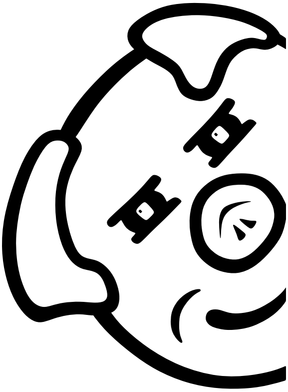
Matematický korespondenční seminář

Milý příteli!



Na jaro venku si možná ještě chvíli počkáme, ale jarní část našeho semináře už dávno zahájila série s dramatickým názvem „Být či nebýt“. Velká část řešitelů odpověď úspěšně nalezla a jejich bodový zisk je určitě potěší. Ale i pokud k nim náhodou nepatříš, nemusíš se bát. Ještě budeš mít několik příležitostí, jak vylepšit své umístění a zabojovat o místo na podzimním soustředění. Po čtvercích a krychlích můžeš zkusit sérii věnovanou algebře. Všem, které okouzlily grupy, přinášíme také závěrečný díl seriálu a jeho poslední tři úlohy. A samozřejmě nesmí chybět tradiční velké finále v podobě Myšmaše, kde si můžeš připomenout všechna letošní témata. Stejně jako v seriálu se Ti počítají všechny úlohy a celkem se v něm tedy hraje až o 35 bodů. A to se vyplatí!

Hodně dobrých nápadů při řešení Ti za všechny organizátory přeje

Kačka Nová

Co je dále v komentářích?

- Vzorová řešení 4. podzimní a 1. jarní série
- Vzorové řešení 2. seriálové série
- Teorie grup III. – Svoboda pro grupy
- Výsledkové listiny

- Příloha: Zadání 3. a 4. jarní série a 3. seriálové série
- Příloha: Pozvánka na jarní výlet

Jarní výlet

Tradiční jarní výlet po krásách naší republiky se letos uskuteční v sobotu 24. března, tedy den po Náboji.[1] Podrobnosti jsou na přiložené pozvánce, tento text na ni chce jen upozornit, abys ji jako zbytečný papír hned nepopsal(a) při řešení nových úloh a nezahodil(a). Těšíme se na Tebe!

Korespondenční seminář
KAM MFF UK
Malostranské náměstí 25
118 00 Praha 1

matfyz

[1] Náboj je mezinárodní týmová matematické soutěž, viz *naboj.org*.

Integers

4. PODZIMNÍ SÉRIE VZOROVÉ ŘEŠENÍ

Úloha 1.

Consider a pair of integers with the following properties:

(i) *Their decimal representations do not contain zeros.*
(ii) *We can remove ten digits from the decimal representation of each of them to get identical numbers (not necessarily the same ten digits for both numbers).*

Show that we can insert ten digits to the decimal representations of the two original numbers to obtain identical numbers.

(Anh Dung „Tonda" Le)

ŘEŠENÍ:

Instead of proving it directly we shall solve an equivalent problem. We will show it is possible (under the given assumptions) to obtain the second number from the first one by adding 10 digits and then erasing 10 digits from it.

Now to prove that this can be done, let $\overline{x_1 x_2 \ldots x_n}$ be the number we get after removing 10 digits from the original numbers. Then both original numbers contain the digits $x_1 x_2 \ldots x_n$ (in this order) and 10 additional digits somewhere in between them. Let $a_1 \ldots a_{10}$ be the digits removed from the first number and $b_1 \ldots b_{10}$ be the digits removed from the second number.

For each i we find the digits b_j between x_i and x_{i+1} in the second original number (if there are any) and insert them in the same order into the first original number between digits x_i and x_{i+1}. We also do the same with the digits before x_1 and after x_n. Then we delete digits $a_1 \ldots a_{10}$ and obtain the second original number.

POZNÁMKY:

Dôvodom, prečo čísla nemali obsahovať nuly, bolo, aby po vymazaní nemohli začínať nulou a teda nedochádzalo k nijakému skracovaniu čísel. Tento fakt vypichlo len málo riešiteľov ale body sme za to nestrhávali, keďže išlo len o viac menej technický detail. Väčšina riešiteľov postupovala trochu inak ako vzorové riešenie. Správne určila, že do prvého čísla treba pridať čísla ktoré sme vyškrtli z druhého a naopak. Potom čísla určite obsahujú tie isté číslice. Kameňom úrazu bolo ale vloženie týchto číslic na správne miesta, tak aby sme dostali dve rovnaké čísla. Niektorí tento krok vôbec neokomentovali a iným zas postup nefungoval pri rôznych rozloženiach číslic. Takéto riešenia boli hodnotené jedným alebo dvoma bodmi podľa závažnosti chýb. Na záver ešte podotýkam, že úloha vyžadovala dokázať to pre ľubovolnú dvojicu čísel spĺňajúcu podmienky zo zadania, a nie ukázať to pre jednu konkrétnu.

(Marta Kossaczká)

Úloha 2.

A knight encountered a hundred-headed dragon. A sign in front of the cave says that knight can cut only 3, 5 or 8 heads in one swing. If he cuts off 3 of its heads, 9 new will grow. If he cuts off 5 heads, 2 new will grow and if he cuts off 8 heads, 11 new heads will grow. However, if the dragon loses its last head, it dies and no heads will regrow. Prove that the knight cannot kill the dragon.

(David Hruška)

Řešení:

Suppose that the knight could kill the dragon. In this case, it would have 3, 5 or 8 heads before the last swing. If a swing does not kill the dragon, its headcount will change by a multiple of 3 (it can either gain 3, gain 6 or lose 3 heads in the process). Hence, the number of dragon's heads will always have the same remainder modulo 3 as in the beginning, which is 1. But none of the numbers 3, 5 and 8 have a remainder of 1, so the dragon is immortal.

Poznámky:

Většina došlých řešení byla správně. Několik řešitelů mylně předpokládalo, že stačí ukázat, že nula má jiný zbytek po dělení třemi než sto. To není pravda, jelikož zbytek se může změnit v posledním máchnutím mečem (drakovi už v takovém případě další hlavy nedorostou).

(Lucien Šíma)

Úloha 3.

Sir Filip and Madam Verča each picked a positive integer and secretly told Štěpán what their choice was. Štěpán wrote the product of the two numbers on one piece of paper and their sum on another one. Then he picked one of the pieces and showed it to Filip and Verča. It read 462. Filip said that he cannot determine Verča's number. After considering Filip's answer for a while Verča still couldn't find his number. What is Verča's number?

(Honza)

Řešení:

Let us denote Filip's number F and Verča's number V. If F was not a divisor of 462, he would know Verča's number instantly, because 462 could not be the product of their numbers and so V would have been $462 - F$. Also, $F \neq 462$, because then Filip would know that $V = 1$. From these two conditions, we (and Verča) know that $F \leq 231$.

Using the same arguments as in the first paragraph we conclude that $V \leq 231$ (Verča doesn't know F). If $V < 231$ then she knows that their numbers won't sum up to 462, so she can compute $F = 462/V$ easily. The only possible value of V is 231.

In the end, let us show that $V = 231$ satisfies our conditions. Suppose that Filip picks either 2 or 231. He doesn't know the number V because he has picked a divisor of 462. Verča doesn't know whether F is equal to 2 or 231 because the first possibility could happen if 462 was the product of their numbers and the second one if it was the sum.

Poznámky:

Většina došlých řešení byla správně. Nejčastější postup byl podobný vzorovému řešení. Někteří řešitelé došli k cíli prošetřením všech možných dělitelů čísla 462.

(Lucien Šíma)

Úloha 4.

Let $s(x)$ denote the sum of the digits in the decimal expansion of x. Find all positive integers n such that[2] $s(n!) = 9$.

(David Hruška)

Řešení:

We need to recall two well-known facts. Firstly, an integer is divisible by nine if and only if the sum of its digits is divisible by nine. Secondly, an integer is divisible by eleven if and only if the alternating sum of its digits is divisible by eleven, in other words, if and only if the difference of the sum of digits at even positions and the sum of digits at odd positions is divisible by eleven.

Now for $n \leq 5$ we can see that $n!$ is not divisible by nine which means that $s(n!)$ is not divisible by nine, therefore $s(n!)$ can't be nine.

Then we calculate $s(6!) = s(7!) = s(8!) = 9$, $s(9!) = s(10!) = 27 \neq 9$.

Finally, we will prove that for $n \geq 11$ the value of $s(n!)$ is not nine. So let us assume, for the sake of contradiction, that we have $n \geq 11$ such that $s(n!) = 9$. Let us denote the sum of its digits at even positions as $s_e(n!)$ and the sum of its digits at odd positions as $s_o(n!)$. Then $11 \mid s_e(n!) - s_o(n!)$ because $11 \mid n!$.

But $|s_e(n!) - s_o(n!)| \leq s_e(n!) + s_o(n!) = 9$ and the only multiple of 11 between -9 and 9 is zero. This means that $s_e(n!) = s_o(n!)$ which implies $2s_e(n!) = 9$. This is the desired contradiction because the left hand side is even and the right hand side is odd, therefore they cannot be equal.

We conclude that $s(n!) = 9$ holds only for $n \in \{6, 7, 8\}$.

Poznámky:

Zaslaná řešení byla poměrně různorodá, především co se týče značení a argumentace. Mnozí řešitelé nějakým způsobem nazvali jednotlivé cifry, sčítali pomocí sum a jejich řešení byla (nejspíše ve snaze o přesnost) až příliš složitá. Navíc jen málokdo na začátku zmínil, že uvažuje n, pro něž je $s(n!) = 9$, jinak to řešitelé předpokládali mlčky a jen z toho vyvozovali důsledky. Při čtení vzorového řešení se proto zkus zaměřit na strukturu důkazu sporem: nejprve řekneme, co chceme dokázat, pak předpokládáme negaci toho výroku, zjistíme, co z ní vyplývá, a dojdeme ke sporu.

Kromě uvedeného postupu několik řešitelů využilo vlastností ciferných součtů násobků 99 a faktu, že číslo n, pro nějž je $n \geq 11$, $s(n!) = 9$, musí být dělitelné 99.

(Bára Kociánová)

Úloha 5.

Anička and Bára have two sacks, one with m balls and the other with n balls. They decided to play a game with the following rules: They will take turns with Anička starting. In each turn, the player has to either remove a ball from one or both of the sacks, or move a ball from one sack to the other. If a ball is moved from one sack to another, it cannot be moved back in the very next move by the other player. Whoever removes the last ball, wins. With respect to m and n, who has the winning strategy[3]*?*

(Rado Švarc)

Řešení:

We shall prove that Bára has a winning strategy if and only if both m and n are even. We will show that if m and n are even, then at least one of them will be odd after Anička's turn. Moreover, Bára can then make them both even again and lower the sum of $m + n$.

When m and n are both even, Anička can:

- take one ball from one sack, which will necessarily lower m or n by one and make it odd,

[2] For a positive integer n we define $n! = 1 \cdot 2 \cdot \ldots \cdot n$ and we call this number *factorial of n*.

[3] A player has a winning strategy if he can achieve a win regardless of the moves of the other player.

- take one ball from both sacks, which will lower both m and n by one and make them both odd,
- take one ball from one sack to the other one, which will also make both m and n odd.

So after Anička's turn, Bára can take one ball from each sack containing odd number of balls (there is at least one such sack) and make the counts even again. This means that Anička always starts with even number of balls in each sack and therefore she can't win, because there will always be at least one non-empty sack after her turn (zero is even). In addition, Bára lowers the sum of $m+n$ in every turn and Anička cannot increase the sum, so the game cannot continue forever and Bára always wins.

On the other hand, if m, n or both of them are odd, Anička can take a ball from each sack with odd number of balls and then follow Bára's strategy from the previous case. This way, Anička has the winning strategy, so Bára can't have it anymore.

Poznámky:
Většina došlých řešení byla správně. Bohužel mírně nadpoloviční většina řešitelů použila k důkazu matematickou indukci, což až na pár světlých výjimek, jakou bylo například řešení *Matěje Doležálka*, vedlo na poměrně zdlouhavý rozbor případů.

Co mi však při opravování vadilo nejvíce, byl fakt, že pouze asi třetinu řešitelů alespoň napadlo, že by měli ukázat, že hra při následování dobré strategie vůbec skončí. Za tuto chybu jsem se rozhodl body nestrhávat, protože je konečnost docela dobře vidět, není však radno na benevolenci opravovatele příliš hřešit.

Jako zajímavost bych uvedl, že jediná *Lucka Krajčoviechová* si všimla, že tak, jak je hra zadána, vlastně v případě, kdy je již na začátku $m=n=0$, nevyhraje nikdo.

(Viki Němeček)

Úloha 6.

Let n be a positive integer. Suppose that we have a partition of all positive integers into n sets such that if two distinct numbers belong to the same set, so does their sum. What is the highest number which can be an element of a singleton[4]?

(Rado van Švarc)

Řešení:
For $n=1$ there cannot be any singleton. Suppose that $n>1$.

Firstly, we'll prove that there is only one set that isn't a singleton. Obviously, there is at least one, since we have infinitely many numbers and only finitely many sets. If there are two distinct sets with at least two elements each (let's call them X and Y), then we pick two pairs of distinct elements $a,b \in X$ and $c,d \in Y$. Since the sets are closed under addition of distinct elements, we can get that from $a,b \in X$ also $a+b \in X$, $a+2b \in X$, ..., $a+db \in X$, $2a+bd \in X$, ..., $ac+bd \in X$. Similarly, we obtain $ac+bd \in Y$. But X and Y are supposed to be disjoint, so we have a contradiction.

Therefore there are $n-1$ singletons and one set S containing the rest of the numbers.

Now we'll prove that no number in a singleton can be larger than $2n-2$. For the sake of contradiction, let k be an element of a singleton such that $k>2n-2$. Then the pairs $(1,k-1)$, $(2,k-2)$, ..., $(n-1,k-(n-1))$ are all distinct and each of them contains two distinct elements with sum k. (Numbers a and $k-a$ are distinct for $a \le n-1$, because $a \le n-1 < k-(n-1) \le k-a$.) But there are $n-1$ such pairs and only $n-2$ singletons other then the one containing k. That means that for some a both a and $k-a$ are in S and they are distinct. But then $k=a+(k-a) \in S$, which is a contradiction. Thus $k \le 2n-2$.

Finally, if we consider singletons $\{1\}$, $\{2\}$, ..., $\{n-2\}$, singleton $\{2n-2\}$, and one other set A consisting of the other elements of $\mathbb{N}$, we get a working example of n sets satisfying the given

[4] *Singleton* is a set which contains exactly one element.

condition (since if $\alpha, \beta \in A$ are distinct, then $\alpha + \beta \geq (n-1) + n = 2n - 1$, so $\alpha + \beta \in A$) with $\{2n-2\}$ being a singleton. So the answer is $2n - 2$.

POZNÁMKY:
Velká část správných řešení postupovala vzorově. Někteří si dobrovolně zkomplikovali život používáním tzv. Chicken McNugget Theorem. *(Rado van Švarc)*

Úloha 7.

Find all pairs of positive integers (n, k) satisfying the equation

$$n^k = (n-1)! + 1.$$

(Anh Dung „Tonda“ Le)

ŘEŠENÍ:
We will refer to the given equation as (♣). First we prove that any n satisfying (♣) must be a prime number. Clearly $n = 1$ is not a solution for any positive integer k. Furthermore, it follows from (♣) that n is coprime with all positive integers up to $n-1$ and these two facts together imply that n is indeed a prime number. Let us rewrite (♣) as

$$n^k - 1 = (n-1)(n^{k-1} + \cdots + 1) = (n-1)!,$$

divide the equation by $n-1$ and work modulo $n-1$:

$$k \equiv (n^{k-1} + \cdots + 1) \equiv (n-2)! \pmod{n-1}.$$

The first congruence is valid since $n \equiv 1 \pmod{n-1}$ and thus for each $0 \leq i \leq n-1$ we have $n^i \equiv 1 \pmod{n-1}$. Assuming $n > 5$ and recalling that n must be prime, then necessarily $2 \mid n-1$ and moreover the integers 2 and $\frac{n-1}{2}$ are distinct and both of them are contained in the product $(n-2)(n-1)\cdots 1 = (n-2)!$. It follows that $n-1 \mid (n-2)!$, and consequently $n-1 \mid k$. Since k is positive, we deduce that $k \geq n-1$. Now, since for $n > 5$ (even for $n > 2$) each number in the product $(n-1)! = 2 \cdot 3 \cdots (n-1)$ is smaller than n, we can make the estimate

$$n^k \geq n^{n-1} = n \cdot n^{n-2} > n^{n-2} + 1 \geq (n-1)! + 1.$$

It means that no prime number $n > 5$ can be a solution of (♣). It remains to check that among $n \in \{1, 2, 3, 4, 5\}$ there are three solutions $(n, k) \in \{(2, 1), (3, 1), (5, 2)\}$.

POZNÁMKY:
Úloha byla zajímavá rozmanitostí přístupů. V první části někteří řešitelé využili *Wilsonovy věty*[5], ve druhé pak tvrzení o p-valuacích výrazů $x^n \pm y^n$, kterému se obvykle říká *Lifting the Exponent Lemma*[6] nebo krátce *LTE*. Přestože se dalo obejít i bez těchto „kanónů“, líbilo se mi, že se je většinou podařilo s úspěchem použít. Na druhou stranu bych chtěl připomenout, že při používání složitějších tvrzení a vět je třeba ověřit jejich předpoklady, které nemusejí být například všude na internetu zformulovány zcela správně, jako je tomu třeba právě u zmíněného LTE. Tři nejelegantnější správná řešení si vysloužila kladný imaginární bod, jedno těžce rozebírací naopak záporný. Příslušnému řešiteli bych chtěl alespoň touto cestou vyjádřit obdiv nad vytrvalostí, jaká jistě byla při sepisování tohoto řešení potřeba, a nad tím, že jsem víceméně uvěřil v jeho správnost :-).
(David Hruška)

[5] https://en.wikipedia.org/wiki/Wilson_theorem

[6] *https://mks.mff.cuni.cz/library/LiftingTheExponentlemmaAL/LiftingTheExponentlemmaAL.pdf*

Úloha 8.

Consider a 2018×2018 *checkerboard covered with* 2×1 *rectangular tiles. Prove that it is possible to fill in all* 1×1 *squares with positive integers in such a way that:*

(i) *The sum of the two numbers on every tile is always the same.*
(ii) *Two neighbouring numbers, whose corresponding squares share a side, are coprime if and only if they belong to the same tile.*

(Anh Dung „Tonda“ Le)

Řešení:
We will call two neighbouring squares from the same tile *cotilear* and two neighbouring squares from different tiles *discontilear*.

Firstly, we will just try to satisfy the second condition.

We will start by writing number 1 into each square. Now for any two discontilear squares we multiply the numbers on both of these squares by a same prime number p, which we haven't used yet.

After updating all discontilear pairs of squares, the second condition is definitely satisfied: If two squares are discontilear, then their numbers are not coprime - we mulitplied both of them by a same prime number. On the other hand, if two squares are cotilear, then their numbers are coprime, since they were at the beginning and it couldn't have changed anywhere in the process (we never updated both of them at once and we used a different prime for each update).

Now, let P be a prime number bigger then the product of any two numbers on cotilear squares. Focus on one such tile with coprime numbers a and b. We know $P > ab$. Since a and b are coprime, there exists $c \in \mathbb{N}$ such that $c \leq b$ and $b \mid P - ac$. Then we change numbers a and b into ac and $P - ac$. We will do this for every tile (using the same P).

Now, every tile has the sum of its two numbers equal to P, so the first condition is satisfied.

Also, since $a \mid ac$ and $b \mid P - ac$, it must still be true, that two discotilear squares have numbers that aren't coprime - they weren't before and we only multiplied each of them by some positive integer.

On the other hand, two numbers on two cotilear squares are coprime, because if some prime p divided both of them, then it divides also their sum, which is P. But P is prime and the two numbers are both positive and smaller, so this can't happen.

And by this construction, we are done.

Poznámky:
Sešla se snůška různých řešení. Některá se odvíjela vzorovým způsobem, některá byla trochu kombinatoričtější a více ad hoc a další byla špatně. I zde se našel někdo, kdo si zkomplikoval život používáním Chicken McNugget Theorem.

(Rado van Švarc)

Být či nebýt

1. jarní série Vzorové řešení

Úloha 1.

Dánsko a Anglie spolu hrály fotbal. Dánský tým dal celkem osm gólů, kdežto anglický pět. Musel během utkání existovat okamžik, kdy se počet gólů, které již Anglie dala, rovnal počtu gólů, které Dánsko ještě dá?

