International Mathematical Camp

Maths Beyond Limits

Camp Brochure

Milówka 2021

Text preparation and editing: Anna Łeń, Szymon Zwara

Problems, solutions: Tomasz Ślusarczyk, Radosław Żak

Handouts: Łukasz Bożyk, Paweł Gadziński, Andrzej Grzesik, Aliaksandra Novik, Marian Poljak, Peter Simon, Semen Słobodianiuk, Robert Szafarczyk, Vladyslav Zveryk

Typesetting (with TEX/LATEX): Łukasz Bożyk, Anna Łeń

Cover project: Justyna Jaworska

ISBN: 978-83-901470-9-3

Warsaw 2021

Maths Beyond Limits

e-mail: mathsbeyondlimits@gmail.com
www: mathsbeyondlimits.eu
Facebook fanpage: facebook.com/mathsbeyondlimits

Polish Children's Fund

ul. Pasteura 7, 02-093 Warsaw
tel. (+48 22) 848 24 68
e-mail: fundusz@fundusz.org
www: fundusz.org

The project is co-financed by the Governments of Czechia, Hungary, Poland and Slovakia through Visegrad Grants from International Visegrad Fund. The mission of the fund is to advance ideas for sustainable regional cooperation in Central Europe.

About the camp

Maths Beyond Limits is a Europe-wide camp for high school students interested in maths.

The aim of the project is to create space for development of young maths enthusiasts through working on interesting and demanding mathematical subjects. It is designed to encourage participants to share their knowledge and passion with others as well as to enhance cooperation and integration of European mathematical societies. Moreover, its goal is to awaken youth's curiosity and to help them make important habits of creative thinking, self-development, ambition and ability to cooperate.

MBL 2021 was the sixth edition of this initiative and was held from the 13th to the 25th of September 2021. To accommodate for the COVID-19 pandemic, two camps took place simultaneously – 45 participants met in Milówka, while 25 others took part in the Virtual MBL (**VMBL**). In total, there were 70 participants and 18 tutors from 21 countries: Belarus, Bosnia and Herzegovina, Czech Republic, France, Germany, Georgia, Hungary, India, Indonesia, Iran, Lithuania, Norway, Poland, Romania, Russia, Serbia, Slovakia, Sweden, Switzerland, Ukraine, United States of America.

MBL was filled with numerous events. Every regular day there were three 80-minute-long blocks of **Mathematical Classes**. They were devoted to some of the most beautiful concepts in mathematics from outside the high school's curriculum. During every block there were 3 lecture sessions to choose from, each concerning different mathematical field, which contributed to the diversity of academic experience participants had on the camp. Classes were followed by an hour-long **TAU**, which stands for **Time Academic Unscheduled** that was designated for the students to work on the problems independently or with the help of tutors. It was also a great opportunity to clarify any points of the classes that were found hard or insufficiently explained. Another regular mathematical events were **Camper Talks**, i.e. a 30-minute-long presentations given by some participants on topics related to mathematics they were interested in. Their main goal was to give participants the opportunity to practice important skills of clear presentation of mathematical topics in English and inspire others with their passion. Students had prepared them beforehand and consulted them with staff members during the camp. At VMBL we also had **Olympic Training**, which consisted of solving olympiad-style problems followed with group discussions.

Maths was not the only thing the camp was about, therefore the hard work was followed by **Evening Activities**. They were fun, challenging, educational or thought-provoking. Most of them were run by the participants, while other by the staff. Lastly, there was also time for **Sports** in the beautiful scenes of Beskidy mountains. Activities included running and workouts as well as playing volleyball, football and frisbee.

At MBL we do not let anyone get bored, therefore also quite a few special events were organised. We went for a **Hike** in Beskidy mountains and solved a bunch of puzzles during both **Escape Wall** and a day-long **Puzzle Hunt**. Participants also got a chance to talk about careers, universities and olympiads with tutors and organisers during the **Questions Evening Café**. Moreover, they were able to improve their problem solving skills thanks to **Relays** (team competition similar to Náboj) and **Team Problem Solving**. Together with our sponsor Jane Street we also ran the **Estimathon**, which was a team-based contest that combined trivia, game theory, and mathematical thinking. All these little things contributed to making MBL 2021 such a great, inspiring and unforgettable camp.

Events of the camp

Most of the mathematical classes was joint for MBL and VMBL paritcipants and most of the special events were held at both camps. Evening Activities and Camper Talks were disjoint, ones from the Virtual camp are marked with "@".

Mathemamatical Classes

- Additive Combinatorics (Kada Williams)
- Automata and Formal Languages (Aleksandra Kowalska)
- Coding Theory (Andrei Nenciu)
- Combinatorics through and through (Ana Bogdan)
- Constructions in Combinatorics via Algebraic Methods (Semen Słobodaniuk)
- Diagram Chasing in Abelian Categories (Robert Szafarczyk)
- Domino Tilings (Łukasz Bożyk)
- Finite Fields in Number Theory (Vladyslav Zveryk)
- Formal Proof Vrtification in Lean (Jakub Wornbard)
- Galois Theory (Łukasz Orski)
- General Topology (Kosma Kasprzak & Radosław Żak)
- How Big Are Infinite Sets (Dominik Holly)
- How to Find the Number of Ways and the Shortest Path (Dominik Holly)
- International Linguistics Olympiad (Tymoteusz Zdunek)
- Introduction to Algebraic Geometry (Aliaksandra Novik)
- Liouville-Ostrowski Theorem (Łukasz Orski)
- Markov Chains (Marcin Augustynowicz)
- Mathematical Games (Peter Simon)
- Menelaos Ceva theorem (Marian Poljak)
- NP-completness and Non-determinism (Paweł Burzyński)
- Number Theory Theorems (Paweł Gadziński)
- Ramsey Theory (Peter Simon)
- Stirling Numbers (Piotr Kamiński)
- Szemerédi Regularity Lemma (Andrzej Grzesik)
- The Geometry of Polynomials (Robert Crumplin)
- Topology in Metric Spaces (Kosma Kasprzak & Radosław Żak)

@ Introduction to Knot Theory (Alyona Nefyodova)

@ How Mathematical Analysis Helps Solving Hard Problems in Number Theory and Algebra (Navid Safaei)

Special Events

- Escape Wall
- Ice-breaking Game
- Puzzle Hunt
- Scavenger Hunt
- Questions Evening Cafe
- Relays
- Team Problem Solving
- Hike

Camper Talks

- About a Forgotten Transformation (Áron Bán-Szabó)
- Brief Introduction to Quantum Computing (Joël Huber)
- De Brujin's Theorem (Milica Vugdelić)
- Killing Two Birds with One Trigonometric Stone (Boris Stanković)
- Mandelbrot and Julia Sets (Michał Wiliński)
- Miquel Point (Márton Lovas)
- Nested Radicals (Illia Antypenko)
- Partitions and Generating Functions (Zsombor Várkonyi)
- Stable Matching Algorithm (Anca Mihaela Sfia)
- What Is in a Grid? (Dániel Hegedűs)

@ Sorting Techniques (Mikołaj Gazeel)
@ Basic Differential Equations (Jakub Zieliński)
@ Introduction to Fractals (Paul Hamrick)
@ Group Theory in Crystallography (Paweł Pielasa)
@ Volume of n-dimensional Objects (Richárd Fekete)

Evening Activities

- Camp Newspaper (Simon Martin & Ania Łeń)
- Cardboard Castle (Ania Łeń)
- Chłoptivity (Dániel Hegedűs & Zsombor Várkonyi)
- Contract Bridge Workshop (Anca Mihaela Sfia)
- Drawing Fantasy Maps (Marcel Chwiałkowski)
- Handmade Bracelets (Ela Vojtková)
- Huge Marble Run (Simon Martin)
- Knot Workshop (Ruth Plümer)
- Macrame (Zuzanna Iwan)
- Master Chef (Piotr Kuc)
- Murder History in Milówka (Adam Bencsik & Áron Bán-Szabo)
- Number Wars (Márton Lovas)
- Orienteering (Matej Urban)
- Philosophy Debate (Mariam Baghdasaryan)
- PowerPoint Karaoke
- Teaching Football (Tamás Kovács & Zsombor Várkonyi)
- Team Trivia
  (Áron Bán-Szabó, Ana Bogdan, Mariam Baghdasaryan, Noah Bjerke & Tomáš Flídr)
- The City Is Sleeping (Gabriella Sztranyák)
- Waltz Session (Ervin Macić)
- Who Wants to Be a MBLionaire?

@ Create your own Discord emoji
@ Creative Corner
@ Fishbowl
@ PowerPoint Karaoke
@ Speed friending
@ Scribble.io
@ Team Trivia
@ Trying to solve a Rubik's Cube (Paul Hamrick)

Testimonials

- **Adam Bencsik:** Wow. MBL is a marvel. Some of the most brilliant people, sharing a common love for math, spending 2 weeks in the roaming hills of Milowka. Deepening their knowledge and forming deep, ever lasting friendships. Thank you.
- **Ana Maria-Iulia Bogdan:** MBL is one of the many communities I had contact with, but it really is the one that I love the most. Everything from the place, to the people, to the activities and classes is amazing. For a couple of weeks, you just travel to another dimension where everything is made out of laughs and really cool math.
- **Jan Radomiński-Lasek:** First of all, it's an amazing opportunity to taste not only olympic maths, but also academic maths on advanced level, and secondly it's so wonderful to meet all of those people. I feel like I could find help in every time, every person, everywhere.
- **Mariam Baghdasaryan:** The camp was amazing in so many ways – the lectures were perfect, because I always could choose a hard one, a medium one or an easier one depending on my mood/energy level, TAU was a great chance to talk to tutors and better understand the topic (stickers are wonderful!), Evening Activities were incredible, since they helped us to have fun and talk to other campers and share our hobbies. All special activities were also great, I really enjoyed the hike and all the puzzles.
- **Marko Dimitrić:** MBL was truly different from all the maths camps I've ever been to, with its focus on pure and applied math and not on olympiad preparations and with all the social activities. There was not much free time during the day, but that was the case just because in every moment there was some activity, mathematical or not, taking place.
- **Michał Wiliński:** Having participated in the virtual version of the camp, I knew the mathematical classes would be top notch and the events fun. What I didn't know was how crucial were the every day interactions between participants. Though we came from different backgrounds, we all like mathematics, and that was the jumping-off point for getting to know more about each other. Throughout the days we bonded, talking about the lectures, tutors, activities, and sharing our experiences with others.
- **Piotr Kuc:** A day on MBL really shows how many different interesting things you can do in just 24 hours. And you will have whole two weeks.
- **Ruth Plümer:** For me, MBL was two weeks of mathematics, two weeks of very international atmosphere, two weeks of challenges, two weeks of card games, sports, random stuff, a lot of fun and very little sleep, and it was two weeks far away from my normal life, far away from reality, two weeks in which I had everything I needed, and I can't imagine how somebody who's ever been to MBL would feel differently about it.
- **Zsigmond Fleiner:** My best math related experience. I haven't met with so many clever, math lover, open-minded people from other countries before.
- **Zsombor Várkonyi:** At MBL people are so nice that you don't even realise how smart everyone is.

Sponsors and project partners

Running MBL would not have been possible without the help of numerous people involved in organising, fundraising or working at the camp itself. All the tutors were volunteers who contributed their free time to prepare classes and come to the camp. MBL was free of charge to all participants thanks to generous sponsors and wonderful project partners, which we had great pleasure of cooperating with.

Project partners

Polish Children's Fund's
`fundusz.org`

Faculty of Mathematics and Physics of Charles University
`mff.cuni.cz`

The Joy of Thinking Foundation
`agondolkodasorome.hu`

Trojsten
`trojsten.sk`

Polish Children's Fund's mission is to support exceptionally gifted children and teenagers from all of Poland in order to enable them to fully develop their talents and scientific as well as artistic passions. The innovative, original aid programme conducted by the Fund for the last 33 years aims to support young people who cannot find opportunities to fully develop their potential in their local environment (both home and school).

Trojsten is a civic association that organizes mathematics, physics and informatics events in Slovakia for elementary and secondary school students. It organises KMS (Correspondent Mathematical Seminar), well-established international mathematical competition Náboj in Slovakia, the International Programming Competition ICPS and co-organises the International Mathematical Seminar iKS.

The Joy of Thinking Foundation supports gifted Hungarian students in fully developing their talents, reaching their goals in life, and becoming useful members of society. It attains this goals via furthering students' abilities in math camps, math circles, one-to-one sessions and small group activities. Among the biggest initiatives of the Foundation are: the weekend math camps and Math is Fun! Camps (abbreviated MaMuT in Hungarian).

Faculty of Mathematics and Physics of Charles University offers maths and computer science programmes open to international students. It also organises manifold conferences, summer schools, camps and competitions for Czech youth such as: an international mathematical competition Náboj, physics competitions FYKOS and Fyziklání and Czech Linguistics Olympiad.

Main Sponsors

The project is co-financed by the Governments of Czechia, Hungary, Poland and Slovakia through Visegrad Grants from **International Visegrad Fund**. The mission of the fund is to advance ideas for sustainable regional cooperation in Central Europe. Grant support is given to original projects namely in the areas of culture, science and research, youth exchanges, cross-border cooperation and tourism promotion, as well as in other priority areas defined in calls for proposals published on the fund's website.

With offices in New York, London, Hong Kong, and Amsterdam, **Jane Street** is a trading firm that operates around the clock and around the globe, trading a wide range of financial products. They are a global liquidity provider and market maker, trading mostly products that are listed on exchanges. They offers internships (as a trader, developer, business developer or researcher) for all university students from freshmen to post-doctoral scholars.

IMC is a leading global market maker, using algorithmic trading and advanced technology to buy and sell securities on multiple trading venues worldwide. They provide liquidity to the financial markets, driving efficiencies for buyers and sellers. They operate globally from offices in Europe, the US and Asia Pacific. Their employees work closely together in multidisciplinary teams, making our success possible. Discover the internship and graduate opportunities at careers.imc.com.

G-Research is the leading quantitative finance research firm. Their Quantitative Research team are some of world's brightest minds. They are working on the fringes of the impossible, trying to beat the efficient market hypothesis with the full "big data" tool set build on the latest academic research into optimisation methods to find innovative solutions to the complexities that Markowitz ignored. They offer a "pure" research role where Researcher's have the freedom to develop and test their ideas with real-world data in an environment that resembles academia. Visit their site at https://www.gresearch.co.uk/

Selected Handouts

Finite Fields in Number Theory

Vladyslav Zveryk

In arctic and tropical climes,
the integers, addition, and times,
taken (mod p) will yield
a full finite field,
as p ranges over the primes.

1. Field Theory and Finite Fields

Definition 1.1. A **field** $(\mathbb{F},+,\cdot)$ is a set with operations $+,\cdot:\mathbb{F}\times\mathbb{F}\to\mathbb{F}$ written as $+(a,b)=:a+b$ and $\cdot(c,d)=:c\cdot d$ and two elements $0,1$ called zero and one respectively such that

1. $a+b=b+a$ for all $a,b\in\mathbb{F}$
2. $a+(b+c)=(a+b)+c$ for all $a,b,c\in\mathbb{F}$
3. $a+0=0+a=a$ for every $a\in\mathbb{F}$
4. for every $a\in\mathbb{F}$ there exists $b\in\mathbb{F}$ denoted $-a$ such that $a+b=0$
5. $a\cdot b=b\cdot a$ for all $a,b\in\mathbb{F}$
6. $a\cdot(b\cdot c)=(a\cdot b)\cdot c$ for all $a,b,c\in\mathbb{F}$
7. $a\cdot 1=1\cdot a=a$ for every $a\in\mathbb{F}$
8. for every $a\in\mathbb{F}\setminus\{0\}$ there exists $b\in\mathbb{F}$ denoted a^{-1} such that $a\cdot b=1$
9. $(a+b)\cdot c=a\cdot c+b\cdot c$ for all $a,b,c\in\mathbb{F}$

Definition 1.2. If $1+\ldots+1=0$ in a field $\mathbb{F}$ for some finite number of ones, then the smallest such number of ones is called the **characteristic** of $\mathbb{F}$. If any finite sum of ones is nonzero, then the characteristic of $\mathbb{F}$ is said to be 0.

During the lecture we will be interested in algebraic extensions of fields. They are given by adjoining roots of polynomials to a field. But while there is a unique way of adjoining a root of an irredicible polynomial to a field, the simultaneous adjoining of two roots of even one polynomial can be problematic.

Consider the following example: a field of polynomial fractions $\mathbb{C}(t)$, its subfield $K:=\mathbb{R}(t^8)$, and a polynomial $f(x)=x^8-t^8$. You can easily check that this polynomial is irreducible in $K[x]$ and

$$f(x)=\prod_{i=0}^{8}(x-\zeta_8^i t),$$

where $\zeta_8 = \frac{\sqrt{2}+i\sqrt{2}}{2}$ is a root of x^8-1 not equal to 1. Now let's adjoin two roots of f to K. First of all, we can choose t and $\zeta_8 t$. Dividing one by another, we get that ζ_8 lies in the field that we get, and we can write $K(t,\zeta_8 t) = \mathbb{R}(\zeta_8, t)$. On the other hand, let's adjoin t and $\zeta_8^2 t$ to K. We will get $\mathbb{R}(\zeta_8^2, t)$, which is easily seen to be a proper subfield of $\mathbb{R}(\zeta_8, t)$. So, adjoining two roots of a polynomial can give even smaller fields than adjoining other two roots (but it is not always the case that one can be considered as a subfield of another)! In other words, if we have a field K and want to adjoin some roots of polynomials to it, then we have to specify how does the addition and multiplication of them work. To deal with this process, we introduce the following notion of the algebraic closure.

Definition 1.3. For a field $\mathbb{F}$, an **algebraic closure** of $\mathbb{F}$ is an algebraic extension $\mathbb{F}^{\mathrm{alg}}$ of $\mathbb{F}$ such that every polynomial in $\mathbb{F}^{\mathrm{alg}}[x]$ splits into linear factors in this field.

To clearify the picture, we have to know that any element of an algebraic extension consists of algebraic numbers. For this, it is enough to show that if α and β are nonzero algebraic numbers, then $\alpha\beta$, $\alpha+\beta$, and α^{-1} are algebraic numbers. We will not prove this in the lecture, but look at Exercise 6.

Theorem 1.4. Let $\mathbb{F}$ be a field. Then there exists an algebraic closure $\mathbb{F}^{\mathrm{alg}}$ of $\mathbb{F}$, which we fix. If L is an algebraic extension of $\mathbb{F}$, it can be considered as a subfield of $\mathbb{F}^{\mathrm{alg}}$. In particular, every two algebraic closures of $\mathbb{F}$ are isomorphic.

Example 1.5. There can be several ways in which L can be considered as a subfield of $\mathbb{F}^{\mathrm{alg}}$. For example, let $\mathbb{F} = \mathbb{Q}$, and consider $\mathbb{Q}^{\mathrm{alg}}$ as a subfield of $\mathbb{C}$ consisting of algebraic numbers over $\mathbb{Q}$. Let $L := \mathbb{Q}(\alpha)$, where α is a root of x^4-2. As a field, L can be described in the following way:

$$L = \left\{ \frac{a_0+a_1\alpha+a_2\alpha^2+a_3\alpha^3}{b_0+b_1\alpha+b_2\alpha^2+b_3\alpha^3} : a_i, b_i \in \mathbb{Q}, (b_1,b_2,b_3,b_4) \neq (0,0,0,0) \right\}$$

with the multiplication as in the field of ractional functions $\mathbb{Q}(x)$ with the difference that $\alpha^4 = 2$. If you solve Exercise 6 then you will even be able to assume that $b_1 = b_2 = b_3 = 0$. You can check that this construction is well-defined, and the abstract field L that we defined can be considered as a subfield of $\mathbb{Q}^{\mathrm{alg}}$ in four ways: we can let α equal to one of $\pm\sqrt[4]{2}, \pm i\sqrt[4]{2}$. But note that the first two embeddings have the same images in $\mathbb{Q}^{\mathrm{alg}}$, while the last two embeddings have the same images in $\mathbb{Q}^{\mathrm{alg}}$, but different from the image of the first two. So, we have got two distincs subfields of $\mathbb{Q}^{\mathrm{alg}}$ which are both isomorphic to L.

Remark 1.6. Algebraic extensions $L/\mathbb{F}$ such that these is only one image of any embedding of L into $\mathbb{F}^{\mathrm{alg}}$ are called **normal**, and they can characterized in the following way: for any irreducible polynomial $f \in \mathbb{F}[x]$, if L contains a root of f, then L contains all roots of f.

Exercise 1.1. Let $\mathbb{F}$ be a field and L be an algebraic extension of F such that every polynomial $f \in \mathbb{F}[x]$ has a root in L. Prove that $L = \mathbb{F}^{\mathrm{alg}}$.

With this theorem, our strategy of adjoining roots will be the following. For a given field $\mathbb{F}$, fix its algebraic closure $\mathbb{F}^{\mathrm{alg}}$. Suppose that we have a family of polynomials $(f_i)_{i\in I}$ in $\mathbb{F}[x]$, and for every $i \in I$ we want to adjoin a_i roots of f_i to $\mathbb{F}$. All fields that we can get in this way are given by choosing for every i elements $x_{i1}, \ldots, x_{ia_i} \in \mathbb{F}^{\mathrm{alg}}$ which are roots of f_i, and taking the field $\mathbb{F} \subset \mathbb{F}(x_{ij}) \subset \mathbb{F}^{\mathrm{alg}}$. In other words, we take roots of polynomials from $\mathbb{F}^{\mathrm{alg}}$ and considering its subfields generated by them.

Theorem 1.7. Let $\mathbb{F}$ be a field, $f \in \mathbb{F}[x]$ a nonconstant polynomial, and $\mathbb{F}^{\text{alg}}$ a fixed algebraic closure of $\mathbb{F}$. Then the roots of f in $\mathbb{F}^{\text{alg}}$ are distinct iff f is coprime with its formal derivative f'.

Definition 1.8. A **finite field** is a field with a finite number of elements. A finite field with q elements is denoted by $\mathbb{F}_q$.

Definition 1.9. Let a field $\mathbb{F}$ be of characteristic p. Then the map $\sigma_p : x \mapsto x^p$ is injective and behaves well with addition and multiplication (hence is so-called homomorphism). It's called a **Frobenius homomorphism**.

Remark 1.10. Frobenius homomorphism a bijection in the case of finite fields, but not only in this case. In fact, any field for which Frobenius map is a bijection is called a **perfect field**. So, finite fields are perfect.

Theorem 1.11 (Classification theorem for finite fields)**.** The following facts about finite fields hold:

1. Let $\operatorname{char}\mathbb{F}_q = p$. Then q is a power of p.
2. Every element $\alpha \in \mathbb{F}_q$ is a root of $x^q - x$. The set $\{\alpha \in \mathbb{F}_p^{\text{alg}} : \alpha^q = \alpha\}$ is a subfield of $\mathbb{F}_p^{\text{alg}}$ with q elements. Thus, for every $q = p^k$ there is a unique finite field with q elements.
3. Let $\mathbb{F}_q$ and $\mathbb{F}_r$ have equal characteristic. Then $\mathbb{F}_q \subset \mathbb{F}_r$ if and only if r is a power of q.

Corollary 1.12. Let $f \in \mathbb{F}_q[x]$ be an irreducible polynomial with roots $\alpha_1, \ldots, \alpha_n$ in the algebraic closure of $\mathbb{F}_q$. Then α_i are pairwise distinct and

$$\{\alpha_1, \alpha_2, \ldots, \alpha_n\} = \{\alpha_1, \alpha_1^{q^1}, \ldots, \alpha_1^{q^{n-1}}\}.$$

In particular, when an irreducible polynomial over $\mathbb{F}_q$ has a root in some $\mathbb{F}_{q^k}$, then all its roots are in $\mathbb{F}_{q^k}$. In the sense of Remark 1.6, this means that finite extensions of finite fields are normal.

Remark 1.13. When we investigated the extensions of $\mathbb{F}_p$, we used the Frobenious homomorphism $\sigma_p : x \mapsto x^p$ which fixed $\mathbb{F}_p$ but had a nontrivial action on any greater field extension on $\mathbb{F}_p$. For any other finite field $\mathbb{F}_q$ the situation is very similar: the automorphism $\sigma_q : x \mapsto x^q$, also called Frobenius, fixes $\mathbb{F}_q$ and moves any greater extension of $\mathbb{F}_q$.

Theorem 1.14 (Gauss's lemma)**.** For a nonzero polynomial $f(x) \in Q[x]$, denote by $c(f)$ the gcd of all its nonzero coefficients (for coefficients in $\mathbb{Q}$ it means that $c(f)$ is a positive number such that $c(f)f$ has coefficients in $\mathbb{Z}$ whose gcd equals 1). If $f(x) = g(x)h(x)$ for two other polynomials $g, h \in \mathbb{Q}[x]$, then $c(f) = c(g)c(h)$. In particular, if $f, g \in \mathbb{Z}[x]$ and $c(g) = 1$, then $h \in \mathbb{Z}[x]$.

Remark 1.15. The Gauss's lemma remains true if $\mathbb{Z}$ is replaced by a factorial ring R, and $\mathbb{Q}$ is replaced by its field of fractions K. For arbitrary rings it looks a bit differently: let R be a ring, and $f(x) \in R[x]$ be a nonzero polynomial. Then the **content** $\operatorname{cont}(f)$ of f is defined to be the ideal of R generated by the coefficients of f. Then we have the inclusion $\operatorname{cont}(gh) \subset \operatorname{cont}(g)\operatorname{cont}(h)$, and this inclusion can be strict. There are a couple of important examples where the equality holds:

1. If $\operatorname{cont}(g)\operatorname{cont}(h) = (1)$, then $\operatorname{cont}(gh) = (1)$.
2. If R is a **Dedekind domain** – a very important class of rings in algebraic number theory.
3. When R is a factorial domain, then $c(f)$ is defined to be a gcd of all elements in $\operatorname{cont}(f)$, and we have $c(gh) = c(g)c(h)$.
4. We have the equality of ideals $(c(f)) = \operatorname{cont}(f)$ for every $f \neq 0$ if and only if R is a principal ideal domain. In fact, every PID is a Dedekind domain, so this example is not new.

2. Primitive Roots of Unity

Definition 2.1. The **Möbius function** is a function $\mu : \mathbb{Z}^+ \to \{-1, 0, 1\}$ such that

$$\mu(n) = \begin{cases} 1, & n \text{ is squarefree and has an even number of prime factors} \\ -1, & n \text{ is squarefree and has an odd number of prime factors} \\ 0, & n \text{ is not squarefree} \end{cases}$$

Theorem 2.2 (Möbius inversion formula)**.** There are two versions of it (in fact, this can be described as one version, but let me split it into two parts to not create confusion about summation and product):

1. Let $f, g : \mathbb{Z}_+ \to G$ be two functions, where G can be any set with commutative addition (a good word for this is an abelian group) that you know (additive group of a field, a ring of polynomials, $\mathbb{Z}$, $\mathbb{Z}/n\mathbb{Z}$). Suppose that these functions satisfy the equality

$$f(n) = \sum_{d|n} g(d)$$

for every positive integer n. Then

$$g(n) = \sum_{d|n} f(d)\mu(n/d)$$

for every $n \in \mathbb{Z}_+$.

2. Let $f, g : \mathbb{Z}_+ \to G$ be two functions, where G can be any set with commutative multiplication that you know (multiplication groups of a field, a ring of polynomials, $\mathbb{Z}$, elements of $\mathbb{Z}/n\mathbb{Z}$ coprime to n). Suppose that these functions satisfy the equality

$$f(n) = \prod_{d|n} g(d)$$

for every positive integer n. Then

$$g(n) = \prod_{d|n} f(d)^{\mu(n/d)}$$

for every $n \in \mathbb{Z}_+$.

Definition 2.3. If the characteristic of $\mathbb{F}$ doesn't divide n, then define a **primitive n-th root of unity** ζ_n to be any root of $x^n - 1$ which is not a root of $x^d - 1$ for any $d < n$.

Definition 2.4. The n-th **cyclotomic polynomial** $\Phi_n \in \mathbb{C}[x]$ is the monic polynomial whose roots are exactly the primitive n-th roots of unity. In fact, $\Phi_n \in \mathbb{Z}[x]$, so we can define Φ_n over any field $\mathbb{F}$ by a natural map of $\mathbb{Z}$ to $\mathbb{F}$.

Theorem 2.5. When the characteristic of $\mathbb{F}$ doesn't divide n, there are $\phi(n)$ primitive n-th roots of unity, and they are exactly the roots of $\Phi_n(x)$.

Corollary 2.6. The multiplicative group $\mathbb{F}_q$ of a finite field is cyclic.

PROOF. Consider ζ_{q-1}. This is an element of $\mathbb{F}_q$ since $\zeta_{q-1}^q = \zeta_{q-1}$. By the definition of ζ_{q-1}, all elements $1, \zeta_{q-1}, \ldots, \zeta_{q-1}^{q-2}$ are distinct. There are $q-1$ of them and $\mathbb{F}_q^*$ has exactly $q-1$ elements, hence

$$\mathbb{F}_q^* = \{1, \zeta_{q-1}, \ldots, \zeta_{q-1}^{q-2}\},$$

as desired. □

REMARK 2.7. Moreover, any finite subgroup of the multiplicative subgroup of any field is cyclic.

THEOREM 2.8. The n-th cyclotomic polynomial is irreducible over $\mathbb{Z}$. Over $\mathbb{F}_p$, where $p \nmid n$ it factors into $\phi(n)/d$ irreducible factors of degree $d = \operatorname{ord}_n p$ each.

THEOREM 2.9. Let $p \nmid n$ be a prime number. Then p divides some value of $\Phi_n(x)$ if and only if $n \mid p-1$.

Exercise 2.1. Let $Q \in \mathbb{F}[x]$ be a polynomial of even degree $2n$, and suppose that $Q(x) = x^{2n}Q(1/x)$. Prove that there exists a unique polynomial $P \in \mathbb{F}[x]$ such that $Q(x) = x^n P(x+1/x)$. This gives us the definition of $\Psi_n(x)$.

DEFINITION 2.10. For $n \geq 3$ let $\Psi_n \in \mathbb{F}[x]$ be the unique polynomial such that

$$\Phi_n(x) = x^{\phi(n)/2}\Psi_n(x+1/x).$$

THEOREM 2.11. When the characteristic of $\mathbb{F}$ doesn't divide n, there are exactly $\phi(n)/2$ numbers of the form $\zeta_n + \zeta_n^{-1}$, where ζ_n is a primitive root of unity, and these numbers are exactly the roots of $\Psi_n(x)$.

THEOREM 2.12. The polynomial $\Psi_n(x)$ is irreducible over $\mathbb{Z}$. Over $\mathbb{F}_p$, where $p \nmid n$ it factors into $\phi(n)/(2d)$ irreducible factors of degree d each, where $d = \operatorname{ord}_n p$ if $2 \nmid \operatorname{ord}_n p$ and $2d = \operatorname{ord}_n p$ if $2 \mid \operatorname{ord}_n p$.

THEOREM 2.13. Let $p \nmid n$ be a prime number. Then p divides some value of $\Psi_n(x)$ if and only if $n \mid p-1$ or $n \mid p+1$.

Exercise 2.2. In this exercise we finish the proof of the fact that there are infinitely many prime numbers of the form $nk-1$.

(i) Let $g \in \mathbb{Z}[x]$ be a polynomial with positive constant term and $g(0) < 0$ and $n \geq 3$ a positive integer. Prove that $g(x)$ has infinitely many prime divisors not of the form $nk+1$.

(ii) Generalize this to a polynomial over $\mathbb{Z}$ with positive constant term that achieves a negative value at some real number.

(iii) Show that $\Psi_n(x)$ achieves negative value at some point. Conclude that there are infinitely many prime divisors of $\Psi_n(x)$ of the form $nk-1$.

3. Discriminant of Polynomials over Finite Fields

DEFINITION 3.1. Let $f \in \mathbb{F}[x]$ be a non-constant polynomial, and $f(x) = (x-\alpha_1)\ldots(x-\alpha_n)$ be its factorization into linear factors in the algebraic closure of $\mathbb{F}$. The number

$$\operatorname{disc}(f) = \Delta(f) := \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)^2 = (-1)^{\frac{n^2-n}{2}} \prod_{i \neq j} (\alpha_i - \alpha_j)$$

is called the **discriminant** of f.

Throughout this section we assume that f has distinct roots, equivalently, $\operatorname{disc}(f)$ is nonzero.

Theorem 3.2. Since $\operatorname{disc}(f)$ is symmetric in terms of α_i, then it's a polynomial of elementary symmetric polynomials of α_i, which are the coefficients of f, hence $\operatorname{disc}(f) \in \mathbb{F}$.

Proposition 3.3. Let $f(x) = x^3 + ax + b$ be a cubic polynomial in $\mathbb{F}[x]$. Then

$$\operatorname{disc}(f) = -4a^3 - 27b^2.$$

If $\operatorname{char}\mathbb{F} \neq 3$, then you can always reduce the polynomial to this case by change of coordinates (it obviously doesn't affect the discriminant).

Theorem 3.4. Let $\mathbb{F}$ be a field with $\operatorname{char}\mathbb{F} \neq 2$ and let f be a cubic polynomial in $\mathbb{F}[x]$ with roots $\alpha_1, \alpha_2, \alpha_3$. Then $\operatorname{disc}(f)$ is a square in $\mathbb{F}$ if and only if $\alpha_2, \alpha_3 \in \mathbb{F}(\alpha_1)$. In other words, it is equivalent to the fact that α_2 and α_3 can be expressed as polynomials of α_1 with coefficients in $\mathbb{F}$.

