Abstract Algebra Theorems and Definitions

MTH 411 - Fall 2023

0 Preliminaries

- **Axiom Well Ordering Principle:** Every nonempty set of positive integers contains a smallest element.
- **Definition Equivalence Relation:** An *equivalence relation* on a set S is a set R of ordered pairs of elements of S such that
    1. $(a, a) \in R \ \forall a \in S$ (reflexive property).
    2. $(a, b) \in R$ implies $(b, a) \in R$ (symmetric property).
    3. $(a, b) \in R$ and $(b, c) \in R$ imply that $(a, c) \in R$ (transitive property).
- **Definition Function (mapping):** A *function* ϕ from a set A to a set B is a rule that assigns to each element a of A exactly one element b of B. The set A is called the *domain* of ϕ, and B is called the *range* of ϕ. If ϕ assigns b to a, then b is called the *image of a under ϕ*. The subset of B comprising all the images of elements of A is called the *image of A under ϕ*.
- **Definition Composition of Functions:** Let $\phi : A \mapsto B$ and $\psi : B \mapsto C$. The *composition* $\psi\phi$ is the mapping from A to C defined by

$$(\psi\phi)(a) = \psi(\phi(a)), \ \forall a \in A.$$

- **Definition One-to-One Functions (injection):** A function ϕ from a set A is called *one-to-one* if for every $a_1, a_2 \in A$, $\phi(a_1) = \phi(a_2)$ implies $a_1 = a_2$.
- **Definition Onto Functions (surjection):** A function ϕ from a set A to a set B is said to be *onto* if each element of B is the image of at least one element of A. In symbols, $\phi : A \mapsto B$ is onto if for each $b \in B$ there is at least one $a \in A$ such that $\phi(a) = b$.
- **Theorem Division Algorithm:** Let $a, b \in \mathbb{Z}$ with $b > 0$. Then there exist unique integers q, r with the property that $a = bq + r$, where $0 \leq r < b$.
- **Theorem GCD is a Linear Combination:** For any nonzero integers a and b, there exist integers s and t such that $\mathsf{gcd}(a, b) = as + bt$. Moreover, $\mathsf{gcd}(a, b)$ is the smallest positive integer of the form $as + bt$.
- **Lemma Euclid's Lemma:** Let p be a prime, and let a, b be integers. If $p|ab$ then $p|a$ or $p|b$.

- **Theorem Fundamental Theorem of Arithmetic:** Every integer greater than 1 is a prime or product of primes. This product is unique, except for the order in which the factors appear. That is, if $n = p_1 p_2 \cdots p_r$ and $n = q_1 q_2 \cdots q_s$, where the p's and q's are primes, then $r = s$ and, after renumbering the q's, we have $p_i = q_i$ for all i.
- **Theorem First Principle of Mathematical Induction:** Let S be a set of integers containing a. Suppose S has the property that whenever some integer $n \geq a$ belongs to S, then the integer $n+1$ also belongs to S. Then, S contains every integer greater than or equal to a.
- **Theorem Second Principle of Mathematical Induction:** Let S be a set of integers containing a. Suppose S has the property that n belongs to S whenever every integer less than n and greater than or equal to a belongs to S. Then, S contains every integer greater than or equal to a.
- **Theorem DeMoivre's Theorem:** For every positive integer n and every real number θ, $(\cos(\theta) + i\sin(\theta))^n = \cos n\theta + i \sin n\theta$.

1 Introduction to Groups

- **Other?** D_4 **(Symmetries of a Square):** $D_4 = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$.
- **Other?** D_n **(Dihedral Groups):** $D_n = \{R_0, R_{\cdot\frac{360}{n}}, \ldots, R_{(n-1)\cdot\frac{360}{n}}\} + n$ other flips across lines.

