Problem Set 5. Solutions. 
Math 322, Fall 2016

(1) Let \( G \) be a group and \( a, b \in G \). Recall that a commutator \([a, b]\) is defined as \( aba^{-1}b^{-1} \). Show that the inverse of a commutator is again a commutator. That is, \([a, b]^{-1} = [c, d] \) for some \( c, d \in G \). Find \( c \) and \( d \) (assuming \( a \) and \( b \) are given).

**Solution:** Let \( a, b \in G \). We have
\[
[a, b]^{-1} = (aba^{-1}b^{-1})^{-1} = bab^{-1}a^{-1} = [b, a].
\]

(2) Let \( G \) be a group and \( H \) be a normal subgroup of \( G \).
(a) If \( G \) is abelian, show that \( G/H \) is also abelian.
(b) If \( G = \langle a_1, \ldots, a_r \rangle \), show that \( G/H = \langle a_1 H, \ldots, a_r H \rangle \). In other words, if \( G \) is generated by \( \{a_1, \ldots, a_r\} \), then \( G/H \) is generated by \( \{a_1 H, \ldots, a_r H\} \).
(c) If \( G \) is cyclic, show that \( G/H \) is cyclic.

**Solution:** (a) Assume \( G \) is abelian. Let \( aH, bH \in G/H \) where \( a, b \in G \). We have
\[
(aH)(bH) = (ab)H = (ba)H = (bH)(aH),
\]
therefore \( G/H \) is abelian.

(b) Assume \( G = \langle a_1, \ldots, a_r \rangle \). Let \( gH \in G/H \) where \( g \in G \). We want to show that \( gH \in \langle a_1 H, \ldots, a_r H \rangle \). Since \( a_1, \ldots, a_r \) generate \( G \), we can write \( g \) as a word, \( g = g_1^{e_1} \ldots g_n^{e_n} \) for some integer \( n \geq 1 \), and some elements \( g_i \in \{a_1, \ldots, a_r\} \). Then \( gH = g_1^{e_1} \ldots g_n^{e_n} H = (g_1 H)^{e_1} \ldots (g_n H)^{e_n} \). Thus \( g_i H \in \{a_1 H, \ldots, a_r H\} \), as desired.

(c) “Cyclic” means “generated by one element”. Thus part (a) is a special case of part (b), with \( r = 1 \).

(3) Let \( G \) be a finite group, \( H \triangleleft G \) be a normal subgroup and \( \pi: G \to G/H \) be the quotient map. Recall that a subgroup \( K \leq G \) is called a complement to \( H \) in \( G \) if (i) \( K \cap H = \{e\} \) and (ii) \( |H| \cdot |K| = |G| \). Show that \( K \) is a complement to \( H \) in \( G \) if and only if \( \pi \) restricts to an isomorphism between \( K \) and \( G/H \).

**Solution:** For notational convenience let us write \( \pi_K \) for the restriction of \( \pi \) to \( K \), i.e. \( \pi_K : K \to G/H \) is defined by \( \pi_K(k) = \pi(k) = kH \).

(\( \Rightarrow \)): Assume \( K \) is a complement to \( H \) in \( G \). Let us write \( \pi_K \) for the restriction of \( \pi \) to \( K \), i.e. \( \pi_K : K \to G/H \) is defined by \( \pi_K(k) = \pi(k) = kH \). It is clear that \( \pi_K \) is a group homomorphism, since \( \pi \) is one and \( K \) is a subgroup of \( G \).

Our goal is to show that \( \pi_K \) is a bijection, i.e., is \( 1 - 1 \) and onto. By condition (ii), \( |K| = \frac{|G|}{|H|} = |G/H| \). Thus by the pigeonhole principle, we only need to check that \( \pi_K \) is \( 1 - 1 \). Equivalently, we need to check that \( \text{Ker}(\pi_K) = \{e\} \). Assume that \( \pi_K(k) = e_{G/H} \) for some \( k \in K \). That is, \( kH = H \) or equivalently, \( k \in H \). Thus since \( k \in K \cap H = \{e\} \), i.e., \( k = e \) as desired.
(⇐) Assume \( \pi_K : K \rightarrow G/H \) is an isomorphism. We need to prove (i) and (ii).

(i) \( K \cap H = K \cap \ker(\pi) = \ker(\pi_K) = \{e\} \), as desired.

(ii) Since the group \( K \) and \( G/H \) are isomorphic, they have the same number of elements. Thus \( |K| = \frac{|G|}{|H|} \) or equivalently, \( |G| = |K||H| \).

(4) Let \( G \) be a group and \( D = \{(g, g) \mid g \in G\} \) be the “diagonal” in \( G \times G \).

