Solutions to Problem Set 4.
Math 322, Fall 2016. Instructor: Reichstein

(1) Let $G$ be a cyclic group of order $pqr$, where $p$, $q$ and $r$ are distinct primes. How many subgroups does $G$ have (counting the trivial subgroup $\{e\}$ and $G$ itself).

**Solution:** Let $G$ be a cyclic group of order $pqr$ where $p, q, r$ are distinct primes. Since $G$ is finite and cyclic, we know that there is exactly one group of order $d$ for each positive divisor $d$ of $pqr$. Thus we only need to count the number of positive integers dividing $pqr$.

By the Fundamental Theorem of Arithmetic, the divisors of $pqr$ have the form $p^{\varepsilon_p}q^{\varepsilon_q}r^{\varepsilon_r}$, where $\varepsilon_p, \varepsilon_q, \varepsilon_r \in \{0, 1\}$. There are two choices for $\varepsilon_p$, two choices for $\varepsilon_q$ and two choices for $\varepsilon_r$. Thus there are $2 \cdot 2 \cdot 2 = 8$ divisors of $pqr$ and therefore 8 subgroups of $G$.

(2) Let $G$ be a finite group, $d \geq 1$ be an integer, and $X = \{a \in G \mid o(a) = d\}$.

(a) Define a relation on $X$ as follows: $(a, b) \in R$ if $\langle a \rangle = \langle b \rangle$, i.e., the cyclic subgroup generated by $a$ is the same as the cyclic subgroup generated by $b$. Show that $R$ is an equivalence relation.

(b) Show that the number of elements of order $d$ in $G$ is a multiple of $\phi(d)$. Here $\phi$ denotes the Euler $\phi$-function.

**Solution:**

(a) Let us prove that $R$ is an equivalence relation on $X$.

- **Reflexivity:** Let $a \in X$, we clearly have $\langle a \rangle = \langle a \rangle$ so $(a, a) \in R$.
- **Symmetry:** Let $a, b \in X$ such that $(a, b) \in R$, i.e., $\langle a \rangle = \langle b \rangle$ then also $\langle b \rangle = \langle a \rangle$ so $(b, a) \in R$.
- **Transitivity:** Let $a, b, c \in X$ such that $(a, b) \in X$ and $(b, c) \in X$. We have $\langle a \rangle = \langle b \rangle = \langle c \rangle$ so $(a, c) \in R$.

Therefore, $R$ is an equivalence relation.

(b) $X$ is partitioned into equivalence classes for the equivalence relation defined in part (a). Thus it suffices to show that each equivalence class contains exactly $\phi(d)$ elements.

Let $Y$ be an equivalence class. Then every element $a$ of $Y$ generates the same cyclic subgroup of order $d$ in $G$. Denote this cyclic subgroup by $C$. Elements of $Y$ are exactly the generators of $C$. We showed in class that a cyclic group of order $d$ has exactly $\phi(d)$ generators. Thus $|Y| = \phi(d)$, as claimed.

(3) Show that a homomorphism of groups $f: G \to H$ is one-to-one if and only if $\text{Ker}(f) = \{e\}$.

**Solution:** Let $f: G \to H$ be a homomorphism of groups.

- **Assume $f$ is one-to-one:** If $g \in \text{Ker}(f)$ then $f(g) = e_H = f(e_G)$ and so $g = e_G$. So $\text{Ker}(f) \subseteq \{e_G\}$. On the other hand, we know that $\text{Ker}(f)$ is a subgroup of $G$; in particular, $e_G \in \text{Ker}(f)$. Thus $\text{Ker}(f) = \{e_G\}$. 

• Assume Ker($f$) = \{e_G\}. Let $g, h \in G$ such that $f(g) = f(h)$ so 
$$e_H = f(g)f(h)^{-1} = f(g)f(h^{-1}) = f(gh^{-1}).$$
We have that $gh^{-1} \in$ Ker($f$) = \{e_G\} so $gh^{-1} = e_G$ and we conclude $g = h$. Thus $f$ is one-to-one.
So a group homomorphism has trivial kernel if and only if it is one-to-one.