2 Groups

- **Definition Binary Operation:** Let G be a set. A *binary operation* on G is a function that assigns each ordered pair of elements of G an element of G.
- **Definition Group:** Let G be a set together with binary operation (usually called multiplication) that assigns to each ordered pair (a, b) of elements of G an element in G denoted by ab. We say G is a *group* under this operation if the following three properties are satisfied.
  1. *Associativity.* The operation is associative; that is, $(ab)c = a(bc)$ for all $a, b, c \in G$.
  2. *Identity.* There is an element e (called the *identity*) in G such that $ae = ea = a$ for all $a \in G$.
  3. *Inverses.* For each element a in G, there is an element b in G (called an *inverse* of a) such that $ab = ba = e$.
- **Theorem Uniqueness of Identity:** In a group G, there is only one identity element.
- **Theorem Uniqueness of Inverses:** For each element a in a group G, there is a unique element $b \in G$ such that $ab = ba = e$.
- **Theorem Cancellation:** In a group G, the right and left cancellation laws hold; that is, $ba = ca$ implies $b = c$ and $ab = ac$ implies $b = c$.

- **Theorem Socks-Shoes:** For group elements a and b, $(ab)^{-1} = b^{-1}a^{-1}$.

3 Finite Groups; Subgroups

- **Definition Order of a Group:** The number of elements of a group (finite or infinite) is called its *order*. We will use $|G|$ to denote the order of G.

- **Definition Order of an Element:** The order of an element g is a group G is the smallest integer n such that $g^n = e$ (in additive notation, this would be $ng = 0$). If no such integer exists, we say that g was *infinite order*. The order of an element g is denoted $|g|$.

- **Definition Subgroup:** If a subset H of a group G is itself a group under the operation of G, we say that H is a *subgroup* of G.

- **Definition Center of a Group:** The *center*, $Z(G)$, of a group G is the subset of elements in G that commute with every element of G. In symbols,
$$Z(G) = \{a \in G | ax = xa,\ x \in G\}.$$

- **Definition Centralizer of a in G:** Let a be a fixed element of a group G. The *centralizer of a in G*, $C(G)$, is the set of all elements in G that commute with a. In symbols,
$$C(a) = \{g \in G | ga = ag\}.$$

- **Theorem One-Step Subgroup Test:** Let G be a group and H a nonempty subset of G. If ab^{-1} is in H whenever a, b are in H, then H is a subgroup of G (in additive notation, if $a - b$ is in H whenever a, b are in H, then H is a subgroup of G).

- **Theorem Two-Step Subgroup Test:** Let G be a group and let H be a nonempty subset of G. If ab is in H whenever a, b are in H (H is closed under the operation), and a^{-1} is in H whenever a is in H (H is closed under taking inverses), then H is a subgroup of G.

- **Theorem Finite Subgroup Test:** Let H be a nonempty finite subset of a group G. If H is closed under the operation G, then H is a subgroup of G.

- **Theorem Center of a Subgroup:** The center of a group G is a subgroup of G.

- **Theorem C(a) is a Subgroup:** For each a in a group G, the centralizer of a is a subgroup of G.

4 Cyclic Groups

- **Definition Euler $\varphi-$Function:** Let $\varphi(1) = 1$, and for any integer $n > 1$, let $\varphi(n)$ denote the number of positive integers less than n and relatively prime to n.

