SOLUTION SET 2

Problem 1 *Let G be a group, and let H and K be subgroups of G. Let X be the set G/H. Show the action of K on X has a fixed point if and only if we have $K \subseteq gHg^{-1}$ for some $g \in G$.*

Suppose that K fixes gH. Then, for all $k \in K$, we have $kgH = gH$, so $kg \in gH$ or $k \in gHg^{-1}$.

Problem 2 *Describe all possible actions of $\mathbb{Z}/2$ on the group $\mathbb{Z}/15$.*

Let ϕ be an automorphism of the group $\mathbb{Z}/15$. The generator 1 must be sent to some other generator a, and then ϕ is uniquely determined by $\phi(1+1+\cdots+1) = a+a+\cdots a$, in other words, $\phi(x) = ax$.

In order to give an action of $\mathbb{Z}/2$, we must have $a^2 = 1$. The solutions of $a^2 = 1$ in the ring $\mathbb{Z}/15$ are 1, 4, 11 and 14.

Problem 3 *Let p be a prime number. Let Ω be the set $\{0, 1, 2, \ldots, p\}$ and let G be the subgroup of S_Ω generated by $\alpha := (0\ 1)(2\ 3)\cdots(p-1\ p)$ and $\beta = (12\cdots p)$.*

(a) Show that G acts transitively on the set $\{(a, b) \in \Omega^2 : a \neq b\}$.

(b) Prove that G is not *simple if $p \equiv 1 \bmod 4$.*

(c) Show that $|G|$ is divisible by $p(p+1)$.

First, consider the action on Ω. The element β has two orbits on Ω: $\{0\}$ and $\{1, 2, \ldots, p\}$. Since α swaps 0 and 1, the group G acts transitively on Ω.

Now to solve the actual problem in part (a): We will show that the orbit of $(0, 1)$ contains every such ordered pair (a, b). First of all, for every (a, b), the orbit of (a, b) contains some pair $(0, c)$, because G acts transitively on Ω. Then β^{c-1} maps $(0, 1)$ to $(0, c)$, so $(0, 1)$ and $(0, c)$ are in the same orbit.

Since $p \equiv 1 \bmod 4$, the quantity $(p+1)/2$ is odd. In other words, β is an odd permutation. So G, as a subgroup of S_{p+1}, is *not* contained in the alternating group A_{p+1}. So $G \cap A_{p+1}$ is a nontrivial normal subgroup of G. The intersection is not the trivial group, because β is an even permutation (and for many other reasons). So G is not simple.

(c) The set in (b) has $(p+1)^2 - (p+1) = p^2 + p$ elements. Since G acts transitively on this set, it's order is divisible by $p(p+1)$.

This was the **problem taken from a QR exam**. I believe that, for $p \equiv 1 \mod 4$, the group G is in fact all of S_{p+1} while, for $p \equiv 3 \mod 4$, I think it is A_{p+1}. I haven't completely checked the details here, though.

Problem 4 *Let G be a group and g an element of G. Define an action of $\mathbb{Z}$ on G by $\phi(k)(h) = g^k h g^{-k}$, for $h \in G$ and $k \in \mathbb{Z}$. Show that $\mathbb{Z} \ltimes_\phi G \cong \mathbb{Z} \times G$.*

Map $\mathbb{Z} \times G$ to $\mathbb{Z} \ltimes_\phi G$ by $\alpha((h, n)) = (hg^{-n}, n)$. We must check that this is a map of groups:

$$\begin{aligned}\alpha((h_1, n_1))\alpha((h_2, n_2)) = (h_1 g^{-n_1}, n_1)(h_2 g^{-n_2}, n_2) &= (h_1 g^{-n_1} g^{n_1} h_2 g^{-n_1-n_2}, n_1 + n_2) \\ &= (h_1 h_2 g^{-n_1-n_2}, n_1 + n_2) = \alpha((h_1 h_2, n_1 + n_2))\end{aligned}$$

It is easy to see that α is bijective; an explicit inverse is given by $\alpha^{-1}((h, n)) = (hg^n, n)$.

This is the shortest way to write the solution; various other ways to think about the problem are to try to split the inclusion $G \to \mathbb{Z} \ltimes_\phi G$, or to find a nonobvious splitting of the projection $\mathbb{Z} \times G \to \mathbb{Z}$ giving the correct action of $\mathbb{Z}$ on G.

Problem 5 *Let G be a subgroup of $GL_n(\mathbb{F}_p)$, with order p^k. Write V for the vector space $\mathbb{F}_p^n$.*

(a) Show that the action of G on V fixes a nonzero vector.

(b) Show that, after changing bases in V, we can arrange for G to be contained in the subgroup

$$\begin{pmatrix} 1 & * & * & \cdots & * \\ 0 & * & * & \cdots & * \\ 0 & * & * & \cdots & * \\ & & & \ddots & \\ 0 & * & * & \cdots & * \end{pmatrix}$$

of $GL_n(\mathbb{F}_p)$.

