid a b$ and $(p, a)=1$ we have $p \mid b$.

If $p$ does not divide $b$, then by switching the roles of $a$ and $b$ (which is okay since $a b=b a$ ) we can conclude that $p \mid a$.

A generalization of Lemma 2.2 is that for each finite list of integers $a_{1}, \ldots, a_{k}$, if $p \mid$ $a_{1} \cdots a_{k}$ then $p \mid a_{i}$ for some $i$. This is trivial for $k=1$, and for $k \geq 2$ it can be proved by induction on $k$. Lemma 2.2 is the base case $k=2$, and if for $k \geq 3$ and the generalization is proved for a prime $p$ dividing products of $k$ integers, then we will prove it for $p$ dividing
products of $k+1$ integers: if $p \mid a_{1} \cdots a_{k+1}$ then rewrite this as $p \mid\left(a_{1} \cdots a_{k}\right) a_{k+1}$. Since $\left(a_{1} \cdots a_{k}\right) a_{k+1}$ is a product of two integers $a_{1} \cdots a_{k}$ and $a_{k+1}$, by Lemma 2.2 either $p \mid$ $a_{1} \cdots a_{k}$ or $p \mid a_{k+1}$. If $p \mid a_{1} \cdots a_{k}$ then $p \mid a_{i}$ for some $i$ from 1 to $k$ by the inductive hypothesis, and including the option $p \mid a_{k+1}$ with these tells us that $p \mid a_{i}$ for some $i$ from 1 to $k+1$, which completes the inductive proof.

Now we can prove prime factorization is unique.
Theorem 2.3. If $p_{1} \cdots p_{r}=q_{1} \cdots q_{s}$ where the $p_{i}$ 's and $q_{j}$ 's are prime, then $r=s$ and after relabeling the factors we have $p_{i}=q_{i}$ for all $i$.

Proof. The key mathematical step is this: when $p_{1} \cdots p_{r}=q_{1} \cdots q_{s}, p_{1}$ must equal some $q_{j}$. This is because

$$
p_{1} \cdots p_{r}=q_{1} \cdots q_{s} \Longrightarrow p_{1}\left|q_{1} \cdots q_{s} \Longrightarrow p_{1}\right| q_{j} \text { for some } j
$$

where the second implication is the generalization of Lemma 2.2 that we mentioned above. That uses primality of $p_{1}$. Since $q_{j}$ is prime and $p_{1} \mid q_{j}$, we must have $p_{1}=q_{j}$ (a prime has no factor greater than 1 other than itself).

To prove the theorem, we will induct on the total number of prime factors in the two equal prime factorizations, which is $r+s .{ }^{1}$ We allow repeated primes.

The base case is $r+s=2$ (why not $r+s=1$ ?) when the equal prime factorization turns into $p_{1}=q_{1}$. Here the conclusion of the theorem is obvious (there is no relabeling needed, since each side has one factor).

Suppose next that $r+s>2$ and the theorem is true for all pairs of equal prime factorizations for which the total number of primes being used is less than $r+s$. If we have $p_{1} \cdots p_{r}=q_{1} \cdots q_{s}$ then $r>1$ and $s>1$ : if $r=1$ or $s=1$ then one side is a prime number and therefore the other side has to be a prime number, so $r=s=1$, but $r+s>2$.

From $p_{1} \cdots p_{r}=q_{1} \cdots q_{s}$ we explained at the start of the proof that $p_{1}$ must be some $q_{j}$. By relabeling the factors on the right, which is okay since the order of multiplication doesn't matter, we can assume $p_{1}=q_{1}$. Then our equal prime factorization becomes

$$
p_{1} p_{2} \cdots p_{r}=p_{1} q_{2} \cdots q_{s} .
$$

Canceling the common factor $p_{1}$ on both sides, we get

$$
\begin{equation*}
p_{2} \cdots p_{r}=q_{2} \cdots q_{s} . \tag{2.1}
\end{equation*}
$$

In this equation of equal prime factorizations, the total number of primes appearing on both sides is $(r-1)+(s-1)=r+s-2$, which is less than $r+s$. By our inductive hypothesis we conclude $r-1=s-1$ (there are $r-1$ primes on the left and $s-1$ primes on the right), so $r=s$, and after relabeling the primes in (2.1) we have $p_{i}=q_{i}$ for all $i \geq 2$. Combining this with $p_{1}=q_{1}$ we have $p_{i}=q_{i}$ for all $i$.
Example 2.4. For a prime $p$ and integer $m \geq 1$, every factor of $p^{m}$ is $\pm p^{k}$ where $0 \leq k \leq m$. Indeed, if $d \mid p^{m}$ then each prime factor of $d$ is a factor of $p^{m}$, and by unique factorization the only prime factor of $p^{m}$ is $p$. Therefore the expression of $d$ as a product of primes up to a sign (if $d \neq \pm 1$ ) must be a product of $p$ 's, so $d= \pm p^{k}$. Since $d \leq p^{m}$ we get $p^{k} \leq p^{m}$, so $0 \leq k \leq m$.

