An Abstract Algebra Primer

<u>Monoids</u>

A *monoid* (M, *) is a set M with a binary operation * that satisfies the following properties:

1. (Closure) For all a, b in M, the result of $a * b$ is also in M.
2. (Associativity) For all a, b and c in M, $(a * b) * c = a * (b * c)$.
3. (Identity) There exists an element e in M such that for all a in M, $e * a = a * e = a$.

<u>Groups</u>

A *group* (G, *) is a monoid with the added property:

1. (Inverse) For each a in G, there exists an element b in G such that $a * b = b * a = e$, where e is the identity element.

In addition, if (G, *) satisfies the **Commutative Property** (for all a and b in G, $a * b = b *$ a), we call it either a *Commutative Group* or an *Abelian Group*.

<u>Rings</u>

A *ring* (R, +, *) is a set, R, equipped with two binary operations + and *, called addition and multiplication, such that for all a, b, c in R, the following properties hold:

1. (Closure in +) $a + b$ is in R;
2. (Associative in +) $(a + b) + c = a + (b + c)$;
3. (Commutative in +) $a + b = b +$ a;
4. (Identity for +) There exists 0 in R, such that $0 + a = a + 0 = a$;
5. (Inverse for +) There exists $-a$ in R such that $a + (-a) = (-a) + a = 0$
6. (Commutative in *) $a * b = b * a$;
7. (Associative in *) $(a * b) * c = a * (b * c)$;
8. (Identity for *) There exists 1 in R, such that $(a * 1) = (1 * a) = a$;
9. (Distribute * over +) $a * (b + c) = (a * b) + (a * c)$.

<u>Fields</u>

A *field* (F, +, *) is a Ring with the added property that for each element a in F, there exists an unique element b in F such that $a * b = b * a = 1$, the multiplicative identity.

<u>In summary:</u>

(1) a monoid is closed, associative and has an identity in one operation;
(2) an abelian group is a monoid with inverses and commutativity;
(3) a ring is an abelian group in one operation and a monoid in another operation with a distributive property;
(4) a field is a group in both operations.