Proof. Note that

$$f'(\alpha_1) = (\alpha_1 - \alpha_2)(\alpha_1 - \alpha_3) = \frac{\sqrt{\operatorname{disc}(f)}}{\alpha_2 - \alpha_3},$$

so if $\operatorname{disc}(f)$ is a square in $\mathbb{F}$, then $\alpha_2 - \alpha_3 \in \mathbb{F}(\alpha_1)$. But we know that $\alpha_1 + \alpha_2 + \alpha_3 \in \mathbb{F}$ as a symmetric polynomial of α_i, so $\alpha_2 + \alpha_3 \in \mathbb{F}(\alpha_1)$. Then $2\alpha_2, 2\alpha_3 \in \mathbb{F}(\alpha_1)$, and since $\operatorname{char}\mathbb{F} \neq 2$, we can divide by 2 and get that $\alpha_2, \alpha_3 \in \mathbb{F}(\alpha_1)$.

Now suppose that $\alpha_2, \alpha_3 \in \mathbb{F}(\alpha_1)$. Then

$$\sqrt{\operatorname{disc}(f)} = (\alpha_2 - \alpha_3) f'(\alpha_1) \in \mathbb{F}(\alpha_1).$$

We will use the terminology and results from the Exercise 6. We have field extension $\mathbb{F} \subset \mathbb{F}(\sqrt{\operatorname{disc}(f)}) \subset \mathbb{F}(\alpha_1)$. Then $[\mathbb{F}(\sqrt{\operatorname{disc}(f)}) : \mathbb{F}]$ divides $[\mathbb{F}(\alpha_1) : \mathbb{F}]$. Since $\sqrt{\operatorname{disc}(f)}$ is a root of $x^2 - \operatorname{disc}(f) \in \mathbb{F}[x]$, then the degree $[\mathbb{F}(\sqrt{\operatorname{disc}(f)}) : \mathbb{F}]$ is at most 2. On the other hand, since α_1 was a root of an irreducible polynomial of degree 3, then $[\mathbb{F}(\alpha_1) : \mathbb{F}] = 3$. We conclude that the divisibility derived earlier can occur iff $[\mathbb{F}(\sqrt{\operatorname{disc}(f)}) : \mathbb{F}] = 1$, i.e. $\sqrt{\operatorname{disc}(f)} \in \mathbb{F}$. □

Theorem 3.5. Let $\mathbb{F}_q$ be a finite field with $2 \nmid q$ and $f \in \mathbb{F}_q[x]$ be a polynomial which splits into distinct irreducible factors as $f = g_1 g_2 \dots g_k$. Then $\operatorname{disc}(f)$ is a square in $\mathbb{F}_q$ if and only if $2 \mid (\deg f - k)$.

Proof. As we know, $\sqrt{\operatorname{disc}(f)} \in \mathbb{F}_q$ iff $\sqrt{\operatorname{disc}(f)}^q = \sqrt{\operatorname{disc}(f)}$. Writing $\sqrt{\operatorname{disc}(f)}$ as

$$\sqrt{\operatorname{disc}(f)} = \prod_{1 \leq i < j \leq n} (\alpha_i - \alpha_j)$$

and knowing that raising to the q-th power permutes the roots α_i of f, we get that $\sqrt{\operatorname{disc}(f)}^q = \sqrt{\operatorname{disc}(f)}$ iff this permutation is even. Note that this is a product of permutations defined by it on the roots of g_i, and by the Corollary 1.12 it is just a cyclic permutation on the roots of any g_i of length $\deg g_i$. So it's even if and only if

$$2 \Big| \sum_{i=1}^{k} (\deg g_i - 1) = \deg f - k.$$

□

Corollary 3.6. Let f be a cubic polynomial in $\mathbb{F}_q[x]$. Then

- If $\operatorname{disc}(f)$ is a square in $\mathbb{F}_q$, then exactly 3 or 0 roots of f are in $\mathbb{F}_q$.
- If $\operatorname{disc}(f)$ is a square in $\mathbb{F}_q$, then exactly one root of f is in $\mathbb{F}_q$. In particular, if you find that the discriminant of a polynomial $f(x)\in\mathbb{Z}[x]$ is not a square modulo p, then some value of f is divisible by p.

And a tough but nice theorem which I am not going to prove:

Theorem 3.7 (Corollary of Kronecker-Weber theorem)**.** Let f be a cubic polynomial over $\mathbb{Q}$ with $\operatorname{disc}(f)$ being a square in $\mathbb{Q}$. Let α be a root of f. Then there exists $n\in\mathbb{Z}_+$ such that $\mathbb{Q}(\alpha)\subset\mathbb{Q}(\zeta_n)$. I remind you that everything is happening in the algebraic closure of $\mathbb{Q}$, which we fix at the first step when we investigate field extensions.

4. Exercises

4.1. Find all integers a for which there exists a polynomial $p(x)$ with integer coefficients satisfying

$$p\left((\sqrt[3]{a})^2+\sqrt[3]{a}\right)=(\sqrt[3]{a})^2-\sqrt[3]{a}.$$

4.2. Let $\mathbb{F}$ be a field. Show that the gcd of x^n-1 and x^m-1 as polynomials in $\mathbb{F}[x]$ is $x^{\gcd(m,n)}-1$.

4.3. For each $n\in\mathbb{N}$ compute the sum of roots of Φ_n.

4.4. If you haven't seen the Gauss's lemma before, then prove it!

4.5. Let m,n be relatively prime numbers and $x>1$ be a real number such that x^m+x^{-m} and x^n+x^{-n} are integers. Prove that $x+x^{-1}$ is also an integer.

4.6. This problem uses basic facts about vector spaces and their bases. Let $K\subset L$ be a field extension. Consider L as a vector space over K, and denote by $[L:K]$ its dimension over K, which we call **the degree** of a field extension L/K.

(i) Let $\alpha\in K^{\text{alg}}$ be an algebraic element over K. Prove that $1,\alpha,\dots,\alpha^{n-1}$ is a basis of $K(\alpha)$ as a vector space over K, where n is the degree of the minimal polynomial of α. For the fact that they generate $K(\alpha)$ you may use that for any coprime polynomials $f,g\in K[x]$ there exist polynomials a,b such that $fa+bg=1$. Therefore, $[K(\alpha):K]$ equals the degree of the minimal polynomial of α over K.

(ii) Using the fact that subspaces of a finite-dimensional vector space are finite-dimentional, prove that if $[L:K]$ is finite, then every element of L is algebraic over K.

(iii) Prove that if M/L and L/K are two field extensions, then $[M:K]=[M:L]\cdot[L:K]$. In particular, if M/L and L/K are finite, then M/K is finite.

(iv) Conclude that if α and β are algebraic numbers with α being nonzero, then $\alpha+\beta$, $\alpha\beta$, and α^{-1} are algebraic.

4.7. In this exercise, you can use the results from the previous exercise freely.

(i) Prove that $[\mathbb{F}_{q^n}:\mathbb{F}_q]=n$ and any irreducible polynomial of degree dividing n with coefficients in $\mathbb{F}_q$ has all its roots in $\mathbb{F}_q$. A beautiful fact, isn't it?

(ii) Deduce that $\mathbb{F}_p^{\mathrm{alg}}=\bigcup_{n=1}^{\infty}\mathbb{F}_{p^{n!}}$.

(ii) Compute the number of irreducible polynomials of degree n in $\mathbb{F}_q$. If you get a sum with every term known, then it will be enough.

4.8. The aim of this exercise is to prove the Law of Quadratic Reciprocity. Fix two distinct prime numbers $p,q>2$ (this is the only place in the text where q is not a general prime power, but a prime). We will proceed in a few steps:

(i) Let ζ_n be a primitive n-th root of unity and $\tau=a_0+a_1\zeta_n^1+\ldots+a_{\phi(n)-1}\zeta_n^{\phi(n)-1}$ be some number in $\mathbb{Q}(\zeta_n)$. For conveniency, write $\tau=f(\zeta_n)$, where $f(x)=a_0+a_1x+\ldots+a_{\phi(n)-1}x^{\phi(n)-1}$. Prove that $a_1=\ldots=a_{\phi(n)-1}=0$ if and only if $\tau=f(\zeta_n^k)$ for every k coprime with n.

(ii) Let ζ_p be a primitive p-th root of unity. Using (i), compute

$$\left(\sum_{k\in((\mathbb{Z}/p)^*)^2}\zeta_p^k\right)\left(\sum_{\substack{k\in(\mathbb{Z}/p)^*\\ k\notin((\mathbb{Z}/p)^*)^2}}\zeta_p^k\right).$$

Let α be the first number above and β the second one. Compute $\alpha+\beta$ and conclude that $\sqrt{p^*}\in\mathbb{Q}(\zeta_p)$ for $p^*=(-1)^{(p-1)/2}p$.

(iii) State a criterion for p^* to be a quadratic residue modulo q using the Frobenius map σ_q.

(iv) Show the analogue of (ii) over $\mathbb{F}_q=\mathbb{Z}/q\mathbb{Z}$ instead of $\mathbb{Q}$. Show that q is a quadratic residue modulo p if and only if $\alpha^q=\alpha$. Finish the proof of the Law of Quadratic Reciprocity.

4.9. I found a strange problem in the Titu Andreescu's and Gabriel Dospinescu's book "Problems from the book": „Prove that for any positive integer n every number of the form $\sqrt{n+1}-\sqrt{n}$ can be expressed as $2\cos\left(\frac{2k\pi}{m}\right)$ for some integers k,m". Prove that this statement is true only for finitely many n.

4.10. Here are some further properties of cyclotomic polynomials.

(i) Given n, let $m=\prod_{p|n}p$. Prove that $\Phi_n(x)=\Phi_m\left(x^{n/m}\right)$. This shows that we can reduce computing $\Phi_n(x)$ to the case when n is squarefree.

(ii) Let $n>1$ be an odd integer. Prove that $\Phi_{2n}(x)=\Phi_n(-x)$.

(iii) Let p be a prime not dividing an integer $n>1$. Prove that $\Phi_{pn}(x)=\Phi_n\left(x^p\right)/\Phi_n(x)$.

4.11. Show that the polynomial $f(x)=x^4-10x^2+1$ is irreducible in $\mathbb{Z}[x]$ but reducible in each $\mathbb{F}_p[x]$. Find an example of a polynomial in $\mathbb{Z}[x]$ which has no roots in $\mathbb{Q}$ but has a root modulo any prime number. As you see, such things may happen.

4.12. Let $p_1,p_2,\ldots,p_n$ be distinct odd primes. Show that $2^{p_1p_2\cdots p_n}+1$ has at least $2^{2^{n-1}}$ divisors.

4.13. Prove that there exist infinitely many positive integers n such that all prime divisors of n^2+n+1 are not greater than $\sqrt{n}$.

4.14. Let b, m, n be positive integers such that b^n-1 and b^m-1 have the same prime factors. Prove that $b+1$ is a power of 2.

4.15. Find all prime numbers p such that there exists a unique $a\in\mathbb{F}_p$ for which $a^3-3a+1=0$ (you may possibly solve it without any knowledge you could have got in the lecture). You can also prove that all prime divisors of a^3-3a+1 are either equal 3 or of the form $9k\pm1$.

4.16. Given a positive integer a, prove that all divisors of $7a^2(a+1)-1$ are of the form $7k\pm1$.

5. Solutions

5.1. Find all integers a for which there exists a polynomial $p(x)$ with integer coefficients satisfying

$$p\left((\sqrt[3]{a})^2+\sqrt[3]{a}\right)=(\sqrt[3]{a})^2-\sqrt[3]{a}.$$

Solution. First we show that $\beta:=(\sqrt[3]{a})^2+\sqrt[3]{a}$ is a root of some monic polynomial of degree 3. Indeed,

$$\begin{aligned}\beta^3&=a(3(\sqrt[3]{a})^2+3\sqrt[3]{a}+a+1),\\ \beta^2&=(\sqrt[3]{a})^2+a\sqrt[3]{a}+2a,\\ \beta&=(\sqrt[3]{a})^2+\sqrt[3]{a},\\ 1&=1,\end{aligned}$$

so we may note that β is a root of $f(x)=x^3+3x^2-(3a+9)x-7a-1$. Thus, we may divide p by f with remainder and assume that $\deg p\le 2$. Write then $p(x)=cx^2+dx+e$. We get

$$(\sqrt[3]{a})^2-\sqrt[3]{a}=(c+d)(\sqrt[3]{a})^2+(ac^2+d)\sqrt[3]{a}+(2ac+e). \tag{5.1}$$

Now note that if a is a cube in $\mathbb{Z}$, then a polynomial p obviously exists. So suppose that a is not a cube in $\mathbb{Z}$. Then $\sqrt[3]{a}$ is not a root of polynomial of degree 2, hence the equation 5.1 leads to the following system of equations:

$$\begin{aligned}c+d-1&=0\\ ac^2+d+1&=0\\ 2ac+e&=0.\end{aligned}$$

Subtracting the first two equations from each other we get $ac^2-c+2=0$. From this we get that $c^2\mid c-2$ which is only possible for $c=-2,-1,1,2$. In these cases we have respectively $a=-1,-3,-1,0$. Since we supposed that a is not a cube, the only possibility is $a=-3$. It's easy to check that for $a=-3$ the system considered has a solution, hence $a=-3$ fits our conditions. □

5.2. Let $\mathbb{F}$ be a field. Show that the gcd of x^n-1 and x^m-1 as polynomials in $\mathbb{F}[x]$ is $x^{\gcd(m,n)}-1$.

Solution. Write $(m,n)=am+bn$ for some $a,b\in\mathbb{Z}$. Then

$$x^{\gcd(m,n)}-1=x^{am+bn}-1=(x^m)^a\cdot(x^n)^b-1,$$

and if some $f(x)$ divides both x^n-1 and x^m-1, then x^m and x^n are 1 modulo f, hence $(x^m)^a\cdot(x^n)^b$ is one modulo f (why can you do this argument with a or b negative?). Thus $x^{\gcd(m,n)}-1$ is divisible the gcd of x^m-1 and x^n-1, and it divides it by trivial reasons. □

Remark 5.1. The fact is true in a more general situation: Let R be a factorial ring (a UFD) and take $x \in R$. Then the gcd of $x^n - 1$ and $x^m - 1$ is $x^{\gcd(m,n)} - 1$. The proof is the same.

5.3. Let m, n be relatively prime numbers and $x > 1$ be a real number such that $x^m + x^{-m}$ and $x^n + x^{-n}$ are integers. Prove that $x + x^{-1}$ is also an integer.

Solution. The statement is obviously true for $x = \pm 1$. For $x \neq \pm 1$ note that the gcd of $(y^n - x^n)(y^n - x^{-n})$ and $(y^m - x^m)(y^m - x^{-m})$ as polynomials of y equals $(y - x)(y - x^{-1})$. The first two polynomials have integer coefficients, hence the third one does, and we are done. □

5.4. For each $n \in \mathbb{N}$ compute the sum of roots of Φ_n.

Solution. Let $f : \mathbb{Z}_+ \to R$ be the the function such that $f(n)$ equals the sum of roots of $\Phi_n(x)$. By the formula

$$x^n - 1 = \prod_{d|n} \Phi_n(x)$$

we get that

$$\sum_{d|n} f(d) = \begin{cases} 0, & n > 1 \\ 1, & n = 1 \end{cases},$$

so by Möbius inversion be get that $f(n) = \mu(n)$. □

5.5. If you haven't seen the Gauss's lemma before, then prove it!

Solution. Since the function $c(-)$ is multiplicative with respect to multiplication by constant, so we can multiply g by $c(g)^{-1}$ and h by $c(h)^{-1}$, so that we get $c(g) = c(h) = 1$ and want to prove that $c(gh) = 1$. It is easy to see from the definition of $c(-)$ that g and h have integer coefficients, and their gcd-s are equal to 1. We know that $c(gh)$ is the gcd of the coefficients of g and h, and suppose that it's divisible by some prime p. Then, looking at g and h modulo p, we get that they are nonzero polynomials with coefficients in $\mathbb{F}_p$ whose product is the zero polynomial. This is clearly impossible, so we get a contradiction. □

5.6. This problem uses basic facts about vector spaces and their bases. Let $K \subset L$ be a field extension. Consider L as a vector space over K, and denote by $[L : K]$ its dimension over K, which we call **the degree** of a field extension L/K.

(i) Let $\alpha \in K^{\text{alg}}$ be an algebraic element over K. Prove that $1, \alpha, \ldots, \alpha^{n-1}$ is a basis of $K(\alpha)$ as a vector space over K, where n is the degree of the minimal polynomial of α. For the fact that they generate $K(\alpha)$ you may use that for any coprime polynomials $f, g \in K[x]$ there exist polynomials a, b such that $fa + bg = 1$. Therefore, $[K(\alpha) : K]$ equals the degree of the minimal polynomial of α over K.

(ii) Using the fact that subspaces of a finite-dimensional vector space are finite-dimentional, prove that if $[L : K]$ is finite, then every element of L is algebraic over K.

(iii) Prove that if M/L and L/K are two field extensions, then $[M : K] = [M : L] \cdot [L : K]$. In particular, if M/L and L/K are finite, then M/K is finite.

(iv) Conclude that if α and β are algebraic numbers with α being nonzero, then $\alpha + \beta$, $\alpha\beta$, and α^{-1} are algebraic.

Solution. We prove the statements one-by-one.

(i) Let $f(x)$ be the minimal polynomial of α, i.e. the monic nonzero polynomial over K of the smallest degree vanishing at α. If $g \in K[x]$ vanishes in α, then we have that $\gcd(f,g) \in K[x]$ also vanishes in α, and since f was of minimal degree, then $f|g$.

Note that $1, \alpha, \ldots, \alpha^{n-1}$ are linearly independent, since any linear combination of them equal to 0

$$0 = a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}$$

would give a polynomial $g(x) = a_0 + a_1 x + \ldots + an - 1x^{n-1}$ which vanishes in α, and since the degree of g is less than n we must have $g \equiv 0$, i.e. the linear combination is trivial. To prove that $1, \alpha, \ldots, \alpha^{n-1}$ generate $K(\alpha)$, recall that

$$K(\alpha) = \left\{ \frac{a(\alpha)}{b(\alpha)} : a, b \in K[x], b(\alpha \neq 0), \deg a \leq n-1, \deg b \leq n-1 \right\}.$$

Note that since $b(\alpha) \neq 0$, then it is coprime to f, hence there exist polynomials $p, q \in K[x]$ such that $pf + bq = 1$. Letting $x = \alpha$ to both sides of this equality, we get $b(\alpha)q(\alpha) = 1$, i.e. the number $a(\alpha)/b(\alpha)$ can be written as $a(\alpha)q(\alpha)$, i.e. a polynomial of α. Getting rid of terms which are of degree greater than n, we finally get that

$$K(\alpha) = \{a(\alpha) : a \in K[x], \deg a \leq n-1\}.$$

The number $a(\alpha)$ is a linear combination of $1, \alpha, \ldots, \alpha^{n-1}$ generate $K(\alpha)$, so we are done.

(ii) Take $\alpha \in L$. Since L/K is finite-dimensional, then the elements $1, \alpha, \alpha^2, \ldots$ cannot be linearly independent, so there exists a nontrivial linear combination of a finite number of them which equals to 0:

$$0 = a_0 + a_1\alpha + \ldots + a_{n-1}\alpha^{n-1}.$$

This gives us that α is a root of $a_0 + a_1 x + \ldots + a_{n-1}x^{n-1}$, hence is algebraic over K.

(iii) If $\{\alpha_i : i \in I\}$ and $\{\beta_i : i \in I\}$ are bases for L/K and M/L respectively, then $\{\alpha_i\beta_j : i \in I, j \in J\}$ is a basis for M/L, so we are done.

(iv) We know by the first item that $K(\alpha)/K$ is finite-dimensional and $K(\alpha)(\beta)/K(\alpha)$ is finite-dimentional, hence by the precious item $K(\alpha,\beta)/K$ is finite-dimentional. Hence we get that $K(\gamma)/K$ is finite-dimensional for every $\gamma \in K(\alpha,\beta)$, hence every such γ is algebraic over K. In particular, we can take $\gamma = \alpha + \beta, \alpha\beta, \alpha^{-1}$ (if $\alpha \neq 0$).

□

5.7. In this exercise, you can use the results from the previous exercise freely.

(i) Prove that $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$ and any irreducible polynomial of degree dividing n with coefficients in $\mathbb{F}_q$ has all its roots in $\mathbb{F}_q$. A beautiful fact, isn't it?

(ii) Deduce that $\mathbb{F}_p^{\text{alg}} = \bigcup_{n=1}^{\infty} \mathbb{F}_{p^{n!}}$.

(iii) Compute the number of irreducible polynomials of degree n in $\mathbb{F}_q$. If you get a sum with every term known, then it will be enough.

Solution. It goes as follows:

(i) We know that $\mathbb{F}_{q^n}$ is a finite-dimentional vector space over $\mathbb{F}_q$, hence if the length of its basis equals k then it contains $q^k = q^n$ elements, therefore $k = n$ and $[\mathbb{F}_{q^n} : \mathbb{F}_q] = n$. If an irreducible polynomial $f \in \mathbb{F}_q[x]$ has degree n, then by item (i) of the previous problem we have $[\mathbb{F}_q(\alpha) : \mathbb{F}_q] = n$ for any its root α, thus $\mathbb{F}_q(\alpha)$ contains exactly q^n elements. But there is only one finite field of q^n elements, hence $\mathbb{F}_q(\alpha) = \mathbb{F}_{q^n}$, so $\mathbb{F}_{q^n}$ contains all roots of f. Recall that if $d \mid n$ then $F_{q^d} \subset \mathbb{F}_{q^n}$, so the statement of the problem is proven.

(ii) We have seen that you get a finite field when you adjoin an algebraic number to $\mathbb{F}_p$, and any finite field is contained in the given union, so we are done.

(iii) Let $f(n)$ be the number of irreducible polynomials of degree n in $\mathbb{F}_q$. Take $\mathbb{F}_{q^n}$, and for every irreducible polynomial in $\mathbb{F}_q$ of degree $d \mid n$ we can attach to it the set of its roots in $\mathbb{F}_{q^n}$. For different monic irreducible polynomials we get nonintersecting sets of their roots, and $\mathbb{F}_{q^n}$ becomes split into such sets of roots because if you take $\alpha \in \mathbb{F}_{q^n}$, then the degree of its minimal polynomial which equals $[\mathbb{F}_q(\alpha) : \mathbb{F}_q]$ divides $n = [\mathbb{F}_{q^n} : \mathbb{F}_q]$ by the item (iii) from the previous exercise. Thus

$$q^n = \#\mathbb{F}_{q^n} = \sum_{d|n} df(d).$$

Using Möbius Inversion Formula, we finally obtain

$$f(n) = \frac{1}{n} \sum_{d|n} q^d.$$

□

5.8. The aim of this exercise is to prove the Law of Quadratic Reciprocity. Fix two distinct prime numbers $p, q > 2$. We will proceed in a few steps:

(i) Let ζ_n be a primitive n-th root of unity and $\tau = a_0 + a_1\zeta_n^1 + \ldots + a_{\phi(n)-1}\zeta_n^{\phi(n)-1}$ be some number in $\mathbb{Q}(\zeta_n)$. For conveniency, write $\tau = f(\zeta_n)$, where $f(x) = a_0 + a_1 x + \ldots + a_{\phi(n)-1}x^{\phi(n)-1}$. Prove that $a_1 = \ldots = a_{\phi(n)-1} = 0$ if and only if $\tau = f(\zeta_n^k)$ for every k coprime with n.

(ii) Let ζ_p be a primitive p-th root of unity. Compute

$$\left(\sum_{k \in ((\mathbb{Z}/p)^*)^2} \zeta_p^k \right) \left(\sum_{\substack{k \in (\mathbb{Z}/p)^* \\ k \notin ((\mathbb{Z}/p)^*)^2}} \zeta_p^k \right).$$

Let α be the first number above and β the second one. Compute $\alpha + \beta$ and conclude that $\sqrt{p^*} \in \mathbb{Q}(\zeta_p)$ for $p^* = (-1)^{(p-1)/2}p$.

(iii) State a criterion for p^* to be a quadratic residue modulo q using the Frobenius map σ_q.

(iv) Show the analogue of (ii) over $\mathbb{F}_q = \mathbb{Z}/q\mathbb{Z}$ instead of $\mathbb{Q}$. Show that q is a quadratic residue modulo p if and only if $\alpha^q = \alpha$. Finish the proof of the Law of Quadratic Reciprocity.

Solution. We prove the statements one-by-one:

(i) Compute the following:

$$\begin{aligned}\phi(n)\tau &= \sum_{\substack{(k,n)=1\\1\le k<n}} f(\zeta_n^k)\\ &= \sum_{i=0}^{\phi(n)-1} a_i \sum_{\substack{(k,n)=1\\1\le k<n}} \zeta_n^{ik}.\end{aligned}$$

Now look at the sequence $(ik)_{(k,n)=1}$ modulo n. We will show that every element appears here the same number of times. Indeed, look at the set $H_i := \{1 \le k < n : (k,n) = 1, ik \equiv i \pmod n\}$. Note that $ki \equiv li \pmod n$ iff $kl^{-1} \in H_i$. This implies that every element of $(ik)_{(k,n)=1}$ appears here $\phi(n)/|H_i|$ times (so $|H_i| \,|\, \phi(n)$). Note also that

$$\{\zeta_n^{ik} : (k,n) = 1\} = \{\zeta_{n/(i,n)}^{l} : (l, n/i) = 1\},$$

where we used the equality $\zeta_n^i = \zeta_{n/(i,n)}$ (just apply definition of primitive root of unity). Using these two facts, we get

$$\begin{aligned}\phi(n)\tau &= \sum_{i=0}^{\phi(n)-1} a_i \sum_{\substack{(k,n)=1\\1\le k<n}} \zeta_n^{ik}\\ &= \sum_{i=0}^{\phi(n)-1} a_i \frac{\phi(n)}{|H_i|} \sum_{\substack{(l,n/(i,n))=1\\1\le l<n/(i,n)}} \zeta_{n/(i,n)}^{l}\\ &= \sum_{i=0}^{\phi(n)-1} a_i \frac{\phi(n)}{|H_i|} b_{n/(i,n)},\end{aligned}$$

where $-b_{n/(i,n)}$ is the coefficient to $x^{\phi(n/(i,n))-1}$ of $\Phi_{n/(i,n)}(x)$ (the numbers $\zeta_{n/(i,n)}^{l}$ form the list of roots of $\Phi_{n/(i,n)}(x)$). In particular, $b_{n/(i,n)}$ are integers, hence $\phi(n)\tau$ is an integer. Thus $f(x) - \tau \in \mathbb{Q}[x]$ and ζ_n is its root. Then, since $\Phi_n(x)$ is irreducible, it should divide $f(x) - \tau$. But $f(x) - \tau$ has degree smaller than $\Phi_n(x)$, hence $f(x) - \tau \equiv 0$, which implies that $a_0 = \tau$ and $a_1 = \ldots = a_{\phi(n)-1} = 0$.

(ii) Note that raising ζ_p to the k-th power fixes α and β if k is a square modulo p and permutes them if k is not a square modulo p. In any case, it fixes $\alpha\beta$, hence by the previous item we get that $\alpha\beta$ is a rational number. Opening the brackets, we can write

$$\alpha\beta = \sum_{0 \le i \le p-1} a_i \zeta_p^i,$$

where a_i is the number of pairs (k,l) with $1 \le k, l \le p-1$, $k + l \equiv i \pmod p$, $k \in ((\mathbb{Z}/p)^*)^2$, and $l \notin ((\mathbb{Z}/p)^*)^2$. So we see that ζ_p is the root of

$$f(x) = a_0 - \alpha\beta + a_1 x + \ldots + a_{p-1} x^{p-1},$$

hence $f(x) \,|\, 1 + x + \ldots + x^{p-1}$ (recall that this polynomial is irreducible and has ζ_p as a root), thus $a_0 - \alpha\beta = a_1 = \ldots = a_p$. Note that $a_0 + a_1 + \ldots + a_{p-1}$ is the number of pairs (k,l) with $k \in ((\mathbb{Z}/p)^*)^2$

and $l \notin ((\mathbb{Z}/p)^*)^2$, so it equals $(p-1)^2/4$. Therefore

$$\frac{(p-1)^2}{4} - \alpha\beta = a_0 - \alpha\beta + a_1 + \ldots + a_{p-1} = p(a_0 - \alpha\beta),$$

so we conclude that $\alpha\beta = \frac{p}{p-1}a_0 + \frac{1-p}{4}$. If $p \equiv 1 \pmod 4$, then k and $-k$ are both quadratic residues or are both non-residues, hence $a_0 = 0$, so $\alpha\beta = \frac{1-p}{4}$ in this case. If $p \equiv -1 \pmod 4$, then $k \in ((\mathbb{Z}/p)^*)^2$ implies that $-k \notin ((\mathbb{Z}/p)^*)^2$. It follows that $a_0 = \frac{p-1}{2}$, hence $\alpha\beta = \frac{1+p}{4}$. In both cases, we have $\alpha\beta = \frac{1-p^*}{4}$, as desired.

Note that $\alpha+\beta = \sum_{i=0}^{p-1} \zeta_p^i = -1$, hence by the previous result α and β are the roots of $x^2 + x + \frac{1-p^*}{4}$. This implies that $\alpha, \beta = \frac{-1 \pm \sqrt{p^*}}{2}$, so in particular $\sqrt{p^*} \in \mathbb{Q}(\zeta_p)$.

(iii) That's the criterion that we used many times: p^* is a square in $\mathbb{F}_q$ iff $\sqrt{p^*}^q = \sqrt{p^*}$ in $\mathbb{F}_q(\sqrt{p^*})$.

(iv) Note that raising to q-th power either fixes α and β, or permutes them. Thus, $(\alpha\beta)^q = \alpha\beta$, so $\alpha\beta \in \mathbb{F}_q$. We may proceed in the same way as in (ii), but there are two arguments that will not work in this case. The first one is that $1 + x + \ldots + x^{p-1}$ is irreducible. But we don't need it: we know that a_i depend only on p, hence modulo q we will get that $a_1 = \ldots = a_{p-1}$. Then

$$0 = f(\zeta_p) = a_0 - \alpha\beta + a_1(\zeta_p + \ldots + \zeta_p^{p-1}) = a_0 - \alpha\beta + a_1,$$

so the equality $a_0 - \alpha\beta = a_1$ is also true here. The second argument that may not work is that we cannot divide by $p-1$ which can be 0 when $q \mid p-1$. To get rid of this, we may just assume that $q > p$. With this assumptions, we've got that the similar result holds for $\mathbb{F}_q$.

Concluding, we have that q is a quadratic residue modulo p iff $\alpha^q = \alpha$, which is true iff $\alpha \in \mathbb{F}_q$, which holds iff $\sqrt{p^*} \in \mathbb{F}_q$, and this is equivalent to the fact that p^* is a quadratic residue modulo q. Therefore,

$$\left(\frac{q}{p}\right) = \left(\frac{(-1)^{(p-1)/2}p}{q}\right) = \left(\frac{(-1)^{(p-1)/2}}{q}\right)\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{p}{q}\right),$$

and we are done. □

Remark 5.2. You may be wondering if we could had in some sense looked at ζ_p, α, and β modulo q and had not considered the proof of (ii) again. In fact, we can do this in this case. Suppose that you have a monic irreducible polynomial $f \in \mathbb{Z}[x]$ and its root τ in $\mathbb{C}$. Let $f = g_1^{\alpha_1} \ldots g_k^{\alpha_k}$ be the factorization of f into irreducible factors over $\mathbb{F}_q$, and let σ be a root of g_1 in the algebraic closure of $\mathbb{F}_q$. Then there exists a map from $\mathbb{Z}[\tau]$ to $\mathbb{F}_p(\sigma)$ sending τ to σ. It's given by

$$\mathbb{Z}[\tau] \simeq \mathbb{Z}[x]/(f(x)) \to \mathbb{Z}[x]/(g_i(x), q) \simeq (\mathbb{Z}/q)[x]/(g_i(x)) \simeq \mathbb{F}_q(\sigma).$$

You can in fact construct this map without dividing by ideals, just by defining it and checking if it's well-defined and is a homomorphism. In our case $\alpha, \beta \in \mathbb{Z}[\zeta_p]$, so by sending ζ_p over $\mathbb{Z}$ to ζ_p over $\mathbb{F}_q$ you map α, β, and $\sqrt{p^*}$ to the same objects in $\mathbb{F}_q$, so the facts that we were proving for them are indeed true.

Remark 5.3. You can use Ψ_8 to prove the criterion for 2 to be a quadratic residue modulo p. Just note that $\Psi_8(x) = x^2 - 2$, and this implies that 2 is a quadratic residue modulo 2 iff $p \equiv \pm 1 \pmod 8$.

5.9. I found a strange problem in the Titu Andreescu's and Gabriel Dospinescu's book "Problems from the book": „Prove that for any positive integer n every number of the form $\sqrt{n+1}-\sqrt{n}$ can be expressed as $2\cos\left(\frac{2k\pi}{m}\right)$ for some integers k,m". Prove that this statement is true only for finitely many n.

