GROUP ACTIONS

Exercises

1. Let $\rho : G \mapsto Sym(\Omega)$ be a representation of the group G on the set Ω. Show that this defines an action of G on Ω by setting $\alpha^x := \alpha^{\rho(x)}$ for all $\alpha \in \Omega$ and $x \in G$, and that ρ is the representation which corresponds to this action.

Proof. Since ρ is a representation of G on Ω, ρ is a homomorphism. Let $\alpha^x := \alpha^{\rho(x)}$, then

$$\begin{aligned} \alpha^1 &= \alpha^{\rho(1)} = \alpha; \\ (\alpha^x)^y &= (\alpha^{\rho(x)})^{\rho(y)} = \alpha^{\rho(xy)} = \alpha^{xy}. \end{aligned}$$

Thus, this defines an action of G on Ω.

2. Explain why we do not usually get an action of a group G on itself by defining $a^x := xa$. Show, however, that $a^x := x^{-1}a$ does give an action of G on itself (called the left regular representation of G). Similarly, show how to define an action of a group on the set of left cosets $aH (a \in G)$ of a subgroup H.

Proof. Let $a^x := xa$, then

$$(a^x)^y = (xa)^y = yxa \neq xya = a^{xy}.$$

The equation holds if and only if G is an abelian group.

For all $a \in G$ and $x \in G$, let $a^x := x^{-1}a$, then

$$\begin{aligned} a^1 &= 1^{-1}a = a; \\ (a^x)^y &= (x^{-1}a)^y = y^{-1}x^{-1}a = (xy)^{-1}a = a^{xy}. \end{aligned}$$

Thus, this defines an action of G on itself.

Let $\Omega = \{aH |\ a \in G\}$, defining an action of G on Ω by setting $(aH)^x := x^{-1}aH$.

3. Show that the kernel of ρ_H in Example 1.3.4 is equal to the largest normal subgroup of G contained in the subgroup H.

Proof. Let $\Gamma_H := \{Ha |\ a \in G\}$ and define an action if G on Γ_H by right multiplication: $(Ha)^x := Hax$. We denote the corresponding representation of G on Γ_H by ρ_H. We have

$$\ker\ \rho_H \ = \bigcap_{a \in G} a^{-1}Ha.$$

Assume that N is the subgroup of H and $N \trianglelefteq G$, then we have $N = N^a \leq H^a$ for any $a \in G$. Thus, we obtained that $N \leq \bigcap_{a \in G} H^a = \ker\ \rho_H$.

Hence, by the arbitrariness of N, ker ρ_H is equal to the largest normal subgroup of G contained in the subgroup H.

4. Use the previous exercise to prove that if G is a group with a subgroup H of finite index n, then G has a normal subgroup K contained in H whose index in G is finite and divides $n!$. In particular, if H has index 2 then H is normal in G.

Proof. By Ex.3, we have that ker ρ_H is the largest normal subgroup of G contained in the subgroup H. Let $K = \ker \rho_H$. Since ρ_H is the action of G on Γ_H by right multiplication: $(Ha)^x := Hax$ and $|G : H| = n$, we have that $G/\ker \rho_H \lesssim S_n$, that is, $|G : K| \mid n!$. Hence, $|G : K|$ is finite and divides $n!$.

If $n = 2$, then $|G : \ker \rho_H|$=1 or 2. If $|G : \ker \rho_H| = 1$, then $G = \ker \rho_H = \bigcap_{a\in G} a^{-1}Ha$ which implies that $G = H$, contradiction. Thus, $|G : \ker \rho_H| = 2$, then $H = \ker \rho_H$, that is, H is normal in G.

5. Let G be a finite group, and let p be the smallest prime which divides the order of G. If G has a subgroup H of index p, show that H must be normal in G. In particular, in a finite p-group(that is, a group of order p^k for some prime p) any subgroup of index p is normal.

Proof. Since $|G : H| = p$, we have that G has a normal subgroup K contained in H whose index in G divides $p!$ by Ex.4. And p is the smallest prime which divides $|G|$, then $|G : K| \mid (p!, |G|) = p$. Thus, $H = K$ which implies that H is normal in G.

If G is p-group, the proof is the same as above.

6. (Number theory application)
Let p be a prime congruent to 1(mod 4), and consider the set

$$\Omega := \{(x, y, z) \in \mathbb{N}^3 | x^2 + 4yz = p\}.$$

Show that the mapping

$$(x, y, z) \mapsto \begin{cases} (x + 2z, z, y - x - z) & \text{if } x < y - z \\ (2y - x, y, x - y + z) & \text{if } y - z < x < 2y \\ (x - 2y, x - y + z, y) & \text{if } x > 2y \end{cases}$$

is a permutation of order 2 on Ω with exactly one fixed point. Conclude that the permutation $(x, y, z) \mapsto (x, z, y)$ must also have at least one fixed point, and so $x^2+4y^2 = p$ for some $x, y \in \mathbb{N}$.

Proof. First we show that the mapping is a permutation of order 2. It's easy to see that the mapping is a permutation, denoted by a.

If $x < y - z$, then $(x, y, z)^a = (x + 2z, z, y - x - z)$ with $x + 2z > 2z$. Then

$$(x + 2z, z, y - x - z)^a = ((x + 2z) - 2z, (x + 2z) - z + (y - x - z), z) = (x, y, z).$$

If $y-z < x < 2y$, then $(x, y, z)^a = (2y-x, y, x-y+z)$ with $y-(x-y+z) < 2y-x < 2y$. Then

$$(2y - x, y, x - y + z)^a = (2y - (2y - x), y, (2y - x) - y + (x - y + z)) = (x, y, z).$$

If $x > 2y$, then $(x, y, z)^a = (x - 2y, x - y + z, y)$ with $x - 2y < (x - y + z) - y$. Then

$$(x - 2y, x - y + z, y)^a = (x - 2y + 2y, y, (x - y + z) - (x - 2y) - y) = (x, y, z).$$

The permutation a only fixed $(1, 1, 1)$ by calculations.

The permutation $(x, y, z) \mapsto (x, y, z)$ has fixed point if and only if $y = z$, that is, $x^2 + 4y^2 = p$.