April 25, 2020

Abstract Algebra Definitions and Theorems

Definition A **group** is a set of elements G together with a binary operation # that have the properties:

1. Closure: If $a,b \in G$ then $a\#b \in G$
2. Associativity: If $a,b,c \in G$ then $a\#(b\#c) = (a\#b)\#c$
3. Identity under #: There is an element $e \in G$ such that if $a \in G$ then $a\#e = e\#a = a$
4. Inverses under #: For each $a \in G$ there is an element $a^{-1} \in G$ such that $a\#a^{-1} = a^{-1}\#a = e$.

As a default, we will use multiplication as the group operation, in which case the above properties are written:

1. Closure: If $a,b \in G$ then $ab \in G$
2. Associativity: If $a,b,c \in G$ then $a(bc) = (ab)c$
3. Identity: There is an element $e \in G$ such that if $a \in G$ then $ae = ea = a$
4. Inverses: For each $a \in G$ there is an element $a^{-1} \in G$ such that $aa^{-1} = a^{-1}a = e$.

But don't use the commutative law unless it is an Abelian group!

Definition: a group *G*, with operation # is an **Abelian** (commutative) group if for every $a,b \in G$ then $a\#b = b\#a$. The default operation symbol for an Abelian group is +.

***Theorem 1:** Function composition is associative.

***Theorem 2**: If *G* is a group, then the identity element *e* is unique.

Unique means that e is the only element of G that has the identity property (group: property 3)

***Theorem 3:** If *G* is a group, then every element of *G* has a unique inverse.

***Theorem 4:** If *G* is a group and $a,b \in G$ then $(ab)^{-1} = b^{-1}a^{-1}$

***Theorem 5:** If *G* is a group and $a \in G$ then $(a^{-1})^{-1} = a$

Definition If *G* is a group, and $H \subseteq G$ is a subset of *G*, such that *H* is a group, then *H* is a **subgroup** of *G*.

Theorem 6: If *G* is a group, and $H \subseteq G$ is a non-empty subset of *G* such that

1. *H* is closed: if $a,b \in H$ then $ab \in H$
2. The inverse of every element in *H* is also in *H*: If $a \in H$ then there is an element $a^{-1} \in H$ such that $aa^{-1} = a^{-1}a = e$

Then H is a subgroup of *G*.

prove theorem 6 by explaining why all 4 of the group properties must be true for H.

April 25, 2020

Well Ordering Axiom Every non-empty subset of the non-negative integers contains a smallest element.

Theorem 7: Let $a \in \mathbb{Z}$ and $b \in \mathbb{Z}^{+}$ (b is a positive integer), then there exist unique integers q, r such that $a = bq + r$ and $0 \le r < b$

Definition: Let *a* and *b* be integers where not both are zero, then $d = \gcd(a,b)$ is the greatest common divisor of *a* and *b*, which means:

- $d \mid a$ and $d \mid b$
- If $c \mid a$ and $c \mid b$ then $c \le d$

Note: our textbook writes $(a,b) = \gcd(a,b)$

Theorem 8 (1.2): Let *a* and *b* be integers where not both are zero, and $d = \gcd(a,b)$. There exist $u, v \in \mathbb{Z}$ such that $d = au + bv$

***Theorem 9 (1.3)**: Let *a* and *b* be integers where not both are zero, and $d = \gcd(a,b)$. Then if $c \mid a$ and $c \mid b$ then $c \mid d$

***Theorem 10 (1.4):** Let $a, b, c \in \mathbb{Z}$ such that $a \mid bc$ and $\gcd(a,b) = 1$ then $a \mid c$

hint: consider $c \cdot 1 = c(au + bv)$

***Theorem 11:** Let $a, b, c \in \mathbb{Z}$, and let $d = \gcd(a,b)$. Then $ax + by = c$ has integer solutions if and only if $d \mid c$ (pg. 16 # 24)

Definition: Let *p* be an integer such that $p \ne 0, \pm 1$, then *p* is **prime** means:

