MATH 3311, FALL 2025: HOMEWORK 6

(1) Decide if the following statements are true or false. Give a line or two in justification.
   (a) Any subgroup of order 189 in a group of order 378 must be normal.

   True: The index of that subgroup in the context of the whole group is $378/189 = 2$. By HW5P4, such a subgroup must be normal.

   (b) There exists a transitive group action $G \curvearrowright X$ where G has 24 elements and X has 15.

   False: For the group action to be transitive, X itself is an orbit. However, $15 \nmid 24$.

   (c) There exists a homomorphism $f : D_{2n} \to G'$ such that $\ker f$ is generated by a reflection.

   False: This is an equivalent statement to $\pi : D_{2n} \to H$ via $g \mapsto gH$ is a homomorphism. This means π must be well defined. Let $H = \{e, \sigma^k\tau\}$. This is how any subgroup generated by a reflection looks like.

   Now, we would expect $(\sigma H)(\sigma H) = (\sigma\sigma^k\tau H)(\sigma H)$ by well definedness of π. Then, $(\sigma\sigma^k\tau H)(\sigma)H = \sigma\sigma^k\tau\sigma H = \sigma^k\tau H = H$. Also, $(\sigma H)(\sigma H) = \sigma^2 H$. By well definedness, $\sigma^2 H = H$. However, σ^2 is a rotation, and thus not in H.

   (d) There exists a non-trivial homomorphism from $\mathbb{Z}/5\mathbb{Z}$ to $\mathbb{Q}$.

   False: If $\phi : \mathbb{Z}/5\mathbb{Z} \to \mathbb{Q}$ is an isomorphism such that $\phi([1]) = a$, then $\phi([6]) = 6a$. Since $[1] = [6]$, $a = 6a$, forcing $a = 0$. Then, $\phi([k]) = k\phi([1]) = k0 = 0$, so ϕ must be trivial.

   (e) There exists a non-trivial homomorphism from D_8 to $\mathbb{Z}$.

   False: If $\phi : D_8 \to \mathbb{Z}$ is a homomorphism with $\phi(\sigma) = a$, then $\phi(\sigma^5) = 5\phi(\sigma) = 5a$. Since $\sigma = \sigma^5$, $\phi(\sigma) = \phi(\sigma^5)$, meaning $a = 5a$, forcing $a = 0$. So for each rotation (including $e = \sigma^0$), ϕ must yield 0.

   Now, if $\phi(\sigma^k\tau) = k\phi(\sigma) + \phi(\tau) = k0 + \phi(\tau) = \phi(\tau)$. So every reflection has the same homomorphism value. Now, if $\phi(\tau) = b$, then $\phi(\tau\tau) = \phi(e) = b^2 = 0$. Then, $b = 0$. So every reflection is also sent to 0.

   Therefore, there does not exist a non-trivial homomorphism from D_8 to $\mathbb{Z}$.

(2) Let G be a finite group and let p be the *smallest* prime dividing $|G|$. Suppose that $H \leq G$ is a subgroup of index p.
   (a) Show that the usual action $G \curvearrowright G/H$ yields a homomorphism

$$\rho : G \to S_p.$$

   Since G acts on $|G/H| = p$ elements, The group action yields a homomorphism from G to S_p.

(b) Show that the image of ρ has order exactly p.

$|G/\ker\rho| = |\mathrm{im}(\rho)|$, so $|G| = |\ker\rho||\mathrm{im}(\rho)|$. Therefore, $\mathrm{im}(\rho) \mid |G|$. Since $\mathrm{im}(\rho) \leq S_p$, $\mathrm{im}(\rho) \mid p!$.

Then, the only possible options for the size would be 1 or p. Else, the size would have a factor with a prime number smaller than p. Now, the image of ρ cannot have size 1, for if $gH \neq H$ (and we know such a g exists because H has index $p > 1$), $\rho(g)(H) \neq \rho(e)(H) \implies \rho(g) \neq \rho(e) \implies |\mathrm{im}(\rho)| > 1$.

So the image of ρ has order exactly p.

(c) Conclude that H must be *normal*.