(a) Show that \( D \) is a subgroup of \( G \times G \).

(b) Show that \( D \) is a normal subgroup of \( G \times G \) if and only if \( G \) is abelian.

(c) Show that the function \( f : G \times G \rightarrow G \) given by \( f(a, b) = ab^{-1} \) is a homomorphism if and only if \( G \) is abelian.

Solution: (a) Let us show \( D \) is a subgroup of \( G \times G \).

Proof 1:
- \( D \) is not empty: Clearly \((e, e) \in D \).
- Closure under composition: Let \((g, g), (h, h) \in D \). Then \((g, g)(h, h) = (gh, gh) \in D \).
- Closure under inversion: Let \((g, g) \in D \). We have \((g, g)^{-1} = (g^{-1}, g^{-1}) \).

(b) \( \Rightarrow \) Assume \( D \) is a normal subgroup of \( G \times G \). Let \( g, h \in G \). Consider the element \((g, g) \in D \). Since \( D \) is normal we have that \((e, h)(g, g)(e^{-1}, h^{-1}) = (g, hgh^{-1}) \in D \), so its two coordinates are the same, hence \( g = hgh^{-1} \). Consequently, \( gh = hg \).

(⇐) Assume \( G \) is abelian. Then the group \( G \times G \) is abelian \(((g, h)(k, \ell) = (gh, k\ell) = (hg, \ell k) = (h, \ell)(g, h))\). By previous assignment we know that every subgroup of \( G = Z(G) \) is normal in \( G \). In particular \( D \) is normal in \( G \times G \).

(c) \( \Rightarrow \) Proof 1: We argue by contradiction. Assume \( f \) is a homomorphism. Then \((g, h) \in \ker(f) \) if and only if \( gh^{-1} = e \), if and only if \((g, h) \in D \). In other words, \( D = \ker(f) \). Since \( D \) is the kernel of a homomorphism, it is a normal subgroup of \( G \times G \). By part (b), \( G \) is abelian.

Proof 2: Assume \( f \) is a homomorphism. Then \( f(hg, h) = (hgh^{-1}) \) but also \( f(hg, h) = f((h, h)(g, e)) = f(h, h)f(g, e) = eg = g \). Thus \( hgh^{-1} = g \) or equivalently, \( hg = gh \).

(⇐) Assume \( G \) is abelian. Then \( f((a, b)(c, d)) = f(ac, bd) = ac(bd)^{-1} = acd^{-1}b^{-1} = ab^{-1}cd^{-1} = f(a, b)f(c, d) \).

Thus \( f \) is a homomorphism.

(5) Let \( G_1 \) and \( G_2 \) be cyclic groups of orders \( m \) and \( n \), respectively. Show that the group \( G_1 \times G_2 \) if cyclic if and only if \( \gcd(m, n) = 1 \).

Solution: (⇐) Assume \( \gcd(m, n) = 1 \). Let \( G \) be a cyclic group of order \( mn \).
Then $G$ contains a cyclic group $H_1$ of order $m$ and a cyclic group $H_2$ of order $n$. The subgroups groups $H_1$ and $H_2$ of $G$ are both cyclic and normal (because $G$ is abelian), $H_1 \cap H_2 = \{e\}$ (because the order of $H_1 \cap H_2$ divides both $m$ and $n$), and $|H_1| \cdot |H_2| = mn = |G|$. In particular, $H_2$ is a normal complement of $H_1$ in $G$. By a theorem proved in class, we know that $G$ is isomorphic to $H_1 \times H_2$. Now note that $H_1$ is isomorphic to $G_1$ (because both are cyclic of order $m$) and similarly $H_2$ is isomorphic to $G_2$. Hence, $G \cong H_1 \times H_2 \cong G_1 \times G_2$, as desired. Here $\cong$ stands for isomorphism of groups.

$(\Rightarrow)$ Conversely, assume $\gcd(m, n) = d > 1$. Then $G_1$ contains a cyclic subgroup $K_1$ of order $d$ and $G_2$ contains a cyclic subgroup $K_2$ of order $d$. Now the group $G = G_1 \times G_2$ contains two cyclic subgroups of order $d$, $K_1 \times \{e_2\}$ and $\{e_1\} \times K_2$, where $e_i$ is the identity element of $G_i$ ($i = 1, 2$). A cyclic group contains at most one subgroup of any given order. Hence, $G_1 \times G_2$ cannot be cyclic.

(6) Let $G$ be a finite group and $k$ be an integer. If $a \in G$ has $m$ conjugates, and $a^k$ has $n$ conjugates, show that $n$ divides $m$.

