Problem 1:

Let G be a group, with $H < G$ and $K < G$.

Let $HK < G$.

Then for all $x, y \in HK$, $xy^{-1} \in HK$.

Let $h \in H$ and $k \in K$. Then $h^{-1} \in H$ and $k^{-1} \in K$. Also, $e \in H$ and $e \in K$. Then $h^{-1}e = h^{-1}, ek^{-1} = k^{-1}, ee = e \in HK$. Because HK is a subgroup, this means that $h^{-1}k^{-1} \in HK$. So, by the subgroup criterion, $e(h^{-1}k^{-1})^{-1} = ekh = kh \in HK$.

To summarize, if $h \in H$ and $k \in K$, $kh \in HK$. That is, any element of KH is contained in HK. Similarly, any element of HK is contained in KH

So $HK = KH$ if HK is a subgroup.

Now, let $HK = KH$.

Then let $x, y \in HK$. There are $h_1, h_2 \in H$, $k_1, k_2 \in K$ such that $h_1k_1 = x$ and $h_2k_2 = y$.

Now, $HK = KH$. So $xy^{-1} = h_1k_1k_2^{-1}h_2^{-1} \in HKKH = HKH = HHK = HK$

So if $x, y \in HK$, then $xy^{-1} \in HK$. This means that HK satisfies the subgroup criterion; HK is a subgroup.

Thus, $HK < G$ if and only if $KH = HK$.

Problem 2:

Let G be a group and $H \trianglelefteq G$ and $K \trianglelefteq G$, such that $H \cup K = \{e\}$.

Part a:

Let $h \in H$, $k \in K$.

Because K is normal, $hkh^{-1} \in K$.

Thus, $hkh^{-1}k^{-1} \in K$.

But because H is normal, $kh^{-1}k^{-1} \in H$.

So $hkh^{-1}k^{-1} \in H$.

So $hkh^{-1}k^{-1} \in H \cup K$, which means that $hkh^{-1}k^{-1} = e$.

So $hkh^{-1} = k$, which means that $hk = kh$.

So $hk = kh$ for all $h \in H$, $k \in K$.

Part b:

From the above, it is clear that $HK = KH$.(If this is not clear: let $x \in HK$. Then $x = hk$ for some $h \in H$, $k \in K$. But this means that $x = kh$.

So $x = kh$ for some $k \in K$, $h \in H$; that is, $x \in KH$. Similarly, if $x \in KH$, then $x \in HK$.)

Moving on, from this fact and problem 1, it follows that HK is a subgroup of G.

Now, let $\phi : H \times K \to HK$ be given by $\phi((h, k)) = hk$.

We show that ϕ is an isomorphism:

First, ϕ is a homomorphism:

Let $(a, b), (c, d) \in H \times K$.

Then

$$\begin{aligned} \phi((a,b)(c,d)) &= \phi((ac, bd)) \\ &= acbd \\ &= abcd \quad \text{(this follows from part a)} \\ &= \phi((a,b))\phi((c,d)) \end{aligned}$$

To summarize the above, $\phi((a, b)(c, d)) = \phi((a, b))\phi((c, d))$ for all $(a, b), (c, d) \in H \times K$. That is, ϕ is a homomorphism.

Next, ϕ is one-to-one:

Let $(a, b) \in \ker(\phi)$. Then $ab = e$. In other words, $a = b^{-1}$. This implies that $a \in K$, which would mean that $a = e$. This means that $b = e$.

So $\ker(\phi) = \{e\}$. This means that ϕ is one-to-one.

(If a homomorphism, ϕ, is not one-to-one, then there are two distinct elements (x, y) that ϕ maps to the same thing (z) so there is an element (xy^{-1}) that ϕ maps to e...So the kernel would have more than one thing in it. Take the contrapositive, and you get the above line. (I can't recall if we've done this in class yet...))

Last ϕ is onto:

Let $x \in HK$. Then $x = hk$ for some $h \in H$, $k \in K$. So $x = \phi((h, k))$ for some $h \in H$, $k \in K$.