- **Theorem Criterion for $a^i = a^j$:** Let G be a group, and let $a \in G$. If a has infinite order, then $a^i = a^j$ if and only if $i = j$. If a has finite order, say n, then $\langle a \rangle = \{e, a, a^2, \dots, a^{n-1}\}$ and $a^i = a^j$ if and only if $n | i - j$.
- **Corollary $|a| = |\langle a \rangle|$:** For any group element a, $|a| = |\langle a \rangle|$.
- **Corollary $a^k = e$ Implies That $|a|$ divides k:** Let G be a group and let a be an element of order n in G. If $a^k = e$, then n divides k.
- **Corollary Relationship Between $|ab|$ and $|a||b|$:** If a and b belong to a finite group and $ab = ba$, then $|ab|$ divides $|a||b|$.
- **Theorem $\langle a^k \rangle = \langle a^{\mathsf{gcd}(n,k)} \rangle$ and $|a^k| = n/\mathsf{gcd}(n,k)$:** Let a be an element of order n in a group and let k be a positive integer. Then $\langle a^k \rangle = \langle a^{\mathsf{gcd}(n,k)} \rangle$ and $|a^k| = n/\mathsf{gcd}(n,k)$.
- **Corollary Orders of Elements in Finite Cyclic Groups:** In a finite cyclic group, the order of an element divides the order of a group.
- **Corollary Criterion for $\langle a^i \rangle = \langle a^j \rangle$ and $|a^i| = |a^j|$:** Let $|a| = n$. Then $\langle a^i \rangle = \langle a^j \rangle$ if and only if $\mathsf{gcd}(n,i) = \mathsf{gcd}(n,j)$, and $|a^i| = |a^j|$ if and only if $\mathsf{gcd}(n,i) = \mathsf{gcd}(n,j)$.
- **Corollary Generators of Finite Cyclic Groups:** Let $|a| = n$. Then $\langle a \rangle = \langle a^j \rangle$ if and only if $\mathsf{gcd}(n,j) = 1$, and $|a| = |\langle a^j \rangle|$ if and only if $\mathsf{gcd}(n,j) = 1$.
- **Corollary Generators of $\mathbb{Z}_n$:** An integer $k \in Z_n$ is a generator of Z_n if and only if $\mathsf{gcd}(n,k) = 1$.
- **Theorem The Fundamental Theorem of Cyclic Groups:** Every subgroup of a cyclic group is cyclic. Moreover, if $|\langle a \rangle| = n$, then the order of any subgroup of $\langle a \rangle$ is a divisor of n; and, for each positive divisor k of n, the group $\langle a \rangle$ has exactly one subgroup of order k–namely, $\langle a^{n/k} \rangle$.
- **Corollary Subgroups of $\mathbb{Z}_n$:** For each positive divisor k of n, the set $\langle n/k \rangle$ is the unique subgroup of Z_n of order k; moreover, these are the only subgroups of Z_n.
- **Theorem Number of Elements of Each Order in a Cyclic Group:** If d is a positive divisor of n, the number of elements of order d in a cyclic group of order n is $\varphi(d)$.

5 Permutation Groups

- **Definition Permutation of A:** A *permutation* of a set A is a function from A to A that is both one-to-one and onto.
- **Theorem Products of Disjoint Cycles:** Every permutation of a finite set can be written as a cycle or as a product of disjoint cycles.
- **Theorem Disjoint Cycles Commute:** If the pair of cycles $\alpha = (a_1, a_2, \dots, a_m)$ and $\beta = (b_1, b_2, \dots, b_m)$ have no entries in common, then $\alpha\beta = \beta\alpha$.

- **Theorem Order of a Permutation:** The order of permutation of a finite set written in disjoint cycle form is the least common multiple of the lengths of the cycles.
- **Theorem Product of 2-Cycles:** Every permutation in S_n, $n > 1$, is a product of 2-cycles.
- **Theorem Always Even or Always Odd:** If a permutation α can be expressed as a product of an even (odd) number of 2-cycles, then every decomposition of α into a product of 2-cycles must have an even (odd) number of 2-cycles. In symbols, if

  $$\alpha = \beta_1\beta_2 \cdots \beta_r \text{ and } \alpha = \gamma_1, \gamma_2 \cdots \gamma_s,$$

  where the β's and γ's are 2-cycles, then r and s are both even or both odd.
- **Definition Even/Odd Permutations:** A permutation that can be expressed as a product of an even number of 2-cycles is called an *even* permutation. A permutation that can be expressed as a product of an odd number of 2-cycles is called an *odd* permutation.
- **Theorem Even Permutations From a Group:** The set of even permutations in S_n forms a subgroup of S_n.
- **Definition Alternating Group A_n:** The group of even permutations of n symbols is denoted by A_n and is called the *alternating group of degree* n.
- **Theorem $|A_n| = \frac{n!}{2}$:** For $n > 1$, A_n has order $\frac{n!}{2}$.

6 Isomorphisms

- **Definition Group Isomorphism:** An *isomorphism* ϕ from a group G onto a group $\overline{G}$ is a one-to-one mapping from G onto $\overline{G}$ that preserves the group operation. That is,

  $$\phi(ab) = \phi(a)\phi(b) \quad \forall a, b \in G.$$

  If there is an isomorphism from G onto $\overline{G}$, we say that G and $\overline{G}$ are *isomorphic* and write $G \approx \overline{G}$.
- **Theorem Cayley's Theorem:** Every group is isomorphic to a group of permutations.
- **Theorem Properties of Isomorphisms (acting on elements):** Suppose that ϕ is an isomorphism from a group G onto a group $\overline{G}$. Then,
  1. ϕ carries the identity of G to the identity of $\overline{G}$.
  2. For every integer n and for every group element $a \in G$, $\phi(a^n) = [\phi(a)]^n$.
  3. For any elements $a, b \in G$, a and b commute if and only if $\phi(a)$ and $\phi(b)$ commute.

