9 Direktni produkt grup

Definicija (kartezični produkt)
Kartezični produkt množic $S_1, S_2, ..., S_n$ je množica vseh urejenih n-teric $(a_1, a_2, ..., a_n)$, kjer je $a_i \in S_i$ za $i = 1, 2, ..., n$. Kartezični produkt pišemo kot: $S_1 \times S_2 \times ... \times S_n$ ali $\prod_{i=1}^{n} S_i$.

1. Naj bosta $(G_1, *)$ in $(G_2, \circ)$ grupi. Za $(a_1, a_2), (b_1, b_2) \in G_1 \times G_2$ definirajmo operacijo množenja po komponenah

$$(a_1, a_2)(b_1, b_2) = (a_1 * b_1, a_2 \circ b_2).$$

(a) Pokaži, da je $G_1 \times G_2$ skupaj s to operacijo grupa.

(b) Če sta $H_1 \leq G_1$ in $H_2 \leq G_2$, pokaži, da je potem $H_1 \times H_2 \leq G_1 \times G_2$.

Izrek (direktni produkt grup)
Naj bodo $G_1, G_2, ..., G_n$ grupe. Za $(a_1, a_2, ..., a_n)$ in $(b_1, b_2, ..., b_n)$ v $\prod_{i=1}^{n} G_i$ definirajmo operacijo množenja po komponentah

$$(a_1, a_2, ..., a_n)(b_1, b_2, ..., b_n) = (a_1 b_1, a_2 b_2, ..., a_n b_n).$$

Potem je $\prod_{i=1}^{n} G_i$ skupaj s to operacijo grupa, ki jo imenujemo direktni produkt grup G_i.

2. Dokaži izrek zgoraj.

3. (a) Napiši vse elemente grupe $U(8) \times U(10)$. Izračunaj $(3, 7) \cdot (5, 3)$ in $(3, 7) \cdot (7, 9)$.

(b) Določi generator grupe $\mathbb{Z} \times \mathbb{Z}_n$.

4. Označimo z $\mathbb{R}^\times$ grupo realnih števil $(\mathbb{R}, \cdot)$ glede na operacijo množenja ter z $\mathbb{C}^\times$ grupo kompleksnih števil $(\mathbb{C}, \cdot)$ glede na operacijo množenja. Pokaži da $\mathbb{R}^\times \times \mathbb{R}^\times \ncong \mathbb{C}^\times$.

5. Napiši vse elemente grupe $\mathbb{Z}_2 \times \mathbb{Z}_3$. Pokaži da je $\mathbb{Z}_6$ ciklična grupa, ter pokaži da je $\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6$.

6. Do izomorfizma natanko poišči vse grupe reda 4.

7. Naj bo $(g, h) \in G \times H$. Pokaži da je red elementa (g, h) enak najmanjšem skupnemu večkratniku redov elementov g in h.

Izrek (red elementa v direktnem produktu)

$$|(g_1, g_2, ..., g_n)| = \text{lcm}(|g_1|, |g_2|, ..., |g_n|)$$

(kjer je lcm "least common multiple" (najmanjši skupni večkratnik) npr. $\text{lcm}(2, 3, 5) = 15$).

8. Dokaži izrek zgoraj.

9. Poišči rede vseh elementov grupe $\mathbb{Z}_2 \times \mathbb{Z}_6$.

10. Določi število elementov reda 5 v grupi $\mathbb{Z}_{25} \times \mathbb{Z}_5$.

Spomnimo se fundamentalnega izreka za ciklične grupe ter izreka o številu elementov reda d v ciklični grupi:

Izrek (fundamentalni izrek za ciklične grupe)
Vsaka podgrupa ciklične grupe je ciklična. Poleg tega, če je $|\langle a \rangle| = n$, potem je red katere koli podgrupe grupe $\langle a \rangle$ delitelj števila n. Za vsaki pozitivni deljitelj k števila n, ima grupa $\langle a \rangle$ natanko eno podgrupo reda k - in sicer $\langle a^{\frac{n}{k}} \rangle$.

