LECTURE 9
Groups acting on sets

PAVEL RŮŽIČKA

ABSTRACT. We study groups acting on sets. We call sets equipped with an action of a group $\boldsymbol{G}$-sets. We define an orbit and a stabilizer of an element of a $\boldsymbol{G}$-sets. We prove the Burnside's lemma and the class formula and we show some applications of these results. In particular, we introduce some ideas of the Pólya's theory of counting.

9.1. **$\boldsymbol{G}$-sets, orbits, and stabilizers.** Let $\boldsymbol{G} = (G, \cdot)$ be a group. An *action* of the group $\boldsymbol{G}$ on a set X is a homomorphism

$$\alpha\colon \boldsymbol{G} \to \boldsymbol{S}_X.$$

A set X equipped with an action of a group $\boldsymbol{G}$ on X is often referred to as a ***$\boldsymbol{G}$-set***.

Having fixed an action α of the group $\boldsymbol{G}$ on a set X, we put $\alpha(g)(x) = g \cdot x$, for all $g \in G$ and $x \in X$. Thus the action corresponds to the map $G \times X \to X$ given by $\langle g, x\rangle \mapsto g \cdot x$. It is easily seen from the definition of a group homomorphism that

(i) $(f \cdot g) \cdot x = f \cdot (g \cdot x)$, for all $f, g \in G$ and all $x \in X$.
(ii) $u_{\boldsymbol{G}} \cdot x = x$, for all $x \in X$.

On the other hand,

Lemma 9.1. *Any map $G \times X \to X$ satisfying properties (i) and (ii) corresponds to an action of the group $\boldsymbol{G}$ on the set X.*

Proof. For each $g \in G$ we define a map $\alpha(g)\colon X \to X$ by $\alpha(g)(x) = g \cdot x$, $x \in X$.

First we prove that $\alpha(g)$ is a bijection for all $g \in G$. Let $g \in G$ and $x \in X$. Then

$$g^{-1} \cdot \alpha(g)(x) = g^{-1} \cdot (g \cdot x) = (g^{-1} \cdot g) \cdot x = u_{\boldsymbol{G}} \cdot x = x,$$

hence the image $\alpha(g)(x)$ determines x, whence $\alpha(g)$ is one-to-one. Since

$$\alpha(g)(g^{-1} \cdot x) = g \cdot (g^{-1} \cdot x) = (g \cdot g^{-1}) \cdot x = u_{\boldsymbol{G}} \cdot x = x,$$

the map $\alpha(g)$ maps the set X onto X. We conclude that $\alpha(g)$ is a bijection, and so α is a map from $\boldsymbol{G}$ to $\boldsymbol{S}_X$.

The Lecture and the tutorial took place in Malá strana, room S11, on December 4, 2018.

For all $f, g \in G$ and all $x \in X$ we have that

$$\alpha(f \cdot g)(x) = (f \cdot g) \cdot x = f \cdot (g \cdot x) = \alpha(f)(\alpha(g)(x)),$$

hence $\alpha(f \cdot g) = \alpha(f) \circ \alpha(g)$. We conclude that $\alpha\colon \boldsymbol{G} \to \boldsymbol{S}_X$ is a group homomorphism. $\square$

Let X be a $\boldsymbol{G}$-set. For each $x \in X$, we set

$$G_x := \{g \in G \mid g \cdot x = x\}.$$

Lemma 9.2. *Let X be a $\boldsymbol{G}$-set. The set G_x determines a subgroup $\boldsymbol{G}_x$ of $\boldsymbol{G}$, for every $x \in X$.*

Proof. A simple verification gives that

$$f \cdot x = g \cdot x = x \implies (f \cdot g) \cdot x = f \cdot (g \cdot x) = f \cdot x = x,$$

for all $f, g \in G$, and

$$g \cdot x = x \implies g^{-1} \cdot x = g^{-1} \cdot (g \cdot x) = (g^{-1} \cdot g) \cdot x = u_{\boldsymbol{G}} \cdot x = x,$$

for all $g \in G$. $\square$

We call the subgroup $\boldsymbol{G}_x$ the *stabilizer*[1] of x. Next we define

$$\mathcal{O}_{\boldsymbol{G}}(x) := \{g \cdot x \mid g \in \boldsymbol{G}\}.$$

The set $\mathcal{O}_{\boldsymbol{G}}(x)$ is called a *$\boldsymbol{G}$-orbit* of x.

