Exercise 12

January 13, 2004

1.

Definition 1 *A binray operation on a non empty set G is a function $+ : G \times G \to G$.*

Definition 2 *An operation $+$ on a set G is associative if*

$$(a + b) + c = a + (b + c)$$

for all $a, b, c \in G$.

Definition 3 *A group is a pair $(G, +)$ of a non empty set G equipped with an associative operation $+$, and containing an element e such that:*

- *$e + a = a = a + e$ for all $a \in G$*
- *for every $a \in G$, there is an element $b \in G$ with*

  $$a + b = e = b + a$$

Definition 4 *Let $(G, +)$ be a finite group. A nonempty subset S of G is a subgroup of G if $a, b \in S$ imply $a + b \in S$.*

Prove the following theorem (it appears in many books on group theory).

Theorem 5 *If G is a finite group and S is a subgroup of G, then the size of S (number of elements) devides the size of G.*

Hint: For $t \in G$ define the set $St = \{s + t : s \in S\}$ (St is called a right coset of S in G). Show that any two right cosets of S in G are either identical or disjoint, and that the size (number of elements) of all right cosets is the same.

2.

1. Show that the set $Z_n = \{0, 1, \ldots, n - 1\}$ with addition modulo n forms a group.

2. Denote by Z_n^* the set of elements in Z_n that are relatively prime to n. Show that the set Z_n^* with multiplication modulo n forms a group.

3. Let $(G, *)$ be a finite group. Show that for every $a \in G$ the set of all powers of a $(a^0, a^1, a^2, \ldots)$ is a subgroup of G. Powers of an element are defined as follows: $a^0 = 1$, and for $k > 1$ $a^k = a^{k-1} * a$.

4. Use (1)-(3) and Lagrange's theorem to prove Fermat's theorem

   Theorem 6 (Fermat) *If p is a prime and a is an integer, then $a^p \equiv a (mod\ p)$*