

Prime Factorization in Principal Ideal Domains

We are all familiar with the prime factorization theorem for the ring \mathbb{Z} of integers. Every natural number is a unique product of prime numbers. Of course this also holds for integers different from zero. Uniqueness is meant "up to a permutation of the factors" and up to sign. That every number is a product of prime numbers is easily established: If n is not already a prime then it is the product of two smaller numbers, that is, $n = a \cdot b$, where both numbers a and b are smaller than n . We can repeat the argument for a and b and get a factorization into still smaller factors. Of course, this procedure must come to a halt which ends with a factorization of n into prime numbers. We also could argue inductively that a and b are both products of primes because they are smaller than n . At any rate, the existence of a prime factorization for any number n is pretty obvious and taught at elementary school.

A similar argument applies to polynomials with real or complex coefficients. Here the prime polynomials are those polynomials of positive degree which are not products of polynomials of smaller degrees. Linear polynomials $p(x) = x - a$ are prime. For the polynomial ring $\mathbb{C}[x]$ these are the only ones. For the ring $\mathbb{R}[x]$ of polynomials with real coefficients, the prime polynomials are all linear polynomials but also certain quadratic polynomials, namely $p(x) = x^2 - 2ax + (a^2 + b^2)$ where $b \neq 0$. These quadratic polynomials have the two conjugate complex roots $x_1 = a + bi$ and $x_2 = a - bi$.

Uniqueness of the prime factorization is more difficult to prove. In order to get a clue, let us assume that the natural number n admits two prime factorizations:

$$n = p_1 \cdot p_2 \cdot \cdots \cdot p_k = q_1 \cdot q_2 \cdot \cdots \cdot q_l$$

We wish to prove that $k = l$ and that up to a permutation, $p_i = q_i$. This would be accomplished in case that we can prove that if a prime p divides a product $a \cdot b$ then it must divide one of the factors. Assume that primes have this *Euclidean* property. Then because p_1 divides $q_1 \cdot (q_2 \cdot \cdots \cdot q_l)$ it must be the case that either p_1 divides q_1 or p_1 divides $(q_2 \cdot \cdots \cdot q_l)$. In case that p_1 divides q_1 we must have that $p_1 = q_1$ because the prime number q_1 is divisible only by 1 or itself. Now, if p_1 divides $(q_2 \cdot \cdots \cdot q_l) = q_2 \cdot (q_3 \cdot \cdots \cdot q_l)$ then p_1 divides q_2 or p_1 divides $(q_3 \cdot \cdots \cdot q_l)$. Thus p_1 is either p_2 or p_1 divides $(q_3 \cdot \cdots \cdot q_l)$. It is clear that we can show that p_1 must be equal to one of the q_j . We can permute the order of the q_j to have that $p_1 = q_1$. We cancel on both sides p_1 and get $p_2 \cdot \cdots \cdot p_k = q_2 \cdot \cdots \cdot q_l$. By the same reasoning as before, we arrive at $p_2 = q_2$. We then cancel on both sides p_2 . This tells us that the right hand side must have at least l -many factors. That is $k \leq l$. But by symmetry then $l \leq k$. Hence $k = l$, and $p_i = q_i$ after a permutation of the factors.

We see that the existence of a prime factorization is guaranteed because in a proper factorization of a number (or a polynomial), factors are smaller, or of lower degree. If primes have the Euclidean property that if they divide a product then they must divide one of the factors, then all prime factorizations are essentially (that is up to permutations of the factors) the same.

In a ring, like \mathbb{Z} or $D = \mathbb{R}[x]$ the prime factorization theorem is actually a fact about the multiplicative structure of the ring. Both rings are commutative and have no zero divisors. That is, if $ab = ac$ and if $a \neq 0$ then $b = c$. Such rings are called *domains*. In a

domain with $1 \neq 0$ the elements different from zero form a commutative, cancellation semigroup with unit.

Definition $\mathbf{H} = (H, \cdot, 1)$ is a commutative cancellation semigroup with unit 1 if

1. $(ab)c = a(bc), ab = ba, a1 = a$
2. $ab = ac$ only if $b = c$

In the following, \mathbf{H} denotes such a semigroup. We then define

Definition a divides b in case that there is some c such that $ac = b$. If this is the case then we write $a|b$.

Exercise Prove the following rules:

1. $a|a; 1|a$.
2. If $a|b$ and $b|c$ then $a|c$.
3. The binary relation \sim on H which holds between elements a and b if they mutually divide each other, is an equivalence relation. That is $a \sim b$ iff $(a|b$ and $b|a)$ is reflexive, transitive and symmetric.

