ABSTRACT ALGEBRA

STEVEN DALE CUTKOSKY

1. Groups and Rings

Suppose that $S$ is a set. A law of composition on $S$ is a map $\mu : S \times S \to S$. We will often write $\mu(a, b) = ab$ (or $a + b$, $a \circ b$, $a * b$, etc.)

Definition 1.1. A group is a set $G$ with a law of composition such that

1. $a(bc) = (ab)c$ for all $a, b, c \in G$.
2. There exists an element $e \in G$ such that $ea = ae = a$ for all $a \in G$.
3. For every element $a \in G$, there exists an element $b \in G$ such that $ab = ba = e$.

A group $G$ is abelian if $ab = ba$ for all $a, b \in G$.

Lemma 1.2. Suppose that $G$ is a group. Then

1. (cancellation) Let $a, b, c \in G$ If $ab = ac$ then $b = c$. If $ba = ca$, then $b = c$.
2. (uniqueness of the identity element) There is a unique element $x \in G$ such that $xa = ax = a$ for all $a \in G$.
3. (uniqueness of the inverse) For every element $a \in G$, there is a unique element $y \in G$ such that $ay = ya = e$.

We often write $a^{-1}$ for the inverse of $a$. If the law of composition is written additively, we write $-a$ for the inverse of $a$. We will write $e_G$ if we want to distinguish the group we are in.

Proof. (of 3). We must prove both existence and uniqueness. Suppose that $a \in G$. The existence of an inverse for $a$ follows from 3 of the definition of a group. We will now prove uniqueness. Suppose that $y$ and $b$ are inverses of $a$. Then $ab = ba = e$ and $ay = ya = e$. We have $ab = ay$, so that $b = y$ by cancellation. \qed

Definition 1.3. Suppose that $G$ and $H$ are groups. A group homomorphism $\varphi : G \to H$ is a mapping such that $\varphi(ab) = \varphi(a)\varphi(b)$ for all $a, b \in G$.

A group homomorphism $\varphi : R \to S$ is an isomorphism if there is a group homomorphism $\psi : S \to R$ such that $\varphi \circ \psi = id_S$ and $\psi \circ \varphi = id_R$.

Definition 1.4. A ring $R$ is a set with two laws of composition $+$ and $\times$ such that

1. $(R, +)$ is an abelian group with an identity 0.
2. Multiplication $\times$ is associative and has an identity 1.
3. For all $a, b, c \in R$, $(a + b)c = ac + bc$ and $c(a + b) = ca + cb$.

A rng (pronounced “rung”) is a ring without a multiplicative identity. A commutative ring is a ring in which multiplication is commutative.

Lemma 1.5. Suppose that $R$ is a ring. Then

1. $0x = x0 = 0$ for all $x \in R$.
2. The multiplicative identity 1 is unique.
3. \((-1)x = -x\) for all \(x \in R\).

We will write \(0_R\) and \(1_R\) if we want to distinguish the ring we are in.

An nonzero element \(a \in R\) is a zero divisor if there exists \(0 \neq b \in R\) such that \(ab = 0\).

An integral domain \(R\) is a nonzero commutative ring having no zero divisors. Cancellation holds in a commutative ring \(R\) if \(ab = ac\) implies \(b = c\) for \(a, b, c \in R\) with \(a \neq 0\).

**Lemma 1.6.** A commutative ring \(R\) is an integral domain if and only if cancellation holds in \(R\).

**Definition 1.7.** Suppose that \(R\) and \(S\) are rings. A ring homomorphism \(\psi : R \to S\) is a mapping such that

1. \(\psi(a + b) = \psi(a) + \psi(b)\) for all \(a, b \in R\).
2. \(\psi(ab) = \psi(a)\psi(b)\) for all \(a, b \in R\).
3. \(\psi(1_R) = 1_S\).

A ring homomorphism \(\varphi : R \to S\) is an isomorphism if there is a ring homomorphism \(\psi : S \to R\) such that \(\varphi \circ \psi = id_S\) and \(\psi \circ \varphi = id_R\).

## 2. The Integers

**Definition 2.1.** An integral domain \(R\) is an ordered domain if there is a subset \(P\) of \(R\), called the positive elements of \(R\), which satisfy the following properties:

1. If \(a, b \in P\) then \(a + b \in P\).
2. If \(a, b \in P\) then \(ab \in P\).
3. If \(a \in R\), then one and only one of the following alternatives holds: \(a \in P\), \(a = 0\) or \(-a \in P\).

We write \(a < b\) if \(b - a \in P\) and we write \(a \leq b\) if \(b - a \in P\) or \(b = a\). If \(a < b\), we say that \(a\) is smaller than \(b\).