4. $G = \langle a \rangle$ if and only if $\overline{G} = \langle \phi(a) \rangle$.
5. $|a| = |\phi(a)|$ for all $a \in G$.
6. For a fixed integer k and a fixed group element $b \in G$, the equation $x^k = b$ has the same number of solutions in G as does the equation $x^k = \phi(b)$ in $\overline{G}$.
7. If G is finite, then G and $\overline{G}$ have exactly the same number of elements of every order.

- **Theorem Properties of Isomorphisms (acting on groups):** Suppose that ϕ is an isomorphism from a group G onto a group $\overline{G}$. Then,
  1. ϕ^{-1} is an isomorphism from $\overline{G}$ onto G.
  2. G is Abelian if and only if $\overline{G}$ is Abelian.
  3. G is cyclic if and only if $\overline{G}$ is cyclic.
  4. If K is a subgroup of G, then $\phi(K) = \{\phi(k)|k \in K\}$ is a subgroup of $\overline{G}$.
  5. If $\overline{K}$ is a subgroup of $\overline{G}$, then $\phi^{-1}(\overline{K}) = \{g \in G|\phi(g) \in \overline{K}\}$ is a subgroup of G.
  6. $\phi(Z(G)) = Z(\overline{G})$.
- **Definition Automorphism:** An isomorphism from a group G onto itself is called an automorphism.
- **Definition Inner Automorphism induced by a:** Let G be a group, and let $a \in G$. The function ϕ_a defined by $\phi_a(x) = axa^{-1}$, $\forall x \in G$ is called the *inner automorphism of G induced by a*.
- **Theorem Aut(G) and Inn(G) Are Groups:** The set of automorphisms of a group and the set of inner automorphisms of a group are both groups under the operation of function composition.
- **Theorem Aut(Z_n) $\approx U(n)$:** For every positive integer n, Aut(Z_n) is isomorphic to $U(n)$.

7 Cosets and La Grange's Theorem

- **Definition Coset of H in G:** Let G be a group and let H be a nonempty subset of G. For any $a \in G$, the set $\{ah|h \in H\}$ is denoted by aH. Analogously, $Ha = \{ha|h \in H\}$ and $aHa^{-1} = \{aHa^{-1}|h \in H\}$. When H is a subgroup of G, the set aH is called the *left coset of H in G containing a*, whereas Ha is called the *right coset of H in G containing a*. In this case, the element a is called the *coset representative of aH (or Ha)*.
- **Theorem Properties of Cosets:** Let H be a subgroup of G, and let $a, b \in G$. Then,
  1. $a \in aH$.
  2. $aH = H$ if and only if $a \in H$.

3. $(ab)H = a(bH)$ and $H(ab) = (Ha)b$.
4. $aH = bH$ if and only if $a \in bH$.
5. $aH = bH$ or $aH \cap bH = \emptyset$.
6. $aH = bH$ if and only if $a^{-1}b \in H$.
7. $|aH| = |bH|$.
8. $aH = Ha$ if and only if $H = aHa^{-1}$.
9. aH is a subgroup of G if and only if $a \in H$.

