

## §25 Group Actions

Many of the important groups we have examined so far are groups of functions.  $S_X$  is the group of one-to-one mappings on the set  $X$ ,  $Isom E$  is the group of distance preserving functions on the Euclidean plane,  $Aut(G)$  is the group of multiplication preserving functions on a group  $G$ . You will see more examples later. In general, when  $X$  is a set with some structure on it (algebraic, geometric, analytic, topological or of some other type), the mappings on  $X$  that preserve this structure form a group. Up to now, we neglected the functional character of the elements of a group they might have. In this paragraph, we consider groups whose elements can be thought of as functions on a set  $X$ . This leads to the idea of group actions.

**25.1 Definition:** Let  $G$  be a group and let  $X$  be a nonempty set. We say that  $G$  acts on  $X$  provided, for all  $x \in X$  and  $g \in G$ , there corresponds a uniquely determined element of  $X$ , denoted by  $xg$ , such that the following hold:

$$\begin{aligned} (xg_1)g_2 &= x(g_1g_2) && \text{for all } x \in X, g_1, g_2 \in G, \\ x1 &= x && \text{for all } x \in X. \end{aligned}$$

More precisely, we say then that  $G$  acts on  $X$  on the right. We similarly define a left action of  $G$  on  $X$  by stipulating that  $(g_1g_2)x = g_1(g_2x)$  and  $1x = x$  for all  $x \in X, g_1, g_2 \in G$ , where  $gx$  is a uniquely determined element of  $X$  corresponding to the pair  $g, x$ .

**25.2 Examples: (a)** Let  $X$  be a nonempty set and  $G = S_X$ . Then  $G$  acts on  $X$  when we naturally interpret  $xg$  as the image of  $x \in X$  under the mapping  $g \in G$ . The condition  $(xg_1)g_2 = x(g_1g_2)$  is satisfied for all  $x \in X$  and for all  $g_1, g_2 \in G$ , for it is nothing else than the definition of composition of mappings. The condition  $x1 = x$  holds, too, since it is the definition of the identity mapping  $1 \in G$  on  $X$ . More generally, if  $G \leq S_X$ , then  $G$  acts on  $X$ .

**(b)** Let  $X = \mathbb{R} \times \mathbb{R}$  and let  $G = GL(2, \mathbb{R})$ . Then  $G$  acts on  $X$  if we put

$$(x,y)\begin{pmatrix} a & b \\ c & d \end{pmatrix} = (xa + yc, xb + yd).$$

We have indeed 
$$\begin{aligned} \left( (x,y)\begin{pmatrix} a & b \\ c & d \end{pmatrix} \right) \begin{pmatrix} e & f \\ g & h \end{pmatrix} &= (xa + yc, xb + yd) \begin{pmatrix} e & f \\ g & h \end{pmatrix} \\ &= ((xa + yc)e + (xb + yd)g, (xa + yc)f + (xb + yd)h) \\ &= (xae + yce + xbg + ydg, xaf + ycf + xbh + ydh) \end{aligned}$$

and 
$$\begin{aligned} (x,y) \left( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} \right) &= (x,y) \begin{pmatrix} ae+bg & af+bh \\ ce+dg & cf+dh \end{pmatrix} \\ &= (x(ae + bg) + y(ce + dg), x(af + bh) + y(cf + dh)) \\ &= (xae + xbg + yce + ydg, xaf + xbh + ycf + ydh) \end{aligned}$$

and so 
$$\left( (x,y)\begin{pmatrix} a & b \\ c & d \end{pmatrix} \right) \begin{pmatrix} e & f \\ g & h \end{pmatrix} = (x,y) \left( \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} e & f \\ g & h \end{pmatrix} \right)$$
 for all  $(x,y) \in X$  and  $\begin{pmatrix} a & b \\ c & d \end{pmatrix}, \begin{pmatrix} e & f \\ g & h \end{pmatrix} \in G$ .

One proves analogously that  $G$  acts on  $Y = \left\{ \begin{pmatrix} x \\ y \end{pmatrix} : x,y \in \mathbb{R} \right\}$  on the left

when we put  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} x \\ y \end{pmatrix} = \begin{pmatrix} ax+by \\ cx+dy \end{pmatrix}$  for all  $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in G, \begin{pmatrix} x \\ y \end{pmatrix} \in Y$ .

Clearly, the field  $\mathbb{R}$  can be replaced by any field in this example.

**(c)** Let  $X = \mathbb{Z} \times \mathbb{Z} \times \mathbb{Z}$  and  $G = SL(2, \mathbb{Z}) = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in Mat_2(\mathbb{Z}) : \alpha\delta - \beta\gamma = 1 \right\}$ .

