Problem 1

$H, K \leq G$ and $|H|, |K| < \infty$. Also, $(|H|, |K|) = 1$.

Show $H \cap K = 1$.

$H \cap K$ is a subgroup of G. Moreover, $H \cap K$ is a subgroup of both H and K. So by Lagrange's theorem, $|H \cap K|$ divides both $|H|$ and $|K|$. But since the only common divisor of $|H|$ and $|K|$ is 1, $|H \cap K| = 1$. So $H \cap K$ contains only the identity element.

Problem 2

Use Lagrange's thm to prove Fermat's little thm:
if p is prime, $a^p \equiv a \pmod p$ $\forall a \in \mathbb{Z}$.

$(\mathbb{Z}/p\mathbb{Z})^\times$ is a group of order $p-1$. By corollary 9,

$\forall a \in \mathbb{Z}/p\mathbb{Z}$, $a^{|(\mathbb{Z}/p\mathbb{Z})^\times|} = 1$. This is equivalent to ✓ (well said)

$\forall a \in \mathbb{Z}$, $a^{|(\mathbb{Z}/p\mathbb{Z})^\times|} \equiv 1 \pmod p$.

$$a^{p-1} \equiv 1$$

$$a^{p-1} \cdot a \equiv 1 \cdot a$$

$$a^p \equiv a \quad ✓$$

3) Since $N \trianglelefteq G$, for $H \leq G$, $NH \leq G$. This means, by Lagrange's theorem, $|NH| \mid |G|$. If $|N| = |H|$, then $|NH| = \frac{|N|^2}{|N \cap H|} \mid |G|$, meaning $|N|^2 \mid |N|[G:N]|N \cap H|$. Thus $|N| \mid [G:N]|N \cap H|$. Since $\gcd(|N|, [G:N]) = 1$, $N \nmid [G:N]$. Thus, it must be the case that $|N \cap H| = |N|$. This would mean that $N = H$, if $|H| = |N|$. Thus, N is a unique subgroup of order $|N|$. ✓

5

Perfect.

4. Let $H \trianglelefteq G$ of prime index p. Then let $K \leq G$, consequently $K \leq N_G(H) = G$. So by the second isomorphism theorem, we know $H \cap K \trianglelefteq K$. Therefore, by Lagrange's theorem, $|H \cap K|$ divides $|H|$. Also by the second isomorphism theorem $HK \leq G$, so by Lagrange's theorem $|HK|$ divides $|G|$. Now we break the problem into two cases.

Case 1: $K \leq H$, great we are done. ✓

Case 2: K is not a subgroup of H. We already know from the pre-case portion of the problem that $KH \leq G$. Therefore, the following quotient divides:

$$\frac{|G|}{|HK|} = \frac{|G|}{|H||K|/|H \cap K|} \qquad \text{(corollary 15)} \checkmark$$

$$= \frac{[G : H]}{|K|/|H \cap K|} \qquad \text{(definition of index)} \checkmark$$

$$= \frac{p}{|K|/|H \cap K|} \checkmark$$

✓

Since $|H \cap K|$ divides $|H|$, $|K|/|H \cap K|$ must be either 1 or p. However, since K is not a subgroup of H, $H \cap K \neq H$ and, therefore, $|H \cap K| < |K|$. ✓ Therefore, $|K|/|H \cap K| = |K/H \cap K|$ must equal p. So $[K : K \cap H] = p$. ✓ Furthermore, this means

$$\frac{|G|}{|HK|} = \frac{p}{|K|/|H \cap K|} = \frac{p}{p} = 1 \checkmark$$

So G has the same cardinality as HK, a subgroup(so also subset). This can only be true if $G = HK$. So we are done. great.

Question 5.

Proof. .

1. Let $z_1, z_2 \in \mu_{p^\infty}(\mathbb{C})$. Then

$$\begin{aligned}\varphi(z_1 z_2) &= (z_1 z_2)^p \\ &= z_1^p z_2^p \\ &= \varphi(z_1)\varphi(z_2)\end{aligned}$$

Hence φ is a homomorphism.

2. Let $z \in G$. Then there exists a natural number n such that $z^{p^n} = 1$. Let us consider the polynomial $q(x) = x^p - z$, which has root $w \in \mathbb{C}$ such that $(w^p)^{p^n} = w^{p^{n+1}} = 1$. So w must be in G. Moreover, since w is a root of $q(x)$, then $\varphi(w) = w^p = z$. Therefore φ is surjective.