- Theorem **La Grange's Theorem:** If G is a finite group and H is a subgroup of G, then $|H|$ divides $|G|$. Moreover, the number of distinct left (right) cosets of H in G is $|G|/|H|$.
- Corollary **$|G : H| = |G|/|H|$:** If G is a finite group and $H \leq G$, then $|G : H| = |G|/|H|$.
- Corollary **$|a|$ divides $|G|$:** In a finite group, the order of each element of the group divides the order of the group.
- Corollary **Groups of Prime Order are Cyclic:** A group of prime order is cyclic.
- Corollary **$a^{|G|} = e$:** Let G be a finite group, and let $a \in G$. Then $a^{|G|} = e$.
- Corollary **Fermat's Little Theorem:** For every integer a and every prime p, $a^p \bmod p = a \bmod p$.
- Theorem **$|HK| = \frac{|H||K|}{|H \cap K|}$:** For two finite subgroups H and K of a group, define the set $HK = \{hk | h \in H, k \in K\}$. Then $|HK| = \frac{|H||K|}{|H \cap K|}$.
- Theorem **Classification of Groups of Order $2p$:** (SKIPPED FOR NOW)
- Definition **Stabilizer of a Point:** Let G be a group of permutations of a set S. For each $i \in S$, let $\mathrm{stab}_G(i) = \{\phi \in G | \phi(i) = i\}$. We call $\mathrm{stab}_G(i)$ the *stabilizer* of i in G.
- Definition **Orbit of a Point:** Let G be a group of permutations of a set S. For each $i \in S$, let $\mathrm{orb}_G(i) = \{\phi(i) | \phi \in G\}$. The set $\mathrm{orb}_G(i)$ is a subset of S called the *orbit of i under G*. We use $|\mathrm{orb}_G(i)|$ to denote the number of elements in $\mathrm{orb}_G(i)$.
- Theorem **Orbit-Stabilizer Theorem:** Let G be a finite group of permutations of a set S. Then, for any $i \in S$, $|G| = |\mathrm{orb}_G(i)||\mathrm{stab}_G(i)|$.

8 External Direct Products

- Definition **External Direct Product:** Let $G_1, G_2, \ldots, G_n$ be a finite collection of groups. The *external direct product* of $G_1, G_2, \ldots, G_n$, written as $G_1 \oplus G_2 \oplus \cdots \oplus G_n$, is the set of all n-tuples for which the ith component is an element of G_i and the operation is component wise.

$$G_1 \oplus G_2 \oplus \cdots \oplus G_n = \{(g_1, g_2, \ldots, g_n) \mid g_i \in G_i\}$$

- Other **Example Classification of Groups of Order 4:** A group of order 4 is isomorphic to Z_4 or $Z_2 \oplus Z_2$.
- Theorem **Order of an Element in a Direct Product:** The order of an element in a direct product of a finite number of finite groups is the least common multiple of the orders of the components of the element. In symbols,
$$|(g_1, g_2, \ldots, g_n)| = \mathbf{lcm}(|g_1|, |g_2|, \ldots, |g_n|).$$
- Theorem **Criterion for $G \oplus H$ to be Cyclic:** Let G and H be finite cyclic groups. Then $G \oplus H$ is cyclic if and only if $|G|$ and $|H|$ are relatively prime.

9 Normal Subgroups and Factor Groups

- Definition **Normal Subgroup:** A subgroup H of a group G is called a *normal* subgroup of G if $aH = Ha$, $\forall a \in G$. We denote this by $H \trianglelefteq G$.
- Theorem **Normal Subgroup Test:** A subgroup H of G is normal if and only if $xHx^{-1} \subseteq H$, $\forall x \in G$.
- Theorem **Factor Groups:** Let G be a group and let H be a normal subgroup of G. The set $G/H = \{aH | a \in G\}$ is a group under the operation $(aH)(bH) = abH$.
- Theorem **G/Z Theorem:** Let G be a group and let $Z(G)$ be the center of G. If $G/Z(G)$ is cyclic, the G is abelian.
- Theorem **$G/Z(G) \approx Inn(G)$:** For any group G, $G/Z(G)$ is isomorphic to $Inn(G)$.
- Theorem **Cauchy's Theorem for Abelian Groups:** Let G be a finite Abelian group and let p be a prime that divides the order of G. Then G has an element of order p.
- Definition **Internal Direct Product:** We say G is the *internal direct product* of H and K and write $G = H \times K$ if H and K are normal subgroups of G and,
$$G = HK \text{ and } H \cap K = \{e\}.$$
- Theorem **Classification of Groups of Order p^2:** Every Group of order p^2, where p is a prime, is isomorphic to Z_{p^2} or $Z_p \oplus Z_p$.