(Anh Dung „Tonda“ Le)

Řešení:
Označme si A počet gólů, které dala Anglie, a D počet gólů, které dalo Dánsko. Zadání se ptá, zda nastane moment, kdy $A = 8 - D$, po úpravě $A + D = 8$. Dohromady daly oba týmy $A + D = 13$ gólů a protože nelze dát dva góly naráz, mění se součet $A + D$ při každé změně skóre právě o jedna. Součet $A + D$ se mění od 0 do 13 po jedné, tedy určitě v nějaký okamžik $A + D = 8$. V tento okamžik se počet gólů, které Anglie dala, rovná počtu gólů, které Dánsko ještě dá.

Poznámky:
Drtivá většina řešení byla stejná jako to vzorové. Někdy se objevila řešení využívající brutální síly výpisu možností, kterých naštěstí nebylo tolik, takže tato cesta až tak pracná nebyla. Byl jsem při bodování velmi benevolentní a i ne zcela přesně popsané řešení jsem uznal za plný počet bodů. Důvod této benevolence tkvěl v tom, že správná myšlenka v řešeních byla, jen formulace byly leckdy pochybné.

(Jan Kadlec)

Úloha 2.

Na tabuli je napsáno číslo 42*. Pokud je na tabuli napsané přirozené číslo n, může Honza zvolit dvě přirozená čísla a, b se součtem n a nahradit číslo na tabuli číslem ab. Existuje posloupnost tahů, kterou se Honzovi povede vytvořit na tabuli číslo* 2018*?*

(Honza Krejčí)

Řešení:
Libovolné přirozené $n > 1$ můžeme zapsat jako $n = 1 + (n - 1)$ a na tabuli dostat součin $1 \cdot (n - 1) = n - 1$. Jakékoli číslo tak můžeme libovolně dlouho o jedna zmenšovat. Stačí nám tedy získat nějaké číslo větší nebo rovno 2018, číslo 2018 pak dostaneme právě popsaným zmenšováním.

Takové číslo můžeme vytvořit například těmito dvěma kroky: Nejprve z $42 = 21 + 21$ dostaneme $21 \cdot 21 = 441 = 220 + 221$, z čehož následně vytvoříme $220 \cdot 221 = 48620$.

Posloupnost tahů, kterou se Honza může dostat od 42 k 2018, tedy existuje.

Poznámky:
S řešením (až na pár chyb ve sčítání dvouciferných čísel) neměl problém téměř nikdo. Zato dost řešitelů si ab v zadání vyložilo jako napsání čísel a a b za sebe místo jejich součinu. Nakonec jsme se shodli, že takovou interpretaci také uznáme, takže i za správné řešení pozměněné úlohy bylo možné

získat plný počet bodů. Nicméně obvykle se výrazem ab myslí vždy součin, pokud není explicitně řečeno jinak.

V zadání byly dvě speciální hodnoty, ale obecně se umíme z libovolného přirozeného $n > 4$ dostat na libovolné větší číslo třeba tak, že opakovaně volíme $a = 2, b = n-2$. Pak $2 \cdot (n-2) = 2n-4 > n$. Takže úloha je řešitelná i pro libovolné $k > 4$ místo 42 a libovolné přirozené l místo 2018.

(Karolína Kuchyňová)

Úloha 3.

Existuje čtveřice bodů v rovině taková, že každá z ní vybraná trojice bodů je osově symetrická[7], *ale celá čtveřice žádnou osu symetrie nemá?*

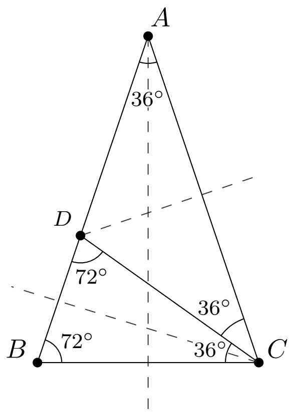
(Honza Krejčí)

Řešení (volně podle Lenky Kopfové):
Ano, existuje. Víme, že tři body jsou osově symetrické, pokud tvoří rovnoramenný trojúhelník nebo pokud leží na jedné přímce (každý bod se v tomto případě zobrazí symetrií sám na sebe podle přímky, na které všechny leží).

Mějme trojúhelník ABC s úhly $36°$, $72°$, $72°$. Bod D zvolíme na přímce AB tak, aby platilo $|BC| = |CD|$. Tím dostaneme rovnoramenný trojúhelník CDB, a tedy $|\sphericalangle BDC| = 72°$. Z toho plyne, že D leží na úsečce AB – nerovnost $90° > 72°$ zaručuje, že D leží na polopřímce BA, a nerovnost $72° > 36°$ zaručuje, že D leží na polopřímce AB. Nyní už snadno dopočteme velikost úhlu ACD, která vyjde $36°$. Z toho plyne, že i $\triangle DCA$ je rovnoramenný.

Všechny trojice bodů jsou osově symetrické: ABC, DCA, CDB tvoří rovnoramenné trojúhelníky a ABD leží na jedné přímce. Zároveň celá čtveřice bodů žádnou osu symetrie nemá. Pokud vám toto tvrzení nepřijde zřejmé, můžeme ho nahlédnout například takto:

Aby se každý bod zobrazil podle osy sám na sebe, musely by všechny ležet v jedné přímce, což evidentně neplatí. Aby symetrie prohodila dva body a zbylé dva nechala na svém místě, muselo by platit, že jedna z přímek tvořená dvojicí bodů je osou úsečky mezi zbývajícími body. To ale také určitě neplatí, protože žádné dvě úsečky na sebe nejsou kolmé. Poslední možností je, že symetrie prohodí dvě dvojice bodů. K tomu by bylo nutné, aby dvě osy stran splývaly. To také neplatí, protože žádné dvě strany nejsou rovnoběžné, a tedy ani jejich osy nemůžou být rovnoběžné a splývat.



[7] Skupinu bodů považujeme za osově symetrickou, i když všechny leží na jedné přímce.

Poznámky:

Úloha se ukázala být docela těžká, správné řešení nám poslalo jen 13 řešitelů. Téměř všechna špatná řešení přitom ztroskotala na podobném problému. Psali jste, že aby byly tři body osově souměrné, musí tvořit rovnoramenný trojúhelník, a z toho jste nějakým způsobem došli k závěru, že i celá čtveřice musí mít osu symetrie. Už předpoklad ovšem nebyl správný. Body jsou osově symetrické i v případě, že všechny leží na jedné přímce. A nemusí ani jeden z nich být středem úsečky tvořené zbývajícími dvěma, protože tyto body jsou symetrické podle přímky, na které leží (každý se symetrií zobrazuje sám na sebe). Úloha byla v tomto směru velmi záludná, a tak jsme se vám v poznámce pod čarou snažili trochu napovědět, že body ležící na jedné přímce jsou vždy osově symetrické.

(Michal Töpfer)

Úloha 4.

Na matfyzu od 8 *do* 16 *hodin pracuje* n *lidí. Každý z nich je během pracovní doby buď na matfyzu, nebo v kavárně. Přechod mezi těmito místy netrvá žádný čas a na každém z nich může člověk zůstat libovolně krátkou dobu. Matfyzáci spolu nechtějí trávit moc času. Pro která* n *umíme zařídit, aby spolu žádní dva zaměstnanci za celou pracovní dobu nestrávili více než čtyři hodiny (sčítá se čas na pracovišti i v kavárně)?*

(Jakub Löwit)

Řešení:

Ukážeme, že to můžeme zařídit pro každé n. Matfyzáky si označíme M_0, M_1, ... ,M_{n-1}. Matfyzák M_i začne svůj den na matfyzu a každých $8 \cdot 2^{-i}$ hodin přejde na druhé místo, než na kterém se právě nachází. To znamená, že matfyzák M_0 bude celou pracovní dobu na matfyzu, M_1 bude čtyři hodiny na matfyzu a pak čtyři v kavárně, M_2 dvě na matfyzu, dvě v kavárně a pak to samé ještě jednou a tak dále.

Ukážeme, že matfyzáci M_i a M_j pro $i \neq j$ spolu strávili právě 4 hodiny. Nechť bez újmy na obecnosti platí $i < j$. Matfyzák M_j pak střídá místa přesně 2^{j-i}krát častěji než M_i. Protože $j-i$ je alespoň jedna, je 2^{j-i} sudé číslo, a tedy bez ohledu na to, kde je matfyzák M_i v daném úseku mezi dvěma svými přechody, stráví s ním matfyzák M_j právě půlku této doby. To ale platí v každém úseku mezi dvěma přechody matfyzáka M_i, a tedy i pro celou pracovní dobu.

Poznámky:

Asi tři čtvrtiny úspěšných řešitelů postupovaly přibližně podle vzoráku. Ve velké části těchto řešení ale chyběl jakýkoli náznak důkazu, že konstrukce funguje. Protože rozhodně není úplně triviální, strhl jsem v takových případech jeden bod.

Ostatní řešitelé typicky řekli, že vyzkouší všechny možné kombinace, jak může být polovina zaměstnanců (zaokrouhlená pro liché n) na matfyzu a polovina v kavárně, a každou z nich nechají probíhat po stejně dlouhou dobu. Při aplikaci tohoto postupu dokonce dokazovaná nerovnost vyšla ostře. Bohužel tato cesta obsahovala poměrně hodně technických úprav s kombinačními čísly, a pokud řešitel nevymyslel, jak to obejít, navíc i potřebu řešit úlohu zvlášť pro liché a sudé n.

K mému překvapení nejelegantnější řešení, které přišlo, patřilo do druhé kategorie. *Martinovi Zimenovi* se úspěšně podařilo obejít všechny technické výpočty mimo jiné tím, že uvažoval za různá rozmístění i ta, která se lišila pouze pořadím pracovníků v kavárně či na matfyzu (přestože stran toho, kdo je s kým, jsou tato rozmístění stejná), čímž si vysloužil jeden kladný imaginární bod.

Pozitivně mě překvapilo, že ani jediný řešitel se nepokusil dokázat, že pro nějaká n již konstrukce neexistuje.

(Viki Němeček)

Úloha 5.

Na kružnici leží několik hrobů. Do každého z nich dal Hamlet několik lebek (klidně žádnou), k nějakému neprázdnému se postavil a začal si hrát podle následujících pravidel. Pokud u sebe nemá žádné lebky, vezme si všechny z hrobu, u kterého právě stojí, a hned se posune o jeden dál. V opačném případě dá jednu lebku do hrobu, u něhož se nachází, a pokud ještě nějakou drží, přejde opět k dalšímu hrobu. Dokažte, že ať Hamlet rozmístí lebky jakkoli a postaví se kamkoli, budou po nějaké době počty lebek v jednotlivých hrobech stejné jako na začátku.

(Anh Dung „Tonda“ Le)

Řešení:

Buď n počet hrobů. Jako *stav* nazveme uspořádanou $(n+2)$-tici čísel, složenou z počtů lebek v n jednotlivých hrobech; počtu lebek, které právě drží Hamlet; a polohy Hamleta (tj. čísla hrobu, u kterého Hamlet právě stojí). To nám bude popisovat situaci těsně před tím, než Hamlet učiní další krok (tj. než se přesune k dalšímu hrobu). Všimneme si, že počet různých *stavů* je konečný. Máme totiž konečně mnoho lebek, takže prvních $n+1$ čísel popisujících *stav* je shora omezeno počtem lebek a zdola nulou a Hamletova pozice může nabývat jen n různých hodnot. Dále si uvědomíme, že ze zadání má Hamlet vždy jasně daný následující krok.

Celou situaci si představíme jako orientovaný graf[8], kde vrcholy jsou *stavy*. Ze *stavu* A do *stavu* B vede šipka právě tehdy, když Hamlet ze *stavu* A přejde do *stavu* B. Díky tomu, že má Hamlet vždy jednoznačně určený následující krok, víme, že z každého *stavu* vede právě jedna šipka.

Dále ukážeme, že v každém *stavu* umíme jednoznačně určit předcházející *stav*, pokud existuje – neboli že do každého vrcholu v orientovaném grafu vede nanejvýš jedna šipka.

Uvažujme tedy nějaký *stav*, do kterého vede šipka. Pokud se Hamlet vyskytuje u hrobu, ve kterém jsou nějaké lebky, znamená to, že tam právě jednu přidal. Předchozí stav tedy najdeme tak, že Hamlet z tohoto hrobu jednu lebku vezme a přejde o hrob zpátky. Pokud se Hamlet vyskytuje u prázdného hrobu, znamená to, že z něj právě musel vzít všechny lebky. Všechny je tam tedy vrátí. (Musel nějaké mít, protože jinak by se nedalo jít o krok zpět.) Tím ovšem neudělá plný krok zpět, protože každý krok začíná tím, že Hamlet přejde k novému hrobu. Jsme ale opět ve stejné situaci jako předtím (Hamlet stojí u hrobu, ve kterém jsou nějaké lebky) a o krok zpět se jednoznačně vrátíme způsobem, jaký je popsán výše.

Takto dokážeme jednoznačně určit předcházející *stav*, to znamená, že v našem orientovaném grafu vede do každého vrcholu nanejvýš jedna šipka. Díky tomu, že je *stavů* konečně mnoho, víme, že po určitém počtu kroků se některý *stav* zopakuje. Protože následující *stav* je jednoznačně určený, bude se odteď Hamlet pohybovat cyklicky. Ukážeme, že počáteční *stav* musí být v tomto cyklu.

Pro spor nechť není v tomto cyklu. Pak existuje první *stav*, nazvěme jej A, který Hamlet navštívil a je obsažen v cyklu. Označíme předcházející *stav* v cyklu B_1 a předcházející *stav* na Hamletově cestě B_2. Z předpokladu není B_2 v cyklu, tedy B_1 a B_2 se liší. To je ovšem spor, protože bychom se uměli do *stavu* A dostat ze dvou různých *stavů*.

Tím jsme ukázali, že počáteční *stav* je vždy obsažen v cyklu, a tedy se po nějakém počtu kroků zopakuje.

Poznámky:

Většina přišlých řešení byla správná. Body jsem snížila za řešení, kde řešitel zapomněl dokázat, že předcházející stav je určen jednoznačně, nebo zapomněl uvést, že stavů je jen konečně mnoho.

(„madam Verča“ Hladíková)

[8] Pokud nevíš, co je orientovaný graf, tak si stačí představovat obrázek s puntíky nazývanými vrcholy a šipkami nazývanými hranami.

Úloha 6.

Existuje nekonečná posloupnost kladných reálných čísel $x_0, x_1, x_2, \ldots$ taková, že pro každé přirozené $n \geq 2$ platí $x_n = \sqrt{x_{n-1}} - \sqrt{x_{n-2}}$?

(Rado van Švarc)

Řešení:

Pro spor předpokládejme, že taková posloupnost existuje. Pokud by pro nějaké $i \in \mathbb{N}$ bylo $x_i \leq x_{i-1}$, pak $\sqrt{x_i} \leq \sqrt{x_{i-1}}$, a tedy $x_{i+1} = \sqrt{x_i} - \sqrt{x_{i-1}} \leq 0$, což nelze. Posloupnost je tedy (ostře) rostoucí.

Pro každé $i \in \mathbb{N}$ také platí

$$x_i < x_{i+1} = \sqrt{x_i} - \sqrt{x_{i-1}} < \sqrt{x_i},$$

tudíž $x_i < \sqrt{x_i}$, a tedy $x_i < 1$.

Nakonec využijeme toho, že $x_0 > 0$. Označme[9] $n = \left\lceil \frac{1}{x_0} \right\rceil + 1$ a odhadněme dvěma způsoby součet $\sum_{i=2}^{n} x_i$:

$$\begin{aligned}\sum_{i=2}^{n} x_i &= \sqrt{x_1} - \sqrt{x_0} + \sqrt{x_2} - \sqrt{x_1} + \cdots + \sqrt{x_{n-1}} - \sqrt{x_{n-2}} \\ &= \sqrt{x_{n-1}} - \sqrt{x_0} < \sqrt{x_{n-1}} < 1,\end{aligned}$$

$$\sum_{i=2}^{n} x_i > \sum_{i=2}^{n} x_0 = \left(\left\lceil \frac{1}{x_0} \right\rceil + 1 - 1 \right) \cdot x_0 \geq \frac{x_0}{x_0} = 1.$$

Tyto dva odhady jsou vzájemně ve sporu, tudíž taková posloupnost nemůže existovat.

Poznámky:

Úloha byla vcelku přímočará, většina řešení postupovala obdobně jako vzorové. Druhou oblíbenou možností bylo využití pokročilého tvrzení, že každá rostoucí shora omezená posloupnost konverguje, a tedy existuje $n \in \mathbb{N}$ takové, že $\sqrt{x_n} - \sqrt{x_{n-1}} < x_0$, což je opět spor.

U špatných řešení byl často problém se správným uchopením pojmu nekonečno – obvykle ve smyslu: „Tuto operaci můžeme provést nekonečněkrát.“ Buď to ale nebylo zdůvodněno, nebo to dokonce nebylo vůbec možné.

(Tomáš Novotný)

Úloha 7.

Rozhodněte, zda mohou být (či nebýt) dva překrývající se konvexní čtyřúhelníky A a B a bod X ležící v obou z nich[10] tak, aby byly splněny následující dvě podmínky:

(i) *Pro každou přímku vedenou bodem X platí, že její část v A je kratší než její část v B.*
(ii) *Obsah A je alespoň 1,9krát větší než obsah B.*

(Rado van Švarc)

[9] $\lceil x \rceil$ značí horní celou část z čísla x, tj. nejmenší celé číslo takové, že není menší než x.
[10] Bod X může ležet i na hranici čtyřúhelníku.

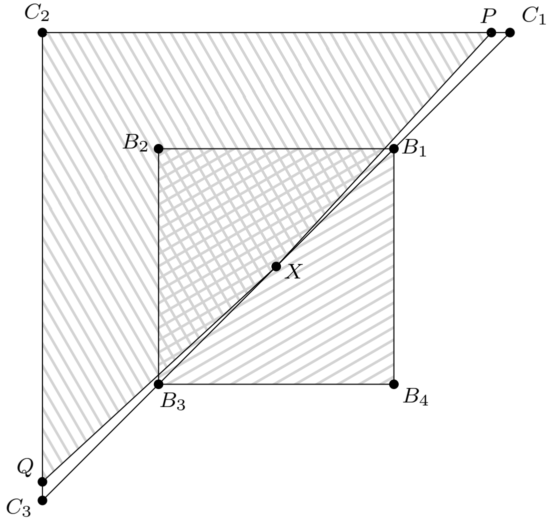
Řešení:

Buď $B_1B_2B_3B_4$ čtverec se stranou délky 1, jehož střed označíme X. Nechť jsou C_1, C_2, C_3 obrazy bodů B_1, B_2, B_3 ve stejnolehlosti se středem X a koeficientem $1{,}99$. Platí, že obsah trojúhelníku $C_1C_2C_3$ je $\frac{1{,}99^2}{2} > 1{,}9$. Buď $x = \frac{1{,}99^2}{2} - 1{,}9$. Nechť P, resp. Q, leží na úsečce C_1C_2, resp. C_2C_3 tak, že obsah trojúhelníku C_1PX, resp. C_2QX je nanejvýš $\frac{x}{2}$.

Za A zvolíme čtyřúhelník PC_2QX a za B čtverec $B_1B_2B_3B_4$. Ukážeme, že vyhovují zadaným podmínkám.

Zjevně B má obsah 1 a A má obsah alespoň $\frac{1{,}99^2}{2} - 2 \cdot \frac{x}{2} = 1{,}9$, tedy A a B splňují druhou podmínku.

Nyní buď ℓ přímka procházející X. Pokud protíná A jenom v bodě X, je podmínka zjevně splněna. V opačném případě nechť protíná obvod A krom bodu X také v bodě Y a nechť Z je průsečík úsečky XY s obvodem B. Ze stejnolehlosti platí, že $|XY| = 1{,}99|XZ|$. Zároveň ale protože X je střed B, protíná ℓ čtverec B v úsečce délky $2|XZ|$. Tedy část ℓ která leží v A (tj. XZ) je kratší, než část ℓ, která leží v B, čímž máme hotovo.



Poznámky:

Většina řešení buď nesprávně tvrdila, že daný útvar neexistuje, nebo ho úspěšně zkonstruovala. Všechny konstrukce byly podobné té vzorové, ačkoliv někteří použili jiný typ trojúhelníka (tj. například jejich $C_1C_2C_3$ byl rovnostranný a B vznikl slepením dvou menších takových trojúhelníčků do kosočtverce). *(Rado van Švarc)*

Úloha 8.