Given $b, c \in \mathbb{Z}$, if $p \mid bc$ then $p \mid b$ or $p \mid c$

Definition: Let *p* be an integer such that $p \ne 0, \pm 1$, then *p* is **irreducible** means the only divisors of p are ± 1 and $\pm p$

***Theorem 12:** An integer *p* be an integer such that $p \ne 0, \pm 1$ is prime if and only of it is irreducible.

***Theorem 13 (1.6):** Let *p* be a prime integer and let $p \mid a_1 a_2 \ldots a_n$ then *p* divides at least one of the factors a_i.

Theorem 14(1.7): Every integer *n* except $0, \pm 1$ is a product of primes.

Theorem 15 (Fundamental Theorem of Arithmetic, 1.8): If $n \in \mathbb{Z}$ and $n \ne 0, \pm 1$ then *n* is a product of primes, and the prime factorization is unique in the sense that if

$n = p_1 p_2 \ldots p_r$ and $n = q_1 q_2 \ldots q_s$

such that all of the p_i and q_j are prime,

then $r = s$ and the q_j factors can be re-ordered such that $p_i = \pm q_i$

(We can use a permutation to write $f : \{1, 2, \ldots s\} \to \{1, 2, \ldots s\}$ is a permutation, and $p_i = \pm q_{f(i)}$)

April 25, 2020

Definition: Let *a, b, n* be integers, with $n > 0$, then ***a* is congruent to *b* modulo *n*** if $n \mid (b-a)$. This is most often written $a \equiv b \pmod{n}$. If it is clear from the context of the problem, that all numbers are to be considered mod *n*, you will sometimes see $a \equiv b$ or $a = b$.

***Theorem 16:** Let *a, b, n* be integers, with $n > 0$, then

a) $a \equiv a \pmod{n}$
b) If $a \equiv b \pmod{n}$ then $b \equiv a \pmod{n}$
c) If $a \equiv b \pmod{n}$ and $b \equiv c \pmod{n}$, then $a \equiv c \pmod{n}$

Definition: Let *a, b, n* be integers, with $n > 0$, then the **congruence class of *a* modulo *n*** is the set of all integers congruent to *a* modulo *n*. Sometimes we write $[a]$ or $[a]_n$, and the equivalence class is defined to be $\{b \mid b \in \mathbb{Z} \text{ and } b \equiv a \pmod{n}\}$.

Theorem 17: $[a]_n = [c]_n$ if and only if $a \equiv c \pmod{n}$

***Theorem 18:** If $a \equiv b \pmod{n}$ and $c \equiv d \pmod{n}$ then

a) $a + c \equiv b + d \pmod{n}$
b) $ac \equiv bd \pmod{n}$

Definition: The set of all congruence classes modulo *n* is denoted $\mathbb{Z}_n$, which is called "Z-n" or the "integers mod n" or "mod n numbers". Elements of $\mathbb{Z}_n$ are sometimes written as $[a]_n$ or $[a]$ but usually they are just written *a*. Each congruence class has a simplest form, which is the element of the equivalence class in the range $0 \le a < n$. In most cases, you should give answers to questions in $\mathbb{Z}_n$ in simplest form.

Definition: Two integers are **relatively prime** if their greatest common divisor is 1.

***Theorem 19:** The element $a \in \mathbb{Z}_n$ has a multiplicative inverse $b \in \mathbb{Z}_n$ if and only if a and n are relatively prime.

***Theorem 20:** $\mathbb{Z}_n, +$ is a group (under addition)

Definition: The set of elements of $\mathbb{Z}_n$ that have multiplicative inverses is called U_n. In set notation: $U_n = \{a \in \mathbb{Z}_n \mid ab = 1 \text{ for some } b \in \mathbb{Z}_n\}$

***Theorem 21:** $U_n, \cdot$ is a group (under multiplication)

*** Theorem 22:** $\mathbb{Z}_p{}^* = \{a \in \mathbb{Z}_p \mid a \not\equiv 0\}$, the set of non-zero elements of $\mathbb{Z}_p$, where *p* is prime, is a group under multiplication.