Thus, there is an isomorphism from $H \times K$ to HK. That is, $H \times K \cong HK$.

Problem 3:

First, Q_8 is non-Abelian. Here is a display of this fact:

$$\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} = \begin{bmatrix} i & 0 \\ 0 & -i \end{bmatrix}$$
$$\begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix} \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = \begin{bmatrix} -i & 0 \\ 0 & i \end{bmatrix}$$

However, all of Q_8's subgroups are normal.

Because $8 = 2 \times 2 \times 2$, any subgroup of Q_8 has order 1,2,4, or 8.

Any subgroup of order 1,4, or 8 is trivially normal, from the discussion in class. (For order 1, the subgroup is necessarily just $\{e\}$. For order 8, the subgroup is necessarily just Q_8. For order 4, we apply the fact that subgroups of order "half the order of the original group" are normal.) It only remains to show that the subgroups of order 2 are normal.

Now, there is only one subgroup of order 2 in Q_8; it is $\{I, -I\}$. This is clear because there is only one element of order 2 in Q_8, and any subgroup of order 2 has to have exactly one element of order 2 (which is trivial from Cayley's theorem... elements of a group must have order dividing the group, and there can only be one element of order 1 (e). So there has to be an element of an order other than 1...there must be an element of order 2. But e has to be in the subgroup, so there's an element of order 1. And because there's only two elements, one of them is e and the other is the element of order 2).

Now, $\{I, -I\}$ is normal:

Let $A \in Q_8$.

Recall that I and $-I$ commute with every matrix.

This means that $AIA^{-1} = IAA^{-1} = II = I$.

And also that $A(-I)A^{-1} = (-I)AA^{-1} = (-I)I = -I$.

So for all $A \in Q_8$ and $B \in \{I, -I\}$, $ABA^{-1} \in \{I, -I\}$. That is, $\{I, -I\}$ is normal.

So all of Q_8's subgroups of order 1, 2, 4, and 8 are normal. That is, all of Q_8's subgroups are normal even though Q_8 isn't abelian.

Problem 4:

Consider $\langle s \rangle < \langle s, r^2 \rangle < D_4$.

Now, $\langle s, r^2 \rangle = \{e, s, r^2, sr^2\}$ has order 4; it is normal in D_4.

Also, $\langle s \rangle$ has order 2; it is normal in $\langle s, r^2 \rangle$.

However, $\langle s \rangle$ is not normal in D_4: $rsr^{-1} = sr^3r^{-1} = sr^2$, and $sr^2 \notin \langle s \rangle$.

So $\langle s \rangle \trianglelefteq \langle s, r^2 \rangle \trianglelefteq D_4$, but $\langle s \rangle$ isn't a normal subgroup of D_4.

Problem 5:

Note: I will suppress the overline notation in this problem. That is, for this problem consider $\overline{a/p^i}$ and a/p^i to be the same thing. Moreover, I am using + as the operation, because this makes the problem more natural.

Part a:

First, $\mathbb{Z}_{p^\infty}$ is infinite:

For each $x \in \mathbb{N}$, $1/p^x \in \mathbb{Z}_{p^\infty}$.

That is, there is an injection of $\mathbb{N}$ into $\mathbb{Z}_{p^\infty}$. So there's an injection of some infinite set into $\mathbb{Z}_{p^\infty}$...that means that $\mathbb{Z}_{p^\infty}$ is infinite.

Second, $\mathbb{Z}_{p^\infty}$ is a subgroup of $\mathbb{Q}/\mathbb{Z}$:

First, we point out that $\mathbb{Q}/\mathbb{Z}$ is a group; $\mathbb{Q}$ is a group, and $\mathbb{Z}$ is an abelian subgroup of $\mathbb{Q}$. This means that $\mathbb{Z}$ is normal in $\mathbb{Q}$.

Now, we apply the subgroup criterion to show that $\mathbb{Z}_{p^\infty}$ is a subgroup of $\mathbb{Q}/\mathbb{Z}$; let $x, y \in \mathbb{Z}_{p^\infty}$.

