CHAPTER VIII

ALGEBRAIC PROPERTIES OF THE INTEGERS

We have identified a musical interval \( I \) with a positive real number \( x \in \mathbb{R}^+ \). Since \( \mathbb{Z}^+ \subset \mathbb{R}^+ \), each positive integer gives an interval. For example, we have seen that the integer 2 represents the octave, and that the integer 3 is an interval about 2 cents greater than the keyboard’s octave-and-a-fifth (1900 cents), as shown by the calculation \( 1200 \log_2 3 \approx 1901.96 \).

We will now investigate some properties of the integers \( \mathbb{Z} \) which relate to musical phenomena.

**Ring.** A non-empty set \( R \) endowed with two associative laws of composition + and \( \cdot \) is called a *ring* if \((R, +)\) is a commutative group, \((R, \cdot)\) is a monoid, and for any \( a, b, c \in R \) we have \( a \cdot (b + c) = a \cdot b + a \cdot c \) and \((b + c) \cdot a = b \cdot a + c \cdot a \) (The latter property is called distributivity.). We call the + operation *addition* and the \( \cdot \) operation *multiplication*, and we often denote the latter by dropping the \( \cdot \) and simply writing \( ab \) for \( a \cdot b \). We write 0 and 1 for the additive and multiplicative identity elements, respectively. We say the ring \( R \) is *commutative* if the monoid \((R, \cdot)\) is commutative. (We have already insisted that \((R, +)\) is commutative.) We will be dealing only with commutative rings here, so henceforth when we say “ring” we will mean “commutative ring”.

Two properties that we would expect to hold for any \( x \) in a ring \( R \) are these: \( \ (-1) \cdot x = -x \) and \( 0 \cdot x = 0 \). We leave it as an exercise that these properties can indeed be deduced from our assumptions.

**Units.** We have assumed that \((R, \cdot)\) is a monoid; it will not be a group in general\(^1\) since 0 has no multiplicative inverse. However, some elements of \( R \) (1, for example) will have multiplicative inverses. If \( x \in R \) is such an element, we call \( x \) a *unit*, and we denote its multiplicative inverse\(^2\) is by \( x^{-1} \). The set of units in \( R \), sometimes denoted \( R^* \), form a

---

\(^1\)The only situation when \((R, \cdot)\) is a group is when \( R = \{0\} \), which coincides with the case 0 = 1. In this case \( R \) is called the *trivial ring*.

\(^2\)The multiplicative inverse \( x^{-1} \) is unique to \( x \). The proof of this mimics the proof that inverses in a group are unique.
group with respect to multiplication.

Cancellation. A ring $R$ is called an integral domain if whenever $a, b \in R$ with $ab = 0$, then $a = 0$ or $b = 0$.

Proposition (cancellation). If $R$ is an integral domain, and $a, b, c \in R$ with $a \neq 0$ and $ab = ac$, then $b = c$.

Proof. We have $0 = ab - ac = a(b - c)$. Since $a \neq 0$ and $R$ is an integral domain, we must have $b - c = 0$, i.e., $b = c$.

Examples. The reader should verify the details in the following four examples.

(1) Integers. The set of integers $\mathbb{Z}$, taking $+$ and $\cdot$ to be the usual addition and multiplication, is the most basic example of a ring. It is commutative, and it is an integral domain. The group of units is $\mathbb{Z}^* = \{1, -1\}$.

(2) Real Numbers. The set $\mathbb{R}$ also becomes a ring under the usual $+$ and $\cdot$. It is also an integral domain. Here we have $\mathbb{R}^* = \mathbb{R} - \{0\}$.

(3) Rational Numbers. $\mathbb{Q}$ is an integral domain, sharing with $\mathbb{R}$ the property that all non-zero elements are units.

(4) Modular Integers. For $m \in \mathbb{Z}^+$, we give $\mathbb{Z}_m$ a ring structure as follows: The additive group $(\mathbb{Z}_m, +)$ is as before. For $[k], [\ell] \in \mathbb{Z}_m$, define $[k] \cdot [\ell] = [k\ell]$. The proofs that this is well defined and that the axioms for a ring are satisfied by $+$ and $\cdot$ are left as an exercise. Note that $[0]$ and $[1]$ are the additive and multiplicative identity elements, respectively, of $\mathbb{Z}_m$.

Ideals. A subset $J \subseteq R$ is called an ideal if it is a subgroup of the additive group $(R, +)$ and if whenever $a \in R$ and $d \in J$, then $ad \in J$.