Solution. Let's consider only $n\geq 3$. Suppose that $\sqrt{n+1}-\sqrt{n}=2\cos\left(\frac{2k\pi}{m}\right)$. Look at the sequence of polynomials:

$$f_n(x)=\prod(x\pm\sqrt{n+1}\pm\sqrt{n})=x^4-(4n+2)x^2+1.$$

We have that $2\cos\left(\frac{2k\pi}{m}\right)$ is a root of $f_n(x)$ and $f_n(x)\in\mathbb{Z}[x]$. Note that $2\cos\left(\frac{2k\pi}{m}\right)=\zeta_m^k+\zeta_m^{-k}$ is a root of $\Psi_n(x)$, so since Ψ_n is irreducible we get that $\Psi_n(x)\mid f_n(x)$. Then $\deg\Psi_n(x)=\phi(n)/2\leq 4$, which is true only for finitely many n. □

5.10. Here are some further properties of cyclotomic polynomials.

(i) Given n, let $m=\prod_{p\mid n}p$. Prove that $\Phi_n(x)=\Phi_m\left(x^{n/m}\right)$. This shows that we can reduce computing $\Phi_n(x)$ to the case when n is squarefree.

(ii) Let $n>1$ be an odd integer. Prove that $\Phi_{2n}(x)=\Phi_n(-x)$.

(iii) Let p be a prime not dividing an integer $n>1$. Prove that $\Phi_{pn}(x)=\Phi_n\left(x^p\right)/\Phi_n(x)$.

Solution. It is convenient to use the complex case: let $\zeta_n=e^{-\frac{2\pi i}{n}}$, and then just compare the roots of the left-hand sides and the right-hand sides. □

5.11. Show that the polynomial $f(x)=x^4-10x^2+1$ is irreducible in $\mathbb{Z}[x]$ but reducible in each $\mathbb{F}_p[x]$.

Solution. First note that modulo 2 the given polynomial factors as $(x+1)^4$, and modulo 3 it equals $(x^2+1)^2$. From this point, assume that we are considering primes greater than 3. It's easy to see that the roots of x^4-10x^2+1 are $\pm\sqrt{5\pm 2\sqrt{6}}=\pm(\sqrt{3}\pm\sqrt{2})$. Look at the following three quadratic divisors of x^4-10x^2+1:

$$(x-(\sqrt{2}+\sqrt{3}))(x+(\sqrt{2}+\sqrt{3}))=x^2-5-2\sqrt{6}$$
$$(x-(\sqrt{2}-\sqrt{3}))(x-(\sqrt{2}+\sqrt{3}))=x^2-2\sqrt{2}x-1$$
$$(x-(\sqrt{3}-\sqrt{2}))(x-(\sqrt{2}+\sqrt{3}))=x^2-2\sqrt{3}x+1$$

Since at least one of 2, 3, and $2\cdot 3=6$ is a quadratic residue modulo every prime $p>3$, we get that at least one of the polynomials written above lies in $\mathbb{F}_p[x]$, hence x^4-10x^2+1 is not irreducible in $\mathbb{F}_p[x]$ for every $p>3$, as desired. □

5.12. Let $p_1,p_2,\ldots,p_n$ be distinct odd primes. Show that $2^{p_1p_2\cdots p_n}+1$ has at least $2^{2^{n-1}}$ divisors.

Solution. Using the fact that p_i are odd we get

$$2^{p_1\cdots p_n}+1=\frac{2^{2p_1\cdots p_n}-1}{2^{p_1\cdots p_n}-1}=\frac{\prod_{d\mid 2p_1\ldots p_n}\Phi_d(2)}{\prod_{d\mid p_1\ldots p_n}\Phi_d(2)}=\prod_{d\mid p_1\ldots p_n}\Phi_{2d}(2).$$

We will show that every $\Phi_{2d}(2)$ has a prime divisor and that every prime divisor of $2^{p_1\cdots p_n}+1$ divides at most two of $\Phi_{2d}(2)$, $d\mid p_1\ldots p_n$. There are 2^n divisors of $p_1\ldots p_n$, so this will imply

that there are at least 2^{n-1} prime numbers dividing $2^{p_1\dots p_n}+1$, hence at least $2^{2^{n-1}}$ divisors of this number.

Let's show that $\Phi_k(x)$ has a prime divisor for $k\geq 2$ and $x\geq 2$. By the obvious inequalities

$$x^d > x^d - 1 \geq \frac{x-1}{x}x^d$$

we have

$$\Phi_k(x) = \prod_{d|k}(x^d-1)^{\mu(k/d)} > \prod_{d|k} x^{d\mu(k/d)}\left(\frac{x-1}{x}\right)^{t(n)},$$

where $t(n)$ is the number of $d\,|\,n$ such that $\mu(n/d)=1$, i.e. half the number of squarefree divisors of n. When $n=p_1^{\alpha_1}\dots p_k^{\alpha_k}$, then it equals $2^k/2=2^{k-1}\leq\phi(n)$. So

$$\Phi_k(x) > \prod_{d|k} x^{d\mu(k/d)}\left(\frac{x-1}{x}\right)^{\phi(n)} = x^{\phi(n)}\cdot\left(\frac{x-1}{x}\right)^{\phi(n)} = (x-1)^{\phi(n)} \geq 1,$$

where the first equality follows from Möbius inversion formula applied to $k=\sum_{d|k}\phi(k)$. It follows that $\Phi_k(x)$ has a prime divisor, in particular in our case $x=2$.

Suppose that $p\,|\,\Phi_{2d}(2)$, where $d\,|\,p_1\dots p_n$. We know that this is the case when $2d=\mathrm{ord}_p 2$, and if $2d\neq\mathrm{ord}_p 2$, then we must have $p\,|\,2d$. Take a prime divisor q of d. Then we have

$$p\,|\,\Phi_{2d}(2)\,|\,\frac{2^d+1}{2^{d/q}+1},$$

which implies that $p\nmid 2^{d/q}+1$ (otherwise we get a contradiction with LTE), so $\frac{1}{2}\mathrm{ord}_p 2$ is divisible by any prime divisor of d different from p. Thus, using the fact that d is squarefree, we finally get $d=\frac{p}{2}\mathrm{ord}_p 2$. This finishes the proof that every prime number divides at most two $\Phi_{2d}(2)$, so we are done. □

5.13. Prove that there exist infinitely many positive integers n such that all prime divisors of n^2+n+1 are not greater than $\sqrt{n}$.

Solution. We are working with $\Phi_3(n)$, so the ideas should be based on the formulas with cyclotomic polynomials. We will substitute $n:=k^m$ for some integers k,m, so let's investigate $\Phi_3(x^m)$ first. Take m coprime to 3. We have

$$\Phi_3(x^m) = \frac{x^{3m}-1}{x^m-1} = \frac{\prod_{d|3m}\Phi_d(x)}{\prod_{d|m}\Phi_d(x)} = \prod_{d|m}\Phi_{3d}(x),$$

where the last equality was obtained after cancelling all the terms $\Phi_d(x)$ with $3\nmid d$. Every $\Phi_{3d}(x)$ grows approximately as $x^{\phi(3d)}\leq x^{2\phi(m)}$. We want this to be less than $x^{m/2}$, so equivalently $4<m/\phi(m)$. This can be obtained by $m=210p$ for p a prime number greater than 7. □

Remark 5.4. We have proven a part of the following property of cyclotomic polynomials: for positive integers m,n with $(m,n)=1$ we have

$$\Phi_n(x^m) = \prod_{d|m}\Phi_{dn}(x)$$

Remark 5.5. You may prove that for every degree 2 polynomial $f \in \mathbb{Z}[x]$ and every positive number C there exists a positive integer n such that the greatest prime divisor of $f(n)$ is at most Cn. It's not known if the similar fact is true even for degree 3 polynomials.

5.14. Let b, m, n be positive integers such that b^n-1 and b^m-1 have the same prime factors. Prove that $b+1$ is a power of 2.

Solution. Suppose that $b+1$ is not a power of 2. First of all, $(b^m-1, b^n-1) = b^{(m,n)}-1$, so we may assume that $m \mid n$. Then, since no new prime number appears in the factorization of x^n-1 different from primes dividing x^m-1, we must have that $p \mid \Phi_n(b)$ implies $p \mid n$. Since $\Phi_n(x)$ divides $(x^n-1)/(x^{n/2}-1)$, we get

$$\nu_p(\Phi_n(b)) \le \nu_p(x^n-1) - \nu_p(x^{n/p}-1).$$

Then by LTE-lemma

$$\nu_p(\Phi_n(b)) \le \begin{cases} 1 & p \neq 2 \\ \nu_2(b^{n/2}+1) & ,p=2. \end{cases}$$

Then, writing $n = 2^\alpha p_1^{\alpha_1} \dots p^{\alpha_k}$ we get that

$$\Phi_n(b) \le 2^{\nu_2(b^{n/2}+1)} p_1 \dots p_k.$$

Using the estimation that we've derived in the Problem 7 and $t(n) \le 2^k$ we get

$$b^{(p_1-1)\dots(p_k-1)} \left(\frac{b-1}{b}\right)^{2^k} \le b^{\phi(n)} \left(\frac{b-1}{b}\right)^{t(n)} < \Phi_n(b) \le 2^{\nu_2(b^{n/2}+1)} p_1 \dots p_k \le \frac{b+1}{3} p_1 \dots p_k, \quad (5.2)$$

where in the last inequality we used that $b+1$ is not a power of 2, hence equals at least $3 \cdot 2^{\nu_2(b^{n/2}+1)}$.

Suppose that $k \ge 1$ and $b \ge 4$, and we will show that the LHS of 5.2 is not smaller than RHS. Suppose that $k \ge 1$ then. Note that as b increases by 1, then the LHS becomes multiplied by at least $(b+1)^2/b^2$, the RHS becomes multiplied by $(b+2)/(b+1) < (b+1)^2/b^2$, so it's enough to prove our claim for $b=3$, i.e. that

$$2^{2(p_1-1)\dots(p_k-1)-2^k} = 4^{(p_1-1)\dots(p_k-1)-2^k} \cdot 2^{2^k} \ge p_1 \dots p_k.$$

Using $p_i \le 2^{p_i-1}$, it's enough to prove that

$$2^{2(p_1-1)\dots(p_k-1)-2^k-p_1-\dots-p_k+k} \ge 1 \Leftrightarrow 2(p_1-1)\dots(p_k-1) \ge 2^k + p_1 + \dots + p_k - k.$$

We can prove it using the induction on k. For $k=1$ this is just $p_1 \ge 3$. Suppose we have $k>1$ and p_k is the greatest prime. Then

$$\begin{aligned} 2(p_1-1)\dots(p_k-1) &\ge (2^{k-1} - (k-1) + p_1 + \dots + p_{k-1})(p_k-1) \\ &> 2^k + (p_1 + \dots + p_{k-1} - (k-1))(p_k-1) \\ &> 2^k + p_1 + \dots + p_{k-1} - (k-1) + p_k - 1, \end{aligned}$$

as desired. So, for $b \ge 4$ we must have $k=0$, so $n = 2^\alpha$. Then $m = 2^\beta$ for $\beta < \alpha$ and $b^{2^\alpha}-1$ is divisible by $(b^{2^\beta}-1)(b^{2^\beta}+1)$. It's easy to see that this number has the same prime divisors as $b^{2^\beta}-1$ iff $b^{2^\beta}+1$ is a power of 2. It's possible only for $\beta=0$ and $b+1$ a power of 2.

Now consider the case $b=2$. Suppose that $k\geq 2$, and we will show that the LHS of 5.2 is not smaller than RHS. This is equivalent to

$$2^{(p_1-1)\ldots(p_k-1)}-1\geq 2^{2^k}p_1\ldots p_k-1.$$

Note that LHS is divisible by $2^{2^k}p_1\ldots p_k$, so the conclusion follows.

The only case left is $b=2$, $k=1$ (the case $k=0$ has already been considered). Note that $\alpha\geq 1$ since in opposite case we would have $n=p_1$, thus $m=1$, but $2^{p_1}-1$ is divisible by some prime, and $2^1-1=1$ is not. Then 5.2 turns to

$$p_1>\Phi_{2^\alpha p_1}(2)=\prod_{d|2^\alpha p_1}(2^d-1)^{\mu(n/d)}=\frac{(2^{2^\alpha p_1}-1)(2^{2^{\alpha-1}}-1)}{(2^{2^{\alpha-1}p_1}-1)(2^{2^\alpha}-1)}=\frac{2^{2^{\alpha-1}p_1}+1}{2^{2^{\alpha-1}}+1}\geq\frac{2^{p_1}+1}{3},$$

and we can easily check that this inequality doesn't hold for any odd prime p_1, so we are done. □

Remark 5.6. This solution can be easily modified to a proof of Zsigmondy's theorem.

5.15. Find all prime numbers p such that there exists a unique $a\in\mathbb{F}_p$ for which $a^3-3a+1=0$ (you may possibly solve it without any knowledge you could have got on the lecture). You can also prove that all prime divisors of a^3-3a+1 either equal 3 or of the form $9k\pm 1$.

Solution. Let $f(a)=a^3-3a+1$. Note that $\operatorname{disc}(f)=-4\cdot 9-27=9$ which is a square modulo every prime number. This implies that $f(x)$ either doesn't have roots in $\mathbb{F}_p$ or splits into linear factors in $\mathbb{F}_p[x]$. So, if $f(x)$ has a root modulo p, then it has all its roots modulo p. Then our goal is to find all primes p such that all roots of f are equal modulo p. The derivative of f equals $3x^2-3$, and it is not coprime to $f(x)$ iff $p=3$ of ± 1 is a root of f. After simple computations we conclude that $p=3$ is the only answer for this problem. □

Remark 5.7. In fact, $f(x)=\Psi_9(x)$, so you immediately get that that all prime divisors of a^3-3a+1 either equal 3 or are of the form $9k\pm 1$.

Remark 5.8. There is a solution using quadratic reciprocity. You can read it here:

`https://artofproblemsolving.com/community/c7h2210278p16723894`

5.16. Given a positive integer a, prove that all divisors of $7a^2(a+1)-1$ are of the form $7k\pm 1$.

Solution. The first part of this solution will be some kind of motivation. Note that for $a=0$ the given polynomial doesn't have prime factors. Changing a to $1/a$ we get $f(a)=x^3-7x-7$, and we need to show that all its prime factors are equal to 7 or of the form $7k\pm 1$. This reminds us about Ψ_7. Note that $\operatorname{disc}(f)=7^2$ which is a square, hence if we denote one root of f by α, then all roots of f lie in $\mathbb{Q}(\alpha)$. By Kronecker-Weber theorem, $\mathbb{Q}(\alpha)$ lies in some $\mathbb{Q}(\zeta_n)$. In fact, we may check that α is real, so $\mathbb{Q}(\alpha)\subset\mathbb{Q}(\zeta_n)\cap\mathbb{R}$, and one may show that $\mathbb{Q}(\zeta_n)\cap\mathbb{R}=\mathbb{Q}(\zeta_n+\zeta_n^{-1})$. This is the root of Ψ_7, so the idea is to show this for $n=7$. Denote $\beta:=\zeta_7+\zeta_7^{-1}$. The degree of Φ_7 equals 3, so $\mathbb{Q}(\beta)$ in some sense has degree 3 over $\mathbb{Q}$, the same as $\mathbb{Q}(\alpha)$, so instead of inclusion $\mathbb{Q}(\alpha)\subset\mathbb{Q}(\beta)$ we want to show that $\mathbb{Q}(\alpha)=\mathbb{Q}(\beta)$.

Suppose for a moment that we've proven this. Then $\beta=p\alpha^2+q\alpha+r$ for some rationals p,q,r. In fact, when you fix the algebraic closure of $\mathbb{Q}$, you may denote any root of f by α, and if you've fixed β then such expressions will be different for distinct choices of α. We don't fix β: for us it's enough to prove that some linear combination of $1,\alpha,\alpha^2$ is a root of $\Psi_7(x)$. Let t be the common denominator of p,q,r. Then $t^3\Psi_7(px^2+qx+r)$ has integer coefficients and a root α, so

by irreducibility of f it's divisible by f. Then if $p \mid f(x)$, we must have $p \mid t^3\Psi_7(px^2+qx+r)$, so either p divides some value of $\Psi_7(x)$ and we are done here, or $p \mid t^3$. So if we additionally show that p,q,r are integers, then we are done.

Write $\Psi_7(x) = x^3+x^2-2x-1$. Then, letting $x = \beta = p\alpha^2+q\alpha+r$ into $\Psi_7(x)$ and using $\alpha^3 = 7\alpha+7$ you get a system of algebraic equations with variables p,q,r to solve. It's enough for you to find one solution, but I'll write here all of them: $\alpha^2-\alpha-5$, $\alpha^2-2\alpha-5$, and $-2\alpha^2+3\alpha+9$. So we are done. □

Remark 5.9. There is an alternative solution for this problem using Thue's lemma. I'll not present it here.

References

[1] P. Stevenhagen, *Algebra III*, `http://websites.math.leidenuniv.nl/algebra/`.

[2] J. Milne, *Galois Theory*, `https://www.jmilne.org/math/CourseNotes/index.html`.

[3] D. Cox, *Galois Theory*, Chapters 9 and 11.

[4] K. Conrad's expository papers: `https://kconrad.math.uconn.edu/blurbs/`.

[5] A. Al-Shaghay, *Some Classes of Generalized Cyclotomic Polynomials.*

[6] D. Dummit, R. Foote, *Abstract Algebra*

[7] D. Marcus, *Number Fields.*

[8] MIT Lecture Notes in Algebraic Number Theory:
`https://math.mit.edu/classes/18.785/2015fa/lectures.html`

[9] Jagiellonian University, *Franciszek Mertens Scholarship*,
`https://matinf.uj.edu.pl/kandydaci/oferta-dla-najlepszych/stypendium-mertensa`

Constructions in Combinatorics via Algebraic Methods

Semen Słobodianiuk

Abstract

In the first section I give some basic facts and definitions from matrix theory.

The second section is devoted to present a problem concerning Moore Graphs of diameter 2. The problem is purely combinatorial but it is solved by means of linear algebra with number theory flavour. Also I present smart constructions of all possible such graphs.

The third section consists of introduction of finite projective planes and some problems about construction certain graphs or families of sets with some extremal properties (and proving some bounds).

The forth section is about constructing a counterexample to Borsuk's conjecture. Here also linear algebra methods are used.

1. Preliminaries

Characteristic vector of subset T of a set S is the vector $\mathbb{1}_{\mathbb{T}} = (x_s)_s$ where coordinates are indexed by elements of S such that $x_s = 1$ iff $s \in T$ and 0 otherwise. For example characteristic vector of subset $\{1,2\}$ of set $\{1,2,3\}$ is $(1,1,0)$. Here we choose natural indexing - $i-th$ coordinate coresponds to element i.

An **indicator function** $\mathbb{1}_{\mathbb{A}}$ of a subset A of a set X is a function from the set X to $\{0,1\}$ such that $\mathbb{1}_A(x) = 1$ iff $x \in A$

Scalar product $\langle x,y\rangle$ of two vectors $x = (x_1, x_2 ... x_n)$ and $y = (y_1, y_2 ... y_n)$ is a number $\sum_{i=1}^{n} x_i y_i$. We say that x and y are **orthogonal** iff $\langle x,y\rangle = 0$

Tensor product $x \otimes y$ is quite the oposite of the scalar product because $x \otimes y$ is a n by n matrix with entries $a_{ij} = x_i y_j$

For a simple graph G with vertex set $V = v_1, ..., v_n$, the adjacency matrix is a square $n \times n$ matrix $A = A_G$ such that its element a_{ij} is one when there is an edge from vertex v_i to vertex v_j, and zero otherwise.

An **eigenvector** v and a corresponding **eigenvalue** $\lambda = \lambda_v$ (of a matrix A) are a nonzero vector and a complex number λ such that $Av = \lambda \cdot v$.

Matrix A is called **symmetric** iff $a_{ij} = a_{ji}$. For example matrix $\begin{pmatrix} 1 & 2 \\ 2 & 1 \end{pmatrix}$ is symmetric

A **basis** of linear space is set of vectors such that every other vector is uniquely expressed as linear combination of basis vectors.

By **Principal Axis Theorem** all eigenvalues of a symmetric matrix A are real and we can choose eigenvectors so they form orthogonal basis (every two basis vectors are orthogonal).

Another important theorem says that $\sum_{\lambda \in spec(A)} \lambda = \sum_{i=1}^{n} a_{ii}$, so the **trace** (sum of diagonal elements) of a matrix A is equal to sum of all eigenvalues of A.

A **field** is, loosely speaking, a set where we have elements with natural operations of division, multiplication, substraction and addition. For example set of all residues modulo p, where p is a prime number, with arithmetic modulo p forms a field.

2. Moore Graphs

Moore graphs with diameter 2 are d-regular and have girth $g=5$, where girth is length of shortest cycle. Thus they are extremely tight but have very few edges, they are in some sense the best possible graphs. Only nontrivial Moore Graphs are celebrated Petersen Graph and Hoffman-Singleton Graph. Their existence is quite miraculous, they have lots of symmetries thus can be considered as truly beautiful. Despite being finite, construction of Hoffman-Singleton Graph is at least nontrivial.

Here is statment and sketch of the proof of

Theorem 2.1 (Hoffman-Singleton)**.** Moore graph with girth 5 has vertex degree equal to $2,3,7$ or 57

Proof. Let d be a degree of the graph. Incidence matrix A of Moore graph satisfies equation $A^2+A-(d-1)I=J$ where J is matrix of ones. Clearly, all-ones vector $\mathbf{1}$ is a trivial eigenvector and every nontrivial eigenvector is orthogonal to $\mathbf{1}$. It is a good exercise to prove that eigenvalue d is of multiplicity 1. Thus every nontrivial (nonequal to d) eigenvalue satisfies the following equation

$$\lambda^2+\lambda-d+1=0$$

and thus is equal to $\frac{-1\pm\sqrt{4d-3}}{2}$, say we have $a^+=\frac{-1+\sqrt{4d-3}}{2}$ and $a^-=\frac{-1-\sqrt{4d-3}}{2}$.
Since $tr(A)=0$ and A is of size d^2+1 we arrive with system of linear equations

$$\begin{cases} a^+ + a^- = d^2 \\ a^+ \cdot \frac{-1+\sqrt{4d-3}}{2} + a^- \cdot \frac{-1-\sqrt{4d-3}}{2} + d = 0 \end{cases}$$

This is a good number theoretical exercise to prove that the system has an integer solution (a^+,a^-) iff $d\in\{2,3,7,57\}$

□

Theorem 2.2 (Hoffman-Singleton)**.** Moore Graph with $d=3$ and $d=7$ exists.

Proof. For $d=3$ we have Petersen Graph. Elegant construction identifies vertices with 2-element subsets of 5-element set where two vertices are connected iff corresponding sets are disjoint.

For $d=7$ we have Hoffman-Singleton Graph. This time draw five cycles P_i and five pentagrams Q_j and connect vertex $P_{i,x}$ with $Q_{j,ix+j}$ □

Remark 2.3. Hoffman-Singleton theorem does not give an answer to the case $d=57$. Problem of existence of (the last) Moore Graph with such vertex degree had been open for around 60 years and was finally solved in 2020.

3. Problems and Finite Projective Planes

Parallel lines do not intersect on the real plane, but we can add point of common intersection of all lines pointing in the same direction and doing so for every direction we obtain projective plane - set of points and lines, such that **every** two lines intersect at exactly one point and every two points lie on exactly one line. We want to construct finite set of "points" and "lines" with the same property. One way to do so is to use three dimensional linear spaces over finite field

Theorem 3.1. Consider three-dimensional (finite) vector space, for example $\mathbb{Z}_p^3$. Call one-dimensional subspaces "points" and two-dimensional subspaces "lines". Then resulting set forms projective plane.

Proof. Intersection of two distinct two-dimensional subspaces is unique one-dimensional subspace. Two distinct one-dimensional subspaces are contained in unique two-dimensional space. □

3.1. What is the number of points and lines in projective plane created from $\mathbb{Z}_p^3$. How many points lie on a line?

Solution. Number of all nonzero vectors in three-dimensional space is equal to p^3-1. This set can be partitioned into equivalence classes each of size $p-1$ - two vectors are in the same class iff they define the same point in projective plane. Thus number of all points is equal to p^2+p+1.

Since points and lines are dual concepts we deduce that number of lines is also equal to p^2+p+1

Similarly a two-dimensional subspace without zero can be partitioned into $\frac{p^2-1}{p-1}=p+1$ cosets as above. Thus the answear is $p+1$ □

3.2. Prove that 4-cycle free graph with n vertices has at most $\frac{n}{4}(1+\sqrt{4n-3})=O(\frac{n^{3/2}}{2})$ edges

Solution. We double count number T of ordered triples of distinct vertices (a,b,c) such that a is connected with b and c. Clearly by Cauchy Schwartz inequality

$$T=\sum_{v\in V} d(v)(d(v)-1)=\sum_{v\in V} d(v)^2-\sum_{v\in V} d(v)\geq \frac{1}{|V|}(\sum_{v\in V} d(v))^2-\sum_{v\in V} d(v)=\frac{4|E|^2}{|V|}-2|E|$$

On the other hand, since there is no 4-cycles, for fixed b and c there is at most one a such that (a,b,c) is the triple we mentioned. Thus $T\leq |V|(|V|-1)$. We arrive at a standard quadratic inequality with variable $|E|$, namely $\frac{4|E|^2}{|V|}-2|E|<|V|(|V|-1)$ □

3.3. Show that bound condition of the previous problem is asymptotically met when we consider graph where points and lines of projective plane are "merged" to one vertex. In other words try graph where vertices are labeled by one-dimensional subspaces

Solution. Indeed consider a graph with p^2+p+1 vertices. Two vertices are connected iff corresponding subspaces are orthogonal (loops are possible, nothing to worry about, we are interested in asymptotic behaviour when $p\to\infty$). Then every vertex has degree $p+1$ and every two vertices are exactly one common neighbour (so there is no 4-cycles). This is because being adjacent to two distinct vertices is equivalent to being a solution of two linear equations. All such solutions form unique one-dimensional subspace (there is a unique direction orthogonal to the plane in three dimensions). □

Remark 3.2. Construction above is not perfect because of loops, it happens when vector is orthogonal to itself (unfortunately there is always such vector). Actually the only case when inequality becomes equality is when our graph is a triangle. (it is because it has to be regular and also be a friendship graph).

Next problem is essentially a Cauchy Schwartz inequality, in probability it is called Chung-Erdos inequality.

3.4. Let $S_1, S_2 ... S_n$ be subsets of n element sets. Prove that $|\cup_{k=1}^{n} S_k| > \frac{(\sum_{k=1}^{n} |S_k|)^2}{\sum_{i,j \leq n} |S_i \cap S_j|}$

Solution. Denote $S = \cup S_k$. Then by Cauchy Schwartz

$$\frac{1}{|S|} \sum_{s \in S} (\sum_{k=1}^{n} \mathbb{1}_{S_k}(s))^2 \geq (\frac{1}{|S|} \sum_{s \in S} \sum_{k=1}^{n} \mathbb{1}_{S_k})^2$$

Since

$$\sum_{s \in S} (\sum_{k=1}^{n} \mathbb{1}_{S_k}(s))^2 = \sum_{k,k' \leq n} \sum_{s \in S} \mathbb{1}_{S_k}(s) \cdot \mathbb{1}_{S_{k'}}(s) = \sum_{k,k' \leq n} |S_k \cap S_{k'}|$$

and

$$\sum_{s \in S} \sum_{k=1}^{n} \mathbb{1}_{S_k} = \sum_{k=1}^{n} \sum_{s \in S} \mathbb{1}_{S_k} = \sum_{k} |S_k|$$

we see that the last inequality is equivalent to our problem

□

3.5. Show that inequality above is optimal. For example I came up with the following family

$|S_k| = 2^{m-1}$, $|S_k \cap S_{k'}| = 2^{m-2}$, $n = 2^m - 1$

Also after modification we can obtain another family with the following parameters:

$|S_k| = 2^{m-1} - 1$, $|S_k \cap S_{k'}| = 2^{m-2} - 1$, $n = 2^m - 1$

Solution. Consider family of sets with sets and elements indexed by all nonzero vectors of $\mathbb{Z}_2^m$ and an element belongs to a set iff coresponding vectors are not orthogonal. Clearly every vertex has degree 2^m, also every two (distinct) sets have exactly 2^{m-2} common neighbours.

We check equality in inequality:

$$2^m - 1 = |S| = \frac{[2^{m-1}(2^m - 1)]^2}{(2^m - 1)2^{m-1} + (2^m - 1)(2^m - 2)2^{m-2}} = \frac{n \cdot |S_1|}{n \cdot S_1 + n(n-1)|S_1 \cap S_2|}$$

It is interesting to see what happens when an element belongs to a set iff coresponding vectors are orthogonal.

□

3.6. Construct small family of subsets $\{S_1, S_2 ... S_n\}$ of size k such that every two sets intersect, but there is no subset of size $n-1$ with such that it intersects all S_i. I have in mind subset of a projective plane. Of course a projective plane has desired property, but it turns out that number of sets can be reduced by half. I heard that one can do even better.

SOLUTION. Family has to be small but somewhat nontrivial. Clearly projective plane is good (so $k=p+1$ and $n=p^2+p+1$ for some prime p), but we are going to choose its subset and preserve our property. Take projective space (elements are points, sets are lines, element belongs to set iff corresponding point lies on corresponding line). Fix arbitrary line l, it consists of points $\{a_0,a_1...a_p\}$. We are going to delete some lines. Leave all lines passing through a_0, delete an arbitrary, but not l, line passing through a_1 then delete arbitrary, but not l, two lines passing through a_2 and so on.

Now suppose we have an p element subset P of points having nontrivial intersection with every remaining line. Then a_0 has to be in P, for otherwise we have to choose a point from every line passing through a_0 (so total $p+1$ points, but P has at most p by assumption). Then a_1 has also to be in P, otherwise we have to choose a point from every remaining line passing through a_1 (again contradiction, a_0 is already chosen and we are forced to choose p more points). Continue in this manner until you reach a_p, but it means that $l\subset P$ so $|P|\geq p+1$

□

3.7. Finish the Hoffman-Singleton theorem. Prove that if the system of equation

$$\begin{cases} x+y=d^2 \\ x\cdot\frac{-1+\sqrt{4d-3}}{2}+y\cdot\frac{-1-\sqrt{4d-3}}{2}+d=0 \end{cases}$$

admits an integer solution (x,y), then $d\in\{2,3,7,57\}$.

If
SOLUTION. if $4d-3$ is not a square then $x=y$ thus we get $2x=d^2$ and $x=d$ thus and we see that d must be equal to 2.

Now suppose $4d-3=r^2$. Then $d=\frac{r^2+3}{4}$ and we get

$x(-1+r)+y(-1-r)+2d=0$ equivalently

$\frac{r^2+3}{4}^2+r(x-y)+2\frac{r^2+3}{4}=0$. After multyplying by 16 and expanding we get

$$r^4-2r^2-16(x-y)r-15=0$$

Thus if r is an integer solution to the above equation it should divide 15 in other words it should belong to the set $\{1,3,5,15\}$. Corresponding values of d are $\{1,3,7,57\}$ but we can discard 1 and add $d=2$ since we found it before.

□

3.8.

4. Borsuk's conjecture

The celebrated Borsuk's conjecture was that every set X in $\mathbb{R}^d$ of finite diameter can be partitioned into $d+1$ subsets of smaller diameter. One can check that this is indeed true for an Euclidean ball and for the standard simplex. A partition with this property will be called a *diameter reducing partition*. Kahn and Kalai disproved Borsuks's conjecture. In this section we shall present their construction.

Theorem 4.1 (Kahn-Kalai)**.** For every prime number p there exists a set X in $\mathbb{R}^{d^2}$, where $d=4p$, with no diameter reducing partition into fewer than 1.1^d parts.

Remark 4.2. We have $1.1^d > d^2+1$ for $d \geq 96$. Thus, we need $p \geq \frac{96}{4} = 24$ to get a counterexample to Borsuk's conjecture from the above theorem. Therefore one should choose $p=29$, in which case $d=116$. Thus the counterexample is constructed in $\mathbb{R}^{13456}$.

We shall prove yet another lemma concerning extremal combinatorics of set systems. This lemma will be crucial in the proof of the Theorem

Lemma 4.3. Let p be a prime number and let F be a family of $(2p-1)$-element subsets of an n-element set. Suppose that $|A \cap B| \neq p-1$ for $A, B \in F$. Then $|F| \leq \binom{n}{0} + \binom{n}{1} + \ldots + \binom{n}{p-1}$.

Corollary 4.4. Let p be a prime number and let F be a family of $(2p-1)$-element subsets of an $n=4p$ element set. Suppose that $|A \cap B| \neq p-1$ for $A, B \in F$. Then $|F| \leq \frac{1}{1.1^n}\binom{n}{2p-1}$.

Remark 4.5. The number of $(2p-1)$-element subsets of an n-element set is $\binom{n}{2p-1}$. For each two distinct $(2p-1)$-element subsets of an n-element set one has $|A \cap B| \in \{0,1,2,\ldots,2p-2\}$. Note that $p-1$ is the middle point of this set of numbers. The corollary says that for $n=4p$ forbidding this middle size intersection forces the family to have much fewer than $\binom{n}{2p-1}$ elements.