Then  $G$  acts on  $X$  when we define  $(a,b,c) \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$  to be

$$(a\alpha^2 + b\alpha\gamma + c\gamma^2, 2a\alpha\beta + b(\alpha\delta + \beta\gamma) + 2c\gamma\delta, a\beta^2 + b\beta\delta + c\delta^2).$$

The verification is left to the reader.

**(d)** Suppose  $G$  acts on  $X$  on the left and we denote the element of  $X$  corresponding to the pair  $g,x$  ( $g \in G, x \in X$ ) by  $g*x$ . Then  $G$  acts on  $X$  on the right when we put  $xg := g^{-1}*x$ , because

$$(xg_1)g_2 = (g_1^{-1}*x)g_2 = g_2^{-1}*(g_1^{-1}*x) = g_2^{-1}g_1^{-1}*x = (g_1g_2)^{-1}*x = x(g_1g_2)$$

and

$$x1 = 1^{-1}*x = 1*x = x$$

for all  $x \in X$ ,  $g_1, g_2 \in G$ . We could not write  $xg := g*x$ , for then we would get  $(xg_1)g_2 = x(g_2g_1)$  instead of  $(xg_1)g_2 = x(g_1g_2)$ . However, if  $G$  is commutative,  $G$  acts on  $X$  on the right when we put  $xg := g*x$ .

**(e)** Let  $F$  be a nonempty subset of the Euclidean plane  $E$ . Then  $Sym F$  acts on  $F$ , because  $f\sigma \in F$  for all  $f \in F$ ,  $\sigma \in Sym F$  and

$$\begin{aligned} f(\sigma_1\sigma_2) &= (f\sigma_1)\sigma_2 \\ f\iota &= f \end{aligned}$$

for all  $f \in F$ ,  $\sigma_1, \sigma_2 \in Sym F$ .

**(f)** Let  $G$  be a group. Then  $Aut(G)$  acts on  $G$ , because  $g(\alpha_1\alpha_2) = (g\alpha_1)\alpha_2$  and  $g\iota = g$  for all  $g \in G$  and for all  $\alpha_1, \alpha_2 \in Aut(G)$ .

**(g)** Let  $\mathfrak{X}$  be the set of all nonempty subsets of the Euclidean plane  $E$ . Then  $S_E$  acts on  $\mathfrak{X}$  since  $(F\alpha)\beta = F(\alpha\beta)$  and  $F\iota = F$  for all  $F \in \mathfrak{X}$  and  $\alpha, \beta \in S_E$  (Lemma 14.1).

**(h)** Assume that a group  $G$  acts on a set  $X$ . Then any subgroup of  $G$  also acts on  $X$ .

In the next two theorems, we shall show that any group action on a set  $X$  is essentially a homomorphism into  $S_X$ .

**25.3 Theorem:** *Let  $G$  act on  $X$ . For each  $g \in G$ , consider  $x \rightarrow xg$  as a function and put  $\rho_g : X \rightarrow X$ . Then  $\rho_g \in S_X$  and the mapping*

$$x \rightarrow xg$$

$$\begin{aligned} \rho : G &\rightarrow S_X \\ g &\rightarrow \rho_g \end{aligned}$$

*is a homomorphism (called the permutation representation of  $G$  corresponding to the action).*

**Proof:** Let  $g \in G$ . Since  $G$  acts on  $X$ , to each  $x \in X$ , there corresponds a uniquely determined element  $xg$  of  $X$ . Hence  $\rho_g : x \rightarrow xg$  is indeed a function from  $X$  into  $X$ .

For any  $x \in X$ ,  $g_1, g_2 \in G$ , we have

$$x\rho_{g_1g_2} = x(g_1g_2) = (xg_1)g_2 = (xg_1)\rho_{g_2} = (x\rho_{g_1})\rho_{g_2} = x(\rho_{g_1}\rho_{g_2}),$$

so 
$$\rho_{g_1g_2} = \rho_{g_1}\rho_{g_2}.$$

(1)

Furthermore,  $x\rho_1 = x1 = x$  for all  $x \in X$ , hence

$$\rho_1 = \iota_X \in S_X.$$

(2)

From (1) and (2), we obtain

$$\rho_g\rho_{g^{-1}} = \rho_{gg^{-1}} = \rho_1 = \iota_X = S_X; \quad \rho_{g^{-1}}\rho_g = \rho_{g^{-1}g} = \rho_1 = \iota_X = S_X$$

and thus  $\rho_g$  is one-to-one and onto (Theorem 3.17(2)). So  $\rho_g \in S_X$  for all  $g$  in  $G$ .

So we have a mapping  $\rho: G \rightarrow S_X$  and it is a homomorphism by (1).