11. Dokaži fundamentalni izrek za ciklične grupe zgoraj.

Definicija (Eulerjeva funkcija fi)

Naj bo $\phi(1) = 1$, in za vsako celo število $n > 1$, označimo z $\phi(n)$ število pozitivnih celih števil, ki so manjša od n, in so tuja z n. Tako definirano funkcijo $\phi(n)$ imenujemo Eulerjeva funkcija fi. Opazimo, da iz definicije grupe $U(n)$ sledi, da $|U(n)| = \phi(n)$. Prvih 12 vrednosti funkcije $\phi(n)$ je danih v naslednji tabeli.

n	1	2	3	4	5	6	7	8	9	10	11	12
$\phi(n)$	1	1	2	2	4	2	6	4	6	4	10	4

Izrek (število elementov reda d v ciklični grupi)

Če je d pozitivno celo število ki deli n, potem je število elementov reda d v ciklični grupi reda n eneko $\phi(d)$.

12. Dokaži izrek zgoraj.

13. Določi število cikličnih podgrup reda 10 v grupi $\mathbb{Z}_{100} \times \mathbb{Z}_{25}$.

14. Določi število elementov reda 15 v grupi $S_3 \times \mathbb{Z}_{30} \times U(9)$.

15. Dokaži izrek spodaj.

Izrek (kriterij da je $G \times H$ ciklična)

Naj bosta G in H končni ciklični grupi. Potem je $G \times H$ ciklična če in samo če sta $|G|$ in $|H|$ tuji.

16. Ugotovi, ali sta dani grupi izomorfni in poišči eksplicitni izomorfizem, če sta:

(a) $\mathbb{Z}_6$ in $\mathbb{Z}_2 \times \mathbb{Z}_3$;
(b) $\mathbb{Z}_4$ in $\mathbb{Z}_2 \times \mathbb{Z}_2$;
(c) $\mathbb{Z}_{30}$ in $\mathbb{Z}_2 \times \mathbb{Z}_3 \times \mathbb{Z}_5$.

17. Pokaži, da je $\mathbb{Z}_m \times \mathbb{Z}_n$ izomorfna ciklični grupi $\mathbb{Z}_{m \cdot n}$ natanko tedaj ko sta m in n tuji si števili.

18. Poišči vse homomorfizme iz grupe $\mathbb{Z}_2 \times \mathbb{Z}_2$ v grupo $\mathbb{Z}_4$.

19. Poišči vse podgrupe grupe $\mathbb{Z}_2 \times \mathbb{Z}_4$.

Rešitve: **1.**(a) [$a_i \in G_i, b_i \in G_i$, $a_1 * b_1 \in G_1$, $a_2 * b_2 \in G_2$] **2.** [$a_i \in G_i, b_i \in G_i$, $a_i b_i \in G_i$] **3.** (a) [$(7,1)$, $(5,3)$] (b) $\mathbb{Z} \times \mathbb{Z}_n = \langle (1,0), (0,1) \rangle$ **4. 5.** [napiši, Cayley-evo tabelo] **6.** [$G \cong \mathbb{Z}_4$, $G \cong \mathbb{Z}_2 \times \mathbb{Z}_2$] **7. 8. 9.** [$|(0,3)| = \text{lcm}(|0|, |3|) = \text{lcm}(1,2) = 2$] **10.** [obstaja 24 element reda 5] **11. 12. 13.** [obstaja 6 cikličnih podgrup reda 10] **14.** [8+16+16+8+16+16+32=104] **15. 16.**(a) [$(1,1)$ generira $\mathbb{Z}_2 \times \mathbb{Z}_3$, grupi sta izomorfni]; (b) [grupa $\mathbb{Z}_2 \times \mathbb{Z}_2$ ni ciklična, grupi nista izomorfni]; (c) [lahko definiramo izomorfizem $\phi(k) = (k \bmod 2, k \bmod 3, k \bmod 5)$] **17. 18.** [4] **19.** [8]

POMEMBNI REZULTATI (Direktni produkt grup.)