10 Group Homomorphisms

- **Definition Group Homomorphism:** A *homomorphism* ϕ from a group G to a group $\overline{G}$ is a mapping from G into $\overline{G}$ that preserves the group operation; that is, $\phi(ab) = \phi(a)\phi(b)$ for all $a, b \in G$.
- **Definition Kernel of a Homomorphism:** The *kernel* of a homomorphism ϕ from a group G to a group with identity e is the set $\{x \in G|\phi(x) = e\}$. The kernel of ϕ is denoted by Kerϕ.
- **Theorem Properties of Elements Under Homomorphisms:** Let ϕ be a homomorphism from a group G to a group $\overline{G}$ and let g be an element of G. Then,
  1. ϕ carries the identity of G to the identity of $\overline{G}$.
  2. $\phi(g^n) = (\phi(g))^n$ for all $n \in \mathbb{Z}$.
  3. If $|g|$ is finite, then $|\phi(g)|$ divides $|g|$.
  4. Kerϕ is a subgroup of G.
  5. $\phi(a) = \phi(b)$ if and only if $a\text{Ker}\phi = b\text{Ker}\phi$.
  6. If $\phi(g) = g'$, then $\phi^{-1}(g') = \{x \in G|\phi(x) = g'\} = g\text{Ker}\phi$.
- **Theorem Properties of Subgroups Under Homomorphisms:** Let ϕ be a homomorphism from a group G to a group $\overline{G}$ and let H be a subgroup of G. Then,
  1. $\phi(H) = \{\phi(h)|h \in H\}$ is a subgroup of $\overline{G}$.
  2. If H is cyclic, then $\phi(H)$ is cyclic.
  3. If H is Abelian, then $\phi(H)$ is Abelian.
  4. If H is normal in G, then $\phi(H)$ is normal in $\phi(G)$.
  5. If $|Ker\phi| = n$, then ϕ is an $n-$to-1 mapping from G onto $\phi(G)$.
  6. If $|H| = n$, then $|\phi(H)|$ divides n.
  7. If $\overline{K}$ is a subgroup of $\overline{G}$, then $\phi^{-1}(\overline{K}) = \{k \in G|\phi(k) \in \overline{K}$ is a subgroup of G.
  8. If $\overline{K}$ is a normal subgroup of $\overline{G}$, then $\phi^{-1}(\overline{K}) = \{k \in G|\phi(k) \in \overline{K}$ is a normal subgroup of G.
  9. If ϕ is onto and Ker$\phi = \{e\}$, then ϕ is an isomorphism from G to $\overline{G}$.
- **Corollary Kernels Are Normal:** Let ϕ be a group homomorphism from G to $\overline{G}$. Then Kerϕ is a normal subgroup of G.
- **Theorem First Isomorphism Theorem:** Let ϕ be a group homomorphism from G to $\overline{G}$. Then the mapping from $G/\text{Ker}\phi$ to $\phi(G)$, given by $g\text{Ker}\phi \longrightarrow \phi(g)$, is an isomorphism. In symbols, $G/\text{Ker}\phi \approx \phi(G)$.
- **Corollary $|\phi(G)|$ Divides $|G|$ and $|\overline{G}|$:** If ϕ is a homomorphism from a finite group G to $\overline{G}$, then $|\phi(G)|$ divides $|G|$ and $|\overline{G}|$.

- **Theorem Normal Subgroups Are Kernels:** Every normal subgroup of a group G is the kernal of a homomorphism of G. In particular; a normal subgroup N is the kernel of the mapping $g \longrightarrow gN$ from G to G/N.

11 Fundamental Theorem of Finite Abelian Groups

- **Theorem Fundamental Theorem of Finite Abelian Groups:** Every finite Abelian group is a direct product of cyclic groups of prime-power order. Moreover, the number of terms in the product and the orders of the cyclic groups are uniquely determined by the group.

12 Introduction to Rings

- **Definition Ring:** A *ring* R is a set with two binary operations, addition (denoted by $a+b$) and multiplication (denoted by ab), such that for all $a, b, c \in R$:
  1. $a+b=b+a$.
  2. $(a+b)+c=a+(b+c)$.
  3. There is an additive identity 0. That is, there is an element 0 in R such that $a+0=a$ for all $a \in R$.
  4. There is an element $-a \in R$ such that $a+(-a)=0$.
  5. $a(bc)=(ab)c$.
  6. $a(b+c)=ab+ac$ and $(b+c)a=ba+ca$.
- **Theorem Rules of Multiplication:** Let a, b, c belong to a ring R. Then,
  1. $a0=0a=0$.
  2. $a(-b)=(-a)b=-(ab)$.
  3. $(-a)(-b)=ab$.
  4. $a(b-c)=ab-ac$ and $(b-c)a=ba-ca$.