April 25, 2020

Definition/Notation: If *G* is a group with operation written as multiplication, and $a \in G$ then $a^2 = aa$ and $a^n = \underbrace{aa...a}_{\text{n factors}}$ if *n* is a positive integer. $a^n = \underbrace{a^{-1}a^{-1}...a^{-1}}_{|n| \text{ factors}}$ if *n* is a negative integer and $a^0 = e$ where *e* is the identity.

Theorem 23: If *G* is a group and $a \in G$ then $a^n a^m = a^{n+m}$

prove the theorem for the cases:

a) $n = 0$ or $m = 0$
b) $n > 0$ and $m > 0$
c) $n < 0$ and $m < 0$
d) $n > 0$ and $m < 0$, and $n > m$
e) $n > 0$ and $m < 0$, and $n < m$
f) $n < 0$ and $m > 0$, and $n > m$
g) $n < 0$ and $m > 0$, and $n < m$

Definition: The order of a group is the number of elements in the group.

Definition: In a group *G* with element $a \in G$, if $a^n = e$ for some integer $n > 0$, then the element *a* has finite order. If *k* is the smallest positive integer such that $a^n = e$, then *a* has order *k*. If $a^n \neq e$ for every positive integer *n*, then *a* has infinite order.

* **Theorem 24:** If *G* is a group and $a \in G$ such that $a^i = a^j$ for two distinct integers $i \neq j$, then *a* has finite order.

* **Theorem 25:** If *G* is a group and $a \in G$ such that $a^n = e$, then the order of *a* is a divisor of *n*.

***Theorem 26:** If *G* is a group and $a \in G$ such that *a* has order *n*, then $a^i = a^j$ if and only if $n \mid (j - i)$

Definition: In a group *G* with elements $a, b \in G$, the set $< a > \subseteq G$ is the smallest subgroup of *G* that contains *a*, and $< a, b >$ is the smallest subgroup of *G* that contains both *a* and *b*.

* **Lemma 27:** In a group *G* (with the default multiplicative notation for the binary operation), and $a \in G$ then $\{a^n \mid n \in \mathbb{Z}\}$ is a subgroup of G.

Theorem 28: In a group *G* (with the default multiplicative notation for the binary operation), and $a \in G$ then $\{a^n \mid n \in \mathbb{Z}\} = < a >$

Definition: A group *G* is **commutative** if for every pair of elements $a, b \in G$, $ab = ba$. A commutative group is also called an **abelian** group.

Theorem 29: In a group *G*, with element $a \in G$, then $< a >$ is an abelian group.

Definition: In a group *G*, with element $a \in G$, the subgroup $< a >$ is called a **cyclic group**.

April 25, 2020

Theorem 30: If G is a group and $a \in G$ has infinite order, then all of the elements a^n where $n \in \mathbb{Z}$ are distinct.

Definition: Given a group G with operation * and H is a group with operation #, and $f : G \to H$ is a relation that pairs elements of G with elements of H. The relation f is a **function** if each element of G is paired with a unique element of H.

Definition: Given a group G with operation * and H is a group with operation #, and $f : G \to H$ is a function. The function f is called a **homomorphism** if it preserves the group operation, which means for any $a, b \in G$, $f(a * b) = f(a) \# f(b)$

Definition: Given sets S and T, a function $f : S \to T$ is **1-to-1** if for every $a, b \in S$, if $f(a) = f(b)$ then $a = b$. A 1-to-1 function is called an **injection**.

Theorem 31: Given sets S and T, a function $f : S \to T$ is an injection if and only if , for every $t \in T$ the set $f^{-1}(t) = \{s \in S \mid f(s) = t\}$ contains at most one element.