1. **(Direktni produkt grup).** Naj bodo $G_1, G_2, ..., G_n$ grupe. Za $(a_1, a_2, ..., a_n)$ in $(b_1, b_2, ..., b_n)$ v $\prod_{i=1}^{n} G_i$ definirajmo operacijo množenja po komponentah $(a_1, a_2, ..., a_n)(b_1, b_2, ..., b_n) = (a_1 b_1, a_2 b_2, ..., a_n b_n)$. Potem je $\prod_{i=1}^{n} G_i$ skupaj s to operacijo grupa, ki jo imenujemo direktni produkt grup G_i.
2. **(Red elementa v direktnem produktu).** $|(g_1, g_2, ..., g_n)| = \text{lcm}(|g_1|, |g_2|, ..., |g_n|)$
3. **(Kriterij, da je $G \times H$ ciklična).** Naj bosta G in H končni ciklični grupi. Potem je $G \times H$ ciklična, če in samo če sta $|G|$ in $|H|$ tuji števili.
4. **(Kriterij za $\mathbb{Z}_{n_1 n_2 ... n_k} \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2} \times ... \times \mathbb{Z}_{n_k}$).** 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.
5. Spomnimo se $U(n) = \{k \in \mathbb{N} \mid k < n, \gcd(k,n) = 1\}$. Naj bosta s, t tuji naravni števili. Potem
$$U(st) \cong U(s) \times U(t).$$
Poleg tega, če je $U_k(n) = \{x \in U(n) \mid x \bmod k = 1\}$ potem $U_s(st) \cong U(t)$ in $U_t(st) \cong U(s)$.

Andrew Wiles

> For spectacular contributions to number theory and related fields, for major advances on fundamental conjectures, and for settling Fermat's Last Theorem.
> *Citation for the Wolf Prize*

In 1993, Andrew Wiles of Princeton electrified the mathematics community by announcing that he had proved Fermat's Last Theorem after seven years of effort. His proof, which ran 200 pages, relied heavily on ring theory and group theory. Because of Wiles's solid reputation and because his approach was based on deep results that had already shed much light on the problem, many experts in the field believed that Wiles had succeeded where so many others had failed. Wiles's achievement was reported in newspapers and magazines around the world. The New York Times ran a front-page story on it, and one TV network announced it on the evening news. Wiles even made People magazine's list of the 25 most intriguing people of 1993! In San Francisco a group of mathematicians rented a 1200-seat movie theater and sold tickets for $5.00 each for public lectures on the proof. Scalpers received as much as $25.00 a ticket for the sold-out event.

The bubble soon burst when experts had an opportunity to scrutinize Wiles's manuscript. By December, Wiles released a statement saying he was working to resolve a gap in the proof. In September of 1994, a paper by Wiles and Richard Taylor, a former student of his, circumvented the gap in the original proof. Since then, many experts have checked the proof and have found no errors. One mathematician was quoted as saying, "The exuberance is back." In 1997, Wiles's proof was the subject of a PBS Nova program.

Wiles was born in 1953 in Cambridge, England. He obtained his bachelor's degree at Oxford and his doctoral degree at Cambridge University in 1980. He was a professor at Oxford, where a building is named in his honor. Among his many prestigious awards is the Fermat prize for his research on Fermat's Last Theorem.