Buď $S = \{-1; 1\}$. Funkce $\operatorname{sg} : \mathbb{R} \to S$ dává $\operatorname{sg}(x) = 1$ pro $x \geq 0$ a $\operatorname{sg}(x) = -1$ pro $x < 0$. Pro $n \in \mathbb{N}$ mějme čísla $a_{i,j}, b_i \in S$, $1 \leq i, j \leq n$ a pro $x_1, x_2, \ldots, x_n \in S$ definujme

$$y_i = \operatorname{sg}\left(\sum_{j=1}^{n} a_{i,j}x_j\right) \qquad \text{a} \qquad z = \operatorname{sg}\left(\sum_{i=1}^{n} b_i y_i\right).$$

Rozhodněte, zda pro každé liché n existují taková $a_{i,j}, b_i \in S$, $1 \leq i, j \leq n$, že pro libovolná $x_1, x_2, \ldots, x_n \in S$ platí $z = x_1x_2\cdots x_n$.

(Rado van Švarc)

Řešení:
Označme si $n = 2k+1$ a $M = \{1, 2, \ldots, n\}$.

Ukážeme, že pro každé n taková čísla $a_{i,j}$, b_i existují. Pro každé i položíme $b_i = 1$. Dále pokud $i - j$ dává po dělení n zbytek menší než k, zvolíme $a_{i,j} = -1$, jinak $a_{i,j} = 1$. Tvrdíme, že tato volba konstant skutečně vyhovuje zadání.

Buď α počet i, pro která je $x_i = -1$. Zjevně chceme ukázat, že $z = (-1)^\alpha$. Protože všechna $a_{i,j}$, b_i, x_i i y_i jsou lichá (jsou to ±1) a n je liché, jsou i všechny uvažované součty liché, a tedy nikdy nebudeme pracovat se $\mathrm{sg}(0)$. Z toho plyne, že tvrzení stačí ukázat pro případ, kdy je α liché. (Tj. chceme pro tento případ ukázat $z = -1$.) Pro sudé α bychom se totiž podívali na posloupnost $x'_i = -x_i$, která by příslušný počet -1 měla lichý. Pro ni by platilo $z' = -1$. Zároveň protože sg je lichá funkce na $\mathbb{R} \setminus \{0\}$ a žádný ze součtů nenabývá nuly, plyne z $x'_i = -x_i$ také $y'_i = -y_i$, a tedy i $z' = -z$, z čehož $z = 1$, což je přesně to, co jsme chtěli.

Dvojici čísel (i, j) nyní nazveme příjemnou, pokud $i, j \in M$ a $i - j \equiv \pm k \pmod n$. Ukážeme, že pokud (i, j) je příjemná dvojice, potom $y_i = -1$ nebo $y_j = -1$.

Nejprve ukážeme, jak z tohoto pozorování již plyne požadované tvrzení. Nechť skutečně pro každou takovou dvojici je $y_i = -1$ nebo $y_j = -1$. Buď $y_a = -1$ (takové existuje – stačí vzít buď y_1, nebo y_{1+k}). Potom (pokud bereme indexy modulo n) platí $y_{a+2pk-k} + y_{a+2pk} \le 0$, tedy $\sum_{i=1}^n b_i y_i = y_a + \sum_{p=1}^k (y_{a+2pk-k} + y_{a+2pk}) \le -1$, z čehož už plyne $z = -1$.

Buď tedy (i, j) příjemná dvojice, BÚNO nechť $j \equiv i + k \pmod n$. Pro spor předpokládejme že $y_i = 1 = y_j$. Buď S_i, resp. S_j, množina všech s takových, že $a_{i,s}$, resp. $a_{j,s}$, je rovno -1. Povšimněme si, že kdyby pro nějaké s bylo $a_{i,s} = -1 = a_{j,s}$ pak jak $i - s$, tak $j - s = i - s + k$ dává zbytek po dělení n menší nebo roven k, což se nemůže stát. Proto jsou množiny S_i a S_j disjunktní.

Buď A množina těch s, pro která je $x_s = -1$. Označme si jako c_i a c_j velikosti množin $A \cap S_i$ a $A \cap S_j$. Zjevně $|A| = \alpha$. Protože S_i obsahuje ta s, pro která je $a_{i,s} = -1$, neboli ta s, pro která je zbytek $i - s$ po dělení n menší než k, je $|S_i| = k$. Protože $|A \cap S_i| + |(M \setminus A) \cap S_i| = |S_i| = k$, platí $|(M \setminus A) \cap S_i| = k - c_i$. Protože $|A \cap S_i| + |A \cap (M \setminus S_i)| = |A| = \alpha$, je $|A \cap (M \setminus S_i)| = \alpha - c_i$. Nakonec protože $|A \cap (M \setminus S_i)| + |(M \setminus A) \cap (M \setminus S_i)| = |M \setminus S_i| = k+1$, je $|(M \setminus A) \cap (M \setminus S_i)| = k + 1 - \alpha + c_i$.

Platí $\sum_{s=1}^n a_{i,s} x_s = |A \cap S_i| - |(M \setminus A) \cap S_i| - |A \cap (M \setminus S_i)| + |(M \setminus A) \cap (M \setminus S_i)| = c_i - (k - c_i) - (\alpha - c_i) + (k + 1 - \alpha + c_i) = 4c_i - 2\alpha + 1$. Protože $y_i = 1$, je tento součet kladný, tedy $4c_i - 2\alpha + 1 \ge 1$, což nám dává $2c_i \ge \alpha$. Díky tomu, že $2c_i$ je sudé a α je liché, je dokonce $2c_i \ge \alpha + 1$. Analogicky $2c_j \ge \alpha + 1$. Z toho sečtením dostáváme $c_i + c_j \ge \alpha + 1$. Potom $\alpha = |A| = |S_i \cap A| + |S_j \cap A| + |(M \setminus (S_i \cup S_j)) \cap A| \ge c_i + c_j \ge \alpha + 1$, což je spor.

Poznámky:
Velmi příjemně mne překvapilo, že všechna došlá řešení byla až na drobnosti správně.

(Rado van Švarc)

Teorie grup II – Procitnutí symetrií

2. seriálová série Vzorové řešení

Úloha 1.

Kolika způsoby můžeme nabarvit krychli, máme-li k dispozici padesát odstínů šedi? Stěnu natřeme vždy celou stejným odstínem a použité odstíny nemusejí být různé; dvě obarvení, která se liší pouze natočením v prostoru, považujeme za totožná.

(Jakub Löwit)

Řešení:

Chceme použít Burnsideovo lemma, a proto nejdříve určíme grupu otočení krychle. Podíváme se na jednu stěnu. Tu je možné otočit na jakoukoliv jinou stěnu, tudíž zde máme 6 možností. Dále můžeme libovolně cyklicky otáčet pořadí vrcholů na této stěně, což nám dává 4 možnosti. Rozmysleme si, že tímto je konfigurace krychle již pevně daná. Celkově má hledaná grupa 24 prvků.

Nyní prvky grupy vyjmenujeme a spočteme počet zafixovaných obarvených krychlí.

- Identita: zde jsou všechny krychle zafixovány, tudíž počet pevných bodů je 50^6.
- Otočení o 90° nebo 270° kolem stěnové osy: stěny provrtané osou zůstávají na místě a ostatní čtyři se cyklicky otočí na sebe, tudíž počet pevných bodů je 50^3. (Máme volnost v obarvení obou provrtaných stěn, zbylé čtyři musejí mít všechny stejnou barvu.) Máme tři páry protilehlých stěn, a proto počet takových otočení je 6.
- Otočení o 180° kolem stěnové osy: stěny provrtané osou zůstávají na místě a ostatní čtyři se dělí na dvě dvojice, které se prohodí, tudíž počet pevných bodů je 50^4. Máme tři páry protilehlých stěn, a proto počet těchto otočení je 3.
- Otočení o 120° nebo 240° kolem tělesové osy: stěny se dělí na dvě trojice, které se cyklicky otočí na sebe, tudíž počet pevných bodů je 50^2. Máme čtyři páry protilehlých vrcholů, proto existuje 8 takových otočení.
- Otočení o 180° kolem osy procházející středem krychle a středem dvou hran: stěny se dělí na tři dvojice, které se otočí na sebe, tudíž počet pevných bodů je 50^3. Máme 6 párů protilehlých hran, a proto je počet těchto otočení 6.

Celkově jsme probrali 24 otočení, takže jsme vyčerpali celou grupu. Nyní stačí dosadit číselné hodnoty do vzorce Burnsideova lemmatu a dostaneme počet orbit, neboli počet obarvení krychle:

$$\frac{1}{24}(50^6 + 6 \cdot 50^3 + 3 \cdot 50^4 + 8 \cdot 50^2 + 6 \cdot 50^3) = 651\,886\,250.$$

Poznámky:

Jedná se o typickou úlohu na Burnsideovo lemma, a proto si s ní řešitelé, kteří správně pochopili seriál, hravě poradili. Bohužel častá chyba byla, že někteří jen vypsali všech 24 otočení a dál už neukázali, že další otočení už neexistují. Je potřeba na to dávat pozor, protože v Burnsideově lemmatu se musí pracovat s celou grupou uvažovaných symetrií. Za tuto chybu jsem strhl jeden bod.

(Tonda Le)

Úloha 2.

Ukažte, že pokud existuje nějaká funkce $f : \mathbb{Z}_n \to \mathbb{Z}_n$ splňující pro všechna $x \in \mathbb{Z}_n$ vztahy

(i) $f(x) \neq x$,
(ii) $f(f(x)) = x$,
(iii) $f(f(f(x+1)+1)+1) = x$,

potom n dává zbytek dva po dělení čtyřmi.

(Rado van Švarc)

Řešení:

Pokud $f(a) = f(b)$, pak $a = f(f(a)) = f(f(b)) = b$, tedy f je prostá. Dále je f na, protože pokud si pro libovolné x označíme $y = f(x)$, pak $f(y) = x$. Z toho plyne, že f je permutace.

Díky druhé podmínce umíme $\mathbb{Z}_n$ rozdělit na množiny tvaru $\{a, b\}$, kde $f(a) = b$ a $f(b) = a$. Díky první podmínce je každá taková množina dvoučlenná, proto je celkový počet prvků dělitelný dvěma, tedy $2 \mid n$.

Buď g permutace taková, že $g(x) = x + 1$ pro každé $x \in \mathbb{Z}_n$. Potom třetí podmínka říká, že permutace $h = f \circ g \circ f \circ g \circ f \circ g$ je identita.

Permutace g má jen jeden cyklus a ten je navíc sudé délky n, proto je $\operatorname{sign}(g) = -1$. Potom $\operatorname{sign}(h) = \operatorname{sign}(f)^3 \operatorname{sign}(g)^3 = -\operatorname{sign}(f)$. Protože h je identita (tedy se dá zapsat pomocí 0 transpozic), má znaménko 1. Tak dostáváme $\operatorname{sign}(f) = -1$. Protože f má $\frac{n}{2}$ cyklů délky 2, musí být $\frac{n}{2}$ liché. Z toho plyne $4 \nmid n$, což v kombinaci s $2 \mid n$ dává požadovaný výsledek.

Poznámky:

Všichni, kdo použili znaménko permutací, došli k řešení. Bez něj to bylo obtížnější a většině jiných řešení se nepovedlo dojít až do konce. *(Rado van Švarc)*

Úloha 3.

Nechť G je konečná grupa taková, že pro každou její vlastní podgrupu H (tj. $H \neq G$) existuje podgrupa K, která splňuje $H \leq K \leq G$ a má v G prvočíselný index. Označme jako p největší prvočíslo, které dělí $|G|$. Dále ať je P libovolná sylowovská p-podgrupa grupy G. Ukažte, že je P normální v G.

(Filip Bialas)

Řešení:

Označme k největší celé číslo takové, že p^k dělí řád G. Předpokládejme pro spor, že P není normální v G. Potom musí být normalizátor $N_G(P)$ vlastní podgrupou G, což znamená, že na něj můžeme volbou $H = N_G(P)$ aplikovat podmínku ze zadání a dostat podgrupu K, která obsahuje $N_G(P)$ a má prvočíselný index v G.

Jelikož K obsahuje $N_G(P)$ jako podgrupu, obsahuje jako podgrupu i P. Z Lagrangeovy věty tedy nutně $|P| = p^k$ dělí $|K|$. Pro konečné grupy platí $[G : K]|K| = |G|$, což znamená, že p nemůže dělit $[G : K]$. Tedy nutně $[G : K] = q$, kde q je prvočíslo menší než p.

Protože je P obsažena v K a $|K|$ je dělitelné stejně velkou mocninou p jako $|G|$, je P sylowovskou p-podgrupou i v K. Zřejmě $N_K(P) = K \cap N_G(P)$, ale protože $N_G(P) \leq K$, tak $N_K(P) = N_G(P)$. Index těchto normalizátorů v K, resp. v G, je roven počtu sylowovských p-podgrup v daných grupách, a ten dává vždy zbytek jedna po dělení p. Takže

$$[K : N_K(P)] = \frac{|K|}{|N_K(P)|} = \frac{|K|}{|N_G(P)|},$$

$$[G : N_G(P)] = \frac{|G|}{|N_G(P)|}$$

dávají zbytek jedna po dělení prvočíslem p. Nicméně platí

$$\frac{|G|}{|N_G(P)|} = \frac{|G|}{|K|}\frac{|K|}{|N_G(P)|} = [G:K][K:N_G(P)] = q[K:N_G(P)].$$

To ale není možné – pravá strana totiž dává zbytek q po dělení p (protože q je menší než p), zatímco levá strana dává zbytek jedna. Tím jsme dospěli ke kýženému sporu.

Poznámky:
Bez Sylowových vět odvozených v seriálu by tato úloha šla vyřešit opravdu těžko. Ve vzorovém řešení se použily snad všechny jejich výsledky. S jejich pomocí se ale několika řešitelům povedlo předvést kompletní důkaz. Všichni využili vlastnost grupy ze zadání pro H rovnou normalizátoru $N_G(P)$ a většina z nich postupovala dále jako ve vzorovém řešení. Trochu složitější, ale možná přirozenější postup zvolil *Matěj Doležálek*, který ukázal, že všechny sylowovské p-podgrupy grupy G musí ležet v K a z poslední rovnosti poté nemusel k odvození sporu vyšetřovat zbytky po dělení prvočíslem p. *(Filip Bialas)*

Milý příteli,

jsme rádi, že jsi otevřel(a) i poslední díl seriálu. Některé kapitolky sice opět nejsou nejlehčí, ale pokud jsi prošel (prošla) první dva díly, tak už by pro Tebe ten třetí měl být příjemným zážitkem. Oproti předchozím dílům však teď budeme mnohem víc pracovat s grafy, a to hlavně s těmi orientovanými. Pokud ses s nějakými grafy už někdy setkal(a), neměl by to být žádný problém. Pokud ne, nevadí – orientovaný graf jsou prostě jenom tečky a šipky mezi nimi. Pro rychlé seznámení s grafy případně doporučujeme třeba začátek PraSečího seriálu *Letem grafovým světem*.

A na co se tentokrát můžeš těšit? Kromě teoretických částí týkajících se abelovských grup a nově definovaných volných grup například i na způsoby, jak se opravdu (ne)vyplatí věšet obraz na zeď.

Příjemné chvilky při čtení přejí
Filip Bialas a Kuba Löwit

Teorie grup III – Svoboda pro grupy

All of mathematics is a tale about groups.

Henri Poincaré

Prolog III

Ve dvacátém století už teorie grup odpovídá na otázky napříč matematikou. Grupy se důkladně proplétají algebrou, geometrií, kombinatorikou i analýzou. Rychle se rozvíjejí další oblasti algebry, přičemž jedna z nejslavnějších matematiček Emmy Noetherová formuluje obecněji například věty o izomorfismu.

Je tu ale jedna poměrně palčivá otázka. Jaké všechny grupy vlastně existují (až na izomorfismus)? Jenže to je složité, protože nekonečné neabelovské grupy mohou být nesmírně pestré a komplikované. S nekonečny to ale bývalo složité vždycky, držme se tedy při zemi. Bylo by alespoň užitečné vědět, jak mohou vypadat všechny konečné grupy. Částečnou odpovědí by ale aspoň bylo určit všechny konečné grupy bez netriviálních normálních podgrup – konečné jednoduché grupy.

Po položení této „nevinné“ otázky následuje přes půl století práce a více než patnáct tisíc stran článků od více než sta lidí. Výsledkem je úplná *klasifikace všech konečných jednoduchých grup*, která obsahuje nekonečný počet grup několika typů a na závěr hromádku dvaceti šesti obrovských, divných a (alespoň ve světle toho, co je zatím známé) úplně náhodných grup v čele s takzvanou *Monster simple group*. Důkazu správnosti této klasifikace ale dnes do všech detailů na světě nikdo nerozumí.[11] V teorii grup stále existují neznámé věci. Určitě tedy nejsme na konci…

Abelovské grupy

Začněme starým vtipem.

„What is commutative and purple?“ „An abelian grape.“

V této části se budeme zabývat abelovskými grupami. Je konvencí používat při studiu čistě abelovských grup aditivní notaci a i my se jí budeme dále držet – grupa bude mít jednu binární operaci $+$, inverzní prvek k a je $-a$, neutrální prvek je 0. Několikanásobné sečtení budeme značit intuitivně $n \cdot a$, kde n je celé číslo a a je prvek grupy (záporné n znamená, že sčítáme prvky $-a$). Navíc značení kosetů je teď smysluplné ve tvaru $g + H$ místo gH a budeme ho takto používat. Připomeňme ještě, že když je grupa abelovská, tak je každá její podgrupa normální.

Naším cílem bude abelovské grupy klasifikovat – přesně popsat, jak všechny vypadají. Avšak abelovské grupy mohou být nekonečné a v matematice se nekonečné objekty často chovají dost jinak nebo složitěji, takže s takto obecným problémem si neporadíme. Na druhé straně, starat se pouze o konečné grupy by byla škoda – například bychom nemohli mluvit ani o celých číslech. Uděláme tedy takový kompromis a budeme se zajímat pouze o konečně generované abelovské grupy. (Tento předpoklad je pro další tvrzení nutný – neděláme ho jen proto, abychom si trochu zjednodušili práci.)

Definice. Grupa je *konečně generovaná*, pokud má nějakou konečnou množinu generátorů.

[11] A kvůli jeho délce se najdou dokonce tací, kteří mu nevěří.

Připomeňme si, že grupa má nějakou množinu generátorů, pokud každý prvek této grupy můžeme zapsat jako konečný součin (nebo teď v případě abelovských součet) generátorů nebo jejich inverzů. Toto je ekvivalentní podmínce, že každá podgrupa obsahující všechny generátory už musí být celá původní grupa.

Cvičení 1. Nechť G je abelovská grupa a X její podmnožina splňující $G = \langle X \rangle$. Potom každý prvek $g \in G$ můžeme zapsat ve tvaru $a_1 \cdot x_1 + a_2 \cdot x_2 + \cdots + a_n \cdot x_n$, kde a_i jsou celá čísla a x_i po dvou různé prvky X.[12]

Cvičení 2. Pro každé přirozené číslo n je $\mathbb{Z}^n$ konečně generovaná.

Cvičení 3. Abelovská grupa racionálních čísel se sčítáním $\mathbb{Q}$ není konečně generovaná.

Tvrzení. *Abelovská grupa G je konečně generovaná s maximálně n-prvkovou množinou generátorů právě tehdy, když je izomorfní $\mathbb{Z}^n/H$, kde H je některá podgrupa $\mathbb{Z}^n$.*

Důkaz. Grupa $\mathbb{Z}^n/H$ je generovaná maximálně n-prvkovou množinou kosetů

$$\{(1,0,\ldots,0)+H, (0,1,\ldots,0)+H, \ldots, (0,\ldots,0,1)+H\},$$

protože každý prvek grupy $\mathbb{Z}^n$ je generovaný množinou prvků s jedničkami v jedné souřadnici a nulami ve zbytku. Druhá implikace je jen o trošičku těžší:

Generátory označme postupně $x_1, \ldots, x_n$. Uvažujme zobrazení $\varphi : \mathbb{Z}^n \to G$ definované vztahem $\varphi((a_1, a_2, \ldots, a_n)) = a_1 \cdot x_1 + a_2 \cdot x_2 + \cdots + a_n \cdot x_n$. Lehce se dá ověřit, že je toto zobrazení homomorfismem (ale využíváme přitom komutativitu sčítací operace).

Protože $x_1, \ldots, x_n$ jsou generátory, lze každé $g \in G$ vyjádřit ve tvaru $a_1 \cdot x_1 + \cdots + a_n \cdot x_n$; proto $\operatorname{Im} \varphi = G$. Jádro φ označme H. Podle první věty o izomorfismu máme $\mathbb{Z}^n / \operatorname{Ker} \varphi \simeq \operatorname{Im} \varphi$, což můžeme přepsat jako $\mathbb{Z}^n/H \simeq G$, a to jsme chtěli přesně dokázat.