Definition: Given sets S and T, a function $f : S \to T$ is **onto** if for every $t \in T$, there exists an element $s \in S$ such that $f(s) = t$. An onto function is called a **surjection**

Theorem 32: Given sets S and T, a function $f : S \to T$ is a surjection if and only if every $t \in T$ the set $f^{-1}(t) = \{s \in S \mid f(s) = t\}$ contains at least one element.

Definition: A function that is both an injection and a surjection is called a **bijection**.

Definition: Given groups G and H, and function $f : G \to H$, then f is an **isomorphism** if it is a bijective homomorphism.

Theorem 33: A cyclic group with finite order n is isomorphic to the group $\mathbb{Z}_n$ with operation addition.

Theorem 34: A cyclic group with infinite order is isomorphic to the group $\mathbb{Z}$ with order addition.

***Theorem 35:** Given groups G and H, and a homomorphism $f : G \to H$, then $f(G) = \{f(x) \mid x \in G\} \subseteq H$ is a subgroup of H.

April 25, 2020

Definition: A **ring** is a set of elements R together with two binary operations that are denoted as addition (+) and multiplication ($\times$or $\cdot$) with the properties:

1) R is closed under addition: if $a,b \in R$ then $a+b \in R$
2) Addition is associative: if $a,b,c \in R$ then $(a+b)+c = a+(b+c)$
3) Addition is commutative: if $a,b \in R$ then $a+b = b+a$
4) R has an additive identity: there exists an element $0 \in R$ such that $0+a = a$
5) Every element in R has an additive inverse: if $a \in R$ then $-a \in R$ such that $a+-a = 0$
6) R is closed under multiplication: if $a,b \in R$ then $ab \in R$
7) Multiplication is associative: if $a,b,c \in R$ then $(ab)c = a(bc)$
8) Multiplication is distributive over addition: if $a,b,c \in R$ then $a(b+c) = ab+ac$ and $(b+c)a = ba+ca$

Definition: A ring R is a **commutative ring** if multiplication is commutative. That is: if $a,b \in R$ then $ab = ba$

Definition: A ring, R, is a ring with **identity** or a ring with **unity** if it has a multiplicative identity: i.e. If there exists an element $1 \in R$ such that $1 \cdot a = a \cdot 1 = a$ for all $a \in R$

Theorem 36: $\mathbb{Z}_n$ is a commutative ring.

Theorem 37: If $R,+,\cdot$ is a ring, then $R,+$ is an abelian group

***Theorem 38:** If $R,+,\cdot$ is a ring, and $a \in R$ then $a \cdot 0 = 0 \cdot a = 0$ (hint: 0+0=0)

Definition: Given a ring R with identity, then an element $a \in R$ is a **unit** if it has a multiplicative inverse in R: i.e. $a \in R$ is a **unit** if there exists an element $a^{-1} \in R$ such that $a \cdot a^{-1} = a^{-1} \cdot a = 1$

Definition: Given a ring R, then an element $a \in R$ is **zero-divisor** if it is one of a non-zero pair of elements whose product is 0: i.e. $a \in R$ is a **zero-divisor** if there is an element $b \in R$ such that $a \neq 0$ and $b \neq 0$ and $ab = 0$ or $ba = 0$.

(*) Theorem 39: The additive identity of a ring R is unique.

***Theorem 40:** The multiplicative identity of a ring with identity (R) is unique. (Hint: if there were two identities, what would their product be?)

(*) Theorem 41: For any element a of a ring R, the additive inverse of a is unique.

***Theorem 42:** For any unit a of a ring R, the multiplicative inverse of a is unique.

***Theorem 43** Prove that any element a of a ring R can't be both a unit and a zero divisor.

Definition: A commutative ring with identity, R, is an **integral domain** if it has no zero-divisors

Definition: A **field** is a commutative ring with identity, where all of the non-zero elements are units.

Definition: If R is a ring, then a subset $S \subseteq R$ is a subring of R if it is a ring (using the same operations that are defined for R).

