1 Homework 7.

1. The Frattini subgroup $\Phi(G)$ of a group G is the intersection of all of its maximal subgroups. Suppose G is a finite group. Notice that under an automorphism of G, a maximal subgroup is sent to a maximal subgroup, and so the Frattini subgroup $\Phi(G)$ is a characteristic subgroup.

   (a) Suppose H is a subgroup of G and $H\Phi(G) = G$. Prove that $H = G$.

   (b) Suppose $S \subseteq G$. Prove that $\langle S \rangle = G$ if and only if $\langle \pi(S) \rangle = G/\Phi(G)$ where $\pi : G \to G/\Phi(G)$ is the natural quotient map.

   (c) Prove that $\Phi(G)$ is nilpotent.

   (d) Prove that G is nilpotent if and only if $G/\Phi(G)$ is nilpotent.

   (**Hint.** (1) Suppose to the contrary that H is a proper subgroup, and let M be a maximal subgroup of G which contains H. Argue why $H\Phi(G) \subseteq M$.

   (2) Suppose P is a Sylow p-subgroup of $\Phi(G)$. Argue why $G = N_G(P)\Phi(G)$ (The Frattini argument). Deduce that $G = N_G(P)$.

   (3) Suppose Q is a Sylow p-subgroup of G. Assuming $G/\Phi(G)$ is nilpotent, deduce that $Q\Phi(G)$ is a normal subgroup of G. Use the Frattini argument and show that $N_G(Q)Q\Phi(G) = G$. Obtain that $N_G(Q) = G$.)

2. Suppose P is a finite group and $|P| = p^n$ where p is prime and n is a positive integer. Let $\mathrm{Max}(P)$ be the set of all maximal subgroups of P.

   (a) Prove that for all $M \in \mathrm{Max}(P)$, $P/M \simeq \mathbb{Z}/p\mathbb{Z}$.

   (b) Prove that $P/\Phi(P)$ is isomorphic to a subgroup of $(\mathbb{Z}/p\mathbb{Z})^{|\mathrm{Max}(P)|}$.

   (c) Prove that $\Phi(P) = P^p[P, P]$ where

   $$P^p[P, P] := \{x^p y \mid x \in P, y \in [P, P]\}.$$

   (d) Suppose $P = \langle S \rangle$ and a proper subset of S does not generate P. Prove that $|S| = \dim_{\mathbb{Z}/p\mathbb{Z}}(P/P^p[P, P])$.

   (**Hint**. (1) Since P is nilpotent, M is a proper subgroup of $N_G(M)$. Deduce that M is a normal subgroup. Use the correspondence theorem and obtain that G/M has no non-trivial subgroup. Deduce that $G/M \simeq \mathbb{Z}/p\mathbb{Z}$.

(2) Consider the group homomorphism,

$$\pi : P \to \prod_{M \in \mathrm{Max}(P)} P/M, \quad \pi(x) := (xM)_{M \in \mathrm{Max}(P)}$$

Argue why the kernel of π is $\Phi(P)$. Deduce that $P/\Phi(P)$ is isomorphic to a subgroup of $(\mathbb{Z}/p\mathbb{Z})^{|\mathrm{Max}(P)|}$.

(3) Use part (b) and deduce that $x^p \in \Phi(P)$ and $[x_1, x_2] \in \Phi(P)$ for all $x, x_1, x_2 \in P$. Obtain that $P^p[P,P] \subseteq \Phi(P)$.

(4) Notice that $P/[P,P]$ is an abelian group, and so $\overline{x} \mapsto \overline{x}^p$ is a group homomorphism from $P/[P,P]$ to itself. The image of this group homomorphism is $P^p[P,P]/[P,P]$. Hence $P^p[P,P]$ is a normal subgroup of P. Consider

$$V := P/P^p[P,P].$$

Notice that V is a finite abelian group and every non-trivial element has order p. Use the additive notation for V. Notice that V can be viewed as a vector space over $\mathbb{Z}/p\mathbb{Z}$. Then every non-zero element $v \in V$ is part of a $\mathbb{Z}/p\mathbb{Z}$-basis of V. Hence there is a subspace W of codimension 1 which does not contain v. Notice that $V/W \simeq \mathbb{Z}/p\mathbb{Z}$, and so W is a maximal subgroup of V. Deduce that for all $x \notin P^p[P,P]$ there is $M \in \mathrm{Max}(P)$ such that $x \notin M$. Hence $\Phi(P) \subseteq P^p[P,P]$.