Proof of Corollary 4.4. If $n \geq 4k$, $k \geq 1$ then

$$\binom{n}{k-1} = \frac{n!}{(n-k+1)!(k-1)!} = \frac{k}{n-k+1} \cdot \frac{n!}{(n-k)!k!} = \frac{k}{n-k+1}\binom{n}{k} \leq \frac{k}{4k-k+1}\binom{n}{k} \leq \frac{1}{3}\binom{n}{k}.$$

Thus for $k=0,1,\ldots,p-1$ we have $\binom{n}{k} \leq \frac{1}{3^{p-k}}\binom{n}{p}$. Applying Lemma 4.3 leads therefore to

$$|F| \leq \left(\frac{1}{3^p} + \frac{1}{3^{p-1}} + \ldots + \frac{1}{3}\right)\binom{n}{p} < \frac{1}{3} \cdot \frac{1}{1-\frac{1}{3}}\binom{n}{p} = \frac{1}{2}\binom{n}{p}.$$

We get

$$\begin{aligned}\frac{\binom{n}{2p-1}}{|F|} &\geq 2\frac{\binom{n}{2p-1}}{\binom{n}{p}} = 2 \cdot \frac{p!}{(2p-1)!} \cdot \frac{(n-p)!}{(n-2p+1)!} = 2 \cdot \frac{p!}{(2p-1)!} \cdot \frac{(3p)!}{(2p+1)!} \\ &= 2 \cdot \frac{3p(3p-1)\ldots(2p+2)}{(2p-1)(2p-2)\ldots(p+1)} = 2 \cdot \frac{3p}{2p-1} \cdot \frac{3p-1}{2p-2} \cdot \ldots \cdot \frac{2p+2}{p+1}.\end{aligned}$$

Since $\frac{3p-k}{2p-1-k} \geq \frac{3}{2}$ for $k=0,1,\ldots,p-2$, we get

$$\frac{\binom{n}{2p-1}}{|F|} \geq 2 \cdot \left(\frac{3}{2}\right)^{p-1} = \frac{4}{3} \cdot \left(\frac{3}{2}\right)^{p} = \frac{4}{3} \cdot \left(\frac{3}{2}\right)^{n/4} > \left(\frac{3}{2}\right)^{n/4} = \left(\sqrt[4]{\frac{3}{2}}\right)^{n} > 1.1^n.$$

□

Proof of Lemma 4.3. We can assume that the underlying set in $\{1,\ldots,n\}$. We shall work over the field $\mathbb{Z}_p$. For $A\in F$ let $\mathbb{1}_A\in\{0,1\}^n$ be its incidence vector, that is the vector whose ith coordinate is 1 if and only if $i\in A$. Consider $f_A:\{0,1\}^n\to\mathbb{Z}_p$ given by

$$f_A(x)=\prod_{k=0}^{p-2}\left(\left(\sum_{i\in A}x_i\right)-k\right),$$

where the values are taken modulo p. Let $V=\{f:\{0,1\}^n\to\mathbb{Z}_p\}$ be the space of all functions on $\{0,1\}^n$ having values in $\mathbb{Z}_p$. We treat V as a vector space over $\mathbb{Z}_p$ (for arbitrary X the space $\{f:X\to\mathbb{Z}_p\}$ can be treated as a vector space over $\mathbb{Z}_p$). Let $V_F=spann\{f_A,A\in F\}$. It is enough to prove the following two claims.

Claim 1. The vectors f_A for $A\in F$ are linearly independent. Thus $\dim(V_F)=|F|$.

Claim 2. We have $\dim(V_F)\le\binom{n}{0}+\binom{n}{1}+\ldots+\binom{n}{p-1}$.

Proof of Claim 1. Note that

$$f_A(\mathbb{1}_A)=\prod_{k=0}^{p-2}(|A|-k)=\prod_{k=0}^{p-2}(2p-1-k)=\prod_{k=0}^{p-2}(2p-1-k)=(-1)^{p-1}\prod_{k=0}^{p-2}(k+1)=(-1)^{p-1}(p-1)!\neq 0,$$

where the last but one equality follows from the fact that we work in $\mathbb{Z}_p$. If now $A\neq B$ then $f_A(\mathbb{1}_B)=\prod_{k=0}^{p-2}(|A\cap B|-k)=0$ as $|A\cap B|\mod p\in\{0,1,2,\ldots,p-2\}$ since $|A\cap B|\neq p-1$ by our assumption. If we now evaluate the equality $\sum_{B\in F}\lambda_B f_B=0$ on $\mathbb{1}_A$ we shall get $\lambda_A(p-1)!=0$ and thus $\lambda_A=0$. This proves the desired independence of the elements f_A. □

Proof of Claim 2. The function f_A is clearly a linear combination of monomials $x_1^{j_1}\ldots x_n^{j_n}$ with $j_1+\ldots j_n\le p-1$ (as it is a product of $p-1$ linear function). But since for $j_i\neq 0$ and $x_i\in\{0,1\}$ we have $x_i^{j_i}=x_i$ we actually see that f_A is a linear combination of monomials $x_1^{j_1}\ldots x_n^{j_n}$ with $j_1,\ldots,j_n\in\{0,1\}$ and $j_1+\ldots+j_n\le p-1$. There are exactly $\binom{n}{0}+\binom{n}{1}+\ldots+\binom{n}{p-1}$ such monomials. Let V' be the space spanned by these monomials. We have $V_F\subseteq V'$ and thus $\dim(V_F)\le\dim(V')\le\binom{n}{0}+\binom{n}{1}+\ldots+\binom{n}{p-1}$. □

The proof of Lemma 4.3 is completed. □

We are now ready to prove Theorem 4.1.

Proof of Theorem 4.1. Let p be a prime number, $d=4p$ and let α be the family of all $(2p-1)$-element subsets of $\{1,\ldots,d\}$. For $A\in\alpha$ w define $u_A\in\mathbb{R}^d$ via $u_A=2\mathbb{1}_A-\mathbb{1}$, where $\mathbb{1}_A$ is the usual incidence vector of A and $\mathbb{1}=\mathbb{1}_{\{1,\ldots,d\}}$ is the vector with all entries equal 1. We will show that $X=\{u_A\otimes u_A:\ A\in\alpha\}$ is the desired set in $\mathbb{R}^{d^2}$. Recall that for $u\in\mathbb{R}^{d_1}$ and $v\in\mathbb{R}^{d_2}$, $u\otimes v$ is the $d_1\times d_2$ matrix with entries $(u_iv_j)_{i\le d_1,j\le d_2}$. Of course every $d_1\times d_2$ matrix can be treated, in a natural way, as an element of $\mathbb{R}^{d_1d_2}$.

Fact. For any $x_1,y_1\in\mathbb{R}^{d_1}$ and $x_2,y_2\in\mathbb{R}^{d_2}$ we have $x_1\otimes x_2\in\mathbb{R}^{d_1d_2}$, $y_1\otimes y_2\in\mathbb{R}^{d_1d_2}$ and $\langle x_1\otimes x_2y_1\otimes y_2\rangle=\langle x_1y_1\rangle\langle x_2y_2\rangle$, where the scalar product $\langle\cdot,\cdot\rangle$ is the standard scalar product in $\mathbb{R}^{d_1d_2}$.

Proof of the Fact. For $x\in\mathbb{R}^d$ let $x^{(i)}$ be the ith coordinate of x. We have

$$\langle x_1\otimes x_2y_1\otimes y_2\rangle=\sum_{i\le d_1,j\le d_2}x_1^{(i)}x_2^{(j)}y_1^{(i)}y_2^{(j)}=\left(\sum_{i\le d_1}x_1^{(i)}y_1^{(i)}\right)\left(\sum_{j\le d_1}x_2^{(j)}y_2^{(j)}\right)=\langle x_1y_1\rangle\langle x_2y_2\rangle.$$

□

We continue the proof of Theorem 4.1. Note that

$$\begin{aligned}\langle u_A u_B\rangle &= \langle 2\mathbb{1}_A - \mathbb{1}2\mathbb{1}_B - \mathbb{1}\rangle = 4|A\cap B| - 2|A| - 2|B| + d\\ &= 4|A\cap B| - 4(2p-1) + 4p = 4|A\cap B| - 4p + 4 = 4(|A\cap B| - p + 1).\end{aligned}$$

In particular, $\langle u_A u_A\rangle = 4(2p-1-p+2) = 4p = d$. Moreover, $\langle u_A u_B\rangle = 0$ if and only if $|A\cap B| = p-1$. Let $q_A = u_A \otimes u_A$. Then by the Fact

$$|q_A - q_B|^2 = \langle q_A q_A\rangle + \langle q_B q_B\rangle - 2\langle q_A q_B\rangle = \langle u_A u_A\rangle^2 + \langle u_B u_B\rangle^2 - 2\langle u_A u_B\rangle^2 = 2d^2 - 2\langle u_A u_B\rangle^2.$$

Since $\langle u_A u_B\rangle^2 \geq 0$ with equality if and only if $|A\cap B| = p-1$. Thus, the diameter of X is $2d^2$ and any subset X' of X has diameter $2d^2$ as long as it contains two points q_A, q_B such that $|A\cap B| = p-1$.

Suppose now we partition X into fewer than 1.1^d parts. Then one of the parts X' of X is of size greater than $\frac{1}{1.1^d}|\alpha| = \frac{1}{1.1^d}\binom{d}{2p-1}$. Then by Corollary 4.4 X' is too big to satisfy $|A\cap B| \neq p-1$ for all its distinct members A, B. So X' has two elements A, B satisfying $|A\cap B| = p-1$. Thus the diameter of X' equals the diameter of X. As a consequence our partition is not diameter reducing.

□

References

[1] `www.overleaf.com/learn/latex/Learn_LaTeX_in_30_minutes`

Diagram Chasing in Abelian Categories

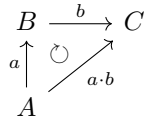
Robert Szafarczyk

1. What is a category?

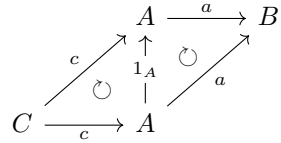
Definition 1.1. (Category) A category consists of objects and morphisms (arrows between objects).

$$A \xrightarrow{a} B$$

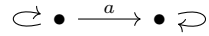
Any two arrows a, b such that one ends where the other begins can be composed yielding another arrow.

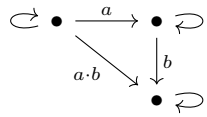


In addition, for every object A there is a special arrow called its identity $1_A : A \to A$, which satisfies $1_A \cdot a = a$ and $c \cdot 1_A = c$ for every $a : A \to B$ and $c : C \to A$.



Example 1.2. Here are some examples of categories:





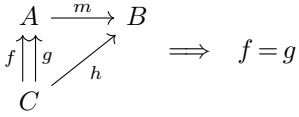
In general though, categories can have many objects and morphisms.

Exercise 1.1. Every object A has exactly one identity arrow (an arrow $j : A \to A$ satisfying $j \cdot a = a$ and $c \cdot j = c$ for all $a : A \to B$ and $c : C \to A$).

Solution. By the definition of a category, A has an identity arrow 1_A. Suppose that there is a different identity arrow $j : A \to A$. Then we have $1_A \neq j = j \cdot 1_A = 1_A$ which is a contradiction. □

We now define a special kind of morphism

Definition 1.3. (Monomorphism) A morphism $m : A \to B$ is said to be a monomorphism (mono in short) if for any C and any two morphisms $f, g : C \to A$ the equality $f \cdot m = h = g \cdot m$ implies $f = g$.

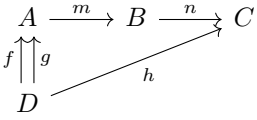


Exercise 1.2. For any A, the identity arrow $1_A : A \to A$, is a mono.

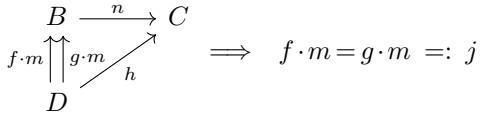
Solution. Take any C and any $f, g : C \to A$. Then $f \cdot 1_A = g \cdot 1_A$ implies $f = f \cdot 1_A = g \cdot 1_A = g$. □

Exercise 1.3. Composition of two (composable) monomorphisms is again a monomorphism.

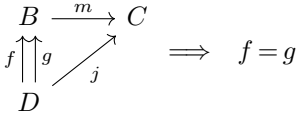
Solution. Take any two composable monomorphisms $A \xrightarrow{m} B \xrightarrow{n} C$ and any object D with arrows $f, g : D \to A$ satisfying $f \cdot m \cdot n = h = g \cdot m \cdot n$



Since n is mono we get

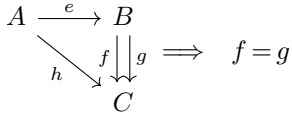


Then, since m is mono, we get



which finishes the proof that $m \cdot n$ is a mono (we showed that $f \cdot m \cdot n = g \cdot m \cdot n$ implies $f = g$). □

Definition 1.4. (Epimorphism) A morphism $e : A \to B$ is said to be an epimorphism (epi in short) if for any C and any two morphisms $f, g : B \to C$ the equality $e \cdot f = h = e \cdot g$ implies $f = g$.



Definition 1.5. (Isomorphism) A morphism $i : A \to B$ is said to be an isomorphism if there exists $j : B \to A$ such that $i \cdot j = 1_A$ and $j \cdot i = 1_B$. We call j the inverse of i. If there exists an isomorphism between A and B we say that A is isomorphic to B and write $A \simeq B$.

When two objects are isomorphic we think of them as being roughly the same.

Exercise 1.4. Show that an isomorphism is both mono and epi.

Solution. Let $i : A \to B$ be an isomorphism with inverse $j : B \to A$. We check that i is mono. Let $f, g : C \to A$ be two morphisms satisfying $f \cdot i = g \cdot i$. Then $f = f \cdot 1_A = f \cdot i \cdot j = g \cdot i \cdot j = g \cdot 1_A = g$. Now we check that it's epi. Let $f', g' : B \to C'$ be such that $i \cdot f' = i \cdot g'$. Then $f' = 1_B \cdot f' = j \cdot i \cdot f' = j \cdot i \cdot g' = 1_B \cdot g' = g'$. □

Proposition 1.6. If $f \cdot g$ is mono, then f is mono. If $f \cdot g$ is epi, then g is epi.

2. Application of category theory

The usefulness of category theory comes from the fact that almost everything that concerns mathematics forms a category.

Example 2.1. (Category of sets) Let **Set** be a category in which:

- objects are sets
- morphisms are functions (for example between a two element and a three element set there are 9 morphisms in one direction and 8 in the other)
- composition of morphisms is the same as composition of functions
- identity morphisms are identity functions (functions $f : X \to X$ given by $f(x) = x$)

The category **Set** allows us to apply what we know about categories to set theory.

One very important observation is that set theory often talks about elements, for example we can define a function $f : \{1, 4\} \to \mathbb{N}$ on elements as $f(1) = 5$, $f(4) = 4$. In category theory we don't have elements. Objects are just anchor points for morphisms, they don't store any information. In **Set** the function f is just an arrow between two objects, the only thing we know is how f behaves under composition with other morphisms (of which we also only know how they compose...).

It might seem that in **Set** we got rid of everything we know about sets, but it turns out that the opposite is true.

Exercise 2.1. Monomorphisms in **Set** are exactly the injective functions.

Solution. First, lets show that if $f : X \to Y$ is injective then it is mono. Suppose, for the contrary, that f is injective but there are two distinct functions $g, h : Z \to X$ such that $g \cdot f = h \cdot f$. Since $g \neq h$ there is an element $z \in Z$ such that $g(z) \neq h(z)$. But then the fact that $f(g(z)) = f(h(z))$ contradicts the injectivity of f.

Now suppose f is mono but is not injective. Then, there are two elements $x \neq y \in X$ such that $f(x) = f(y)$. Let $*$ be a one element set. Let $\tilde{x} : * \to X$ be a function taking this single element to x and let $\tilde{y} : * \to X$ be a function taking the single element to y. Since $x \neq y$ we also have $\tilde{x} \neq \tilde{y}$, but since $f(x) = f(y)$ we have $\tilde{x} \cdot f = \tilde{y} \cdot f$ which contradicts f being a monomorphism. □

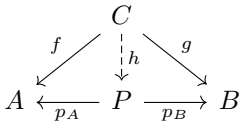
Notice that the definition of an injective function is local (concerns only two sets and one function), whereas the definition of a monomorphism is global (the whole category takes part) and still they are the same in **Set**.

Since we already showed that the composition of two monomorphisms is again mono we get

Corollary 2.2. Composition of two injective functions is again injective.

3. Universal constructions

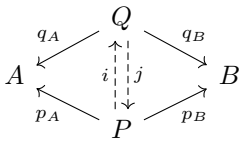
Definition 3.1. (Product) We fix two objects A and B. An object P equipped with morphisms $p_A : P \to A$ and $p_B : P \to B$ is called their product if it satisfies the "universal property" that for any object C and morphisms $f : C \to A$, $g : C \to B$ there exists a unique (exactly one) morphism $h : C \to P$ such that $f = h \cdot p_A$ and $g = h \cdot p_B$.



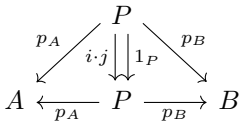
Warning: the product might not exist!

Exercise 3.1. Suppose that P equipped with $p_A : P \to A$, $p_B : P \to B$ and Q equipped with $q_A : Q \to A$, $q_B : Q \to B$ both satisfy the universal property of a product. Show that $P \simeq Q$ (we say that the product is unique up to an isomorphism).

Solution. Since both P and Q satisfy the universal property we obtain two arrows.



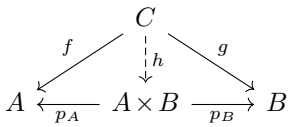
It remains to show that $i \cdot j = 1_P$ and $j \cdot i = 1_Q$. Since $i \cdot j \cdot p_A = i \cdot q_A = p_A$ and $i \cdot j \cdot p_B = i \cdot q_B = p_B$ both $i \cdot j$ and 1_P make the following diagram commute.



But the universal property states that there exists a unique arrow making this diagram commute, thus $i \cdot j = 1_P$. A symmetrical argument shows that $j \cdot i = 1_Q$ and therefore that $P \simeq Q$. □

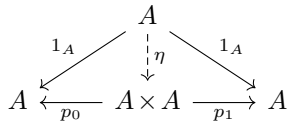
The above exercise ilustrates that the universal property might be used not only to construct morphisms but also to show equality of morphisms via uniqueness.

Remark 3.2. Since for any A and B their product, if it exists, is unique up to an isomorphism we might say "the product" and denote it by $A \times B$. We can then redraw the universal property of the product.



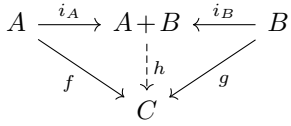
Exercise 3.2. Suppose that $A\times A$ exists. Construct in a "natural" way a morphism $\eta: A\to A\times A$.

Solution.



□

Definition 3.3. (Coproduct) We fix two objects A and B. Their coproduct is an object $A+B$ equipped with morphisms $i_A: A\to A+B$ and $i_B: B\to A+B$ satisfying the universal property that for any object C and morphisms $f: A\to C$, $g: B\to C$ there exists a unique morphism $h: A+B\to C$ such that $f = i_A\cdot h$ and $g = i_B\cdot h$.



Warning: the coproduct might not exist!

Proposition 3.4. In **Set** products take form of cartesian products and coproducts take form of disjoint unions (for example $\{\circ\circ\}+\{\circ\}\simeq\{\circ\circ\circ\}$).

Definition 3.5. (Zero Object) If it exists, we denote by 0 an object having the property that for any object A there exists a unique arrow from 0 to A and a unique arrow from A to 0.

Remark 3.6. Let A and B be two objects in a category, which has a zero object. Then by composing the unique arrows $A\to 0\to B$ we obtain the unique arrow from A to B passing through the zero object. We denote this arrow as $0: A\to B$.

Does **Set** have a zero object?

Proposition 3.7. In **Set** an object A has the property that for any object B in **Set** there is exactly one arrow from B to A if and only if A is a one element set.

Therefore, if the zero object exists it must be the one element set. From the other hand, from a one element set to a two element set there are two functions, thus the one element set is not the zero object.

Since for our purposes we'd like to have a zero object in our category we abandon **Set** and move our examples to a new category.

Example 3.8. (Category of pointed sets) Let $\mathbf{Set}_*$ be a category in which:

- objects are pointed sets (sets in which one of the elements is highlighted, for example a four element pointed set looks like this $\{*\circ\circ\circ\}$. The element $*$ is called the base point)

- morphisms are functions of pointed sets (functions which preserve the base point, that is functions $f: A\to B$ which send the base point of A to the base point of B)

- composition of morphisms is the same as composition of functions

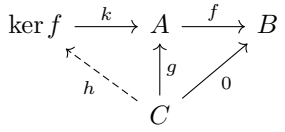
- identity morphisms are identity functions

Proposition 3.9. In $\mathbf{Set}_*$ the one element set is the zero object.

4. Abelian categories

From now on we only consider categories containing a zero object (and therefore zero morphisms).

Definition 4.1. (Kernel) We fix a morphism $A \xrightarrow{f} B$. It's kernel is an object $\ker f$ equipped with a morphism $k : \ker f \to A$ such that $k \cdot f = 0$ satisfying the universal property that for any object C and arrow $g : C \to A$ such that $g \cdot f = 0$ there exists a unique morphism $h : C \to \ker f$ such that $g = h \cdot k$.

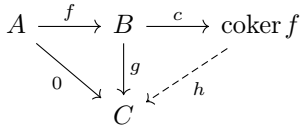


Warning: the kernel might not exist!

Exercise 4.1. Show that in $\mathbf{Set}_*$ the kernel of a morphism $f : X \to Y$ is the set $\{x \in X : f(x) = *\}$ together with its inclusion into X.

Solution. Let $K = \{x \in X : f(x) = *\}$ with inclusion $k : K \to X$ (clearly $k \cdot f = 0$) and let Z and $g : Z \to X$ be such that $g \cdot f = 0$ (therefore for all $z \in Z$ we have $g(f(z)) = * \in Y$). Then, for all $z \in Z$ the element $g(z)$ is contained in $K \subset X$. This defines a morphism $h : Z \to K$ sending each z to $g(z) \in K$. Then, by the construction of k we get $g = h \cdot k$. The uniqueness of h follows from the fact that k as an injective function is mono. □

Definition 4.2. (Cokernel) We fix a morphism $A \xrightarrow{f} B$. It's cokernel is an object $\operatorname{coker} f$ equipped with a morphism $c : B \to \operatorname{coker} f$ such that $f \cdot c = 0$ satisfying the universal property that for any object C and arrow $g : B \to C$ such that $f \cdot g = 0$ there exists a unique morphism $h : \operatorname{coker} f \to C$ such that $g = c \cdot h$



Warning: the cokernel might not exist!

Proposition 4.3. In $\mathbf{Set}_*$ the cokernel of $f : X \to Y$ is the set $\{*\} \cup \{y \in Y : \forall_{x \in X} f(x) \neq y\}$ together with a map from Y sending each y in the image of f to $*$ and each y not in the image of f to itself.

Definition 4.4. (Abelian category) An abelian category is a category satisfying the following conditions:

- it has a zero object

- morphisms with the same beginning and end can be added together (in particular we have $f + 0 = f$ and $f = g \iff f - g = 0$) and addition agrees with composition, $f \cdot (g + h) = f \cdot g + f \cdot h$

- for any two objects, A and B, both their product and coproduct exist and they coincide. We thus call it a biproduct and write $A \oplus B$.

- kernels and cokernels exist for all morphisms

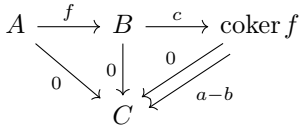
- $\operatorname{coker} \ker f \simeq \ker \operatorname{coker} f$ (we call it the image $\operatorname{Im} f$ of f)

From now on we only consider abelian categories.

Unfortunately, $\mathbf{Set}_*$ is not abelian as we cannot add morphisms together.

Exercise 4.2. Show that for all f the arrow $c: B \to \operatorname{coker} f$ is an epimorphism.

Solution. Suppose to the contrary that there exist C and morphisms $a, b: B \to C$ such that $a \neq b$ but $c \cdot a = c \cdot b$. Then, since $c \cdot (a - b) = 0$ we get the following commutative diagram.

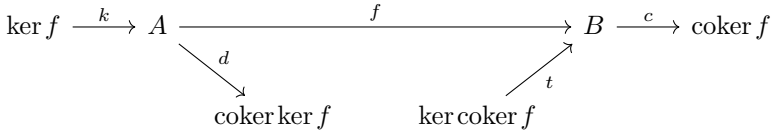


but the universal property of a cokernel says that there is only one morphism making this diagram commute, therefore $a - b = 0$, which means that $a = b$, a contradiction. □

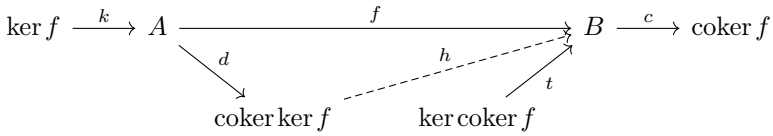
Proposition 4.5. For all f the arrow $k: \ker f \to A$ is a monomorphism.

Exercise 4.3. Construct a morphism $\mu: \operatorname{coker} \ker f \to \ker \operatorname{coker} f$.

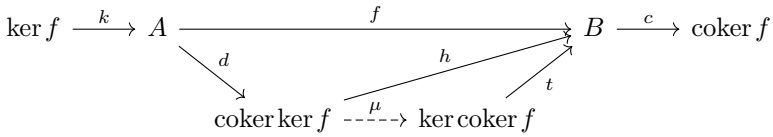
Solution. We have the following diagram.



Since by definition $k \cdot f = 0$ we obtain a morphism (cokernel's universal property).

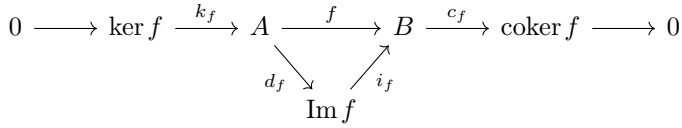


Then, since d is an epimorphism and $d \cdot h \cdot c = f \cdot c = 0 = d \cdot 0$ we get $h \cdot c = 0$, from which we obtain a morphism (kernel's universal property).



□

Remark 4.6. The definition of an abelian category says that μ is an isomorphism. Thus, for a morphism f we can draw the following diagram.



Where, i_f is the kernel of c_f, d_f is the cokernel of k_f and $f = d_f \cdot i_f$.

5. Exact sequences

Definition 5.1. (Exact sequence) An exact sequence is a configuration of morphisms

$$A_0 \xrightarrow{f_1} A_1 \xrightarrow{f_2} \ \dots \ \xrightarrow{f_n} A_n$$

such that $f_i \cdot f_{i+1} = 0$ and the universal morphism $A_i \to \ker f_{i+1}$ is epi.

Straight from the definition we get the following statement.

Proposition 5.2. The sequence

$$A_0 \xrightarrow{f_1} A_1 \xrightarrow{f_2} \ \dots \ \xrightarrow{f_n} A_n$$

is exact if and only if for all i the sequence

$$A_{i-1} \xrightarrow{f_i} A_i \xrightarrow{f_{i+1}} A_{i+1}$$

is exact.

Definition 5.3. (Short exact sequence) We call an exact sequence short if it is of the following form.

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

Proposition 5.4. The zero morphism $0 : A \to B$ is a monomorphism if and only if $A \simeq 0$ and is an epimorphism if and only if $B \simeq 0$.

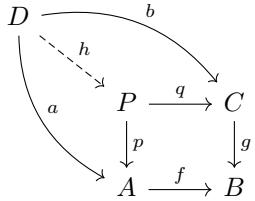
Exercise 5.1. Show that $m : A \to B$ is a monomorphism if and only if $0 \longrightarrow A \xrightarrow{m} B$ is exact if and only if $\ker m \simeq 0$.

Solution. From the definition $0 \longrightarrow A \xrightarrow{m} B$ is exact if and only if $0 : 0 \to \ker m$ is epi, which we know to be equivalent with $\ker m \simeq 0$. Now suppose that $m : A \to B$ is mono. Let $k : \ker m \to A$ be the kernel of m. We know that k is mono and thus $k \cdot m$ is mono, but $k \cdot m = 0 : \ker m \to B$ therefore $\ker m \simeq 0$. From the other hand, if $\ker m \simeq 0$ and $a, b : C \to A$ are such that $a \cdot m = b \cdot m$ we get that $a - b$ factors through $\ker m \simeq 0$ and therefore $a - b = 0$, thus $a = b$. □

Proposition 5.5. Morphism $e : A \to B$ is epi if and only if $A \xrightarrow{e} B \longrightarrow 0$ is exact if and only if $\operatorname{coker} e \simeq 0$.

Proposition 5.6. Sequence $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C$ is exact if and only if f is the kernel of g. Sequence $A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$ is exact if and only if g is the cokernel of f.

Definition 5.7. (Pullback) The pullback of a diagram $A \xrightarrow{f} B \xleftarrow{g} C$, if it exists, is an object P equipped with morphisms $p : P \to A$ and $q : P \to C$ such that $p \cdot f = q \cdot g$ satisfying the universal property that for any object D and arrows $a : D \to A$ and $b : D \to C$ such that $a \cdot f = b \cdot g$ there exists a unique arrow $h : D \to P$ such that $a = h \cdot p$ and $b = h \cdot q$.



Proposition 5.8. In abelian categories all pullbacks exist.

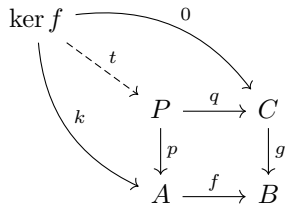
Exercise 5.2. Let the following be a pullback diagram.

$$\begin{array}{ccc} P & \xrightarrow{q} & C \\ \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle g} \\ A & \xrightarrow{f} & B \end{array}$$

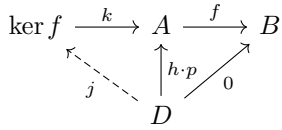
Let $k : \ker f \to A$ be the kernel of f. Then, there exists t such that $t : \ker f \to P$ is the kernel of q and satisfies $k = p \cdot t$.

$$\begin{array}{ccccc} \ker f & \xrightarrow{t} & P & \xrightarrow{q} & C \\ \downarrow{\scriptstyle 1_{\ker f}} & & \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle g} \\ \ker f & \xrightarrow{k} & A & \xrightarrow{f} & B \end{array}$$

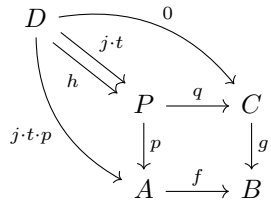
Solution. Since $k \cdot f = 0 = 0 \cdot g$ we can define t as follows.



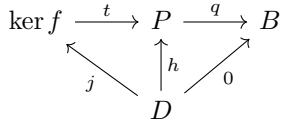
Thus, we get $k = t \cdot p$. It remains to show that t is the kernel of q. The fact that $t \cdot q = 0$ follows from the above diagram. Let $h : D \to P$ be such that $h \cdot q = 0$. Since $h \cdot p \cdot f = h \cdot q \cdot g = 0 \cdot g = 0$ we get (kernel's universal property) a unique arrow $j : D \to \ker f$ satisfying $h \cdot p = j \cdot k$.



Since $h \cdot p = j \cdot k = j \cdot t \cdot p$ and $h \cdot q = 0$ both h and $j \cdot t$ make the following diagram commute.



Thus, $h = j \cdot t$.



To show j unique assume that there is another arrow $j' : D \to \ker f$ such that $j' \cdot t = h$. Then $j' \cdot k = j' \cdot t \cdot p = h \cdot p = j \cdot t \cdot p = j \cdot k$, but k is a kernel, and therefore a monomorphism, so $j' = j$. □

Proposition 5.9. In a pullback diagram

$$\begin{array}{ccc} P & \xrightarrow{q} & C \\ \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle g} \\ A & \xrightarrow{f} & B \end{array}$$

the natural morphism $\operatorname{coker} q \to \operatorname{coker} f$ is mono.

Corollary 5.10. In a pullback diagram

$$\begin{array}{ccc} P & \xrightarrow{q} & C \\ \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle g} \\ A & \xrightarrow{f} & B \end{array}$$

if f is epi then q is epi.

Proof. Since $\operatorname{coker} q \to 0 \simeq \operatorname{coker} f$ is mono we get $\operatorname{coker} q \simeq 0$. Therefore, q is epi. □

The above proposition together with the previous exercise yield the following useful lemma.

