15 Osnovni izrek o končnih Abelskih grupah.

Spomnimo se: Naj bo $m = n_1 n_2 ... n_k$. Potem sta grupi $\mathbb{Z}_m$ in $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times ... \times \mathbb{Z}_{n_k}$ izomorfni če in samo če so si števila n_1, n_2, ..., n_k v paroma tuja.

1. Ki od naslednjih trditvi so točne: (odgovor obrazloži)

(a) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_5$.

(b) $\mathbb{Z}_2 \times \mathbb{Z}_6 \times \mathbb{Z}_5 \cong \mathbb{Z}_2 \times \mathbb{Z}_{30}$.

(c) $\mathbb{Z}_2 \times \mathbb{Z}_{30} \cong \mathbb{Z}_{60}$.

(d) $\mathbb{Z}_2 \times \mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5 \cong \mathbb{Z}_6 \times \mathbb{Z}_{10}$.

(e) $\mathbb{Z}_2 \times \mathbb{Z}_{30} \cong \mathbb{Z}_6 \times \mathbb{Z}_{10}$.

Izrek (Osnovni izrek o končnih Abelskih grupah)
Vsaka končna abelska grupa je direktni produkt cikličnih grup, katerih red je praštevilska potenca. Število cikličnih grup v produktu in njihov red sta enolično določena.

Ker je vsaka ciklična grupa reda n izomorfna grupi $\mathbb{Z}_n$, osnovni izrek o končnih Abelskih grupah torej pove, da je vsaka končna abelska grupa G izomorfna grupi oblike

$$\mathbb{Z}_{{p_1}^{n_1}} \times \mathbb{Z}_{{p_2}^{n_2}} \times ... \times \mathbb{Z}_{{p_k}^{n_k}}$$

kjer so p_i praštevila (ki niso nujno različna), in kjer so števila ${p_1}^{n_1}$, ${p_2}^{n_2}$, ..., ${p_k}^{n_k}$ $(n_i \in \mathbb{N})$ enolično določena z grupo G.

2. Do izomorfizma natančno poišči vse Abelske grupe reda

(i) 11.

(ii) 49.

(iii) 27.

(iv) 625.

3. Do izomorfizma natančno poišči vse Abelske grupe reda

(i) 36.

(ii) 80.

(iii) 1176.

4. Naj bo G abelska grupa reda 1176, v kateri obstaja element reda 8. Če vemo, da v grupi G obstaja tudi obstaja element reda 49, določi grupo, ki je izomorfna grupi G.

5. Napiši Cayley-evo tabelo za grupo $U(10)$. Kateri grupi je izomorfna grupa $U(10)$?

$*$	e	a	b	c
e	e	a	b	c
a	a	e	c	b
b	b	c	e	a
c	c	b	a	e

6. Dana je grupa G z grupno tabelo levo. Kateri znani grupi je izomorfna grupa G?

7. Grupa G je podana s tabelo

$\circ$	1	a	b	c	d	e	f	g
1	1	a	b	c	d	e	f	g
a	a	e	c	g	b	f	1	d
b	b	c	f	1	e	g	d	a
c	c	g	1	a	f	d	b	e
d	d	b	e	f	a	c	g	1
e	e	f	g	d	c	1	a	b
f	f	1	d	b	g	a	e	c
g	g	d	a	e	1	b	c	f

(a) Poišči red vsakega elementa grupe G.

(b) Ugotovi, kateri znani grupi je izomorfna grupa G in poišči eksplicitni izomorfizem.

8. Dana je grupa $G = \{1, 8, 12, 14, 18, 21, 27, 31, 34, 38, 44, 47, 51, 53, 57, 64\}$ za operacijo množenja po modulu 65.

(i) Ugotovi, kateri znani grupi je izomorfna grupa G.

(ii) Če je mogoče, določi $a, b \in G$ tako da je $G = \langle a \rangle \times \langle b \rangle$.

9. Dana je grupa $G = \{1, 8, 17, 19, 26, 28, 37, 44, 46, 53, 62, 64, 71, 73, 82, 89, 91, 98, 107, 109, 116, 118, 127, 134\}$ za operacijo množenja po modulu 135.

(i) Ugotovi, kateri znani grupi je izomorfna grupa G.

(ii) Če je mogoče, določi $a, b \in G$ tako da je $G = \langle a \rangle \times \langle b \rangle$.

Spomnimo se:

<u>Izrek</u> (fundamentalni izrek za ciklične grupe). Vsaka podgrupa ciklične grupe je ciklična. Poleg tega, če je $|\langle a\rangle| = n$, potem je red katerekoli podgrupe grupe $\langle a\rangle$ delitelj števila n. Za vsak pozitiven deljitelj k števila n, ima grupa $\langle a\rangle$ natanko eno podgrupo reda k - namreč $\langle a^{\frac{n}{k}}\rangle$.

<u>Posledica.</u> Za vsak pozitiven delitelj k števila n, je množica $\langle n/k\rangle$ podgrupa grupe $\mathbb{Z}_n$ reda k. Poleg tega, te podgrupe so edine podgrupe grupe $\mathbb{Z}_n$.