Právě dokázané tvrzení nám říká, že každá konečně generovaná abelovská grupa je faktorgrupou $\mathbb{Z}^n$. Tuto skutečnost budeme potřebovat k důkazu následující věty:

Věta. (Klasifikace konečně generovaných abelovských grup) *Každá konečně generovaná abelovská grupa je izomorfní direktnímu součinu konečně mnoha cyklických grup.*

Tato věta říká, že struktura konečně generovaných abelovských grup je vlastně hrozně jednoduchá. Jedná se o direktní součin cyklických grup, takže každý prvek lze popsat pomocí n-tice prvků ležících v těchto cyklických grupách. Každá konečná cyklická grupa je navíc izomorfní $\mathbb{Z}_n$ pro nějaké n a každá nekonečná je izomorfní $\mathbb{Z}$. Triviální abelovskou grupu $\{e\}$ můžeme v jistém smyslu vnímat jako součin nulového počtu cyklických grup, ale to je stejně tak nanicovatý případ, že se v důkaze jistě stačí omezit na grupy obsahující alespoň dva prvky.

Hledaný direktní součin samozřejmě nebude jednoznačný. Už v minulém díle jsme si v kapitole Čínská zbytková věta ukazovali, že pro nesoudělná p, q platí $\mathbb{Z}_{pq} \simeq \mathbb{Z}_p \times \mathbb{Z}_q$. Díky tomuto tvrzení bychom po důkazu zmiňované věty mohli tvrdit i to, že každá konečně generovaná abelovská grupa je izomorfní direktnímu součinu konečně mnoha cyklických grup, z nichž každá má řád buď nekonečný, nebo rovný mocnině nějakého prvočísla. (Každou, která nemá řád mocniny prvočísla, můžeme totiž izomorfně rozdělit na direktní součin těch, které takový řád mají.)

Důkaz. Jak jsme již ukázali, každá konečně generovaná abelovská grupa je izomorfní $\mathbb{Z}^n/H$, kde $H \leq \mathbb{Z}^n$, pro nějaké přirozené n. Stačí nám tedy dokázat, že pro $H \trianglelefteq \mathbb{Z}^n$ je $\mathbb{Z}^n/H$ izomorfní direktnímu součinu konečně mnoha cyklických grup. Důkaz provedeme indukcí podle tohoto n.

Pro $n = 1$ si stačí uvědomit, jak vypadají všechny podgrupy grupy $\mathbb{Z}$. Pokud bude $H = \{0\}$, tak $\mathbb{Z}/H \simeq \mathbb{Z}$ je cyklická (a tedy direktní součin jedné cyklické grupy). Uvažujme tudíž případ, kdy H není triviální. Z nenulových celých čísel z H vyberme to, jehož absolutní hodnota je nejmenší. Označme toto číslo a. Pak jistě i $-a \in H$, takže také $|a| \in H$. Protože se jedná o grupu, musí navíc

[12] Ovšem pozor, je-li X nekonečná, nejsou prvky $x_1, \ldots, x_n$ určeny pevně, nýbrž závisejí na tom, který prvek g právě vyjadřujeme.

do H patřit i každé $k \cdot a$ pro $k \in \mathbb{Z}$. Předpokládejme pro spor, že se v H nachází i nějaké další číslo b. Pak zbytek čísla b po vydělení $|a|$ je roven přirozenému číslu většímu než nula a menšímu než $|a|$. Toto číslo navíc dokážeme zapsat jako $b - k \cdot |a|$ pro nějaké $k \in \mathbb{Z}$, takže patří do H. To je ale ve sporu s minimalitou $|a|$. Proto $H = \{k \cdot a \mid k \in \mathbb{Z}\}$. Tím pádem přímo z definice plyne $\mathbb{Z}/H \simeq \mathbb{Z}_{|a|}$, což je cyklická grupa.

Případ pro $n = 1$ jsme vlastně ani nemuseli řešit zvlášť, jak bude vidno z indukčního kroku. Nicméně to byl jednoduchý příklad principu, který budeme používat dále. V minulém odstavci jsme ukázali, že podgrupa H je generována jen jedním prvkem a, a to pomocí snahy minimalizovat jeho velikost. V obecném případě uděláme něco podobného, jen budeme o nalezení takového „áčka“ usilovat jen v jedné souřadnici.

Mějme nyní konečně generovanou abelovskou grupu G, která je izomorfní $\mathbb{Z}^n/H$, kde n je nějaké pevné přirozené číslo větší než jedna. Pokud je podgrupa $H = \{e\}$, tak máme $\mathbb{Z}^n/H \simeq \mathbb{Z}^n$. Vyšetřovaná grupa je tedy direktním součinem n cyklických grup.

V opačném případě má grupa H alespoň jeden nenulový prvek. Každý prvek $h \in H$ můžeme psát jako $h = (h_1, \dots, h_n)$. Pro $H \le \mathbb{Z}^n$ označme symbolem $m(H)$ minimální nenulovou absolutní hodnotu h_i, která se vyskytuje v některém prvku $h \in H$ (tj. „nejmenší kladné číslo, které se kdekoli v celé grupě H vyskytuje“). Z těch H, pro něž $G \simeq \mathbb{Z}^n/H$, vyberme takovou H, aby výraz $m(H)$ byl nejmenší možný. Z této pevné grupy H nyní vezmeme prvek a, v němž pro některé i platí $a_i = m(H)$. Bez újmy na obecnosti můžeme popřeházet souřadnice, takže dále předpokládejme, že $i = 1$.

Nyní pro všechna $h \in H$ musí nutně platit $a_1 \mid h_1$, neboť jinak bychom mohli obdobně jako v případě $n = 1$ vydělit tato dvě čísla se zbytkem a dostat prvek grupy H, který bude mít první souřadnici nenulovou a v absolutní hodnotě menší než a_1.

Podobně ukážeme, že můžeme zvolit generující množinu X grupy H takovou, že $a \in X$ a pro všechna ostatní $x \in X$ platí $x_1 = 0$. Pro každé $h \in H$ různé od a dejme do X prvek $h' = h - \frac{h_1}{a_1} \cdot a$. Když do X nakonec přihodíme i a, dostáváme (obrovskou) generující množinu, protože každý prvek $h \in H$ jde nagenerovat jako součet h' a konečně mnoha a nebo $-a$.

Nyní provedeme opravdový trik. Naším cílem bude nějakým způsobem zařídit, aby se a rovnalo $(a_1, 0, \dots, 0)$. Nejdříve sporem ukážeme, že naše volba H zajišťuje, aby $a_1 \mid a_i$ pro všechna $2 \le i \le n$. Pokud by tomu tak pro nějaké i nebylo, mohli bychom dělit se zbytkem a psát $a_i = qa_1 + r$. Jak nyní dojdeme ke sporu? Vezmeme jinou množinu generátorů! Uvažme zobrazení φ, které jde ze $\mathbb{Z}^n$ do $\mathbb{Z}^n$ a prvku $(g_1, \dots, g_{i-1}, g_i, g_{i+1}, \dots, g_n)$ přiřadí $(g_1, \dots, g_{i-1}, g_i - qg_1, g_{i+1}, \dots, g_n)$. Ukážeme, že je φ automorfismus. To, že se jedná o homomorfismus, by se ověřilo úplně snadno. Navíc snadno zjistíme, že $\chi : \mathbb{Z}^n \to \mathbb{Z}^n$, které prvku $(g_1, \dots, g_{i-1}, g_i, g_{i+1}, \dots, g_n)$ přiřadí $(g_1, \dots, g_{i-1}, g_i + qg_1, g_{i+1}, \dots, g_n)$, je k zobrazení φ inverzní, takže φ musí být prosté i na. Ukázali jsme, že je φ opravdu automorfismus $\mathbb{Z}^n$.

Navíc φ zobrazí generující množinu X na množinu X', ve které se vyskytuje prvek $(a_1, \dots, a_{i-1}, r, a_{i+1}, \dots, a_n)$. Zřejmě také $\varphi(\langle X \rangle) = \langle X' \rangle$, a tedy i $\mathbb{Z}^n/H = \mathbb{Z}^n/\langle X \rangle \simeq \varphi(\mathbb{Z}^n)/\varphi(\langle X \rangle) = \mathbb{Z}^n/\langle X' \rangle$. Oboje platí díky tomu, že automorfismus úplně zachovává strukturu grup. Ale tímto se dostáváme do sporu s volbou grupy H jako takovou, protože $a_1 = m(H)$ mělo být nejmenší možné, jenže $r \ge m(\langle X' \rangle)$ je ještě menší.

Podobně jako při důkazu existence X, v níž je první složka nenulová pouze u prvku a, nyní ukážeme, že můžeme předpokládat, že máme X, v níž je a navíc nulový ve všech ostatních složkách. Už víme, že můžeme brát X tak, aby v prvku a platilo $a_1 \mid a_i$ pro všechna $2 \le i \le n$. Uvažme nyní zobrazení ψ, které prvku $(g_1, g_2, \dots, g_n) \in \mathbb{Z}^n$ přiřadí prvek $(g_1, g_2 - \frac{a_2}{a_1} \cdot a_1, \dots, g_n - \frac{a_n}{a_1} \cdot a_1)$. Důkaz, že je ψ automorfismus $\mathbb{Z}^n$, je obdobný jako u φ. Navíc zobrazí prvek a na $(a_1, 0, \dots, 0)$ a ostatní prvky z X na prvky, které mají první složku pořád nulovou. Existuje tedy grupa $\tilde{H} = \langle \tilde{X} \rangle$, pro niž $\mathbb{Z}^n/H \simeq \mathbb{Z}^n/\tilde{H}$ a jejíž množina generátorů je ve tvaru $\tilde{X} = \{(a_1, 0, \dots, 0)\} \cup Y$, kde Y obsahuje pouze prvky, které mají nulovou první složku. Ve zbytku důkazu budeme bez újmy na obecnosti předpokládat, že jsme tuto šikovnou grupu H zvolili již na začátku, takže už nebudeme psát vlnky nad H a X.[13]

Již jsme skoro u konce. Ukážeme, že $\mathbb{Z}^n/\langle X\rangle \simeq \mathbb{Z}/\langle a_1\rangle \times \mathbb{Z}^{n-1}/\langle Y'\rangle$, kde Y' je množina, která obsahuje prvky z Y bez první složky. Chceme tedy $\mathbb{Z}^n/H \simeq \mathbb{Z}_{|a_1|} \times \mathbb{Z}^{n-1}/\langle Y'\rangle$, přičemž poslední grupa je z indukčního předpokladu direktním součinem cyklických grup a budeme ji nadále značit A. K důkazu tohoto izomorfismu nám stačí uvážit zobrazení $\Phi : \mathbb{Z}^n \to \mathbb{Z}_{|a_1|} \times A$, které prvku $(g_1, \dots, g_n)$ přiřadí prvek $(g_1 + \langle a_1\rangle, (g_2, \dots, g_n) + \langle Y'\rangle)$.

To, že je Φ homomorfismus, by se zase ověřilo snadno. Navíc je na, protože na prvek $(g_1 + \langle a_1\rangle, (g_2, \dots, g_n) + \langle Y'\rangle)$ se zobrazí $(g_1, g_2, \dots, g_n)$. Stačí nám již jen ukázat, že $\operatorname{Ker}\Phi = H$. Prvky $g = (g_1, \dots, g_n) \in \mathbb{Z}^n$, které se zobrazí na nulu, musejí mít v první složce násobek a_1 a ve zbytku složek nějaký konečný součet prvků z Y nebo jejich inverzů. Ale pak musí být $g \in H$, neboť $H = \langle X\rangle = \langle\{(a_1, 0, \dots, 0)\} \cup Y\rangle$. A naopak je také jasné, že se všechny prvky z H zobrazí na nulu. Tím pádem je skutečně $\operatorname{Ker}\Phi = H$ a z první věty o izomorfismu dostáváme kýžený izomorfismus $\mathbb{Z}^n/H \simeq \mathbb{Z}_{|a_1|} \times A$, čímž jsme s důkazem hotovi.

Důkaz byl trochu delší, ale výsledek je skvělý. Neumíme sice klasifikovat úplně všechny abelovské grupy, ale třeba ty konečné máme zvládnuté dokonale. Pokud chceme znát všechny abelovské grupy nějakého pevného řádu, tak nám stačí podívat se na prvočíselný rozklad tohoto řádu a vyzkoušet několik možností.

Cayleygrafy

V předchozích částech seriálu nás už grupy mnohokrát přesvědčily o tom, že jsou symetriemi rozličných objektů. Představme si proto ještě jeden druh objektu, jehož symetrie jsou překvapivě bohaté. Přesněji, budeme se zabývat některými orientovanými grafy. Pojďme se tedy domluvit na několika pojmech.

Úmluva. *Orientovaným grafem* $Q = (V, E)$ myslíme množinu *vrcholů* V společně s množinou orientovaných hran E, jimž někdy budeme říkat *šipky*[14]. Je-li C množina barev, *barevným orientovaným grafem* nazveme orientovaný graf Q, jehož každá hrana má právě jednu barvu z C.

Po celou dobu přitom povolujeme i nekonečné grafy, práce s nimi však v rámci seriálu nebude skrývat žádné velké nástrahy.

Nyní si definujme takzvané *Cayleyho grafy*, zkráceně *cayleygrafy*.

Definice. Ať G je grupa a C nějaká množina jejích generátorů. *Cayleygrafem grupy G* vzhledem k C nazveme orientovaný barevný graf Q, jehož vrcholy odpovídají prvkům G a z vrcholu u vede do vrcholu v hrana barvy c právě tehdy, když $v = cu$.

Ano, na prvky množiny C se díváme zároveň jako na generátory grupy G i jako na barvy, a vůbec nám to nevadí – právě naopak. Přechod po šipce barvy c v grafu odpovídá násobení generátorem c.

Definice. Ať C je nějaká množina barev. *Zajímavým* grafem nazveme jakýkoli barevný orientovaný graf $G = (V, E)$, který splňuje následující tři axiomy:

(1) mezi každými dvěma vrcholy grafu G vede (ne nutně orientovaná) cesta (*souvislost*),
(2) do každého vrcholu i ven z něho vede právě jedna hrana od každé barvy (*regularita*),
(3) pro každé dva vrcholy $u, v \in V$ existuje nějaká permutace vrcholů, která zobrazuje $u \mapsto v$ a přitom zachovává barevné šipky (*homogenita*).

[13] Komu tento přístup vadí, může si buď vlnky všude doplnit, nebo si představovat, že jsme na začátku jednak požadovali, aby bylo co nejmenší $m(H)$, jednak to, aby v prvku a byl co nejmenší součet absolutních hodnot v ostatních souřadnicích.

[14] Povolujeme i násobné hrany a hrany se stejným začátkem a koncem. Druhé uvedené se běžně nazývají „smyčky“, my však tento výraz máme rezervovaný pro něco jiného – budeme je proto označovat jako *očka*. Předem však prozradíme, že pro nás v této pasáži nijak zajímavé nebudou a klidně bychom je mohli i zakázat.

Ještě by se slušelo trochu osvětlit třetí z podmínek. Říkáme, že permutace $\sigma \in S_V$ *zachovává barevné šipky*, jestliže z vrcholu x vede hrana barvy c do vrcholu y právě tehdy, když z vrcholu $\sigma(x)$ vede hrana barvy c do vrcholu $\sigma(y)$. Homogenita vyjadřuje, že pokud nás někdo postaví do libovolného vrcholu u grafu G, chozením barevnými cestičkami nemáme šanci určit, do kterého vrcholu jsme byli postaveni.

Proč by nás ale měly zrovna zajímavé grafy zajímat?

Tvrzení. *Každý cayleygraf je zajímavý, každý zajímavý graf je cayleygrafem nějaké grupy.*

Důkaz. Nejprve ukažme, že každý cayleygraf je zajímavý. Ať tedy Q je cayleygraf grupy G. Pokud se podíváme na vrchol odpovídající prvku $e \in G$, můžeme z něj postupným násobením zprava prvky z generující množiny C a jejich inverzy získat libovolný prvek $g \in G$. Proto z vrcholu e vede cesta do vrcholu g; nalezneme ji tak, že budeme postupně zprava číst součin odpovídající prvku g, za generátor c se posuneme ve směru hrany c, za jeho inverz v protisměru. Každé dva vrcholy Q jsou proto spojeny přes vrchol e, tedy Q je souvislý.

Podívejme se na to, jak na sobě G působí levou translací; toto působení označme α. Speciálně sledujme α_c pro nějaké $c \in C$. Šipky barvy c v cayleygrafu Q přesně odpovídají permutaci α_c. Protože je α_c bijekce, je Q regulární. Elementárněji řečeno, z daného vrcholu u vede právě jedna šipka barvy c, a to do vrcholu cu; do daného vrcholu u vede právě jedna šipka barvy c, a to z vrcholu $c^{-1}u$, .

Konečně, ať u, v jsou nějaké vrcholy Q. Vezměme si permutaci vrcholů, která je daná násobením prvkem $u^{-1}v$ zprava (tj. jedná se o působení **pravou** translací). Ta posílá $u \mapsto uu^{-1}v = v$. Navíc tato permutace zachovává barevné šipky: v cayleygrafu Q vede z vrcholu g do vrcholu h šipka barvy c právě tehdy, když $h = cg$, což po vynásobení prvkem vu^{-1} zprava dává ekvivalentní rovnost $hvu^{-1} = cgvu^{-1}$. Z vrcholu gvu^{-1} tedy vede hrana barvy c do vrcholu hvu^{-1}, čímž jsme ověřili homogenitu.

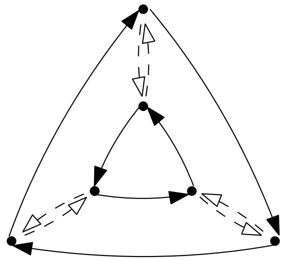
Nyní ukážeme druhý směr tvrzení: k libovolnému zajímavému grafu Q vyrobíme grupu G tak, aby Q byl její cayleygraf. Za grupu G vezměme jednoduše grupu všech symetrií grafu Q – tedy grupu všech permutací jeho vrcholů, které zachovávají směry i barvy šipek. Jak tato G vypadá? Zvolme libovolný vrchol grafu Q a označme jej e. Každá symetrie grafu Q posílá e na nějaký vrchol Q. Díky homogenitě však pro každý vrchol v skutečně existuje symetrie převádějící $e \mapsto v$.

Souvislost a regularita Q však zaručují, že taková symetrie existuje nejvýše jedna: Do libovolného vrcholu w se dá dojít po hranách z vrcholu e. Protože však naše symetrie zachovává barvy i orientace hran, do obrazu v musíme z vrcholu v dojít jednoznačně určenou cestou po stejných barvičkách. Tím jsme spárovali vrcholy Q s jednotlivými symetriemi z G. Symetrie odpovídající posunutí e do vedlejšího vrcholu ve směru nějaké šipky jsou přesně naznačeny šipkami odpovídající barvy. Vezmeme-li tedy těchto $|C|$ symetrií za generátory G, zkonstruováním příslušného cayleygrafu dostaneme nazpátek graf Q. To je vše.

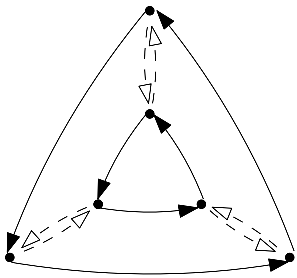
Pojem zajímavého grafu jsme zavedli jen proto, aby bylo v předchozí diskuzi jasně rozlišeno, kdy konstruujeme grupu z grafu a kdy naopak graf z grupy. Protože jsme ale právě nahlédli, že třída zajímavých grafů přesně odpovídá třídě cayleygrafů všech možných grup, budeme dále místo pojmu zajímavý graf používat pojem cayleygraf.

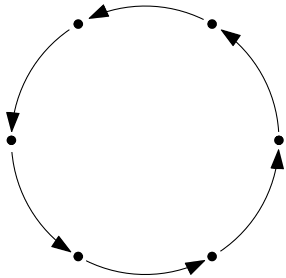
Zdůrazněme jednu skvělou věc, kterou jsme mimoděk dokázali. Povedlo se nám totiž ukázat, že libovolná grupa G je izomorfní grupě symetrií svého cayleygrafu. Takový cayleygraf tedy dokonale vystihuje svou grupu. Získáváme tak nový způsob, jak si grupy představovat. Jednu grupu tak můžeme znázornit mnoha velmi rozdílnými grafy – stačí volit různé množiny jejích generátorů. Tyto grafy sice musejí mít vždy stejný počet vrcholů (který odpovídá řádu grupy), šipky v nich ale mohou vypadat velmi odlišně.

Příklad. Grupa $D_6 \simeq S_3$ s množinou generátorů tvořenou minimální rotací r a translací σ má následující cayleygraf se šesti vrcholy:



Příklad. Abelovská grupa $\mathbb{Z}_6$ má také šest prvků. První z následujících cayleygrafů odpovídá jednoprvkové množině generátorů obsahující pouze číslo 1. Druhý odpovídá volbě dvojice generátorů 2, 3.





