University of California San Diego

MATH 100 Notes

Textbook: *Abstract Algebra by I.N. Herstein (3rd ed.)*

Organized by Ray Tsai

MATH 100A

Definition.

A nonempty set G is said to be a *group* if in G there is defined an operation $*$ such that:

(a) $a, b \in G$ implies that $a * b \in G$. (*Closure*)

(b) Given $a, b, c \in G$, then $a * (b * c) = (a * b) * c$. (*Associativity*)

(c) There exists a special element $e \in G$ such that $a * e = e * a = a$ for all $a \in G$. (*Identity element*)

(d) For every $a \in G$ there exists an element $b \in G$ such that $a * b = b * a = e$. (*Inverse element*)

Lemma 1.3.1.

If $h : S \to T$, $g : T \to U$, and $f : U \to V$, then $f \circ (g \circ h) = (f \circ g) \circ h$.
Note: overpowered for checking associativity

Definition.

A group G is said to be a *abelian* if $a * b = b * a$, for all $a, b \in G$.

Lemma 2.2.1.

If G is a group, then:

(a) Its identity element is *unique*.

(b) Every $a \in G$ has a *unique* inverse $a^{-1} \in G$.

(c) If $a \in G$, $(a^{-1})^{-1} = a$.

(d) For $a, b \in G$, $(ab)^{-1} = b^{-1}a^{-1}$.

Lemma 2.2.2.

In any group G and $a, b, c \in G$, we have:

(a) If $ab = ac$, then $b = c$.

(b) If $ba = ca$, then $b = c$.

Definition.

A nonempty subset, H, of a group G is called a *subgroup* of G if, relative to the product in G, H itself forms a group.

Lemma 2.3.1.

A nonempty subset $A \subset G$ is a subgroup of G if and only if A is closed with respect to the operation of G and, given $a \in A$, then $a^{-1} \in A$.

Definition.

The *cyclic subgroup of* G generated by a is a set $\{a^i \mid i \in \mathbb{Z}\}$. It is denoted (a).

Lemma 2.3.2.

Suppose that G is a group and H a nonempty *finite* subset of G closed under the product in G. Then H is a subgroup of G.

Corollary.

If G is a finite group and H a nonempty subset of G closed under multiplication, then H is a subgroup of G.

Definition.

A relation is $\sim$ on a set S is called an *equivalence relation* if, for all $a, b, c \in S$, it satisfies:

(a) $a \sim a$. (*reflexivity*)

(b) $a \sim b$ implies that $b \sim a$. (*symmetry*)

(c) $a \sim b, b \sim c$ implies that $a \sim c$. (*transitivity*)

Definition.

If $\sim$ is an equivalence relation on S, then $[a]$, the *class* of a, is defined by $[a] = \{b \in S \mid b \sim a\}$.

Theorem 2.4.1.

If $\sim$ is an equivalence relation on S, then $S = \cup[a]$, where this union runs over one element from each class, and where $[a] \neq [b]$ implies that $[a] \cap [b] = \emptyset$. That is, $\sim$ partition S into equivalence classes.

Theorem 2.4.2 (Lagrange's Theorem).

If G is a finite group and H is a subgroup of G, then the order of H divides the order of G.

Theorem 2.4.3.

A group G of prime order is cyclic.

Definition.

If G is finite, then the *order* of a, written $o(a)$, is the *least positive integer* m such that $a^m = e$.

Theorem 2.4.4.

If G is finite and $a \in G$, then $o(a) \mid |G|$.

Theorem 2.4.5.

If G is a finite group of order n, then $a^n = e$ for all $a \in G$.

Theorem 2.4.6.

$\mathbb{Z}_n$ forms a cyclic group under the addition $[a] + [b] = [a + b]$.

Definition.

The *Euler φ-function*, $\varphi(n)$, is defined by $\varphi(1) = 1$ and, for $n > 1$, $\varphi(n) =$ the number of positive integers m with $1 \leq m < n$ such that $(m, n) = 1$.

Theorem 2.4.7.

U_n forms an abelian group, under the product $[a][b] = [ab]$, of order $\varphi(n)$.

Theorem 2.4.8 (Euler).

If a is an integer relatively prime to n, then $a^{\varphi(n)} \equiv 1 \mod n$.

Corollary (Fermat).

If p is a prime and $p \nmid a$, then

$$a^{p-1} \equiv 1 \mod p.$$

For any integer b, $b^p \equiv b \mod p$.