Perhaps you think the uniqueness of prime factorization is obvious, since it is consistent with all of your prior experience. Is there really a need to give a proof at all? Here are three answers to that question.

[^0](1) There are number systems where prime factorization exists but is not unique.
(2) Even if uniqueness holds for small numbers, without a proof how do we know uniqueness can't break down for big numbers? For instance, $n=11501689$ can be written as $2747 \cdot 4187$ and $3239 \cdot 3551$. Does that violate uniqueness of prime factorization? No, because those factorizations don't use primes: $2747=41 \cdot 67$ and $4187=53 \cdot 79$, while $3239=41 \cdot 79$ and $3551=53 \cdot 67$. The prime factorization of $n$ is really $41 \cdot 53 \cdot 67 \cdot 79$.
(3) Historically, nobody saw a need to prove Theorem 1.1 until Gauss in 1801 (Article 16 in his book Disquisitiones Arithmeticae). Previously, Legendre and Euler stated the existence of prime factorization in their work, but gave no proof of its uniqueness even if they implicitly used it. In ancient Greece, Euclid's Elements has a proof that each $n>1$ has a prime factor (Prop. 31 in Book VII). It has no proof that prime factorizations exist or are unique, although it does have a proof of Example 2.4 when $d>0$ (Prop. 13 in Book IX).
We turn next to unique factorization of polynomials, and we will see that almost everything we have done for integers will carry over to the polynomial setting except that we have to keep track of scalar multiples of irreducible factors.

## 3. Proof of Theorem 1.2

To prove $F[T]$ has unique factorization, we will first prove irreducible factorizations exist for all nonconstant polynomials and then we will show they are unique (up to the order of multiplication and scaling by nonzero constants). This is similar to the strategy in $\mathbf{Z} .{ }^{2}$
Theorem 3.1. Every nonconstant polynomial in $F[T]$ has an irreducible factorization.
Proof. We will argue by strong induction on the degree of polynomials.
Our base case is degree 1. Every polynomial in $F[T]$ of degree 1 is irreducible, so they are each a product of irreducibles using just one term.

Now assume $d>1$ and every nonconstant polynomial in $F[T]$ with degree less than $d$ has an irreducible factorization. Pick a polynomial $f(T) \in F[T]$ of degree $d$. We want to show $f(T)$ has an irreducible factorization.

Case 1: The polynomial $f(T)$ is irreducible.
Here $f(T)$ is a one-term product of irreducibles.
Case 2: The polynomial $f(T)$ is irreducible prime.
There is a factorization $f(T)=g(T) h(T)$ where $0<\operatorname{deg} g<\operatorname{deg} f$ and $0<\operatorname{deg} h<\operatorname{deg} f$. By the strong inductive hypothesis, $g(T)$ and $h(T)$ each have irreducible factorizations, and putting these irreducible factorizations together gives us an irreducible factorization of $f(T)$ : if $g(T)=p_{1}(T) \cdots p_{k}(T)$ and $h(T)=\widetilde{p}_{1}(T) \cdots \widetilde{p}_{\ell}(T)$ with irreducible $p_{i}(T)$ and $\widetilde{p}_{j}(T)$ in $F[T]$, then

$$
f(T)=g(T) h(T)=p_{1}(T) \cdots p_{k}(T) \widetilde{p}_{1}(T) \cdots \widetilde{p}_{\ell}(T),
$$

which expresses $f(T)$ as a product of irreducibles in $F[T]$.
To prove the irreducible factorization in $F[T]$ is unique, we need the following analogue of Lemma 2.2.

Lemma 3.2. If $p(T)$ is irreducible in $F[T]$ and $p(T) \mid a(T) b(T)$ in $F[T]$, then $p(T) \mid a(T)$ or $p(T) \mid b(T)$.

[^1]Proof. This is proved just like Lemma 2.2. If $p(T)$ does not divide $a(T)$ then $(p(T), a(T))=$ 1 in $F[T]$ because $p(T)$ is irreducible. From Bezout's identity in $F[T]$, the conditions $p(T) \mid a(T) b(T)$ and $(p(T), a(T))=1$ imply $p(T) \mid b(T)$. Similarly, if $p(T)$ does not divide $b(T)$ then $p(T) \mid a(T)$ by swapping the roles of $a(T)$ and $b(T)$.