  Furthermore, if R has a unity element 1, then

  5. $(-1)a=-a$.
  6. $(-1)(-1)=1$.
- **Theorem Uniqueness of the Unity and Inverses:** If a ring has a unity, it is unique. If a ring element has a multiplicative inverse, it is unique.
- **Definition Subring:** A subset S of a ring R is a *subring* of R if S is itself a ring with the operations of R.
- **Theorem Subring Test:** A nonempty subset S of a ring R is a subring if S is closed under subtraction and multiplication, that is, if $a-b$ and ab are in S whenever $a, b \in S$.

13 Integral Domains

- **Definition Zero-Divisors:** A *zero-divisor* is a nonzero element a of a commutative ring R such that there is a nonzero element $b \in R$ with $ab = 0$.
- **Definition Integral Domains:** An *integral domain* is a commutative ring with unity and no zero-divisors.
- **Theorem Cancellation:** Let a, b, c belong to an integral domain. If $a \neq 0$ and $ab = ac$, then $b = c$.
- **Definition Field:** A *field* is a commutative ring with unity in which every nonzero element is a unit.
- **Theorem Finite Integral Domains are Fields:** A finite integral domain is a field.
- **Corollary $\mathbb{Z}_p$ is a Field:** For every prime p, $\mathbb{Z}_p$, the ring of integers modulo p, is a field.
- **Definition Characteristic of a Ring:** The *characteristic* of a ring R is the least positive integer n such that $nx = 0$ for all $x \in R$. If no such integer exists, we say R has characteristic 0. The characteristic of R is denoted by char R.

14 Ideals and Factor Rings

- **Definition Ideal:** A subring A of a ring R is called a (two-sided) *ideal* of R if for every $r \in R$ and every $a \in A$, both ar and ra are in A.
- **Theorem Ideal Test:** A nonempty subset A of a ring R is an ideal of R if
  1. $a - b \in A$ whenever $a, b \in A$.
  2. ra and ar are in A whenever $a \in A$ and $r \in R$.
- **Theorem Existence of Factor Rings:** Let R be a ring and let A be a subring of R. The set of cosets $\{r + A | r \in R\}$ is a ring under the operations $(s + A) + (t + A) = s + t + A$ and $(s + A)(t + A) = st + A$ if and only if A is an ideal of R.
- **Definition Prime Ideal:** A *prime ideal* A of a commutative ring R is a proper ideal of R such that $a, b \in R$ and $ab \in A$ imply $a \in A$ or $b \in A$.
- **Definition Maximal Ideal:** A *maximal ideal* of a commutative ring R is a proper ideal of R such that, whenever B is an ideal of R and $A \subseteq B \subseteq R$, then $B = A$ or $B = R$.
- **Theorem R/A Is an Integral Domain If and Only If A Is Prime:** Let R be a commutative ring with unity and let A be an ideal of R. Then, R/A is an integral domain if and only if A is prime.

- **Theorem R/A Is an Field If and Only If A Is Maximal:** Let R be a commutative ring with unity and let A be an ideal of R. Then R/A is a field if and only if A is maximal.

  Let f be a ring homomorphism from a ring R to a ring S. Let A be a subring of R and let B be an ideal of S. 1. For any r [R and any positive integer n, f(nr) 5 nf(r) and f(rn) 5 (f(r))n. 2. f(A) 5 f(a) — a [A is a subring of S. 3. If A is an ideal and f is onto S, then f(A) is an ideal. 4. f21(B) 5 r [R — f(r) [B is an ideal of R. 5. If R is commutative, then f(R) is commutative. 6. If R has a unity 1, S 2 0, and f is onto, then f(1) is the unity of S. 7. f is an isomorphism if and only if f is onto and Ker f 5 r [R — f(r) 5 0 5 0. 8. If f is an isomorphism from R onto S, then f21 is an isomorphism from S onto R.