□

$$g \rightarrow \rho_g$$

**25.4 Theorem:** *Let  $X$  be a nonempty set and let  $\sigma: G \rightarrow S_X$  be a group homomorphism. Then  $G$  acts on  $X$  when we put*

$$xg = x(g\sigma)$$

for all  $x \in X$ ,  $g_1, g_2 \in G$ . Furthermore, the permutation representation of  $G$  corresponding to this action is  $\sigma$ .

**Proof:** The proof consists in observing that  $\sigma$  is a homomorphism. We have

$$(xg_1)g_2 = (xg_1)(g_2\sigma) = (x(g_1\sigma))(g_2\sigma) = x((g_1\sigma)(g_2\sigma)) = x((g_1g_2)\sigma) = x(g_1g_2)$$

and

$$x1 = x(1\sigma) = x$$

for all  $x \in X$ ,  $g_1, g_2 \in G$ . Here we use the fact that  $1\sigma \in S_X$  is the identity element of the group  $S_X$  (Lemma 20.3(a)), which is the identity mapping on  $X$ . Thus setting  $xg = x(g\sigma)$  does define a group action.

Let us find the permutation representation of  $G$  corresponding to this action. This is  $\rho: G \rightarrow S_X$ ,  $g \rightarrow \rho_g$  where  $\rho_g$  is the mapping  $x \rightarrow xg$  on  $G$ . Since

$$x\rho_g = xg = x(g\sigma)$$

for all  $x \in X$ ,  $g \in G$ , we have  $\rho_g = g\sigma$  for all  $g \in G$ . Hence  $\rho = \sigma$  by the definition of equality of mappings.  $\square$

We now show that group actions define an equivalence relation on the underlying set  $X$ . The number of elements in an equivalence class can be expressed in group theoretical terms. This gives some arithmetical information about groups.

**25.5 Lemma:** *Let  $G$  act on  $X$ . for any  $x, y \in X$ , we put  $x \sim y$  if and only if there is an element  $g \in G$  such that  $xg = y$ . Then  $\sim$  is an equivalence relation on  $X$ .*

**Proof:** (cf. Lemma 15.7.) (i) Since  $1 \in G$  and  $x1 = x$  for all  $x \in X$ , we have  $x \sim x$  for all  $x \in X$ . Thus  $\sim$  is reflexive.

(ii) If  $x, y \in X$  and  $x \sim y$ , then there is a  $g \in G$  such that  $xg = y$ , so  $yg^{-1} = (xg)g^{-1} = x(gg^{-1}) = x1 = x$ . From  $g^{-1} \in G$  and  $yg^{-1} = x$ , we conclude  $y \sim x$ . Thus  $\sim$  is symmetric.

(iii) Suppose  $x, y, z \in X$  and  $x \sim y$ ,  $y \sim z$ . Then there are  $g, h \in G$  such that  $xg = y$  and  $yh = z$ . Then  $x(gh) = (xg)h = yh = z$ . From  $gh \in G$  and  $x(gh) = z$ , we conclude  $x \sim z$ . Thus  $\sim$  is transitive.

So  $\sim$  is an equivalence relation on  $X$ .  $\square$

**25.6 Definition:** Let  $G$  act on  $X$ . The equivalence classes of the equivalence relation in Lemma 25.5 are called *orbits*. The equivalence class  $\{xg \in X: g \in G\}$  of  $x \in X$  is called the *orbit of  $x$* .

**25.7 Lemma:** *Let  $G$  act on  $X$ . For  $x \in X$ , we write*

$$Stab_G(x) = \{g \in G: xg = x\}.$$

*Then  $Stab_G(x)$  is a subgroup of  $G$  (called the stabilizer of  $x$  in  $G$ ).*

**Proof:** The proof is a routine application of our subgroup criterion.

(i) Let  $g, h \in \text{Stab}_G(x)$ . Then  $xg = x$  and  $xh = x$ . So  $x(gh) = (xg)h = xh = x$ , so  $gh \in \text{Stab}_G(x)$ . Hence  $\text{Stab}_G(x)$  is closed under multiplication.

(ii) Let  $g^{-1} \in \text{Stab}_G(x)$ . Then  $xg = x$ . So  $xg^{-1} = (xg)g^{-1} = x(gg^{-1}) = x1 = x$ , so  $g^{-1} \in \text{Stab}_G(x)$ . Hence  $\text{Stab}_G(x)$  is closed under the forming of inverses.

Thus  $\text{Stab}_G(x) \leq G$ . □

Stabilizers of elements in the same orbit are closely related.