Let U be the group of invertible elements in H . Then:

4. For the equivalence class $[a] = \{b|a \sim b\}$ we have that $[a] = aU = \{au|u \text{ is invertible}\}$. That is, if $a|b$ and $b|a$, then $b = au$ where u is an invertible element.

The elements of $[a]$ are called the associates of a . These and the invertible elements are the *trivial* divisors of a .

Definition An element q in H is called **irreducible** if it has only trivial divisors.

Definition An element p in H is called **prime** in case that whenever $p|ab$ then one has that $p|a$ or $p|b$.

Remark The idea of an irreducible object is that it is not divisible into smaller parts. To say that an object is prime means, that if it is contained in a complex object, then it must fit completely into one of its parts. Both concepts capture the idea of an atom.

Exercise A prime p in H is always irreducible.

Exercise $H = \{4n + 1|n \in \mathbb{N}\}$ is closed under multiplication and therefore a commutative, cancellation semigroup with unit. Prove that every element of H is a product of irreducible elements but the factorization is not always unique. Find irreducible elements that are not prime.

Theorem Assume that in H the divisor chain condition holds. That is, there is no infinite chain $a_1Ra_2Ra_3\dots$ where aRb stands for " b is a proper divisor of a ." Then every element is a product of irreducible elements. In case that irreducible elements are prime, any such factorization is essentially unique. That is, if

$$a = p_1 \cdot p_2 \cdot \dots \cdot p_k = q_1 \cdot q_2 \cdot \dots \cdot q_l$$

then $k = l$ and after a permutation one has that $p_i \sim q_i$.

Definition A commutative ring with unit $1 \neq 0$ is called a domain D if $ab = ac$ implies

that $b = c$. This is equivalent to $ab = 0$ only if $a = 0$ or $b = 0$.

Definition A domain D where every ideal is principal is called a principal ideal domain (PID).

Example \mathbb{Z} is a PID. For any field F , the polynomial ring $F[x]$ is a PID.

Exercise For a domain D , one has that $H = (D \setminus \{0\}, \cdot)$ is a commutative cancellation semigroup with unit. We have that $a|b$ if and only if $(a) \supseteq (b)$ with proper inclusion in case that a is a proper divisor.

Theorem Let D be a PID. Then every infinite chain of ideals $I_1 \subseteq I_2 \subseteq I_3 \subseteq \dots$ terminates. That is, there is some n such that $I_n = I_{n+1} = \dots$.

Proof Take the union $I = \bigcup I_n$ of these ideals. Then $I = (a)$ where a belongs to some of the ideals, say $a \in I_n$. Then for all $j \geq n$ one has that $I_j = I_n = I$.

Corollary In a PID, every element $a \neq 0$ is a product of irreducible elements.

For elements a and b in any commutative ring R , the smallest ideal that contains these elements is called the sum of $(a) + (b)$.

Exercise $(a) + (b) = \{xa + yb | x, y \in R\}$

Definition d is the greatest common divisor of elements a and b in a domain D if

1. $d|a$ and $d|b$.
2. If $e|a$ and $e|b$ then $e|d$.

Notation: $\gcd(a, b)$.

Exercise For a PID one has that $(a, b) = (d)$ where d is the greatest common divisor of a and b .

Definition a and b are relatively prime in D if 1 (or any unit) is the $\gcd(a, b)$. That is $1 = xa + yb$ for suitable elements x and y .

Theorem In a PID one has that irreducibles are prime.

Proof Assume that p is an irreducible element of D and that $p|ab$. Assume that p does not divide a . We wish to show that p divides b . Now, because p does not divide a , and because p has only trivial divisors, it must be the case that p and a are relatively prime. That is, $1 = xp + ya$. But then $b = xpb + yab$. The element p divides xpb and yab , so it divides the sum b .

Corollary In a PID, every element a admits an essentially unique factorization into irreducible elements.

Exercise The ring of Gaussian integers $\mathbb{Z}[i] = \{m + ni | a, b \in \mathbb{Z}\}$ is a PID. We obviously have that $\mathbb{Z} \subset \mathbb{Z}[i]$. Find primes in \mathbb{Z} which are no longer primes in $\mathbb{Z}[i]$. Prove that if m and n are relatively prime in \mathbb{Z} they remain relatively prime in $\mathbb{Z}[i]$.