May 8, 2019

Abstract Algebra Notes

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 $aa^{-1} = a^{-1}a = e$.

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 1: 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 1 by explaining why all 4 of the group properties must be true for H.

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

May 8, 2019

Theorem 6 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 $m > 0$
e) $n < 0$ and $m < 0$

Theorem 7: Function composition is associative.

Theorem 8: The D_3, the set of symmetry transformations of an equilateral triangle, is a group, where the group operation is function composition.

Unless you are specifically asked to prove one of these is a group (eg. Thm 8), you may assume that all of these are groups:

$\mathbb{C}$ = complex numbers (with addition)

D_n = dihedral group of degree *n* (symmetries of a regular *n*-gon, with operation function composition), for integers $n \geq 3$

S_n = permutation group of degree *n* = symmetric group of degree *n* (permutations of *n* elements, where *n* is a positive integer, with operation function composition)

$M_2 = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \middle| a,b,c,d \in \mathbb{R} \right\}$ = real valued 2x2 matrices (with addition)

Additionally, you may assume that we know that multiplication is associative for $\mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{Z}$ and M_2, and multiplication is commutative for $\mathbb{R}, \mathbb{C}, \mathbb{Q}, \mathbb{Z}$

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.

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

Lemma 10: 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.

May 8, 2019

Theorem 11: 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 12: In a group G, with element $a \in G$, then $< a >$ is an abelian group.

Definition: For two integers $n, m \in \mathbb{Z}$, the following statements are equivalent:

- $n \mid m$ (say: "*n* divides *m*")
- m is evenly divisible by n
- n is a factor of m
- $m = nk$ for some integer $k \in \mathbb{Z}$

Definition: Two elements, numbers, groups, functions etc. are **distinct** if they are not equal. This is a common word in math, and not specific to Abstract Algebra.

Theorem 13: 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 14: 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 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 15: Given sets S and T, a function $f : S \to T$, the following conditions are equivalent:

- For every $a, b \in S$, if $f(a) = f(b)$ then $a = b$
- For every $a, b \in S$ if $a \neq b$ then $f(a) \neq f(b)$
- 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 $f(s) = t$.

Theorem 16: Given sets S and T, a function $f : S \to T$, the following conditions are equivalent:

- For every $t \in T$, there exists an element $s \in S$ such that $f(s) = t$.
- For every $t \in T$ the set $f^{-1}(t) = \{s \in S \mid f(s) = t\}$ contains at least one element.

Definition: Given groups G and H, and function $f : G \to H$, then f is an **isomorphism** if it is a 1-to-1 and onto homomorphism.

May 8, 2019

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

Theorem 17: 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 18 (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 19 (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 20 (1.4): Let $a, b, c \in \mathbb{Z}$ such that $a \mid bc$ and $\gcd(a,b) = 1$ then $a \mid c$

Theorem 20.5: 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 21: An integer p be an integer such that $p \ne 0, \pm 1$ is prime if and only of it is irreducible.

Theorem 22 (1.6): Let p be a prime integer and let $p \mid a_1 a_2 ... a_n$ then p divides at least one of the factors a_i.

Theorem 23 (1.7): Every integer n except $0, \pm 1$ is a product of primes.

Theorem 24 (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

$$n = p_1 p_2 ... p_r \text{ and } n = q_1 q_2 ... q_s$$

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 $f : \{1, 2, ... s\} \to \{1, 2, ... s\}$ is a permutation, and $p_i = \pm q_{f(i)}$)

May 8, 2019

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 25: 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 26: $[a]_n = [c]_n$ if and only if $a \equiv c \pmod{n}$

Theorem 27: 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: 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 $ab = ba$

Theorem 28: $\mathbb{Z}_n$ is a commutative ring.

May 8, 2019

Theorem 29: If $R,+,\cdot$ is a ring, then $R,+$ is an abelian group

Theorem 29.5: If $R,+,\cdot$ is a ring, and $a \in R$ then $a \cdot 0 = 0 \cdot a = 0$ (hint: 0+0=0)

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 $a \in R$

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

Theorem 31: For any non-zero element $a \in \mathbb{Z}_n$, prove that $\gcd(a,n) = 1$ if and only if *a* is a unit.