We wish to prove $H = \ker\rho$. By HW5P6c, $\ker\rho = \bigcap_{g\in G} gHg^{-1}$. Since $e \in G$, $\ker\rho \subseteq H = eHe^{-1}$. Now, $|\ker\rho| = |G|/|\mathrm{im}(\rho)| = |G|/p$. In addition, since $|G/H| = p$, $|H| = |G|/p$. So the sizes of $\ker\rho$ and H are the same.

Therefore, it must be the case that $\ker\rho = H$. Since we have proven that kernels of any homomorphisms are normal subgroups, H must be normal.

(3) Suppose that $K \trianglelefteq G$ is a normal subgroup with quotient homomorphism $\pi : G \to G/K$.

(a) Suppose that $H \leq G$ is a subgroup containing K. Show that K is a normal subgroup of H and that we have $H/K \xrightarrow{\simeq} \pi(H) \leq G/K$.

$\forall h \in H$, since $h \in G$, $hKh^{-1} = K$. Therefore, K is a normal subgroup of H.

Now, $\pi(H)$ is exactly H/K. $hK \in \pi(H) \iff hK \in H/K \iff h \in H$.

Now, we demonstrate $\pi(H) \leq G/K$ i.e. $H/K \leq G/K$.

Since $K \trianglelefteq G$, H/K is a group in its own right. Therefore, closure, identity, and inverses are all satisfied. We only need to check if $H/K \subseteq G/K$. This is obvious. $\forall hK \in H/K$, since $h \in H \subseteq G$, $h \in G$, meaning $hK \in G/K$.

We have shown that K is a normal subgroup of H with $H/K \xrightarrow{\simeq} \pi(H) \leq G/K$.

(b) Conversely, show that every subgroup of G/K is of the form H/K for some subgroup $H \leq G$ containing K.

Suppose $G/K = \{g_1K, g_2K, ...\}$ (not necessarily terminating). Then, take any subgroup $Q \leq G/K$. Now, let $H = \bigcup_{g_iK\in Q} g_iK$, meaning elements of H would look like g_ik for some $k \in K$ when $g_iK \in Q$.

We wish to prove this is a subgroup of G:
Identity: $eK \in Q \implies ee = e \in H$. Closure: $\forall g_ik_1, g_jk_2 \in H, g_iKg_jK \in Q$, so $g_ik_1g_jk_2 \in K$.
Inverses: $\forall g_ik$, so $g_iK \in Q$, so $(g_iK)^{-1} \in Q$, meaning $(g_ik)^{-1} \in H$.

Now, H contains K: $eK = K \in Q$, so $\forall k \in K, k \in H$.

Finally, we wish to prove $Q = H/K$. $H/K \subseteq Q$ because every element of H/K looks like $g_ikK = g_iK$ where $g_ik \in g_iK \in Q$. $Q \subseteq H/K$ because $\forall g_iK \in Q$, $g_ie = g_i \in H$, so $g_iK \in H/K$.

Therefore, $Q = H/K$.

We have shown that every subgroup of G/K is of the form H/K for some $H \leq G$ containing K.

(c) Conclude that the assignment

$$H \mapsto H/K = \pi(H)$$

is a bijection between the set of subgroups of G containing K and the set of subgroups of G/K. By part 1, each subgroup $H \leq G$ containing K yields a subgroup $H/K = \pi(H) \leq G/K$.

Suppose $\pi(H) = \pi(H')$, Then, $\forall h \in H \exists h' \in H' : \pi(h) = \pi(h') \iff hK = h'K \iff h'^{-1}h \in K$. This means $h'^{-1}h = k$ for some $k \in K$, meaning $h = h'k$. Since $k \in K \implies k \in H', h = h'k \in H'$ by closure. So $H \subseteq H'$. By the same logic mirrored, $H' \subseteq H$. So $\pi(H) = \pi(H') \implies H = H'$, showing that the assignment is injective.

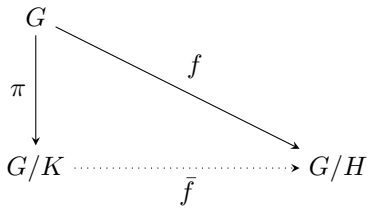
By part 2, every subgroup of G/K is of the form H/K for some H/K, so the assignment is surjective.