**25.8 Lemma:** Let  $G$  act on  $X$ . Let  $x \in X$  and  $g \in G$ . Then

$$\text{Stab}_G(xg) = g^{-1}\text{Stab}_G(x)g.$$

**Proof:** As

$$\begin{aligned} h \in \text{Stab}_G(xg) &\Leftrightarrow (xg)h = xg \\ &\Leftrightarrow x(gh) = xg \\ &\Leftrightarrow (x(gh))g^{-1} = x \\ &\Leftrightarrow x(ghg^{-1}) = x \\ &\Leftrightarrow ghg^{-1} \in \text{Stab}_G(x) \\ &\Leftrightarrow h \in g^{-1}\text{Stab}_G(x)g, \end{aligned}$$

$$\text{Stab}_G(xg) = g^{-1}\text{Stab}_G(x)g. \quad \square$$

The kernel of the permutation representation can be expressed in terms of the stabilizers.

**25.9 Lemma:** Assume  $G$  acts on  $X$  and let  $\rho: G \rightarrow S_X$  be the permutation representation. Then  $\text{Ker } \rho = \bigcap_{x \in X} \text{Stab}_G(x)$ .

**Proof:** For  $g \in G$ , we have  $\rho: g \rightarrow \rho_g \in S_X$ , where  $\rho_g: x \rightarrow xg$ . Hence

$$\begin{aligned} \text{Ker } \rho &= \{g \in G: \rho_g = 1 \in S_X\} \\ &= \{g \in G: x\rho_g = x \text{ for all } x \in X\} \end{aligned}$$

$$\begin{aligned}
&= \{g \in G: xg = x \text{ for all } x \in X\} \\
&= \bigcap_{x \in X} \{g \in G: xg = x\} \\
&= \bigcap_{x \in X} \text{Stab}_G(x). \quad \square
\end{aligned}$$

The following elementary counting principle has many applications.

**25.10 Lemma:** *Let  $G$  act on  $X$ . For any  $x \in X$ , we have*

$$|\text{orbit of } x| = |G:\text{Stab}_G(x)|.$$

**Proof:** The orbit of  $x$  is the set  $\{xg \in X: g \in G\}$ . The index  $|G:\text{Stab}_G(x)|$  is the number of right cosets of  $\text{Stab}_G(x)$  in  $G$ , more precisely, the cardinal number of  $\mathfrak{R} = \{\text{Stab}_G(x)g: g \in G\}$ . We must find a one-to-one correspondence between the orbit  $\{xg \in X: g \in G\}$  of  $x$  and the set  $\mathfrak{R} = \{\text{Stab}_G(x)g: g \in G\}$  of the right cosets of  $\text{Stab}_G(x)$  in  $G$ . The description of these sets leads us to consider the mapping

$$\begin{aligned}
\alpha: \text{orbit of } x &\rightarrow \mathfrak{R}, \\
xg &\rightarrow Sg
\end{aligned}$$

where we put  $S = \text{Stab}_G(x)$  for brevity. Let us see if  $\alpha$  is one-to-one and onto.

Before that, however, we must check that  $\alpha$  is well defined, for one and the same element in the orbit of  $x$  can have representations  $xg, xh$  with  $g \neq h$ . We must prove that  $xg = xh$  implies  $Sg = Sh$ . If  $xg = xh$ , then  $x(gh^{-1}) = (xg)h^{-1} = (xh)h^{-1} = x(hh^{-1}) = x1 = x$ , so  $gh^{-1} \in S$  and therefore  $Sg = Sh$  by Lemma 10.2(5). Thus  $\alpha$  is well defined.

That  $\alpha$  is one-to-one follows by reversing the argument above. If  $(xg)\alpha = (xh)\alpha$ , then  $Sg = Sh$ , then  $gh^{-1} \in S$ , then  $x(gh^{-1}) = x$ , then  $(x(gh^{-1}))h = xh$ , so  $xg = xh$ . Therefore  $\alpha$  is one-to-one.

$\alpha$  is certainly onto, since any  $Sg \in \mathfrak{R}$  is the image of  $xg$  in the orbit of  $x$ .

Thus  $\alpha$  is a one-to-one mapping from the orbit of  $x$  onto  $\mathfrak{R}$ . This gives

$$|\text{orbit of } x| = |G:\text{Stab}_G(x)|. \quad \square$$

**25.11 Definition:** Let  $G$  act on  $X$ . We say  $G$  acts transitively on  $X$  or the action of  $G$  on  $X$  is said to be a *transitive* action if, for any  $x, y \in X$ , there is a  $g \in G$  such that  $xg = y$ . If  $G$  does not act transitively on  $X$ , then  $G$  is said to act *intransitively* on  $X$ .

Thus  $G$  acts transitively on  $X$  if and only if there is one and only one orbit. The whole set  $X$  is the single orbit of the action.

