14 Grupa automorfizmov.

Definicija (center grupe) Center, $Z(G)$, grupe G je podmnožica elementov grupe G, ki komutirajo s vsakim elementom grupe G. S simboli zapisano:

$$Z(G) = \{a \in G \mid ax = xa \text{ za vse } x \in G\}.$$

Izrek (center je podgrupa)
Center grupe G je podgrupa grupe G.

1. (a) Pokaži da je $Z(G) = G$ če in samo če je G abelska. (b) Pokaži da je $Z(S_n) = \{id\}$ če je $n \geq 3$.

2. Spomnimo se, da se diederska grupa D_n (reda $2n$) lahko generira z rotacijo $R_{360/n}$ (reda n) in refleksijo F (reda 2) za katere velja, da je $FR_{360/n}F = R_{360/n}^{-1}$. Poišči $Z(D_n)$ za poljuben $n \geq 3$.

3. Naj bo G grupa, in naj bo a poljubni element iz grupe G. Definirajmo preslikavo $\varphi_a : G \to G$ na naslednji način $\varphi_a(x) = axa^{-1}$. Dokaži da $\varphi_h = \varphi_g$ če in samo če $g^{-1}h \in Z(G)$.

4. Naj bo G grupa. Pokaži da je potem $Z(G) \lhd G$.

	I	A	B	AB	BA	ABA
I	I	A	B	AB	BA	ABA
A	A	I	AB	B	ABA	BA
B	B	BA	I	ABA	A	AB
AB	AB	ABA	A	BA	I	B
BA	BA	B	ABA	I	AB	A
ABA	ABA	AB	BA	A	B	I

5. Množica $G = \{I, A, B, AB, BA, ABA\}$ tvori grupo glede na operacijo množenja, in njena Cayley-eva tabela je dana zgoraj. Izručunaj $Z(G)$.

Izrek (G/Z izrek) Naj bo G grupa in naj bo $Z(G)$ center grupe G. Če je $G/Z(G)$ ciklična grupa, potem je G abelska.

Spomnimo se, da je $\mathbb{Z}_p$ edina grupa (do izomorfizma) praštevilskoga reda p.

6. Naj bo p praštevilo in naj bo G taka grupa, da $|G| = p^3$. Če je $Z(G) \neq \{e\}$ in $Z(G) \neq G$, pokaži da je potem $Z(G) \cong \mathbb{Z}_p$.

7. Naj bo G taka grupa, da je $[G : Z(G)] \leq 3$. Pokaži, da je potem G abelska.

8. Naj bo G končna grupa in naj bosta p, q dve praštevili, ne nujno različni. Če je $|G| = pq$, pokaži, da je potem G bodisi abelska, ali pa je $Z(G) = 1$.

9. Naj bo π permutacija. Pokaži da je potem $\pi(a_1a_2...a_k)\pi^{-1} = (\pi(a_1)\pi(a_2)...\pi(a_k))$.

Spomnimo se: Preslikava ϕ iz grupe G sama vase se imenuje automorfizem grupe G če in samo če (i) $\phi(ab) = \phi(a)\phi(b)$ za $\forall a, b \in G$; (ii) ϕ je injekcija; (iii) ϕ je surjekcija.

10. (a) Naj bo G nek grupa, kjer je $a^2 \neq e$ za nek $a \in G$. Pokaži, da ima grupa G netrivialne automorfizme.

(b) Naj bo f automorfizem grupe G. Če je H podgrupa grupe G, pokaži, da je potem $f(H)$ tudi podgrupa grupe G.

Izrek Naj bo f automorfizem grupe G. Če je N edinka grupe G, potem je $f(N)$ tudi edinka grupe G.

11. (a) Naj bo G grupa in naj bo Z center grupe G. Če je f automorfizem grupe G, pokaži da je potem $f(Z) \subseteq Z$.

(b) Naj bo G grupa in naj bo f automorfizem grupe G. Če za $a \in G$ definiramo $N(a) = \{x \in G : ax = xa\}$, pokaži da potem velja $N(f(a)) = f(N(a))$.