(c) Show that, after changing bases in V, we can arrange for G to be contained in the subgroup

$$\begin{pmatrix} 1 & * & * & \cdots & * \\ 0 & 1 & * & \cdots & * \\ 0 & 0 & 1 & \cdots & * \\ & & & \ddots & \\ 0 & 0 & 0 & \cdots & 1 \end{pmatrix}.$$

(a) Since $|G| = p^k$, every orbit of G on V has size p^s for some $s \leq k$. Note that $V \setminus \{0\}$ has $p^n - 1$ elements, and $p^n - 1$ is not divisible by p. So at least one of the orbits of G on $V \setminus \{0\}$ must have size not divisible by p. This orbit must have size $p^0 = 1$. The element in this orbit is a nonzero vector fixed by G.

(b) If we change bases in V so that the nonzero fixed vector from part (a) is $(1, 0, 0, 0, \ldots, 0)^T$, then the fact that G fixes this vector means that it is in the given subgroup.

(c) Write e_i for $(0, 0, \ldots, 0, 1, 0, \ldots, 0)$ with 1 in the ith position. An element g of $GL_n(\mathbb{F}_p)$ is in the specified subgroup if g fixes e_1, and g fixes e_2 as an element of $V/(e_1)$, and g fixes e_3 as an element of $V/(e_1, e_2)$, and so forth.

To accommodate the "after changing bases" statement, we must find a basis v_1, v_2, v_3, ..., of V so that v_i is fixed by the G action on $V/(v_1, v_2, \ldots, v_{i-1})$. We find such a basis inductively, using part (a) over and over.

Problem 6 *Let A be an abelian group and let K be a group. Define a* **central extension** *of A by K to be a short exact sequence $1 \to A \to G \to K \to 1$ where A is central in G. Define two central extensions $1 \to A \to G_1 \to K \to 1$ and $1 \to A \to G_2 \to K \to 1$ to be* **equivalent** *if there is a an isomorphism $G_1 \cong G_2$ making the following diagram commute:*

$$\begin{array}{ccccccccc} 1 & \to & A & \longrightarrow & G_1 & \longrightarrow & K & \to & 1 \\ & & \| & & \downarrow\cong & & \| & & \\ 1 & \to & A & \longrightarrow & G_2 & \longrightarrow & K & \to & 1 \end{array}$$

Let $H^2(K, A)$ be the set of equivalence classes of central extensions. In this problem, we will put the structure of an abelian group on $H^2(K, A)$.

Let G_1 and G_2 be central extensions, with π_1 and π_2 denoting the maps to K. Define $G_1 \tilde{+} G_2$ to be $\{(g_1, g_2) \in G_1 \times G_2 : \pi_1(g_1) = \pi_2(g_2)$. Define $Z \subset G_1 \tilde{+} G_2$ to be $\{(a, -a) : a \in A\}$.

(a) Show that Z is a normal subgroup of $G_1 \tilde{+} G_2$. We define $G_1 + G_2$ to be $G_1 \tilde{+} G_2/Z$.

(b) Show that there is a central extension $1 \to A \to G_1 + G_2 \to K \to 1$. We consider $+$ as an operation on $H^2(K, A)$

(c) Show that $+$ is commutative and associative.

(d) Show that the direct product, $K \times_\phi A$, is the identity for $+$.

*(e) (**Harder**) Show that $H^2(K, A)$ has inverses.*

(a) First, we check that Z is a subgroup at all! Notice that $(a_1, -a_1) + (a_2, -a_2) = ((a_1 + a_2), -(a_1 + a_2))$, so Z is closed under multiplication; it is similarly easy to check that Z is closed under inversion. Although straightforward, note that this would not work if A was not abelian. We now check that Z is normal: Since A is central in both G_1 and G_2, we have $(g_1, g_2)(a, -a)(g_1^{-1}, g_2^{-1}) = (a, -a)$ for any $(g_1, g_2) \in G_1 \times G_2$ (and, in particular, in the subgroup $G_1 \tilde{+} G_2$ of $G_1 \times G_2$.)

(b) Include A into $G_1 \tilde{+} G_2$ by $\iota(a) = (a, 0)$, and map A to $G_1 + G_2$ by the composition $A \to G_1 \tilde{+} G_2 \to G_1 + G_2$. Since $\iota(A) \cap Z$ is trivial, the composition map is an injection.

We now compute $G_1 + G_2/A$. We have $G_1 + G_2/A \cong G_1 \tilde{+} G_2/(Z + \iota(A))$. Since every element (a, b) in $A \times A$ can be written as $(-b, b) + \iota(a + b)$, the group $Z + \iota(A)$ is clearly $A \times A$, and the quotient $G_1 + G_2/A$ is $G_1 \tilde{+} G_2/(A \times A)$, which is clearly K.