(4) Recall that the centre $Z(G)$ of a group $G$ is defined as follows:
$$Z(G) := \{ h \in G \mid hg = gh \text{ for every } g \in G \}.$$  
In the previous assignment you showed that $Z(G)$ is a subgroup of $G$. Now show that any subgroup $K \subset Z(G)$ is normal in $G$.

Solution: Let $g \in G$. For all $k \in K$ we have $gk = kg$ and thus 
$$gkg^{-1} = k \in K.$$  
This shows that $K$ is a normal subgroup of $G$.

(5) Suppose $G$ is a group, $H$ is a subgroup and $g$ is an element of $G$. In the previous assignment you showed that $H^g := \{ ghg^{-1} \mid h \in H \}$ is a subgroup of $G$. Now show that the intersection $K := \bigcap_{g \in G} H^g$ is a normal subgroup of $G$.

Solution: Let $H$ be a subgroup of $G$ and $K = \bigcap_{g \in G} H^g$. Let $a \in G$. We have 
$$aKa^{-1} = a \left( \bigcap_{g \in G} H^g \right) a^{-1} = \bigcap_{g \in G} aH^g a^{-1} = \bigcap_{g \in G} H^{ag} = K.$$  
The last equality is a consequence of the fact that the function $g \mapsto a^{-1}g$ is onto. Thus, for a fixed $a$, $H^{ag}$ ranges over all conjugates of $H$, as $g$ ranges over $G$. We conclude that $K$ is normal in $G$.

(6) Show that a subgroup $H$ of $G$ is normal if and only if it has the following property: for any $x, y \in G$ such that $xy \in H$, we also have $yx \in H$.

Hint: This is an "if and only if statement". You need to show that (i) every normal subgroup of $G$ has the above property, and (ii) every subgroup of $G$ which has this property is normal.

Solution: Let $G$ be a group.
• Let $H$ be a subgroup of $G$ with the property that if $xy \in H$ then $yx \in H$. Let us prove that $H$ is normal. Let $g \in G$ and $h \in H$. Take $x = hg^{-1}$ and $y = g$. We have $xy = hg^{-1}g = h \in H$ so by the property, we have $yx = ghg^{-1} \in G$. So for every $g \in G$ and every $h \in H$, we have $ghg^{-1} \in H$. In other words, $H$ is normal in $G$.
• Assume that $H$ is normal. Let $x, y \in G$ such that $xy \in H$. Since $H$ is normal we also have $yx = x^{-1}(xy)x \in H$, as desired.
(7) Let $G$ be a group and $H$ be a normal subgroup of $G$. Assume that $H$ is finite and cyclic. Show that every subgroup of $H$ is also normal in $G$.

**Solution:** Let $K$ be a subgroup of $H$ of order $d$. We want to show that $K$ is normal in $G$.

Let $g \in G$. We have $gKg^{-1} \subseteq gHg^{-1} = H$ since $H$ is normal in $G$. Therefore, $gKg^{-1}$ is a subgroup of $H$, isomorphic to $K$ via the group isomorphism $x \mapsto gxg^{-1}$. In particular, $gKg^{-1}$ also has order $d$. Since $H$ is a finite cyclic group, it only has one subgroup of order $d$. Thus, $gKg^{-1} = K$ for all $g \in G$. This shows that $K$ is normal in $G$.

(8) Let $G$ be a finite group and $H$ be a subgroup of index $[G:H] = n$. Recall that $[G:H]$ is the number of left cosets of $H$ in $G$.

(a) If $H$ is a normal subgroup of $G$, show that $x^n \in H$ for every $x \in G$.

(b) Give an example, showing that if $H$ is not assumed to be normal, the assertion of part (a) may fail. Let $G$ be a finite group and $H$ be a subgroup of index $[G:H] = n$. Recall that $[G:H]$ is the number of left cosets of $H$ in $G$.

(a) If $H$ is a normal subgroup of $G$, show that $x^n \in H$ for every $x \in G$.

(b) Give an example, showing that if $H$ is not assumed to be normal, the assertion of part (a) may fail.

