12 Delovanje grupe na množici.

Definicija (delovanje grupe na množici)
Naj bo X poljubna množica in naj bo G neka grupa. Delovanje grupe G na množici X (z leve strani) je preslikava $G \times X \to X$ za katero velja:

(i) $ex = x$ za vsak $x \in X$,

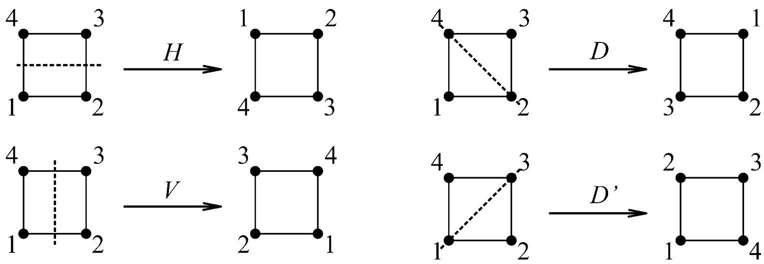
(ii) $(g_1 g_2)x = g_1(g_2 x)$ za vsak $x \in X$ in za vsaka $g_1, g_2 \in G$.

Pod temi pogoji množico X imenujemo G-množica. Upoštevajmo, da ne zahtevamo od množice X da bo v kakršni koli povezavi z grupom G.

1. Naj bo $G = GL_2(\mathbb{R})$ in naj bo $X = \mathbb{R}^2$. Pokaži da grupa G deluje na množici X v skladu z levim množenjem.

2. Naj bo $G = S_5$ in naj bo $X = \{\{i,j\} : i \neq j,\ i,j \in \{1,2,3,4,5\}\}$. Pokaži, da grupa G deluje na množici X v skladu z naslednjim predpisom: $G \times X \to X$, $\sigma\{i,j\} = \{\sigma i, \sigma j\}$.

3. Dan je kvadrat katerega oglјišča so označena s števi 1, 2, 3 in 4. Naj bo $D_4 = \{R_0, R_{90}, R_{180}, R_{270}, H, V, D, D'\}$ diederska grupa reda 8, kje je R_α rotacija za kot α, medtem ko so H, V, D in D' zrcaljenja opisana s slikami desno. Obrazloži, na kakšen način elementi R_{90}, H in D' grupe D_4 delujejo na oglјiščih 1 in 3. Če je $X = \{1,2,3,4\}$ napiši grupo D_4 v obliki grupe permutacij množice X. Pokaži, da grupa D_4 deluje na množici X.



4. Dana je grupa G in naj bo $X = G$. Definirajmo preslikavo $G \times X \to X$ na naslednji način: $g * x = x^g = gxg^{-1}$ (tako definirana preslikava se imenuje konjugacija). Pokaži, da je konjugacija delovanje grupe.

5. Predpostavimo da grupa G deluje na množici X. (a) Pokaži, da če je $x \in X$, $g \in G$ in $y = gx$, potem je $x = g^{-1}y$. (b) Pokaži, da če je $x \neq x'$ potem $gx \neq gx'$.

Izrek. Naj bo X G-množica. Za vsak $g \in G$, je funkcija $\sigma_g : X \to X$ definirana z $\sigma_g(x) = gx$ za $x \in X$, permutacija množice X. Tudi, preslikava $\phi : G \to S_X$ definirana z $\phi(g) = \sigma_g$ je homomorfizem z lastnostjo, da je $\phi(g)(x) = gx$.

Definicija (orbita elementa x pri delovanju grupe G)
Naj grupa G deluje na množici X in naj bo $x \in X$. Množici

$$Gx = \{gx \mid g \in G\}$$

pravimo orbita elementa x pri delovanju grupe G na množici X.

6. (a) Dana je grupa $G = \{(1), (123), (132), (45), (123)(45), (132)(45)\} \leq S_5$ in dana je množica $X = \{1,2,3,4,5\}$ (X je G-množica). Določi orbite množice X glede na grupo G.

(b) Poišči orbite delovanja podgrupe $H = \langle (13), (247) \rangle \leq S_8$ na množici $X = \{1,2,3,4,5,6,7,8\}$.

