Homework Assignment 2

Tagore Zhao

MATH250A
Instructor: Richard Borcherds
Due Date: September 15, 2024

Problem 12

Let G be a group, and let H, N be subgroups of G with N normal in G. Let γ_x be the conjugation by an element $x \in G$.

(a)

Show that $x \mapsto \gamma_x$ induces a homomorphism $f : H \to \mathrm{Aut}(N)$.

Solution

Since N is normal in G, for any $n \in N$ and $g \in G$, we have:

$$\gamma_g(n) = gng^{-1} \in N.$$

This implies that $\gamma_g \in \mathrm{Aut}(N)$ for all $g \in G$.

Define $f : H \to \mathrm{Aut}(N)$ by $f(h) = \gamma_h$. Since $\gamma_h \in \mathrm{Aut}(N)$ for every $h \in H$, the function f is well-defined.

We need to prove that f is a homomorphism, i.e.,

$$f(h_1h_2) = f(h_1)f(h_2).$$

To show this, we need to demonstrate that $\gamma_{h_1h_2} = \gamma_{h_1} \circ \gamma_{h_2}$.

For any element $n \in N$:

$$\gamma_{h_1h_2}(n) = (h_1h_2)n(h_1h_2)^{-1} = h_1(h_2nh_2^{-1})h_1^{-1} = \gamma_{h_1}(\gamma_{h_2}(n)).$$

Thus,

$$\gamma_{h_1h_2} = \gamma_{h_1} \circ \gamma_{h_2}.$$

Therefore, $f(h_1h_2) = \gamma_{h_1h_2} = \gamma_{h_1} \circ \gamma_{h_2} = f(h_1) \circ f(h_2)$, showing that f is indeed a homomorphism.

(b)

Given subgroups H and N of G with N normal in G and $H \cap N = \{e\}$, show that the map $H \times N \to HN$ given by $(x, y) \mapsto xy$ is a bijection, and that this map is an isomorphism if and only if f is trivial, i.e., $f(x) = \mathrm{id}_N$ for all $x \in H$.

Solution

Define $H \cap N = \{e\}$ and consider the mapping $f : H \times N \to HN$ given by $f(x, y) = xy$.

To show injectivity, suppose $f(x_1, y_1) = f(x_2, y_2)$. Then:

$$x_1 y_1 = x_2 y_2.$$

Multiplying both sides on the right by y_2^{-1} and on the left by x_1^{-1}, we get:

$$x_1^{-1} x_2 = y_1 y_2^{-1}.$$

Since $x_1^{-1} x_2 \in H$ and $y_1 y_2^{-1} \in N$, and $H \cap N = \{e\}$, we must have $x_1^{-1} x_2 = e$ and $y_1 y_2^{-1} = e$. Thus, $x_1 = x_2$ and $y_1 = y_2$, proving that f is injective.

Next, to show surjectivity, let $g \in HN$. By definition, HN consists of all products of the form xy with $x \in H$ and $y \in N$. Thus, every element of HN can be expressed as the product of an element in H and an element in N, showing that f is surjective.

Since f is both injective and surjective, it is bijective.

Now, we move forward to show that the map is an isomorphism if and only if f is trivial, i.e., $f(x) = \mathrm{id}_N$ for all $x \in H$.

Assume f is an isomorphism, meaning it is bijective and a homomorphism. For any $x_1, x_2 \in H$ and $y_1, y_2 \in N$:

$$f((x_1, y_1)(x_2, y_2)) = f(x_1 x_2, y_1 y_2) = x_1 x_2 y_1 y_2.$$

Since f preserves the group operation, we have:

$$f((x_1, y_1)) f((x_2, y_2)) = x_1 y_1 x_2 y_2 = x_1 x_2 y_1 y_2.$$

To prove that f is trivial, we need to show that $\gamma_x = \mathrm{id}_N$ for all $x \in H$, i.e., $xnx^{-1} = n$ for all $n \in N$. Since $H \cap N = \{e\}$, this condition implies that the conjugation action of H on N is trivial, confirming the structure is similar to a direct product.

Conversely, if f is trivial with $f(x) = \mathrm{id}_N$ for all $x \in H$, then f preserves the structure of HN as a direct-like product, fulfilling the conditions of an isomorphism.

We conclude that f is an isomorphism if and only if it is trivial.