12. Naj bo G grupa in naj bo a poljubni ampak fiksen element grupe G. Naj bo f_a preslikava iz G v G definirana z $f_a(x) = a^{-1}xa$, $x \in G$. Pokaži, da je preslikava f_a dobro definirana in da je automorfizem grupe G.

Definicija (notranji in zunanji automorfizem)
Naj bo $a \in G$. Automorfizem $f_a(x) = a^{-1}xa$, $x \in G$, se imenuje notranji automorfizem grupe G, ki ustreza elementu a. Automorfizem, ki ni notranji automorfizem, se imenuje zunanji automorfizem.

13. Naj bo G aditivna grupa celih števil. Poišči notranji automorfizem grupe G, ki ustreza elementu 5 grupe G.

14. Poišči zgled grupe G v kateri obstajata elementa $a, b \in G$, $a \neq b$, tako da velja $f_a = f_b$ (f_a in f_b sta dva notranja automorfizma grupe G, tako da $f_a = f_b$).

15. Naj bo $f : G \to G$ homomorfizem in naj f komutira z vsakim notranjim automorfizmom grupe G. Pokaži da je $H = \{x \in G : f^2(x) = f(x)\}$ edinka grupe G.

Izrek Za abelske grupe je edini notranji automorfizem identična preslikava, medtem ko za neabelske grupe obstaja netrivialen notranji automorfizem.

Definicija (grupa automorfizmov) Grupo Aut(G), vseh automorfizmov grupe G, glede na operacijo kompozicije funkcij, imenujemo grupa automorfizmov grupe G.

16. (a) Naj bo G ciklična grupa reda 4. Pokaži, da je grupa automorfizmov grupe G, reda 2.

(b) Če je $|\mathrm{Aut}(G)| > 1$, pokaži da je potem $|G| > 2$.

17. (a) Naj bo G neskončna ciklična grupa. Pokaži, da je $|\mathrm{Aut}(G)| = 2$.

(b) Naj bo G končna ciklična grupa reda n. Pokaži, da je potem $|\mathrm{Aut}(G)| = \phi(n)$, kjer je ϕ Eulerjeva funkcija fi.

18. (a) Naj bo G grupa in naj bo Aut(G) množica vseh automorfizmov grupe G. Pokaži, da je množica Aut(G) grupa glede na operacijo kompozicije funkcij.

(b) Naj bo G grupa in naj bo Inn(G) množica notranjih automorfizmov grupe G. Pokaži, da je množica Inn(G) grupa glede na operacijo kompozicije.

Definicija (Inn(G)) Grupo Inn(G) vseh notranjih automorfizmov grupe G, glede na operacijo kompozicije, imenujemo grupa notranjih automorfizmov grupe G.

Izrek Množica Inn(G) vseh notranji automorfizmov grupe G je edinka grupe Aut(G) vseh automorfizmov grupe G.

Izrek (Inn$(G) \cong G/Z(G)$) Za vsako grupo G, je $G/Z(G)$ izomorfna z Inn(G).

19. (a) Določi Inn(D_4) (po potrebi uporabi Cayley-evo tabelo, ki smo jo imeli v eni od prejšnjih nalog).

(b) Pokaži, da je $\mathrm{Aut}(\mathbb{Z}_n) \cong U(n)$.

(c) Naj bo $G = S_3$. Pokaži, da je $\mathrm{Inn}(G) \cong G$.

POMEMBNI REZULTATI (Grupa automorfizmov.)