3. The kernel of φ is $\{z \in \mathbb{C} \mid z^p - 1\}$ which we know to be nontrivial by the first fundamental theorem of algebra. And by the first isomorphism theorem, $\mu_{p^\infty}(\mathbb{C})/\ker\varphi \simeq \operatorname{im}\varphi$. And $\operatorname{im}\varphi = \mu_{p^\infty}(\mathbb{C})$ since φ is surjective.

□

6. First let us suppose that $\varphi \circ i = 1$. We want to show that there can exist $\bar{\varphi} \circ \pi \circ i = \varphi \circ i$. If we let $\bar{\varphi}$ be the trivial homomorphism, then the can see that for all $n \in N$ $\varphi \circ i(n) = 1 = \bar{\varphi} \circ \pi \circ i(n)$. The trivial homomorphism is a homomorphism trivially, so we have one direction of implication.

Then assume that there exists $\bar{\varphi}$, a homomorphism that makes the diagram commute (i.e. $\bar{\varphi} \circ \pi \circ i = \varphi \circ i$). From here we would like to show that $\varphi \circ i = 1$. Observe that for $n \in N$, $\pi(n) = \pi \circ i(n) = nN = N$. Then, $\bar{\varphi}(N) = 1$ because N is a normal subgroup of G. So $\varphi \circ i = \bar{\varphi} \circ \pi \circ i = 1$. Thus $\bar{\varphi}$ exists and is a homomorphism if and only if $\varphi \circ i = 1$.

7. Note that by the second isomorphism theorem, since $M \leq N$, (N) and

7) Define a map $\varphi: G \to (G/M) \times (G/N)$ by $\varphi(g) = (gM, gN)$.
Since $G = MN$, for $g \in G$, $g = mn$ for some
$m \in M$ and $n \in N$. Then for $g, g' \in G$, $\varphi(gg') =$
(5) $(gg'M, gg'N) = (gMg'M, gNg'N) = (gM, gN)\cdot(g'M, g'N)$
$= \varphi(g)\varphi(g')$. Thus, φ is homomorphic. Note for $a \in M \cap N$, a word.
"is a homomorphism" — homomorphic is not
$\varphi(a) = (aM, aN) = (M, N)$. Thus, $\varphi(M \cap N) = (M, N)$, ~~or~~
the identity of $(G/M \times G/N)$. As proven previously,
there must exists a unique homomorphic mapping
$\bar{\varphi}: G/M \cap N \to G/M \times G/N$, such that $\varphi = \bar{\varphi} \circ \pi$, where
π is the natural projection $\pi: g \to g(M \cap N)$. Now
take an element $g \in G$. Since $G = MN$, $g = mn$ for
some $m \in M$ and $n \in N$. Thus, for an arbitrary
element $(gM, g'N)$ in $G/M \times G/N$, $(gM, g'N) = (mnM, m'n'N)$
$= (nM, m'N)$ for some $n \in M$ and $n \in N$. Thus, picking
not necessarily the same n
$a \in G$ to be $a = m'n$, we find $\varphi(a) = \varphi(m'n) = \varphi(m')\varphi(n)$
$= (m'M, m'N)\cdot(nM, nN) = (nM, m'M) = (nnM, m'n'M) = (gM, g'N)$.
Thus, φ is surjective, meaning $\text{im}\,\varphi = G/M \times G/N$.
Since no other elements of G satisfy yes.
the property $(gM, gN) = (M, N)$ except for $g \in M \cap N$

$\mathbb{Z}/mn\mathbb{Z} \cong \mathbb{Z}/m\mathbb{Z} \times \mathbb{Z}/n\mathbb{Z}$. good.