(c)

Let N, H be groups, and let $\psi : H \to \mathrm{Aut}(N)$ be a given homomorphism. Construct a semidirect product as follows. Let G be the set of pairs (x, h) with $x \in N$ and $h \in H$. Define the composition law:

$$(x_1, h_1)(x_2, h_2) = (x_1 \psi(h_1)(x_2), h_1 h_2).$$

Show that this is a group law, and yields a semidirect product of N and H, identifying N with the set of elements $(x, 1)$ and H with the set of elements $(1, h)$.

Solution

Given groups N, H and a homomorphism mapping $\psi : H \to \mathrm{Aut}(N)$, define the composition law:

$$(x_1, h_1)(x_2, h_2) = (x_1 \psi(h_1)(x_2), h_1 h_2),$$

for all $(x_1, h_1), (x_2, h_2) \in G$ with $x_1, x_2 \in N$ and $h_1, h_2 \in H$. We aim to show that this is a group law.

Closure

Define $\psi : H \to \mathrm{Aut}(N)$ by $\psi(h)(x) = \gamma_h(x)$, where γ_h is the conjugation by h. We first show that G is closed under this composition:

Let $(x_1, h_1), (x_2, h_2) \in G$ with $x_1, x_2 \in N$ and $h_1, h_2 \in H$. Then,

$$(x_1, h_1)(x_2, h_2) = (x_1\psi(h_1)(x_2), h_1h_2) \in G,$$

since $x_1 \in N, \psi(h_1)(x_2) \in N$, and $h_1h_2 \in H$. Therefore, $(x_1\psi(h_1)(x_2), h_1h_2) \in G$.

Associativity

To prove associativity, we compute:

$$((x_1, h_1)(x_2, h_2))(x_3, h_3) = (x_1\psi(h_1)(x_2), h_1h_2)(x_3, h_3) = (x_1\psi(h_1)(x_2)\psi(h_1h_2)(x_3), h_1h_2h_3).$$

Similarly,

$$(x_1, h_1)((x_2, h_2)(x_3, h_3)) = (x_1, h_1)(x_2\psi(h_2)(x_3), h_2h_3) = (x_1\psi(h_1)(x_2\psi(h_2)(x_3)), h_1h_2h_3).$$

Since ψ is a homomorphism, $\psi(h_1h_2)(x_3) = \psi(h_1)(\psi(h_2)(x_3))$. Thus,

$$((x_1, h_1)(x_2, h_2))(x_3, h_3) = (x_1, h_1)((x_2, h_2)(x_3, h_3)),$$

showing associativity.

Identity

The identity element in G is (e, e), where e is the identity in both N and H. We show this by letting $(x, h) \in G$:

$$(e, e)(x, h) = (e\psi(e)(x), eh) = (x, h), \quad (x, h)(e, e) = (x\psi(h)(e), he) = (x, h).$$

Thus, (e, e) acts as the identity.

Inverse

We want to show that for every $(x, h) \in G$, there exists $(x', h') \in G$ such that:

$$(x, h)(x', h') = (e, e).$$

Let $(x, h) \in G$. For the inverse to exist, set:

$$(x, h)(\psi(h^{-1})(x^{-1}), h^{-1}) = (x\psi(h)(\psi(h^{-1})(x^{-1})), hh^{-1}) = (e, e).$$

Thus, the inverse of (x, h) is $(\psi(h^{-1})(x^{-1}), h^{-1})$.

Semidirect Product

We have shown that this composition law indeed defines a group. We now demonstrate that the mapping $H \times N \to H \ltimes_\psi N$ defined by the above composition law is a semidirect product.

Define N as the set of elements $(x, 1)$ and H as the set of elements $(1, h)$. It is clear that $(x, 1), (1, h) \in G$ and:

$$(x, 1)(1, h) = (x\psi(1)(1), h) = (x, h).$$

Hence, $G = NH$.

Next, we show $N \triangleleft G$. We need to prove that for any $(x, 1) \in N$ and $(x', h) \in G$:

$$(x', h)(x, 1)(x', h)^{-1} = (x', h)(x, 1)(\psi(h^{-1})(x'^{-1}), h^{-1}).$$

Simplifying:

$$= (x'\psi(h)(x), h)(\psi(h^{-1})(x'^{-1}), h^{-1}) = (x'\psi(h)(x)\psi(h)(x'^{-1}), e) = (x, e).$$

Since N is invariant under conjugation, $N \triangleleft G$. Therefore, G is a semidirect product of N and H.