Lemma 5.11. Let the following be a short exact sequence.

$$0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C \longrightarrow 0$$

Let $h : D \to C$ be any morphism. Then, taking the pullback of $B \xrightarrow{g} C \xleftarrow{h} D$ yields the following commutative diagram with exact rows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle 1_A} & & \uparrow{\scriptstyle p} & & \uparrow{\scriptstyle h} & & \\ 0 & \longrightarrow & A & \xrightarrow{t} & P & \xrightarrow{q} & D & \longrightarrow & 0 \end{array}$$

Proof. From the previous exercise we get the following commutative diagram with exact rows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle 1_A} & & \uparrow{\scriptstyle p} & & \uparrow{\scriptstyle h} & & \uparrow \\ 0 & \longrightarrow & A & \xrightarrow{t} & P & \xrightarrow{q} & D & \longrightarrow & \operatorname{coker} q \end{array}$$

From the above proposition we get that $0 : \operatorname{coker} q \to 0$ is mono, which means that $\operatorname{coker} q \simeq 0$. Thus, we indeed get the following commutative diagram with exact rows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & A & \xrightarrow{f} & B & \xrightarrow{g} & C & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle 1_A} & & \uparrow{\scriptstyle p} & & \uparrow{\scriptstyle h} & & \\ 0 & \longrightarrow & A & \xrightarrow{t} & P & \xrightarrow{q} & D & \longrightarrow & 0 \end{array}$$

□

6. The Snake Lemma

Lemma 6.1. (Snake Lemma) Let the following be a commutative diagram with exact rows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & X & \xrightarrow{x} & Y & \xrightarrow{y} & Z & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle f} & & \uparrow{\scriptstyle g} & & \uparrow{\scriptstyle h} & & \\ 0 & \longrightarrow & A & \xrightarrow{a} & B & \xrightarrow{b} & C & \longrightarrow & 0 \end{array}$$

Then, we get the following exact sequence of kernels and cokernels.

$$\begin{array}{ccccccccc} & & \operatorname{coker} f & \to & \operatorname{coker} g & \to & \operatorname{coker} h & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle c_f} & & \uparrow{\scriptstyle c_g} & & \uparrow{\scriptstyle c_h} & & \\ 0 & \longrightarrow & X & \xrightarrow{x} & Y & \xrightarrow{y} & Z & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle f} & & \uparrow{\scriptstyle g} & & \uparrow{\scriptstyle h} & & \\ 0 & \longrightarrow & A & \xrightarrow{a} & B & \xrightarrow{b} & C & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle k_f} & & \uparrow{\scriptstyle k_g} & & \uparrow{\scriptstyle k_h} & & \\ 0 & \longrightarrow & \ker f & \longrightarrow & \ker g & \longrightarrow & \ker h & & \end{array}$$

Proof. The proof is written in full detail in the next section. □

The following observations will help us in applying the snake lemma.

Proposition 6.2. Morphism f is an isomorphism if and only if $0 \longrightarrow A \xrightarrow{f} B \longrightarrow 0$ is exact. That is, f is an isomorphism if and only if f is mono and epi (this is not always true in some non-abelian categories).

Proposition 6.3. An exact sequence

$$A_0 \xrightarrow{f_1} A_1 \xrightarrow{f_2} \ \dots \ \xrightarrow{f_n} A_n$$

gives rise to the following short exact sequences.

$$0 \longrightarrow \ker f_1 \xrightarrow{k_{f_1}} A_0 \xrightarrow{d_{f_1}} \operatorname{Im} f_1 \longrightarrow 0$$

$$0 \longrightarrow \operatorname{Im} f_i \xrightarrow{i_{f_i}} A_i \xrightarrow{d_{f_{i+1}}} \operatorname{Im} f_{i+1} \longrightarrow 0$$

$$0 \longrightarrow \operatorname{Im} f_n \xrightarrow{i_{f_n}} A_n \xrightarrow{c_{f_n}} \operatorname{coker} f_n \longrightarrow 0$$

Lemma 6.4. (Five Lemma) Let the following be a commutative diagram with exact rows.

$$\begin{array}{ccccccccc} B_1 & \xrightarrow{b_1} & B_2 & \xrightarrow{b_2} & B_3 & \xrightarrow{b_3} & B_4 & \xrightarrow{b_4} & B_5 \\ \uparrow{\scriptstyle f_1} & & \uparrow{\scriptstyle f_2} & & \uparrow{\scriptstyle f_3} & & \uparrow{\scriptstyle f_4} & & \uparrow{\scriptstyle f_5} \\ A_1 & \xrightarrow{a_1} & A_2 & \xrightarrow{a_2} & A_3 & \xrightarrow{a_3} & A_4 & \xrightarrow{a_4} & A_5 \end{array}$$

Then, if f_1, f_2, f_4 and f_5 are isomorphisms, then f_3 is an isomorphism.

PROOF. By g_i we denote the natural (given by the commutativity of the above diagram and an appropriate universal property) morphism $\operatorname{Im} a_i \to \operatorname{Im} b_i$, by t the natural morphism $\ker a_1 \to \ker b_1$ and by s the natural morphism $\operatorname{coker} a_4 \to \operatorname{coker} b_4$. We have the following commutative diagram with exact rows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \ker b_1 & \longrightarrow & B_1 & \longrightarrow & \operatorname{Im} b_1 & \longrightarrow & 0 \\ & & {\scriptstyle t}\uparrow & & {\scriptstyle f_1}\uparrow & & {\scriptstyle g_1}\uparrow & & \\ 0 & \longrightarrow & \ker a_1 & \longrightarrow & A_1 & \longrightarrow & \operatorname{Im} a_1 & \longrightarrow & 0 \end{array}$$

Thus, from the snake lemma we get that

$$0 \longrightarrow \ker t \longrightarrow \ker f_1 \longrightarrow \ker g_1 \longrightarrow \operatorname{coker} t \longrightarrow \operatorname{coker} f_1 \longrightarrow \operatorname{coker} g_1 \longrightarrow 0$$

is exact. In particular, the sequence

$$\operatorname{coker} f_1 \longrightarrow \operatorname{coker} g_1 \longrightarrow 0$$

is exact. But, since f_1 is an isomorphism we have $\operatorname{coker} f_1 \simeq 0$ and therefore $\operatorname{coker} g_1 \simeq 0$. Then, the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \operatorname{Im} b_1 & \longrightarrow & B_2 & \longrightarrow & \operatorname{Im} b_2 & \longrightarrow & 0 \\ & & {\scriptstyle g_1}\uparrow & & {\scriptstyle f_2}\uparrow & & {\scriptstyle g_2}\uparrow & & \\ 0 & \longrightarrow & \operatorname{Im} a_1 & \longrightarrow & A_2 & \longrightarrow & \operatorname{Im} a_2 & \longrightarrow & 0 \end{array}$$

yields, via the snake lemma, the following exact sequence.

$$0 \longrightarrow \ker g_1 \longrightarrow \ker f_2 \longrightarrow \ker g_2 \longrightarrow \operatorname{coker} g_1 \longrightarrow \operatorname{coker} f_2 \longrightarrow \operatorname{coker} g_2 \longrightarrow 0$$

Then, sequences

$$\ker f_2 \longrightarrow \ker g_2 \longrightarrow \operatorname{coker} g_1$$

and

$$\operatorname{coker} f_2 \longrightarrow \operatorname{coker} g_2 \longrightarrow 0$$

are also exact. Since f_2 is an isomorphism we have $\ker f_2 \simeq 0$ and $\operatorname{coker} f_2 \simeq 0$. Moreover, we have $\operatorname{coker} g_1 \simeq 0$ and therefore, we get $\ker g_2 \simeq 0$ as well as $\operatorname{coker} g_2 \simeq 0$. From the other hand, since f_5 is an isomorphism ($\ker f_5 \simeq 0$) and the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \operatorname{Im} b_4 & \longrightarrow & B_5 & \longrightarrow & \operatorname{coker} b_4 & \longrightarrow & 0 \\ & & {\scriptstyle g_4}\uparrow & & {\scriptstyle f_5}\uparrow & & {\scriptstyle s}\uparrow & & \\ 0 & \longrightarrow & \operatorname{Im} a_4 & \longrightarrow & A_5 & \longrightarrow & \operatorname{coker} a_4 & \longrightarrow & 0 \end{array}$$

is commutative with exact rows we obtain, from the snake lemma, that $\ker g_4 \simeq 0$. Then, since

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \operatorname{Im} b_3 & \longrightarrow & B_4 & \longrightarrow & \operatorname{Im} b_4 & \longrightarrow & 0 \\ & & {\scriptstyle g_3}\uparrow & & {\scriptstyle f_4}\uparrow & & {\scriptstyle g_4}\uparrow & & \\ 0 & \longrightarrow & \operatorname{Im} a_3 & \longrightarrow & A_4 & \longrightarrow & \operatorname{Im} a_4 & \longrightarrow & 0 \end{array}$$

is commutative with exact rows, f_4 is an isomorphism and $\ker g_4 \simeq 0$ we get, from the snake lemma, $\ker g_3 \simeq 0$ and $\operatorname{coker} g_3 \simeq 0$. At last, since $\ker g_2 \simeq 0$, $\operatorname{coker} g_2 \simeq 0$, $\ker g_3 \simeq 0$, $\operatorname{coker} g_3 \simeq 0$ and the diagram

$$\begin{array}{ccccccccc} 0 & \longrightarrow & \operatorname{Im} b_2 & \longrightarrow & B_3 & \longrightarrow & \operatorname{Im} b_3 & \longrightarrow & 0 \\ & & {\scriptstyle g_2}\uparrow & & {\scriptstyle f_3}\uparrow & & {\scriptstyle g_3}\uparrow & & \\ 0 & \longrightarrow & \operatorname{Im} a_2 & \longrightarrow & A_3 & \longrightarrow & \operatorname{Im} a_3 & \longrightarrow & 0 \end{array}$$

is commutative with exact rows we get, form the snake lemma, that $\ker f_3 \simeq 0$ and $\operatorname{coker} f_3 \simeq 0$. Thus, f_3 is both mono and epi and therefore is an isomorphism. □

In the statement of the following theorem we will write the cokernel of a monomorphism $A \to B$ as B/A. This notation comes from the fact that in algebra quotient groups, quotient modules, quotient algebras etc. are in fact just cokernels of appropriate monomorphisms.

Theorem 6.5. (Third Isomorphism Theorem) Let $T \to N$ and $N \to M$ be monomorphisms. Then, there exists a monomorphism $N/T \to M/T$ and $(M/T)/(N/T) \simeq M/N$.

Proof. The following diagram commutes and has exact rows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & N & \longrightarrow & M & \longrightarrow & M/N & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & T & \longrightarrow & T & \longrightarrow & 0 & \longrightarrow & 0 \end{array}$$

Applying the snake lemma we get.

$$\begin{array}{ccccccccc} & & N/T & \to & M/T & \to & M/N & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & N & \longrightarrow & M & \longrightarrow & M/N & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & T & \longrightarrow & T & \longrightarrow & 0 & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & 0 & \longrightarrow & 0 & \longrightarrow & 0 & & \end{array}$$

Thus, we obtain the following short exact sequence.

$$0 \longrightarrow N/T \longrightarrow M/T \longrightarrow M/N \longrightarrow 0$$

Which finishes the proof. □

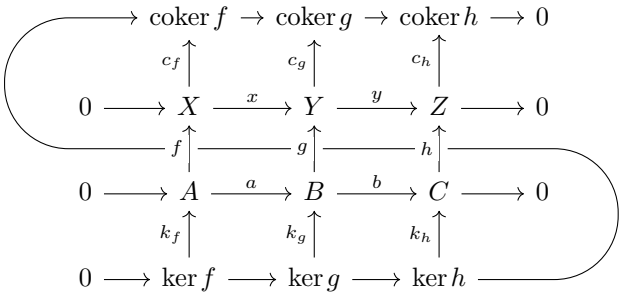
7. The Snake Lemma — Proof

I highly recommend that you try to prove the snake lemma by yourself checking with my proof when you get stuck. The proof is rather long and not very easy, so I don't expect you to be able to come up with it in full detail. But, since every concept we talked about throughout the course gets used here you can learn a lot by just trying to tackle it. In fact, this is the first time I've fully proven the snake lemma and even I can feel that I learnt quite a bit.

Lemma 7.1. (Snake Lemma) Let the following be a commutative diagram with exact rows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & X & \xrightarrow{x} & Y & \xrightarrow{y} & Z & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle f} & & \uparrow{\scriptstyle g} & & \uparrow{\scriptstyle h} & & \\ 0 & \longrightarrow & A & \xrightarrow{a} & B & \xrightarrow{b} & C & \longrightarrow & 0 \end{array}$$

Then, we get the following exact sequence of kernels and cokernels.

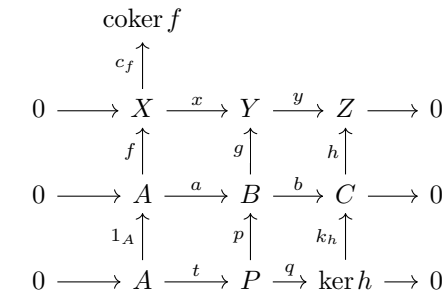


Proof. First, we construct all the morphisms. Since $k_f \cdot a \cdot g = k_f \cdot f \cdot x = 0$, $k_g \cdot b \cdot h = k_g \cdot g \cdot y = 0$, $f \cdot x \cdot c_g = a \cdot g \cdot c_g = 0$ and $g \cdot y \cdot c_h = b \cdot h \cdot c_h = 0$ we obtain ((co)kernel's universal properties) the following morphisms.

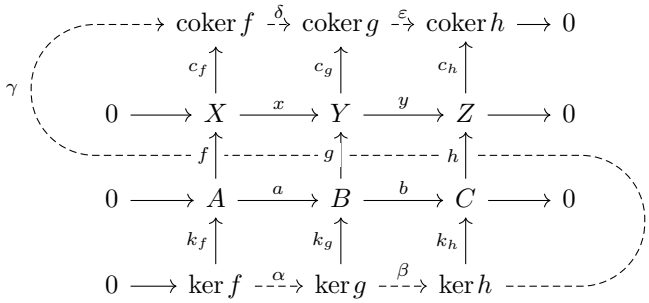
$$\begin{array}{ccccccccc} & & \operatorname{coker} f & \xrightarrow{\delta} & \operatorname{coker} g & \xrightarrow{\varepsilon} & \operatorname{coker} h & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle c_f} & & \uparrow{\scriptstyle c_g} & & \uparrow{\scriptstyle c_h} & & \\ 0 & \longrightarrow & X & \xrightarrow{x} & Y & \xrightarrow{y} & Z & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle f} & & \uparrow{\scriptstyle g} & & \uparrow{\scriptstyle h} & & \\ 0 & \longrightarrow & A & \xrightarrow{a} & B & \xrightarrow{b} & C & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle k_f} & & \uparrow{\scriptstyle k_g} & & \uparrow{\scriptstyle k_h} & & \\ 0 & \longrightarrow & \ker f & \xrightarrow{\alpha} & \ker g & \xrightarrow{\beta} & \ker h & & \end{array}$$

Let P be the pullback of $B \xrightarrow{b} C \xleftarrow{k_h} \ker h$. Then, we get the following commutative diagram

with exact rows.



Since $p\cdot g\cdot y = p\cdot b\cdot h = q\cdot k_h\cdot h = 0$ we get (kernel's universal property) the unique arrow $u: P\to X$ such that $u\cdot x = p\cdot g$. Morphism x is mono, thus from $1_A\cdot f\cdot x = t\cdot p\cdot g = t\cdot u\cdot x$ we get $1_A\cdot f = t\cdot u$. Then, $t\cdot u\cdot c_f = 1_A\cdot f\cdot c_f = 0$ and we obtain (cokernel's universal property) the unique morphism $\gamma: \ker h\to \operatorname{coker} f$ satisfying $q\cdot\gamma = u\cdot c_f$. Our diagram then looks like this.



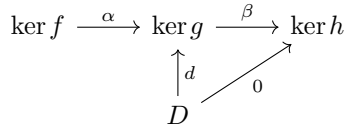
It remains to show exactness of the kernel and cokernel sequence.

$$0 \longrightarrow \ker f \xrightarrow{\alpha} \ker g \xrightarrow{\beta} \ker h \xrightarrow{\gamma} \operatorname{coker} f \xrightarrow{\delta} \operatorname{coker} g \xrightarrow{\varepsilon} \operatorname{coker} h \longrightarrow 0$$

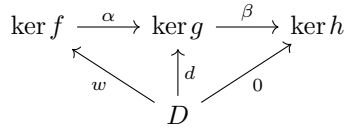
We first check that

$$0 \longrightarrow \ker f \xrightarrow{\alpha} \ker g \xrightarrow{\beta} \ker h$$

is exact, which is equivalent with $\alpha: \ker f\to\ker g$ being the kernel of β. Let D and $d: D\to\ker g$ be such that $d\cdot\beta = 0$.



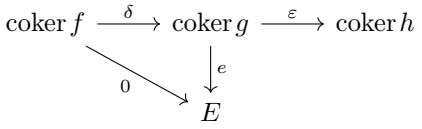
Then, since $d\cdot k_g\cdot b = d\cdot\beta\cdot k_h = 0$ there exists (kernel's universal property) a unique morphism $v: D\to A$ such that $v\cdot a = d\cdot k_g$. Thus, since x is mono and $v\cdot f\cdot x = v\cdot a\cdot g = d\cdot k_g\cdot g = 0 = 0\cdot x$ we get $v\cdot f = 0$ and therefore there exists (kernel's universal property) a unique morphism $w: D\to\ker f$ satisfying $w\cdot k_f = v$. Then, since k_g is mono and $w\cdot\alpha\cdot k_g = w\cdot k_f\cdot a = v\cdot a = d\cdot k_g$ we get $w\cdot\alpha = d$.



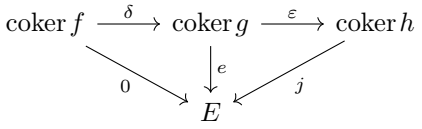
To show uniqueness of w consider an arrow $w' : D \to \ker f$ satisfying $w' \cdot \alpha = d$. Morphisms k_f and a are mono, therefore $k_f \cdot a$ is mono. Thus, from $w \cdot k_f \cdot a = w \cdot \alpha \cdot k_g = d \cdot k_g = w' \cdot \alpha \cdot k_g = w' \cdot k_f \cdot a$ we obtain $w' = w$. Now, lets show that

$$\operatorname{coker} f \xrightarrow{\delta} \operatorname{coker} g \xrightarrow{\varepsilon} \operatorname{coker} h \longrightarrow 0$$

is exact, which we know to be equivalent with $\varepsilon : \operatorname{coker} g \to \operatorname{coker} h$ being the cokernel of δ. Let E and $e : \operatorname{coker} g \to E$ be such that $\delta \cdot e = 0$.



Then, since $x \cdot c_g \cdot e = c_f \cdot \delta \cdot e = 0$ there exists (cokernel's universal property) a unique morphism $i : Z \to E$ such that $y \cdot i = c_g \cdot e$. Thus, since b is epi and $b \cdot h \cdot i = g \cdot y \cdot i = g \cdot c_g \cdot e = 0 = b \cdot 0$ we get $h \cdot i = 0$ and therefore there exists (cokernel's universal property) a unique morphism $j : \operatorname{coker} h \to E$ satisfying $c_h \cdot j = i$. Then, since c_g is epi and $c_g \cdot \varepsilon \cdot j = y \cdot c_h \cdot j = y \cdot i = c_g \cdot e$ we get $\varepsilon \cdot j = e$.



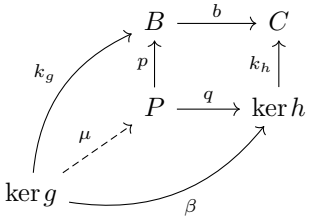
To show uniqueness of j consider an arrow $j' : \operatorname{coker} h \to E$ such that $\varepsilon \cdot j' = e$. Morphisms y and c_h are epi, therefore $y \cdot c_h$ is epi. Thus, from $y \cdot c_h \cdot j' = c_g \cdot \varepsilon \cdot j' = c_g \cdot e = c_g \cdot \varepsilon \cdot j = y \cdot c_h \cdot j$ we obtain $j' = j$. It remains to show that

$$\ker g \xrightarrow{\beta} \ker h \xrightarrow{\gamma} \operatorname{coker} f \xrightarrow{\delta} \operatorname{coker} g$$

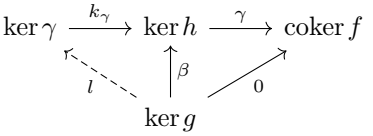
is exact, which we will prove in two steps. First, lets show that

$$\ker g \xrightarrow{\beta} \ker h \xrightarrow{\gamma} \operatorname{coker} f$$

is exact. Since P is the pullback of $B \xrightarrow{b} C \xleftarrow{k_h} \ker h$ we get.



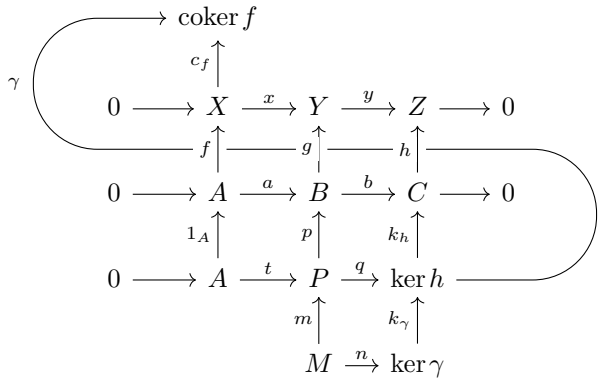
Recall the morphism $u : P \to X$ satisfying $u \cdot x = p \cdot g$ and $u \cdot c_f = q \cdot \gamma$. Then, since x is mono and $\mu \cdot u \cdot x = \mu \cdot p \cdot g = k_g \cdot g = 0 = 0 \cdot x$ we get $\mu \cdot u = 0$. Therefore, $\beta \cdot \gamma = \mu \cdot q \cdot \gamma = \mu \cdot u \cdot c_f = 0 \cdot c_f = 0$. We thus obtain the unique morphism.



We want to show that l is an epimorphism. Let M be the pullback of $P \xrightarrow{q} \ker h \xleftarrow{k_\gamma} \ker\gamma$.

$$\begin{array}{ccc} P & \xrightarrow{q} & \ker h \\ {\scriptstyle m}\uparrow & & \uparrow{\scriptstyle k_\gamma} \\ M & \xrightarrow{n} & \ker\gamma \end{array}$$

Then, we obtain the following diagram.



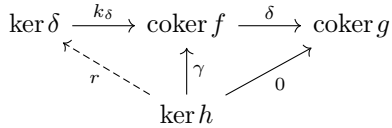
Recall that the morphism $u : P \to X$ satisfies $u \cdot c_f = q \cdot \gamma$. Since $m \cdot u \cdot c_f = m \cdot q \cdot \gamma = n \cdot k_\gamma \cdot \gamma = 0$ we get (recall that by definition $i_f : \operatorname{Im} f \to X$ is the kernel of c_f) the unique morphism $\eta : M \to \operatorname{Im} f$ satisfying $\eta \cdot i_f = m \cdot u$. Let O be the pullback of $A \xrightarrow{d_f} \operatorname{Im} f \xleftarrow{\eta} M$ (recall that by defintion $d_f : A \to \operatorname{Im} f$ is the cokernel of k_f).

$$\begin{array}{ccc} A & \xrightarrow{d_f} & \operatorname{Im} f \\ {\scriptstyle o}\uparrow & & \uparrow{\scriptstyle \eta} \\ O & \xrightarrow{s} & M \end{array}$$

Since $(s \cdot m \cdot p - o \cdot a) \cdot g = s \cdot m \cdot p \cdot g - o \cdot a \cdot g = s \cdot m \cdot u \cdot x - o \cdot f \cdot x = s \cdot \eta \cdot i_f \cdot x - o \cdot d_f \cdot i_f \cdot x = s \cdot \eta \cdot i_f \cdot x - s \cdot \eta \cdot i_f \cdot x = 0$ we get the unique morphism $\zeta : O \to \ker g$ satisfying $\zeta \cdot k_g = s \cdot m \cdot p - o \cdot a$. Then, since $k_\gamma \cdot k_h$ is mono and $\zeta \cdot l \cdot k_\gamma \cdot k_h = \zeta \cdot \beta \cdot k_h = \zeta \cdot k_g \cdot b = (s \cdot m \cdot p - o \cdot a) \cdot b = s \cdot m \cdot p \cdot b - o \cdot a \cdot b = s \cdot m \cdot q \cdot k_h - o \cdot 0 = s \cdot n \cdot k_\gamma \cdot k_h$ we get $\zeta \cdot l = s \cdot n$. Since d_f is epi and O is a pullback we get that s is epi. Since b is epi, P and M are pullbacks we get that n is epi. Thus, $\zeta \cdot l = s \cdot n$ is epi and therefore l is epi. We will now show that

$$\ker h \xrightarrow{\gamma} \operatorname{coker} f \xrightarrow{\delta} \operatorname{coker} g$$

is exact. Once again, recall the arrow $u : P \to X$ satisfying $u \cdot x = p \cdot g$ and $u \cdot c_f = q \cdot \gamma$. Since q is epi and $q \cdot \gamma \cdot \delta = u \cdot c_f \cdot \delta = u \cdot x \cdot c_g = p \cdot g \cdot c_g = 0 = q \cdot 0$ we get $\gamma \cdot \delta = 0$. Therefore, we obtain the unique morphism.



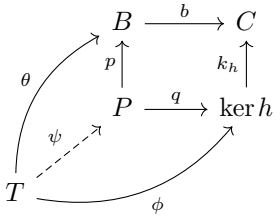
We want to show that r is an epimorphism. Let S be the pullback of $\ker\delta \xrightarrow{k_\delta} \operatorname{coker} f \xleftarrow{c_f} X$.

$$\begin{array}{ccc} \ker\delta & \xrightarrow{k_\delta} & \operatorname{coker} f \\ {\scriptstyle\lambda}\uparrow & & \uparrow{\scriptstyle c_f} \\ S & \xrightarrow{\nu} & X \end{array}$$

Then, since $\nu\cdot x\cdot c_g=\nu\cdot c_f\cdot\delta=\lambda\cdot k_\delta\cdot\delta=0$ we obtain the unique morphism $\kappa: S\to\operatorname{Im} g$ satisfying $\kappa\cdot i_g=\nu\cdot x$. Let T be the pullback of $S \xrightarrow{\kappa} \operatorname{Im} g \xleftarrow{d_g} B$.

$$\begin{array}{ccc} S & \xrightarrow{\kappa} & \operatorname{Im} g \\ {\scriptstyle\tau}\uparrow & & \uparrow{\scriptstyle d_g} \\ T & \xrightarrow{\theta} & B \end{array}$$

Since $\theta\cdot b\cdot h=\theta\cdot g\cdot y=\theta\cdot d_g\cdot i_g\cdot y=\tau\cdot\kappa\cdot i_g\cdot y=\tau\cdot\nu\cdot x\cdot y=\tau\cdot\nu\cdot 0=0$ we get the unique morphism $\phi: T\to\ker h$ that satisfies $\phi\cdot k_h=\theta\cdot b$. Therefore, we get the following morphism.



Since x is mono and $\psi\cdot u\cdot x=\psi\cdot p\cdot g=\theta\cdot g=\theta\cdot d_g\cdot i_g=\tau\cdot\kappa\cdot i_g=\tau\cdot\nu\cdot x$ we get $\psi\cdot u=\tau\cdot\nu$. Since k_δ is mono and $\phi\cdot r\cdot k_\delta=\phi\cdot\gamma=\psi\cdot q\cdot\gamma=\psi\cdot u\cdot c_f=\tau\cdot\nu\cdot c_f=\tau\cdot\lambda\cdot k_\delta$ we get $\phi\cdot r=\tau\cdot\lambda$. Since d_g is epi and T is a pullback we get that τ is epi. Since c_f is epi and S is a pullback we get that λ is epi. Thus, $\phi\cdot r=\tau\cdot\lambda$ is epi and therefore r is epi. □

The End

This is the end of my MBL 2021 course "Diagram Chasing in Abelian Categories". I want to thank you very much for attending. I hope that in the future you will keep in mind the categorical approach to mathematics and try to restate theorems, exercises, lemmas etc. in categorical terms. From my own experience I can say that the categorical view helped me immensly in understanding and comprehending all parts of mathematics I've encountered. Now, I cannot help but see categories appear everywhere.

8. Exercises — Day 1

Exercise 8.1. Construct a category in which there are no monomorphisms nor epimorphisms except for the identity arrows (the category must have at least one nonidentity arrow).

Exercise 8.2. Which of the following form categories:

- finite sets and functions
- sets and strictly increasing functions
- sets and injective functions

Exercise 8.3. Prove that the composition of two (composable) epimorphisms is an epimorphism.

Exercise 8.4. Let i be both mono and epi. Must i be an isomorphism?

Exercise 8.5. Show that if $f \cdot g$ is mono, then f is mono. Show that if $f \cdot g$ is epi, then g is epi.

Exercise 8.6. What are the epimorphisms in **Set**? What are the isomorphisms in **Set**?

Exercise 8.7. Construct in a "natural" way a morphism $\varepsilon : A + A \to A$.

Exercise 8.8. What functions correspond to morphisms $\eta : A \to A \times A$ and $\varepsilon : A + A \to A$ in **Set**?

Exercise 8.9. Show that, if it exists, the coproduct is unique up to an isomorphism.

Exercise 8.10. In a category with a zero object show that $A + 0 \simeq A$. What about $A \times 0$?

Exercise 8.11. Construct an arrow $(A \times B) + (A \times C) \to A \times (B + C)$.

Exercise 8.12. What are the monomorphisms, epimorphisms and isomorphisms in $\mathbf{Set}_*$?

Exercise 8.13. What are the products and coproducts in $\mathbf{Set}_*$?

Exercise 8.14. Show that two objects, A and B are isomorphic if and only if every arrow $A \to A$ factors through B and every arrow $B \to B$ factors through A (an arrow $X \to Y$ factors through Z if it is a composition of some arrows $X \to Z \to Y$).

9. Exercises — Day 2

In the following exercises we assume being in an abelian category.

Exercise 9.1. Does the category $\mathbf{Set}_*$ satisfy $\ker\operatorname{coker} f \simeq \operatorname{coker}\ker f$ for all f? If not, then for what f is this satisfied?

Exercise 9.2. Show that for all $f : A \to B$ the kernel $k_f : \ker f \to A$ is a monomorphism.

Exercise 9.3. Let the following be a commutative diagram.

$$\begin{array}{ccc} A & \xrightarrow{f} & B \\ \uparrow & & \uparrow \\ C & \xrightarrow{g} & D \end{array}$$

Show that it naturally induces arrows $\ker g \to \ker f$, $\operatorname{Im} g \to \operatorname{Im} f$ and $\operatorname{coker} g \to \operatorname{coker} f$.

Exercise 9.4. Show that the sequence

$$A_0 \xrightarrow{f_1} A_1 \xrightarrow{f_2} \ \dots \ \xrightarrow{f_n} A_n$$

is exact if and only if for all i the sequence

$$A_{i-1} \xrightarrow{f_i} A_i \xrightarrow{f_{i+1}} A_{i+1}$$

is exact.

Exercise 9.5. Show that the zero morphism $0 : A \to B$ is a monomorphism if and only if $A \simeq 0$ and is an epimorphism if and only if $B \simeq 0$.

Exercise 9.6. Show that a morphism $e : A \to B$ is epi if and only if $A \xrightarrow{e} B \longrightarrow 0$ is exact if and only if $\operatorname{coker} e \simeq 0$.

Exercise 9.7. Show that $0 \longrightarrow A \xrightarrow{f} B \xrightarrow{g} C$ is exact if and only if f is the kernel of g.

Exercise 9.8. The diagram $A \xrightarrow{f} B \xleftarrow{-g} C$ induces (coproduct's universal property) the unique morphism $h : A \oplus C \to B$ satisfying $i_A \cdot h = f$ and $i_C \cdot h = -g$. Show that the following is a pullback square.

$$\begin{array}{ccc} \ker h & \xrightarrow{k_h \cdot p_C} & C \\ \downarrow{\scriptstyle k_h \cdot p_A} & & \downarrow{\scriptstyle g} \\ A & \xrightarrow{f} & B \end{array}$$

Where $k_h : \ker h \to A \oplus C$ is the kernel of h. Conclude that in an abelian category all pullbacks exist.

Exercise 9.9. Show that in a pullback diagram

$$\begin{array}{ccc} P & \xrightarrow{q} & C \\ \downarrow{\scriptstyle p} & & \downarrow{\scriptstyle g} \\ A & \xrightarrow{f} & B \end{array}$$

the natural morphism $\operatorname{coker} q \to \operatorname{coker} f$ is mono.

10. Exercises — Day 3

In the following exercises we assume being in an abelian category.

Exercise 10.1. Show that f is an isomorphism if and only if $0 \longrightarrow A \xrightarrow{f} B \longrightarrow 0$ is exact.

Exercise 10.2. Show that an exact sequence

$$A_0 \xrightarrow{f_1} A_1 \xrightarrow{f_2} \ \dots \ \xrightarrow{f_n} A_n$$

gives rise to the following short exact sequences.

$$0 \longrightarrow \ker f_1 \xrightarrow{k_{f_1}} A_0 \xrightarrow{d_{f_1}} \operatorname{Im} f_1 \longrightarrow 0$$

$$0 \longrightarrow \operatorname{Im} f_i \xrightarrow{i_{f_i}} A_i \xrightarrow{d_{f_{i+1}}} \operatorname{Im} f_{i+1} \longrightarrow 0$$

$$0 \longrightarrow \operatorname{Im} f_n \xrightarrow{i_{f_n}} A_n \xrightarrow{c_{f_n}} \operatorname{coker} f_n \longrightarrow 0$$

Exercise 10.3. Consider the following commutative diagram with exact rows.

$$\begin{array}{ccccccccc} 0 & \longrightarrow & X & \xrightarrow{x} & Y & \xrightarrow{y} & Z & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle f} & & \uparrow{\scriptstyle g} & & \uparrow{\scriptstyle h} & & \\ 0 & \longrightarrow & A & \xrightarrow{a} & B & \xrightarrow{b} & C & \longrightarrow & 0 \end{array}$$

Show that:

- if f and h are mono then g is mono
- if f and h are epi then g is epi
- if f and h are isomorphisms then g is an isomorphism
- if g is epi then h is epi
- if g is mono then f is mono

Exercise 10.4. (Nine Lemma) Let the following be a commutative diagram with exact rows.

$$\begin{array}{ccccccccc} & & 0 & & 0 & & 0 & & \\ & & \uparrow & & \uparrow & & \uparrow & & \\ 0 & \longrightarrow & C_1 & \xrightarrow{c_1} & C_2 & \xrightarrow{c_2} & C_3 & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle g_1} & & \uparrow{\scriptstyle g_2} & & \uparrow{\scriptstyle g_3} & & \\ 0 & \longrightarrow & B_1 & \xrightarrow{b_1} & B_2 & \xrightarrow{b_2} & B_3 & \longrightarrow & 0 \\ & & \uparrow{\scriptstyle f_1} & & \uparrow{\scriptstyle f_2} & & \uparrow{\scriptstyle f_3} & & \\ 0 & \longrightarrow & A_1 & \xrightarrow{a_1} & A_2 & \xrightarrow{a_2} & A_3 & \longrightarrow & 0 \\ & & \uparrow & & \uparrow & & \uparrow & & \\ & & 0 & & 0 & & 0 & & \end{array}$$

Show that if the first two columns are exact then the third is exact. Show that if the last two columns are exact then the first is exact. Show that if $f_2 \cdot g_2 = 0$ and the first and last columns are exact then the middle column is exact.