**Solution:**

(a) Let $x \in G$. Since $H$ is normal, $G/H$ is a group of order $[G:H] = n$. By Lagrange theorem, $x^n H = (xH)^n = H$ is the identity element of $G/H$. We conclude that $x^n \in H$.

(b) Let $G = S_3$ and $H = \{id, (1\ 2)\}$. Then $[G:H] = \frac{|G|}{|H|} = \frac{6}{2} = 3$. Set $x := (2\ 3)$. Then $x^3 = (2\ 3)^3 = (2\ 3) \notin H$.

(9) Show that $V = \{id, (1\ 3)(2\ 4), (1\ 4)(2\ 3), (1\ 2)(3\ 4)\}$ is a normal subgroup of $S_4$.

**Solution:** For notational convenience, let us set

\[
a := (1\ 3)(2\ 4), \quad b := (1\ 4)(2\ 3) \quad \text{and} \quad c := (1\ 2)(3\ 4).
\]

Let us check first that $V$ is a subgroup of $S_4$.

- **$V$ is not empty:** Clear.
- **$V$ is closed under inversion:** An easy computation shows that $id^2 = a^2 = b^2 = c^2 = id$. Thus every element of $V$ is its own inverse. Consequently, $V$ is closed under taking inverses.
- **$V$ is closed under composition:** We want to show that if $\sigma, \tau \in V$, then $\sigma \tau \in V$. This is clear if $\sigma = id$, $\tau = id$ or $\sigma = \tau$. To prove that $\sigma \tau \in V$ for $\sigma, \tau = a, b, c$, we first check, by explicitly composing $a$ and $b$, that $ab = ba = c$. Now $ac = a(ab) = b \in V$, $ca = (ab)a = a(ab) = b \in V$, and similarly $bc = b(ba) = a \in V$, $cb = (ab)b = a \in V$.

This proves that $V$ is a subgroup of $S_4$. 

It remains to show that $V$ is normal in $S_4$. That is, we want to show that for any $\tau \in V$ and any $\sigma \in S_4$,

$$\sigma \tau \sigma^{-1} \in V.$$ 

If $\tau = \text{id}$, this is clear: $\sigma \text{id} \sigma^{-1} = \text{id} \in V$. Thus we may assume that $\tau = a, b$ or $c$, i.e., $\tau$ is a product of two disjoint 2-cycles, $\tau = (i \ j)(k \ \ell) \in V$, where $i, j, k$ and $\ell$ are 1, 2, 3, and 4, up to reordering. Note that $V$ contains every permutation of this form. Now

$$\sigma(i \ j)(k \ \ell)\sigma^{-1} = \sigma(i \ j)\sigma^{-1}\sigma(k \ \ell)\sigma^{-1} = (\sigma(i) \ \sigma(j))(\sigma(k) \ \sigma(\ell)) \in V$$

is again a product of disjoint 2-cycles and hence, is an element of $V$. This shows that $V$ is a normal subgroup of $S_4$.

(10) Suppose $G$ is a finite group, and $H$ is a normal subgroup of $G$. Assume $|H| = m$ and $[G : H] = n$. If $\gcd(m, n) = 1$, show that $|H|$ is the only subgroup of $G$ of order $m$.

**Solution:** Let $K$ be a subgroup of $G$ of order $m$. Our goal is to show that $K \subset H$. If we can do this, then since $|K| = |H| = m$, we will conclude that $K = H$, and the problem will be solved.

To prove that $K \subset H$, consider the image of $K$ under the quotient homomorphism $\pi : G \to G/H$, defined by $\pi(x) = xH$. We know that $H$ is the kernel of $\pi$. Thus in order to show that $K \subset H$, it is enough to show that $K \subset \ker(\pi)$ or equivalently, that $\pi(k) = e_{G/H}$ for every $k \in K$.

We know that the order of $\pi(k)$ divides the order of $k$, which in turn, divides $m = |K|$. On the other hand, by Lagrange’s theorem, the order of $\pi(k)$ divides $|G/H| = n$. In summary, the order of $\pi(k)$ divides both $m$ and $n$. Since $\gcd(m, n) = 1$, the order of $\pi(k)$ is 1, i.e., $\pi(k) = e_{G/H}$, as desired.