Problem 13

(a) Let H, N be normal subgroups of a finite group G. Assume that the orders of H and N are relatively prime. Prove that $xy = yx$ for all $x \in H$ and $y \in N$, and that $H \times N \cong HN$.

(b) Let $H_1, \ldots, H_r$ be normal subgroups of G such that the order of H_i is relatively prime to the order of H_j for $i \neq j$. Prove that

$$H_1 \times \ldots \times H_r \cong H_1 \cdots H_r.$$

Solution to (a)

Let $H, N \triangleleft G$ with $|H| = p$ and $|N| = q$, where $\gcd(p, q) = 1$.

Since $H \triangleleft G$ and $N \triangleleft G$, for all $g \in G$, we have $gHg^{-1} = H$ and $gNg^{-1} = N$. Thus, H and N are normal subgroups of G, and therefore $NH = HN$.

Also, $H \cap N \triangleleft G$. By Lagrange's Theorem, since p and q are coprime, it follows that $|H \cap N| = 1$. Hence, $H \cap N = \{e\}$.

We also know that $|HN| = |H||N| = pq$, and by Lagrange's Theorem, this implies $|HN| = |H \times N|$. Therefore, the map $H \times N \to HN$ given by $(x, y) \mapsto xy$ is a bijective homomorphism, hence an isomorphism. Thus, we have:

$$H \times N \cong HN.$$

Now, we show commutativity. Pick $x \in N$ and $y \in H$. Consider $xyx^{-1}y^{-1}$. Since $H \triangleleft G$, we have:

$$xyx^{-1} \in H, \quad y^{-1} \in H, \quad \text{thus } xyx^{-1}y^{-1} \in H.$$

Similarly, since $N \triangleleft G$,

$$y^{-1}xy \in N, \quad x \in N, \quad \text{thus } xyx^{-1}y^{-1} \in N.$$

Since $H \cap N = \{e\}$, it follows that:

$$xyx^{-1}y^{-1} = e \implies xy = yx.$$

Thus, x and y commute for all $x \in H$ and $y \in N$, completing the proof.

Solution to (b)

Let $H_1, H_2, \ldots, H_r$ be normal subgroups of G. Assume the order of H_i is relatively prime to the order of H_j for $i \neq j$. Thus, $H_i \cap H_j = \{e\}$ for $i \neq j$. The intersection of $H_1, \ldots, H_r$ contains only the identity element.

Define the map $\phi : H_1 \times \ldots \times H_r \to H_1 \ldots H_r$ given by:

$$\phi(h_1, \ldots, h_r) = h_1 \cdots h_r.$$

To prove injectivity, let $\phi(h_1, \ldots, h_r) = e$. Then, since $h_i \in H_i$ and each $H_i \cap H_j = \{e\}$ for $i \neq j$, it follows that $h_1 = h_2 = \ldots = h_r = e$. Therefore, the kernel of ϕ is trivial, implying that ϕ is injective.

For surjectivity, every element in $H_1 \ldots H_r$ can be expressed as a product $h_1 \cdots h_r$ with $h_i \in H_i$. Thus, ϕ is surjective.

Let $h_i \in H_i$, $h_j \in H_j$, for any i, j with $i \neq j$. Consider the expression $h_i h_j h_i^{-1} h_j^{-1}$.

Since $H_j \lhd G$, we have:

$$h_i h_j h_i^{-1} \in H_j, \quad \text{and} \quad h_j^{-1} \in H_j, \quad \text{thus } h_i h_j h_i^{-1} h_j^{-1} \in H_j.$$

Similarly, since $H_i \lhd G$, we have:

$$h_j h_i h_j^{-1} \in H_i, \quad \text{and} \quad h_i^{-1} \in H_i, \quad \text{thus } h_i h_j h_i^{-1} h_j^{-1} \in H_i.$$

Therefore,

$$h_i h_j h_i^{-1} h_j^{-1} \in H_i \cap H_j.$$

Since $H_i \cap H_j = \{e\}$, it follows that:

$$h_i h_j h_i^{-1} h_j^{-1} = e,$$

which implies $h_i h_j = h_j h_i$.