Theorem 44: If R is a ring, then a subset $S \subseteq R$ is a subring of R if it satisfies the conditions:

i. S is closed under addition (if $a,b \in S$ then $a+b \in S$)
ii. S is closed under multiplication (if $a,b \in S$ then $ab \in S$)
iii. every element of S has an additive inverse in S (if $a \in S$ then $-a \in S$ where $a + -a = 0$)

* **Theorem 45:** If $a,b \in R$ then $a(-b) = -(ab)$ and $(-a)b = -(ab)$

* **Theorem 46:** If $a \in R$ then $-(-a) = a$

* **Theorem 47:** If $a,b \in R$ then $-(a+b) = -a + -b$

* **Theorem 48:** If $a,b \in R$ then $(-a)(-b) = ab$

Definition: Saying that ring R, has the **multiplicative cancellation property** means: for $a,b,c \in R$, if $ab = ac$ or $ba = ca$ then $b = c$

* **Theorem 49:** A ring R has the multiplicative cancellation property if and only if R has no zero divisors.

* **Theorem 50** If $S \subseteq R$ and $T \subseteq R$ are both subrings of R, then $S \cap T$ is a subring of R.

Definition: If R and S are rings and $f : R \to S$ is a function and $a,b \in R$, then f is a ring **homomorphism** if $f(a+b) = f(a) + f(b)$ and $f(ab) = f(a)f(b)$.

Definition: If R and S are rings and $f : R \to S$ is a function, then f is a ring **isomorphism** if it is a ring homomorphism, and it is one-to-one and onto.

Theorem 51: If R and S are rings, and $f : R \to S$ is a ring homomorphism, and if we name the additive identities of R and S to be 0_R and 0_S respectively, then $f(0_R) = 0_S$

Theorem 52: If R and S are rings, and $f : R \to S$ is a ring homomorphism, and $a \in R$, then $f(-a) = -f(a)$.

Theorem 53: If R and S are rings, and $f : R \to S$ is a ring homomorphism, then $f(R) = \{f(x) \mid x \in R\} \subseteq S$ is a subring of S.

April 25, 2020

Theorem 54: If R is a ring and $a \in R$ then the set $aR = \{ax \mid x \in R\} \subseteq R$ is a subring of R and the set $Ra = \{xa \mid x \in R\} \subseteq R$ is a subring of R.

Theorem 55: Given a ring R, we can adjoin a formal element x to create a ring $R[x]$ of formal polynomials with coefficients in R with the following properties:

- R is a subring of $R[x]$
- If $a \in R$ then $ax = xa$ (note: elements of R commute with x, but they don't necessarily commute with each other)
- Every element has a unique representation as a polynomial.

Definition: The **degree** of a polynomial $p(x) \in R[x]$ is the highest exponent that has a non-zero coefficient.

Theorem 56: If F is a field and $f(x), g(x) \in F[x]$ such that $g(x) \neq 0$ then there exist unique $q(x), r(x) \in F[x]$ such that $f(x) = g(x)q(x) + r(x)$ and $\deg(r(x)) < \deg(g(x))$ or $r(x) = 0$.

Definition: If $f(x), g(x) \in F[x]$, then $f(x) \mid g(x)$ means there exists $h(x) \in F[x]$ such that $g(x) = f(x)h(x)$.

Definition: If R is a ring with identity, then a **monic** polynomial in $R[x]$ is a polynomial whose leading coefficient is 1. (Note: the leading coefficient is the coefficient of the term with the highest power of x)

Definition: If F is a field, and $f(x), g(x) \in F[x]$, then $f(x)$ and $g(x)$ are **associates** if $f(x) = cg(x)$ where $c \in F$ and $c \neq 0$.

Theorem 57: If F is a field and $f(x) \in F[x]$, then $f(x)$ has a unique associate which is a monic polynomial.

Definition: If $f(x), g(x) \in F[x]$ such that not both of f and g are 0, then the **greatest common divisor** of f and g is the monic polynomial of highest degree that divides both $f(x)$ and $g(x)$.