Therefore, this assignment is a bijection between the set of subgroups of G containing K and the set of subgroups of G/K.

(4) Let G be a group, $K \trianglelefteq G$ a normal subgroup, and $H \leq G$ a subgroup containing K. Use the factoring triangle to give a rigorous proof of the following fact: H is a normal subgroup of G if and only if H/K is a normal subgroup of G/K, and, in this case, there is an isomorphism of groups

$$G/H \xrightarrow{\simeq} (G/K)/(H/K).$$

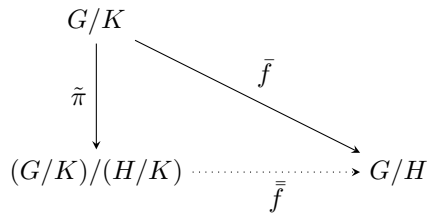
In most textbooks, this is called the 'third isomorphism theorem', but it is in fact a consequence of the factoring triangle.



When $K \trianglelefteq G$ with $H \leq G$ containing K, $\pi : G \to G/K$ via $g \mapsto gK$ is always a homomorphism.

First note that $\ker \pi = \{g \in G : gK = K\} = K$. Also, $\ker f = \{g \in G : gH = H\} = H$.

Step 1: H is a normal subgroup of G.
Step 2: $f : G \to G/H$ via $g \mapsto gH$ is a homomorphism.
Step 3: Since $K \leq H$ and $K = \ker \pi \leq \ker f = H$ (external fact), it is true that $\exists \bar{f} : G/K \to G/H$ such that $\bar{f} \circ \pi = f$ (in fact, $\bar{f} : G/K \to G/H$ is given by $gK \mapsto gH$).
Step 4: $\bar{f}$ is a group homomorphism.
Step 5: $H/K \trianglelefteq G/K$.
Now, the previous statements are all logically following iff statements. So $H \trianglelefteq G \iff H/K \trianglelefteq G/K$.



It remains to prove that there is an isomorphism of groups from G/H to $(G/K)/(H/K)$.

$\tilde{\pi} : G/K \to (G/K)/(H/K)$ via $gK \mapsto gK(H/K)$ is a group homomorphism. $\bar{f}$ is the same function as defined before.

$\ker \tilde{\pi} = \{gK \in G/K : gK(H/K) = H/K\} = H/K$ and $\ker \bar{f} = \{gK \in G/K : gH = H\} = \{gK : g \in H\} = H/K$.

Since $H/K = \ker \tilde{\pi} \leq \ker \bar{f} = H/K$, there is a group homomorphism $\bar{\bar{f}} : (G/K)/(H/K) \to G/H$ via $gK(H/K) \mapsto gH$.

$\bar{\bar{f}}$ is injective: $gK(H/K) \neq g'K(H/K) \implies gKeK \neq g'KeK \implies gK \neq g'K \implies \bar{\bar{f}}(gK(H/K)) \neq \bar{\bar{f}}(g'K(H/K))$. The first implication holds because cosets are completely disjoint.

$\bar{\bar{f}}$ is surjective: we can obtain any $gH \in G/H$ using $gK(H/K) \in (G/K)/(H/K)$.

Therefore, $\bar{\bar{f}}$ is an isomorphism. So there is an isomorphism of groups $G/H \xrightarrow{\simeq} (G/K)/(H/K)$, namely $\bar{\bar{f}}^{-1}$.

(5) Given integers $n, m \in \mathbb{Z}$, let $n(\mathbb{Z}/m\mathbb{Z}) \leq \mathbb{Z}/m\mathbb{Z}$ be the subgroup generated by n. Prove that

$$(\mathbb{Z}/m\mathbb{Z})/n(\mathbb{Z}/m\mathbb{Z})$$

is isomorphic to $\mathbb{Z}/\gcd(m,n)\mathbb{Z}$.
One way of thinking about this is that killing m and then n is the same as killing their gcd.

We want to first demonstrate that $n(\mathbb{Z}/m\mathbb{Z}) = \gcd(m,n)(\mathbb{Z}/m\mathbb{Z})$.

