The prime factor module

Liam Williams

January 3, 2017

1 Prerequisites

Theorem 1 (Fundamental theorem of arithmetic [1]) *Every positive integer greater than one can be represented in exactly one way apart from rearrangement as a product of one or more primes.*

Example 1 $30 = 2 \times 3 \times 5$

Corollary 1 *Every positive rational number greater than one can be represented in exactly one way apart from rearrangement as a ratio of the product of one or more primes.*

Example 2 $\frac{100}{15} = \frac{2^2 5^2}{3^1 5^1} = 2^2 3^{-1} 5^1$.

Corollary 2 *Every positive rational greater than one can be expressed as an infinite product of prime powers:*

$$n = \prod_{p_i \text{ prime}} p_i^{\alpha_i} \text{ for some } \alpha_i \in \mathbb{Z}.$$

Definition 1 (Module [3]) The module V over a commutative ring R is a set that is closed under finite vector addition and scalar multiplication.

The following conditions must hold for all elements $\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{Z} \in V$ and any scalars $r, s \in R$:

1. Commutativity:
$$\boldsymbol{X} + \boldsymbol{Y} = \boldsymbol{Y} + \boldsymbol{X}$$

2. Associativity of vector addition:
$$(\boldsymbol{X} + \boldsymbol{Y}) + \boldsymbol{Z} = \boldsymbol{X} + (\boldsymbol{Y} + \boldsymbol{Z})$$

3. Additive identity: For all $\boldsymbol{X}$,
$$\boldsymbol{0} + \boldsymbol{X} = \boldsymbol{X} + \boldsymbol{0} = \boldsymbol{X}$$

4. Additive inverse: For any $\boldsymbol{X}$, there exists a $-\boldsymbol{X}$ such that
$$\boldsymbol{X} + (-\boldsymbol{X}) = \boldsymbol{0}$$

5. Associativity of scalar multiplication:
$$r(s\boldsymbol{X}) = (rs)\boldsymbol{X}$$

6. Distributivity of scalar sums:
$$(r + s)\boldsymbol{X} = r\boldsymbol{X} + s\boldsymbol{X}$$

7. Distributivity of vector sums:
$$r(\boldsymbol{X} + \boldsymbol{Y}) = r\boldsymbol{X} + r\boldsymbol{Y}$$

8. Scalar multiplication identity:
$$1\boldsymbol{X} = \boldsymbol{X}$$

Example 3 The integers $\mathbb{Z}$ is an example of a commutative ring.

2 The prime factor module

The fundamental theorem of arithmetic (Theorem 1) told us that every positive rational number can be expressed as an infinite product of prime powers (Corollary 2).

If we think of each prime as a separate dimension, there is a module that arises which encodes sequences of integers into a single positive rational.

Definition 2 Let V be the set of sequences of integers that represent the unique prime factor decomposition of the positive rational numbers $\mathbb{Q}$.

Example 4 The sequence $(1, -2, 3, 0, 2)$ represents the fraction $\frac{2^1 3^0 5^3 7^0 11^2}{2^0 3^2 5^0 7^0 11^0} = \frac{30250}{9}$.

Theorem 2 *There is a bijection from $\mathbb{Q}$ to V (Definition 2)*

PROOF We will construct a bijection $f : \mathbb{Q} \to V$.

Using Corollary 2:

$$q \in \mathbb{Q} = \prod_{p_i \text{ prime}} p_i^{q_i} \text{ for some } q_i \in \mathbb{Z}$$

Which we can encode as:

$$f(q) = (q_1, q_2, q_3, \cdots)$$

This is injective, since:

$$f(a) = f(b) \iff (a_1, a_2, a_3, \cdots) = (b_1, b_2, b_3, \cdots) \iff \prod_{p_i \text{ prime}} p_i^{a_i} = \prod_{p_i \text{ prime}} p_i^{b_i} \Rightarrow a = b$$

It is surjective, since:

$$v \in V = (v_1, v_2, v_3, \cdots) = f\left(\prod_{p_i \text{ prime}} p_i^{v_i}\right)$$

□

Theorem 3 *The set V (Definition 2) over the ring $\mathbb{Z}$ is a module.*

PROOF We will define $\mathbf{0}$, 1, $+$, $\times$ and then show that these form a module of V over $\mathbb{Z}$.

The zero element $\mathbf{0} \in V = 1 \in \mathbb{Q}$.

The scalar identity element is $1 \in \mathbb{Z}$.

Let any $\boldsymbol{X}, \boldsymbol{Y}, \boldsymbol{Z} \in V$ represent the decomposition of $x, y, z > 0 \in \mathbb{Q}$ and $r, s \in F$ be any scalars.

Addition is defined as:

$$\boldsymbol{X} + \boldsymbol{Y} = xy$$

Multiplication by a scalar is defined as:

$$r\boldsymbol{X} = x^r$$

The module conditions hold:

1. Commutativity:
$$\boldsymbol{X} + \boldsymbol{Y} = xy = yx = \boldsymbol{Y} + \boldsymbol{X}$$

2. Associativity of vector addition:
$$(\boldsymbol{X} + \boldsymbol{Y}) + \boldsymbol{Z} = (xy)z = x(yz) = \boldsymbol{X} + (\boldsymbol{Y} + \boldsymbol{Z})$$

3. Additive identity: For all $\boldsymbol{X}$,
$$\boldsymbol{0} + \boldsymbol{X} = 1x = x1 = x = \boldsymbol{X} + \boldsymbol{0} = \boldsymbol{X}$$

4. Additive inverse: For any $\boldsymbol{X}$, there exists a $-\boldsymbol{X} = \frac{1}{x}$ such that
$$\boldsymbol{X} + (-\boldsymbol{X}) = \frac{x}{x} = 1 = \boldsymbol{0}$$

5. Associativity of scalar multiplication:
$$r(s\boldsymbol{X}) = (x^s)^r = x^{(sr)} = (rs)\boldsymbol{X}$$

6. Distributivity of scalar sums:
$$(r + s)\boldsymbol{X} = x^{(r+s)} = x^r + x^s = r\boldsymbol{X} + s\boldsymbol{X}$$

7. Distributivity of vector sums:
$$r(\boldsymbol{X} + \boldsymbol{Y}) = (xy)^r = x^r y^r = r\boldsymbol{X} + r\boldsymbol{Y}$$

8. Scalar multiplication identity:
$$1\boldsymbol{X} = x^1 = x = \boldsymbol{X}$$

□

References

[1] G. H. Hardy and E. M. Wright. *An Introduction to the Theory of Numbers*. Fifth. Oxford University Press, 1979, pp. 2–3.

[2] Luke Palmer. *Prime basis is a vector space*. Nov. 15, 2004. URL: `https://lukepalmer.wordpress.com/2004/11/15/prime-basis-is-a-vector-field/` (visited on 12/2016).

[3] Eric W. Weisstein. *"Module", From MathWorld – A Wolfram Web Resource*. URL: `http://mathworld.wolfram.com/VectorSpace.html` (visited on 01/2017).