To prove that ϕ is a homomorphism, consider:

$$\begin{aligned}
\phi((h_1, \ldots, h_r)(h'_1, \ldots, h'_r)) &= \phi(h_1 h'_1, \ldots, h_r h'_r) \\
&= h_1 h'_1 \cdots h_r h'_r \\
&= h_1 h_2 \cdots h'_{r-1} h'_r \\
&= \phi(h_1, \ldots, h_r)\phi(h'_1, \ldots, h'_r).
\end{aligned}$$

Since ϕ is both injective and surjective, it is a bijective homomorphism, hence:

$$H_1 \times \ldots \times H_r \cong H_1 \cdots H_r.$$

Problem 19

Let G be a finite group operating on a finite set S.

(a)

For each $s \in S$, show that

$$\sum_{t \in Gs} \frac{1}{\#(G_t)} = 1.$$

Solution

We first clarify some notation: let $\#(G_t) = |G_t| = |G_s|$, where G_s is the stabilizer of s. Define:

$$Gs = \{g \cdot s \mid g \in G\}, \quad \text{and} \quad G_t = \{gt \mid t \in Gs, g \in G\}.$$

For $t \in Gs$, $gt = g(g's) = Gs$ for some $g' \in G$. We can conclude that $Gs = G_t$.

Thus, we have:

$$\sum_{t \in Gs} \frac{1}{|G_t|} = \frac{1}{|G_s|} \sum_{s \in Gs} 1 = \frac{|Gs|}{|G_s|} = 1.$$

(b)

For each $x \in G$, define $f(x)$ as the number of elements $s \in S$ such that $xs = s$. Prove that the number of orbits of G in S is equal to:

$$\frac{1}{\#(G)} \sum_{x \in G} f(x).$$

Solution

We denote the number of orbits of G in S as $|S/G|$. Recall the Orbit-Stabilizer Theorem, which states that for any $s \in S$:

$$|G| = |\mathrm{Orb}(s)| \cdot |\mathrm{Stab}(s)|,$$

where:

$$\mathrm{Orb}(s) = \{g \cdot s \mid g \in G\} \quad \text{and} \quad \mathrm{Stab}(s) = \{g \in G \mid g \cdot s = s\}.$$

Next, let's rewrite the sum $\sum_{x \in G} f(x)$. This sum counts the total number of pairs (g, s) such that $g \cdot s = s$:

$$\sum_{x \in G} f(x) = \#\{(g, s) \mid g \in G, s \in S, g \cdot s = s\} = \sum_{s \in S} |\mathrm{Stab}(s)|.$$

We now express this sum using the Orbit-Stabilizer Theorem:

$$\sum_{s \in S} |\mathrm{Stab}(s)| = \sum_{s \in S} \frac{|G|}{|\mathrm{Orb}(s)|}.$$

Since the set S is partitioned into disjoint orbits under the action of G, we can rewrite the above sum as:

$$\sum_{s \in S} \frac{|G|}{|\mathrm{Orb}(s)|} = |G| \sum_{C \in S/G} \sum_{s \in C} \frac{1}{|\mathrm{Orb}(s)|}.$$

Each inner sum over $s \in C$ simplifies to 1 because each element in an orbit contributes exactly $\frac{1}{|\text{Orb}(s)|}$ for each element of G fixing s. Hence, we have:

$$\sum_{C \in S/G} \sum_{s \in C} \frac{1}{|\text{Orb}(s)|} = |S/G|.$$

Therefore, we conclude:

$$|S/G| = \frac{1}{|G|} \sum_{g \in G} f(g).$$

This completes the proof that the number of orbits of G in S is given by $\frac{1}{|G|} \sum_{g \in G} f(g)$.

Problem 20

Let P be a p-group. Let A be a normal subgroup of order p. Prove that A is contained in the center of P.

Solution

Given that P is a p-group and $A \triangleleft P$ with $|A| = p$, we want to show that $A \subseteq Z(P)$, where:

$$Z(P) = \{z \in P \mid \forall p \in P,\ zp = pz\}.$$

Since P is a p-group, every element of P has order a power of p. Given that $A \triangleleft P$ and $|A| = p$, we conclude that A is cyclic of order p.

Let $a \in A$ and $p \in P$. By normality of A, we have $pap^{-1} \in A$. Since A is cyclic of order p, it is generated by a. Therefore, pap^{-1} must be of the form a^k for some integer k.