Lemma 9.3. *Let X be a $\boldsymbol{G}$-set. The binary relation $\sim_{\boldsymbol{G}}$ defined on the set X by $y \sim_{\boldsymbol{G}} x$ if $y = g \cdot x$ for some $g \in G$ is an equivalence on X and $\boldsymbol{G}$-orbits correspond to blocks of $\sim_{\boldsymbol{G}}$.*

Proof. Since $x = u_{\boldsymbol{G}} \cdot x$, the relation $\sim_{\boldsymbol{G}}$ is reflexive. If $y = g \cdot x$, then $x = u_{\boldsymbol{G}} \cdot x = (g^{-1} \cdot g) \cdot x = g^{-1} \cdot (g \cdot x) = g^{-1} \cdot y$, and so $\sim_{\boldsymbol{G}}$ is symmetric. Finally, if $x = f \cdot y$ and $y = g \cdot z$, then $x = f \cdot y = f \cdot (g \cdot z) = (f \cdot g) \cdot z$, hence $\sim_{\boldsymbol{G}}$ is transitive. We conclude that $\sim_{\boldsymbol{G}}$ is an equivalence on X. It is clear from the definition of $\boldsymbol{G}$-orbits that they correspond to blocks of $\sim_{\boldsymbol{G}}$. $\square$

Lemma 9.4. *Let X be a $\boldsymbol{G}$-set and $x \in X$. Then*

$$|\mathcal{O}_{\boldsymbol{G}}(x)| = [\boldsymbol{G} : \boldsymbol{G}_x]. \tag{9.1}$$

Proof. Observe that

$$f \cdot x = g \cdot x \iff g^{-1} \cdot f \in G_x,$$

for all $f, g \in G$. Applying Lemma 4.2, we see that elements of the $\boldsymbol{G}$-orbit $\mathcal{O}_{\boldsymbol{G}}(x)$ correspond to left cosets of $\boldsymbol{G}_x$. Equation (9.1) readily follows. $\square$

Corollary 9.5. *Let X be a $\boldsymbol{G}$-set and $x \in X$. Then*

$$|G| = |\mathcal{O}_{\boldsymbol{G}}(x)| \cdot |G_x|.$$

[1] Some authors call $\boldsymbol{G}_x$ the *isotropy subgroup* of x.

9.2. **Counting orbits.** Let X be a $\boldsymbol{G}$-set. We denote by $X/\boldsymbol{G}$ the set

$$X/\boldsymbol{G} := \{\mathcal{O}_{\boldsymbol{G}}(x) \mid x \in X\}$$

of all $\boldsymbol{G}$-orbits of X.

Lemma 9.6. *Let X be a $\boldsymbol{G}$-set. Then*

$$|X/\boldsymbol{G}| = \frac{1}{|G|}\sum_{x\in X}|G_x|. \tag{9.1}$$

Proof. Let Δ be a set of representatives of $\boldsymbol{G}$-orbits, i.e., Δ picks one element from each $\boldsymbol{G}$-orbit. Then we have that

$$|X/\boldsymbol{G}| = |\Delta| = \sum_{y\in\Delta}\frac{|\mathcal{O}_{\boldsymbol{G}}(y)|}{|\mathcal{O}_{\boldsymbol{G}}(y)|} = \sum_{y\in\Delta}\sum_{x\in\mathcal{O}_{\boldsymbol{G}}(y)}\frac{1}{|\mathcal{O}_{\boldsymbol{G}}(x)|} = \sum_{x\in G}\frac{1}{|\mathcal{O}_{\boldsymbol{G}}(x)|}. \tag{9.2}$$

It follows from Corollary 9.5 that

$$\frac{1}{|\mathcal{O}_{\boldsymbol{G}}(x)|} = \frac{|G_x|}{|G|},$$

for all $x \in X$. We conclude from (9.2) that

$$|X/\boldsymbol{G}| = \sum_{x\in G}\frac{1}{|\mathcal{O}_{\boldsymbol{G}}(x)|} = \sum_{x\in G}\frac{|G_x|}{|G|} = \frac{1}{|G|}\sum_{x\in G}|G_x|.$$