**Lemma 2.2.** In an ordered domain, we have

1. If \(a < b\) then \(a + c < b + c\).
2. If \(a < b\) and \(0 < c\) then \(ac < bc\).

**Theorem 2.3.** Let \(D\) be an ordered domain. Then the square of every non zero element of \(D\) is positive.

**Definition 2.4.** An ordered domain is well ordered if every nonempty subset of the positive elements \(P\) has a smallest element.

**Theorem 2.5.** There exists an ordered domain in which the positive elements are well ordered.

The proof of Theorem 2.5 requires more set theory.

**Theorem 2.6.** Any two ordered domains in which the positive elements are well ordered are isomorphic by an order preserving ring homomorphism.

We call the unique (up to order preserving isomorphism) ordered domain in which the positive elements are well ordered the integers, and write it as \(\mathbb{Z}\). We write \(\mathbb{Z}_+\) to denote the positive integers. The natural numbers, \(\mathbb{N}\), is the union of \(\mathbb{Z}_+\) and \(\{0\}\) (most “modern” books follow this definition of the natural numbers).
Suppose that \( x \in \mathbb{Z} \); that is, \( x \) is a number. Define

\[
|x| = \begin{cases} 
  x & \text{if } x \text{ is positive} \\
  0 & \text{if } x = 0 \\
  -x & \text{if } x \text{ is negative}
\end{cases}
\]

A number \( x \) is negative if \( -x \) is positive.

**Theorem 2.7.** There is no integer \( x \) such that \( 0 < x < 1 \).

**Proof.** Let \( S \) be the set of positive elements \( c \) of \( \mathbb{Z} \) such that \( 0 < c < 1 \). We will suppose that \( S \) is not empty, and derive a contradiction. Assuming that \( S \) is nonempty, there is a smallest element \( m \in S \) (since the positive elements are well ordered). We have \( 0 < m < 1 \) by assumption. By Lemma 2.2, we have \( 0 < m^2 < m \times 1 = m < 1 \). Thus \( m^2 \in S \) is less than \( m \), a contradiction. \( \square \)

**Theorem 2.8.** Suppose that \( S \) is a nonempty subset of \( \mathbb{Z} \) which is bounded from below (there exists \( c \in \mathbb{Z} \) such that \( x \geq c \) for all \( x \in S \)). Then \( S \) has a smallest element.

**Theorem 2.9.** (Principle of Mathematical Induction) Suppose that \( P(n) \) are propositions for \( n \in \mathbb{N} \) such that

1. \( P(0) \) is true and
2. If \( P(n) \) is true for some \( n \in \mathbb{N} \) then \( P(n + 1) \) is true.

Then \( P(n) \) is true for all \( n \in \mathbb{N} \).

**Proof.** Let \( S = \{ n \in \mathbb{N} \mid P(n) \text{ is not true} \} \). We must prove that \( S = \emptyset \). Suppose not. Then there exists a smallest element \( m \in S \) (by Theorem 2.8). Since \( P(0) \) is true, \( m > 0 \), so \( m \geq 1 \) by Theorem 2.7, and thus \( m - 1 \in \mathbb{N} \). But then \( P(m - 1) \) is true so \( P(m) \) must be true, and thus \( m \not\in S \), a contradiction. Thus \( S = \emptyset \). \( \square \)

A useful variation on this theorem is the following.

**Theorem 2.10.** Suppose that \( c \in \mathbb{Z} \) and \( T = \{ n \in \mathbb{Z} \mid n \geq c \} \). Suppose that \( P(n) \) are propositions for \( n \in T \) such that

1. \( P(c) \) is true and
2. If \( P(n) \) is true for some \( n \in T \) then \( P(n + 1) \) is true.

Then \( P(n) \) is true for all \( n \in T \).

**Theorem 2.11.** (Euclidean Division) Suppose \( m, n \in \mathbb{Z} \) with \( m > 0 \). Then there exists a unique expression \( n = qm + r \) with \( q, r \in \mathbb{Z} \) and \( 0 \leq r < m \).

**Proof.** We first proof existence. Let

\[
S = \{ n - am \mid a \in \mathbb{Z} \text{ and } n - am \text{ is nonnegative} \}.
\]

We will establish that \( S \) is nonempty. We have that \( 1 \leq m \) (by Theorem 2.7) Thus \( |n| = |n| \times 1 \leq |n| \times m \), so that \( -|n|m \leq -|n| \leq n \), and \( n + |n|m \in S \). Thus \( S \) is nonempty. \( S \) is a nonempty set which is bounded from below, so it has a smallest element, \( r \).