Theorem 32: Given that $p > 0$ is a prime integer, prove that every non-zero element of $\mathbb{Z}_p$ is a unit.

Theorem 33: For any non-zero element $a \in \mathbb{Z}_n$, prove that $\gcd(a,n) > 1$ if and only if *a* is a zero-divisor.

Theorem 34: The additive identity of a ring *R* is unique.

Theorem 35: The multiplicative identity of a ring with identity (*R*) is unique.

Theorem 36: For any element *a* of a ring *R*, the additive inverse of *a* is unique.

Theorem 37: For any unit *a* of a ring *R*, the multiplicative inverse of *a* is unique.

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 38: 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 39: If $a,b \in R$ then $a(-b) = -(ab)$ and $(-a)b = -(ab)$

Theorem 40: If $a \in R$ then $-(-a) = a$

Theorem 41: If $a,b \in R$ then $-(a+b) = -a + -b$

Theorem 42: 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 43: A ring *R* has the multiplicative cancellation property if and only if *R* has no zero divisors.

Theorem 44: If $S \subseteq R$ and $T \subseteq R$ are both subrings of *R*, then $S \cap T$ is a subring of *R*.

Theorem 45: 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*.

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 46: 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 47: 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 48: If *R* and *S* are rings, and $f : R \to S$ is a ring homomorphism, then $f(R) = \{f(x) \mid x \in R\}$ is a subring of *S*.

Theorem 49: 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 50: If *D* is an integral domain, and $f(x), g(x) \in D[x]$, then $\deg(f(x) \cdot g(x)) = \deg(f(x)) + \deg(g(x))$

Theorem 51: If *D* is an integral domain, then $D[x]$ is also an integral domain.

May 8, 2019

Theorem 52: If F is a field, then $F[x]$ is an integral domain, and the units in $F[x]$ are the non-zero constants in F.

Theorem 53: If F is a field, and $f(x), g(x) \in F[x]$ such that $g(x) \neq 0$, then there exist unique polynomials $q(x)$ and $r(x)$ such that $f(x) = g(x)q(x) + r(x)$ where either $\deg(r(x)) < \deg(g(x))$ or $r(x) = 0$.

Definition: If F is a field, and $f(x), g(x) \in F[x]$, then $f(x)$ **divides** $g(x)$, or $f(x)$ **is a factor of** $g(x)$, or $g(x)$ **is a multiple of** $f(x)$ means that there is an $h(x) \in F[x]$ such that $g(x) = f(x)h(x)$. We write $f(x) \mid g(x)$.

Theorem 54: If F is a field, and $f(x), g(x) \in F[x]$ such that $f(x) \neq 0$, $c \in F$ such that $c \neq 0$, and if $f(x) \mid g(x)$ then $cf(x) \mid g(x)$

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 of a polynomial is the coefficient of the term with the highest exponent of x.

Definition: If F is a field, and $f(x), g(x) \in F[x]$ 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 55: 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 $d(x) = u(x)f(x) + v(x)g(x)$

Theorem 56: 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 a monic polynomial $d(x)$ is the greatest common divisor of f and g if and only if

- $d(x) \mid f(x)$ and $d(x) \mid g(x)$
- If $c(x) \mid f(x)$ and $c(x) \mid g(x)$ then $c(x) \mid d(x)$

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 $c \neq 0$.

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.

Definition: Let F be a field and let $p(x) \in F[x]$ be a non-constant polynomial, then $p(x)$ is **prime** if for any $f(x), g(x) \in F[x]$ such that $p(x) \mid f(x)g(x)$ then $p(x) \mid f(x)$ or $p(x) \mid g(x)$

Theorem 58: Let F be a field and let $p(x) \in F[x]$ be a non-constant polynomial, then $p(x)$ is prime if and only if it is irreducible.

Theorem 58: 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.