Then $x = a/p^i$ for some $a \in \mathbb{Z}$, $i \geq 0$.

Also, $y = b/p^j$ for some $b \in \mathbb{Z}$, $j \geq 0$.

So $x + y^{-1} = a/p^i - b/p^j = \frac{ap^j - bp^i}{p^{i+j}}$. That is, $x + y^{-1} = c/p^k$ for some $c \in \mathbb{Z}$, $k \geq 0$. So $x + y^{-1} \in \mathbb{Z}_{p^\infty}$.

So applying the subgroup criterion, $\mathbb{Z}_{p^\infty}$ is a subgroup of $\mathbb{Q}/\mathbb{Z}$.

Last, $\mathbb{Z}_{p^\infty}$ is abelian:

Let $x, y \in \mathbb{Z}_{p^\infty}$.

Then $x = a/p^i$ for some $a \in \mathbb{Z}$, $i \geq 0$.

Also, $y = b/p^j$ for some $b \in \mathbb{Z}$, $j \geq 0$.

This means that

$$\begin{aligned}
x + y &= a/p^i + b/p^j \\
&= \frac{ap^j + bp^i}{p^{i+j}} \\
&= \frac{bp^i + ap^j}{p^{i+j}} \\
&= b/p^j + a/p^i \\
&= y + x
\end{aligned}$$

So for all $x, y \in \mathbb{Z}_{p^\infty}$, $x + y = y + x$.

So $\mathbb{Z}_{p^\infty}$ is an infinite abelian subgroup of $\mathbb{Q}/\mathbb{Z}$. That means that $\mathbb{Z}_{p^\infty}$ is an infinite abelian group.

Part b:

Let $H < \mathbb{Z}_{p^\infty}$ with $H \neq \mathbb{Z}_{p^\infty}$.

Part (i):

First, there is an element $1/p^n \in H$, for some $n \in \mathbb{N}$; the identity is of the form $1/p^0$.

Next, there is a largest $n \in \mathbb{N}$ such that $1/p^n \in H$:

Assume not.

Now, if $1/p^N \in H$, then $1/p^n \in H$ for all $n < N$; because H is a subgroup, $1/p^N \in H$ implies that $1/p^{N-1} = p/p^N \in H$. Similarly, $1/p^{N-2}$,$1/p^{N-3}$...and $1/p^{N-N}$ are all in H.

But there is no largest $n \in \mathbb{N}$ such that $1/p^n \in H$. So by the above line, for every $n \in \mathbb{N}$, $1/p^n \in H$ (because we can just pick a sufficiently large $n \in \mathbb{N}$ and apply the above line to it...).

But we know that H is a subgroup; this means that $a/p^n \in H$ for all $ain\mathbb{Z}$, $n \in \mathbb{N}$ (either add $1/p^n$ a times if $a \geq 0$, or add $-1/p^n$ $-a$ times if $a < 0$). In other words, $a/p^i \in H$ for all $a \in \mathbb{Z}$ and $i \geq 0$.

And the above line means that $H = \mathbb{Z}_{p^\infty}$, which we assumed to not be the case.

Last, $H = \langle 1/p^n \rangle$:

Let $x \in H$.

Then $x = a/p^i$ for some $a \in \mathbb{Z}$, $i \in \mathbb{N}$.

If $x = 0$, then $x \in \langle 1/p^n \rangle$.

Else, we can reduce the above fraction so that a and p are relatively prime (if we don't have it fully reduced, we can just reduce the fraction until it is in that form or until we wind up with an integer...in which case, $x = 0$).

Now, we know (from number theory) that there are $r, s \in \mathbb{Z}$ such that $ra + sp^i = 1$.

Consider rx;

$$\begin{aligned} rx &= ra/p^i \\ &= ra/p^i + sp^i/p^i \\ &= (ra + sp^i)/p^i \\ &= 1/p^i \end{aligned}$$

This means that if $x \in H$ is such that $x = a/p^i$, then $1/p^i \in H$. Because we know that there is a largest n such that $1/p^n \in H$, this means that $i \leq n$.