Menelaus-Ceva Theorem

Marian Poljak

Abstract

See a geometric problem asking you to prove collinearity of three points or concurrency of three lines? We can often successfully apply Menelaus's and Ceva's theorem to these types of problems. The mentioned theorems also give us insight into many famous points of a triangle. Let's learn these interesting bits of geometry :)

1. Our tools

Theorem 1.1. (Menelaus's theorem) In a triangle ABC there are points X, Y, Z on lines BC, CA, AB, respectively, different from A, B, C. The lines AX, BY, CZ are collinear if and only if

$$\frac{|BX|}{|XC|}\cdot\frac{|CY|}{|YA|}\cdot\frac{|AZ|}{|ZB|}=1.$$

Theorem 1.2. (Ceva's theorem) In a triangle ABC there are points X, Y, Z on lines BC, CA, AB, respectively, different from A, B, C. The lines AX, BY, CZ are concurrent (or parallel) if and only if

$$\frac{|BX|}{|XC|}\cdot\frac{|CY|}{|YA|}\cdot\frac{|AZ|}{|ZB|}=1.$$

Equivalently, in the language of trigonometry,

$$\frac{\sin\angle XAC}{\sin\angle BAX}\cdot\frac{\sin\angle YBA}{\sin\angle CBY}\cdot\frac{\sin\angle ZCB}{\sin\angle ACZ}=1.$$

Theorem 1.3. (Law of sines) In a triangle ABC, with angles α, β, γ denoted as usual, it holds that

$$\frac{|BC|}{\sin\alpha}=\frac{|CA|}{\sin\beta}=\frac{|AB|}{\sin\gamma}.$$

Theorem 1.4. (Power of a point) Let $ABCD$ be a cyclic quadrilateral inscribed in a circle ω and let $X = AB\cap CD$ and T be a point such that XT is a tangent to ω. Then

$$|XA|\cdot|XB|=|XC|\cdot|XD|=|XT|^2.$$

Exercise 1.1. Show, using Ceva's theorem, that these triplets of lines are concurrent:

- The medians.
- The angle bisectors.
- The altitudes.
- The lines connecting vertices with the points where the incircle and the opposite side touch.
- The lines connecting vertices with the points where the excircle and the opposite side touch.

Exercise 1.2. Realize how Ceva's theorem implies the existence of isogonal conjugates. What are the isogonal conjugates of well-known points in a triangle?

Exercise 1.3. In a triangle ABC, denote N the midpoint of a median AM. Let P be a point on the side AC such that $|AC|=3|AP|$. Decide whether B, N, P are collinear.

Exercise 1.4. In a triangle ABC, the angle bisector from A meets BC at D, let I be the incenter. Express the ratio $|AI|/|ID|$ using the triangle side lengths.

2. Problems

2.1. (Van Aubel's theorem) In a triangle ABC let AD, BE, CF be cevians concurrent at X. Then it holds that

$$\frac{|AX|}{|XD|} = \frac{|AE|}{|EC|} + \frac{|AF|}{|FB|}.$$

2.2. The diagonals AC and BD of a quadrilateral $ABCD$ meet at M in such a way that $|AM| = |MC|$ and $|DM| = 2\cdot|MB|$. Suppose that X and Y are points on MC and BC respectively such that $\frac{|AC|}{|MX|} = \frac{|BY|}{|YC|} = 3$. Show that the points D, X and Y are collinear.

2.3. Let AD, BE, CF be altitudes in a triangle ABC. We denote M, N, P the midpoints of EF, FD, DE, respectively. Prove that AM, BN, CP are concurrent.

2.4. In a non-isosceles triangle ABC, denote I the incenter and D, E, F the points where the incircle touches the sides BC, CA, AB, respectively. Denote X a point inside ABC such that the inscribed circle of XBC touches BC in D and let the other two touches with XB, XC be Y, Z, respectively. Prove that EF, YZ and BC are concurrent.

2.5. (Newton-Gauss line) We have a convex quadrilateral $ABCD$, whose opposite sides are not parallel. Let $Q = BC \cap DA$ a $R = AB \cap CD$. Next denote X, Y, Z the midpoints of AC, BD, QR. Prove that X, Y, Z are collinear.

2.6. The diagonals of a convex quadrilateral $ABCD$ meet at P. Prove that

$$\frac{\sin\angle DAP}{\sin\angle PAB} \cdot \frac{\sin\angle ABP}{\sin\angle PBC} \cdot \frac{\sin\angle BCP}{\sin\angle PCD} \cdot \frac{\sin\angle CDP}{\sin\angle PDA} = 1.$$

2.7. We have a triangle ABC. A line through its centroid G meets AB and AC in F and E, respectively. Prove that

$$\frac{|BF|}{|FA|} + \frac{|CE|}{|EA|} = 1.$$

2.8. Let us have a triangle ABC and cevians AD, BE, CF. The circle circumscribed to triangle DEF intersects the sides once more in points D', E', F', respectively. Prove that AD', BE', CF' are also concurrent.

2.9. On a line p there are points A, Z, B in this order, Z is not the midpoint of AB. Choose arbitrarily some point X not on p and then arbitrary Y on the segment XZ. Denote $D = AX \cap BY$ and $E = BX \cap AY$. Now we got a line DE whose construction depends on our choice of X, Y. Prove that any such DE goes through a fixed point.

2.10 (Pascal's theorem)**.** Points A, B, C, D, E, F lie on the same circle (in any order). Let $L = AB \cap DE$, $M = BC \cap EF$, $N = CD \cap FA$. Prove that L, M, N are collinear.

2.11. Let ABC be any triangle and P any point in its interior. Let P_1, P_2 be the feet of the perpendiculars from P to the two sides AC and BC. Draw AP and BP and from C drop perpendiculars to AP and BP. Let Q_1 and Q_2 be the feet of these perpendiculars. If $Q_2 \neq P_1$ and $Q_1 \neq P_2$, then prove that the lines P_1Q_2, Q_1P_2 and AB are concurrent.

2.12 (Desargues's theorem)**.** Let ACB and $A'B'C'$ be two given triangles such that the lines AA',BB' and CC' are concurrent. Let X, Y and Z be, respectively, the points of intersection of the lines AB and $A'B'$, BC and $B'C'$ and CA and $C'A'$. Then X, Y and Z are collinear.

2.13. (IMO 2006 SL) Let $ABCDE$ be a convex pentagon such that $\angle BAC = \angle CAD = \angle DAE$ and $\angle ABC = \angle ACD = \angle ADE$. The diagonals BD and CE meet at P. Prove that the line AP bisects the side CD.

2.14. (USAMO 2012) There is a triangle ABC and a point P inside. A line p goes through P. We denote A' to be an intersection of BC and an image of line AP reflected by the line p. Analogically, we denote B', C'. Prove that A', B', C' are collinear.

2.15. Let A_1, A_2, A_3 be three points in the plane. For convenience, let $A_4 = A_1$ and $A_5 = A_2$ for $n = 1, 2, 3$, suppose that B_n is the midpoint of A_nA_{n+1} and suppose that C_n is the midpoint of A_nB_n. Suppose that A_nC_{n+1} and B_nA_{n+2} meet at D_n and that A_nB_{n+1} and C_nA_{n+2} meet at E_n. Calculate the ratio of the area of triangle $D_1D_2D_3$ to the area of triangle $E_1E_2E_3$.

2.16. (MEMO 2008) Let ABC be an isosceles triangle with $|AC| = |BC|$. Its incircle touches AB and BC at D and E, respectively. A line (different from AE) passes through A and intersects the incircle at F and G. The lines EF and EG intersect the line AB at K and L, respectively. Prove that $|DK| = |DL|$.

2.17. (IMO 2006 SL) Circles ω_1 and ω_2 with centres O_1 and O_2 are externally tangent at point D and internally tangent to a circle ω at points E and F, respectively. Line t is the common tangent of ω_1 and ω_2 at D. Let AB be the diameter of ω perpendicular to t, so that A, E and O_1 are on the same side of t. Prove that lines AO_1, BO_2, EF and t are concurrent.

2.18. In a triangle ABC, let I be the incenter, and let A', B', C' be the reflections of I through sides BC, CA, AB, respectively. Prove that the lines AA', BB', and CC' are concurrent.

2.19. (2005 Chinese Math Olympiad) A circle meets the three sides BC, CA, AB of triangle ABC at points $D_1, D_2; E_1, E_2$ and F_1, F_2, respectively. The line segments D_1E_1 and D_2F_2 intersect at point L, line segments E_1F_1 and E_2D_2 intersect at point M, line segments F_1D_1 and F_2E_2 intersect at point N. Prove that the three lines AL, BM and CN are concurrent.

References

[1] Math correspondence seminar PraSe library [www.prase.cz]

[2] Mathematical Excalibur 2005, Vol. 10, No. 3

Ramsey theory

Peter Simon

1. Problems for everyone

1.1. Every point of the plane is coloured either red or blue. Show that some **rectangle** has its vertices all the same color.

1.2.

(a) Every edge of a complete graph with 6 vertices (K_6) is coloured either red or blue. Show that there is a monochromatic triangle.

(b) Is this still true if we colour K_5?

1.3.

(a) Every positive integer is coloured either red or blue. Show that there is a monochromatic 3-term arithmetic progression.

(b) * Is it still true if we use **three** colours?

1.4. Show that there is an n for which the following true: if the edges of K_n is coloured either red or blue then there exists a monochromatic red triangle OR a monochromatic blue K_4.

1.5. Every point of the plane is coloured either red or blue. Prove that there exists $x, y \in \mathbb{R}$ and $d > 0$ such that the points (x,y), $(x+d,y)$ and $(x,y+d)$ have the same colour.

1.6.

(a) Let $R(k,l)$ be the smallest positive integer n, such that if the edges of the K_n is coloured either red or blue then there must be either a red K_k OR a blue K_l.

Prove that $R(k,l)$ exists and it is finite.

(b) Prove that $(n-1)^2 \leq R(n,n) \leq 4^n$.

1.7.

(a) $\mathbb{N}$ is 2-coloured. Prove that there exists a monochromatic 4-term AP.

(b) (Van der Waerden theorem) For every positive integers k and l there exists n such that if 1, 2, ..., n are k-coloured then there exists a monochromatic l-term AP.

1.8.

(a) The plane is 3-coloured. Show that there exist $x, y \in \mathbb{R}$ and $d > 0$ such that (x,y), $(x+d,y)$ and $(x,y+d)$ have the same colour.

(b) Show that it is still holds when the plane is k-coloured for any positive integer k.

1.9. The plane is 2-coloured. Show that there exists a monochromatic square.

2. Extra

2.1.

(a) The numbers 1, 2, ..., 100 are coloured either red or blue. Show that there is monochromatic solution to the equation $x+y=z$ ($x=y$ is allowed).

(b) x and y must be different.

2.2.

(a) How many 3-element subset of $\{1,2,\ldots,100\}$ can be chosen such that any pair of subsets has exactly one element in common.

(b) What if any pair of subsets does **not** have exactly one element in common?

2.3. The edges of a complete infinite graph is coloured either red or blue. Is it true that there must be a monochromatic complete infinite subgraph?

2.4. What is the minimal value for n in question 1.4?

Domino Tilings

Łukasz Bożyk

Abstract

Tiling boards with dominoes is a topic which evokes associations with some classical problems, but it turns out to be surprisingly deeper than just using the checkerboard coloring. During the course we will see and prove some not that well-known results about domino tilings. In particular we will be able to calculate (by hand!) the total number of tilings of an 8×8 chessboard with dominoes and explore some properties of figures called Aztec diamonds.

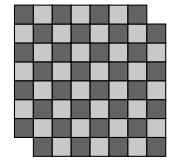
1. Preliminaries

1.1. Three basic observations

We will consider *figures* composed of *cells*, usually unit squares. Two cells are *adjacent* (or *neighboring*) if they share a side. If not stated otherwise, we will assume that figures are *connected*, i.e. starting from any cell we can reach every other by moving only between adjacent cells.

A *domino* is a 1×2 rectangle composed of two cells arranged *vertically* or *horizontally*. We say that a figure $\mathcal{F}$ can be *tiled with dominoes* if it can be covered with a collection of dominoes in such a way that each cell of $\mathcal{F}$ is covered by some domino and each domino covers exactly two whole cells of $\mathcal{F}$.

A *checkerboard coloring* of $\mathcal{F}$ is either of the two colorings of its cells with two colors (*light* and *dark*) with the property that every two adjacent cells have distinct colors. We denote by $\square(\mathcal{F})$ and $\blacksquare(\mathcal{F})$ the numbers of cells of respective colors (and omit the argument $\mathcal{F}$ when it's clear from the context).



Observation 1.1. If a figure $\mathcal{F}$ can be tiled with dominoes, then $\square = \blacksquare$.

Example 1.2 (Mutilated chessboard problem)**.** An 8×8 chessboard with two opposite corners removed cannot be tiled with dominoes.

Observation 1.3. If a figure $\mathcal{F}$ can be tiled with dominoes, then for every set L of light cells of $\mathcal{F}$ there are at least $|L|$ dark cells of $\mathcal{F}$ adjacent to at least one cell from L (we call these cells *neighbors* of L).

Example 1.4. Figure  satisfies $\square = \blacksquare$ but cannot be covered with dominoes.

Observation 1.5. If a figure $\mathcal{F}$ is tiled with dominoes and ℓ is a line dissecting $\mathcal{F}$ along cell borders in such a way that on both sides of ℓ there is an odd (respectively: even) number of cells of $\mathcal{F}$, then ℓ passes through (*cuts*) an odd (respectively: even) number of dominoes.

Example 1.6. For every tiling of the 6×6 square with dominoes there exists a line dissecting it into two smaller rectangles and not cutting any domino (such line is called a *fault line*).

1.2. The graph theoretical view

For a figure $\mathcal{F}$ define the *underlying graph* $G(\mathcal{F})$ as follows: vertices are the cells of $\mathcal{F}$ and edges join pairs of adjacent cells.

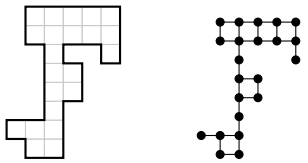
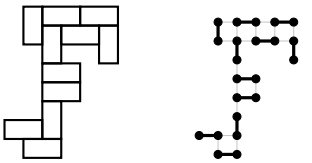


Figure $\mathcal{F}$ and the underlying graph $G(\mathcal{F})$.



A domino tiling of $\mathcal{F}$ and the corresponding perfect matching in $G(\mathcal{F})$.

Note that $\mathcal{F}$ is connected if and only if $G(\mathcal{F})$ is connected. Moreover, $G(\mathcal{F})$ is bipartite (with bipartition classes corresponding to colors of cells in the checkerboard coloring). Figure $\mathcal{F}$ can be tiled with dominoes if and only if $G(\mathcal{F})$ admits a *perfect matching*, i.e. a collection of edges covering each vertex exactly once.

Problems

Warm-up

1.1. In a tiling of a figure with a checkerboard coloring we can distinguish four types of dominoes (according to the position of the covered dark cell):

north  , *south*  , *east*  , *west*  .

Prove that in every tiling of a rectangular board there are equally many north and south tiles (analogously: equally many east and west tiles).

1.2. Find all positive integers n with the property that a $2n \times 2n$ square board admits a domino tiling with equally many horizontal and vertical tiles.

1.3. Consider an arbitrary domino tiling of a rectangular board $m \times n$ with $m, n \geq 2$.

(a) Prove that there exist two dominoes which form a 2×2 square.

(b) Prove that if there is only one such square, then $|m-n| \leq 2$.

1.4. Does every domino tiling of the 5×6 rectangle have a fault line?

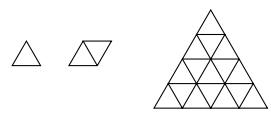
1.5. Prove that if $G(\mathcal{F})$ is Hamiltonian, then $\mathcal{F}$ can be tiled with dominoes in at least two different ways.

1.6. A 7×7 square is tiled with 24 dominoes and one 1×1 square. Determine all possible positions of the single 1×1 tile.

1.7 (Gomory's theorem)**.** Prove that if two cells of different colors are removed from an 8×8 chessboard, then the remaining figure (possibly containing holes) can be tiled with dominoes.

1.8. Prove that if a figure satisfies □ = ■ and every set L of light cells has at least $|L|$ dark neighbors, then every set D of dark cells has at least $|D|$ light neighbors.

1.9. In this problem cells are equilateral triangles of side 1 (*unit triangles*). *Lozenge* is a figure consisting of two adjacent cells. Suppose that an equilateral triangle of side n is tiled with a collection of unit triangles and lozenges. Find the least possible number of unit triangles used in such a tiling.



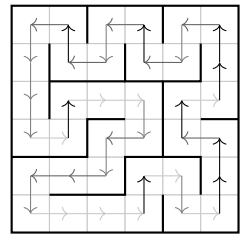
Challenge

1.10 (Hall's theorem)**.** Prove that if a figure satisfying □ = ■ can be tiled with dominoes if and only if every set L of light cells has at least $|L|$ dark neighbors.

1.11 (Encoding tilings with colorings)**.** We will say that a 2-coloring of a figure is *consistent* with a domino tiling of this figure if each domino covers cells of both colors. E.g. the checkerboard coloring is consistent with every tiling.

Consider any domino tiling T of an $m \times n$ board. Prove that there exists a coloring of this board which is consistent only with T (and no other tiling).

1.12. The picture presents a *maze* (closed loop visiting each cell exactly once) on a 6×6 board with the following property: in order to traverse the maze once, one has to perform equal number of steps in each of the four directions.



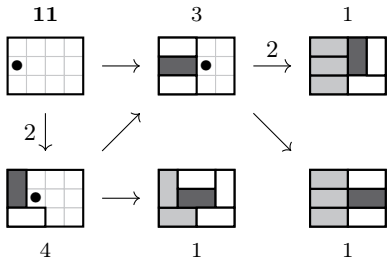
Can you design a maze with this property on an 8×8 board?

2. Direct counting

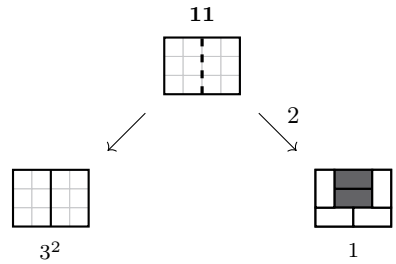
2.1. Case branching

In order to count tilings of a particular (small) figure, one can just carefully enumerate them, making sure that every tiling has been taken into account exactly once. Below we present a systematic way of simplifying such calculations and making it easier not to miss any case. It is simply a casework based upon possible placements of dominoes over respective cells or lines.

Example 2.1. There are 11 domino tilings of 3×4 rectangle.



Branching by possible placements of tiles covering cells marked with •.

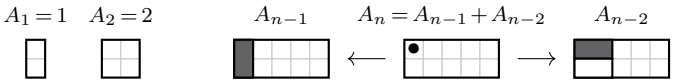


Branching by possible placements of tiles being cut by the dashed line.

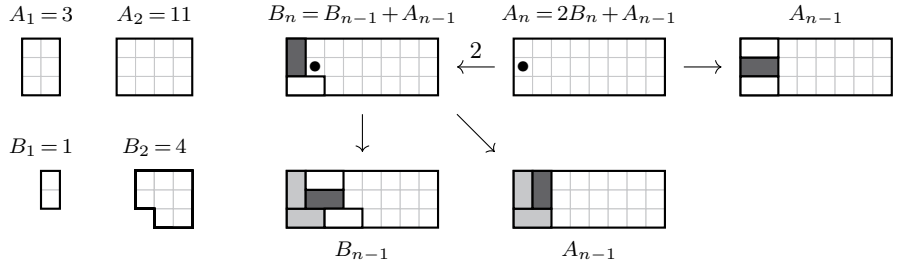
2.2. Recurrences

For general classes of figures (parameterized by some variables) it might be difficult to derive an exact formula. However, sometimes it is possible to obtain a recurrence relation between sought numbers of tilings of different sized figures.

Example 2.2. Let A_n be the number of domino tilings of $2\times n$ rectangle. Then $A_1=1$, $A_2=2$ and $A_n=A_{n-1}+A_{n-2}$ for $n\geq 2$.



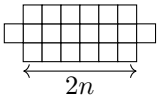
Example 2.3. Let A_n be the number of domino tilings of $3\times 2n$ rectangle. Then $A_1=3$, $A_2=11$ and $A_n=4A_{n-1}-A_{n-2}$ for $n\geq 2$.



Problems

Warm-up

2.1. How many domino tilings does a *candy* of length $2n$ have?

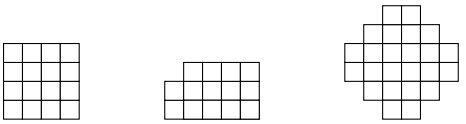


2.2. Count (directly) domino tilings of:

(a) 4×4 square;

(b) 3×5 rectangle without a corner cell;

(c) *Aztec diamond* of order 3.

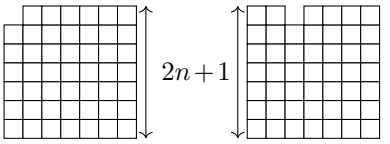


(a) (b) (c)

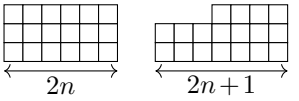
2.3. What is the number of ways to build a $2\times 2\times n$ chimney from $2\times 2\times 1$ bricks?

2.4. How many domino tilings of $2\times 2n$ board have equally many horizontal and vertical tiles?

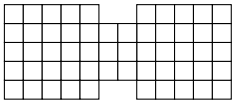
2.5. Prove that for every $n\geq 1$ the number of domino tilings of $(2n+1)\times(2n+1)$ board with one corner cell removed is equal to the number of domino tilings of this board with one cell at distance 2 from a corner cell removed.



2.6. Prove that the numbers of domino tilings of a $3\times 2n$ board and a $3\times(2n+1)$ board without a 1×3 corner are equal.



2.7. Prove that the number of domino tilings of the figure shown below is a perfect square.



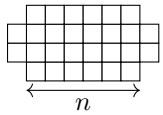
Challenge

2.8. Prove that for every n there exists a figure having exactly n domino tilings.

2.9. Count (directly and by hand) domino tilings of 6×6 square and check that the result is twice a perfect square.

2.10. Prove that for every n the number of ways to build a $2\times 2\times 2n$ chimney from $1\times 1\times 2$ bricks is a perfect square.

2.11. Find a recurrence (and sufficiently many boundary conditions) for the number of *fat candies* od length n.



2.12. Let $N(m,n)$ be the number of domino tilings of $m\times n$ board, where mn is even. Prove that for sufficiently large m and n:

$$1.272^{mn}\approx\sqrt{\varphi}^{mn}<N(m,n)<\sqrt{2}^{mn}\approx 1.414^{mn},$$

where $\varphi=\frac{1}{2}(1+\sqrt{5})$.

Fun fact. The actual asymptotic behavior of $N(n,n)$ (with n even) is:

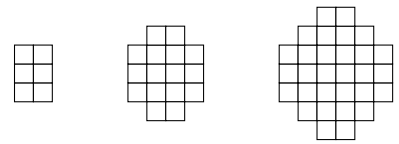
$$N(n,n)\sim\left(\mathrm{e}^{G/\pi}\right)^{n^2}\approx 1.339^{n^2},$$

where G is the *Catalan's constant* defined as

$$G=\sum_{k=0}^{\infty}\frac{(-1)^k}{(2k+1)^2}=1-\frac{1}{9}+\frac{1}{25}-\frac{1}{49}+\ldots$$

3. Augmented Aztec diamonds and Delannoy numbers

Augmented Aztec diamond of order n is the figure obtained from a $2n\times(2n+1)$ rectangle by cutting off $1+2+\ldots+(n-1)$ cells from each of the four corners in a way presented below.



Delannoy numbers $D_{m,n}$ are defined as follows: $D_{m,n}=1$ if $m=0$ or $n=0$, and for all $m,n\geq 1$

$$D_{m,n}=D_{m-1,n}+D_{m,n-1}+D_{m-1,n-1}.$$

m \ n	0	1	2	3
0	1	1	1	1
1	1	3	5	7
2	1	5	13	25
3	1	7	25	63

Theorem 3.1 (Sachs, Zernitz, 1991)**.** An augmented Aztec diamond of order n has exactly $D_{n,n}$ domino tilings.

Sketch of the proof. Consider not only symmetric diamonds, but also *skew* ones (defined with two parameters) to get the desired recurrence. Don't forget about checking the boundary conditions.

Problems

Warm-up

3.1. Prove that

$$D_{n,n} = \sum_{k=0}^{n} \binom{n}{k}^2 2^k.$$

3.2. Consider a $3^n \times 3^n$ matrix of Delannoy numbers $D_{i,j}$, where $0 \le i,j < 3^n$. Describe the set of entries of this matrix divisible by 3.

3.3. For a positive integer N let p_N denote the probability that Delannoy number $D_{m,n}$ is divisible by 3 if m and n are independently taken uniformly at random from the set $\{1,2,3,\ldots,N\}$. Calculate $\lim_{N\to\infty} p_N$.

Challenge

3.4. Prove that

$$D_{n,n} = \sum_{k=0}^{n} \binom{n}{k}\binom{n+k}{k}.$$

3.5. Delannoy number $D_{n,n}$ is a number of paths from the corner $(0,0)$ of a rectangular grid to the corner (n,n), using only single steps north, northeast, or east. Prove that among all these paths precisely $\lfloor D_{n,n} \rfloor$ consist of an odd number of steps.

4. Diagonal symmetry and tiling squares

With quite involved linear algebraic methods it is possible to derive the exact formula for the number of domino tilings of an $m \times n$ rectangular board. It was first proved in 1961 independently by Kasteleyn and by Fisher and Temperley that this number is equal to

$$\prod_{j=1}^{\lfloor \frac{m}{2} \rfloor} \prod_{k=1}^{\lfloor \frac{n}{2} \rfloor} \left(4\cos^2 \frac{\pi j}{m+1} + 4\cos^2 \frac{\pi k}{n+1} \right).$$

This number turns out to be an integer (and reduces properly to zero if mn is odd), however the form above makes it hard to explore its number theoretic properties. In 1994 Jockush provided a general combinatorial argument that for square boards the result is always a perfect square or twice a perfect square; we will prove a variant of this theorem.

Theorem 4.1 (Pachter, 1997)**.** The number of domino tilings of a $2n \times 2n$ board is of the form $2^n(2m+1)^2$ where m is a non-negative integer.

Sketch of the proof. There are three steps.

Step 1. Given a tiling T consider the tiling T' symmetric to T with respect to one of the board's diagonals d. Merge underlying graphs of both tilings to get a family of cycles (possibly some of length 2) and note that exactly n cycles pass through d. Within each of them (separately) one can switch between T and T', so the tilings group in sets of 2^n.

Step 2. From each group choose a proper representative: if w.l.o.g. d is dark require that tiles covering all cells of d contained in odd-numbered rows are either west, or south (cf. Problem 1.1). Note that the entire board can be cut into two congruent stair-shaped regions H_n without cutting any domino.

Step 3. Show that the number of tilings of H_n is odd by induction (reducing to H_{n-1}).

Problems

Warm-up

4.1. Verify that the general formula (the one with cosines) returns 0 if mn is odd.

4.2. Calculate the number of domino tilings of an 8×8 board.

4.3. Prove that for every $n\geq 1$ the number of domino tilings of an $n\times(n+1)$ rectangle is odd.

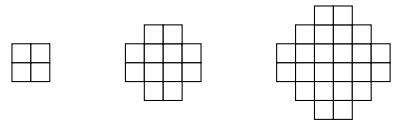
4.4. Prove that for every non-negative integer n the number of domino tilings of an $2^n\times 2^{n+1}$ rectangle is odd.

Challenge

4.5 (IMO 2016 Shortlist, Problem C8)**.** Let n be a positive integer. Determine the smallest positive integer k with the following property: it is possible to mark k cells on a $2n\times 2n$ board so that there exists a unique partition of the board into dominoes, none of which contains two marked cells.

5. The Aztec Diamond theorem

An *Aztec diamond* of order n is the figure consisting of $4\cdot\frac{1}{2}n(n+1)$ cells, as presented below.



$n=1$ $n=2$ $n=3$

Surprisingly, the formula for the number of tilings of such figures is seemingly simpler than the one for rectangles. It was first delivered by Elkies, Kuperberg, Larsen, and Propp in 1992 along with four different proofs. As of now there are many more proofs known.

Theorem 5.1 (Elkies, Kuperberg, Larsen, Propp, 1992)**.** The number of domino tilings of an Aztec diamond of order n is equal to $2^{1+2+\cdots+n}$.

Sketch of proof. Check out [5] for the entire proof.

Problems

Warm-up

5.1. For which n can an Aztec diamond of order n be covered with equally many north, south, east, and west tiles (cf. Problem 1.1)?

Challenge

5.2. For any covering of an Aztec diamond by dominoes, we may rotate by 90° any 2×2 square covered by exactly two dominoes. Prove that at most $\frac{1}{6}n(n+1)(2n+1)$ rotations are needed to transform an arbitrary covering into the covering consisting only of horizontal dominoes.

Further reading

[1] F. Ardila, R. P. Stanley: *Tilings**, Math Intelligencer **32**, 32–43 (2010). Available online: `arXiv:math/0501170`.

[2] W. Jockush: *Perfect Matchings and Perfect Squares*, Journal of Combinatorial Theory, Series A **67** (1994), 100–115.

[3] W. Jockusch, J. Propp, P. Shor: *Random Domino Tilings and the Arctic Circle Theorem*, `arXiv:math/9801068` (1998).

[4] N. Elkies, G. Kuperberg, M. Larsen, J. Propp: *Alternating sign matrices and domino tilings I, II*, Journal of Algebraic Combinatorics **1** (1992), 111–132, 219–234. Available online: `arXiv:math/9201305`.

[5] M. Fendler, D. Grieser: *A New Simple Proof of the Aztec Diamond Theorem*, Graphs and Combinatorics **32** (2016), 1389–1395. Available online: `arXiv:1410.5590`.

[6] M. Fisher, H. Temperley: *Dimer problem in statistical mechanics — an exact result*, Philosophical Magazine, **6** (1961), 1061–1063.

[7] P. Kasteleyn: *The statistics of dimers on a lattice I. The number of dimer arrangements on a quadratic lattice*, Physica **27** (1961), 1209–1225.

[8] L. Pachter: *Combinatorial Approaches and Conjectures for* 2*-Divisibility Problems Concerning Domino Tilings of Polyominoes*, The Electronic Journal of Combinatorics **4** (1997), #R29.

[9] H. Parlier, S. Zappa: *Distances in Domino Flip Graphs*, The American Mathematical Monthly **124** (2017), 710–722.

[10] J. Propp: *Dimers and dominoes*, `arXiv:1405.2615` (2014).

[11] J. Propp: *Enumeration of Tilings*, Handbook of Enumerative Combinatorics, edited by M. Bóna, CRC Press (2015), 541–588. Available online: `http://faculty.uml.edu/jpropp/eot.pdf`.

[12] H. Sachs, H. Zernitz: *Remark on the dimer problem*, Discrete Applied Mathematics **51** (1994), 171–179.

[13] W. Thurston: *Conway's tiling groups*, American Mathematical Monthly **97** (1990), 757–773.

Number Theory Theorems

Paweł Gadziński

1. Chebyshev theorem

We are going to prove this theorem in a few steps. We assume that $n > 80000$.

Lemma 1.1.

$$\prod_{m+1<p\leqslant 2m+1} p \leqslant 2^{2m} \quad \text{for all} \quad m \geqslant 1$$

Hint: consider $\binom{2m+1}{m}$.

Lemma 1.2.

$$\prod_{p\leqslant x} p \leqslant 4^{x-1} \quad \text{for all} \quad x \geqslant 2$$

Now, let's estimate value of $\binom{2n}{n}$.

Lemma 1.3. Prove that

$$\binom{2n}{n} \geqslant \frac{4^n}{2n}$$

Now we will try to obtain upper bound for $\binom{2n}{n}$.

Lemma 1.4. Prove that for prime $n \geqslant p > \frac{2}{3}n$, the number $\binom{2n}{n}$ is not divisible by p.