1. **(G/Z izrek)** Naj bo G grupa in naj bo $Z(G)$ center grupe G. Če je $G/Z(G)$ ciklična grupa, potem je G abelska.
2. Naj bo f automorfizem grupe G. Če je H podgrupa grupe G, potem je $f(H)$ tudi podgrupa grupe G.
3. Naj bo f automorfizem grupe G. Če je N edinka grupe G, potem je $f(N)$ tudi edinka grupe G.
4. Za abelske grupe je edini notranji automorfizem identična preslikava, medtem ko za neabelske grupe obstaja netrivialen notranji automorfizem.
5. Množica Inn(G) vseh notranjih automorfizmov grupe G je edinka grupe Aut(G) (vseh automorfizmov grupe G).
6. Za vsako grupo G je $G/Z(G)$ izomorfna z Inn(G) (kjer je $Z(G)$ center grupe G).

Emmy Noether

> ...she discovered methods which have proved of enormous importance in the development of the present-day younger generation of mathematicians.
> *Albert Einstein, The New York Time*

Emmy Noether was born on March 23, 1882, in Germany. When she entered the University of Erlangen, she was one of only two women among the 1000 students. Noether completed her doctorate in 1907.

In 1916, Noether went to Göttingen and, under the influence of David Hilbert and Felix Klein, became interested in general relativity. While there, she made a major contribution to physics with her theorem that whenever there is a symmetry in nature, there is also a conservation law, and vice versa. In a 2012 issue of the New York Times science writer Ranson Stephens said "You can make a strong case that her theorem is the backbone on which all of modern physics is built." Hilbert tried unsuccessfully to obtain a faculty appointment at Göttingen for Noether, saying, "I do not see that the sex of the candidate is an argument against her admission as Privatdozent. After all, we are a university and not a bathing establishment."

It was not until she was 38 that Noether's true genius revealed itself. Over the next 13 years, she used an axiomatic method to develop a general theory of ideals and noncommutative algebras. With this abstract theory, Noether was able to weld together many important concepts. Her approach was even more important than the individual results. Hermann Weyl said of Noether, "She originated above all a new and epochmaking style of thinking in algebra."

With the rise of Hitler in 1933, Noether, a Jew, fled to the United States and took a position at Bryn Mawr College. She died suddenly on April 14, 1935, following an operation.

Sophie Germain

> One of the very few women to overcome the prejudice and discrimination that tended to exclude women from the pursuit of higher mathematics in her time was Sophie Germain.

Sophie Germain was born in Paris on April 1, 1776. She educated herself by reading the works of Newton and Euler in Latin and the lecture notes of Lagrange. In 1804, Germain wrote to Gauss about her work in number theory but used the pseudonym Monsieur LeBlanc because she feared that Gauss would not take seriously the efforts of a woman. Gauss gave Germain's results high praise and a few years later, upon learning her true identity, wrote to her:

> But how to describe to you my admiration and astonishment at seeing my esteemed correspondent Mr. LeBlanc metamorphose himself into this illustrious personage who gives such a brilliant example of what I would find it difficult to believe. A taste for the abstract sciences in general and above all the mysteries of numbers is excessively rare: it is not a subject which strikes everyone; the enchanting charms of this sublime science reveal themselves only to those who have the courage to go deeply into it. But when a person of the sex which, according to our customs and prejudices, must encounter infinitely more difficulties than men to familiarize herself with these thorny researches, succeeds nevertheless in surmounting these obstacles and penetrating the most obscure parts of them, then without doubt she must have the noblest courage, quite extraordinary talents, and a superior genius.[35]

Germain is best known for her work on Fermat's Last Theorem. She died on June 27, 1831, in Paris.

[35] Quote from Math's Hidden Woman, Nova Online, `http://www.pbs.org/wgbh/nova/proof/germain.html`

Computer Tutorial 14.[36][37]

smallest group of permutations

Input	Meaning

`F:=PermutationGroup<5|`
`(1,2,3,4,5),(1,2)>;`
	Creates the smallest group of permutations of the set $\{1, 2, 3, 4, 5\}$ that contains $(1, 2, 3, 4, 5)$ and $(1, 2)$.

`#F, #Sym(5);`
`F eq Sym(5);`
	How many permutations are there in F? And how many permutations of $\{1, 2, 3, 4, 5\}$ exist that are not in F?