V cayleygrafech je na první pohled vidět mnoho algebraických vlastností příslušné grupy. Třeba abelovskost grupy G je ekvivalentní následující podmínce: Kdykoli vezmeme dvě barvy c, d a libovolný vrchol v, cesty z v po barvách cd a dc skončí ve stejném vrcholu. K abelovskosti G totiž zřejmě stačí, aby spolu komutovaly všechny generátory grupy G.

Mějme například grupy $H \leq G$ a vhodně zvolené množiny jejich generátorů po řadě C', C takové, aby $C' \subseteq C$. Vezměme si příslušný cayleygraf grupy G. Pokud z něj smažeme všechny hrany s barvami z $C \setminus C'$, rozpadne se na nějaké menší grafy. Nějaký vrchol grafu Q přitom reprezentoval identitu $e \in G$. Komponenta obsahující tento vrchol vzniklá smazáním hran s barvami z $C \setminus C'$ je pak zřejmě cayleygrafem grupy H. Jenže díky homogenitě grafu Q mohlo být e libovolným vrcholem Q. Graf se tedy rozpadl na menší cayleygrafy odpovídající kopím cayleygrafu grupy H, které přesně odpovídají pravým kosetům podgrupy H v G.

Podobně je velmi snadné poznat, kdy je $H \trianglelefteq G$. To nastává právě tehdy, když pravé a levé kosety H v G splývají. Není těžké si rozmyslet, že to přesně odpovídá případu, kdy akce G levou translací na sobě samé permutuje pravé kosety podgrupy H, což stačí ověřit pro generátory G. A to se stane přesně tehdy, když všechny šipky každé barvy z $C \setminus C'$ vedou z každého cayleygrafu grupy H do právě jednoho jiného. Když se pak podíváme na kopie cayleygrafu grupy H jako na vrcholy a necháme v grafu šipky s barvami z $C \setminus C'$, dostaneme cayleygraf faktorgrupy G/H.

Právě uvedené „obrázkové“ vlastnosti grup si můžete hezky rozmyslet na dvou cayleygrafech znázorněných výše. Při vhodné volbě generátorů je vidět, že se liší pouze vzájemnou orientací trojcyklů. Pro jejich vlastnosti to však má velké důsledky: $\mathbb{Z}_6$ je abelovská, zatímco S_3 ani omylem, $\mathbb{Z}_6$ má normální podgrupy řádu 3 i 2, zatímco S_3 má jedinou normální podgrupu řádu 3 atd.

Jak vyrobit… volné grupy!

Když jsme se v předešlých dílech seriálu zabývali nějakou konkrétní grupou, typicky v ní platilo hodně „bonusových rovností“ mezi prvky, které abstraktní definice grupy nijak nevynucuje. (Například spolu některé prvky mohly komutovat, některý prvek mohl splňovat $g^3 = e$, pro trojici generátorů g_1, g_2, g_3 mohlo platit $g_1^7 g_2^{-3} g_3^{-1} g_2^2 = e$ apod.) Nyní se pokusíme o výrobu úplného protikladu – zkonstruujeme grupy, ve kterých žádné vztahy „navíc“ neplatí. Tyto prototypy grup se nazývají *volné grupy*.

Předem vyslovíme drobné varování: s volnými grupami budeme pracovat poměrně formálně a opatrně. To se na první pohled může zdát až přehnané, některá tvrzení o volných grupách (jako třeba jejich samotná existence) se mohou zdát úplně zjevná. Čím víc toho ale o nich zjistíme, tím méně zjevná se nám budou zdát. Některá jiná zřejmá tvrzení o volných grupách ve skutečnosti ani neplatí – opatrnost je proto na místě.

Konstrukce. (krácením slov)

Mějme tedy neprázdnou (klidně i nekonečnou) množinu X, jejíž prvky budou jakási *písmena*. Tato písmena budou představovat generátory naší volné grupy F. Pokud má být F grupa, každý její prvek musí mít inverz. Vezměme si tedy novou množinu stejně velkou jako X, kterou příhodně označíme X^{-1}. Množina X^{-1} obsahuje pro každé písmeno $x \in X$ jednoznačně určené inverzní písmeno, které budeme příhodně značit x^{-1}. Žádné další prvky v X^{-1} neleží.

Nyní pomocí disjunktních X a X^{-1} vyrobíme množinu W, která sestává ze všech konečných řetězců symbolů z $X \cup X^{-1}$. Prvkům W budeme říkat *slova*. Speciálně W obsahuje i prázdné slovo, které budeme značit e.[15] Zdůrazněme, že na W zatím neexistují žádné grupové operace.

Naším snem je, aby W byla nosnou množinou grupy F. Jako binární operace se doslova nabízí takzvané *zřetězení* – psaní slov za sebe. Zřetězení je na množině W určitě asociativní, prázdné slovo e se navíc chová jako identita. Je tu ale malý zádrhel ohledně invertování – napsáním dvou slov za sebe nelze žádné z nich zkrátit. Chtěli bychom, aby slovo $abcc^{-1}b^{-1}a^{-1}$ bylo ve skutečnosti prázdné slovo, z pohledu množiny W jsou to ale dva různé prvky.

Jinými slovy, má-li přiřazení $x \mapsto x^{-1}$ odpovídat invertování prvků písmen z X, samy axiomy grupy už vynucují rovnosti některých slov. Například slova $abaa^{-1}$, ab, $b^{-1}bab$ musejí reprezentovat stejný prvek grupy F. Očividným řešením této těžkosti je takové prvky za stejné skutečně považovat. Formálněji, dva prvky $u, v \in W$ budeme považovat za stejné, pokud je na sebe lze převést postupným vepisováním resp. mazáním sousedících písmen xx^{-1} resp. $x^{-1}x$ pro libovolné $x \in X$. Na množině W' takových skupinek bychom pak rádi definovali grupové operace stejně jako původně, což už opravdu jde.

A proč že to jde? Skutečně totiž není jasné, jestli výsledek zřetězení náhodou nezávisí na volbě konkrétní slovní reprezentace. Stačilo by ukázat, že každý prvek W' lze reprezentovat jednoznačně určeným *zkráceným* slovem, tj. slovem, které neobsahuje žádnou sousedící dvojičku písmen tvaru xx^{-1} resp. $x^{-1}x$. To ponecháme jako hravé cvičení.

Cvičení 4. Dokažte, že každý prvek W' lze reprezentovat jednoznačně určeným zkráceným slovem.

Za nosnou množinu grupy F tudíž můžeme jednoduše vzít množinu všech takových zkrácených slov a binární operací pak bude zřetězení s případným promazáním sousedících dvojiček xx^{-1} resp. $x^{-1}x$. Prázdné slovo e je potom skutečně identitou, invertování prvků X přiřazením $x \mapsto x^{-1}$ lze roztáhnout na všechny prvky F pomocí předpisu $(ab)^{-1} = b^{-1}a^{-1}$. Asociativita teď úplně jasná není, důkladným rozborem několika možností by ji však nebyl problém dokázat.

Podle potřeby někdy budeme vnímat volnou grupu jako „grupu všech zkrácených slov“, jindy se na ni formálně budeme dívat jako na „grupu sestávající ze skupinek ekvivalentních slov“. Dle právě provedeného rozboru to ale vyjde nastejno.

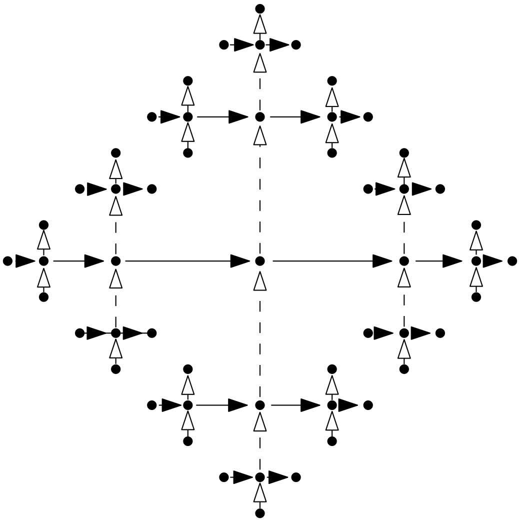
Přestože je volná grupa sama o sobě docela intuitivní objekt, její vyrábění skýtalo několik záludností.[16] Ještě než se posuneme dál, předvedeme si alternativní konstrukci volných grup, a to pomocí cayleygrafů. Tato konstrukce je méně přímočará, zato je však neuvěřitelně elegantní. Následujícímu postupu se někdy (podle jeho tvůrce) přezdívá *van der Waerdenův trik*.

Konstrukce. (van der Waerdenův trik)

[15] Nejlepší by bylo značit ji prázdný místem, to je ale typicky špatně vidět.

[16] Kombinatorický rozbor asociativity jsme z lenosti a hlavně pro úsporu místa ani neprovedli.

Opět začneme s množinou X. Sestrojíme nekonečný cayleygraf Q jako na obrázku: Bude to nekonečný strom[17], z každého jeho vrcholu bude vycházet po jedné šipce od každé barvy z množiny X. Do každého vrcholu také bude vcházet jedna šipka každé barvy. Přesněji, začneme jedním vrcholem, nakreslíme všech $2|X|$ jeho šipek, na konec každé dáme nový vrchol… a tak budeme pokračovat dál. Žádná nově vytvořená šipka nevede do už vytvořeného vrcholu – strom se neustále rozrůstá do dalších a dalších pater.



Je vcelku zřejmé, že Q je cayleygraf (největší rozmýšlení vyžaduje homogenita). Označme tedy F jeho grupu symetrií. Okamžitě víme, že F je skutečně dobře definovaná grupa a její binární operace je skládání symetrií grafu Q. Zvolme si libovolný vrchol e grafu Q. Každá symetrie Q jednoznačně odpovídá posunutí e do některého vrcholu v. V grafu Q jsou však každé dva vrcholy spojeny jednoznačně určenou posloupností hran. Každou symetrii $g \in F$ tedy můžeme ztotožnit s touto jednoznačně určenou posloupností hran z e do v, kterou lze popsat jednoznačně určeným slovem z písmen $X \cup X^{-1}$ (písmena odpovídají barvám na zmíněné posloupnosti hran, exponenty jejich směru). To je vše.[18]

Na závěr si ještě uvedeme několik příkladů volných grup. Obecně budeme volnou grupu na písmenech z množiny X značit jako F_X. Pro n-prvkovou množinu X budeme někdy příslušnou volnou grupu značit jako F_n.[19]

Příklad. Zvolme jednoprvkovou bázi X, její jediný prvek označme a. Jak pak vypadá odpovídající volná grupa F_1? Množina W všech konečných slov nad $X \cup X^{-1}$ obsahuje pouze konečné posloupnosti písmen a, a^{-1}. Nosná množina grupy F_1 pak odpovídá zkráceným slovům z W. Zkrácená slova ale nutně obsahují nejvýše jeden ze symbolů a, a^{-1}. Označíme-li napsání písmene a přesně k-krát za sebe jako a^k, napsání písmene a^{-1} přesně k-krát za sebe jako a^{-k} a prázdné slovo jako a^0, sestává nosná množina grupy F právě ze slov tvaru a^k pro $k \in \mathbb{Z}$. Okamžitě tedy vidíme,

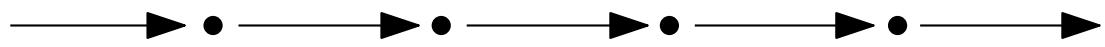
[17] *Stromem* myslíme graf, který neobsahuje žádnou – ani neorientovanou – kružnici.

[18] Nedůvěřivý čtenář si snadno může zkontrolovat, že jsme zkonstruovali tu stejnou grupu F jako původně.

[19] Pro stejně velké množiny generátorů nám výše uvedená konstrukce samozřejmě vyrobí izomorfní grupy. Volné grupy na stejně velkých množinách písmen tedy můžeme považovat v podstatě za stejné.

že volná grupa F na jednom generátoru je izomorfní nekonečné cyklické grupě $\mathbb{Z}$ (skrz izomorfismus $a^k \mapsto k$).

Cayleygraf této grupy představuje pouze nekonečná orientovaná cesta:



Jak už jsme nastínili dříve, pro bázi s velikostí alespoň dva je situace o poznání zajímavější.

Příklad. Vezměme dvouprvkovou bázi $X = \{a, b\}$ a uvažme příslušnou volnou grupu F_2. Na její nosnou množinu se můžeme dívat jako na množinu všech zkrácených slov nad písmeny a, b, a^{-1}, b^{-1}. Taková slova už ale na rozdíl od minulého příkladu nijak lépe popsat neumíme. Když budeme provádět jejich zřetězení, může docházet k dosti nepřehlednému krácení písmen. Zkoumání struktury F_2 už tedy může být poměrně zajímavé. Její cayleygraf je zvěčněn na obrázku uprostřed konstrukce volných grup.

Popis grupy F_2 zakončíme několika cvičeními, ze kterých by mělo být patrné, s jakou opatrností je potřeba k volným grupám přistupovat.

Cvičení 5. Grupa F_2 je zřejmě generována dvěma prvky. Zdůvodněte, že jeden generátor nestačí.

Naopak ale platí následující mírně překvapivé lumpárny.

Cvičení 6. Najděte vlastní podgrupu $H < F_2$ takovou, že $H \simeq F_2$.

Úloha 1. Najděte podgrupu $H \leq F_2$ takovou, že $H \simeq F_3$.

Úloha 2. Ukažte, že existuje podgrupa $K \leq F_2$, která je izomorfní F_X pro nějakou nekonečnou množinu X.

Důkazy předchozích dvou úloh bylo možné provést bez použití nějaké hlubší teorie. My se naštěstí v průběhu seriálu naučíme mnohem sofistikovanější finty, pomocí kterých budou tvrzení podobného rázu mnohem jasnější.

Grupa F_2 tedy obsahuje podgrupy, které jsou volné s bází velikosti n pro libovolné $n \in \mathbb{N}$, a dokonce i takové, jejichž báze svou velikostí odpovídá množině přirozených čísel. Jenže všechny tyto její podgrupy opět obsahují podgrupu izomorfní s F_2 ... legrační, ne?

Volné grupy zbavené pout

Když už jsme si dali tolik práce s výrobou volných grup, bylo by vhodné je chvíli obecně zkoumat. V předešlé části jsme je konstruovali velmi konkrétně (z dané množiny X jsme vyrobili příslušnou volnou grupu). Volné grupy však lze ekvivalentně definovat následujícím mnohem abstraktnějším způsobem.

Tvrzení. (univerzální vlastnost volných grup) *Grupa F je volná právě tehdy, když existuje podmnožina $X \subseteq F$ taková, že pro každou grupu H a každé zobrazení $f : X \to H$ existuje právě jeden homomorfismus $\varphi : F \to H$, který se na prvcích X shoduje s f. (Podmnožina X se pak nazývá volná báze).*

Důkaz. Nejprve dokážeme, že libovolná volná grupa zkonstruovaná v předešlé části splňuje podmínku z tvrzení. Ať tedy X je libovolná množina a F_X příslušná volná grupa; množinu všech slov nad $X \cup X^{-1}$ označme opět W. Nahlédneme, že X je volnou bází F_X. Je tedy třeba ověřit, že pro libovolné zobrazení $f : X \to H$ existuje právě jeden homomorfismus $\varphi : F_X \to H$, který rozšiřuje f. Protože $F = \langle X \rangle$, takový homomorfismus f může existovat nejvýše jeden. Každé slovo $w \in W$ je pouze konečnou posloupností písmen z $X \cup X^{-1}$. Má-li být φ homomorfismus, musí nutně posílat $x^{-1} \mapsto f(x)^{-1}$, označme proto f' zobrazení $X \cup X^{-1} \to H$, které tímto způsobem rozšiřuje f i na prvky X^{-1}. Dále musí být prvek $\varphi(w) \in H$ roven součinu obrazů jednotlivých písmen w v zobrazení f' (ve stejném pořadí).

Pokud tímto způsobem φ můžeme definovat na všech slovech z W, triviálně už to bude homomorfismus $F \to H$. Je tedy třeba ukázat, že různé slovní reprezentace stejného prvku grupy F toto φ opravdu pošle na stejný prvek v H. To je ale jasné – takové slovní reprezentace se liší pouze konečnou posloupností připisování a mazání dvojiček xx^{-1} a $x^{-1}x$, které se ale tak jako tak po provedení zobrazení f' v grupě H pokrátí. Tím je první část důkazu u konce.

Nyní už jen vypozorujeme následující: Pro každou velikost[20] volné báze X existuje až na izomorfismus nejvýše jedna grupa s volnou bází této velikosti. Potom už budeme hotovi, neboť touto jednoznačně určenou grupou je dle první části důkazu právě F_X.

Mějme tedy dvě grupy G, H s volnými bázemi po řadě X, Y, mezi kterými existuje bijekce (tu označme f). Protože je X volná báze G, existuje homomorfismus $\varphi : G \to H$ rozšiřující f. Protože je Y volná báze H, existuje homomorfismus $\psi : H \to G$ rozšiřující f^{-1}. Jenže homomorfismus $\psi \circ \varphi : G \to G$ rozšiřuje identické zobrazení $f^{-1} \circ f$, tedy (opět díky vlastnostem volné báze) je $\psi \circ \varphi$ identické zobrazení na G. Obdobně je $\varphi \circ \psi$ identické zobrazení na H. Z prvního ze vztahů je ale φ prosté, díky druhému je φ na. Tím jsme našli izomorfismus grup G a H.

Z právě provedeného důkazu plyne, že množina X jednopísmenných slov z konstrukce volné grupy F_X je volnou bází této grupy. Nijak ale není zaručeno, že je to jediná taková množina. Trochu nás však může uklidnit alespoň následující tvrzení.

Tvrzení. *Ať F_X, F_Y jsou volné grupy s bázemi po řadě X, Y. Jsou-li X a Y různě velké, pak grupy F_X a F_Y nejsou izomorfní.*

Důkaz. Tvrzení budeme dokazovat jen pro konečně velké X, Y. Obecně funguje velmi podobný argument, my se však nekonečnům raději vyhneme. Uvažme podgrupu $K \leq F_X$, která obsahuje právě všechny prvky tvaru g^2 pro $g \in F_X$. Přitom $K \trianglelefteq F_X$, neboť pro libovolné $h \in F_X$ platí $hg^2h^{-1} = (hgh^{-1})^2$ (což platí zcela obecně v každé grupě). Faktorgrupa F_X/K je tedy dobře definovaná a každý její prvek má řád 2, je tedy dokonce abelovská[21].

Ukážeme, že F_X/K je izomorfní direktnímu součinu $|X|$ grup $\mathbb{Z}_2$. Na to dle minulého dílu stačí stačí nalézt $|X|$ jejích normálních podgrup, které ji generují a zároveň má každá z nich triviální průnik s grupou generovanou všemi ostatními. To je ale snadné, stačí vzít cyklické podgrupy generované jednotlivými kosety tvaru xK pro písmena $x \in X$. Všechny tři podmínky pak triviálně platí.

Díky tomu je nutně F_X/K izomorfní direktnímu součinu $\mathbb{Z}_2^{|X|}$, má tedy přesně $2^{|X|}$ prvků. Pro různé velikosti X je tedy F_X/K různě velká. Z čísla $2^{|X|}$ lze ale zpětně jednoznačně určit velikost $|X|$, takže volné grupy s různě velkými bázemi izomorfní být nemohou.

Jak už bylo řečeno dříve, pokud je $|X| = |Y|$, volné grupy F_X a F_Y izomorfní jsou (pouze se písmena v jejich bázích jmenují jinak). Různých volných grup tedy existuje přesně tolik, kolik je různě velkých množin – pro každou velikost jedna.

Podobně jako se každá grupa dá vnořit do vhodné symetrické grupy, každá grupa se dá vyfaktorizovat z šikovné volné grupy. Volné grupy jsou proto v jistém dalším smyslu prototypem grup:

Tvrzení. *Každá grupa je izomorfní faktorgrupě nějaké volné grupy.*

Důkaz. Vezměme si tedy libovolnou grupu G. Dále si vezměme (možná dost velikou) volnou grupu F s bází velikosti G. Ta má volnou bázi velikosti $|G|$, existuje tedy zobrazení f z této báze do grupy G, které je na. Díky univerzální vlastnosti volných grup pak existuje homomorfismus $\varphi : F \to G$ rozšiřující f. Zobrazení φ je tedy tím spíše na. Dle první věty o izomorfismu platí $F/\operatorname{Ker}\varphi \simeq \operatorname{Im}\varphi = G$, což jsme chtěli.