□

For each $g \in G$ we define

$$X_g := \{x \in X \mid g\cdot x = x\}.$$

Observe (see Figure 1) that

$$\sum_{x\in X}|G_x| = |\{\langle g, x\rangle \in G\times X \mid g\cdot x = x\}| = \sum_{g\in G}|X_g|. \tag{9.3}$$

Lemma 9.7 (Burnside's Lemma[2])**.** *Let X be a $\boldsymbol{G}$-set. Then*

$$|X/\boldsymbol{G}| = \frac{1}{|G|}\sum_{g\in G}|X_g|. \tag{9.4}$$

Proof. Apply Lemma 9.6 and equation (9.3). □

Burnside's lemma can be elegantly applied to solve some combinatorial problems.

Let $\mathcal{C}$ be a (finite) set of colors. By a *$\mathcal{C}$-coloring* of a set X we mean a map $\gamma\colon X \to \mathcal{C}$. We denote by ${}^X\mathcal{C}$ the set of all $\mathcal{C}$-colorings of the set X. A group $\boldsymbol{G}$ acting on the set X naturally acts on ${}^X\mathcal{C}$ via

$$(g\cdot\gamma)(x) = \gamma(g\cdot x), \quad \text{for all} \quad x \in X, \tag{9.5}$$

for all $\langle g, \gamma\rangle \in G \times {}^X\mathcal{C}$.

[2]Burnside's lemma is actually due to Frobenius (1887).

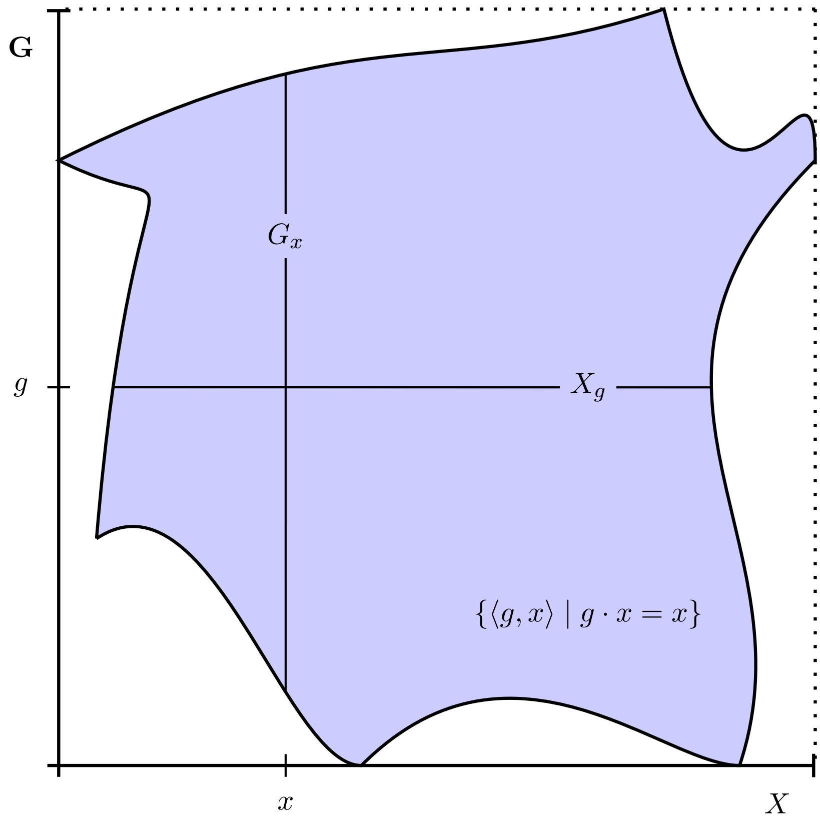

FIGURE 1. The set $\{\langle g, x\rangle \mid g \cdot x = x\}$

Lemma 9.8. *Let* $\alpha\colon \boldsymbol{G} \to \boldsymbol{S}_X$ *be an action of a group* G *on a set* X *and* $\mathcal{C}$ *a set of colors. Then*

$$|{}^{\mathcal{C}}X_g| = |\mathcal{C}|^k,$$

where k *is the number of cycles of* $\alpha(g) \in S_X$*, for all* $g \in G$.