B) We have a group G which is solvable. This means there exists a composition series $1 = G_0 \trianglelefteq G_1 \trianglelefteq \dots \trianglelefteq G_s = G$ such that G_{i+1}/G_i is abelian for $i = 0, 1, \dots, s-1$. Take a subgroup H of G. Let $H_i = H \cap G_i$. All of these are subgroups since H and G_i are subgroups, ✓ and are all therefore nonempty since $1 \in H$ and $1 \in G_i$. Since $G_i \trianglelefteq G_{i+1}$, $H_i = H \cap G_i \trianglelefteq H \cap G_{i+1} = H_{i+1}$. Furthermore, $\frac{H_{i+1}}{H_i} = \frac{H_{i+1}}{H_{i+1} \cap G_i}$. By the second isomorphism theorem, $\frac{H_{i+1}}{H_i} \cong \frac{H_{i+1} G_i}{G_i}$. Since all elements of H_{i+1} are ✓ in G_{i+1}, and the same holds for G_i, $\frac{H_{i+1}}{H_i} \cong \frac{H_{i+1} G_i}{G_i} \leq \frac{G_{i+1}}{G_i}$. Since $\frac{G_{i+1}}{G_i}$ is abelian, $\frac{H_{i+1} G_i}{G_i}$ is abelian, ✓ meaning $\frac{H_{i+1}}{H_i}$ is abelian. Thus, any subgroup $H \leq G$ is solvable if G is solvable. ✓ Now consider the quotient group H/B, where $B \trianglelefteq H$ and $H \leq G$. As proven previously, H is solvable. Thus, for subgroups H_i in the composition series of H, $B \trianglelefteq H_i$. By ✓ the fourth isomorphism theorem, since $H_i \leq H_{i+1}$, ✓ $H_i/B \leq H_{i+1}/B$. Furthermore, $(H_{i+1}/B)/(H_i/B) \cong H_{i+1}/H_i$ ✓ by the third isomorphism theorem. Since H_{i+1}/H_i ✓ is abelian, $(H_{i+1}/B)/(H_i/B)$ is abelian. Thus, H/B is solvable. Therefore, any quotient group of G is solvable. □ ✓

5

9. $\epsilon(\sigma) = \pm 1$. Furthermore, ϵ is a homomorphism, so $\epsilon(\sigma^2) = \epsilon(\sigma)\epsilon(\sigma) = (-1)(-1) = 1$ or $= (1)(1) = 1$. Therefore regardless of whether or not σ is odd or even, σ^2 is even.

Problem 10. Show that $S_n = \langle (1\ 2), (1\ 2\ 3\ \cdots\ n) \rangle$ for all $n \geq 2$.
As shown in class, any permutation σ can be expressed as a product of transpositions, so it suffices to show that $\langle (1\ 2), (1\ 2\ 3\ \cdots\ n) \rangle$ generates an arbitrary transposition. Let $(a\ b)$ be the desired transposition. Note that $(1\ a)(1\ b)(1\ a) = (a\ b)$. So if we can transpose $(1\ a)$ for all $a \leq n$, the result follows. In fact, $(1\ 2)(1\ 2\ 3\ \cdots\ n) = (2\ 3\ \cdots\ n)$, and in general powers of this allow us to shift all elements except for 1 by arbitrary amounts. If we do this until 1 occupies position $a+1$, insert one more $(1\ 2\ 3\ \cdots\ n)$, and then cycle through again until a reaches position 1, then we have exchanged 1 and a. The result follows. σ K

Question 11.

Proof. .

1. I define $\varphi : A_4 \to M$.
2. $\sigma \in A_4$ can take three forms:
   (a) $\sigma = 1$ in which case $\varphi(1) = 1$. you are confusing σ and $\varphi(\sigma)$ right idea two...
   (b) $\sigma = (a\ b\ c)$. Here σ keeps one element constant and rotates the other three elements. There are three such σs in A_4, so define $\varphi(\sigma) = r^i$ where r the rigid motion where one vertex is fixed and the other three rotate positions. $r \in \{1, 2, 3\}$. good.

(c) $\sigma = (a\ b)(c\ d)$. Define $\varphi(\sigma) = s_{ab}r^i$, where s_{ab} represents the swap of vertices a and b, i.e. if a is our fixed vertex, move b to a's position and now consider b to be the fixed vertex. Then perform the necessary rotations remaining in the formula under the same rules as the previous step.

3. That was wordy and detailed, so here is the simpler form:

   (a) An even permutation can encode one of two things:

   (b) First, keep one element constant and rotate the other three, i.e $\sigma = (b\ c\ d)$. On the tetrahedron, simply keep vertex a in place and rotate b, c and d. Note that the identity element is keeping one element constant and not rotating the other three.

   (c) Second, swap the two elements, and then swap two different elements, i.e. $\sigma = (a\ b)(c\ d)$. On the tetrahedron, begin by considering vertex a as fixed. Then rotate such that a and b swap places. Now consider b as the fixed vertex. Keeping b's position constant, rotate the other three vertices until c and d are the other's original position. Hence we can think of this as a reflection and then rotation.

4. There are 12 elements in both A_4 and M, and during the construction of φ, it's clear that φ is a homomorphism and bijective. The fact that φ is a homomorphism follows from the fact that the rotations and reflections that permutations map to are composable.

Nice.

Easy to see; hard to write out. □