We will assume \( r \geq m \) and derive a contradiction. We have an expression \( r = n - am \) for some \( a \in \mathbb{Z} \).

\[
0 \leq r - m = n - am - m = n - (a + 1)m < r.
\]

Thus \( r - m \in S \), a contradiction to our assumption that \( r \) was the smallest element of \( S \). We thus have that \( 0 \leq r < m \). Set \( q = a \). We have an expression \( n = qm + r \) with \( 0 \leq r < m \).
We now prove uniqueness. Suppose we have expressions \( n = qm + r \) with \( 0 \le r < m \) and \( n = q_1m + r_1 \) with \( 0 \le r_1 < m \). We will prove that \( r = r_1 \) and \( q = q_1 \). If \( r = r_1 \), then \( 0 = (q - q_1)m \) implies \( q = q_1 \), since \( \mathbb{Z} \) is a domain. Suppose \( r \neq r_1 \). Without loss of generality, we may suppose that \( r > r_1 \). Since \( r_1 \ge 0 \) and \( r < m \) we have that \( r - r_1 < m \). We also have that \( 0 < r - r_1 = m(q_1 - q) \). Thus \( q_1 - q > 0 \) and we have \( q_1 - q \ge 1 \) (by Theorem 2.7). So \( r - r_1 \ge m \), a contradiction. We thus have that \( r = r_1 \), and \( q = q_1 \). □

An integer \( b \) divides an integer \( a \) if \( a = cb \) for some integer \( c \). Write \( b \mid a \) if \( b \) divides \( a \). We will also say that \( a \) is a multiple of \( b \).

**Definition 2.12.** An integer \( d \) is a greatest common divisor of the integers \( a \) and \( b \) if \( d \) is a common divisor of \( a \) and \( b \) which is a multiple of every other common divisor of \( a \) and \( b \).

**Theorem 2.13.** Any two integers \( a \) and \( b \), which are not both zero, have a unique positive greatest common divisor \( d \). There exist integers \( m \) and \( n \) such that \( d = ma + nb \).

**Proof.** We will first prove the existence of a positive greatest common divisor. Let

\[
S = \{ma + nb \mid m, n \in \mathbb{Z} \text{ and } ma + nb > 0\}.
\]

\( S \) is a nonempty subset of the positive integers, so \( S \) has a smallest element \( d \).

We will first show that every element of \( S \) is divisible by \( d \). Suppose \( x \in S \). We have an expression \( x = pd + q \) with \( 0 \le q < d \), by Euclidean division. If \( q = x - pd > 0 \), then \( q \in S \) but \( q < d \), which would contradict the fact that \( d \) is the smallest element of \( S \). Thus \( q = 0 \), and \( x \) is divisible by \( d \).

Since \( |a| \) and \( |b| \) are in \( S \), \( d \) is a common divisor of \( a \) and \( b \). Suppose \( x \) is a common divisor of \( a \) and \( b \). Then \( a = \alpha x \) and \( b = \beta x \) for some \( \alpha, \beta \in \mathbb{Z} \). Since \( d \in S \), we have an expression \( d = ma + nb \) for some \( m, n \in \mathbb{Z} \). \( d = m\alpha x + n\beta x = (m\alpha + n\beta)x \), so \( d \) is a multiple of \( x \). We have established that \( d \) is a greatest common divisor of \( a \) and \( b \).

We will now establish uniqueness of the positive greatest common divisor. Suppose that \( d \) and \( e \) are positive integers which are greatest common divisors of \( a \) and \( b \). Then \( d \) divides \( e \) and \( e \) divides \( d \), so we have expressions \( d = \alpha e \) and \( e = \beta d \). \( \alpha \) and \( \beta \) are positive since \( d \) and \( e \) are, so \( 1 \le \alpha \) and \( 1 \le \beta \) (by Theorem 2.7). We have \( 1 \times e = e = \alpha\beta e \). By cancellation, \( 1 = \alpha\beta \). \( \alpha < 1 \) or \( 1 < \beta \) is impossible since this would imply \( 1 < \alpha\beta \). Thus \( \alpha = \beta = 1 \) and \( d = e \). □

We will call the positive greatest common divisor of two integers \( a \) and \( b \), which are not both zero, the greatest common divisor of \( a \) and \( b \) (ignoring the negative greatest common divisor), and write \( d = \gcd(a, b) \). Two integers \( a \) and \( b \) are relatively prime if \( \gcd(a, b) = 1 \).

**Definition 2.14.** An integer \( p > 1 \) is a prime number if \( p = ab \) with \( a \) and \( b \) positive integers implies \( a = p \) or \( b = p \).

**Theorem 2.15.** An integer \( p > 1 \) is a prime number if and only if for any integer \( a \) either \( p \mid a \) or \( \gcd(p, a) = 1 \).