V předchozím důkazu jsme na velikosti volné grupy ani v nejmenším nešetřili. Většinou nám přitom stačí mnohem menší volná grupa. Pokud bude obraz f obsahovat nějakou množinu generátorů grupy G, bude už nutně $\operatorname{Im}\varphi = G$. Pro libovolnou množinu generátorů X lze tedy grupu G vyfaktorizovat dokonce z volné grupy F_X.

[20] Dvě nekonečné množiny jsou stejně velké právě tehdy, když mezi nimi existuje bijekce – tak je pojem „velikosti" definován.

[21] Jak by řešitelé první seriálové série měli vědět.

Tento abstraktní fakt vede k velmi praktickému způsobu vytváření a zaznamenávání grup – takzvaným prezentacím. Chceme-li zachytit nějakou grupu G, stačí ji vyfaktorizovat z nějaké volné grupy F pomocí vhodného homomorfismu φ a zapamatovat si velikost grupy F společně s její normální podgrupou $\operatorname{Ker}\varphi$. Není však nutné pamatovat si celou $\operatorname{Ker}\varphi$ – postačí zapamatovat si něco jako její „generátory". Protože je $\operatorname{Ker}\varphi$ normální (a my líní), stačí si dokonce pamatovat jen množinu jejích prvků, z nichž lze vytvořit celou $\operatorname{Ker}\varphi$ pomocí grupových operací a **konjugování** prvky z F.

Definice. *Prezentace* grupy sestává z množiny *generátorů* X a množiny *relací* $R \subseteq F_X$. Tato dvojice pak definuje grupu $G = F_X/K$, kde K je nejmenší normální podgrupa F obsahující množinu R. To značíme jako $G = \langle X \mid R\rangle$.

Na relace se můžeme dívat i mnohem intuitivnějším způsobem. Na celou grupu G nahlížíme jako na slova nad abecedou $X \cup X^{-1}$. Některá různá slova ale zachycují stejný prvek G (tak tomu je dokonce i v případě, kdy je G volná). My bychom rádi poznali, která slova odpovídají stejným prvkům. Je-li grupa G definována jako $G = \langle X \mid R\rangle$, potom dvě slova odpovídají stejnému prvku G právě tehdy, když je na sebe lze převést konečnou posloupností vepisování a mazání dvojiček xx^{-1}, $x^{-1}x$ a **libovolné relace z** R. Relace jsou vzorová slovíčka, která při faktorizaci zmizí.

V tomto smyslu jsou volné grupy grupami „bez nadbytečných relací" – jediné jejich relace jsou ty, které jsou vynuceny axiomy grup.

Z historických důvodů se relace často zapisují pomocí rovností. Například relace a^2b^{-1} se občas zapisuje jako rovnost $a^2 = b$, pomocí které lze „upravovat slova" bez toho, abychom měnili prvek G, který pojmenovávají.

Příklad. Zkusíme nalézt nějakou prezentaci dihedrální grupy D_{2n}. Tu lze nagenerovat dvěma prvky – nejmenší rotací r (v libovolném směru) a nějakou reflexí σ. Určitě ji proto lze vyfaktorizovat z volné grupy F_2. Označme si $\{a, b\}$ volnou bázi F_2. Budeme chtít, aby slovo a odpovídalo rotaci r a slovo b odpovídalo reflexi σ. Vezměme si tedy zobrazení $f : \{a, b\} \to D_{2n}$, které posílá $a \mapsto r$, $b \mapsto \sigma$; to lze rozšířit na homomorfismus $\varphi : F_2 \to D_{2n}$.

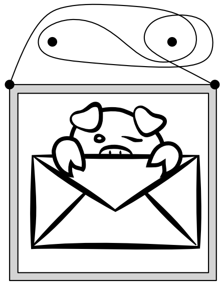
Zbývá nalézt jeho jádro v F_2. V grupě D_{2n} platí díky jejímu geometrickému významu identity $r^n = 1$, $\sigma^2 = 1$ a $\sigma r\sigma = r^{-1}$, takže prvky a^n, b^2, $(ba)^2$ leží v $\operatorname{Ker}\varphi$. Označíme-li K nejmenší normální podgrupu F, která obsahuje tyto tři prvky, máme tedy $K \subseteq \operatorname{Ker}\varphi$. Faktor F_2/K ale obsahuje nejvýše $2n$ prvků, neboť díky uvedeným třem relacím leží v každém jeho kosetu alespoň jeden prvek tvaru a^k či σa^k pro $k \in \{0, 1, \ldots, n-1\}$, a těch je dohromady jen $2n$. Nutně tedy $[G : K] \geq [G : \operatorname{Ker}\varphi]$, takže dokonce $K = \operatorname{Ker}\varphi$. Celkem je proto $\left\langle a, b \mid a^n, b^2, (ba)^2\right\rangle$ skutečně prezentací grupy D_{2n}.

Prezentace grup je velmi silný prostředek. Opravdu efektivně popisuje známé grupy, a navíc dává návod, jak lze libovolnou grupu vyrobit – stačí si vybrat nějakou volnou grupu a množinu našich oblíbených relací. Nevýhodou prezentací je, že z nich může být velmi těžké určit některé vlastnosti vyrobené grupy, jako je třeba už jenom její velikost. I když bude generátorů i relací pouze konečně mnoho, nelze ani algoritmicky rozhodnout, zda zadané slovo reprezentuje identitu.

Jak nevěšet obraz na zeď

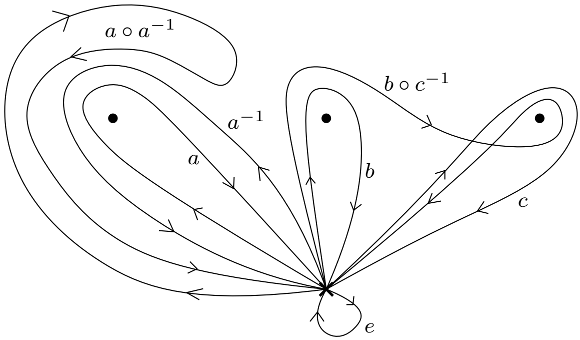
Pojďme si pro změnu hrát s úlohou, která s grupami na první pohled vůbec nesouvisí. Chcete-li se nad ní na chvíli zamyslet sami, vřele to doporučujeme – posléze bude řešení vyzrazeno.

Úloha. (Obraz na zdi) Ve zdi jsou zatlučeny dva hřebíky, za které chceme provázkem zavěsit obraz. Oba konce provázku jsou přitom připevněné k obrazu. Lze to udělat tak, aby obraz na zdi držel, ale po vyndání libovolného hřebíku spadl?



Při řešení této úlohy narážíme na problém, jak si věšení obrazu jednoduše představit. Jedním z nejsilnějších matematických triků je ale umění zapomínat. Při věšení obrazu na zeď nám může být úplně jedno, jak daleko jsou od sebe oba hřebíky. Může nám být také úplně jedno, kudy přesně provázek vede. Přitom ale musíme zapomínat chytře – musíme si pamatovat, z jakých stran a v jakém pořadí provázek prochází kolem hřebíků.

Abychom mohli věšení obrazu dobře uchopit, budeme se na něj dívat následujícím způsobem. Stěnu, na které má obraz viset, si představíme jako běžnou eukleidovskou rovinu. Dále si pevně zvolíme bod O, ve kterém budou oba konce provázku připevněny k obrazu (obraz samotný nás očividně nezajímá, stačí se zabývat motáním smyčky z provázku okolo hřebíků). Hřebíky pro nás budou další různé body v rovině. A konečně – konkrétní omotání provázku kolem hřebíků si představíme jako orientovanou křivku[22] v rovině, která začíná i končí v bodě O.



Dvě takové orientované křivky pro nás budou ekvivalentní, jestliže je na sebe lze spojitě přetransformovat bez projetí některým hřebíkem. Navíc tato spojitá transformace musí zachovat směr křivky. Pokud by v rovině žádný hřebík nebyl, budou všechny křivky ekvivalentní. Jakmile v ní však alespoň jeden hřebík je, dostáváme dokonce nekonečný počet neekvivalentních křivek – různé počty obtočení provázku kolem některého hřebíku dávají neekvivalentní křivky. Množinu všech skupin ekvivalentních křivek označme P.

Všimněme si, že každé dvě z našich křivek lze *zřetězit* – jejich slepením za sebe opět dostáváme nějakou orientovanou křivku, která začíná i končí v O. To nám zní trochu povědomě. Určitě navíc existuje triviální křivka, která žádný hřebík neobtáčí, tedy je ekvivalentní degenerované jednobodové křivce odpovídající bodu O. Vzhledem k zřetězování se proto chová jako identita. Navíc ke každé křivce existuje křivka opačného směru, ty se spolu vždy složí na triviální křivku.

Právě popsané operace přitom lze provádět s celými skupinami křivek, tj. prvky z P. Stačí totiž vzít libovolné prvky z příslušných skupinek a podívat se, do které skupiny výsledek padne. Že

[22] S pojmem křivky budeme rámci seriálu pracovat pouze intuitivně.

výsledek nezávisí na konkrétní volbě křivek, je intuitivně zřejmé. Dohromady jsme tedy na množině P definovali všechny grupové operace.

Je-li ve zdi zatlučeno n hřebíků, označme pro $i \in \{1, \dots, n\}$ symbolem a_i skupinu křivek odpovídajících jednomu obtočení ve směru hodinových ručiček kolem i-tého hřebíku. Každé zamotání provázku kolem hřebíků lze dostat zřetězením a_i a jejich inverzů. Grupu P tedy je možné vyfaktorizovat z F_n. Intuitivně ale vidíme, že každé netriviální zkrácené slovo odpovídá netriviální křivce. Jádro této faktorizace je proto triviální, dle první věty o izomorfismu je proto $F_n \simeq P$.

Shrneme, co víme: neekvivalentní omotání provázku kolem n hřebíků jednoznačně odpovídají různým slovům v grupě F_n s písmeny $\{a_1, \dots, a_n\}$, přičemž jednopísmenná slova odpovídají smyčkám kolem jednotlivých hřebíků. Nyní už máme nabito na sestřelení obecnější verze motivační úlohy.

Tvrzení. *Ve zdi je zatlučeno $n \in \mathbb{N}$ hřebíků. Potom lze pověsit obraz tak, aby spadl po odebrání libovolného hřebíku.*

Důkaz. Budeme hledat vhodné slovo w_n v grupě F_n, které odpovídá hledanému odmotání. Odebrání i-tého hřebíku způsobí právě zmizení všech výskytů znaků a_i, a_i^{-1} z tohoto slova, neboť se tím každá smyčka okolo i-tého hřebíku stane ekvivalentní triviální smyčce. Trochu přesněji (v řeči prezentací), odebrání i-tého hřebíku přesně odpovídá přidání relace $a_i = 1$.

Chceme tedy nalézt takové redukované slovo $w_n \in F_n$, které se po smazání všech výskytů a_i, a_i^{-1} pro libovolné dané i změní na slovo ekvivalentní prázdnému slovu 1. Pro $n = 1$ triviálně funguje jednopísmenné slovo $w_1 = a_1$. Pro $n = 2$ funguje slovo $w_2 = a_1 a_2 a_1^{-1} a_2^{-1}$, které se skutečně po vyndání libovolného hřebíku zkrátí až na prázdné slovo. Induktivně není problém pokračovat dál, stačí vzít $w_n = w_{n-1} a_n w_{n-1}^{-1} a_n^{-1}$. To je zkrácené slovo, které zřejmě není prázdné. Po odebrání n-tého hřebíku dostaneme slovo $w_{n-1} w_{n-1}^{-1}$, které je ekvivalentní prázdnému slovu. Odebráním libovolného a_i pro $i \in \{1, \dots, n-1\}$ budou z indukčního předpokladu obě slova w_{n-1}, w_{n-1}^{-1} ekvivalentní prázdnému slovu, takže i celé w_n bude ekvivalentní prázdnému slovu.

Intuitivně je přitom jasné, že na konkrétní volbě počátečního bodu O vůbec nezáleželo. Grupu P, se kterou jsme pracovali, lze sestrojit i pro jiné prostory než „rovinu s dírami“. Jedná se o takzvanou *fundamentální grupu* příslušného prostoru a jde se o velmi důležitý nástroj pro zkoumání takových prostorů.

Předchozí konstrukce však vyrábí velmi dlouhá slova, na pověšení obrazu by pak byl třeba provázek exponenciální délky v závislosti na n (slovo w_n je totiž víc než dvakrát delší než w_{n-1}). Nabízí se otázka, jak moc je možné ušetřit.

Úloha 3. Nalezněte zamotání provázku kolem n hřebíků, které řeší naši úlohu a přitom používá nejvýše $2n^2$ otáček.

Volnost podgrup a krycí grafy

Tvrzení o volných grupách mluví o krácení uvnitř konečných slov – jsou to tedy tvrzení kombinatorického rázu. Jak už jsme viděli, někdy mohou být velmi překvapivá. Chování volných grup má navíc důsledky i v dalších oblastech matematiky (vzpomeňme si na věšení obrazů). Třídu všech volných grup přitom známe velmi přesně – pro každou velikost volné báze existuje právě jedna.

Nabízí se zajímavá otázka: dědí podgrupy volnost? Po chvíli zamyšlení není odpověď vůbec jasná. Nic nám na první pohled nezaručuje, že by podgrupa volné grupy měla mít nějakou volnou bázi. Její generátory totiž mohou být velmi komplikovaná slova, která spolu mohou podezřelými způsoby interagovat. Volné grupy jsou velmi bohaté objekty (každá grupa z nich jde vyfaktorizovat!), dá se tedy čekat, že i jejich podgrupy budou velmi různorodé.

Překvapivě ale podgrupy volných grup ve skutečnosti opravdu volné jsou. Důkaz tohoto poznatku však vůbec není snadný. Samozřejmě je možné jej celkem rychle provést pomocí teorie zdaleka přesahující poznatky tohoto textu. Se zatnutím zubů a hromadou práce jej lze dokázat i čistě kombinatoricky. My nastíníme velmi pěkný a trikový důkaz, který nám ukáže další souvislost grup, grafů a geometrie.

Úmluva. Souvislým orientovaným grafem[23] $Q = (V, E)$ nyní budeme myslet množinu vrcholů V společně s množinou orientovaných hran E, přičemž každé dva vrcholy jsou spojeny nějakou posloupností (libovolně orientovaných) hran. Opět povolujeme i násobné hrany a očka.[24]

Na graf se můžeme dívat jako na hromadu ostrůvků spojených mosty. Každý most je průchozí v obou směrech, jeho orientace pouze říká, jak se tyto směry jmenují. Ostrůvky a mosty tvoří jakýsi prostor, ve kterém se můžeme vydat na procházku. V každém prostoru se ale skrývá jedna grupa, a to ta fundamentální.

Na rozdíl od roviny je ale graf dost hranatý objekt, při našem výletu bude nutné přejít daný most vždy celý naráz. Výlety po grafu můžeme kódovat velmi snadno. Každé hraně přiřadíme nějaké písmeno x. Její projití ve směru orientace bude odpovídat symbolu x, projití v protisměru symbolu x^{-1}. Každou procházku pak můžeme zakódovat slovem, jehož písmena odpovídají navazujícím hranám.

Zvolme si nějaký pevný vrchol $o \in V$ a uvažme všechny procházky, které začínají i končí ve vrcholu o. Takové výlety lze přirozeným způsobem řetězit i invertovat, přičemž prázdná procházka se chová jako identita. Zřetězení dvou procházek bude odpovídat napsání jejich slov za sebe zleva doprava. Procházky odpovídající ekvivalentním slovům budeme v jistém smyslu považovat za stejné. Dvě procházky tedy budou ekvivalentní, pokud je na sebe lze převést přidáváním a odebíráním zacházek typu „tam a zpátky“, tj. navazujících dvojic písmen xx^{-1} resp. $x^{-1}x$. Každou takovou skupinu ekvivalentních procházek (které začínají i končí v bodě o) nazveme *smyčkou*. Na množině smyček pak lze definovat pomocí zřetězení libovolných reprezentantů grupu P_Q.

Ta má i pěkný geometrický význam. Na ostrově o jsme se před začátkem výletu přivázali provázkem, pak jsme se prošli a nakonec jsme opět skončili v o. Dvě procházky odpovídají stejné smyčce právě tehdy, když se provázek jedné z nich dá v rámci mostů přetvarovat na provázek druhé z nich. Grupa P_Q je tedy vlastně fundamentální grupou našich ostrůvků s mosty (grafu Q).

Později se nám bude hodit uvažovat i procházky, které mohou začínat i končit v libovolných (klidně různých) vrcholech grafu. To má jediný problém – takové procházky obecně není možné řetězit, grupu z nich tudíž jednoduše vyrobit nelze. Pokud na sebe však některé dvě náhodou navazují, zřetězit je můžeme. I takové (ne nutně uzavřené) procházky lze rozdělit do skupinek podle toho, zda jsou ekvivalentní. Těmto skupinám budeme říkat *polosmyčky*.

Je jasné, že grupa P_Q vůbec nezávisí na tom, jak jsme si označili směry jednotlivých cest. Díky souvislosti Q dokonce P_Q nezávisí ani na volbě počátečního vrcholu o – uzavřené smyčky z vrcholu o_1 lze pomocí obousměrné procházky mezi o_1 a o_2 převést na uzavřené smyčky z o_2, přičemž toto převedení respektuje ekvivalenci procházek i grupové operace s nimi. Grupa P_Q se tím pádem dokonce dá získat uvažováním všech možných smyček v grafu Q, tedy bez fixování nějakého konkrétního vrcholu (pro řetězení je ovšem nutné obě smyčky reprezentovat uzavřenou procházkou se stejným začátkem).

Tvrzení. *Fundamentální grupa P_Q libovolného souvislého grafu Q je volná.*

Důkaz. Naším úkolem tedy je najít nějakou její volnou bázi. Začněme volbou libovolného počátečního vrcholu o. Zvolme si libovolnou neorientovanou kostru[25] grafu Q. Tato kostra T díky souvislosti grafu Q obsahuje všechny jeho vrcholy – v opačném případě by bylo možné přidat hranu a nevytvořit kružnici. Protože T neobsahuje kružnice, všechny smyčky v ní jsou ekvivalentní.

[23] Přívlastky „souvislý“ a „orientovaný“ budeme v textu dále často vynechávat.

[24] Na rozdíl od cayleygrafů se nám ale nyní očka a násobné hrany hodit budou. Připomínáme, že očkem myslíme hranu, která vede do téhož vrcholu, z něhož vychází.

[25] *Kostrou* nazýváme libovolný podgraf, který neobsahuje žádné neorientované kružnice, ale po přidání libovolné hrany už kružnici obsahovat bude.

Označme A množinu těch hran Q, které neleží v T. Zvolme libovolné $a \in A$. K jejímu počátečnímu vrcholu lze z vrcholu o dojít jednoznačně určenou polosmyčkou p v rámci T, podobně existuje jednoznačně určená polosmyčka p' v rámci T z konce a do o. Prvku a pak přiřadíme smyčku tvaru $p_a = pap'$. Vytvořené smyčky p_a určitě generují celou P_Q, neboť libovolnou procházku umíme získat chozením v rámci T (které odpovídá identitě) společně s procházením jednotlivých p_a.

Zbývá ukázat, že mezi různými smyčkami p_a neexistují žádné netriviální relace. To lze snadno nahlédnout ze slovní reprezentace jejich procházek. Je-li totiž slovo odpovídající některé procházce ekvivalentní prázdnému slovu, musí se na něj dát převést přidáváním a odebíráním dvojiček xx^{-1}, $x^{-1}x$. Pokud se však mosty z množiny A nezkrátí triviálně, dalším výletováním po grafu T je dokrátit nelze. Smyčky p_a pak odpovídají volné bázi grupy P_Q.

Nyní si definujeme velmi důležitý grafový pojem, který nám otevře dveře ke krásným trikům.

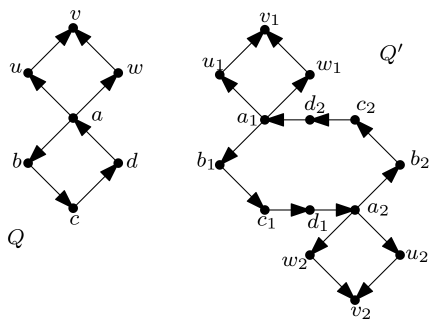
Definice. Ať $Q = (V, E)$ je souvislý orientovaný graf. Souvislý orientovaný neprázdný graf $Q' = (V', E')$ nazveme *krytím* grafu G, existuje-li *krycí zobrazení* $f : V' \to V$ splňující: Pro každý vrchol $v' \in V'$ existuje bijekce g mezi hranami vycházejícími z vrcholu v' a hranami vycházejícími z vrcholu $f(v')$ taková, že je-li h' hrana z v' do u', potom je $g(h')$ hrana z $f(v')$ do $f(u')$; analogicky pro hrany vstupující do v' a $f(v')$.