Lemma 1.5. Prove that

$$p^{v_p\left(\binom{2n}{n}\right)} < 2n$$

and

$$v_p\left(\binom{2n}{n}\right) = 1 \quad \text{for} \quad p > \sqrt{2n}.$$

Lemma 1.6. Prove that

$$\frac{4^n}{2n} \leqslant \prod_{p\leqslant\sqrt{2n}} 2n \cdot \prod_{\sqrt{2n}\leqslant p\leqslant\frac{2}{3}n} p \cdot \prod_{n<p\leqslant 2n} p$$

Now we are ready to prove the Theorem. Assume that $\prod_{n<p\leqslant 2n} p = 1$. Now we can show that estimation from Lemma above can't be true for big n.

Theorem 1.7. For every positive integer n there exist a prime number p which satisfies

$$2n \geqslant p > n.$$

2. Divergence of the sum of the reciprocals of primes

Assume that sum $\sum_{i=1}^{\infty} \frac{1}{p_i}$ converges. Let's take a natural number k. We are going to specify it later.

Definition 2.1. For some positive integer x, let M_x be the set of the numbers from $\{1,2,3,...,x\}$ that are divisible only by the primes equal or less than p_k.

Lemma 2.2. Prove that

$$|M_x| \leqslant 2^k \sqrt{x}.$$

Lemma 2.3. Prove that

$$|\{1,2,3,...,x\} - M_x| \leqslant \sum_{i=k+1}^{\infty} \frac{x}{p_i}.$$

Theorem 2.4. Let $p_1 = 2$, $p_2 = 3$, $p_3 = 5$, ..., be the sequence of all prime numbers. Then

$$\frac{1}{p_1} + \frac{1}{p_2} + \frac{1}{p_3} + ... = \infty$$

3. Lagrange's four-square theorem

At first, we will prove this theorem for prime numbers.

Lemma 3.1. Let a, b be the numbers that can be expressed as a sum of four squares. Prove that ab has this property too.

Proof.

$$\begin{aligned}(x_1^2+x_2^2+x_3^2+x_4)^2 \cdot (y_1^2+y_2^2+y_3^2+y_4)^2 = &(x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2+\\ &+(x_1y_2-x_2y_1+x_3y_4-x_4y_3)^2+\\ &+(x_1y_3-x_2y_4-x_3y_1+x_4y_2)^2+\\ &+(x_1y_4+x_2y_3-x_3y_2-x_4y_1)^2.\end{aligned}$$

□

Lemma 3.2. Let p be the prime numbers. Prove that there exists some numbers x_1, x_2, x_3, x_4 that the number

$$x_1^2+x_2^2+x_3^2+x_4^2$$

is divisible by p and less than p^2

Assume that

$$x_1^2+x_2^2+x_3^2+x_4^2 = mp,$$

where $m \leqslant p$ and m is the smallest possible.

Lemma 3.3. Prove that there exists integers y_1, y_2, y_3, y_4 that in the identity

$$\begin{aligned}(x_1^2+x_2^2+x_3^2+x_4^2)\cdot(y_1^2+y_2^2+y_3^2+y_4^2) =&(x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2+\\ &+(x_1y_2-x_2y_1+x_3y_4-x_4y_3)^2+\\ &+(x_1y_3-x_2y_4-x_3y_1+x_4y_2)^2+\\ &+(x_1y_4+x_2y_3-x_3y_2-x_4y_1)^2.\end{aligned}$$

every component of the right side is divisible by m^2 and

$$y_1^2+y_2^2+y_3^2+y_4^2<m^2$$

Lemma 3.4. For every prime p there exists numbers x_1, x_2, x_3, x_4 that

$$p=x_1^2+x_2^2+x_3^2+x_4^2.$$

4. Irrationality of e and e^2

Definition 4.1. Let number e be

$$e=\lim_{n\to\infty}\left(1+\frac{1}{n}\right)^n$$

Lemma 4.2. Prove that

$$e=\sum_{k=0}^{\infty}\frac{1}{k!}$$

Theorem 4.3.

$$e^x=\sum_{k=0}^{\infty}\frac{x^k}{k!}$$

Assume that $e=\frac{a}{b}$ for some non-zero integers a, b.

Theorem 4.4. Prove that e is irrational.

Theorem 4.5. Prove that e^2 is irrational.

5. Sophie Germain Theorem

Theorem 5.1. Let p be the prime number, that $q=2p+1$ is also a prime number. If a, b, c are the integers that

$$a^p+b^p+c^p=0,$$

then $p\mid abc$.

Lemma 5.2. Let $q=2n+1>3$ be a prime number and a, b, c be integers that

$$a^n\pm b^n\pm c^n\equiv 0 \pmod q,$$

then $abc\equiv 0 \pmod q$

Definition 5.3. Let $p>2$ be the prime number. We call p a Sophie Germain prime if and only if number $q=2p+1$ is also prime.

Let p be the Sophie Germain prime and let $q=2p+1$. Assume that there exists such integers a, b and c that

$$a^p+b^p+c^p=0,$$

and abc is not divisible by p.

Lemma 5.4. Prove that there exist integers a, b, c that

$$a^p+b^p+c^p=0,$$

and $gcd(a,b,c)=1$.

Let's write

$$(-a)^p=(b+c)(b^{p-1}-b^{p-2}c+...-bc^{p-2}+c^{p-1})$$

Lemma 5.5. Prove that

$$gcd(b+c,\ b^{p-1}-b^{p-2}c+...-bc^{p-2}+c^{p-1})=1.$$

We can conclude that $a+b$, $b+c$, $c+a$ are of the from x^p. Let

$$a+b=A^p,\quad c+a=B^p,\quad a+b=C^p.$$

Also we can write

$$b^{p-1}-b^{p-2}c+...-bc^{p-2}+c^{p-1}=X^p.$$

Lemma 5.6. Prove that $q\,|\,abc$.

WLOG assume that $q\,|\,a$.

Lemma 5.7. Prove that $q\,|\,A$.

Lemma 5.8. Prove that $X^p\equiv\pm1 \pmod q$.

Theorem 5.9. Let p be the prime number, that $q=2p+1$ is also a prime number. If a, b, c are the integers that

$$a^p+b^p+c^p=0,$$

then $p\,|\,abc$.

6. Very fancy proof of Two Squares Theorem

This proof is extremely tricky and short. Let $p=4k+1$. Consider set S of a triples (x,y,z) of non-negative numbers which satisfy

$$x^2+4yz=p.$$

Consider such function f

$$f(x,y,z)\mapsto\begin{cases}(x+2z,\ z,\ y-x-z), & \text{if } x<y-z\\ (2y-x,\ y,\ x-y+z), & \text{if } y-z<x<2y\\ (x-2y,\ x-y+z,\ y), & \text{if } x>2y\end{cases}$$

Lemma 6.1. Prove that f is involution(it means that $f(f(x,y,z)) = (x,y,z)$.

Lemma 6.2. Determine all triples (x,y,z) such that $f(x,y,z) = (x,y,z)$

Lemma 6.3. Conclude that number of the elements of the S is odd.

Lemma 6.4. Prove that the involution $g(x,y,z) = (x,z,y)$ has a fixed point.

Szemerédi Regularity Lemma

Andrzej Grzesik

Abstract

Szemerédi Regularity Lemma is one of the most powerful tool in extremal graph theory. Informally, the lemma states that we can partition the vertices of any large graph into a bounded number of parts so that edges between almost all parts behave "random-like". Since such randomly behaving parts are easier to treat, the lemma usually offers conceptually simple proofs for asymptotic results. During the course we will explain the lemma, sketch its proof and provide some of its important applications, in particular Counting Lemma, Graph Removal Lemma, Embedding Lemma and Roth's theorem on arithmetic progressions.

1. Regular pairs

Before we state the lemma we need to fix some notation and present basic definitions.

Let $e(G)$, $\Delta(G)$, $\delta(G)$ and $\chi(G)$ be respectively the number of edges, the maximum degree, the minimum degree and the chromatic number of G. By $N(v)$ and $\deg(v)$ we denote the set of neighbors of a vertex v and its degree, and by $\deg_Y(v)$ the number of neighbors of v in some set Y.

Definition 1.1. Given a graph $G=(V,E)$ and disjoint vertex subsets $X,Y\subseteq V$ let $e(X,Y)$ and $d(X,Y)$ be the number of edges and the *edge density* between X and Y, that is,

$$e(X,Y) := |\{(x,y)\in X\times Y \ : \ xy\in E(G)\},$$

$$d(X,Y) := \frac{e(X,Y)}{|X||Y|}.$$

Definition 1.2 (regular pair)**.** For $\varepsilon>0$, a pair (X,Y) of disjoint vertex subsets is *ε-regular* if for any $A\subseteq X$, $B\subseteq Y$ with $|A|\geq\varepsilon|X|$, $|B|\geq\varepsilon|Y|$, it holds

$$|d(A,B)-d(X,Y)|<\varepsilon.$$

We call a pair ε-irregular if it is not ε-regular.

Roughly, a regular pair (X,Y) is a pair whose edge density is close to the edge density of any two subsets A and B that are not too small. In other words, an ε-regular pair (X,Y) has "uniform" edge distribution — edges between any pair of large (ε-proportion) subsets are distributed roughly the same as in the whole pair.

1.1. Prove that for any bipartite graph with parts A and B, and for all integers $k<|A|$, $\ell<|B|$,

$$d(A,B)=\frac{1}{\binom{|A|}{k}\binom{|B|}{\ell}}\sum(d(C,D) \ : \ C\subset A,|C|=k,D\subset B,|D|=\ell).$$

Conclude from it that in order to verify if a pair (X,Y) is ε-regular it is sufficient to check the regularity condition only for sets of size $|A|=\lfloor\varepsilon|X|\rfloor+1$ and $|B|=\lfloor\varepsilon|Y|\rfloor+1$.

Solution. After multiplying both sides by $\binom{|A|}{k}\binom{|B|}{\ell}k\ell$ we get on both sides the number of edges $e(A,B)$ counting each edge exactly $\binom{|A|-1}{k-1}\binom{|B|-1}{\ell-1}$ times. The conclusion follows from the triangle inequality. □

One of the most important property of regular pairs is that almost all vertices in a regular pair have nicely distributed neighbors.

Lemma 1.3 (Degree lemma)**.** If (X,Y) is an ε-regular pair with density d, then for any $B\subset Y$, $|B|\geq\varepsilon|Y|$ we have

$$|\{x\in X\ :\ deg_B(x)\leq(d-\varepsilon)|B|\}|<\varepsilon|X|.$$

1.2. Prove Lemma 1.3.

Solution. Assume the contrary and take A as the set of vertices with small degree to B. We get a contradiction with the regularity condition for (A,B). □

The next lemma states that regularity is inherited by large subsets of pairs (with a slightly worse regularity). This lemma is useful as it implies that we can further refine a regular partition to get additional properties without losing regularity.

Lemma 1.4 (Slicing lemma)**.** Let (X,Y) be an ε-regular pair with density d, and, for some $\alpha\geq\varepsilon$, let $X'\subset X$, $|X'|\geq\alpha|X|$, $Y'\subset Y$, $|Y'|\geq\alpha|Y|$. Then (X',Y') is an ε'-regular pair with density d', where $\varepsilon'=\max\{\varepsilon/\alpha,2\varepsilon\}$ and $|d-d'|<\varepsilon$.

1.3. Prove the slicing lemma.

Solution. Firstly, observe that since $|X'|\geq\varepsilon|X|$ and $|Y'|\geq\varepsilon|Y|$, the ε-regularity of (X,Y) gives $|d(X',Y')-d(X,Y)|=|d'-d|<\varepsilon$.

Now for any $A\subseteq X'$, $|A|\geq\varepsilon'|X'|\geq\frac{\varepsilon}{\alpha}|X'|\geq\varepsilon|X|$, and $B\subseteq Y'$, $|B|\geq\varepsilon'|Y'|\geq\varepsilon|Y|$, the ε-regularity of (X,Y) gives $|d(A,B)-d(X,Y)|<\varepsilon$. Hence, by the triangle inequality,

$$|d(A,B)-d(X',Y')|\leq|d(A,B)-d(X,Y)|+|d(X,Y)-d(X',Y')|<2\varepsilon\leq\varepsilon',$$

which means that (X',Y') is ε'-regular, as desired. □

This lemma allows for example to prove generalization of Lemma 1.3 saying that not only single vertices have nicely distributed degrees, but also pairs of vertices (or bigger sets).

Lemma 1.5 (Common neighborhood lemma)**.** Let (X,Y) be an ε-regular pair with density d. For any subset $B\subseteq Y$ with $|B|\geq\varepsilon|Y|/(d-\varepsilon)$, we have

$$|\{(u,v)\in X\times X\ :\ |B\cap N(u)\cap N(v)|<(d-\varepsilon)^2|B|\}|\leq2\varepsilon|X|^2.$$

1.4. Prove the common neighborhood lemma.

Solution. Follows from the degree lemma and slicing lemma. □

1.5. State and prove a similar lemma for bigger size of the common neighborhood.

Solution. For a set of size s, take $|B|\geq\varepsilon|Y|/(d-\varepsilon)^{s-1}$ and prove that the common neighborhood is smaller than $(d-\varepsilon)^s|B|$ only for at most $s\varepsilon|X|^s$ sets of size s. The proof follows by induction using degree lemma as the base step and slicing lemma in the induction step. □

1.6. Prove that the number of 4-cycles in a regular pair is roughly the same as in random bipartite graph. Formally speaking, prove that if (X,Y) is an ε-regular pair in a graph G with $|X|=|Y|=n$ and density $d\geq 2\varepsilon$, then the number of 4-cycles $v_1v_2v_3v_4$ in G with $v_1,v_3\in X$ and $v_2,v_4\in Y$ is at least $((1-\varepsilon)^2(d-\varepsilon)^4-2/n)n^4$.

SOLUTION. Let X_0 be the set of vertices of X with less than $(d-\varepsilon)n$ neighbors in Y. By Lemma 1.3, $|X_0|<\varepsilon n$. We will count only the 4-cycles with $v_1\in X\setminus X_0$. Let Y_1 be the set of neighbors of v_1 in Y. Then $|Y_1|\geq(d-\varepsilon)n\geq\varepsilon n$. Let X_1 be the set of vertices of X with less than $(d-\varepsilon)|Y_1|$ neighbors in Y_1. By Lemma 1.3, $|X_1|<\varepsilon n$.

Let us now estimate the number c of choices of $v_1\in X\setminus X_0$ and $v_3\in X\setminus X_1$, and their common neigbors v_2, $v_4\in Y$. The number of common neighbors of v_1 and v_3 is at least $(d-\varepsilon)|Y_1|\geq(d-\varepsilon)^2n$. Since $|X\setminus X_0|\geq(1-\varepsilon)n$ and $|X\setminus X_1|\geq(1-\varepsilon)n$, we have $c\geq(1-\varepsilon)^2(d-\varepsilon)^4n^4$.

Not all choices counted by c are 4-cycles, since we can have $v_1=v_3$ or $v_2=v_4$. However, the number of such "degenerate" 4-cycles is at most $2n^3$. Therefore, the number of all sought 4-cycles is at least $c-2n^3\geq((1-\varepsilon)^2(d-\varepsilon)^4-2/n)n^4$. □

1.7. Let G be a graph and let (A,B), (B,C) and (A,C) be ε-regular pairs in G for some $\varepsilon>0$, with $|A|=|B|=|C|=n$ and $d(A,B),d(B,C),d(A,C)\geq 2\varepsilon$. Prove that the number of triangles abc in G with $a\in A$, $b\in B$, $c\in C$ is at least

$$(1-2\varepsilon)(d(A,B)-\varepsilon)(d(B,C)-\varepsilon)(d(A,C)-\varepsilon)n^3.$$

SOLUTION. Let A_0 be the set of vertices of A with less than $(d(A,B)-\varepsilon)n$ neighbors in B, and let A_1 be the set of vertices of A with less than $(d(A,C)-\varepsilon)n$ neighbors in C. By Lemma 1.3, $|A_0|,|A_1|<\varepsilon n$. We will count only the triangles with $a\in A\setminus(A_0\cup A_1)$.

Let B_a and C_a be the sets of neighbors of a in B and C, respectively. Then $|B_a|\geq(d(A,B)-\varepsilon)n\geq\varepsilon n$ and $|C_a|\geq(d(A,C)-\varepsilon)n\geq\varepsilon n$. By the ε-regularity of (B,C), we have $d(B_a,C_a)\geq d(B,C)-\varepsilon$. To give the lower bound for the sought number of triangles, we estimate the number of choices $a\in A\setminus(A_0\cup A_1)$, $b\in B_a$ and $c\in C_a$ such that b and c are adjacent. We have $|A\setminus(A_0\cup A_1)|\geq(1-2\varepsilon)n$ and

$$e(B_a,C_a)\geq(d(B,C)-\varepsilon)|B_a||C_a|\geq(d(B,C)-\varepsilon)(d(A,B)-\varepsilon)(d(A,C)-\varepsilon)n^2.$$

Hence, the number of triangles is at least $(1-2\varepsilon)(d(A,B)-\varepsilon)(d(B,C)-\varepsilon)(d(A,C)-\varepsilon)n^3$. □

This can be highly generalized into the following very useful theorem.

THEOREM 1.6 (Counting Lemma)**.** Let H be a graph on k vertices and let $V_1,V_2,\ldots,V_k$ be disjoint sets of size n such that all pairs (V_i,V_j) are ε-regular and $d(V_i,V_j)=d_{ij}>C\varepsilon$, where C is a constant depending only on H. Then the number of copies of H in $V_1\cup V_2\cup\ldots\cup V_k$ is at least

$$\prod_{ij\in E(H)}(d_{ij}-C\varepsilon)n^k.$$

2. Regularity Lemma

Theorem 2.1 (Szemerédi Regularity Lemma, 1978)**.** For every $\varepsilon > 0$ and m there exists M such that every graph on at least M vertices has a partition of the vertex set into $k+1$ classes $V_0, V_1, V_2, \ldots, V_k$ satisfying:
— $m \le k \le M$,
— $|V_0| < \varepsilon |V|$,
— $|V_1| = |V_2| = \ldots = |V_k|$,
— all but at most εk^2 of the pairs (V_i, V_j) with $1 \le i < j \le k$ are ε-regular.

If we have a sequence (G_n) of graphs with $e(G_n) = o(n^2)$, the Regularity Lemma becomes trivial: G_n is approximated by the empty graph. Thus the Regularity Lemma is useful only for large, dense graphs.

The role of m is to make the classes V_i sufficiently small, so that the number of edges inside those classes is negligible.

We can have no exceptional set (by distributing V_0 equally to other parts) and instead have $||V_i| - |V_j|| \le 1$ for all $1 \le i \le j \le k$.

2.1. Show that the Szemerédi Regularity Lemma is false when all pairs of parts are required to be ε-regular.
Hint: Consider the bipartite graph with two sets of vertices $A = B = \{1, 2, \ldots, n\}$ such that $a \in A$ and $b \in B$ are joined by an edge if $a + b \ge n$.

Before we proceed to the proof of the Szemerédi Regularity Lemma we sketch the main idea how to find the sought partition. We start with any partition and whenever the current partition is not ε-regular, for each (V_i, V_j) that is not ε-regular we find $A_{i,j} \subset V_i$ and $A_{j,i} \subset V_j$ witnessing the irregularity of (V_i, V_j), and simultaneously refine the partition using all $A_{i,j}$. If this process stops after a bounded number of steps, the regularity lemma would be successfully proven. To show that we will stop in a bounded amount of time, we will apply a technique called the energy increment argument. We define a measure called index (or energy) measuring how regular the pairs are in the partition. Each refinement will enlarge the index, but since it is bounded, we will stop after a finite number of steps.

We say that a partition P of V into $V_0, V_1, \ldots, V_k$ is *equitable* if $V_1 = V_2 = \ldots = V_k$. We define the *index* of an equitable partition P as

$$\operatorname{ind}(P) = \frac{1}{k^2} \sum_{1 \le i < j \le k} d^2(V_i, V_j).$$

Note that obviously, $\operatorname{ind}(P) \le \frac{1}{2}$. Here is the central observation in the proof of the Regularity Lemma.

Lemma 2.2. Let $G = (V, E)$ be a graph on n vertices and let P be an equitable partition of V into classes $V_0, V_1, \ldots, V_k$ with $|V_0| < \varepsilon n$ and $4^k > 600\varepsilon^{-5}$. If more than εk^2 pairs (V_i, V_j) for $1 \le i < j \le k$ are ε-irregular, then there is a refinement Q of P with $1 + k4^k$ classes, such that

$$\operatorname{ind}(Q) \ge \operatorname{ind}(P) + \frac{\varepsilon^5}{20}$$

and the exceptional class of Q is of size at most $|V_0| + \frac{n}{4^k}$.

The proof of the lemma is very technical, so we omit it. This lemma is enough to prove the Szemerédi Regularity Lemma.

PROOF OF THEOREM 2.1. Let s be the smallest integer satisfying $4^s > 600\varepsilon^{-5}$, $s \geq m$ and $s > 2/\varepsilon$. Take any equitable partition with $s+1$ parts and the exceptional set of size at most $\varepsilon n/2$. Let $f(k)+1$ be the number of classes after k applications of Lemma 2.2, i.e., $f(0) = s$ and $f(k+1) = f(k)4^{f(k)}$ for all positive integers k. Since the index of a partition is bounded by $1/2$, there exists an integer t being the largest integer for which there exists an equitable partition P of V into $1+f(t)$ classes with

$$\mathrm{ind}(P) \geq t\frac{\varepsilon^5}{20}.$$

By the maximality of t, Lemma 2.2 implies that this partition is ε-regular. Moreover,

$$|V_0| \leq \varepsilon n\left(1 - \frac{1}{2^{t+1}}\right) < \varepsilon n.$$

Setting $M = f(\lfloor 10\varepsilon^{-5} \rfloor)$, we have produced the partition we wanted. □

The upper bound on M coming from the above proof of the regularity lemma is rather large, it is a tower function with height $2\varepsilon^{-5}$. Such a tower bound is indeed needed, as Gowers constructed a graph with ε-regular partitions requiring a tower of 2's with height $\varepsilon^{-1/16}$.

In most applications of the Regularity Lemma one starts with applying Theorem 2.1 to create a regular partition, then gets rid of all edges within the classes of the partition, the edges of irregular pairs, as well as those of regular pairs with too low densities. The leftover "pure" graph is much easier to handle and it still contains most of the original edges. The following precise formulation of this process is a simple consequence of the Regularity Lemma.

THEOREM 2.3 (Degree Form)**.** For every $\varepsilon > 0$ there exists an integer M such that for any real number $d \in [0,1]$ and every graph G there is a subgraph $G' \subseteq G$ with partition of the vertex set V into $k+1$ classes $V_0, V_1, V_2, \ldots, V_k$ satisfying:
— $k \leq M$,
— $|V_0| < \varepsilon|V|$,
— $|V_1| = |V_2| = \ldots = |V_k| \leq \varepsilon|V|$,
— there are no edges in G' inside V_i for all $i \geq 1$,
— $\deg_{G'}(v) > \deg_G(v) - (d+\varepsilon)|V|$ for all $v \in V$,
— all pairs (V_i, V_j) in G' with $1 \leq i < j \leq k$ are ε-regular with density either 0 or greater than d.

In applications we often start with a graph G on n vertices and appropriate parameters ε and d, obtain G' with a partition $V_0, V_1, \ldots, V_k$, and then drop the set V_0 to get a "pure" graph G''. This graph G'' is much easier to deal with, and it still contains most of the original edges as

$$\deg_{G''}(v) > \deg_G(v) - (d+\varepsilon)n - |V_0| \geq \deg_G(v) - (d+2\varepsilon)n \quad \text{for all} \quad v \in V(G'')$$

and

$$e(G'') > e(G) - (d+3\varepsilon)n^2/2.$$

3. Applications

Typical applications of the Szemerédi Regularity Lemma are reducing the considered extremal problem A on large graphs to a problem B on small weighted graphs using the random behavior of the regular partition, and solving problem B using classical results in graph theory. Therefore let's start with the formal definition of the reduced graph obtained from applying regularity lemma to a large graph.

Definition 3.1 (Reduced graph)**.** For an ε-regular partition $V_0, V_1, V_2, \ldots, V_k$ of G and $d > 0$, the *reduced graph* $R = R(\varepsilon, d)$ is a graph with $V(R) = \{1, 2, \ldots, k\}$ and edge ij if and only if (V_i, V_j) is ε-regular pair with density at least d.

Important consequence of the Regularity Lemma is the triangle removal lemma due to Ruzsa and Szemerédi, which states that an almost triangle-free graph (with $o(n^3)$ triangles) can be made triangle-free by removing a negligible amount of edges ($o(n^2)$). The reverse implication is easy.

3.1. Prove that if n-vertex graph G contains at least cn^3 triangles for some constant c, then one need to remove at least cn^2 edges to make it triangle-free.

Theorem 3.2 (Triangle Removal Lemma)**.** For every $c > 0$ there exists $a > 0$ such that every n-vertex graph G contains at least an^3 triangles, or can be made triangle-free by removing at most cn^2 edges.

Proof. Apply Szemerédi Regularity Lemma in the degree form (Theorem 2.3) for sufficiently small ε and $d = 3\varepsilon$ to obtain the reduced graph R. If R has a triangle, then the Counting Lemma (Theorem 1.6, or the exercise before it) implies the lower-bound in the number of triangles, which contradicts the assumption (provided the chosen ε is small enough). If R is triangle-free, then also G'' is triangle-free, thus the edges removed from G while constructing G'' are the sought edges and their number is upper-bounded by $(d + 3\varepsilon)n^2/2 = 3\varepsilon n^2$. □

This theorem can be generalized from triangles to any subgraphs.

Theorem 3.3 (Graph Removal Lemma)**.** For every $c > 0$ and graph H on k vertices there exists $a > 0$ such that every n-vertex graph G contains at least an^k subgraphs isomorphic to H, or can be made H-free be removing at most cn^2 edges.

3.2. Prove the Graph Removal Lemma for $H = K_4$.

3.3. Show that the following modification of the Graph Removal Lemma is false. For every $c > 0$ and graph H on k vertices there exists $a > 0$ such that every n-vertex graph G contains at least an^k induced copies of H or there exists $F \subseteq E(G)$ such that $|F| \leq cn^2$ and $G \setminus F$ has no induced copy of H.

Solution. As graph H take an independent set of size 2, while as graph G take the complete graph without one edge. □

Historically, a major motivation for proving the Triangle Removal Lemma was its connection with the following theorem.

Theorem 3.4 (Roth)**.** For every $\varepsilon > 0$ there exists n_0 such that for every $n > n_0$ and any subset $A \subseteq \{1, 2, \ldots, n\}$ of size $|A| \geq \varepsilon n$, there exists a 3-term arithmetic progression in A.

PROOF. For a fixed $\varepsilon>0$ and subset $A\subseteq\{1,2,\ldots,n\}$ of size $|A|=\varepsilon n$. We construct an auxiliary tripartite graph G on the vertex set $V=X\cup Y\cup Z$, where $X=\{1,2,\ldots,n\}$, $Y=\{1,2,\ldots,2n\}$, $Z=\{1,2,\ldots,3n\}$, by putting edge between $x\in X$ and $y\in Y$ if $y-x\in A$, between $y\in Y$ and $z\in Z$ if $z-y\in A$, and between $x\in X$ and $z\in Z$ if $(z-x)/2\in A$. Hence, $N=|V(G)|=6n$ and $|E(G)|=3\varepsilon n^2$ edges.

For any $x\in X$ and arbitrarily $a\in A$ the triple x, $y=x+a$, and $z=x+2a$ defines a triangle in G and all of them are pairwise edge-disjoint. Number of such triangles is at least $n|A|=\varepsilon n^2=\frac{\varepsilon}{36}N^2$. It follows that it is not possible to make G triangle-free by removing less than $\frac{\varepsilon}{36}N^2$ edges.

Because of that, the Triangle Removal Lemma (Theorem 3.2) for $c=\frac{\varepsilon}{40}$ implies that G has at least aN^3 triangles. Notice that any triangle in G is a 3-term arithmetic progression in A, however, it may be a trivial progression if $y=x+a$ and $z=x+2a$. Since the number of such triangles coming from trivial progressions is equal to $|X||A|=\varepsilon n^2$, there are at least $aN^3-\varepsilon n^2=216an^3-\varepsilon n^2$ other triangles. Therefore, for $n>n_0\geq\frac{\varepsilon}{216a}$), there exists a triangle corresponding to a non-trivial 3-term arithmetic progression. □

3.4. Let a, b and c be integers satisfying $a+b=c$. Prove that for every $\varepsilon>0$ there exists n_0 such that for every $n\geq n_0$ any subset of $\{1,2,\ldots,n\}$ with size at least εn contains numbers x, y and z such that $ax+by=cz$.

SOLUTION. We do analogously as in the proof of Theorem 3.4, but place edge xy if $cx-by\in A$, edge yz is $ay+cz\in A$ and xz if $ax+bz\in A$. Condition $a+b=c$ gives many trivial triangles. □

3.5. Prove that if the condition $a+b=c$ in the previous problem is not satisfied, then the statement fails.

SOLUTION. For $a+b>c$ take $\varepsilon=(a+b-c)/(a+b)$ and set $A=\{n-\varepsilon n+1,\ldots,n\}$. Then $ax+by>(a+b)(n-\varepsilon n)=cn\geq cz$. For $a+b<c$ take $\varepsilon=(c-a-b)/c$ and set $A=\{n-\varepsilon n+1,\ldots,n\}$. Then $cz>cn(1-\varepsilon)=(a+b)n\geq ax+by$. □

3.6. Prove that for every $\varepsilon>0$ there exists n_0 such that for every $n\geq n_0$ any subset of $\{1,2,\ldots,n\}$ with size εn contains numbers x, y, z and w such that $x+2y+3z=6w$.

SOLUTION. As in the proof of Theorem 3.4, but in 4-partite graph with all edges ac, bd, and ab if $a-b\in A$, bc if $(b-c)/2\in A$, cd if $(c-d)/3\in A$ and ad if $(a-d)/6\in A$. □

To present the next application of the Szemerédi Regularity Lemma we need one more definition. For any graph R and an integer s let $R(s)$ be a *blow-up* of R with s vertices in each blob, i.e., a graph obtained from R by replacing every vertex by a group of s independent vertices and replacing every edge by a complete bipartite graph $K_{s,s}$ between the corresponding groups.

The crucial application of Szemerédi Regularity Lemma is basically saying that whenever we can find in $R(s)$ some subgraph H of a bounded maximum degree, then we can find it also in every big enough G with reduced graph R.

THEOREM 3.5 (Embedding Lemma)**.** For any $d\in(0,1]$ and $\Delta\geq 1$, there exists $\varepsilon_0>0$ such that the following holds for any $\varepsilon\leq\varepsilon_0$. Let H be a graph with $\Delta(H)\leq\Delta$, $s\in\mathbb{N}$ and $R=R(\varepsilon,d)$ be the reduced graph of some graph G with parts of size at least $2s/d^{\Delta}$. Then if H is a subgraph of $R(s)$, then H is also a subgraph of G.

Let us recall that the Turán number $\mathrm{ex}(n,F)$ is the biggest possible number of edges in graph on n vertices that do not contain graph F as a subgraph. Turán's theorem is saying that $\mathrm{ex}(n,K_r)=e(T_{n,r-1})$, where $T_{n,r-1}$ is the complete $(r-1)$-partite n-vertex graph with as equal as possible vertex parts. The Erdős-Stone theorem provides an asymptotic answer, showing that the Turán number $\mathrm{ex}(n,F)$ is controlled by the chromatic number $\chi(F)$:

$$\mathrm{ex}(n,F)=\left(1-\frac{1}{\chi(F)-1}\right)\binom{n}{2}+o(n^2).$$

The lower bound comes from considering graph $T_{n,\chi(F)-1}$. The upper bound is equivalent to showing that for every $\alpha>0$ and n sufficiently large, $\mathrm{ex}(n,F)\le\left(1-\frac{1}{\chi(F)-1}+\alpha\right)\binom{n}{2}$, which is implied by the following theorem.

Theorem 3.6 (Erdős-Stone, 1946)**.** For any $r,s\in\mathbb{N}$ and $\alpha>0$ there exists n_0 such that if G is a graph on $n\ge n_0$ vertices with at least $\left(1-\frac{1}{r-1}+\alpha\right)\binom{n}{2}$ edges, then G contains $K_r(s)$.

Proof. Apply Szemerédi Regularity Lemma in the degree form (Theorem 2.3) for $d=\alpha/3$, appropriately small ε and sufficiently large graph G. We obtain a graph $G''\subset G$ with at least $\left(1-\frac{1}{r-1}+\frac{\alpha}{3}\right)\binom{n}{2}$ edges. From Turán's theorem it contains K_r and since edges in G'' are only between ε-regular pairs, then also the reduced graph R contains K_r. Now, the Embedding Lemma (Theorem 3.5) implies that G contains $K_r(s)$. □

3.7. Find the extremal number (with error term $o(n^2)$) of cycle of any odd length, the Petersen graph, the icosahedron graph and the truncated icosahedron graph (soccer ball).

Solution. Erdős-Stone theorem implies that it is enough to find the chromatic number of the considered graphs, which is respectively 3, 3, 4 and 3. □

3.8. Let $\mathrm{ex}(n,\{F_1,F_2,\dots,F_t\})$ be the maximum number of edges in an n-vertex graph containing no copy of any graph F_i. Determine the asymptotic value (up to $o(n^2)$) for $\mathrm{ex}(n,\{F_1,F_2,\dots,F_t\})$.