7. Naj bo $G \subseteq \mathrm{Mat}_{2\times 2}(\mathbb{R})$ grupa vseh obrnljivih matrik in naj bo $X = \mathbb{R}^2$ (G deluje na množici X). Določi orbite množice X glede na grupo G.

8. Naj bo G dana grupa in naj bo $X = G$. Grupa G deluje na množici X v skladu z levim množenjem. Določi orbite množice X glede na delovanje grupe G.

Definicija (stabilizator elementa x)

Naj grupa G deluje na množici X in naj bo $x \in X$. Množici

$$G_x = \{g \in G : gx = x\}$$

pravimo stabilizator elementa x v grupi G.

9. Naj bo X kvadrat in naj bo G grupa vseh simetrij kvadrata X ($G = \mathrm{Sym}(X)$). Opazimo, da G deluje na X. Določi orbito in stabilizator elementa $x \in X$ če je (a) x neko ogljišče kvadrata; (b) x sredina stranice kvadrata; (c) x točka na $\frac{1}{3}$ dolžine neke stranice kvadrata.

10. Naj bo G grupa realnih števil z opearcijo seštevanja. Naj bo delovanje elementa $\alpha \in G$ na množici $\mathbb{R}^2$ dano z rotacijo ravnine $\mathbb{R}^2$ okoli $(0,0)$ za α radianov v nasproti smeri urinega kazalca. Naj bo T poljubna točka v ravnini.

(a) Pokaži, da je $\mathbb{R}^2$ G-množica.

(b) Geometrijsko opiši orbito, ki vsebuje točko T.

(c) Poišči stabilizator G_T.

11. Grupa $G := \mathrm{GL}_2(\mathbb{R})$ deluje na množici $\mathbb{R}^2$ v skladu z levim množenjem $A \cdot v := Av$.

(a) Izračunaj $G_{[0,0]^\top}$.

(b) Izračunaj $G_{[1,0]^\top}$.

(c) Določi vse orbite.

Izrek. Naj bo X G-množica in naj bosta $x \in X$, $g \in G$ poljubna elementa. Potem je $G_{gx} = gG_xg^{-1}$. Še več, če je H neka neprazna množica, potem je $G_{gH} = gG_Hg^{-1}$.

12. Dokaži izrek zgoraj.

13. Naj bo $X = \{1,2,3,4,5,6,7,8,9\}$, $\sigma = (123)(456)(789)$, $\tau = (12)(34)(56)(78)$, $G = \langle \sigma, \tau \rangle$. Poglejmo si delovanje grupe G na množici X. Opazimo, da je $\tau \in G_9$ in da je $\tau \in G_{\{3,4\}}$. Kaj lahko brez neposrednoga računanja rečemo o $\sigma\tau\sigma^{-1}$.

14. Dan je pravilni petkotnik čigaar oglišča so označena s števili 1, 2, 3, 4 in 5. Če sta $\rho = (13524)$ in $\mu = (25)(34)$, brez neposrednog računanja določi $\rho\mu\rho^{-1}$.

Izrek. Naj bo X G-množica in naj bosta $x \in X$, $g \in G$ poljubna elementa. Če je $gx = y$ in $T = \{t \in G \,|\, tx = y\}$, potem je $T = gG_x$.

Izrek (orbita-stabilizator izrek)

Naj bo X G-množica in naj bo $x \in X$. Potem je $|Gx| = [G : G_x]$. Če je G končna, potem je $|Gx|$ deljitelj od $|G|$. Poleg tega

$$|G| = |Gx| \cdot |G_x|.$$

15. Dokaži izreki zgoraj.

16. (a) Naj bo X kocka in naj bo $G = \mathrm{RotSym}(X)$ grupa vseh rotacijskih simetrija kocke X. Določi red grupe G. (b) Naj bo X dodekaeder in naj bo $G = \mathrm{RotSym}(X)$ grupa vseh rotacijskih simetrija dodekaedra X. Določi red grupe G.