Hint: Compare the centralizers of $a$ and $a^k$.

**Solution:** Note that $C_G(a)$ and $C_G(a^k)$ are subgroups of $G$. If $g \in C_G(a)$ then $gg^{-1} = a$ hence $ga^kg^{-1} = (gag^{-1})^k = a^k$ so $g \in C_G(a^k)$. Therefore, $C_G(a)$ is a subgroup of $C_G(a^k)$, so by Lagrange theorem we have that $|C_G(a)|$ divides $|C_G(a^k)|$. That is, $|C_G(a^k)| = d|C_G(a)|$ for some integer $d$. Now

$$m = |G : C_G(a)| = \frac{|G|}{|C_G(a)|} = \frac{|G|}{d|C_G(a^k)|} = d|G : C_G(a^k)| = dn.$$ 

In other words, $n$ divides $m$.

(7) Let $G$ be a group and $H \leq Z(G)$ be a central subgroup of $G$. (Here, as usual, $Z(G)$ denotes the center of $G$.) We know from a previous homework assignment that $H$ is normal in $G$. Thus we can form the quotient group $G/H$. If $G/H$ is cyclic, show that $G$ is abelian.

**Solution:** Assume that $H$ is central and $G/H$ is cyclic. We will prove that $G/H$ is cyclic. There is $\gamma \in G$ such that $G/H = \langle \gamma H \rangle$. Let $a, b \in G$; our goal is to show that $a$ and $b$ commute.

There are $k, \ell \in \mathbb{Z}$ such that $aH = \gamma^k H$ and $bH = \gamma^\ell H$. In other words, $a = \gamma^k h_1$ and $b = \gamma^\ell h_2$ for some $h_1, h_2 \in H$. Now

$$ab = \gamma^k h_1 \gamma^\ell h_2$$

$$= \gamma^{k+\ell} h_1 h_2$$

$$= \gamma^\ell \gamma^k h_1 h_2$$

$$= \gamma^\ell h_2 \gamma^k h_1$$

$$= ba,$$
so $G$ is abelian. Note that we were free to move $h_1, h_2$ past $\gamma$ and past each other, since these elements are central, i.e., they commute with every element of $G$.

(8) Suppose $G$ is a group with exactly two conjugacy classes. Show that $|G| = 2$.

Solution: Assume that $G$ has exactly 2 conjugacy classes. Suppose $|G| = n$.

The conjugacy class of $e$ is always $\{e\}$. This means that there is another conjugacy class, $C$ containing the remaining $n - 1$ elements. Since $|C|$ divides $|G| = n$, we see that $n - 1$ divides $n$. In other words,

$$\frac{N}{n-1} = 1 + \frac{1}{n-1}$$

is an integer. This is only possible if $n - 1 = 1$, i.e., $n = 2$

(9) Suppose $G$ is a group of order $2p$, where $p$ is a prime. Show that there exists an onto homomorphism $G \rightarrow H$, where $H$ is a group of order 2.

Hint: Use Cauchy’s theorem.

Solution: By Cauchy’s theorem, $G$ has a cyclic subgroup order $p$. Denote this subgroup by $H$. Then $[G : H] = \frac{2p}{p} = 2$. By a theorem proved in class, $H$ is normal in $G$. The quotient homomorphism $\pi: G \rightarrow G/H$ has the desired properties; it is onto, and $|G/H| = [G : H] = 2$.

(10) Suppose $G$ be a group of order $p^n$, where $p$ is a prime. (Such groups are called $p$-groups.) Show that $Z(G) \neq \{e\}$.

Hint: Use the class equation.

Solution: Assume that $|G| = p^n$ for some $n \geq 1$. If $G$ is abelian, then $G = Z(G)$ and the result is immediate. Else there are $g_1, \ldots, g_m$ representatives of nontrivial conjugacy classes of $G$ such that

$$|G| = |Z(G)| + \sum_{i=1}^m [G : C_G(g_i)].$$

Note that $[G : C_G(g_i)]$ divides $|G| = p^n$ hence $[G : C_G(g_i)] = p^{\ell_i}$ for some $\ell_i \geq 1$ (indeed $\ell_i \neq 0$ since it would imply that $C_G(g_i) = G$ so $g_i \in Z(G)$).

We showed that $p$ divides $[G : C_G(g_i)]$ for all $i$, and $p$ divides $|G|$ therefore $p$ must divide $|G| - \sum_{i=1}^m [G : C_G(g_i)] = |Z(G)|$. Since $p \geq 2$ and $p$ divides $|Z(G)|$ we must have $|Z(G)| \geq 2$ so $Z(G) \neq \{e\}$. 