Pro jistotu ještě jednou zdůrazněme, že všechny uvažované grafy jsou souvislé. Krycí zobrazení vlastně omotává graf Q' na graf Q takovým způsobem, že nejbližší okolí každého vrcholu $v' \in V'$ vypadá stejně jako nejbližší okolí $f(v') \in V$.

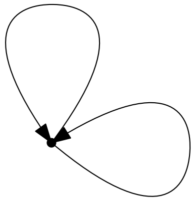
Každý graf triviálně kryje sám sebe, má však i větší krycí grafy. Pro každý graf Q dokonce existuje nekonečný krycí graf U, který neobsahuje žádné kružnice, tedy má triviální fundamentální grupu P_U. Sestrojit takové U je snadné – stačí vzít Q a „rozmotat ho, jak jen to jde“, tj. začít od jednoho počátečního vrcholu nulté úrovně, k němu dokreslit všechny potřebné šipky a na konec každé nakreslit vrchol první úrovně; dále vždy k vrcholům i-té úrovně dokreslit všechny scházející šipky dovnitř i ven a na jejich opačné konce přikreslit nové vrcholy úrovně $i + 1$.

Abychom si uměli představit, jak krytí a krycí zobrazení vlastně fungují, ukážeme si nejprve dva příklady.

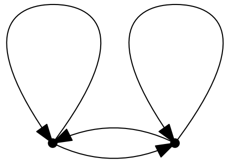
Příklad. Graf Q na obrázku má třeba následující krytí. Na posledním z obrázků je jeho krytí U.



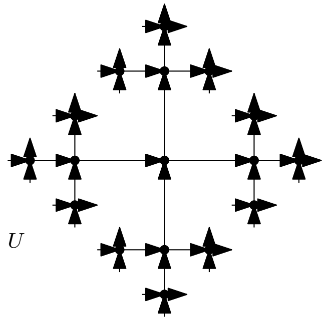
Příklad. Všimněme si, že fundamentální grupa grafu z předchozího příkladu je ve skutečnosti důvěrně známá F_2. Na následujícím obrázku je jiný graf Q_1, který má F_2 za fundamentální grupu, nějaký jeho krycí graf Q_2 a jeho úplné rozmotání U. Všimněme si, že tento U je shodou okolností přesně cayleygrafem grupy F_2. Tato souvislost není náhodná.



Q_0



Q_1



U

Než se pustíme dál, rozmysleme si následující snadné cvičení.

Cvičení 7. Kryje-li Q' graf Q pomocí krycího zobrazení f, potom je f na.

Zobrazení f podle své definice funguje jenom na vrcholech grafu V, očividným způsobem jej však lze rozšířit i na hrany – je-li $d' \in E'$ hrana z vrcholu u' do v', z vrcholu $f(u')$ pak s použitím bijekce g mezi hranami z vrcholu u a vrcholu u' vede jednoznačně určená hrana d odpovídající hraně d', jejíž koncový vrchol je roven $f(v')$. Tuto skutečnost nám nic nebrání označit jako $f(d') = d$. Všimněte si, že toto rozšířené zobrazení f se chová pěkně k začátkům a koncům hran, přičemž dodržuje i jejich směr. Bez problémů tedy můžeme f rozšířit dokonce na libovolné procházky, jejich obrazy budou opět procházky. Pochopitelně toto f zobrazuje ekvivalentní procházky na ekvivalentní procházky. Dává tedy přirozeně vzniknout šikovnému zobrazení f_*, které zobrazuje polosmyčky v grafu Q' na nějaké polosmyčky v Q, přičemž obrazy smyček jsou opět smyčky.

V předchozím odstavci jsme popsali, jak lze krycí zobrazení f rozšířit na všechno, co nás grafech momentálně zajímá. Rádi bychom však uměli postupovat i v opačném směru. To jednoznačně provést nelze, neboť krytí f typicky nebude prosté. Díky lokální podobnosti obou grafů je to ale proveditelné alespoň skoro.

Lemma. (zvedací) *Ať graf $Q' = (V', E')$ je krytím grafu $Q = (V, E)$ skrz krycí zobrazení f. Dále ať $o \in V$ je jeho libovolný vrchol a o' je nějaký jeho vzor v zobrazení f. Potom lze každou procházku p z bodu o v grafu Q jednoznačně „zvednout“ na takovou procházku p' z bodu o' v grafu Q', že $f(p') = p$.*

Důkaz. Lemma je v zásadě těžší vyřknout než dokázat. Takovou procházku p' jsme nuceni zrekonstruovat postupně po hranách. Protože je ale zobrazení f krycí, v každou chvíli máme na výběr právě jednu hranu, kterou nám daruje sama definice krycího zobrazení. Induktivně tak lze zkonstruovat právě jednu vyhovující cestu p'.

Proceduru z předchozího lemmatu si můžeme představit jako částečné rozmotání procházky v Q na procházku v Q'. Stejně jako před chvílí dává zvedání smysl i pro smyčky a polosmyčky.

Když už víme, co jsou krycí grafy, odhalíme jejich vztah s grupami.

Tvrzení. *Je-li $Q' = (V', E')$ krytí $Q = (V, E)$, potom $P_{Q'} \leq P_Q$.*

Důkaz. Ať f je nějaká krycí funkce $Q' \to Q$. Zvolme si libovolné $o' \in V'$, dále ať $o = f(o')$, příslušné fundamentální grupy budou obsahovat smyčky se začátkem a koncem v o', resp. o. Je-li $p \in P_{Q'}$, je to smyčka se začátkem i koncem v o', takže $f(p)$ je smyčka začínající i končící v o, tedy $f(p) \in P_Q$. Zobrazení f respektuje zřetězení smyček, takže je to dokonce grupový homomorfismus $P_{Q'} \to P_Q$.

Zbývá ukázat, že je prostý, neboť pak bude $P_{Q'} \simeq f(Q') \leq P_Q$. To však plyne ze zvedací vlastnosti krytí: Každá smyčka p v grafu Q se začátkem v o má jednoznačný vzor v grafu Q' se začátkem v o'. Pozor, tento vzor už nemusí být smyčkou, neboť může končit v jiném vzoru bodu o.

Každopádně, je-li smyčka $p \in P_Q$ triviální, dá se reprezentovat slovem, které se zkrátí. Jeho jednoznačný vzor v Q' se pak ale také musí zkrátit, zvednutí triviální smyčky je tedy triviální smyčka. To ale znamená, že netriviální smyčky v $P_{Q'}$ homomorfismus f zobrazuje na netriviální smyčky v P_Q, tedy má triviální jádro, takže je prostý.

Tvrzení intuitivně říká, že v krycím grafu Q' jsou některé kružnice grafu Q „rozmotány“, takže jejich netriviální smyčky v Q se v Q' trivializují. Jiné smyčky tímto přechodem nezmizí, tyto přeživší smyčky pak nutně odpovídají nějaké podgrupě původní grupy P_Q.

Uvedená korespondence však překvapivě funguje i na druhou stranu, jak odhaluje následující silné a pěkné tvrzení.

Tvrzení. *Ať Q je souvislý graf. Potom pro každou podgrupu $H \leq P_Q$ existuje jeho krytí Q' takové, že $H \simeq P_{Q'}$.*

Důkaz. Naším úkolem tedy je rozmotat graf Q „tak akorát“ – takovým způsobem, aby toto rozmotání přežily právě prvky H. Začněme tím, že ho rozmotáme úplně, tedy vyrobíme nekonečný strom U, jehož fundamentální grupa je triviální. Označme si ještě μ krycí zobrazení, které zprostředkovává krytí grafu Q grafem U. Vyberme počáteční vrchol o grafu U, za počáteční vrchol Q pak považujme $\mu(o)$. Díky zvedání má každá procházka v Q z bodu $\mu(o)$ jednoznačnou vzorovou pocházku v U začínající v o.

Pokud byla grupa H triviální, U je hledaný graf. Pokud je H netriviální, je nyní potřeba graf U zase trochu zmenšit poslepováním některých vrcholů, čímž vznikne graf Q'. Kde ho ale vyhrabeme? Explicitně jej popsat by bylo obtížné, my ho naopak fikaně donutíme, aby se vyrobil sám.

Definujme graf Q' následujícím způsobem. Jeho vrcholy budou odpovídat skupinám vrcholů z U, podobně jeho hrany. Vezměme dva vrcholy u, v grafu U. Protože je U strom, existuje v něm jednoznačná zkrácená procházka mezi o a u a jednoznačná zkrácená procházka mezi o a v. Z nich lze vytvořit jednoznačnou polosmyčku p_u z o do u a jednoznačnou polosmyčku $p_{v^{-1}}$ z v do o. Vrcholy u, v dáme do stejné skupinky (což označíme $u \sim v$) právě tehdy, pokud lze smyčky $\mu_*(p_u)$ a $\mu_*(p_{v^{-1}})$ v grafu Q zřetězit (tj. druhá začíná tam, kde první končí, neboli $\mu(u) = \mu(v)$) a pokud je toto zřetězení dokonce prvkem H.

Dávají takové skupinky vůbec smysl? Protože H obsahuje identitu, každý prvek je ve skupince se sebou samým. Díky existenci inverzů v H nastane $u \sim v$ právě tehdy, když $v \sim u$. A je-li $u \sim v$ a $v \sim w$, díky uzavřenosti H na zřetězení je i $u \sim w$. Rozdělení na skupinky je tedy skutečně smysluplné a lepení se dá provést.

Hrany v Q' pak zvolíme přirozeným způsobem: pro daný vrchol u' grafu Q' si vezmeme libovolného jeho reprezentanta u uvnitř grafu U a podíváme se na hrany z u. Pak projdeme všechny vrcholy s, do nichž vede hrana z u, a za každou takovou hranu z u do s pak do Q' nakreslíme právě jednu hranu z u' do s'. Nezávisí však tento postup na volbě reprezentanta u'? Skutečně ne. Je-li $u \sim v$, bylo možné slepit příslušné cesty v Q, takže $\mu(u) = \mu(v)$. Ze zvedací vlastnosti tedy mají body u, v stejná okolí. Vede-li tedy z u hrana d_s do nějakého jeho souseda s a zároveň $u \sim v$, vede též z vrcholu v nějaká hrana d_t do takového t, že $\mu(s) = \mu(t)$. Potom však lze polosmyčky $\mu(p_s)$ a $\mu(p_t)$ v grafu Q zřetězit, přičemž výsledná smyčka je (smazáním triviální zacházky tvaru $\mu(d_s)\mu(d_t)^{-1}$) ekvivalentní smyčce $\mu(p_u)\mu(p_{v^{-1}}) \in H$.

Fikaně definovaný graf Q' tedy skutečně existuje, zobrazení přiřazující vrcholu $u \in U$ jeho skupinku v Q' je díky předchozímu odstavci dokonce krycí. Označme π zobrazení vrcholů Q' na vrcholy Q, které každému vrcholu u' grafu Q' přiřadí $\mu(u)$, kde u je jeho libovolný reprezentant v U. Jsou-li $u \sim v$ dva vzory u' v grafu U, smyčky $\mu(p_u), \mu(p_{v^{-1}})$ bylo možné zřetězit, takže speciálně $\mu(u) = \mu(v)$, zobrazení π tedy dává smysl definovat. Protože U je krytím Q' a zobrazení π se chová jako μ, je také krycí.

Konečně nahlédneme, že $P_{Q'} \simeq H$. Za počáteční vrchol grafu Q' zvolme projekci o' vrcholu o. Rozmyslíme si, jak vypadají smyčky v $P_{Q'}$. Vezměme si tedy nějakou polosmyčku p' v grafu Q', která začíná v o'. Ať p je jí příslušná jednoznačně určená polosmyčka v U, která začíná v bodě o. Polosmyčka p' je prvkem $P_{Q'}$ právě tehdy, když také končí v bodě o, což nastane právě v případě, kdy jsme slepili začátek a konec procházky p. Jenže ty jsme slepili právě v případě, když $\pi(p') = \mu(p) \in H$. Zobrazení π indukuje prostý homomorfismus $P_{Q'} \to P_Q$, jehož obraz je dle předešlého přesně H, což jsme chtěli.

Všimněme si, že důkaz předchozího tvrzení skutečně nijak neříká, jak bude graf Q' přesně vypadat. Namísto toho se nám povedlo pomocí vlastností podgrupy H jeho existenci zařídit. Skutečná explicitní výroba takového grafu by obecně byla složitá, neboť zahrnuje hromadu kombinatorického krácení slov, které geometricky odpovídá kolabování grafu U. Předem ohlašovanou větu o podgrupách volných grup nyní dostaneme jako snadný důsledek.

Věta. *Každá podgrupa volné grupy je volná.*

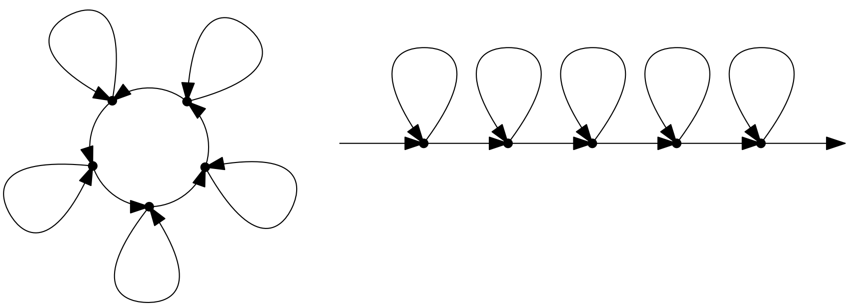
Důkaz. Volná grupa s bází X je fundamentální grupou kytice $|X|$ oček – grafu Q s jedním vrcholem, jehož $|X|$ hran v něm začíná i končí. To je okamžitě vidět, neboť takový graf má triviální kostru, takže všechny jeho hrany odpovídají generátorům příslušné fundamentální grupy. Je-li $H \leq G$, potom H je fundamentální grupou nějakého grafu Q' (který dokonce kryje Q). Grupa H je tedy také volná, neboť fundamentální grupy všech grafů jsou volné.

Pro ilustraci síly právě dokázaného výroku si na závěr rozmysleme několik faktů, které z něj okamžitě plynou.

Přestože lze každou grupu vyfaktorizovat z nějaké volné, podgrupy volných grup jsou pouze volné grupy. Volné grupy v sobě skrytě nesou struktury všech jiných grup, aniž by je samy obsahovaly jako podgrupy.

Také si vzpomeňme, jak složité je algoritmicky uchopit grupu zadanou nějakou prezentací $G = \langle X \mid R \rangle$. Přitom je ale normální podgrupa K příslušná relacím také volná. Sice tedy víme (až na počet generátorů), jak bude K vypadat, přesto algoritmicky neumíme najít, jak se v F_X schovává.

Dávno už víme, že F_2 obsahuje podgrupy izomorfní volným grupám s mnohem větší bází. Tento překvapivý fakt ale nyní dokážeme pochopit hlouběji. Podgrupy volné grupy F_2 odpovídají krytím grafu Q, který je tvořen jediným vrcholem a dvěma hranami (které začínají i končí v onom vrcholu). Podgrupy izomorfní s F_1 a F_2 obsahuje triviálně. Pro $n \geq 3$ zvolme krycí graf Q' jako $(n-1)$-cyklus, který má v každém vrcholu smyčku, z jehož existence plyne existence podgrupy grupy F_2 izomorfní s F_n. Existenci podgrupy izomorfní s $F_{\mathbb{N}}$ dostáváme volbou krycího grafu Q', který odpovídá nekonečné cestě se smyčkou v každém vrcholu. Jiným pěkným krycím grafem Q', který odpovídá takové grupě, je třeba nekonečná čtvercová mřížka. Z těchto grafů pak lze zpětně získat jim příslušné podgrupy.



Pomocí popsané korespondence volných grup a grafů dostávají volné grupy krásný geometrický význam, jehož sílu jsme právě mohli okusit. Chceme-li například pro nějakou podgrupu volné grupy najít velikost její báze, stačí najít krycí graf, který jí odpovídá, a podívat se, kolik hran v něm zbude po odebrání maximální kostry.

Síla vybudované teorie tkví přesně v tom, že jsme získali „slovník“, který nám umožňuje překlad mezi kombinatorikou na slovech a geometrií grafů. My zde však zkoumání volných grup ukončíme.

Závěr

Pokud jste dočetli až sem, cítíme se velice polichoceni. Ačkoli je nám to líto, budeme se nyní muset rozloučit. Přitom doufáme, že jste si naši dobrodružnou procházku teorií grup co nejvíc užili. Naším textem samozřejmě nic nekončí – pokud byste se chtěli dozvědět z teorie grup a moderní algebry více, můžeme vám doporučit třeba pěknou knížku od Josepha J. Rotmana „An Introduction to the Theory of Groups".

Těšíme se na vaše řešení třetí seriálové série a v tomto roce se s vámi se seriálem loučíme.

Návody ke cvičením

1. Víme, že můžeme každé $g \in G$ zapsat jako součet konečně mnoha prvků z X a jejich inverzů. Prvky X, které byly v daném součtu použity (buď přímo, nebo v podobě svých inverzů), označíme po řadě x_i. Jelikož je G abelovská, sčítání komutuje. Tím pádem můžeme seskupit všechny výskyty x_1 a $-x_1$, za nimi shluknout všechny výskyty x_2 a $-x_2$ a tak dále. Číslo a_i potom bude udávat počet výskytů x_i mínus počet výskytů $-x_i$.

2. Dá se jednoduše ověřit, že $\mathbb{Z}^n = \langle (1,0,\dots,0),(0,1,\dots,0),\dots,(0,0,\dots,1)\rangle$. Tím pádem má n-prvkovou, a tedy konečnou množinu generátorů.

3. Předpokládejme pro spor, že má konečnou množinu generátorů X. Nechť $X = \{\frac{p_1}{q_1}, \frac{p_2}{q_2}, \dots, \frac{p_n}{q_n}\}$, kde p_i jsou celá a q_i přirozená. Potom pro libovolná celá $a_1,\dots,a_n$ bude mít racionální číslo $a_1 \cdot \frac{p_1}{q_1} + a_2 \cdot \frac{p_2}{q_2} + \dots + a_n \cdot \frac{p_n}{q_n}$ v základním tvaru jmenovatel $q_1 q_2 \cdots q_n$ nebo dokonce nějaký dělitel tohoto čísla. Tím pádem jistě nedokážeme vygenerovat třeba $\frac{1}{q_1 q_2 \cdots q_n + 1}$ a dostáváme spor s předpokladem, že můžeme vygenerovat celé $\mathbb{Q}$.

5. Ačkoli se tvrzení zdá zřejmé, je třeba najít rozumný důvod, který jej vynutí. Jednou z možných argumentací je ta následující: Kdyby bylo možné F_2 nagenerovat jedním prvkem, byla by cyklická, tedy i abelovská. Jenže zkrácená slova a, b spolu nekomutují – slova ab, ba jsou zkrácená, jedná se tedy o různé prvky F_2.

6. Ať F_2 je vyrobena z množiny písmen $X = \{a, b\}$. Volme $H = \langle a^2, b^2 \rangle$. To je vlastní podgrupa grupy F_2, neboť všechna její slova obsahují sudý počet znaků z $\{a, a^{-1}\}$ a sudý počet znaků z $\{b, b^{-1}\}$ (přičemž krácení či vkládání dvojic vzájemně inverzních písmen tuto paritu nemění). Snadno navíc můžeme ověřit, že přiřazení $a^2 \mapsto a$, $b^2 \mapsto b$ lze rozšířit na izomorfismus $\psi : H \to F_2$.

7. Protože je Q' z definice neprázdný, na některý vrchol u grafu Q se něco zobrazit muselo. Protože je Q souvislý, existuje v něm z vrcholu v procházka do libovolného vrcholu u. Této procházce ale díky lokální podobnosti obou grafů odpovídá nějaká procházka v Q', její poslední vrchol je proto vzorem v.

Návody k úlohám

1. Vezměme třeba podgrupu $H = \langle a^2, b^2, ab \rangle$. První dva její generátory obsahují sudý počet písmen z $\{a, a^{-1}\}$ a sudý počet písmen z $\{b, b^{-1}\}$. Ten se ale při přidávání a mazání povolených dvojiček nemění, slovo ab pomocí nich tedy nagenerovat nelze. Nyní ukážeme, že pomocí prvků a^2, ab nelze nagenerovat b^2. To bychom museli získat napsáním slov $\{a^2, a^{-2}, ab, b^{-1}a^{-1}\}$ za sebe. Pro spor předpokládejme, že jsme vyrobili slovo w, které je ekvivalentní slovu b^2. Protože je b^2 redukované a každá třída ekvivalentních slov obsahuje právě jedno redukované slovo, lze w převést na b^2 pouze mazáním. Nejdříve tedy zkraťme sousední slova z množiny $\{a^2, a^{-2}, ab, b^{-1}a^{-1}\}$, která k sobě byla inverzní. Může se nyní některé písmeno b pokrátit? Vezměme momentálně nejbližší dvojici písmen b, b^{-1}, která se spolu mohou ještě někdy pokrátit. Potom ale mezi nimi je a v nějaké sudé nenulové mocnině, pokud tedy už jenom mažeme, nikdy se nepokrátí. Poslední ze tří dvojic nemůže generovat a^2 díky symetrickému argumentu. Zobrazení přiřazující prvkům a^2, b^2, ab prvky volné báze F_3 pak díky jejich nezávislosti umíme rozšířit na homomorfismus. Ten je triviálně na a díky nezávislosti našich generátorů má triviální jádro, tedy je to hledaný izomorfismus.