One example of an ideal in $R$ is the zero ideal $\{0\}$. Any other ideal will be called a non-zero ideal. The ring $R$ itself is an ideal.

Given $a \in R$ we can form the set of all multiples of $a$ in $R$, namely the set

$$aR = \{x \in R \mid x = ab \text{ for some } b \in R\}.$$ 

Such an ideal is called a principal ideal, and the element $a$ is called a generator for the ideal. Note that $\{0\}$ and $R$ are principle ideals by virtue of $\{0\} = 0R$ and $R = 1R$.

If $R$ is an integral domain in which every ideal is principal, we call $R$ a principal ideal domain, abbreviated PID.

For example, the set of even integers forms an ideal in $\mathbb{Z}$. This ideal is a principal ideal, since it is equal to $2\mathbb{Z}$. We will now show that:

Theorem. $\mathbb{Z}$ is a principal ideal domain.

Proof. This is based on the Euclidean algorithm. Let $J$ be an ideal in $\mathbb{Z}$. If $J = \{0\}$, then $J = 0\mathbb{Z}$ and we are done. Otherwise $J$ contains non-zero integers, and since $n \in J$
implies \((-1)n = -n\) is in \(J\), then \(J\) must contain some positive integers. Let \(n\) be the smallest positive integer in \(J\) (such an \(n\) exists by the well ordering principle). We claim that \(J = n\mathbb{Z}\). Clearly \(n\mathbb{Z} \subseteq J\). To see the other containment, let \(m \in J\), and use the Euclidean algorithm to write \(m = qn + r\) with \(0 \leq r < n\). Then \(r\) is in \(J\) since \(r = m - qn\). By the minimality of \(n\), we conclude \(r = 0\), hence \(n = qn \in b\mathbb{Z}\) as desired.

If \(J \subseteq \mathbb{Z}\) is an ideal with \(J \neq 0\), and if \(n\) is a generator for \(J\), then the only other generator for \(J\) is \(-n\). This follows easily from the fact that any two generators are multiples of each other, and will be left as an exercise. Thus any non-zero ideal has a unique positive generator.

**Greatest Common Divisor.** Given \(m, n \in \mathbb{Z}\), We note that the subset \(m\mathbb{Z} + n\mathbb{Z}\), by which we mean the set of all integers \(a\) which can be written \(a = hm + kn\) for some \(h, k \in \mathbb{Z}\), is an ideal in \(\mathbb{Z}\). Therefore it has a unique positive generator \(d\), which divides both \(m\) and \(n\). If \(e\) is any other positive integer which divided both \(m\) and \(n\) then \(m, n \in e\mathbb{Z}\) so \(m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z} \subseteq e\mathbb{Z}\), and hence \(e\) divides \(d\). Therefore \(d \geq e\) and we (appropriately) call \(d\) the greatest common divisor of \(m\) and \(n\). The greatest common divisor is denoted \(\gcd(m, n)\). Since \(d\mathbb{Z} = m\mathbb{Z} + n\mathbb{Z}\), there exist integers \(h, k\) such that \(d = hm + kn\).

To say that \(\gcd(m, n) = 1\) is to say that the only common divisors of \(m\) and \(n\) in \(\mathbb{Z}\) are \(\pm 1\). In this case we say that \(m\) and \(n\) are relatively prime.

**Prime Numbers.** A positive integer \(p\) is called prime if it is divisible in \(\mathbb{Z}\) by precisely two positive integers, namely 1 and \(p\). (Note that 1 is not prime by virtue of the word “precisely”.) The first ten prime numbers are:

\[(1) \quad 2, 3, 5, 7, 11, 13, 17, 19, 23, 29\]

It will be left as an exercise to show that if \(p\) is prime and \(n \in \mathbb{Z}\), then either \(p\) divides \(n\) or \(\gcd(p, n) = 1\).

**Sieve of Eratosthenes.** A systematic procedure for finding the prime numbers was given by the Greek astronomer/mathematician Eratosthenes of Cyrene (3rd century BC). We conceive of the positive integers as an infinite list \(1, 2, 3, 4, 5, 6, \ldots\), then proceed to cross out certain numbers on the list, as follows. After crossing out 1, we cross out all numbers following 2 which are divisible by 2.

\[
\pm 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, \\
\quad 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, \ldots
\]

Then we find the next number after 2 which is still on the list, which is 3. We then cross out all numbers following 3 which are not divisible by 3.

\[
\pm 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, \\
\quad 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, \ldots
\]
When this process can be continued up to an integer \( n \), the the numbers below \( n \) which remain on the list are precisely the primes which are \( \leq n \).

\[ 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25, 26, 27, 28, 29, 30, \ldots \]

We have shown that the primes \( \leq 30 \) are the ten integers in the list (1) above.