So if $x \in H$, then if we take $x = a/p^i$, we have that $x = ap^j/p^n$ for some $j \geq 0$. That means that $x \in \langle 1/p^n \rangle$;

So we have that $H \subset \langle 1/p^n \rangle$. But because $1/p^n \in H$ and H is a subgroup, this means that $H \supset \langle 1/p^n \rangle$. So we have that $H = \langle 1/p^n \rangle$.

So, $H = \langle 1/p^n \rangle$ for some $n \geq 0$.

Moving on, $\langle 1/p^n \rangle \cong \mathbb{Z}_{p^n}$ (Here, I guess that $\mathbb{Z}_{p^n} = \{a/p^n : a \in \mathbb{Z}\}$.):

Consider the map $\phi : \langle 1/p^n \rangle \to \mathbb{Z}_{p^n}$ given by $a/p^n \mapsto a/p^n$. (Note that this is just the identity map.)

First, ϕ is a homomorphism:

Let $x, y \in \langle 1/p^n \rangle$. Then

$$\begin{aligned} \phi(x + y) &= x + y \\ &= \phi(x) + \phi(y) \end{aligned}$$

Next, ϕ is one-to-one:

Let $x, y \in \langle 1/p^n \rangle$ be such that $\phi(x) = \phi(y)$.

Then

$$\begin{aligned} \phi(x) &= \phi(y) \\ x &= y \end{aligned}$$

Last, ϕ is onto:

Let $x \in \mathbb{Z}_{p^n}$. Then $\phi(x) = x$. So there is a $y \in \langle 1/p^n \rangle$ such that $\phi(y) = y$.

So ϕ is a bijective homomorphism; it is an isomorphism. That means that $\langle 1/p^n \rangle \cong \mathbb{Z}_{p^n}$.

To summarize the above, we have shown that $H = \langle 1/p^n \rangle \cong \mathbb{Z}_{p^n}$

Part (ii):

First, we point out that H is normal, because this is an abelian group. That means that $\mathbb{Z}_{p^\infty}/H$ is defined.

Moving on, we exhibit an isomorphism from $\mathbb{Z}_{p^\infty}$ to $\mathbb{Z}_{p^\infty}/H$.

Consider $\phi : \mathbb{Z}_{p^\infty} \to \mathbb{Z}_{p^\infty}/H$ given by $x \mapsto \overline{x/p^n}$.

Now, ϕ is a homomorphism:

Let $x, y \in \mathbb{Z}_{p^\infty}$. Then:

$$\begin{aligned} \phi(x + y) &= (x + y)/p^n \\ &= x/p^n + y/p^n \\ &= \phi(x) + \phi(y) \end{aligned}$$

So $\phi(x+y) = \phi(x) + \phi(y)$; ϕ is a homomorphism.

Also, ϕ is one-to-one:

Let $x \in \ker(\phi)$. Then $x/p^n \in H$. So $x/p^n = a/p^n$ for some $a \in \mathbb{Z}$. This means that $x \in \mathbb{Z}$, and we are working in $\mathbb{Q}/\mathbb{Z}$; this means that $x = 0$.

We already know that $\ker(\phi) = \{0\}$ implies that ϕ is one-to-one if ϕ is a homomorphism. So because ϕ is a homomorphism with $\ker(\phi) = \{0\}$, ϕ is one-to-one.

Last ϕ is onto:

Let $y \in \mathbb{Z}_{p^\infty}/H$. Then there is an $x \in \mathbb{Z}_{p^\infty}$ such that $\overline{x} = y$. Now, $\phi(xp^n) = \overline{x} = y$. So there is an $x \in \mathbb{Z}_{p^\infty}$ such that $\phi(x) = y$.

So for all $y \in \mathbb{Z}_{p^\infty}/H$, there is an $x \in \mathbb{Z}_{p^\infty}$ such that $\phi(x) = y$.

So ϕ is onto.

Thus, ϕ is a bijective homomorphism; it is an isomorphism. That means that $\mathbb{Z}_{p^\infty} \cong \mathbb{Z}_{p^\infty}/H$.