10. Izpiši vse podgrupe grupe $\mathbb{Z}_{30}$.

11. Če m deli red končne abelske grupe G, potem pokaži, da potem v grupi G obstaja podgrupa reda m.

12. (a) Katero je najmanjše pozitivno celo število n, za katerega obstajata natanko dve neizomorfni abelski grupi reda n? Navedite obe grupi.

(b) Katero je najmanjše pozitivno celo število n, za katerega obstajata natanko tri neizomorfni abelski grupi reda n? Navedite vse tri grupe.

(c) Katero je najmanjše pozitivno celo število n, za katerega obstajata natanko štiri neizomorfni abelski grupi reda n? Navedite vse štiri grupe.

13. (a) Koliko elementov reda 2 obstaja v vsaki od naslednjih štiri grup: $\mathbb{Z}_{16}$, $\mathbb{Z}_8 \times \mathbb{Z}_2$, $\mathbb{Z}_4 \times \mathbb{Z}_4$ and $\mathbb{Z}_4 \times \mathbb{Z}_2 \times \mathbb{Z}_2$? Naredite isto za elemente reda 4.

(b) Koliko elementov reda 3 obstaja v vsaki od naslednjih treh grup: $\mathbb{Z}_{27}$, $\mathbb{Z}_9 \times \mathbb{Z}_3$ in $\mathbb{Z}_3 \times \mathbb{Z}_3 \times \mathbb{Z}_3$?

14. Pokaži, da ima vsaka Abelska grupa reda 45 element reda 15. Ali ima vsaka abelska grupa reda 45 element reda 9?

15. (a) Pokaži, da obstajata dve (neizomorfni) abelski grupi reda 108, ki imata natanko eno podgrupo reda 3.

(b) Pokaži, da obstajata dve (neizomorfni) abelski grupi reda 108, ki imata natanko štiri podgrupe reda 3.

(c) Pokaži, da obstajata dve (neizomorfni) abelski grupi reda 108, ki imata natanko trinajst podgrup reda 3.

16. Predpostavimo, da je G Abelska grupa reda 120 in predpostavimo da G vsebuje natanko tri elementa reda 2. Do izomorfizma natančno poišči vse Abelske grupe, ki so izomorfne z G.

Naslednje tri naloge (naloge 17-19.) reši brez uporabe Osnovnega izreka o končnih Abelskih grupah.

17. Naj bo G končna abelska grupa reda $p^n m$, kjer je p praštevilo, ki ne deli m. Pokaži, da je potem $G = H \times K$, kjer $H = \{x \in G \,|\, x^{p^n} = e\}$ in $K = \{x \in G \,|\, x^m = e\}$. Poleg tega, $|H| = p^n$.

18. Naj bo G končna abelska grupa, ketere red je enak p^n, kjer je p praštevilo in $n \in \mathbb{N}$. Naj bo a element največjega reda v grupi G. Pokaži, da se potem grupa G lahko napiše v obliki $\langle a\rangle \times K$.

19. Končna Abelska grupa reda p^n, kjer je p praštevilo in $n \in \mathbb{N}$, je direktni produkt cikličnih grup.

POMEMBNI REZULTATI (Osnovni izrek o končnih Abelskih grupah.)

1. **(Osnovni izrek o končnih Abelskih grupah.)** Vsaka končna abelska grupa je direktni produkt cikličnih grup, katerih red je praštevilska potenca. Število cikličnih grup v produktu in njihov red sta enolično določena.

Ker je vsaka ciklična grupa reda n izomorfna grupi $\mathbb{Z}_n$, osnovni izrek o končnih Abelskih grupah torej pove, da je vsaka končna abelska grupa G izomorfna grupi oblike

$$\mathbb{Z}_{{p_1}^{n_1}} \times \mathbb{Z}_{{p_2}^{n_2}} \times ... \times \mathbb{Z}_{{p_k}^{n_k}}$$

kjer so p_i praštevila (ki niso nujno različna), in kjer so števila ${p_1}^{n_1}$, ${p_2}^{n_2}$, ..., ${p_k}^{n_k}$ $(n_i \in \mathbb{N})$ enolično določena z grupo G.

Olga Taussky-Todd

> "Olga Taussky-Todd was a distinguished and prolific mathematician who wrote about 300 papers."
>
> Edith Cuchins and
> Mary Ann McLoughlin,
> Notices of the American
> Mathematical Society, 1996

Olga Taussky-Todd was born on August 30, 1906, in Olmütz in the Austro-Hungarian Empire. Taussky-Todd received her doctoral degree in 1930 from the University of Vienna. In the early 1930s she was hired as an assistant at the University of Göttingen to edit books on the work of David Hilbert. She also edited lecture notes of Emil Artin and assisted Richard Courant. She spent 1934 and 1935 at Bryn Mawr and the next two years at Girton College in Cambridge, England. In 1937, she taught at the University of London. In 1947, she moved to the United States and took a job at the National Bureau of Standards' National Applied Mathematics Laboratory. In 1957, she became the first woman to teach at the California Institute of Technology as well as the first woman to receive tenure and a full professorship in mathematics, physics, or astronomy there. Thirteen Caltech Ph.D. students wrote their Ph.D. theses under her direction.