However, since the only automorphisms of a cyclic group of prime order p are the identity and the map sending each element to its inverse, the map $x \mapsto pxp^{-1}$ must be the identity. Thus:

$$pap^{-1} = a.$$

This implies $pa = ap$. Therefore, for every $a \in A$, a commutes with every element of P. Hence, we have:

$$A \subseteq Z(P).$$

Problem 24

Let p be a prime number. Show that a group of order p^2 is abelian, and that there are only two such groups up to isomorphism.

Solution

We will first rewrite the statement in a form that is easier to check: We will show that a group of order p^2 is abelian and is isomorphic to either a cyclic group of order p^2 or a direct product of two cyclic groups of order p.

Let G be a group of order p^2. We know that G is a p-group, so it must have a nontrivial center. Since $Z(G)$ is a subgroup of G, it must have order p^2 or p.

- If $|Z(G)| = p^2$, then $Z(G) = G$, implying that G is abelian.
- If $|Z(G)| = p$, then $|G/Z(G)| = \frac{|G|}{|Z(G)|} = \frac{p^2}{p} = p$ by Lagrange's Theorem.

Thus, $G/Z(G)$ is cyclic and abelian.

Let $gZ(G)$ be the generator of $G/Z(G)$. Then any element $x \in G$ can be expressed as $x = g^n z$ for some $z \in Z(G)$. Let $x = g^m z_1$ and $y = g^n z_2$ for some $z_1, z_2 \in Z(G)$. Then:

$$xy = (g^m z_1)(g^n z_2) = g^m g^n z_1 z_2 = g^{m+n} z_1 z_2 = g^n g^m z_2 z_1 = (g^n z_2)(g^m z_1) = yx.$$

Therefore, G is always abelian.

By Sylow's Theorem, a group G of order p^2 has at most one subgroup of order p and p^2. If G is generated by a single element, then it is cyclic and is isomorphic to $\mathbb{Z}/p^2\mathbb{Z}$.

If G is not cyclic, it must contain elements of order p except the identity. By Sylow's Theorem, there exists a subgroup H of order p. Let $x \in G$ be an element of order p, and $H = \langle x \rangle$. Let $y \in G$ be another element of order p, and let $K = \langle y \rangle$. Since $H \cap K = \{e\}$, we have:

$$|HK| = \frac{|H||K|}{|H \cap K|} = p^2 \implies G \cong H \times K \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}.$$

Thus, the only two groups of order p^2 up to isomorphism are $\mathbb{Z}/p^2\mathbb{Z}$ and $\mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/p\mathbb{Z}$.

Problem 26

(a) Let G be a group of order pq, where p, q are primes with $p < q$. Assume that $q \not\equiv 1 \mod p$. Prove that G is cyclic.

(b) Show that every group of order 15 is cyclic.

Solution

(a)

Let G be a group with $|G| = pq$, where p, q are primes and $p < q$ with $q \not\equiv 1 \mod p$.

Let n_p be the number of Sylow p-subgroups of G. By Sylow's theorems, we have:

$$n_p \equiv 1 \mod p \quad \text{and} \quad n_p \mid q.$$

Similarly, let n_q be the number of Sylow q-subgroups of G. Then:

$$n_q \equiv 1 \mod q \quad \text{and} \quad n_q \mid p.$$

Since $p < q$, it follows that $n_p = 1$ and n_q can be either 1 or p. Given $n_q \equiv 1 \mod q$, we conclude that $n_q = 1$.

Since there exist unique subgroups H of order p and K of order q, we have $H \triangleleft G$ and $K \triangleleft G$.

Both H and K are groups of prime order, making them cyclic and abelian, with $H \cap K = \{e\}$.

By the previous problem's result, we know $G \cong H \times K \cong \mathbb{Z}/p\mathbb{Z} \times \mathbb{Z}/q\mathbb{Z}$. Consider the element $(1, 1) \in H \times K$, where 1 denotes the generator of each cyclic group. The order of this element is given by:

$$\text{lcm}(\text{order of } p, \text{ order of } q) = \text{lcm}(p, q) = pq.$$

Since G has an element of order pq, it follows that G is cyclic.

(b)

Let G be a group with $|G| = 15$. Since $|G| = 3 \cdot 5$, with 3 and 5 being primes, we have:

$$5 \not\equiv 1 \mod 3.$$

By part (a), G must be cyclic. Hence, every group of order 15 is cyclic.