Lemma 3.2 generalizes by induction on the number of terms to say that if $p(T)$ is irreducible in $F[T]$ and $p(T) \mid a_{1}(T) \cdots a_{k}(T)$ then $p(T) \mid a_{i}(T)$ for some $i$. The proof is just like its analogue in $\mathbf{Z}$ that we discussed earlier. With this generalization we can prove the uniqueness of irreducible factorizations in $F[T]$.
Theorem 3.3. If $p_{1}(T) \cdots p_{r}(T)=q_{1}(T) \cdots q_{s}(T)$ where the $p_{i}(T)$ 's and $q_{j}(T)$ 's are irreducible, then $r=s$ and after relabeling the factors we have $p_{i}(T)=c_{i} q_{i}(T)$ for all $i$ where the $c_{i}$ are nonzero in $F$.

Proof. As in the proof Theorem 2.3, the key step is that if $p_{1}(T) \cdots p_{r}(T)=q_{1}(T) \cdots q_{s}(T)$ then $p_{1}(T)=c_{j} q_{j}(T)$ for some $j$ and nonzero $c_{j}$ in $F$. This follows from

$$
p_{1}(T) \cdots p_{r}(T)=q_{1}(T) \cdots q_{s}(T) \Longrightarrow p_{1}(T)\left|q_{1}(T) \cdots q_{s}(T) \Longrightarrow p_{1}(T)\right| q_{j}(T) \text { for some } j .
$$

By relabeling, we can take $j=1$, i.e., $p_{1}(T) \mid q_{1}(T)$. That implies $p_{1}(T)$ is a constant multiple of $q_{1}(T)$ since the only nonconstant factors of an irreducible polynomial in $F[T]$ are constant multiples of itself. (This is different from prime numbers, where the only positive factor is the number itself!) Therefore $p_{1}(T)=c_{1} q_{1}(T)$ for some constant $c_{1}$.

Our theorem will be proved by induction on the total number of irreducible factors in the equal irreducible factorizations, which is $r+s$. The base case is $r+s=2$, when the equation is $p_{1}(T)=q_{1}(T)$, and this case is obvious.

Now suppose $r+s>2$ and the theorem is true for all pairs of equal irreducible factorizations for which the total number of irreducibles is less than $r+s$. If $p_{1}(T) \cdots p_{r}(T)=$ $q_{1}(T) \cdots q_{s}(T)$ then $r>1$ and $s>1$ by the same proof as in the integer case. By relabeling the factors we have assume $p_{1}(T)=c_{1} q_{1}(T)$, so

$$
p_{1}(T) p_{2}(T) \cdots p_{r}(T)=\frac{1}{c_{1}} p_{1}(T) q_{2}(T) \cdots q_{s}(T) .
$$

Canceling $p_{1}(T)$ from both sides,

$$
\begin{equation*}
p_{2}(T) \cdots p_{r}(T)=\frac{1}{c_{1}} q_{2}(T) \cdots q_{s}(T) . \tag{3.1}
\end{equation*}
$$

We need to be careful here: the factor $1 / c_{1}$ on the right is not irreducible. It's just a constant. We can attach it to $q_{2}(T)$ : the polynomial $\left(1 / c_{1}\right) q_{2}(T)$ is irreducible. Therefore the left side of (3.1) has $r-1$ irreducible factors and the right side has $s-1$ irreducible factors (namely $\left.\left(1 / c_{1}\right) q_{2}(T), q_{3}(T), \ldots, q_{s}(T)\right)$. From $(r-1)+(s-1)=r+s-2<r+s$, by the inductive hypothesis $r-1=s-1$, so $r=s$. Also by the inductive hypothesis, after relabeling the factors we have $p_{2}(T)=c\left(1 / c_{1}\right) q_{2}(T)$ and $p_{i}(T)=c_{i} q_{i}(T)$ for all $i \geq 3$, where $c, c_{3}, \ldots$ are all nonzero constants. Set $c_{2}=c / c_{1}$, and then along with $p_{1}(T)=c_{1} q_{1}(T)$ we have shown each $p_{i}(T)$ is a constant multiple of $q_{i}(T)$ and our proof is complete.

Other than some extra bookkeeping to account for constant multiples, the proof of unique factorization in $F[T]$ is basically the same as the proof of unique factorization in $\mathbf{Z}$.
Example 3.4. If $p(T)$ is irreducible in $F[T]$ and $m \geq 1$ then every factor of $p(T)^{m}$ in $F[T]$ is $c p(T)^{k}$ where $c$ is nonzero in $F$ and $0 \leq k \leq m$. The proof is along the same lines as in Example 2.4. Details are left to the reader.


[^0]:    ${ }^{1}$ Another possibility is to induct on $\max (r, s)$ with very similar steps to the proof we give.

[^1]:    ${ }^{2}$ The page https://mathoverflow.net/questions/15137 discusses the history of unique factorization in polynomials.