Theorem 58: If F is a field, and $f(x), g(x) \in F[x]$ such that $f(x) \neq 0$ or $g(x) \neq 0$, then there is a unique greatest common divisor $d(x) = \gcd(f(x), g(x))$, and there exist polynomials $u(x), v(x) \in F[x]$ (not necessarily unique) such that $d(x) = u(x)f(x) + v(x)g(x)$

Definition: Let F be a field and let $p(x) \in F[x]$ be a non-constant polynomial, then $p(x)$ is **irreducible** if its only divisors are non-zero constants and its associates.

***Theorem 59 (factor theorem):** If F is a field, $a \in F$ and $f(x) \in F[x]$ then $f(a) = 0$ if and only if $(x - a) \mid f(x)$

Theorem 60: Let F be a field and let $f(x) \in F[x]$ be a non-constant polynomial, then $f(x)$ is factorable into irreducible polynomials, and that factorization is unique up to associates.

April 25, 2020

Theorem 61 (remainder theorem): If F is a field, $a \in F$ and $f(x), g(x) \in F[x]$ such that $\deg(g(x)) = 1$ and $g(a) = 0$. Let $r(x) \in F[x]$ be the remainder polynomial that satisfies $f(x) = g(x)q(x) + r(x)$ and $\deg(r(x)) < \deg(g(x))$ or $r(x) = 0$. Then $r(x)$ is a constant and $f(a) = r(x)$.

Theorem 62 (Fundamental Theorem of Algebra): Every polynomial in $\mathbb{C}[x]$ has a complex root (that is, if $f(x) \in \mathbb{C}[x]$ and $\deg(f(x)) > 0$ then there exists a number $a \in \mathbb{C}$ such that $f(a) = 0$.

Theorem 63 (Corollary to the Fundamental Theorem of Algebra): Every polynomial in $\mathbb{C}[x]$ is factorable into degree 1 polynomials.

…………….

Definition: If $I \subseteq R$ is a subring of R, and if for any $i \in I$ and $r \in R$ then $ir \in I$ and $ri \in I$, then I is called an **ideal**

Theorem 64: If I is a non-empty subset of R, then I is an ideal if:

i. I is closed under addition (if $a, b \in I$ then $a + b \in I$)
ii. Every element of I has an additive inverse in I (if $a \in I$ then $-a \in I$ where $a + -a = 0$)
iii. I absorbs elements of R under multiplication: if $a \in I$ and $r \in R$ then $ir \in I$ and $ri \in I$

***Theorem 65:** If R is a commutative ring and $c \in R$, then $cR = \{cx \mid x \in R\}$ is an ideal in R.

Definition: If R is a commutative ring that has a (multiplicative) identity, and $c \in R$, then $cR = \{cx \mid x \in R\}$ is a **principal ideal** of R. This ideal has two standard representations: in addition to cR the textbook uses the notation: (c) to represent the principal ideal generated by c. This notation is particularly common when talking about principal ideals in a polynomial ring.

Definition: If I is an ideal in a ring R, and $a \in R$ then the **coset** $a + I \subseteq R$ is the set: $a + I = \{a + x \mid x \in I\}$

Theorem 66: If I is an ideal in a ring R, then every element $a \in R$ is in some coset of I, and in particular, $a \in a + I$

Theorem 67: : If I is an ideal in a ring R, and $a + I$ shares an element with $b + I$ then $a + I = b + I$

> *Note:* The contrapositive of theorem 67 says that if the cosets are not equal, then they are disjoint, which means they do not share any elements

Definition: If I is an ideal in a ring R, and $a, b \in R$ then ***a* is congruent to *b* modulo *I*** if $b + (-a) \in I$. We write $a \equiv b \pmod{I}$

April 25, 2020

Theorem 68: If I is an ideal in a ring R, and $a \in R$ then $a \equiv a \pmod{I}$

Theorem 69: If I is an ideal in a ring R, and $a, b \in R$ such that $a \equiv b \pmod{I}$ then $b \equiv a \pmod{I}$