2. To dokážeme pomocí předchozí úlohy. Už umíme nalézt podgrupu $H_0 < F_2$, která je izomorfní s F_3, takové tři prvky jsou třeba $\langle a^2, b^2, ab \rangle$. Také už víme $F_2 \simeq F_2' = \langle a^2, b^2 \rangle$. Na F_2' tedy můžeme předvedený postup aplikovat znovu, což dává podgrupu $H_1 < F_2'$ definovanou jako $\langle ab, a^2b^2, a^4, b^4 \rangle$. Díky vlastnostem H_0 však ab nelze nagenerovat pomocí zbytku, díky vlastnostem H_1 jsou na sobě nezávislé i prvky a^2b^2, a^4, b^4. Induktivně pokračujme dál. Grupa $K = \langle ab, a^2b^2, a^4b^4, \dots \rangle$ je pak volná grupa s nekonečnou bází. Stejně jako minule totiž lze její generátory bijektivně zobrazit na generátory volné grupy $F_{\mathbb{N}}$, přičemž vlastností H_i jsou její generátory nezávislé.

To samozřejmě není jediný předpis takové divné podgrupy. Funguje třeba i $\langle bab^{-1}, b^2ab^{-2}, b^3ab^{-3}\rangle$ nebo $\langle ab, a^2b^2, a^3b^3, \dots\rangle$ a mnoho dalších, což si s trochou opatrnosti není problém rozmyslet.

3. Pro přehlednost zavedeme pro prvky x, y nějaké grupy značení $[x,y] = xyx^{-1}y^{-1}$. Předchozí dlouhé řešení tedy můžeme zapsat ve tvaru $w_n = [[\dots[[a_1,a_2],a_3],\dots],a_n]$. Rapidně ušetřit dokážeme následujícím trikem. Místo rozdělování písmen a_i v každém kroku na „poslední“ a „zbytek“ je zkusíme rozdělit přibližně na poloviny.

Vyrobme tedy slova v_n následujícím rekurzivním způsobem: Slovo v_n bude tvořeno písmeny z vhodné n-prvkové abecedy. Opět mějme $v_1 = a_1$. Máme-li už všechna slova v_i pro $i \le n-1$, nejprve označme[26] $m = \lceil \frac{n}{2} \rceil$ a $m' = \lfloor \frac{n}{2} \rfloor$ a následně definujme $v_n = [u_m, u'_{m'}]$, kde u_m značí slovo v_m na prvních m písmenech a $u'_{m'}$ značí slovo $v_{m'}$ na posledních m' písmenech. Je-li tedy $2^{j-1} \le n < 2^j$, je třeba při této rekurzivní definici v_n použít hranaté závorky nejvýše j-krát. Spočtěme tedy, kolikrát se každé a_i může nejvýše vyskytovat v v_n. Pro $n = 1$ se tam vyskytuje jednou. Každé další použití závorek nejvýše zdvojnásobí počet výskytů pevného a_i, takových kroků je nejvýše $j = \log_2 n + 1$, takže výskytů a_i je nejvýše $2^{\log_2 n+1} = 2n$. Slovo v_n používá n písmen, takže jeho délka je nejvýše $2n^2$.

---

[26]Symbolem $\lceil x \rceil$ se označuje nejmenší celé číslo, které je alespoň tak velké jako x, podobně symbolem $\lfloor x \rfloor$ značíme největší celé číslo, které není větší než x.

4. podzimní série – Integers

Výsledková listina

1.	*Matěj*	*Doležálek*	3	G Humpolec	2 3 3 5 5 5 5 5	25	**25,00**
2.	*Jakub*	*Parada*	2	G Gröss BA	3 1 – 5 5 5 5 –	23	**23,71**
3.	*Magdaléna*	*Mišinová*	1	GKepleraPH	1 3 3 5 5 5 – –	21	**23,42**
4.	*Josef*	*Minařík*	3	GJarošeBO	– 1 3 5 5 3 5 5	23	**23,03**
5.	*Jonáš*	*Havelka*	2	G Jírov ČB	3 3 3 5 5 0 1 5	21	**22,79**
6.	*Mikuláš*	*Brož*	1	GNadŠtolPH	3 3 3 5 5 – – –	19	**22,43**
7.	*Danil*	*Koževnikov*	4	GKepleraPH	– – – 5 5 5 4 5	24	**22,33**
8.	*Viktor*	*Fukala*	1	GKepleraPH	3 3 3 5 5 – – –	19	**22,32**
9.	*Michal*	*Beránek*	0	GVoděraPH	3 3 3 5 3 3 5 –	19	**21,95**
10.	*Jan*	*Kaifer*	2	GKepleraPH	1 3 3 5 0 4 4 –	19	**21,36**
11.	*Lucia*	*Krajčoviechová*	2	GJHroncaBA	– 3 3 5 5 5 – –	21	**21,34**
12.	*Adéla Karolína*	*Žáčková*	1	GZborovPH	– 3 3 5 0 1 5 0	17	**21,30**
13.	*Miroslav*	*Macko*	2	LeafAcademy	3 3 3 5 5 3 2 –	19	**21,25**
14.	*Petr*	*Khartskhaev*	1	PORG PH	3 3 3 5 3 – 2 1	17	**21,05**
15.	*Pavel*	*Hudec*	4	GJarkovPH	– – – 5 5 4 4 5	23	**20,72**
16.	*David*	*Beinhauer*	3	MendelG OP	3 3 3 5 5 – – –	$19 - 2i$	**20,09**
17.	*Martin*	*Raška*	4	WichtG OS	– 1 – 5 5 5 5 –	$21 + i$	**20,07**
18.	*Filip*	*Čermák*	4	MendelG OP	2 1 3 5 5 5 4 –	$22 - i$	**19,82**
19.	*David*	*Klement*	2	GNadAlejPH	3 3 3 1 5 3 – –	17	**19,69**
20.	*Ondřej*	*Krabec*	3	G KomHavíř	1 3 3 5 5 – 3 –	19	**19,60**
21.–22.	*Adam*	*Křivka*	2	CMGPgBrno	3 3 3 2 5 1 – –	16	**19,37**
21.–22.	*Martin*	*Starovič*	2	ŠpMNDaG BA	1 3 3 5 4 – – –	16	**19,37**
23.	*Alexandr*	*Jankov*	4	MatičníGOS	– 3 3 5 5 2 5 –	$21 + i$	**19,12**
24.	*Hedvika*	*Ranošová*	4	GBudějovPH	3 3 3 5 5 5 – 4	22	**19,09**
25.	*Lucie*	*Kundratová*	3	G TGM Zlín	2 1 3 5 5 – 5 –	$20 + i$	**19,08**
26.	*Lenka*	*Kopfová*	3	MendelG OP	– 1 – 5 5 5 5 –	21	**19,03**
27.	*Petr*	*Gebauer*	4	G Mělník	3 1 – 5 5 5 4 –	$22 - i$	**18,61**
28.	*Jan*	*Vavřín*	1	PORG PH	1 3 3 – 5 – 2 –	14	**18,35**
29.	*Zuzana*	*Urbanová*	4	GFXŠaldyLI	3 3 3 – 5 5 4 –	20	**18,07**
30.–31.	*Tomáš*	*Ganz*	2	ŠpMNDaG BA	1 2 3 5 3 – 1 –	14	**17,77**
30.–31.	*Kateřina*	*Panešová*	2	G Teplice	3 3 3 – 5 – – –	14	**17,77**
32.	*Vojtěch*	*Gaďurek*	1	PORG PH	3 3 3 – 3 – – –	12	**17,59**
33.	*Ján*	*Pavlech*	4	GsJozefaNM	1 3 3 5 5 – 1 –	17	**17,00**
34.	*Klára*	*Churá*	1	GNerudCheb	1 1 3 – 5 1 – –	11	**16,83**
35.	*Radek*	*Olšák*	3	GMensaPH	3 3 3 5 5 – – –	19	**16,73**
36.	*Anna*	*Mlezivová*	4	GCoubTábor	2 3 3 5 5 – – –	18	**16,46**
37.	*Martin*	*Zimen*	3	GJMasar JI	2 3 3 5 4 – – –	17	**15,81**
38.	*Jakub*	*Růžička*	3	G Nymburk	3 3 3 – 5 – – –	$14 - i$	**15,53**
39.	*Tomáš*	*Flídr*	0	GMasarykKM	2 3 3 – – – – –	8	**15,25**
40.	*Klára*	*Pernicová*	1	GŠlapanice	2 3 3 – 1 – – –	9	**14,89**

41.	*Jan*	*Hrubeš*	3	G ČKrumlov	1 3 3 – 5 – – –	12	**14,47**
42.	*Klára*	*Hloušková*	2	G Kolín	2 3 3 2 0 – – –	10	**13,41**
43.	*Martin*	*Hubata*	2	GMikul23PL	2 3 3 2 – 0 – –	10	**13,27**
44.	*David*	*Ryzák*	4	G Trutnov	3 3 3 – 5 – – –	14	**13,01**
45.	*Dominik*	*Stejskal*	3	G Krnov	3 3 3 – 1 – – –	10	**12,45**
46.	*Kateřina*	*Charvátová*	3	GBNěmcovHK	– 3 3 5 – – – –	11	**11,05**
47.	*Filip*	*Chudoba*	4	PORG PH	1 3 3 5 – – – –	12	**9,48**
48.	*Jonáš*	*Stoilov*	2	PORG PH	– 3 3 – – – – –	6	**9,26**
49.	*Dominika*	*Hájková*	3	GPísnickPH	1 3 3 – – – – –	7	**9,17**
50.	*Alžběta*	*Manová*	3	G UherBrod	2 1 3 1 – – – –	7	**8,58**
51.	*Victoria María*	*Nájares Romero*	4	GZborovPH	2 3 3 4 – 1 – –	13	**8,32**
52.	*Dominik*	*Majkus*	3	GNVPlániPH	– 3 3 – – – – –	6	**8,00**
53.	*Martin*	*Bakoš*	4	GPBystrica	3 3 3 – – – – –	9	**7,04**
54.	*Petr*	*Zahradník*	3	GŠmejkalÚL	2 1 3 – – – – –	6	**6,86**
55.	*Tomáš*	*Čelko*	4	GPBystrica	3 3 3 – – – – –	9	**6,81**
56.–57.	*Soňa*	*Husáková*	1	GČeskoliPH	3 0 – – – – – –	3	**6,79**
56.–57.	*Klára*	*Zemanová*	1	PORG PH	– – 3 – – – – –	3	**6,79**
58.	*Šimon*	*Hutař*	3	PORG PH	1 3 1 – – – – –	5	**6,61**
59.	*Anna*	*Musilová*	2	PORG PH	1 1 – 1 – 1 – 0	4	**6,09**
60.	*Vilém*	*Raška*	2	GJarošeBO	– 3 – – – – – –	3	**5,27**
61.	*Jakub*	*Čurda*	3	PORG PH	0 1 3 – – – – –	4	**5,11**
62.	*Zuzana*	*Šraierová*	3	GČeskoliPH	– 1 – – – 1 1 –	3	**4,17**
63.	*David*	*Ha*	3	MasG Plzeň	– 1 2 – – – – –	3	**4,13**
64.	*Jaroslav*	*Paidar*	4	SPŠMasarLI	– 3 3 – – – – –	6	**3,96**
65.	*Vít*	*Gaďurek*	3	PORG PH	1 2 – – – – – –	3	**3,31**
66.	*Michal*	*Chudoba*	3	GLitoměřPH	0 3 – – – – – –	3	**3,29**
67.	*Václav*	*Nevyhoštěný*	2	GJarošeBO	– 1 – – – – – –	1	**1,91**

1. jarní série – Být či nebýt

Výsledková listina

1.–2.	*Matěj*	*Doležálek*	3	G Humpolec	3 3 – 5 5 5 5 5	25	**25,00**
1.–2.	*Josef*	*Minařík*	3	GJarošeBO	3 – – 5 5 5 5 5	25	**25,00**
3.	*Michal*	*Beránek*	0	GVoděraPH	3 3 1 5 5 5 5 –	23	**24,10**
4.	*Radek*	*Olšák*	3	GMensaPH	3 – – 4 5 5 5 5	24	**23,46**
5.	*Magdaléna*	*Mišinová*	1	GKepleraPH	3 3 – 5 – 5 – 5	21	**23,42**
6.	*Jan*	*Kaifer*	2	GKepleraPH	3 3 – 4 5 5 – 5	22	**23,30**
7.	*Timea*	*Szöllsová*	2	G Gröss BA	3 3 – 5 5 – 5 –	21	**22,79**
8.	*Adéla Karolína*	*Žáčková*	1	GZborovPH	3 3 3 5 – – 5 –	19	**22,43**
9.	*Jakub*	*Parada*	2	G Gröss BA	3 3 3 5 5 5 – –	21	**22,33**
10.	*Jonáš*	*Havelka*	2	G Jírov ČB	3 3 3 4 5 5 0 –	20	**22,17**
11.	*Ondřej*	*Krabec*	3	G KomHavíř	3 3 2 5 5 5 – –	21	**21,44**
12.	*Lucia*	*Krajčoviechová*	2	GJHroncaBA	3 3 – 5 5 5 – –	21	**21,34**
13.–14.	*Mikuláš*	*Brož*	1	GNadŠtolPH	3 3 2 5 4 – – –	17	**21,30**
13.–14.	*Samuel*	*Krajči*	3	GAlejKošic	3 – 3 5 5 – 5 –	21	**21,30**
15.	*David*	*Klement*	2	GNadAlejPH	3 3 2 5 – 5 – –	18	**20,45**
16.	*Danil*	*Koževnikov*	4	GKepleraPH	– – – 4 5 5 5 4	23	**20,11**
17.	*Klára*	*Pernicová*	1	GŠlapanice	3 3 2 4 – 3 – –	15	**20,00**
18.	*Lucie*	*Kundratová*	3	G TGM Zlín	3 3 – 5 5 5 – –	21	**19,95**
19.	*Klára*	*Churá*	1	GNerudCheb	3 3 3 5 – – 0 –	14	**19,28**
20.–21.	*Petr*	*Khartskhaev*	1	PORG PH	3 3 1 4 2 – 0 –	13	**18,18**
20.–21.	*Miroslav*	*Macko*	2	LeafAcademy	3 1 1 5 5 – – –	15	**18,18**
22.	*Vojtěch*	*Gaďurek*	1	PORG PH	3 3 1 4 – – 0 –	11	**16,71**
23.	*David*	*Beinhauer*	3	MendelG OP	3 3 1 5 – 2 – –	14	**16,19**
24.	*Kateřina*	*Panešová*	2	G Teplice	3 3 3 – 3 – – –	12	**16,00**
25.	*Jan*	*Vavřín*	1	PORG PH	3 3 – 5 – – – –	11	**15,72**
26.	*Adam*	*Křivka*	2	CMGPgBrno	3 3 – 5 – – – –	11	**15,05**
27.	*Martin*	*Zimen*	3	GJMasar JI	3 3 0 5 5 – – –	$16 + i$	**15,03**
28.	*Dominik*	*Stejskal*	3	G Krnov	3 3 – 5 – – – –	11	**13,47**
29.	*Adam*	*Mendl*	1	GCoubTábor	3 3 – 4 – – – –	10	**13,05**
30.	*Tomáš*	*Flídr*	0	GMasarykKM	3 3 – – – – – –	6	**12,88**
31.	*Jonáš*	*Stoilov*	2	PORG PH	3 3 0 3 – – – –	9	**12,77**
32.	*Ján*	*Pavlech*	4	GsJozefaNM	3 3 3 4 – – – –	$13 - i$	**12,73**
33.	*Tomáš*	*Čelko*	4	GPBystrica	3 3 1 4 – 4 – –	15	**12,50**
34.	*Jakub*	*Růžička*	3	G Nymburk	3 3 – 4 – – – –	10	**11,82**
35.	*Jan*	*Nekarda*	2	GUHradiště	3 3 2 – – – – –	8	**11,56**
36.–38.	*Tomáš*	*Hulla*	1	GTajBanBys	3 3 0 – – – – –	6	**11,38**
36.–38.	*Soňa*	*Husáková*	1	GČeskoliPH	3 3 0 – – – 0 –	6	**11,38**
36.–38.	*Klára*	*Zemanová*	1	PORG PH	3 3 0 – – – – –	6	**11,38**
39.	*Klára*	*Hloušková*	2	G Kolín	3 3 1 1 – – 0 –	8	**11,25**
40.	*Lenka*	*Kopfová*	3	MendelG OP	3 3 3 5 – – – –	14	**10,93**

41.	*Michal*	*Chudoba*	3	GLitoměřPH	3 3 0 4 – – – –	10	**10,64**
42.	*Filip*	*Chudoba*	4	PORG PH	3 3 1 4 – 2 – –	13	**10,44**
43.	*Matěj*	*Holubička*	2	G Hořice	3 3 – – – – – –	6	**9,41**
44.	*Martin*	*Hubata*	2	GMikul23PL	3 2 1 – – – – –	6	**8,74**
45.	*Dominika*	*Hájková*	3	GPísnickPH	3 3 0 – – – – –	6	**8,00**
46.	*Martin*	*Bakoš*	4	GPBystrica	3 3 – 4 – – – –	10	**7,93**
47.	*Zuzana*	*Doležalová*	0	ZŠ Slov	3 – – – – – – –	3	**7,79**
48.	*Josef*	*Král*	3	MendelG OP	3 3 0 – – – – –	6	**7,65**
49.	*Kateřina*	*Charvátová*	3	GBNěmcovHK	– 3 3 – – 1 – –	7	**7,04**
50.	*Anna*	*Jerhotová*	2	GJosefskPH	3 – 0 0 – 0 – –	3	**5,27**
51.	*Alžběta*	*Manová*	3	G UherBrod	3 – – – – – – –	3	**3,88**
52.	*Aleš*	*Horák*	1	SPŠ Třebíč	1 – – – – – – –	1	**2,67**

2. seriálová série – Teorie grup II

Výsledková listina

1.–2.	*Matěj*	*Doležálek*	3	G Humpolec	5	5	5	15	**15,00**
1.–2.	*Danil*	*Koževnikov*	4	GKepleraPH	5	5	5	15	**15,00**
3.	*Michal*	*Beránek*	0	GVoděraPH	4	4	5	13	**14,06**
4.	*Alexandr*	*Jankov*	4	MatičníGOS	4	5	5	14	**13,32**
5.	*Klára*	*Churá*	1	GNerudCheb	4	2	–	6	**9,54**
6.	*Ondřej*	*Krabec*	3	G KomHavíř	4	–	5	9	**9,49**
7.	*Adéla Karolína*	*Žáčková*	1	GZborovPH	5	–	–	5	**8,51**
8.	*Radek*	*Olšák*	3	GMensaPH	5	5	–	10	**8,42**
9.	*Martin*	*Zimen*	3	GJMasar JI	4	4	–	8	**7,21**
10.	*David*	*Beinhauer*	3	MendelG OP	5	–	–	5	**6,29**
11.	*Lucia*	*Krajčoviechová*	2	GJHroncaBA	5	–	–	5	**5,36**
12.	*Josef*	*Minařík*	3	GJarošeBO	5	–	–	5	**5,05**
13.	*Magdaléna*	*Mišinová*	1	GKepleraPH	–	2	–	2	**4,43**
14.	*Petr*	*Gebauer*	4	G Mělník	–	5	–	5	**2,71**
15.	*Jonáš*	*Havelka*	2	G Jírov ČB	1	0	0	1	**1,85**
16.	*Jan*	*Kaifer*	2	GKepleraPH	1	–	–	1	**1,77**
17.–18.	*Matěj*	*Holubička*	2	G Hořice	0	–	–	0	**0,00**
17.–18.	*Michal*	*Chudoba*	3	GLitoměřPH	0	–	–	0	**0,00**

adresa: *Korespondenční seminář*
KAM MFF UK
Malostranské náměstí 25
118 00 Praha 1
web: *http://mks.mff.cuni.cz/*
e-mail: *mks@mff.cuni.cz*