17. Naj bo $X = \{1,2,3,4,5,6,7,8,9\}$, $\sigma = (123)(456)(789)$, $\tau = (12)(34)(56)(78)$, $G = \langle \sigma, \tau \rangle$. Oglejmo si delovanje grupe G na množici X. (a) Kaj je orbita delovanja grupe G na elementu 2? na elementu 6? na elementu 8? (b) Izrazi $|G_1|$ preko $|G|$. (c) naj bo $Y = \{\{a,b\} \,|\, a,b \in X\}$. Ali G deluje na Y? Zakaj? Kako? Kaj lahko rečemo o orbitah? (d) Opazimo, da je $\tau \in G_9$ in da je $\tau \in G_{\{3,4\}}$. Kaj lahko brez neposrednog računanja rečemo o $\sigma\tau\sigma^{-1}$.

18. Predpostavimo, da grupa G deluje na množici X. (a) Pokaži, da so različne orbite disjunktne. (b) Za poljuben element $x \in X$ pokaži, da je stabilizator G_x elementa x podgrupa grupe G.

19. (a) Naj bo G grupa reda 15, katera deluje na množici X reda 22. Predpostavimo, da množica X nima fiksnih točk. Določi število orbit. (b) Naj bo G grupa reda 75, katera deluje na množici X reda 11. Predpostavimo da množica X nima fiksnih točk. Določi število orbit.

Pierre de Fermat

> This theorem [Fermat's Little Theorem] is one of the great tools of modern number theory.
>
> *William Dunham*

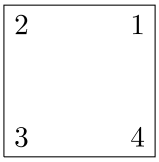
Pierre de Fermat (pronounced Fair-mah) was born in Beaumont-de-Lomagne, France in August of 1601 and died in 1665. Fermat obtained a Bachelor's degree in civil law from the University of Orleans in 1631. While earning his living practicing law he did mathematics as a hobby. Rather than proving and publishing theorems he sent the statements of his results and questions to leading mathematicians. One of his important observations is that any prime of the form $4k+1$ can be written as the sum of two squares in one and only one way, whereas a prime of the form $4k-1$ cannot be written as the sum of two squares in any manner whatever. Mathematics historian William Dunham asserts that Fermat's discovery of this dichotomy among primes ranks as one of the landmarks of number theory. Addressing Fermat's contributions to number theory Andrá Weil wrote that "...what we possess of his methods for dealing with curves of genus 1 is remarkably coherent; it is still the foundation for the modern theory of such curves." A Wikipedia article on Fermat concluded with the statement "Fermat essentially created the modern theory of numbers."

Beyond his contributions to number theory, Fermat found a law of optics and is considered as one of the founders of analytic geometry and probability theory. In 1989 the Institut de Mathétiques de Toulousem in France established the Fermat prize for research in fields in which Fermat made majors contributions. Among the recipients are Andrew Wiles and Richard Taylor.

On the Google Drive, please find solutions for the following problems:

1. Let G be a group. Suppose that G acts on a set X. (a) Define a relation on X as $x \sim y \Leftrightarrow \exists g \in G,\ g \cdot x = y$. Show that this is an equivalent relation. (b) Show that the equivalent class $\overline{y}$ is precisely Gy. **2.** The conjugation action tells us some interesting results on the structure of finite groups. Suppose that $|G| = p^n$ for some prime number p. Show that $|Z(G)| > 1$. **3.** Let $\alpha \in S_n$. Write α as a product of disjoint cycles $\alpha_1\alpha_2...\alpha_r$ where $\ell(\alpha_1) = \ell(\alpha_2) = ... = \ell(\alpha_r)$. We say that α is of type $b_1 + b_2 + ... + b_r$ if $\ell(\alpha_1) = b_1$, $\ell(\alpha_2) = b_2$, $...\ell(\alpha_r) = b_r$ where $\ell(\alpha_i)$ is the length of the cycle α_i. For instance, $\alpha = (152)(638)(47)$ is of type $3+3+2$. Consider the conjugation action on S_n. (a) Show that if $\alpha, \beta \in S_n$ are in the same conjugacy class, then α and β are of the same type. (b) Show the converse, i.e., show that if $\alpha, \beta \in S_n$ are of the same type then they are in the same conjugacy class. (c) By using (a) and (b), count the number of orbits in S5 and find the size of each orbit. **4.** Determine the number of ways in which the four corners of a square can be colored with two colors. Two colorings are equivalent if one can be obtained from another by applying symmetry group permutation (D_4). (It is permissible to use a single color on all four corners.) **5.** Determine the number of ways in which the faces of a cube can be colored with three colors. **6.** Four dwarves and four elves are going to discuss how to protect Middle earth from the attack of Sauron. On a round table with eight seats, how many distinguishable ways can they be seated? **7.** Determine the number of different necklaces that can be made using 13 white beads and 3 black beads. **8.** Determine the number of ways in which the vertices of an equilateral triangle can be colored with five colors so that at least two colors are used. **9.** Determine the number of ways in which the edges of a square can be colored with six colors so that no color is used on more than one edge. **10.** Determine the number of ways in which the faces of a cube can be colored with three colors. **11.** How many ways can the five points of a five-pointed crown be painted if three colors of paint are available?