(c) Proof of commutativity: We need to build an isomorphism $G_1 + G_2 \to G_2 + G_1$ which commutes with the inclusions of A and the maps to K. There is an obvious map from $G_1 \tilde{+} G_2$ to $G_2 \tilde{+} G_1$ taking $(g_1, g_2) \mapsto (g_2, g_1)$. Since this map carries the subgroup Z of $G_1 \tilde{+} G_2$ to the similarly named subgroup of $G_2 \tilde{+} G_1$, it descends to the quotients, giving an isomorphism σ from $G_1 + G_2$ to $G_2 + G_1$. It is easy to see that the maps to K commute with σ. The inclusions of A are more subtle. Mapping $A \to G_1 \tilde{+} G_2 \to G_2 \tilde{+} G_1$ sends $a \mapsto (a, 0) \mapsto (0, a)$, where as the inclusion $A \to G_2 \tilde{+} G_1$ sends $a \mapsto (a, 0)$. Fortunately, $(a, 0)$ is equal to $(0, a)$ modulo Z, so these are the same.

Proof of associativity: Define $G_1 \tilde{+} G_2 \tilde{+} G_3$ to be the group $\{(g_1, g_2, g_3) \in G_1 \times G_2 \times G_3 : \pi_1(g_1) = \pi_2(g_2) = \pi_3(g_3)\}$. The group $(G_1 + G_2) + G_3$ is the quotient of $G_1 \tilde{+} G_2 \tilde{+} G_3$ by the subgroup of elements of the form $(a, -a, 0) + (b, 0, -b)$, for a and b in A. Similarly, $G_1 + (G_2 + G_3)$ is the quotient of $G_1 \tilde{+} G_2 \tilde{+} G_3$ by the subgroups of elements of the form $(0, c, -c) + (d, -d, 0)$, for c and d in A. These are the same subgroup: they are both $\{(e_1, e_2, e_3) \in A^3 : e_1 + e_2 + e_3 = 0\}$.

(d) Let G_0 be the direct product, and let G be any central extension. So $G \tilde{+} G_0$ is $\{(g, (a, k)) : g \in G, a \in A, k \in K, \pi(g) = k\}$. This can be rewrriten as simply $\{(g, (a, \pi(g))) : g \in G, a \in A\}$. The group Z, in this notation, is $\{(a, (-a, 0)) :\}$. Mapping $G \tilde{+} G_0$ to G by $(g, (a, \pi(g))) \mapsto (ga)$ is a map of groups (recall that A is central in G!), clearly surjective and has kernel Z. So this map shows that $G \tilde{+} G_0/Z \cong G$. I leave it as an exercise to check that this isomorphism commutes with the maps from A and to K.

(e) Let G be a central extension of K by A. Define the central extension $\bar{G}$ as follows: As a group $\bar{G} = G$, and the map $\bar{G} \to K$ is the same as the map $G \to K$. However, the inclusion $A \to \bar{G}$ sends a to $-\iota(a)$, where ι is the inclusion of A into G. We claim that

$$G + \bar{G} \cong A \times K.$$

Identify $G \times \bar{G}$ with $G \times G$ (since $\bar{G}$ and G are the same group). Then $G \tilde{+} \bar{G}$, as a subgroup of $G \times G$, is $\{(g_1, g_2) : \pi(g_1) = \pi(g_2)\}$ and Z is $\{(a, a) : a \in A\}$. We will henceforth write elements of $G \tilde{+} \bar{G}$ and Z in this manner.

Choose an arbitrary map of sets $\sigma : K \to G$, so that $\pi(\sigma(k)) = k$. Define $\tau : K \to G + \bar{G}$ by $\tau(k) = (\sigma(k), \sigma(k))$. We claim that τ is a map of groups. We start by computing:

$$\tau(k_1 k_2)\tau(k_2)^{-1}\tau(k_1)^{-1} = (\sigma(k_1 k_2)\sigma(k_2)^{-1}\sigma(k_1)^{-1}, \sigma(k_1 k_2)\sigma(k_2)^{-1}\sigma(k_1)^{-1}) \quad (*)$$

Since π is a map of groups, and $\pi \circ \sigma$ is the identity, we have $\pi\left(\sigma(k_1 k_2)\sigma(k_2)^{-1}\sigma(k_1)^{-1}\right) = 1$. In other words, $\sigma(k_1 k_2)\sigma(k_2)^{-1}\sigma(k_1)^{-1}$ is in A. So the right hand side of $(*)$ is of the form (a, a), and hence in Z. We see that

$$\tau(k_1 k_2)\tau(k_2)^{-1}\tau(k_1)^{-1} = 1$$

in $G + \bar{G}$. In other words, τ is a map of groups.

We have now split the sequence $0 \to A \to G + \bar{G} \to K \to 0$, so this sequence is semidirect. But A is central, so the conjugation action on A is trivial, and we deduce that the sequence is exact.

Remark: In fact, this method is good for more than just central extensions. Let A be abelian, and fix an action ϕ of K on A (by group automorphisms). One can similarly define $H^2(K, A, \phi)$ to be the set of exact sequences $0 \to A \to G \to K \to 0$ where the conjugation action of $G/A \cong K$ on A is by ϕ, modulo a natural equivalence relation. This is again an abelian group, with $K \ltimes_\phi A$ as the identity.

As the notation suggests, $H^2(K, A)$ is just one of an infinite sequence of groups $H^0(K, A)$, $H^1(K, A)$, $H^2(K, A)$, ..., which appear in various areas of group theory and number theory. The study of these groups is called *group cohomology*.