In addition to her influential contributions to linear algebra, Taussky-Todd did important work in number theory.

Taussky-Todd received many honors and awards. She was elected a Fellow of the American Association for the Advancement of Science and vice president of the American Mathematical Society. In 1990, Caltech established an instructorship named in her honor. Taussky-Todd died on October 7, 1995, at the age of 89.

Jessie MacWilliams

> She was a mathematician who was instrumental in developing the mathematical theory of error-correcting codes from its early development and whose Ph.D. thesis includes one of the most powerful theorems in coding theory.
>
> vera pless, SIAM News

An important contributor to coding theory was Jessie MacWilliams. She was born in 1917 in England. After studying at Cambridge University, MacWilliams came to the United States in 1939 to attend Johns Hopkins University. After one year at Johns Hopkins, she went to Harvard for a year.

In 1955, MacWilliams became a programmer at Bell Labs, where she learned about coding theory. Although she made a major discovery about codes while a programmer, she could not obtain a promotion to a math research position without a Ph.D. degree. She completed some of the requirements for the Ph.D. while working full-time at Bell Labs and looking after her family. She then returned to Harvard for a year (1961–1962), where she finished her degree. Interestingly, both MacWilliams and her daughter Ann were studying mathematics at Harvard at the same time.

MacWilliams returned to Bell Labs, where she remained until her retirement in 1983. The Institute of Electrical and Electronics Engineers published an issue of its journal IEEE on Information Theory Transactions containing papers dedicated to her in 1983. While at Bell Labs, she made many contributions to the subject of error-correcting codes, including The Theory of Error-Correcting Codes, written jointly with Neil Sloane. One of her results of great theoretical importance is known as the MacWilliams Identity. She died on May 27, 1990, at the age of 73.

Vera Pless

> Vera Pless is a leader in the field of coding theory.

Vera Pless was born on March 5, 1931, to Russian immigrants on the West Side of Chicago. She accepted a scholarship to attend the University of Chicago at age 15. The program at Chicago emphasized great literature but paid little attention to physics and mathematics. At age 18, with no more than one precalculus course in mathematics, she entered the prestigious graduate program in mathematics at Chicago, where, at that time, there were no women on the mathematics faculty or even women colloquium speakers. After passing her master's exam, she took a job as a research associate at Northwestern University while pursuing a Ph.D. there. In 1957, she obtained her degree.

Over the next several years, Pless stayed at home to raise her children while teaching part-time at Boston University. When she decided to work full-time, she found that women were not welcome at most colleges and universities. One person told her outright, "I would never hire a woman." Fortunately, there was an Air Force Lab in the area that had a group working on error-correcting codes. Although she had never even heard of coding theory, she was hired because of her background in algebra. When the lab discontinued basic research, she took a position as a research associate at MIT in 1972. In 1975, she went to the University of Illinois–Chicago, where she remained until her retirement.

During her career, Pless wrote more than 100 research papers, authored a widely used textbook on coding theory, and had 11 Ph. D. students.

Paul Erdös

> Paul Erdös is a socially helpless Hungarian who has thought about more mathematical problems than anyone else in history.
>
> The Atlantic Monthly

Paul Erdös (pronounced AIR-dish) was one of the best-known and most highly respected mathematicians of the 20th century. Unlike most of his contemporaries, who have concentrated on theory building, Erdös focused on problem solving and problem posing. The problems and methods of solution of Erdös-like those of Euler, whose solutions to special problems pointed the way to much of the mathematical theory we have today - have helped pioneer new theories, such as combinatorial and probabilistic number theory, combinatorial geometry, probabilistic and transfinite combinatorics, and graph theory.

Erdös was born on March 26, 1913, in Hungary. Both of his parents were high school mathematics teachers. Erdös, a Jew, left Hungary in 1934 at the age of 21 because of the rapid rise of anti-Semitism in Europe. For the rest of his life he traveled incessantly, rarely pausing more than a month in any one place, giving lectures for small honoraria and staying with fellow mathematicians. He had little property and no fixed address. All that he owned he carried with him in a medium-sized suitcase, frequently visiting as many as 15 places in a month. His motto was, "Another roof, another proof." Even in his eighties, he put in 19-hour days doing mathematics.

Erdös wrote more than 1500 research papers. He coauthored papers with more than 500 people. These people are said to have Erdös number 1. People who do not have Erdö number 1, but who have written a paper with someone who does, are said to have Erdös number 2, and so on, inductively.

Erdös received the Cole Prize in number theory from the American Mathematical Society, the Wolf Prize for lifelong contributions, and was elected to the U.S. National Academy of Sciences. Erdös died of a heart attack on September 20, 1996.