**25.12 Examples: (a)** A group  $G$  acts on itself by right multiplication: to the pair  $x, g \in G$ , there corresponds the product  $xg \in G$ . The conditions  $(xg_1)g_2 = x(g_1g_2)$  and  $x1 = x$  (for all  $x, g_1, g_2 \in G$ ) are immediate from the associativity of multiplication and from the definition of the identity element. This action is transitive, because, given any  $x, y \in G$ , there is an element  $g$  in  $G$ , namely  $g = x^{-1}y$ , such that  $xg = y$ . Hence, for any  $x \in G$ , we have  $|G| = |\text{orbit of } x| = |G:Stab_G(x)|$ , thus  $Stab_G(x) = 1$ , as can be seen also from  $Stab_G(x) = \{g \in G: xg = x\} = \{g \in G: g = 1\} = \{1\} = 1$ . This action is called the *regular action of  $G$  on  $G$* . The kernel of the permutation representation  $\rho: G \rightarrow S_X$  is  $Ker \rho = \bigcap_{x \in X} Stab_G(x) = 1$  by Lemma 25.9. Thus  $\rho$  is one-to-one and Theorem 20.16 gives  $G \cong G/1 = G/Ker \rho \cong Im \rho \leq S_G$ .

**(b)** The preceding example can be generalized. Let  $H \leq G$  and let  $\mathfrak{R} = \{Ha: a \in G\}$  be the set of all right cosets of  $H$  in  $G$ . Then  $G$  acts on  $\mathfrak{R}$  by right multiplication, where, to the pair  $Ha, g$ , there corresponds the coset  $Hag$ , because

$$((Ha)g_1)g_2 = (Hag_1)g_2 = H((ag_1)g_2) = H(a(g_1g_2)) = (Ha)(g_1g_2)$$

and

$$(Ha)1 = Ha1 = Ha$$

for all  $Ha \in \mathfrak{R}$ ,  $g_1, g_2 \in G$ .

This action is transitive, because, given any  $Ha, Hb \in \mathfrak{R}$ , there is an element  $g$  in  $G$ , namely  $g = a^{-1}b$ , such that  $(Ha)g = Hb$ .

We have  $Stab_G(H) = \{g \in G: Hg = H\} = \{g \in G: g \in H\} = H$

and  $Stab_G(Ha) = a^{-1}Stab_G(H)a = a^{-1}Ha$

by Lemma 25.8.

The kernel of the permutation representation  $\rho: G \rightarrow S_{\mathfrak{R}}$  is, by Lemma 25.9,

$$\text{Ker } \rho = \bigcap_{Ha \in \mathfrak{R}} \text{Stab}_G(Ha) = \bigcap_{a \in G} \text{Stab}_G(Ha) = \bigcap_{a \in G} a^{-1}Ha.$$

The intersection  $\bigcap_{a \in G} a^{-1}Ha$  is called the *core of H in G*, and is designated by  $H_G$ . Theorem 20.16 gives now  $G/H_G = G/\text{Ker } \rho \cong \text{Im } \rho \leq S_{\mathfrak{R}}$ .

**25.13 Theorem :** *Let G be a group.*

(1) (Cayley's theorem) *G is isomorphic to a subgroup of  $S_G$ .*

(2) *Let  $H \leq G$  be of index  $|G:H| = n$ . Then  $G/H_G$  is isomorphic to a subgroup of  $S_n$ .*

**Proof:** (1) This follows from Example 25.12(a).

(2) From Example 25.12(b), it follows that  $G/H_G$  is isomorphic to a subgroup of  $S_{\mathfrak{R}}$ , where  $\mathfrak{R}$  is a set with  $n$  elements. Let  $\mu: \mathfrak{R} \rightarrow \{1, 2, \dots, n\}$  be a one-to-one mapping from  $\mathfrak{R}$  onto  $\{1, 2, \dots, n\}$ . Then, for each  $f \in S_{\mathfrak{R}}$ , the mapping  $\mu^{-1}f\mu$  is a one-to-one mapping from  $\{1, 2, \dots, n\}$  onto  $\{1, 2, \dots, n\}$ , so  $\mu^{-1}f\mu \in S_n$ . Now the function

$$\begin{aligned} M: S_{\mathfrak{R}} &\rightarrow S_n, \\ f &\rightarrow \mu^{-1}f\mu \end{aligned}$$

is easily verified to be a homomorphism:  $fgM = \mu^{-1}fg\mu = \mu^{-1}f\mu\mu^{-1}g\mu = fMgM$  for all  $f, g \in S_{\mathfrak{R}}$ ; and  $M$  is one-to-one and onto, because the mapping

$$\begin{aligned} N: S_n &\rightarrow S_{\mathfrak{R}} \\ \sigma &\rightarrow \mu\sigma\mu^{-1} \end{aligned}$$

is such that  $MN = \text{identity mapping on } S_{\mathfrak{R}}$  and  $NM = \text{identity mapping on } S_n$  (Theorem 3.17(2)). Hence  $M$  is an isomorphism and  $S_{\mathfrak{R}} \cong S_n$ . Together with  $G/H_G \cong S_{\mathfrak{R}}$ , this gives  $G/H_G \cong S_n$ .  $\square$