Theorem 70: If I is an ideal in a ring R, and $a, b, c \in R$ such that $a \equiv b \pmod{I}$ and $b \equiv c \pmod{I}$ then $a \equiv c \pmod{I}$

Theorem 71: If I is an ideal in a ring R, and $a \in R$ then $a + I = \{x \mid x \in R \text{ and } a \equiv x\}$

Theorem 72: If I is an ideal in a ring R, and $a, b, c, d \in R$ such that $a \equiv b \pmod{I}$ and $c \equiv d \pmod{I}$ then $a + c \equiv b + d \pmod{I}$.

Note: This is equivalent to: $(a+I)+(b+I) = \{a+i+b+j \mid i, j \in I\} \subseteq (a+b)+I$

Theorem 73: If I is an ideal in a ring R, and $a, b, c, d \in R$ such that $a \equiv b \pmod{I}$ and $c \equiv d \pmod{I}$ then $ac \equiv bd \pmod{I}$

Note: This is equivalent to: $(a+I)(b+I) = \{(a+i)(b+j) \mid i, j \in I\} \subseteq (ab)+I$

Definition: If I is an ideal in a ring R, and, then the set of cosets consists of all of the cosets of I

Theorem 74: If I is an ideal in a ring R, then the set of cosets of I is also a ring, where addition and multiplication are defined by $(a+I)+(b+I) = (a+b)+I$ and $(a+I)(b+I) = (ab)+I$. We call R/I the **quotient ring of *R* mod *I*.** We write $R/I = \{a+I \mid a \in R\}$

Theorem 75: If R and S are rings, and $f : R \to S$ is a ring homomorphism, then $f(0_R) = 0_S$ where 0_R is the additive identity in R, and 0_S is the additive identity in S.

Theorem 76: If R is a ring that has a multiplicative identity 1_R, and S is a field whose multiplicative identity is 1_S, and $f : R \to S$ is a ring homomorphism and there is some $a \in R$ such that $f(a) \neq 0$, then $f(1_R) = 1_S$

Theorem 77: If R and S are rings, and $f : R \to S$ is a ring homomorphism and $a \in R$, then $f(-a) = -f(a)$

Theorem 53/78: If R and S are rings, and $f : R \to S$ is a ring homomorphism, then $f(R) = \{f(x) \mid x \in R\} \subseteq S$ is a subring of S.

Definition: The **kernel** of a function on rings $f : R \to S$ is the set of all elements that map to 0: $\ker(f) = \{x \in R \mid f(x) = 0_S\}$

Theorem 79: If R and S are rings, and $f : R \to S$ is a ring homomorphism, then $\ker(f) \subseteq R$ is an ideal in R.

Theorem 80 (First Isomorphism Theorem): If R and S are rings, and $f : R \to S$ is a surjective (onto) ring homomorphism, then $R / \ker(f) \cong S$ with isomorphism $\phi(r + \ker(f)) = f(r)$ where $r + \ker(f) \in R / (\ker(f))$

Theorem 81: If $f(x) \in F[x]$ is an irreducible polynomial with coefficients in the field F, then $F[x]/(f(x))$ is a field.

Definition: If F is a field subfield of $\mathbb{C}$, and $\alpha \in \mathbb{C}$, then $F(\alpha)$ is the smallest subfield of $\mathbb{C}$ that contains both F and α

Theorem 82: If $f(x) \in F[x]$ is an irreducible polynomial with coefficients in a field F such that $\mathbb{Q} \subseteq F \subseteq \mathbb{C}$, and $\alpha \in \mathbb{C}$ such that $f(\alpha) = 0$ then $\phi : F[x]/(f(x)) \to F(\alpha)$ defined by $\phi\big(g(x) + \big(f(x)\big)\big) = g(\alpha)$ for every $g(x) + \big(f(x)\big) \in F[x]/\big(f(x)\big)$ is an isomorphism