PROBLEM SET 3
DUE: Mar.10

Problem 1

(1). Compute the centralizer of the group $GL_n(F)$, where F is a field.

Let G be a group and S a subset of G. Then

(2). Show that $Z_S \lhd N_S$, where Z_S and N_S are the **centralizer** and **normalizer** of S respectively.

We say two subsets A and B are conjugate in G if there exists an element $g \in G$ such that $A = gBg^{-1}$, and two elements x and y are conjugate if $\{x\}$ and $\{y\}$ are conjugate.

(3). Show that conjugation in G is an equivalence relation.

A conjugacy class is the equivalence class under this equivalence relation.

(4). Show that the number of conjugate sets to S is equal to the index $[G : N_S]$ of the normalizer of S.

(5). Use (4) to prove the **class formula**:

$$|G| = \sum_{x \in C} [G : Z_x],$$

where C is a set of representatives for the distinct conjugacy classes, and the sum is taken over all $x \in C$.

(6). Let H be a proper subgroup of a finite group G. Show that G can not be written as the union of all the conjugates of H.

Problem 2

We say an element $a \in G$ is of order (or period) n ($n \in \boldsymbol{Z}$), if n is the smallest positive integer such that $a^n = e$, denoted by $ord(a) = n$. If for any positive integer n, $a^n \neq e$, then we say a has infinite order (or period).

(1). Let G ba an abelian group and $a, b \in G$. If $ord(a) = m$, $ord(b) = n$, then show that $ord(ab) = [m, n]$, where $[m, n]$ denotes the least common multiple of m and n.

(2). Show that the same conclusion does not hold for a nonabelian group.

(3). Prove that if $H \lhd G$, $[G : H] = n$, then for any $g \in G$, we have $g^n \in H$.

*(4). Given a group $G = \{g_1, g_2, ..., g_n\}$ with n odd. Set $x = g_1 g_2 ... g_n$. Show that x is an element of the commutator subgroup of G.

Problem 3

Prove the following basic properties of cyclic groups:

(1). Show that a cyclic group is either isomorphic to $\boldsymbol{Z/nZ}$ *or* $\boldsymbol{Z}$ ($n \in \boldsymbol{Z}$).

(2). Show that a subgroup of a cyclic group is also cyclic.

(3). Let G be a finite cyclic group of order n. Then for any positive integer d dividing n, there exists a unique subgroup of order d.

*(4). Conversely, let G be a finite group of order n. If for any positive integer d dividing n, there exists at most one subgroup of order d, then G must be cyclic. (Hint: use the following identity:

$$n = \sum_{d|n} \varphi(d),$$

and see problem 5 for the definition of φ).

Problem 4

(1). Let $(G, *)$ be a finite abelian group containing no elements $a \neq e$ with $a^2 = e$. Evaluate $a_1 * a_2 * .... * a_n$ where $a_1, a_2, ..., a_n$ is a list with no repetitions, of all elements of G.

(2). Then prove the **Wilson's theorem**: If p is a prime, then

$$(p-1)! \equiv -1 \bmod p$$

(Hint: The nonzero elements of $\boldsymbol{Z}/p\boldsymbol{Z}$ form a multiplicative group).

Problem 5

Definition. The **Euler φ-function** is defined as follows:

$$\varphi(1) = 1; if \quad n > 1, \quad then \quad \varphi(n) = |\{k : 1 \leq k \leq n \quad and \quad (k, n) = 1\}|.$$

(1). If $G =< a >$ is cyclic of order n, then a^k is also a generator of G

if and only if $(k,n)=1$. Conclude that the number of generators of G is $\varphi(n)$.

(2). Let $G=<a>$ have order rs, where $(r,s)=1$. Show that there are unique $b,c\in G$ with b of order r, c of order s, and $a=bc$.

(3). Use (2) to prove that if $(r,s)=1$, then $\varphi(rs)=\varphi(r)\varphi(s)$.

(4). If p is a prime, then $\varphi(p^k)=p^k-p^{k-1}=p^k(1-1/p)$.

(5). Finally, if the distinct prime divisors of n are $p_1,p_2,.....,p_t$, then

$$\varphi(n)=n(1-\frac{1}{p_1})(1-\frac{1}{p_2})....(1-\frac{1}{p_t})$$

.

Problem 6 (problem 5 continued)(**Euler's theorem**)

If $(r,s)=1$, then $s^{\varphi(r)}\equiv 1 mod r$. (Hint: The order of the multiplicative group of $\boldsymbol{Z}/n\boldsymbol{Z}$ is $\varphi(n)$).

Problem *7

Use the Euler's theorem and Wilson's theorem to show that the equation $x^2+y^2=p$ is solvable in $\boldsymbol{Z}$, where p is a prime and $p\equiv 1$ mod 4. (This result will be used in the ideal theory, as a famous example).

Problem 8

The **dihedral group** D_{2n} is the symmetric group of regular n-gon. It can be characterized by

$$D_{2n}=<\sigma,\tau|\sigma^n=\tau^2=e,\quad \tau\sigma\tau=\sigma^{-1}>,$$

where $\sigma$is the counterclockwise rotation of degree $\frac{2\pi}{n}$, and τ is the certain reflection.

Prove that the dihedral group D_{2n} is isomorphic to the semidirect product of $\boldsymbol{Z}/2\boldsymbol{Z}$ and $\boldsymbol{Z}/n\boldsymbol{Z}$.

Problem 9

We say a normal tower of a group G

$$G=G_0\triangleright G_1\triangleright G_2\triangleright ....\triangleright G_n=0$$

is a composition series, if all the factors G_i/G_{i+1} are simple.

(1). Give a composition series of $GL_2(\boldsymbol{F_2})$ where $\boldsymbol{F_2}$ is the finite field of two elements.

(2). One should regard the Jordan-Holder theorem as a unique factorization theorem. Then use the theorem to prove the **Fundamental Theorem of Arithmetic**: The primes and their multiplicities occurring in the factorization of an integer $n \geq 2$ are uniquely determined by n. (Hint: write down a composition series of the cyclic group $\boldsymbol{Z}/n\boldsymbol{Z}$.)