Proof. Let $g \in G$ and γ be a $\mathcal{C}$-coloring of the set X. It follows from (9.5) that $g \cdot \gamma = \gamma$ if and only if $\gamma(x) = \gamma(g \cdot x)$, for all $x \in X$.This is equivalent to all elements of each cycle of $\alpha(g)$ having the same color. Therefore the size of ${}^{\mathcal{C}}X_g$ is the number of all possible colorings of cycles of g, which is $|\mathcal{C}|^k$. □

Example 9.9. *By coloring the faces of a cube by* n *colors, we can obtain exactly*

$$\frac{n^2}{24}\left(n^4 + 3n^2 + 12n + 8\right)$$

distinct cubes.

Proof. Let $\mathcal{C}$ be the set of n given colors. Two colorings of faces of a cube give identical cubes if and only they can be obtained from each other by rotations. The group $\boldsymbol{R}$ of all rotations of a cube acts on the set X of all faces of a cube (via the map $\alpha\colon \boldsymbol{R} \to \boldsymbol{S}_X$) and consequently $\boldsymbol{R}$ acts on the set of all colorings of the faces by colors from $\mathcal{C}$. Therefore the number of distinct cubes obtained by coloring faces of a cube equals to the size of the set ${}^{\mathcal{C}}X/\boldsymbol{R}$ of all $\boldsymbol{R}$-orbits of ${}^{\mathcal{C}}X$. Conjugated rotations act on X as conjugated permutations and so they have the same type (see Theorem 5.4), in particular, they have the same number of cycles. We have the following rotation of a cube:

(i) 1 identity u which corresponds to the type $\langle 6,0,0,0\rangle$, and so $|{}^{\mathcal{C}}X_u| = n^6$,
(ii) 3 rotation p over the axes connecting the centers of two opposite edges over the angle 180^o. Then $\operatorname{type}\alpha(p) = \langle 2,2,0,0\rangle$, and so $|{}^{\mathcal{C}}X_p| = n^4$,
(iii) 6 flips r, that is, rotations over axes connecting the centers of two opposite faces over the angle 180^o. Then $\operatorname{type}\alpha(r) = \langle 0,3,0,0\rangle$, and so $|{}^{\mathcal{C}}X_r| = n^3$,
(iv) 8 rotations s over diagonals of the cube. Then $\operatorname{type}\alpha(s) = \langle 0,0,2,0\rangle$, and so $|{}^{\mathcal{C}}X_s| = n^2$,
(v) 6 rotations t over axes connecting the centers of two opposite faces over the angle 90^o. Then $\operatorname{type}\alpha(t) = \langle 2,0,0,1\rangle$, and so $|{}^{\mathcal{C}}X_t| = n^3$.

According to Example 6.12 the group $\boldsymbol{R}$ is isomorphic to $\boldsymbol{S_4}$ and so it has 24 elements. Applying Burnside's lemma we compute that

$$|{}^{\mathcal{C}}X/\boldsymbol{R}| = \frac{1}{24}\left(n^6 + 3n^4 + 6n^3 + 8n^2 + 6n^3\right) = \frac{n^2}{24}\left(n^4 + 3n^2 + 12n + 8\right).$$

□

9.3. **Translations and the Lagrange's theorem revised.** We denote by $\mathcal{P}(X)$ the set of all subsets of a set X. Given a group $\boldsymbol{G}$, we set

$$\Lambda(g)(X) := g \cdot X, \quad \text{for all } g \in G, X \subseteq G.$$

Thus $\Lambda(g)\colon \mathcal{P}(G) \to \mathcal{P}(G)$ is a map with an inverse $\Lambda(g^{-1})$. It is straightforward to verify that $\Lambda\colon G \to S_{\mathcal{P}(G)}$ is an action of the group $\boldsymbol{G}$ on the set $\mathcal{P}(X)$.

