Duke Math Meet 2016: Power Round
Finite Groups

During this round, we will learn about finite groups. There are **Five** problems in total, each divided into partial parts. Some of the later problems may need earlier results, so feel free to use any previous parts even if you are not able to prove them yet. You can also use any given theorems or definitions, starting with the following:

Definition 1.1: A *binary operation* $*$ on a set S is a composition law: $S \times S \to S, (a, b) \mapsto (a * b) \in S$. That is, we apply this operation to two elements in S and get another element in S. Some properties that a binary operation on a set S may have:

1. **Associativity** : $(a * b) * c = a * (b * c)$

2. **Commutativity** : $a * b = b * a$

3. **Identities** : The identity e (if there is one) satisfies $e * a = a * e = a$ for all $a \in S$ and it is unique.

4. **Inverse** : Assume that the identity e exists. For all element $a \in S$, the unique inverse of a, denoted by a^{-1}, is an element in S such that $a * a^{-1} = a^{-1} * a = e$.

Example 0: Addition and multiplication on the set of real numbers $\mathbb{R}$ are binary operations.

Definition 1.2: A *group* G is a set with a binary operation $*$, which is associative and has identity element, and such that every element in G has an inverse.

Some Notations:

i) We use $(G, *)$ to refer to the group and its binary operation.

ii) The product of n ordred elements $a_1, \ldots, a_n$ is $a_1 * a_2 * \cdots * a_n$.

iii) For powers of an element, we use the same notation for powers of integers. For example, $a * a = a^2$; $a * a * \cdots * a = a^n$, where we apply operation $*$ $(n - 1)$ times.

Hence, $a^{m+n} = a^m * a^n$, $(a^m)^n = a^{mn}$, and $(a^n)^{-1} = a^{-n}$, also $a^0 = e$.

Example 1: The set of positive real numbers $\mathbb{R}^+$ with multiplication forms a group whose identity is 1, and the inverse of an element g is $1/g$.

Definition 1.3: A group G is *finite* if it has finitely many elements. The *Order* of a finite group G is the total number of elements in G, and it is denoted by $|G|$.

Definition 1.4: The order of an element g in G, denoted by $ord_G(g)$, is the smallest positive integer n such that $g^n = e$, the identity.

Definition 1.5: H is a subgroup of G if H is a subset of G such that if a, b are in H then $a*b$ is in H, and the inverse of an element of H is in also H. In this case, $(H, *)$ is a group.

Definition 1.6: If g is an element of the finite group $(G, *)$ then $\langle g \rangle$ is the set of elements in G of the form $\{e, g, g^2, ...\}$.

Example 2: Let $T = \{1, 2, \ldots 6\}$ be the group of nonzero residues with multiplication module 7. For example $2 * 3 = 6$ and $4 * 5 = 6$ since $20 = 2 * 7 + 6$.

Since $2^2 = 4$ and $2^3 = 1$ modulo 7, the order of 2 in R is 3. Also 2 and 4 are inverses of each other.

Example 3: The set $M = \{2^i \mid i = 0, \pm 1, \pm 2 \ldots\}$ is a Group with usual multiplication and the identity is $2^0 = 1$.

Problem 1:

a. (2 pts) Find the inverses and orders of 3, 5, and 6 in T in Example 2.

b. (2 pts) Describe $\langle 2 \rangle$ and $\langle 3 \rangle$ in T in Example 2.

Problem 2: Consider a group $(G, *)$.

a. (2 pts) Prove that if $g \in G$ has order n, then any multiple m of n also satisfies $g^m = e$.

b. (2 pts) Prove that if d is a positive integer such that $g^d = e$, then d is divisible by $ord_G(g)$. (Hint: Use division with remainder.)

Theorem 1 (Lagrange): Let G be a finite group. Let H be a subgroup of G.
Then: $|H|$ divides $|G|$.

Problem 3: Let g be an element with order $ord_G(g) = k$ in a finite group $(G, *)$.

a. (2 pts) Prove that $\langle g \rangle$ is a subgroup of G and $|\langle g \rangle| = k$.
(Hint: $g^x = g^y$ implies $g^{|x-y|} = e$.)

b. (1 pts) Prove that k divides $|G|$ and deduce that $g^{|G|} = e$, for all $g \in G$.
(Hint: use Theorem 1.)

c. (2 pts) Prove that if k is a prime, then for all $1 \leqslant i < k$, g^i also has order k.
(Hint: use Problem 1b.)

d. (2 pts) Prove that if k is a prime and b is another element with order k, then $\langle g \rangle = \langle b \rangle$ or $\langle g \rangle \cap \langle b \rangle = e$.

Next, we will explore the conjugacy maps within a finite group $(G, *)$.

Definition 2.1: For each element $h \in G$, the conjugacy map by h is the function $f_h : G \to G, g \mapsto f_h(g) = h * g * h^{-1}$. Hence, f_h sends elements in G to elements in G.

Problem 4: Let $(G, *)$ be a finite group, g be an element of order k.

a. (1 pts) Prove that $f_h(g_1 * g_2) = f_h(g_1) * f_h(g_2)$ for all $g_1, g_2 \in G$.

b. (2 pts) Prove that $f_h(g)$ also has order k, for all $h \in G$.

c. (2 pts) Prove that the conjugacy map f_h is a bijection from G to G for all h.

Finally, we will explore Sylow's theorems on subgroups of order a power of a prime.

Definition 2.2: A subgroup T of G is *normal* if and only if for all $h \in G$, f_h maps T to itself, in other words, $f_h(T) = \{f_h(g) \mid \forall g \in T\} = T$.

Definition 2.3: A finite group G is *simple* if and only if the only normal subgroups in G are $\{e\}$ and G.

Example 4: In Example 2, $\langle 2 \rangle$ is normal in $(R, *)$ where $*$ is the multiplication modulo 7, and R is not simple.

Definition 2.4: Given a finite group $(G, *)$ and a prime p, where $|G| = p^k m$ and $p \nmid m$.
A *Sylow p-subgroup* of G is a subgroup of order p^k in G.

Theorem 2 (Sylow): Let $n_p(G)$ be the number of Sylow p-subgroups in G, where p is a prime, $|G| = p^k m$ and $p \nmid m$. We have the following:
i) p divides $(n_p(G) - 1)$. (Hence, $n_p(G)$ is nonzero.)
ii) $n_p(G)$ divides m.
iii) Any conjugacy map f_h will map a Sylow p-subgroup to another Sylow p-subgroup.

Problem 5: Let G be a finite group.
a. (1 pts) Let P be a Sylow p-subgroup of G, g be any non-identity element in P. Prove that g has order a power of p.
b. (2 pts) Say $|G| = 56$ and G is simple. How many Sylow 7-subgroups does G have? How many elements of order 7 does G have?
c. (2 pts) Say $|G| = 520$. Prove that G is not simple.