① Prove that if $G = \langle a \rangle$ and H is any group, then every homomorphism $f: G \longrightarrow H$ is completely determined by $f(a) \in H$.

For $x \in f(G)$ we have $x = f(b)$ for $b \in G = \langle a \rangle$, so $b = a^n$. Hence $x = f(a^n)$.

Prove that $f(a^n) = f(a)^n$ for all $n \in \mathbb{Z}$. There are three cases: $n > 0$, $n = 0$, and $n < 0$. For this last case, use $f(a^{-1}) = f(a)^{-1}$.

② What is $\mathrm{Aut}(\mathbb{Z}/m\mathbb{Z})$ for arbitrary $m \in \mathbb{Z}^+$?

For $\alpha \in \mathrm{Aut}(\mathbb{Z}/m\mathbb{Z})$, by problem ① it is determined by $\alpha(\bar{1}) \in \mathbb{Z}/m\mathbb{Z}$. Check that $\alpha(\bar{1})$ must be a unit (because $\bar{1}$ is a unit). For every unit $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$, we can define:

$$\begin{aligned} \alpha_{\bar{a}}: \mathbb{Z}/m\mathbb{Z} &\longrightarrow \mathbb{Z}/m\mathbb{Z} \\ \bar{1} &\longmapsto \bar{a} \end{aligned}$$

Check that $\alpha_{\bar{a}} \neq \alpha_{\bar{b}}$ if and only if $\bar{a} \neq \bar{b}$. Check that $\alpha_{\bar{a}} \in \mathrm{Aut}(\mathbb{Z}/m\mathbb{Z})$ for every unit $\bar{a} \in \mathbb{Z}/m\mathbb{Z}$.

Check that:

$$\begin{aligned} \alpha: (\mathbb{Z}/m\mathbb{Z})^\times &\longrightarrow \mathrm{Aut}(\mathbb{Z}/m\mathbb{Z}) \\ \bar{a} &\longmapsto \alpha_{\bar{a}} \end{aligned}$$

is a bijective group homomorphism.

③ a) Let G be a group and $\{H_i\}_{i \in I}$ a family of subgroups. State and prove a condition that will imply that $\bigcup_{i \in I} H_i$ is a subgroup.

b) Give an example of a group G and a family of subgroups $\{H_i\}_{i \in I}$ with

$$\bigcup_{i \in I} H_i \neq \left\langle \bigcup_{i \in I} H_i \right\rangle.$$

a) Suppose that $\{H_i\}_{i\in I}$ contains its least upper bound H. Then $H = \bigcup_{i\in I} H_i$.

b) Take $G = \mathbb{Z}/6\mathbb{Z}$, $H_1 = \langle 3\rangle$, $H_2 = \langle 2\rangle$, then $H_1 \cup H_2 = \{0,2,3,4\}$. Now:

$2+3=5 \notin H_1 \cup H_2$ but $5 \in \langle H_1 \cup H_2\rangle$.

④ Prove that S_n has order $n!$.

Let $\sigma \in S_n$. We have n choices for $\sigma(1)$, $n-1$ choices for $\sigma(2)$, $n-2$ choices for $\sigma(3), \dots$, 2 choices for $\sigma(n-1)$, 1 choice for $\sigma(n)$. Formalize this with induction.

⑤ a) Prove that the relation $a \sim b \Leftrightarrow a-b \in \mathbb{Z}$ is a congruence relation on $\mathbb{Q}$.

b) Prove that the set $\mathbb{Q}/\mathbb{Z}$ is an infinite abelian group.

a) Check that this is reflexive, symmetric, and transitive.

If $a_1 \sim a_2$ and $b_1 \sim b_2$, check that $(a_1+b_1) \sim (a_2+b_2)$.

b) We have seen in class that a) means that $\mathbb{Q}/\mathbb{Z}$ is well defined and abelian because $\mathbb{Q}$ is abelian. To see that $\mathbb{Q}/\mathbb{Z}$ is infinite, check that

$\frac{1}{m} + \mathbb{Z} = \overline{\frac{1}{m}}$ and $\frac{1}{n} + \mathbb{Z} = \overline{\frac{1}{n}}$ are equal in $\mathbb{Q}/\mathbb{Z}$ if and only if $m=n$.

Then $\mathbb{Q}/\mathbb{Z}$ has infinitely many elements.

⑥ If G is a group and $a,b \in G$ with $bab^{-1} = a^r$ for some $r \in \mathbb{N}$, prove that

$b^i a b^{-i} = a^{r^i}$ for all $i \in \mathbb{N}$.

Use induction. This is true for $i=0$. Suppose that it is true for some $i>0$.

Then $b^{i+1} a b^{-(i+1)} = b(b^i a b^{-i})b^{-1} = b a^{r^i} b^{-1}$ by induction hypothesis. Now:

$$b a^{r^i} b^{-1} = b a \cdots a b^{-1} = b a (b^{-1} b) a (b^{-1} b) \cdots (b^{-1} b) a (b^{-1} b) a b^{-1} = (b a b^{-1})^{r^i} \underset{\substack{\uparrow \\ \text{we are told so}}}{=} (a^r)^{r^i} = a^{r^{i+1}}.$$

⑦ Let $Q_8 = \langle A, B \rangle$ with $A = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}$ and $B = \begin{bmatrix} 0 & i \\ i & 0 \end{bmatrix}$. Show that Q_8 is a <u>non</u>-abelian group of order 8.

Note that A, A^2, A^3 are different, and $A^4 = \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}$ the identity element in Q_8.

Now $BA = A^3 B$, so we can move all the A's to the left, all the B's to the right, and every element in Q_8 is of the form $A^i B^j$ for $i,j \in \mathbb{Z}$. Moreover $BA \neq AB$ so Q_8 is <u>not</u> abelian. Check that $B^2 = A^2$ and $B^3 = A^2 B$, so every element in Q_8 is of the form A^i or $A^i B$, $i \in \mathbb{Z}$. Since A has order 4, we at least have $Q_8 = \{ \mathbb{1}, A, A^2, A^3, B, AB, A^2 B, A^3 B \}$. Check that these are all different.

To see that this is the same group as we defined in class, put $A = i$, $B = j$, and $AB = k$.