If the procedure were continued infinitely to completion, the complete list of primes would remain.

**Theorem.** If \( p \) is a prime number and if \( p \) divides \( mn \), where \( m, n \in \mathbb{Z} \), then \( p \) divides \( m \) or \( p \) divides \( n \).

**Proof.** Suppose \( p \) does not divide \( m \). Then \( \gcd(m, p) = 1 \) and we can write \( 1 = hm + kp \) for some integers \( h \) and \( k \). Multiplying this equation by \( n \) gives \( n = hmn + knp \). Note that \( p \) divides both summands on the right, since \( p \) divides \( nm \). Therefore \( p \) divides \( n \). This concludes the proof.

One can easily conclude that if a prime number \( p \) divides a product \( m_1m_2 \ldots m_s \), then \( p \) divides at least one of \( m_1, m_2, \ldots, m_s \).

**Unique Factorization.** We now establish the fact that every positive integer can be factored uniquely as the product of primes.

**Theorem.** Let \( n \geq 1 \) be an integer. Then \( n \) can be factored as

\[ n = p_1^{a_1}p_2^{a_2} \cdots p_r^{a_r} \]

where \( r \geq 0, p_1, p_2 \ldots, p_r \) are distinct primes, and \( a_1, a_2, \ldots, a_r \geq 1 \). Moreover, this factorization is unique, meaning that if \( n = q_1^{\beta_1}q_2^{\beta_2} \cdots q_t^{\beta_t} \) is another such factorization, then \( t = r \) and after rearranging we have \( p_1 = q_1, p_2 = q_2, \ldots, p_r = q_r \).

**Proof.** We first establish the existence of a prime factorization for all integers \( \geq 1 \). If not all positive integers admit a prime factorization, then by the Well-Ordering Principle we can choose a smallest integer \( n \) which fails to admit a factorization. We note that \( n \) itself could not be prime, otherwise it admits the factorization in the theorem with \( r = 1 \) and \( p_1 = n \). Since \( n \) is not prime, it has a positive divisor \( m \) which is neither \( n \) nor 1. We have \( n = ml \) and clearly \( l \) is neither \( n \) nor 1. We must have \( 1 < m, l < n \), so by the minimality of \( n \), both \( m \) and \( l \) have prime factorizations. But if \( m \) and \( l \) have prime factorizations, then so does \( n \) since \( n = ml \). This is a contradiction. Hence all integers \( \geq 1 \) have a prime factorization.

It remains to show the uniqueness. If \( p_1^{a_1}p_2^{a_2} \cdots p_r^{a_r} = q_1^{\beta_1}q_2^{\beta_2} \cdots q_t^{\beta_t} \), then \( p_1 \) divides \( q_1^{\beta_1}q_2^{\beta_2} \cdots q_t^{\beta_t} \). Since \( p_1 \) is prime it must divide one of \( q_1, q_2, \ldots, q_t \). Say \( p_1 \) divides \( q_1 \). Since \( q_1 \) is also prime we must have \( p_1 = q_1 \), so we can cancel to get \( p_1^{a_1-1}p_2^{a_2} \cdots p_r^{a_r} = q_1^{\beta_1}q_2^{\beta_2} \cdots q_t^{\beta_t} \). We continue cancelling \( p_1 \) to deduce that \( a_1 = \beta_1 \). The remaining equation is \( p_2^{a_2} \cdots p_r^{a_r} = q_2^{\beta_2} \cdots q_t^{\beta_t} \). As above we can argue that \( p_2 = q_2 \) (after rearranging) and that \( a_2 = \beta_2 \). We continue to get the desired result.
Modular Integers. The algebraic properties we have established for \(\mathbb{Z}\) tell us many things about the rings of modular integers \(\mathbb{Z}_m\), for \(m \in \mathbb{Z}^+\). One such fact concerns the matter of when an element \([n] \in \mathbb{Z}_m\) is a generator of the additive group \((\mathbb{Z}_m, +)\).