Suppose that the vertices of a regular pentagon are numbered 1, 2, 3, 4, 5. Draw a diagram, and use it to find a permutation a that corresponds to a rotation symmetry of the pentagon, and a permutation b that corresponds to a reflection symmetry.	If the vertices of the regular pentagon are labelled 1, 2, 3, 4, 5 (cyclically) then $a = (1, 2, 3, 4, 5)$ is a rotation symmetry and $b = (2, 5)(3, 4)$ a reflection symmetry. (Other choices are possible: for example, $(1, 3, 5, 2, 4)$ is a rotation and $(1, 4)(2, 3)$ a reflection.) The permutation group generated by a and b has order 10. Its elements correspond to the five rotation symmetries and five reflection symmetries of the pentagon.

`D:=PermutationGroup`
`<5|(1,2,3,4,5),(1,4)(2,3)>;`
	Define D to be the smallest group of permutations containing your permutations a and b. Check that D has order 10. (It is called the dihedral group of order 10.)

`A:=Alt(5);`	The alternating group of degree n consists of all even permutations of the numbers $1, 2, ..., n$. The MAGMA command `A:=Alt(5)` creates the alternating group of degree 5.

`#A,#D;`
`D subset A;`
	From the command `print D subset A;` you will find out whether all the elements of D are even.

`D1:=Set(D);`
`Others:=Set(A) diff D1;`
`c:=Random(Others); c;`
`D2:={x*c : x in D};`
`Others:=Others diff D2;`
`d:=Random(Others); d;`
`D3:={x*d : x in D};`
`Others:=Others diff D3;`
`e:=Random(Others); e;`
	Find all the cosets of D in A. Label them $D1$, $D2$, ... How many do you expect? (Make sure that your list $D1$, $D2$, ... does not contain any repetitions.)
	For each pair of distinct cosets, find out how many elements they have in common. (If X and Y are sets, their intersection is given by `X meet Y`.)

`D4:={x*e : x in D};`
`Others:=Others diff D4;`
`f:=Random(Others); f;`
`D5:={x*f : x in D};`
`Others:=Others`diff D5;
`g:=Random(Others); g;`
`D6:={x*g : x in D};`
`D6 eq Others;`
`#D1,#D2,#D3,#D4,#D5,#D6;`
`Set(A) eq (D1 join D2 join D3 join`
`D4 join D5 join D6);`
	The 10 elements of D all lie in the group $A = \mathrm{Alt}(5)$, which has order 60. So D is a subgroup of A, and the index of D in A is $60/10 = 6$. That is, there are 6 cosets of D in A.
	According to MAGMA, the six sets $D_1 ... D_6$ each have 10 elements, and their union is the whole `Set(A)`, which has 60 elements. So they must be disjoint from each other. But rather than simply trusting MAGMA, the student should do at least some calculations by hand and check that the answers agree with MAGMA's.

`z:=Random(A); z;`
`E:={x*z:x in D}; E;`
`E in {D1,D2,D3,D4,D5,D6};`
`z:=Random(A); z;`
`E:={x*z:x in D}; E;`
`E in {D1,D2,D3,D4,D5,D6};`
...
`E:={x*y: x in D2, y in D3}; #E;`
	We create some new sets E_1, E_2 and then check that the sets E_1, E_2 etc. are just the cosets D_1, D_2, etc. in some order.
	If X, Y are subsets of a group G then we define $XY = \{xy \mid x \in X, y \in Y\}$. If $X = Hg_1$ and $Y = Hg_2$ are cosets of the subgroup H then it may or may not happen that $(Hg_1)(Hg_2)$ is also a subgroup of H. Note that since $g_1 \in Hg_1$ and $g_2 \in Hg_2$ it is always true that $g_1 g_2 \in (H_{g_1})(H_{g_2})$...

[36] To write MAGMA code please open: `http://magma.maths.usyd.edu.au/calc/`

[37] See also: `http://www.maths.usyd.edu.au/u/bobh/UoS/MATH2008/ctut08.pdf`