Let $\boldsymbol{H}$ be a subgroup of the group $\boldsymbol{G}$. The stabilizer

$$\boldsymbol{G}_H = \{g \in G \mid g \cdot H = H\}$$

is the group $\boldsymbol{H}$ itself and the $\boldsymbol{G}$-orbit of H is the set

$$\mathcal{O}_{\boldsymbol{G}}(H) = \{g \cdot H \mid g \in G\}$$

of all left cosets of $\boldsymbol{H}$. The Lagrange's theorem is then follows from Lemma 9.4 and Corollary 9.5, indeed

$$|G| = |\mathcal{O}_{\boldsymbol{G}}(H)| \cdot |G_H| = [\boldsymbol{G} : \boldsymbol{H}] \cdot |H|.$$

9.4. **Conjugations and the class formula.** Let $\boldsymbol{G}$ be a group. An isomorphism $\boldsymbol{G} \to \boldsymbol{G}$ is called an *automorphism* of the group $\boldsymbol{G}$. It is straightforward that automorphisms of $\boldsymbol{G}$ are closed under composition and inverses, and so they form a group which we denote by $\mathrm{Aut}(\boldsymbol{G})$.

Recall that ${}^f g = f \cdot g \cdot f^{-1}$ denotes the conjugation of an element $g \in G$ by an element $f \in G$. Observe that

$$ {}^f(g \cdot h) = f \cdot (g \cdot h) \cdot f^{-1} = (f \cdot g \cdot f^{-1})(f \cdot h \cdot f^{-1}) = {}^f g \cdot {}^f h \tag{9.1} $$

and

$$ {}^{f \cdot g} h = (f \cdot g) \cdot h \cdot (f \cdot g)^{-1} = f \cdot g \cdot h \cdot g^{-1} \cdot f^{-1} = {}^f({}^g h), \tag{9.2} $$

for all $f, g, h \in G$. It follows from (9.1) and (9.2) that the conjugation by an element $f \in G$ induces an automorphism G with the inverse given by the conjugation by f^{-1}. The automorphisms induced by conjugations are called *inner automorphisms*. They form a subgroup of $\mathrm{Aut}(\boldsymbol{G})$ which we denote by $\mathrm{Inn}(\boldsymbol{G})$. Moreover, it follows from (9.2) that the map $\phi\colon \boldsymbol{G} \to \mathrm{Aut}(\boldsymbol{G})$ given by $f \mapsto (g \mapsto {}^f g)$ corresponds to the action

$$ G \times G \to G $$
$$ \langle f, g \rangle \mapsto {}^f g $$

of the group $\boldsymbol{G}$ on the set G. It is straightforward to see that the image of ϕ is the subgroup $\mathrm{Inn}(\boldsymbol{G})$ of all inner automorphisms and the kernel of ϕ is the center of $\boldsymbol{G}$ (cf. 6.2).

Let Δ be a set of representatives of orbits of ϕ. The orbits of ϕ correspond to conjugacy classes of $\boldsymbol{G}$. Since G is a disjoint union of the conjugacy classes, we have that

$$ |G| = \sum_{g \in \Delta} |\mathcal{O}_{\boldsymbol{G}}(g)|. \tag{9.3} $$

Lemma 9.10. *Let $\boldsymbol{G}$ be a group acting on itself by conjugation. Then*

$$ Z(\boldsymbol{G}) = \{g \in G \mid \mathcal{O}_{\boldsymbol{G}}(g) = \{g\}\}. $$

Proof. Let $g \in G$. Then

$$ {}^f g = g \iff f \cdot g \cdot f^{-1} = g \iff f \cdot g = g \cdot f, $$

for all $f \in G$. Therefore ${}^f g = g$ for all $f \in G$ if and only if $g \in Z(\boldsymbol{G})$. $\square$

It follows that $Z(\boldsymbol{G}) \subseteq \Delta$ and we infer from (9.3) that

$$ |G| = |Z(\boldsymbol{G})| + \sum_{g \in \Delta \setminus Z(\boldsymbol{G})} |\mathcal{O}_{\boldsymbol{G}}(g)|. \tag{9.4} $$

Let $\boldsymbol{u}_{\boldsymbol{G}}$ denote the trivial subgroup of $\boldsymbol{G}$. It follows from Lemma 9.4 that $|\mathcal{O}_{\boldsymbol{G}}(g)| = [\boldsymbol{G} : \boldsymbol{G}_g]$, for all $g \in G$. This allow us to reformulate (9.3) as

$$ [\boldsymbol{G} : \boldsymbol{u}_{\boldsymbol{G}}] = \sum_{g \in \Delta} [\boldsymbol{G} : \boldsymbol{G}_g] \tag{9.5} $$

and (9.4) can be stated in the form

$$|G| = |Z(\boldsymbol{G})| + \sum_{g \in \Delta \setminus Z(\boldsymbol{G})} [\boldsymbol{G} : \boldsymbol{G}_g]. \tag{9.6}$$

Equation (9.5) is often referred to as *the class formula*. We show some non-trivial applications of (9.6) which, indeed, is a version of the class formula.