Computer Tutorial 12.[31][32]

<table>
<caption>symmetries of a square</caption>
<tr><th>Input</th><th>Meaning</th></tr>
<tr><td>Think of the vertices of the square as occupying the positions labelled 1, 2, 3 and 4 in following diagram.

</td><td>The symmetries of the square will be represented by permutations of the set $\{1, 2, 3, 4\}$. The reflection s in the vertical line bisecting the square corresponds to the permutation $(1, 2)(3, 4)$; the reflection t in the diagonal from 2 to 4 corresponds to $(1, 3)$. (Note that the numbers label positions on the paper, and do not move. Think of $(1, 3)$ as saying "move the contents of Location 1 to Location 3, and the contents of Location 3 to Location 1".)</td></tr>
<tr><td>S := Sym(4);
print #S;</td><td>The collection of all permutations of $\{1, 2, 3, 4\}$ is a group, called the symmetric group Sym(4). Let us call it S for short: S:=Sym(4);. The number of elements in a group is called the order of the group. Find order of S.</td></tr>
<tr><td>s := S!(1,2)(3,4);
t := S!(1,3);
s*s, s*t, t*s, t*t;</td><td>Our first aim is to find out how many symmetries can be constructed just from s and t alone. We can do this by computing things like st, ts, s^2, t^2, $(st)s$, and so on, until we find that we do not get anything new by multiplying together any of the permutations we have already obtained.
Because $s^2 = id$ and $t^2 = id$, we need only consider products in which s and t alternate: consecutive s's or t's cancel out.
<u>Remark.</u> <u>Note that in product st MAGMA first compute s, and after that t.</u> How is this different from our initial settings?</td></tr>
<tr><td>s*t*s, t*s*t, s*t*s*t, t*s*t*s;</td><td>Because $stst = tsts$, any alternating product of length greater than 4 equals a product with two consecutive s's or t's, and hence equals something shorter. For example, $ststs = (stst)s = (tsts)s = (tst)s^2 = tst$. So in fact the only permutations you can get from s and t are id, s, t, st, ts, sts, tst and $stst$.</td></tr>
<tr><td>X := {s,t};

print forall{ <x,y> : x in X, y in X | x*y in X };</td><td>We are trying to find the smallest set that contains s and t and is closed under multiplication. Start by defining X to be the set containing just s and t.
Print true if it is true for all ordered pairs <x,y> with x, y in X that xy is in X, otherwise it will print false.</td></tr>
<tr><td>X := {s,t};
forall { <x,y> : x in X, y in X | x*y in X };
X1 := {s,t,s*t,t*s};
forall { <x,y> : x in X, y in X1 | x*y in X };
X2 := {id(S),s,t,s*t,t*s};
forall { <x,y> : x in X, y in X2 | x*y in X };
X3 := {id(S),s,t,s*t,t*s,s*t*s, t*s*t,s*t*s*t};
forall {<x,y> : x in X, y in X3 | x*y in X };</td><td>Experiment with various sets, such as $X_1 := \{s, t, st, ts\}$ and see if you can find one that contains s and t and is closed. For example, if X_1 is not closed, try adding an extra element, such as sts, and then testing it again. If it is still not closed, add another, and so on.</td></tr>
<tr><td>Y := { x*y : x,y in X };
print Y;
print Y subset X;</td><td>Another way to test whether a set such as X is closed is to form the set of all products of pairs of elements of X and test whether it is a subset of X.</td></tr>
</table>

[31] To write MAGMA code please open: http://magma.maths.usyd.edu.au/calc/
[32] See also: http://www.maths.usyd.edu.au/u/bobh/UoS/MATH2008/ctut12.pdf