**25.14 Example:** Another important group action is *conjugation*. For any  $x, g \in G$ , we call  $g^{-1}xg$  the *conjugate of x by g*. In order to avoid any

confusion with right multiplication, we shall write  $x^g$  for  $g^{-1}xg$ . This notation is standard. Since

$$(x^{g_1})^{g_2} = (g_1^{-1}xg_1)^{g_2} = g_2^{-1}(g_1^{-1}xg_1)g_2 = g_2^{-1}g_1^{-1}xg_1g_2 = (g_1g_2)^{-1}x(g_1g_2) = x^{(g_1g_2)}$$

and

$$x^1 = 1^{-1}x1 = x$$

for all  $x, g_1, g_2 \in G$ , conjugation is indeed an action of  $G$  on  $G$ .

The orbit  $\{x^g : g \in G\} = \{g^{-1}xg : g \in G\}$  of  $x \in G$  is called the *conjugacy class* of  $x$ . We have

$$\text{Stab}_G(x) = \{g \in G : x^g = x\} = \{g \in G : g^{-1}xg = x\} = \{g \in G : xg = gx\};$$

so  $\text{Stab}_G(x)$  consists of the all those elements in  $G$  which commute with  $x$ . It is called the *centralizer of  $x$  in  $G$*  in this case and is denoted by  $C_G(x)$ .

The permutation representation is  $\tau : G \rightarrow S_G$ , where  $\tau_g : G \rightarrow G$ . Hence  $\tau_g$  is

$$g \rightarrow \tau_g \quad x \rightarrow x^g$$

the inner automorphism of  $G$  induced by  $g$ . We get

$$\text{Ker } \tau = \bigcap_{x \in G} C_G(x) = \bigcap_{x \in G} \{g \in G : xg = gx\} = \{g \in G : xg = gx \text{ for all } x \in G\} = Z(G)$$

as we know also from the proof of Theorem 23.10. In this case, Lemma 25.10 assumes the following form.

**25.15 Lemma:** *Let  $G$  be a group and  $x \in G$ . Then*

$$|\text{conjugacy class of } x| = |G:C_G(x)|. \quad \square$$

**25.16 Lemma (Class equation):** *Let  $G$  be a finite group. Assume  $G$  has  $k$  distinct conjugacy classes and let  $x_1, x_2, \dots, x_k$  be representatives of these classes. Then*

$$|G| = \sum_{i=1}^k |G:C_G(x_i)|.$$

**Proof:** Conjugacy is an equivalence relation on  $G$  and gives rise to a partition of  $G$  (Theorem 2.5):

$$G = \bigcup_{i=1}^k \text{conjugacy class of } x_i,$$

the union being disjoint. Counting the number of elements on both sides, and using Lemma 25.15, we obtain

$$|G| = \sum_{i=1}^k |\text{conjugacy class of } x_i| = \sum_{i=1}^k |G:C_G(x_i)|. \quad \square$$

We give an important application of the class equation.

**25.17 Theorem:** *Let  $G$  be a group of order  $p^n$ , where  $p$  is prime and  $n$  is a natural number. Then  $Z(G) \neq 1$ .*

**Proof:** Let  $k$  be the number of conjugacy classes in  $G$ , and let  $x_1, x_2, \dots, x_k$  be representatives of these classes. Then, in the class equation

$$|G| = \sum_{i=1}^k |G:C_G(x_i)|,$$

each summand on the right hand side is a divisor of  $p^n$  by Lagrange's theorem. So  $|G:C_G(x_i)| = p^{m_i}$  with suitable nonnegative integers  $m_i$  (for each  $i = 1, 2, \dots, k$ ). Thus the class equation is

$$p^n = p^{m_1} + p^{m_2} + \dots + p^{m_k}.$$

Here  $p^{m_i} = 1$  if and only if  $|G:C_G(x_i)| = 1$ , so if and only if  $C_G(x_i) = G$ , and so if and only if  $x_i \in Z(G)$ . Thus exactly  $|Z(G)|$  summands on the right hand side are equal to 1, and the class equation gives

$$p^n = |Z(G)| + (\text{a sum of powers of } p \text{ greater than } p^0 = 1)$$

(The second term is absent in case  $|G| = |Z(G)|$ ; in this case  $Z(G) = G \neq 1$ ). The last equation tells us that  $|Z(G)|$  is divisible by  $p$ , so  $|Z(G)| \neq 1$ , hence  $Z(G) \neq 1$ . □