Let $\boldsymbol{G}$ be a group and $g \in G$. Then $o(g)$ is the order of the cyclic group generated by g, hence $o(g) \mid |G|$ due to the Lagrange's theorem. According to Lemma 8.3 if a group $\boldsymbol{G}$ is cyclic that for every $m \mid |G|$ there is a unique subgroup of $\boldsymbol{G}$ of order m. The subgroup is necessarily cyclic, due to Lemma 8.2, and so generated by an element of order m. In general, finite groups may not have subgroups of order m for every divisor m of their order. For example, the alternating group of permutations $\boldsymbol{A_5}$ has order $5!/2 = 60$ but it has no a subgroup of order 30. Otherwise the subgroup would be normal due to Exercise 4.3 which would contradict the simplicity $\boldsymbol{A_5}$ justified by Theorem 7.7. Nevertheless we prove that a finite group $\boldsymbol{G}$ has an element (and consequently a subgroup) of order p for every prime divisor p of $|G|$.

Theorem 9.11 (Cauchy)**.** *Let $\boldsymbol{G}$ be a finite group and p a prime dividing its order. Then there is $g \in G$ with $o(g) = p$.*

Proof. We prove the theorem by induction on the order of $\boldsymbol{G}$. If $|G| = p$, then $\boldsymbol{G}$ is necessarily cyclic and each of its non-unit elements has order p.

Suppose first that the group $\boldsymbol{G}$ is Abelian (i.e, comutative[3]) If $\boldsymbol{G}$ is cyclic, it has an element of order p due to Lemma 8.3. Otherwise $\boldsymbol{G}$ has a proper non-trivial subgroup, say $\boldsymbol{H}$. Since $|G| = |G/H| \cdot |H|$ due to Lagrange's theorem, either $p \mid |H|$ or $p \mid |G/H|$. In the first case we are done by the induction hypothesis, since $|H| < |G|$. If the latter holds true, the factor group $\boldsymbol{G/H}$ contains an element of order p again by the induction hypothesis. Therefore there is an element $g \in G \setminus H$ such that $g^p \in H$. Put $q = o(g^p)$ and observe that $o(g^q) = p$.

Now let $\boldsymbol{G}$ be an arbitrary finite group. If there is a proper subgroup $\boldsymbol{H}$ of $\boldsymbol{G}$ such that $p \mid |H|$, then $\boldsymbol{H}$ contains an element of order p by the induction hypothesis. Otherwise $p \nmid |G_g|$, hence $p \mid [\boldsymbol{G} : \boldsymbol{G}_g]$, for all $g \in \Delta \setminus Z(\boldsymbol{G})$. Formula (9.6) gives that

$$|Z(\boldsymbol{G})| = |G| - \sum_{g \in \Delta \setminus Z(\boldsymbol{G})} [\boldsymbol{G} : \boldsymbol{G}_g].$$

Since the right hand side is divisible by p, we conclude that $p \mid |Z(\boldsymbol{G})|$. Since the group $Z(\boldsymbol{G})$ is commutative, we are done by the previous paragraph. □

There is another tricky proof of Theorem 9.11.

[3] Commutative groups are usually called *Abelian groups* in tribute to Norwegian mathematician Niels Henrik Abel (1802 - 1829).

Proof. [Another proof of Theorem 9.11] Let X denote the set

$$X := \{\langle g_0, g_1, \dots, g_{p-1}\rangle \in G^p \mid g_0 \cdot g_1 \cdots g_{p-1} = u_{\boldsymbol{G}}\}.$$

Observe that a tuple $\langle g_0, g_1, \dots, g_{p-1}\rangle$ belongs to X if and only if

$$g_{p-1} = (g_0 \cdot g_1 \cdots g_{p-2})^{-1} = g_{p-2}^{-1} \cdot g_{p-3}^{-1} \cdots g_0^{-1}.$$

Therefore g_{p-1} is determined by the previous entrances $g_0, g_1, \dots, g_{p-2}$, and these can be arbitrary. We infer that $|X| = |G|^{p-1}$.