**Theorem.** Given \([n] \in \mathbb{Z}_m\), the following three conditions are equivalent.

1. \(\gcd(m, n) = 1\).
2. \([n]\) is a generator of the additive group \((\mathbb{Z}_m, +)\).
3. \([n]\) is a unit in the ring \(\mathbb{Z}_m\) (i.e., \([n] \in \mathbb{Z}_m^*\)).

**Proof.** We first consider conditions (2) and (3). If \([n]\) is a generator of \((\mathbb{Z}_m, +)\), then all elements of \(\mathbb{Z}_m\) can be written as \(k \cdot [n]\), for some \(k \in \mathbb{Z}\). (This is the way we write exponentiation in an additive group.) In particular, we have \([1] = k \cdot [n]\). But, by the definition of multiplication in \(\mathbb{Z}_m\), \(k \cdot [n] = [k] \cdot [n]\). Therefore \([k] \cdot [n] = [1]\), which shows \([n]\) is a unit. Conversely, if \([n] \in \mathbb{Z}_m^*,\) with inverse \([k] = [n]^{-1}\), then for any \([\ell] \in \mathbb{Z}_m\) we have \([\ell] = [\ell] \cdot [1] = [\ell] \cdot [k] \cdot [n] = [\ell k] \cdot [n] = \ell k \cdot [n]\), which shows that \([\ell]\) is a multiple ("power") of \([n]\). Hence \([n]\) is a group generator for \((\mathbb{Z}_m, +)\).

The equivalence of (1) with these conditions, the proof of which uses greatest common divisors, is left as an exercise.

**Euler Phi Function.** For any \(m \in \mathbb{Z}^+\), we have defined the *Euler phi function* \(\phi(m)\) to be the number of positive integers \(n\) with \(1 \leq n < m\) which are relatively prime to \(m\). According to the above theorem, \(\phi(m)\) also counts the number of elements in \(\mathbb{Z}_m^*\), and the number of group generators for \((\mathbb{Z}_m, +)\). By virtue of the latter, \(\phi(m)\) counts the number of generating intervals in the \(m\)-chromatic scale.

For example \(\phi(12) = 4\), since the numbers 1, 5, 7, 11 are precisely the positive integers \(\leq 12\) which are relatively prime to 12. This reflects the fact that the generating intervals in the 12-chromatic scale are the semitone, the fourth, the fifth, and the major seventh.

**Exercises**

1. Prove that in any (commutative) ring \(R\) we have \((-1) \cdot x = -x\) and \(0 \cdot x = 0\), for any \(x \in R\).

2. Give the prime factorizations of these integers, writing the primes in ascending order, as in \(2^3 \cdot 3 \cdot 7^2\).

(a) 110  
(b) 792  
(c) 343  
(d) 3422  
(e) \(15 \times 10^{23}\)

3. Call a musical interval a *prime interval* if its interval ratio is a prime integer; call it a *rational interval* if its interval ratio is a rational number. Show that all rational intervals can be written as compositions of prime intervals and their opposites.

4. Express each of these ideals in \(\mathbb{Z}\) in the form \(n\mathbb{Z}\), where \(n\) is a positive integer:

(a) \(12\mathbb{Z} + 15\mathbb{Z}\)  
(b) \(5\mathbb{Z} + (-20)\mathbb{Z}\)

(c) \(10\mathbb{Z} + 44\mathbb{Z}\)  
(d) \(13\mathbb{Z} + 35\mathbb{Z}\)
(5) Verify that \( \mathbb{Q} \) (the rational numbers) is a ring, and, in fact, an integral domain. Show that the only ideals in \( \mathbb{Q} \) are \{0\} and \( \mathbb{Q} \).

(6) Prove that there are infinitely many prime numbers. (Hint: If \( p_1, \ldots, p_n \) were a complete list of primes, consider a prime factor of \( p_1 \cdots p_n + 1 \).)

(7) Prove that if \( p \) is prime and \( n \in \mathbb{Z} \), then either \( p \mid n \) or \( \gcd(p, n) = 1 \).

(8) Given \( m \in \mathbb{Z}^+ \) and \( n \in \mathbb{Z} \), prove that \([n]\) is a generator for \( \mathbb{Z}_m \) if and only if \( \gcd(m, n) = 1 \). Interpret this as a statement about generating intervals in the modular \( m \)-chromatic scale.

(9) Prove that \( m \) iterations of any \( m \)-chromatic interval is a multioctave. Interpret this as a statement about an element \([k]\) of \( \mathbb{Z}_m \), and use this statement to prove that the order \( r \) of \([k]\) divides \( m \).