13 Izreki Sylowa

Izrek (Cauchijev izrek za abelske grupe)
Naj bo G končna abelska grupa in naj p deli $|G|$, kje je p praštevilo. Potem obstaja element $a \in G$ $(a \neq e)$ t.d. $a^p = e$.

Izrek (Cauchijev izrek)
Naj bo G končna grupa in naj p deli $|G|$, kje je p praštevilo. Potem obstaja element $a \in G$ $(a \neq e)$ t.d. $a^p = e$ (obstaja element reda p).

1. Pokaži, če je G grupa reda $2p$, kje je p praštevilo, potem ima G edinko reda p.

2. Naj bosta p in q praštevili. Pokaži, da je abelska grup reda pq ciklična.

3. (a) Pokaži, da je vsaka abelska grupa reda 6 ciklična.

(b) Poišči, vse ne-abelske grupe reda 6.

Izrek (Obrat Lagrange-ovog izreka za končene abelske grupe)
Naj bo G končna abelska grupa. Če m deli red grupe G, potem obstaja $H \leq G$ reda m.

4. Naj bo G končna grupa reda p^n, kje je p praštevilo. Pokaži, da ima G podgrupo reda 1, p, p^2, ..., p^n.

5. Pokaži, če je $|G| = p^2$, kjer je p praštevilo, potem je G abelska.

Izrek (prvi izrek Sylowa)
Naj bo G končna grupa reda $p^k q$, kjer je p praštevilo, $k, q \in \mathbb{N}$ in $\gcd(p, q) = 1$. Potem za vsak i $(1 \leq i \leq k)$ velja, da ima G najmanj edno podgrupo reda p^i.

6. Če praštevilo p deli red končne grupe G, potem G vsebuje najmanj en element reda p.

Pripomba. Posledica tega primera je Cauchy-ev izrek za končne grupe.

Definicija (p-podgrupa, p-grupa)
Naj bo p praštevilo. Podgrupa H grupe G se imenuje p-podgrupa, če je red vsakega elementa iz H enak potenci števila p. Podobno, če je red vsakega elementa iz grupe G enak potenci števila p, potem se G imenuje p-grupa.

Izrek Končna grupa G je p-grupa če in samo če je $|G|$ enak potenci števila p.

7. Dokaži izrek zgoraj.

8. Katera od naslednjih grup je p-grupa:

(i) grupa G reda 21?

(ii) grupa G reda 25?

(iii) grupa G reda 128?

Definicija (Sylowa p-podgrupa)
Naj bo G končna grupa in naj bo p praštevilo. Podgrupa grupe G reda p^k $(k \in \mathbb{N})$ se imenuje Sylowa p-podgrupa grupe G, če p^k deli $|G|$ in p^{k+1} ne deli $|G|$.

Pripomba. Po definiciji Sylowe p-podgrupe, so vse Sylove p-podgrupe končne grupe istega reda.

9. Če je P Sylowa p-podgrupa končne grupe G, potem je za vsak $x \in G$, $x^{-1}Px$ tudi Sylowa p-podgrupa grupe G.

Opomba. Če je P edina Sylowa p-podgrupa, potem je $x^{-1}Px = P$ $\forall x \in G$. Naj bosta $g \in G$, $h \in P$. Potem $ghg^{-1} = (g^{-1})^{-1}hg^{-1} = x^{-1}hx \in x^{-1}Px$ (vzemo $x = g^{-1}$), $ghg^{-1} \in P$ $\forall g \in G$, $h \in P$, P je edinka v grupi G.

10. Naj bo $|G| = p^k q$ kje je p praštevilo, $k, q \in \mathbb{N}$ in $\gcd(p, q) = 1$ in naj bo P Sylowa p-podgrupa grupe G. Če je H p-podgrupa grupe G t.d. $P \subseteq H \subseteq G$, potem pokaži, da je $H = P$.

Opomba. Iz primera zgoraj opazimo, da p-podgrupa grupe G ne more strogo vsebovati Sylowe p-podgrupe grupe G.

Definicija (konjugirane podgrupe)
Naj bo G grupa in naj bosta H, T podgrupe grupe G. Pravimo, da je podgrupa H konjugirana podgrupi T, če obstaja element $g \in G$ t. d. $H = g^{-1}Tg = \{g^{-1}tg : t \in T\}$.

Izrek (drugi izrek Sylowa)
Naj bo G končna grupa reda $p^k q$, kjer je p praštevilo, $k, q \in \mathbb{N}$ in $\gcd(p, q) = 1$. Potem sta vsaki dve podgrupi reda p^k konjugirani.

Izrek (tretji izrek Sylowa)
Naj bo G končna grupa reda $p^k q$, kjer je p praštevilo, $k, q \in \mathbb{N}$ in $\gcd(p, q) = 1$. Potem je število podgrup reda p^k oblike $1 + mp$, kjer je m neko ne-negativno celo število. Velja tudi, da $1 + mp$ deli $|G|$.