Observe that the set X is closed under cyclic permutations. Indeed, if $\langle g_0, g_1, \dots, g_{p-1}\rangle \in X$, equivalently $g_0 \cdot g_1 \cdots g_{p-1} = u_{\boldsymbol{G}}$, then $g_1 \cdots g_{p-1} \cdot g_0 = g_0^{-1} \cdot (g_0 \cdot g_1 \cdots g_{p-1}) \cdot g_0 = u_{\boldsymbol{G}}$, equivalently, $\langle g_1, \cdots, g_{p-1}, g_0\rangle \in X$.

Let the cyclic group $\mathbb{Z}_p$ act on the set X by cyclic permutations, that is

$$i \cdot \langle g_0, g_1, \dots, g_{p-1}\rangle = \langle g_i, g_{1+_p i}, \dots, g_{p-1+_p i}\rangle,$$

for all $i \in \mathbb{Z}_p$ and $\langle g_0, g_1, \dots, g_{p-1}\rangle \in X$. The set X is a disjoint union of $\boldsymbol{G}$-orbits. Therefore, picking a set Δ of representatives of the orbits, we have the equality

$$p^{p-1} = |X| = \sum_{\boldsymbol{g} \in \Delta} |\mathcal{O}_{\mathbb{Z}_p}(\boldsymbol{g})|. \tag{9.7}$$

Since the size of an orbit of a tuple $\boldsymbol{g} = \langle g_0, g_1, \dots, g_{p-1}\rangle$ is the index of its stabilizer, it divides $|\mathbb{Z}_p| = p$. Therefore every orbit has either p elements or a single element. Let Y denote the set of p-tuples from X whose orbits are singleton. It follows from (9.7) that $p \mid |Y|$.

Observe that $\langle g_0, g_1, \dots, g_{p-1}\rangle \in Y$ if and only if $g_0 = g_1 = \cdots = g_{p-1}$ and $g_0^p = u_{\boldsymbol{G}}$. In particular, the tuple $\langle u_{\boldsymbol{G}}, u_{\boldsymbol{G}}, \dots, u_{\boldsymbol{G}}\rangle$ belongs to Y. Therefore the set Y has at least p-elements. It follows that there is a non-unit element $g \in G$ with $g^p = u_{\boldsymbol{G}}$. We conclude that $o(g) = p$. □

Exercises

Exercise 9.1. *Let p be a prime number and $\boldsymbol{G}$ a group of size p^n for some positive integer n. Prove that a $\boldsymbol{G}$-set X with $p \nmid |X|$ contains an element x such that $g \cdot x = x$ for all $g \in G$.*

Exercise 9.2. *Let p be a prime and $\boldsymbol{G}$ a sub-group of the group of all automorphisms of a finitely generated vector space $\boldsymbol{V}$ over the field $\mathbb{Z}_p$. Prove that if $|\boldsymbol{G}| = p^n$, for some $n \in \mathbb{N}$, then*

(i) *There is a non-zero vector $\boldsymbol{v} \in V$ such that $f(\boldsymbol{v}) = \boldsymbol{v}$, for all $f \in G$.*
(ii) *There is a basis of $\boldsymbol{V}$ such that all endomorphisms from $\boldsymbol{G}$ are represented with respect to the bases by upper triangular matrices.*

Exercise 9.3. *Count the number of all colorings of a regular tetrahedron by n colors up to rotations.*

Exercise 9.4. *Suppose we color tiles of a chessboard by n colors. How many distinct boards we can obtain?*

Exercise 9.5. *Suppose that we are making necklaces each from k beads. How many distinct necklaces we can make when we use beads of n colors? How many distinct necklaces can be made from 5 blue and 5 red beads?*

Exercise 9.6. *Prove Lemma 9.4 and Corollary 9.5 directly without applying Lagrange's theorem.*

Exercise 9.7. *Let $\boldsymbol{G}$ be a group. Prove that $\operatorname{Inn}(\boldsymbol{G}) \trianglelefteq \operatorname{Aut}(\boldsymbol{G})$ and that $\operatorname{Inn}(\boldsymbol{G}) \simeq \boldsymbol{G}/Z(\boldsymbol{G})$.*