$\forall n[a] \in n(\mathbb{Z}/m\mathbb{Z})$, since $n = k\gcd(m,n)$ for some integer k, $n[a] = k\gcd(m,n)[a] = \gcd(m,n)[ka] \in \gcd(m,n)(\mathbb{Z}/m\mathbb{Z})$, meaning $n(\mathbb{Z}/m\mathbb{Z}) \subseteq \gcd(m,n)(\mathbb{Z}/m\mathbb{Z})$.

Now, $\forall \gcd(m,n)[a] \in \gcd(m,n)(\mathbb{Z}/m\mathbb{Z})$. Since $\exists s,t \in \mathbb{Z} : \gcd(m,n) = ms + nt$, $\gcd(m,n)[a] = (ms+nt)[a] = ms[a] + nt[a] = 0 + nt[a] = nt[a] \in n(\mathbb{Z}/m\mathbb{Z})$. Therefore, $\gcd(m,n)(\mathbb{Z}/m\mathbb{Z}) \subseteq n(\mathbb{Z}/m\mathbb{Z})$.

Combining our two results, $n(\mathbb{Z}/m\mathbb{Z}) = \gcd(m,n)(\mathbb{Z}/m\mathbb{Z})$.

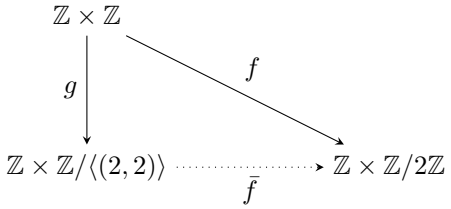
Therefore, $(\mathbb{Z}/m\mathbb{Z})/n(\mathbb{Z}/m\mathbb{Z}) = (\mathbb{Z}/m\mathbb{Z})/\gcd(m,n)\mathbb{Z}/m\mathbb{Z}$. By problem 5, the left hand side is isomorphic to $\mathbb{Z}/\gcd(m,n)\mathbb{Z}$, meaning $(\mathbb{Z}/m\mathbb{Z})/n(\mathbb{Z}/m\mathbb{Z})$ is isomorphic to $\mathbb{Z}/\gcd(m,n)\mathbb{Z}$.

(6) If $|G| = 2014 * 37$, and $H \trianglelefteq G$ is a normal subgroup of index 37, show that all elements of order 1007 in G are in fact contained in H.

$\forall g \in G$ where $|g| = 1007$, $(gH)^{37} = g^{37}H = H$ because $|gH| \mid |G/H| = 37$. This means $g^{37} \in H$.

Now, $\gcd(1007, 37) = 1$, as such, $\exists s, t : 1007s + 37t = 1$. Now, $g = g^{1007s+37t} = (g^{1007})^s(g^{37})^t = e^s(g^{37})^t = (g^{37})^t \in H$ by closure. Therefore, $g \in H$. We have shown all elements of order 1007 in G are contained in H.

(7) Show that the quotient of $\mathbb{Z} \times \mathbb{Z}$ by the subgroup generated by $(2, 2)$ is isomorphic to $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$.



g is the usual quotient homomorphism. It exists and is well defined because $\mathbb{Z} \times \mathbb{Z}$ is abelian, and thus every subgroup is normal.

f is given by taking (a, b) to $(a - b, a \pmod 2)$. This is a homomorphism: $f((a, b) + (c, d)) = f((a + c, b + d)) = (a + c - b - d, a + c \pmod 2) = (a - b, a \pmod 2) + (c - d, c \pmod 2) = f((a, b)) + f((c, d))$

This is also surjective. $(k, [j])$ is given by $f((j, j - k))$.

Finally, $\ker f = \{(a, b) \in \mathbb{Z} \times \mathbb{Z} : a - b = 0 \wedge a = 2k \text{ for some integer } k\} = \{(2k, 2k) : k \in \mathbb{Z}\} = \langle(2, 2)\rangle$.

Therefore, $\bar{f}$ in the diagram exists and is an isomorphism. The quotient of $\mathbb{Z} \times \mathbb{Z}$ by the subgroup generated by $(2, 2)$ is isomorphic to $\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ through $\bar{f}$.

An **automorphism** of a group G is an isomorphism $f : G \xrightarrow{\simeq} G$. We write $\mathrm{Aut}(G)$ for the set of automorphisms of G.