11. Določi mogoče število Sylowih p-podgrup grupe S_3, pa poišči vse Sylowe 2-podgrupe in vse Sylowe 3-podgrupe grupe S_3.

Definicija (enostavna grupa)
Grupa G je enostavna, če sta njeni edini edinki trivijalna grupa in grupa G.

12. Poišči mogoče število Sylowih 11-podgrup, Sylovih 7-podgrup in Sylowih 5-podgrup v grupi reda 1925.

13. (a) Pokaži, da grupa reda 28 ni enostavna.

(b) Pokaži, da grupa reda 40 ni enostavna.

14. Pokaži, da v grupi reda 20449 obstaja Sylowa 11-podgrupa, ter da grupa ni enostavna.

15. (a) Pokaži, da grupa reda 30 ni enostavna.

(b) Pokaži, da grupa reda 56 ni enostavna.

16. Če ima grupa G reda 28 edinko reda 4, potem pokaži, da je grupa G abelska.

17. Pokaži, da ne obstaja enostavna grupa reda 48.

18. (a) Do izomorfizma natančno določi vse grupe reda 99.

(b) Do izomorfizma natančno določi vse grupe reda 66.

19. Pokaži, da je edina grupa reda 255 grupa $\mathbb{Z}_{255}$.

POMEMBNI REZULTATI (Izreki Sylowa.)

1. **(Cauchijev izrek.)** Naj bo G končna grupa in naj p deli $|G|$, kje je p praštevilo. Potem obstaja element $a \in G$ $(a \neq e)$ t.d. $a^p = e$ (obstaja element reda p).
2. Naj bo G končna abelska grupa. Če m deli red grupe G, potem obstaja $H \leq G$ reda m.
3. **(prvi izrek Sylowa)** Naj bo G končna grupa reda $p^k q$, kjer je p praštevilo, $k, q \in \mathbb{N}$ in $\gcd(p, q) = 1$. Potem za vsak i $(1 \leq i \leq k)$ velja, da ima G najmanj edno podgrupo reda p^i.
4. **(drugi izrek Sylowa)** Naj bo G končna grupa reda $p^k q$, kjer je p praštevilo, $k, q \in \mathbb{N}$ in $\gcd(p, q) = 1$. Potem sta vsaki dve podgrupi reda p^k konjugirani.
5. **(tretji izrek Sylowa)** Naj bo G končna grupa reda $p^k q$, kjer je p praštevilo, $k, q \in \mathbb{N}$ in $\gcd(p, q) = 1$. Potem je število podgrup reda p^k oblike $1 + mp$, kjer je m neko ne-negativno celo število. Velja tudi, da $1 + mp$ deli $|G|$.

Ludwig Sylow

> Sylow's Theorem is 100 years old. In the course of a century this remarkable theorem has been the basis for the construction of numerous theories.
>
> *L. A. Shemetkov*

Ludwig Sylow (pronounced "SEE-loe") was born on December 12, 1832, in Christiania (now Oslo), Norway. While a student at Christiania University, Sylow won a gold medal for competitive problem solving. In 1855, he became a high school teacher; despite the long hours required by his teaching duties, Sylow found time to study the papers of Abel. During the school year 1862-1863, Sylow received a temporary appointment at Christiania University and gave lectures on Galois theory and permutation groups. Among his students that year was the great mathematician Sophus Lie (pronounced "Lee"), after whom Lie algebras and Lie groups are named. From 1873 to 1881, Sylow, with some help from Lie, prepared a new edition of Abel's works. In 1902, Sylow and Elling Holst published Abel's correspondence.

Sylow's spectacular theorems came in 1872. Upon learning of Sylow's discovery, C. Jordan called it "one of the essential points in the theory of permutations." The results took on greater importance when the theory of abstract groups flowered in the late 19th century and early 20th century.

In 1869, Sylow was offered a professorship at Christiania University but turned it down. Upon Sylow's retirement from high school teaching at age 65, Lie mounted a successful campaign to establish a chair for Sylow at Christiania University. Sylow held this position until his death on September 7, 1918.

Michael Aschbacher

> Fresh out of graduate school, he [Aschbacher] had just entered the field, and from that moment he became the driving force behind my program. In rapid succession he proved one astonishing theorem after another. Although there were many other major contributors to this final assault, Aschbacher alone was responsible for shrinking my projected 30-year timetable to a mere 10 years.
>
> *Daniel Gorenstein, Scientific American*

Michael Aschbacher was born on April 8, 1944, in Little Rock, Arkansas. Shortly after his birth, his family moved to Illinois, where his father was a professor of accounting and his mother was a high school English teacher. When he was nine years old, his family moved to East Lansing, Michigan; six years later, they moved to Los Angeles.