(5) Notice that $P = \langle S \rangle$ implies that $\pi(S)$ generates $P/\Phi(P)$. By part (c), $P/\Phi(P)$ is a vector space over $\mathbb{Z}/p\mathbb{Z}$. Hence the $\mathbb{Z}/p\mathbb{Z}$-span of $\pi(S)$ is $P/\Phi(P)$. Therefore there is a $\mathbb{Z}/p\mathbb{Z}$-basis $\overline{S}'$ of $P/\Phi(P)$ which is a subset of $\pi(S)$. Suppose $S' \subseteq S$ is such that $|S'| = |\overline{S}'|$ and $\overline{S}' = \pi(S')$. Argue why $\langle S' \rangle = P$. Deduce that $S' = S$, and obtain that $|S| = \dim_{\mathbb{Z}/p\mathbb{Z}}(P/\Phi(P))$.)

(**Remark.** Part (d) implies that every two minimal generating set of P have the same cardinality. This statement is false if P is not a finite p-group. For instance $G := \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z}$ is a cyclic group and so it can be generated by 1 element, but the set $\{(1,0),(0,1)\}$, which has 2 elements, is also a minimal generating set of G.)

3. Suppose G is a finite group and H is a non-trivial subgroup of G.

(a) Show that there exists a function $f : \mathrm{Syl}_p(H) \to \mathrm{Syl}_p(G)$ such that for all $\overline{P} \in \mathrm{Syl}_p(H)$, $\overline{P} = f(\overline{P}) \cap H$. Deduce that

$$|\mathrm{Syl}_p(H)| \le |\mathrm{Syl}_p(G)|.$$

(b) Suppose G does not have a non-trivial normal p-subgroup. Suppose $\overline{P}$ is a non-trivial p-subgroup of G. Prove that

$$|\mathrm{Syl}_p(N_G(\overline{P}))| < |\mathrm{Syl}_p(G)|.$$

(**Hint.** To prove the second part, use the contrary assumption and deduce that f is surjective. Use the surjectivity of f and show that the intersection of all Sylow p-subgroups of G is a non-trivial subgroup.)

(**Remark.** The intersection of all the Sylow p-subgroups of G is denoted by $O_p(G)$. This is the largest normal p-subgroup of G; this means $O_p(G) \trianglelefteq G$ and if $\overline{P}$ is a normal p-subgroup of G, then $\overline{P} \subseteq O_p(G)$. In the above argument, you are showing that if $|\mathrm{Syl}_p(H)| = |\mathrm{Syl}_p(G)|$, then

$$O_p(H) = O_p(G) \cap H.)$$

4. Suppose G is a group of order $p^n q$ where p and q are primes. Prove that G is solvable.

(**Hint.** Use the following steps.

(a) First show that it is enough to argue why a group of order $p^n q$ is not a non-abelian simple group.

(b) Suppose to the contrary that there exists a non-abelian simple group G of order $p^n q$.

(c) Prove that G has exactly q Sylow p-subgroups.

(d) Let $\overline{P}$ be maximal among the intersections of pairs of Sylow p-subgroups. Suppose $\overline{P} \neq \{1\}$, and let $H := N_G(\overline{P})$. Prove that H has at least 2 Sylow p-subgroups.

(e) Prove that $|\mathrm{Syl}_p(H)| = q$. Get a contradiction using Problem 1.

(f) Let $Q := G \setminus (\bigcup_{P\in \mathrm{Syl}_p(G)}(P\setminus\{1\})$. Prove that $|Q| = q$, and deduce that G has a unique Sylow q-subgroup. Get a contradiction.)

(**Remark.** Burnside used character theory of finite groups to prove that a group of order $p^n q^m$ is solvable.)

5. Suppose $G = \langle a, b\rangle$ and $a^2 = b^2 = 1$.

   (a) Prove that G is solvable.

   (b) Show that G is not necessarily finite.

   (**Hint.** Let $N = \langle ab\rangle$. Prove that $a, b \in N_G(N)$ and deduce that $N \trianglelefteq G$.)

6. Suppose G is a group and $a, b \in G$. Suppose

$$ab^2a^{-1} = b^3 \quad \text{and} \quad ba^2b^{-1} = a^3.$$

   Prove that $a = b = 1$.

   (**Hint.** Consider $a^2b^4a^{-2}$ and prove that $a \in C_G(b^4)$.)

   (**Remark.** Given a set of relations R and two words w_1 and w_2, we can ask whether there exists an algorithm to decide if $w_1 = w_2$. This is called *the word problem*. Novikov proved that in general the answer to this question is negative. This is in contrast to vector spaces, where we can use the reduced row process and find out if a vector is 0. The concept of Gröbner basis gives us an affirmative answer to the commutative ring theoretic analogue of this question.)