(8) (a) Show that $\mathrm{Aut}(G)$ is a subgroup of $\mathrm{Bij}(G)$.

Identity: Since $\forall g, g' \in G, \mathrm{Id}(gg') = gg' = \mathrm{Id}(g)\mathrm{Id}(g')$, the identity is a bijective homomorphism from G to G and thus is an automorphism in $\mathrm{Aut}(G)$.

Closure: We know isomorphisms composed with each other are themselves isomorphisms. With two elements in the subgroup of automorphisms of G, they are isomorphisms from G to G. So composing those two would yield in another isomorphism from G to G, meaning it is also an automorphism in $\mathrm{Aut}(G)$.

Inverses: We know inverses of isomorphisms are isomorphisms. Here, the mapping is still G to G, so the inverse is an automorphism in $\mathrm{Aut}(G)$.

As a consequence of the aforementioned properties, $\mathrm{Aut}(G) \leq \mathrm{Bij}(G)$.

(b) Describe the groups $\mathrm{Aut}(\mathbb{Z})$ and $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z})$ in terms of groups you already know.
We know isomorphisms between cyclic groups must map generators to generators. Also, we know that to define an isomorphism between cyclic groups, we only need to know where a generator goes to.

The integers has generators 1 and -1. So the two possible automorphisms is given by the trivial automorphism where $1 \mapsto 1$, and also the automorphism where $1 \mapsto -1$ (which means $a \mapsto -a$).

So $\mathrm{Aut}(\mathbb{Z})$ has order 2, meaning it is a cyclic group of order 2.

On the other hand, the integers modulo n has generators that are coprime to n. Since $[1]$ is always a generator for this group, an automorphism would look like $[1] \mapsto [k]$ for $k \in \mathbb{Z}$ with $\gcd(k, n) = 1$. Note that if we were to compose $[1] \mapsto [j]$ with the previous one, we would get $[1] \mapsto [jk]$. Intuitively, $\mathrm{Aut}(\mathbb{Z}/n\mathbb{Z}) \simeq (\mathbb{Z}/n\mathbb{Z})^\times$.

(9) (a) Show that, for any $g \in G$, the map

$$\begin{aligned} G &\to G \\ h &\mapsto ghg^{-1} \end{aligned}$$

is an automorphism of G.

Call this function f_g. It is a homomorphism: $\forall h, h' \in G, f_g(hh') = ghh'g^{-1} = ghg^{-1}gh'g^{-1} = f_g(h)f_g(h')$.

Now, f_g is injective: $f_g(h) = f_g(h') \implies ghg^{-1} = gh'g^{-1} \implies h = h'$.

f_g is surjective. First note that $gGg^{-1} = G$: by closure, $\forall g' \in G, gg'g^{-1} \in G$. Then for $k \in G$, $k \in gGg^{-1}$. Then, let $k = gk'g^{-1}$. Then, $f_g(k') = k$.

So the map is an isomorphism from G to G, meaning it is an automorphism of G.

(b) Denote the automorphism from (a) by $\mathrm{int}(g)$. Show that

$$G \xrightarrow{g \mapsto \mathrm{int}(g)} \mathrm{Aut}(G)$$

is a group homomorphism.
Hint: This is just the group action homomorphism for the conjugation action!

$G \curvearrowright G$ via $g \cdot h = ghg^{-1}$ is a group action. Then, $G \xrightarrow{g \mapsto \mathrm{int}(g)} \mathrm{Bij}(G)$ is a group homomorphism. Now, the range of this homomorphism can be limited to $\mathrm{Aut}(G)$, as we showed that g is mapped to an automorphism via $\mathrm{int}(g)$. Therefore, $G \xrightarrow{g \mapsto \mathrm{int}(g)} \mathrm{Aut}(G)$ is a group homomorphism.

(c) What is the kernel of the homomorphism in (b)?

$\ker \mathrm{int} = \{g \in G : \mathrm{int}(g) = \mathrm{Id}\} = \{g \in G : \forall h \in G, ghg^{-1} = h\} = \{g \in G : \forall h \in G, gh = hg\} = Z(G)$. So the kernel of the homomorphism in part b is $Z(G)$.