After high school, Aschbacher enrolled at the California Institute of Technology. In addition to his schoolwork, he passed the first four actuary exams and was employed for a few years as an actuary, full-time in the summers and part-time during the academic year. Two of the Caltech mathematicians who influenced him were Marshall Hall and Donald Knuth. In his senior year, Aschbacher took abstract algebra but showed little interest in the course. Accordingly, he received a grade of C.

In 1966, Aschbacher went to the University of Wisconsin for a Ph.D. degree. He completed his dissertation in 1969, and, after spending one year as an assistant professor at the University of Illinois, he returned to Caltech and quickly moved up to the rank of professor.

Aschbacher's dissertation work in the area of combinatorial geometries had led him to consider certain group theoretic questions. Gradually, he turned his attention more and more to purely group theoretic problems, particularly those bearing on the classification of finite simple groups. The 1980 Cole Prize Selection Committee said of one of his papers, "[It] lifted the subject to a new plateau and brought the classification within reach." Aschbacher has been elected to the National Academy of Sciences, the American Academy of Sciences, and the vice presidency of the American Mathematical Society. In 2011, Aschbacher received the $75000 Rolf Schock Prize from the Royal Swedish Academy of Sciences for "his fundamental contributions to one of the largest mathematical projects ever, the clasification of finite simple groups." In 2012, he shared the $100 000 Wolf Prize for his work in the theory of finite groups and shared the American Mathematical Society's Steele Prize for Exposition.

Computer Tutorial 13.[33][34]

order of an element

Input	Meaning
`print x;` `x;`	Recall that to print out the value of a variable x you use the command `print x;`, or simply `x;`. You should do this rather often.

`S:=Sym(6);`
`a:=S!(1,2)(3,4);`
`b:=S!(1,2,3);`
`c:=S!(1,2,3,4)(5,6);`
`d:=S!(1,2,3,4,5,6);`
`e:=S!(1,2,3)(4,5);`
	Define the five permutations below as elements of the symmetric group Sym(6) (calling them a, b, c, d and e respectively): $(1,2)(3,4)$, $(1,2,3)$, $(1,2,3,4)(5,6)$, $(1,2,3,4,5,6)$, $(1,2,3)(4,5)$.

`a^2; b^2; b^3; c^2; c^3; c^4;`
`for i in [1..7] do`
`  d^i;`
`end for;`
`for i in [1..7] do`
`  e^i;`
`end for;`
	For each of the elements $x \in \{a,b,c,d,e\}$, find all of its powers x, x^2, x^3, x^4, and so on. (Note that you can stop when you get the identity element, since after that the powers will repeat.)
	
	It's quicker if you use "for" loop.

`for i in [1..7] do`
`  d^(-i);`
`end for;`
`for i in [1..7] do`
`  e^(-i);`
`end for;`
	For each of the elements $x \in \{a,b,c,d,e\}$ find all of its powers x^{-1}, x^{-2}, x^{-3}, x^{-4}, and so on.
	If x^n is the identity, then $x^{n-1} = x^{-1}$, and $x^{n-2} = (x^2)^{-1} = x^{-2}$, and so on. So looping through the negative powers gives the same elements as obtained by looping through the positive powers, but in the reverse order.

`a^0, b^0, c^0, d^0, e^0;`	What do you think that x^0 should be? See if MAGMA agrees. (By definition, if G is a group and $x \in G$ then x^0 is the identity element of G.)

What is the order of each of the elements of $x \in \{a,b,c,d,e\}$?
 	
`Order(a), Order(b), Order(c);`
`Order(d), Order(e);`
	The order of x is the least positive integer n such that x^n is the identity. (This is another usage of the word "order": recall that the number of elements in a group is called the order of the group).
	Find order of each element by using your results from above, and then check your answers using the MAGMA function `Order`. (You can type `Order(a);` to get the order of a.)
	Our calculations above showed that the least positive integer n with $a^n = \mathrm{id}$ is $n = 2$. So the order of a is 2. Similarly b has order 3, c has order 4, and d and e both have order 6.

`H:=sub<S|a>;`
`#H;`
`H:=sub< S | b >;`
`#H;`
`#sub<S|c>, #sub<S|d>, #sub<S|e>;`
	The subgroup generated by a single element x is the set of all of its powers (positive, negative and zero). If G is a group and x an element of G then the MAGMA command `H:=sub<G|x>;` constructs the subgroup of G generated by x. The order of H is given by `#H`. Use this to print the orders of the subgroups generated by the elements listed above.
	The order of the subgroup generated by x is the same as the order of x, since if x has order n then the subgroup generated by x consists of the n elements $x^0 = \mathrm{id}$, x, x^2, ..., x^{n-1}.

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

[34] See also: `http://www.maths.usyd.edu.au/u/bobh/UoS/MATH2008/ctut06.pdf`