**25.18 Lemma:** *Let  $p$  be a prime number. If  $G$  is a group of order  $p^2$ , then  $G$  is abelian.*

**Proof:** We must show  $Z(G) = G$ , or, equivalently,  $|Z(G)| = p^2$ . We know  $|Z(G)| = 1$  or  $p$  or  $p^2$  by Lagrange's theorem, and  $|Z(G)| \neq 1$  by Theorem 25.17. We suppose, by way of contradiction, that  $|Z(G)| = p$ . Since  $Z(G) \triangleleft$

$G$  (Theorem 23.3), we can build the factor group  $G/Z(G)$ , which has order  $p^2/p = p$  and which is therefore cyclic by Theorem 11.13. Then  $G$  must be abelian by Lemma 23.5, and  $|Z(G)| = p^2$ , contrary to the assumption  $|Z(G)| = p$ . Thus  $|Z(G)| = p$  is impossible and there remains only the possibility  $|Z(G)| = p^2$ . Hence  $G$  is abelian.

□

We wish to present the basic idea in the proof of Theorem 25.17 in its purest form. We need a definition.

**25.19 Definition:** Let  $G$  act on  $X$ . If  $x \in X$ ,  $g \in G$  and  $xg = x$ , we say that  $g$  fixes  $x$ . The set

$$\{x \in X: xg = x \text{ for all } g \in G\} = \{x \in X: \text{Stab}_G(x) = G\}$$

of all elements in  $X$  which are fixed by each element of  $G$  is called the *fixed point subset of  $X$*  and denoted by  $\text{Fix}_X(G)$ .

Thus  $\text{Fix}_X(G)$  consists of all those elements in  $X$  which form an orbit with only one element in it. When we count the number of elements in  $X$  as the sum of the number of elements in each orbit, each element in  $\text{Fix}_X(G)$  contributes 1 to this sum. Notice that, under the action of a group  $G$  on itself by conjugation,  $\text{Fix}_G(G)$  is nothing else than  $Z(G)$ .

**25.20 Lemma:** Let  $G$  act on  $X$ . If  $G$  has order  $p^n$ , where  $p$  is a prime number and  $n \in \mathbb{N}$ , and  $X$  is a finite set, then

$$|X| \equiv |\text{Fix}_X(G)| \pmod{p}.$$

**Proof:** We consider the equivalence relation  $\sim$  of Lemma 25.5 on  $X$ . Under this equivalence relation,  $X$  is partitioned into finitely many disjoint orbits, say

$$X = \bigcup_{i=1}^k \text{orbit of } x_i.$$

Counting the number of elements on both sides, we get

$$|X| = \sum_{i=1}^k |\text{orbit of } x_i|$$

Hence, by Lemma 25.10,  $|X| = \sum_{i=1}^k |G:\text{Stab}_G(x_i)|.$

Now each of the indices  $|G:\text{Stab}_G(x_i)|$  is a divisor of  $|G| = p^n$ , hence is equal to some power  $p^{m_i}$  of  $p$  with a nonnegative integer  $m_i$ . Here  $p^{m_i} = p^0 = 1$  if and only if  $G = \text{Stab}_G(x_i)$ , that is to say, if and only if  $x_i \in \text{Fix}_X(G)$ . Thus there are exactly  $|\text{Fix}_X(G)|$  summands equal to 1, and the sum above becomes

$$|X| = (\mathbf{1} + \mathbf{1} + \cdots + \mathbf{1}) + (\text{sum of } p^{m_i} \text{ with } m_i > 0)_{|\text{Fix}_X(G)| \text{ times}}$$

(the second term is missing in case there is no  $p^{m_i}$  with  $m_i > 0$ ). So

$$|X| = |\text{Fix}_X(G)| + (\text{a number divisible by } p)$$

and therefore  $|X| \equiv |\text{Fix}_X(G)| \pmod{p}$ , as was to be proved. □

We end this paragraph with a generalization of conjugation.

**25.21 Example:** Let  $G$  be a group and let  $\mathfrak{X}$  be the set of all nonempty subsets of  $G$ . For any  $U \in \mathfrak{X}$  and  $g \in G$ , we put

$$U^g = \{u^g \in G: u \in U\} = \{g^{-1}ug \in G: u \in U\} = g^{-1}Ug.$$

$U^g$  consists therefore of conjugates by  $g$  of the elements of  $U$  and is called the *conjugate of  $U$  by  $g$* . With this definition,  $G$  acts on  $\mathfrak{X}$ , because

$$(U^{g_1})^{g_2} = \{u^{g_1} \in G: u \in U\}^{g_2} = \{(u^{g_1})^{g_2} \in G: u \in U\} = \{u^{(g_1g_2)} \in G: u \in U\} = U^{(g_1g_2)}$$

and

$$U^1 = 1^{-1}U1 = U$$

for all  $U \in \mathfrak{X}, g_1, g_2 \in G$ .