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

1. (a) In $\mathbb{Z}_9 \times \mathbb{Z}_6$, find all possible orders of elements. Give an element for each order. (b) Count the number of elements for each order. **2.** (a) For two groups G_1 and G_2, prove that $G_1 \times G_2 \cong G_2 \times G_1$. (b) Suppose that $G_1 \cong H_1$ and $G_2 \cong H_2$. Show that $G_1 \times G_2 \cong H_1 \times H_2$. **3.** For two groups G_1 and G_2, show that $Z(G_1 \times G_2) = Z(G_1) \times Z(G_2)$. **4.** Give examples of four groups of order 12, no two of which are isomorphic. Give reasons why no two are isomorphic. **5.** Find as many non-isomorphic Abelian groups of order 24 as you can. Explain why they are not isomorphic. **6.** Show that in $\mathbb{Z}_p \times \mathbb{Z}_p$ for a prime p, there are precisely $p + 1$ subgroups of order p. **7.** Prove or disprove that $\mathbb{Z} \times \mathbb{Z}$ is a cyclic group. **8.** Prove, by comparing orders of elements, that $\mathbb{Z}_8 \times \mathbb{Z}_2$ is not isomorphic to $\mathbb{Z}_4 \times \mathbb{Z}_4$. **9.** In $\mathbb{Z}_{40} \times \mathbb{Z}_{30}$, find two subgroups of order 12. **10.** Find all subgroups of order 4 in $\mathbb{Z}_4 \times \mathbb{Z}_4$. **11.** Find a subgroup of $\mathbb{Z}_{12} \times \mathbb{Z}_4 \times \mathbb{Z}_{15}$ that has order 9. **12.** Prove that $\mathbb{R}^* \times \mathbb{R}^*$ is not isomorphic to $\mathbb{C}^*$.

Appendix.[24][25]

combinatorics

factorial	`Factorial(10);`
binomial coefficient	`Binomial(10, 3);`
multinomial coefficient	`Multinomial(12, [3, 4, 5]);`
integer partitions	`Partitions(10);`
and count	`NumberOfPartitions(10);`
set partitions	`StirlingSecond(10, 3);`
and Bell number	`Bell(10);`
permutations with k disjoint cycles	`Abs(StirlingFirst(n, k));`
fibonacci number	`Fibonacci(10);`
and lucas number	`Lucas(10);`
bernoulli number	`BernoulliNumber(100);`
catalan number	`Catalan(10);`

number theory

pseudoprime test	`IsProbablyPrime(7);`
true prime test	`IsPrime(7);`
divisors	`// [1,2,4,5,10,20,25,50,100]:` `Divisors(100);`
prime factors	`// [2, 3, 7]:` `PrimeDivisors(84);`
next prime	`NextPrime(1000);`
and preceding	`PreviousPrime(1000);`
nth prime	`NthPrime(100);`
greatest common divisor	`Gcd(14, 21);`
and relatively prime test	`Gcd(Gcd(14, 21), 777);`
least common multiple	`Lcm(14, 21);`
moebius function	`MoebiusMu(11);`

subgroups

all subgroups	`Subgroups(Sym(4));`
subgroup lattice	`SubgroupLattice(Sym(4));`
maximal subgroups	`MaximalSubgroups(Sym(4));`
frattini subgroup	`D4 := DihedralGroup(4);` `FrattiniSubgroup(D4);`
normal subgroups	`NormalSubgroups(Sym(4));`

center	`Z4 := CyclicGroup(4);`
	`D6 := DihedralGroup(6);`
	`G := DirectProduct(Z4, D6);`
	`center := Centre(G);`

subgroup index	`Index(Sym(4), AlternatingGroup(4));`
example	`Q<s,t,u>, h := Group< s, t, u |`
Q is the finitely presented group	`t^2, u^17, s^2 = t^s = t, u^s = u^16, u^t = u >;`
in generators s, t, u;	`Q;`
	`S := sub< Q | t*s^2, u^4>;`
S is subgroup of Q generated by ts^2 and u^4	`S;`

[24]To write MAGMA code please open: `http://magma.maths.usyd.edu.au/calc/`
[25]See also: `http://www.maths.usyd.edu.au/u/bobh/UoS/MATH2008/ctut09.pdf`
[26]or `http://hyperpolyglot.org/more-computer-algebra`