The orbit  $\{U^g: g \in G\} = \{g^{-1}Ug: g \in G\}$  of  $U \in \mathfrak{X}$  is called the *conjugacy class* of  $U$ . We have

$$\text{Stab}_G(U) = \{g \in G: U^g = U\} = \{g \in G: g^{-1}Ug = U\} = \{g \in G: Ug = gU\};$$

so  $\text{Stab}_G(U)$  consists of the all those elements in  $G$  which fix  $U$  as a set. It is called the *normalizer of  $U$  in  $G$*  in this case and is denoted by  $N_G(U)$ .

The set

$$\begin{aligned} & \{g \in G: u^g = u \text{ for all } u \in U\} \\ &= \{g \in G: g^{-1}ug = u \text{ for all } u \in U\} = \{g \in G: ug = gu \text{ for all } u \in U\} \end{aligned}$$

of all those elements in  $G$  which fix each element of  $U$  under conjugation, or, what is the same, which commute with every element of  $U$ , is called the *centralizer of  $U$  in  $G$*  and is denoted by  $C_G(U)$ . So  $C_G(U)$  is the intersection of the centralizers of the elements of  $U$ :

$$C_G(U) = \bigcap_{u \in U} C_G(u).$$

In particular,  $C_G(U)$  is a subgroup of  $G$ . We have  $C_G(U) \leq N_G(U) \leq G$ .

The orbit of  $U \in \mathfrak{X}$  is

$$\{U^g \in \mathfrak{X}: g \in G\} = \{g^{-1}Ug \in \mathfrak{X}: g \in G\}$$

and is called the *conjugacy class of  $U$  in  $G$* . We have

$$|\text{conjugacy class of } U| = |G:N_G(U)|$$

by Lemma 25.10.

In general,  $U$  neither contains nor is contained in  $C_G(U)$  or  $N_G(U)$ . However, if  $U$  happens to be a subgroup of  $G$ , we have  $g^{-1}ug \in U$  for all  $u, g$  in  $U$ , so  $U^g = \{u^g \in G: u \in U\} = \{g^{-1}ug \in G: u \in U\} \subseteq U$  and, for any  $g$  in  $U$ , we get  $U \subseteq (U^{g^{-1}})^g \subseteq U^g \subseteq U$ , thus  $U^g = U$  and  $U \leq N_G(U)$ .

We collect the last two remarks in a theorem.

**25.22 Theorem:** *Let  $G$  be a group and let  $H$  be a subgroup of  $G$ . Then*

$$H \leq N_G(H) \leq G \text{ and } |\text{conjugacy class of } H| = |G:N_G(H)|. \quad \square$$

## Exercises

1. Prove that  $SL(2, \mathbb{Z})$  acts on  $X := \left\{ \begin{pmatrix} a & b/2 \\ b/2 & c \end{pmatrix} : a, b, c \in \mathbb{Z} \right\}$  when we associate the matrix  $g^t x g$  with the pair  $(x, g) \in X \times SL(2, \mathbb{Z})$ .
2. Let  $G$  act on  $X$  and let  $H$  be a subgroup of  $G$ . Show that
$$Stab_G(x) = Stab_G(x) \cap H$$
for any  $x \in X$ .
3. Let  $G$  act on  $X$  and  $H$  act on  $Y$ . Prove that the direct product  $G \times H$  acts on the cartesian product  $X \times Y$ .
4. Give an examples of groups  $G$  and subsets  $U$  of  $G$  such that  $U \not\subseteq N_G(U)$ ,  $N_G(U) \not\subseteq U$ ,  $U \not\subseteq C_G(U)$ ,  $C_G(U) \not\subseteq U$ .
5. Prove that  $C_G(U) \trianglelefteq N_G(U)$  for any nonempty subset  $U$  of a group  $G$ .
6. Let  $H \leq G$ . Show that  $N_G(H)$  acts on  $H$  by conjugation. Considering the permutation representation of this action, prove that  $N_G(H)/C_G(H)$  is isomorphic to a subgroup of  $Aut(H)$ .
7. Assume  $G$  acts on  $X$ , and let  $K$  be the kernel of the permutation representation of this action. Suppose  $H \trianglelefteq G$  and  $H \leq K$ . Show that  $G/H$  acts on  $X$  when we put  $x(Hg) = xg$  for all  $x \in X$ ,  $Hg \in G/H$ . What is the kernel of the permutation representation?