Solution. Let F be the graph among $F_1,F_2,\dots,F_t$ with the smallest chromatic number. The complete multipartite graph on $\chi(F)-1$ parts does not contain any of the graphs $F_1,F_2,\dots,F_t$, while Erdős-Stone theorem implies that if we have asymptotically more edges then we will find a copy of F. □

Introduction to Algebraic Geometry

Aliaksandra Novik

1. Application

Example 1.1. Let us start with the following example:

$$C_n = \{(x,y) \in \mathbb{C}^2 : y^2 = (x-1)\dots(x-(2n-1))(x-2n)\} \subset \mathbb{C}^2$$

For this case is possible to write down all solutions, because the equation is seem to be easy solved for a variable y. We should just pick some x and after count a square from it. But let us look a bit closer, by Euler formula we can write down a complex non zero number as:

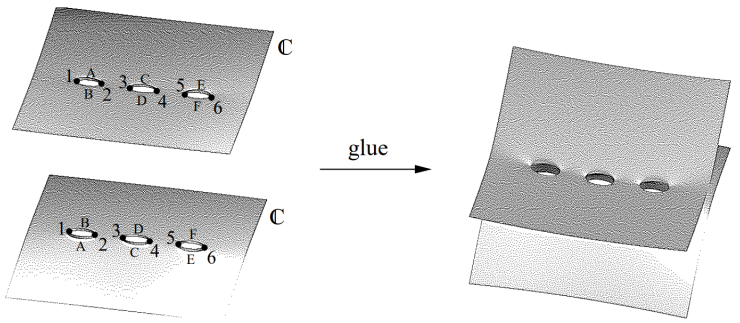
$$x = re^{i\phi} \text{ for } \phi \in [0, 2\pi] \text{ and fixed } r > 0,$$

and the square root of this number looks like:

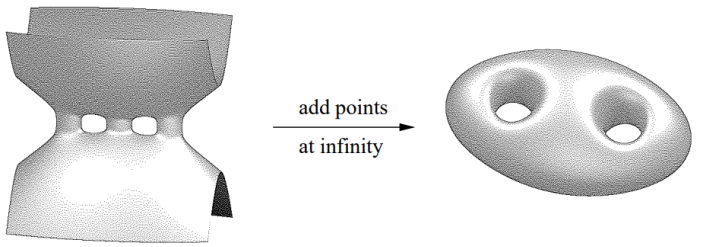
$$\sqrt{x} = \sqrt{r}e^{\frac{i\phi}{2}},$$

which gives us the opposite values when $\phi = 0$ and $\phi = 2\pi$. What does it mean? The two roots of a complex number get exchanged if you run around the origin once. In other words, if in C_n we run around one of the points $1, \dots, 2n$, we go from one copy of the plane to the other.

Now we want describe what it topologically means. Let us cut planes along the lines $[1,2], \dots, [2n-1, 2n]$, and to glue the two planes along these lines as in this picture (lines marked with the same letter are to be identified):



By adding a point ∞. If we do this here, we end up with a compact surface with $n-1$ handles:



Exercise 1.1. What will we get for this equation instead previous:

$$C'_n = \{(x,y) \in \mathbb{C}^2 : y^2 = (x-1)\dots(x-(2n-1))\} \subset \mathbb{C}^2$$

Another application of Algebraic Geometry can be shown by simple version of Bezout's Theorem:

Theorem 1.2. Suppose that X and Y are two plane curves defined over a field $\mathbb{K}$ that do not have a common component. Then the total number of intersection points of X and Y, counted with their multiplicities, is less or equal to the product of the degrees of X and Y.

Or Cayley–Bacharach theorem:

Theorem 1.3. Assume that two cubics X and Y in the projective plane meet in nine (different) points, as they do in general over an algebraically closed field. Then every cubic that passes through any eight of the points also passes through the ninth point.

2. Algebraic staff

Definition 2.1. Recall that a **ring** is a set R with operations $+$ and $\cdot$ on it satisfying the following conditions:

1. R is an abelian group under addition.
2. Multiplication is associative and has multiplicative identity 1, s. t. for every element a holds $a \cdot 1 = 1 \cdot a = a$.
3. Multiplication is distributive with respect to addition, meaning that: $(a+b)\cdot c = a\cdot c + b\cdot c$ and $a\cdot(b+c) = a\cdot b + a\cdot c$.

Definition 2.2. Recall that a **field** is a set $\mathbb{K}$ with operations $+$ and $\cdot$ on it and two elements 0 and 1 called zero and one respectively, such that:

1. $(\mathbb{K}, +, \cdot)$ is a commutative ring.
2. Zero and one are different elements.
3. Multiplicative is inverse, so for every element a there exist elements a^{-1} s. t. $a \cdot a^{-1} = 1$.

Definition 2.3. An **algebraically closed field** is a field in which every non-constatnt polynomial has a root in this field.

Definition 2.4. An **ideal** $(I, +)$ of a ring $(R, +, \cdot)$ is a subgroup of $(R, +)$, such that:

$$\text{for every } r \in R \text{ and } x \in I : rx \text{ and } xr \in I.$$

More precisely will be to say that this is a two-sided ideal, but in this notes the word "two-sided" will be skipped.

Example 2.5. In the ring of integer numbers $\mathbb{Z}$ a set of all even numbers is an ideal in it. Or we can look at another example, we a bit more interested in, in the ring of all polynomial functions $\mathbb{K}[x_1, x_2, \dots, x_n]$ a set of all polynomials for which free coefficient is equal to zero is also an ideal.

Definition 2.6. An ideal I in commutative ring R is called **prime** if I is not a whole ring R and if it is satysfies next condition:

$$\text{if } ab \in I \text{ then } a \in I \text{ or } b \in I.$$

Example 2.7. In the ring $\mathbb{Z}$ a subset of numbers divided by prime number p is a prime ideal.

Exercise 2.1. Show that the ideal (y^2-x^3-x-1) is prime in the ring $\mathbb{C}[x,y]$, where given ideal is of the form:

$$(y^2-x^3-x-1) = \{f(x,y)(y^2-x^3-x-1) : f(x,y) \in \mathbb{C}[x,y]\}.$$

Definition 2.8. For given ring R and the ideal I let us define a **quotient ring**, determined as R/I using relation $\sim$, s. t.:

$$a \sim b \iff a-b \in I.$$

In a case $a \sim b$, we say that a and b are **congruent modulo** I. And for any element a in the ring R we define the **equivalence class** as:

$$[a] := a+I = \{a+r : r \in I\}.$$

The set of all equivalence classes is exactly a quotient ring R/I.

Example 2.9. Consider the ring of integers $\mathbb{Z}$ and the ideal of even numbers $2\mathbb{Z}$, then quotient ring $\mathbb{Z}/2\mathbb{Z}$ consists from two elements zero and one.

Exercise 2.2. Suppose that $\mathbb{Z}_3$ is a ring consisting of 3 elements, how many elements has a quotient ring

$$\mathbb{Z}_3[x]/(2x^2+x+2),$$

where given ideal is of the form:

$$(2x^2+x+2) = \{f(x)\cdot(2x^2+x+2) : f(x) \in \mathbb{Z}_3[x]\}.$$

3. Algebraic sets and Zariski topology

Definition 3.1. Let $\mathbb{K}$ is an arbitrary field (you may always think that it is just the complex numbers). We define **affine n-space** over $\mathbb{K}$, denoted by $\mathbb{A}^n_{\mathbb{K}}$, to be a set of f all n-tuples of elements of $\mathbb{K}$, so it is just $\mathbb{K}^n$. For a given set $S \subset \mathbb{K}[x_1,...,x_n]$ of polynomials, we call

$$Z(S) := \{P \in \mathbb{A}^n_{\mathbb{K}} : f(P) = 0 \text{ for all } f \in S\} \subset \mathbb{A}^n_{\mathbb{K}}$$

the **zero locus** (or **zero set**) of the set S. A subset $X \subset \mathbb{A}^n_{\mathbb{K}}$ is called **algebraic set** if $X = Z(S)$ for some set $S \subset \mathbb{K}[x_1,...,x_n]$.

Example 3.2. Here are some basic and simple examples of algebraic sets:

1. Affine n-space itself is an algebraic set: $\mathbb{A}^n_{\mathbb{K}} = Z(0)$.
2. The empty set is an algebraic set: $\varnothing = Z(1)$.
3. Any single point in $\mathbb{A}^n_{\mathbb{K}}$ is an algebraic set: $P = (a_1,...,a_n) = Z(x_1-a_1,...,x_n-a_n)$.

4. Linear subspaces of $\mathbb{A}^n_{\mathbb{K}}$ are algebraic sets.

Exercise 3.1. By **(S)** we define an **ideal generated by** S as:

$$(S) = \{f_1 g_1 + \cdots + f_k g_k : f_i \in S, g_i \in \mathbb{K}[x_1, ..., x_n]\}.$$

Then one can proof that:

$$Z(S) = Z((S)).$$

Definition 3.3. Recall that a **topology** on any set X can be defined by its closed sets. So for family specifying which subsets of X are to be considered closed sets, provided that the following conditions hold:

1. The empty set $\varnothing$ and the whole space X are closed.
2. Arbitrary intersections (non necessary finite) of closed sets are closed.
3. Finite unions of closed sets are closed.

Example 3.4. For standard definition of the topology on $\mathbb{R}$ generated by the open intervals we can similarly define it using all closed intervals, putting that they generate a family of all closed subsets in the topology on $\mathbb{R}$.

Definition 3.5. We define the **Zariski topology** on $\mathbb{A}^n_{\mathbb{K}}$ to be the topology whose closed sets are the algebraic sets. This topology is quite different from the usual ones and sometimes is very weak.

Example 3.6. A Zariski closed subset of $\mathbb{A}^1_{\mathbb{K}}$ is either the whole space $\mathbb{A}^1_{\mathbb{K}}$ or is a finite set.

Exercise 3.2. Prove that any algebraic set $V \subset \mathbb{A}^2_{\mathbb{K}}$ is a finite union of points and curves.

4. Hilbert's Nullstellensatz

Now we want to establish the precise connection between algebraic sets in $\mathbb{A}^n_{\mathbb{K}}$ and ideals in $\mathbb{K}[x_1, ..., x_n]$, hence between geometry and algebra.

Definition 4.1. For arbitrary subset $X \subset \mathbb{A}^n_{\mathbb{K}}$, we define:

$$I(X) := \{f \in \mathbb{K}[x_1, \ldots, x_n] : f(P) = 0 \text{ for all } P \in X\}$$

to be an **ideal** of X. Actually this operator is a kind of an inverse operator for $Z(\cdot)$.

Exercise 4.1. Let $X \subset \mathbb{A}^3$ be the union of the three coordinate axes. Determine generators for the ideal $I(X)$. Show that $I(X)$ cannot be generated by fewer than 3 elements.

Theorem 4.2. Hilbert's Nullstellensatz ("theorem of the zeros") Assume that the field $\mathbb{K}$ is algebraically closed (e. g. $\mathbb{K} = \mathbb{C}$). Then the maximal ideals of $\mathbb{K}[x_1, ..., x_n]$ are exactly the ideals of the form $(x_1 - a_1, \ldots, x_n - a_n)$ some point $(a_1, \ldots, a_n) \in \mathbb{A}^n_{\mathbb{K}}$.

Lemma 4.3. An ideal I of a ring R is maximal if and only if R/I is a field.

Remark 4.4. Without assuming that $\mathbb{K}$ is algebraically closed, this theorem doesn't work. Let us look at the non algebraically closed field $\mathbb{R}$ and the ideal (x^2+1). Then one can show that:

$$\mathbb{R}[x]/(x^2+1) \cong \mathbb{C}.$$

Then using the fact that $\mathbb{C}$ is a field we obtain that (x^2+1) is a maximal ideal by Lemma 4.3 what obviously isn't true.

Definition 4.5. For any ideal $I \subset \mathbb{K}[x_1,\ldots,x_n]$, we define a **radical** of I to be:

$$\sqrt{I} := \{f \in \mathbb{K}[x_1,\ldots,x_n] : f^k \in I \text{ for some } k>0\}.$$

Example 4.6. The radical of the ideal $4\mathbb{Z}$ (set of numbers divisible by four) is $2\mathbb{Z}$. Or if we consider that $I=(y^3)$, then $\sqrt{I}=(y)$.

Exercise 4.2. Let X and Y are algebraic sets in $\mathbb{A}^n_{\mathbb{K}}$, show that:

1. $I(X \cup Y) = I(X) \cap I(Y)$.
2. $I(X \cap Y) = \sqrt{I(X)+I(Y)}$.

Exercise 4.3. Prove that:

1. If $X \subset Y$ then $I(Y) \subset I(X)$.
2. For any algebraic set $X \subset \mathbb{A}^n_{\mathbb{K}}$ then we have $Z(I(X)) = X$.

Theorem 4.7. Also Hilbert's Nullstellensatz If $\mathbb{K}$ is algebraically closed, then for any ideal $J \subset \mathbb{K}[x_1,...,x_n]$ we have $I(Z(J)) = \sqrt{J}$.

5. Affine varieties

Definition 5.1. A set X is said to be **irreducible** if it can not be written as a union $X = X_1 \cup X_2$, where X_1 and X_2 are (non-empty) closed subsets of X not equal to X. An irreducible algebraic set in $\mathbb{A}^n_{\mathbb{K}}$ with Zariski topology is called an **affine variety**.

Remark 5.2. Also this definition preserves for any topological space, but in this case it is important to use Zariski topology. As an example one can show that $\mathbb{A}^1_{\mathbb{C}}$ is an affine variety, but in a standard topology on $\mathbb{C}$ this set isn't irreducible.

Proposition 5.3. An algebraic set $X \subset \mathbb{A}^n_{\mathbb{K}}$ is an affine variety if and only if its ideal $I(X) \subset \mathbb{K}[x_1,\ldots,x_n]$ is a prime ideal.

Example 5.4.

1. $\mathbb{A}^n_{\mathbb{K}}$ is affine variety, because $\mathbb{A}^n_{\mathbb{K}} = (0)$.
2. If $f \in \mathbb{K}[x_1,\ldots,x_n]$ is irreducible then $Z(f)$ is affine variety.
3. The collection of m points in $\mathbb{A}^n_{\mathbb{K}}$ is affine variety is and only if $m=1$.

Exercise 5.1. Let the set $X \subset \mathbb{A}^3$ is given by $x^2 - yz = xz - x = 0$. Compute its irreducible components and their ideals.

Exercise 5.2. Let $X = \{(t, t^3, t^5) : t \in \mathbb{K}\} \subset \mathbb{A}^3_{\mathbb{K}}$. Show that X is an affine variety and compute $I(X)$.

Definition 5.5. For algebraic set $X \subset \mathbb{A}^n_{\mathbb{K}}$ let us define the coordinate ring $\mathbb{K}[X]$ by:

$$\mathbb{K}[X] := \{f : X \to \mathbb{K} | f \text{ is a polynomial function}\} \cong \mathbb{K}[x_1, \ldots x_n]/I(X).$$

Exercise 5.3. Compute the coordinate rings of $y = x^2$ and $xy = 1$ in $\mathbb{A}^2_{\mathbb{K}}$ and show they are non-isomorphic.

Exercise 5.4. (twisted cubic). Let $C = \{(t, t^2, t^3), t \in \mathbb{K}\}$. Show that C is an affine variety and find generators of the ideal $I(C)$. Show that its coordinate ring is isomorphic to $\mathbb{K}[t]$.

Team Problem Solving

Chill Division — Problems

1. Does there exist a subset A of positive integers such that any infinite arithmetic sequence has at least one term in A and at least term outside of A?

2. Let p be a prime number. A set of $p+2$ positive integers, not necessarily distinct, is called *sacrilegious* if the sum of any p of them is divisible by each of the other two. Find all sacrilegious sets.

3. Let P be a point inside a triangle ABC. Let A', B', C' be such points that

$$\angle A'CP = \angle A'BP = \angle B'AP = \angle B'CP = \angle C'AP = \angle C'BP = 90^\circ .$$

Let R, S, T be the orthocenters of triangles $A'BC$, $B'CA$ and $C'AB$ respectively. Show that areas of triangles RST and ABC are equal.

4. In some country there are n cities, some of which are connected by two-way roads. It is known there is no $k \geq 3$ and pairwise distinct cities A_1, A_2, …, A_k such that there is a road between A_i and A_{i+1} for every $i \in 1, 2, \ldots, n$ (we define $A_{k+1} = A_1$). Call this property $(*)$. Moreover, there is no city with exactly two roads leaving it. City is called *terminal* if there is at most one road leaving it. Show that there are at least $\frac{n}{2}$ terminal cities.

5. Find all pairs of real numbers (x, y) satisfying the following equations

$$x^2 + 2 = x + y = y^2 .$$

Medium Division — Problems

1. Polynomial $x^2+13x+5$ is written on a blackboard. Every second Radek changes one of the coefficients of this polynomial by ± 1, such that after some number of seconds polynomial $x^2+5x+13$ remains. Is it possible that the polynomial on the blackboard could never split? We say that the polynomial $P(x)$ splits if it can be expressed as a product of degree 1 polynomials with integer coefficients.

2. Let D be the midpoint of side AB in triangle ABC. Let E be such point on circumcircle of BCD that line DE is tangent to circumcircle of ACD. Let F be a point on the line BC such that $CF=\frac{1}{2}BC$ and $BF=\frac{3}{2}BC$. Show that $\angle CAF=\angle BAE$.

3. Let $A=\{a+b\sqrt{2}|a,b\in\mathbb{Q}\}$. Find all functions $f:A\to A$ which satisfy

$$f(x+f(y))=f(x)+y$$

for any $x,y\in A$ and that $f(\mathbb{Q})\subset\mathbb{Q}$.

4. Determine whether there exists an infinite set A of integers, such that for any finite subset $B\subset A$, the sum of elements of B can't be expressed as a proper power of an integer (with an integer exponent greater than 1).

5. Tomek has drawn on the whiteboard all planar graphs with 2020 vertices. Radek assigns to every vertex of every graph a *label* – sequence of 70 numbers, each of which is equal to 0 or 1. Tomek now secretly chooses one of the graphs G on a whiteboard and two distinct vertices A and B of this graph and tells Radek the labels assigned to these vertices. Is there a strategy for Radek which will allow him to determine whether A and B are adjacent in G, no matter which graph G and vertices A, B Tomek picks?

Hard Division — Problems

1. Let $a,b,c \in [-1,1]$ be such that $1+2abc \geq a^2+b^2+c^2$ and let n be a positive integer. Show that $1+2(abc)^n \geq a^{2n}+b^{2n}+c^{2n}$.

2. Two circles ω_1 and ω_2 intersect in points A, B. Their common external tangent touches ω_1 in X and ω_2 in Y. On line XY point Z was chosen. Circle Ω, passing through A, B and Z, intersects line XY in point $W \neq Z$. Let M be the midpoint of segment ZW. Line MB intersects ω_1, ω_2 and Ω in P, Q and R respectively. Point D on line XY satisfies $|MR| = |MD|$. Prove that circle passing through P, Q and D is tangent to line XY.

3. Let G be a graph with vertices $v_1, v_2, \ldots, v_n$ and let E be set of pairs (i,j) such that $i<j$ and v_i and v_j are neighbours. Let $P_G(x_1,x_2,\ldots,x_n)$ be a polynomial defined as following:

$$P_G(x_1,x_2,\ldots,x_n) = x_1^2+x_2^2+\cdots+x_n^2 - \sum_{(i,j)\in E} x_i x_j\,.$$

We say that G is *happy* if for any real $x_1,x_2,\ldots,x_n$ such that $x_1^2+x_2^2+\cdots+x_n^2 \neq 0$ the value $P_G(x_1,x_2,\ldots,x_n)$ is positive. Find all happy graphs.

4. Solve equation

$$(3-\sqrt{2})^k + (4+\sqrt{2})^l = (5-\sqrt{2})^m$$

in positive integers k, l, m.

5. Consider the following game: Alice and Bob alternately write an integer greater than 1 on a table, and this integer can't be a sum of numbers which are already on the table (we can take each number to the sum as many time as we want – e.g. after 5 and 11 are written, then 10 and $38 = 3\cdot 11+5$ are among forbidden numbers). The person who can't make a move, loses.

In the first move, Alice wrote 2021 on the table. Who has a winning strategy in this moment of the game?

Chill Division — Solutions

1. Let A be the set of positive integers with odd number of digits. Take any arithmetic sequence $a_n = a + nd \in \mathbb{N}$. Then for any k such that $10^k > a, d$ we know that there is at least one term of our sequence a_n in the set $10^k, 10^k + 1, \ldots 10^k + d - 1$. All of these numbers have exactly $k+1$ digits. Since we can choose k to have any parity we want, we are able to find a term of our sequence with odd number of digits (in A), as well as one with even number of digits (not in A).

2. Let T be a sacrilegious set, and s be the sum of its elements. Then we know that for any $a, b \in T$ we have $s - a - b$ divisible by both a and b; so $s - a$ is divisible by b. For any $a, b, c \in T$ we have that $s - b$ and $s - c$ are divisible by a, so $b - c$ is also divisible by a. As this holds for any permutation of (a, b, c), we may suppose that $a \geqslant b, c$, but since all these numbers are positive, we have $a > |b - c|$ so $b = c$. This way we can see that T consists of some maximal number m, and $p+1$ other numbers, all equal to some n. Now taking subset consisting of p numbers n, we see that $m \mid np$, and taking subset of m and $p-1$ numbers n, we have $n \mid m$. Therefore either $m = n$ or $m = np$.

Thus any sacrilegious set has form $(n, n, \ldots, n, n)$ or $(n, n, \ldots, n, np)$ for some n (we checked already that these sets are indeed sacrilegious.

3. Observe that $BR \perp A'C \perp CP$ and $CR \perp A'B \perp BP$, so $BRCP$ is a parallelogram. Similarly, $CSAP$ and $ATBP$ are parallelograms. Thus segments BR, CP and AS are parallel and equal, hence $BRSA$ is also a parallelogram, with $AB = RS$. Analogously $BC = ST$ and $CA = TR$, so triangles ABC and RST are congruent, thus have the same area.

4. Firstly we claim that country satisfying property $(*)$ has less than n roads. We prove it by induction on the number of cities. Base case of country with one city is obviously true. If there exists a city with at most one road leaving it, we may erase it and the resulting country still satisfies property $(*)$. By induction assumption the rest of the cities have less than $n-1$ roads, hence adding our city back we have less than n roads. If there is no such city, then each of them has at least two roads leaving it. Choose any A_1, any A_2 connected to A_1, and keep picking inductively A_{i+1} - city connected to A_i other than A_{i-1}. Clearly we need to have $A_i = A_j$ for some $i < j$, and then $A_i, A_{i+1}, A_{i+2}, \ldots, A_{j-1}$ forms a cycle, which gives a contradiction.
So country satisfying $(*)$ has less than n roads.

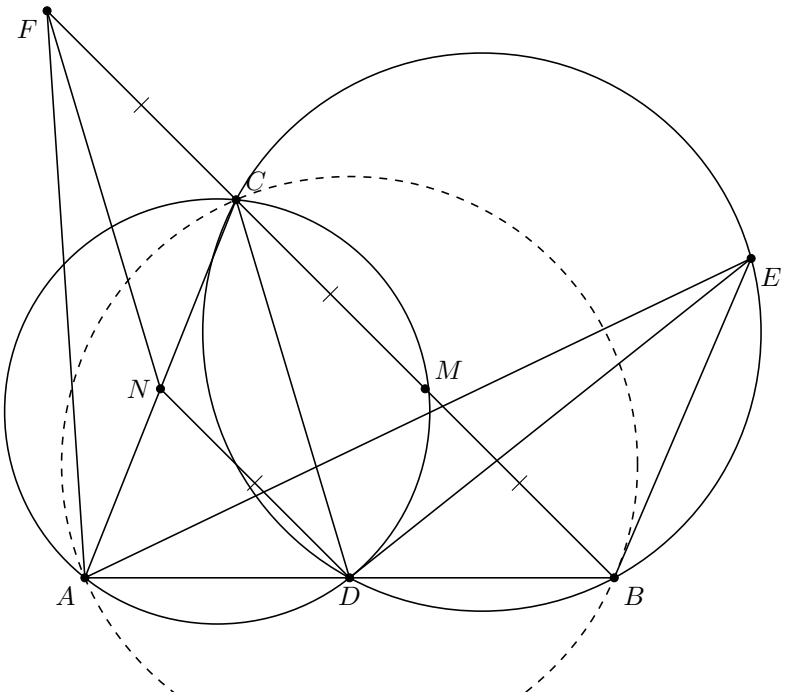
Now let t be the number of terminal cities. Let us calculate the sum of numbers of roads leaving all the cities. On one hand, it is at least $t + 3(n - t)$, as there is no city with two roads leaving from it. On the other hand, as each road leaves exactly from 2 cities, by above result we get something less than $2n$. Therefore $t + 3(n - t) \leqslant 2n$, so $\frac{n}{2} \leqslant t$, which ends the proof.

5. Summing equalities $x^2 + 2 = x + y$ and $y^2 = x + y$ we get $x^2 + y^2 + 2 = 2x + 2y$, so $(x-1)^2 + (y-1)^2 = 0$. This implies that if a solution exists, it must be equal $(1, 1)$; but this is not a solution, hence there are none.

Medium Division — Solutions

1. Observe how $P(-1)$ changes over time. It starts at value -7, we want it to end at 9, and we see that after each second its value changes by ± 1. Therefore at some second we will get polynomial $Q(x)$, such that $Q(-1)=0$. But this means that Q is divisible by $x+1$, so it is reducible.

2. *Solution 1.* Let N be the center of segment AC. Then $FC=ND=\frac{1}{2}BC$ and $ND||BC$, so $NDCF$ is a parallelogram, in particular $FN||CD$. We have $\angle CAB=\angle CDE=\angle CBE$, so line BE is tangent to the circumcircle of ABC.



Observe that

$$\angle DEB=\angle DCB=\angle NFB=\angle NFC$$

and

$$\angle ABE=180^\circ-\angle ACB=\angle FCN,$$

so triangles ΔFCN and ΔEBD are similar. This implies that $\frac{FC}{CN}=\frac{EB}{BD}$, so also $\frac{FC}{CA}=\frac{EB}{BA}$. Hence we get that triangles ΔFCA, ΔEBA are similar, which gives $\angle CAF=\angle BAE$, as desired.

Solution 2. Let M be the midpoint of BC. Denote by $T^X_{\lambda,\alpha}$ spiral similarity with center X, scale λ and rotation by α (counterclockwise). Consider transformation

$$f(X)=T^A_{\frac{CA}{AB},\angle BAC}\circ T^C_{\frac{BC}{CA},\angle ACB}\circ T^B_{\frac{AB}{BC},\angle CBA}(X)$$

Since $\frac{AB}{BC}\cdot\frac{BC}{CA}\cdot\frac{CA}{AB}=1$, f is an isometry. As $f(C)=C$, and f has total rotation by 180°, the only possibility is that f is a reflection in C. Thus $f(M)=F$. But $T^B_{\frac{AB}{BC},\angle CBA}(M)=D$ and $T^C_{\frac{BC}{CA},\angle ACB}(D)=E$ (the first one is obvious, the second one follows from $\angle BAC=\angle EDC$ and $\angle CBA=\angle CED$). Hence $T^A_{\frac{CA}{AB},\angle BAC}(E)=F$. This is exactly what we need hence finishes the proof.

3. Substituting $x=y=0$ gives $f(f(0))=f(0)$. Now $x=0$, $y=f(0)$ yields $f(0)=2f(0)$, so $f(0)=0$. With $x=0$ we get $f(f(y))=y$. This means that f is a bijection. By substituting $f(y)$ for y, we get $f(x+y)=f(x)+f(y)$. It is well-known that any such function on $\mathbb{Q}$ has form $f(x)=cx$, for some $c\in\mathbb{Q}$. Since we know that $f(\mathbb{Q})\subset\mathbb{Q}$, we can indeed say that $f(x)=cx$ for all rational x. Substituting this into original equation with x, y rational, we get

$$cx+c^2y=cx+y,$$

so $c=\pm1$. Observe that f satisfies the original equation if and only if $f(f(y))=y$ and $f(x+y)=f(x)+f(y)$. So if f is a valid solution then so is $-f$. So suppose for the rest of the proof that $c=1$.

From $f(x+y)=f(x)+f(y)$, we note that for any rational λ, $f(\lambda x)=\lambda f(x)$. Suppose now $f(\sqrt{2})=a+b\sqrt{2}$ for $a,b\in\mathbb{Q}$, then

$$\sqrt{2}=f(f(\sqrt{2}))=f(a+b\sqrt{2})=f(a)+f(b\sqrt{2})=a+bf(\sqrt{2})=a+b(a+b\sqrt{2}),$$

which yields $b^2=1$ and $a+ab=0$. So if $b=1$ then $a=0$, and we get that $f(r+s\sqrt{2})=r+sf(\sqrt{2})=r+s\sqrt{2}$, so the function is $f(x)=x$. If $b=-1$, we work out that any $a\in\mathbb{Q}$ works, which similarly as above gives us $f(r+s\sqrt{2})=r+as-s\sqrt{2}$. Clearly both of the above functions satisfy $f(x+y)=f(x)+f(y)$, and one checks that:

$$f(f(r+s\sqrt{2}))=f(r+as-s\sqrt{2})=r+as+a\cdot(-s)+s\sqrt{2}=r+\sqrt{2},$$

so such functions also satisfy the problem statement. If we also include solutions with $f(1)=c=-1$, we get four classes of solutions: $f(x)=x$, $f(x)=-x$, $f(r+s\sqrt{2})=r+as-s\sqrt{2}$ and $f(r+s\sqrt{2})=-r-as+s\sqrt{2}$ with some $a\in\mathbb{Q}$.

4. We will show that such set exists, in fact, we can take

$$A=\{2^n3^{n+1}\ :\ n\in\mathbb{Z}_+\}.$$

Let $v_p(n)$ for prime p and nonzero integer n denote the p-adic exponent of n, i.e. $v_p(n)$ is an integer such that $p^{v_p(n)}\mid n$ but $p^{v_p(n)+1}\nmid n$. Note that if n is a k-th power, we have $k\mid v_p(n)$ for any prime p.

Let $B\subset A$ be an arbitrary finite subset of A, that is

$$B=\{2^{n_1}3^{n_1+1},\ 2^{n_2}3^{n_2+1},\ \ldots,\ 2^{n_m}3^{n_m+1}\},$$

and assume without loss of generality that $n_1<n_2<\ldots<n_m$. Sum of elements in B is:

$$\begin{aligned}S&=2^{n_1}3^{n_1+1}+2^{n_2}3^{n_2+1}+\cdots+2^{n_m}3^{n_m+1}\\&=2^{n_1}3^{n_1+1}\left(1+2^{n_2-n_1}3^{n_2-n_1}+2^{n_3-n_1}3^{n_3-n_1}+\cdots+2^{n_m-n_1}3^{n_m-n_1}\right).\end{aligned}$$

Note that for any m the sum

$$1+2^{n_2-n_1}3^{n_2-n_1}+2^{n_3-n_1}3^{n_3-n_1}+\cdots+2^{n_m-n_1}3^{n_m-n_1}$$

is not divisible by 6 as 1 is not divisible by 6 while all other summands are. Therefore,

$$v_2(S)=v_2(2^{n_1}3^{n_1+1})=n_1$$
$$v_3(S)=v_3(2^{n_1}3^{n_1+1})=n_1+1.$$

Assume that S is some k-th power. Then $k\,|\,v_2(S)=n_1$ and $k\,|\,v_2(S)=n_1+1$ which implies $k=1$. Therefore S is not a proper power which completes the solution.

5. We will prove that it is possible even with labels of length 66. Since $2020<2^{11}$, Radek can start with assigning an 11-digit long tags to each vertex of each graph, that will be unique among tags of vertices in the same graph. He can do it in such a way that a tag consisting of eleven zeros will be unused. Now, for each vertex v he can choose a set $S(v)$ of at most five vertices, and say that a label of v starts with the tag of v, and then tags of elements of $S(v)$ follow (in any order; if $S(v)$ has less than five elements, let's add zeros at the end).

This way, given labels of vertices v and w, we can easily determine if w is in $S(v)$ (the assumption about the zero tag allows us to avoid some tag-label collisions). We will prove that we can choose sets $S(v)$ in such a way that v and w are adjacent if and only if $v\in S(w)$ or $w\in S(v)$.

We will proceed by induction on the number of vertices of our graph. If we have at most two vertices, it is easy. Suppose there are more than two vertices. We claim that there is a vertex with degree at most five. If not, all degrees are equal to at least six. This remains true if we added some edges so that each edge would belong to two faces. Let V,E,F be the numbers of vertices, edges and faces in our graph, respectively. By hand-shaking lemma, $V\leqslant\frac{E}{3}$. Each face has at least three edges, and each edge is in two faces, so by summing edges of all the faces we get $2E$, but, by the above inequality, this number is also greater or equal to $3F$. So $F\leqslant\frac{E}{3}$, and by Euler's formula $2=V-E+F\leqslant\frac{E}{3}-E+\frac{2E}{3}=0$. We get a contradiction.

Thus, we have some vertex v of degree at most 5. Let us put all its neighbours in $S(v)$. Now, we don't need to worry about v, so we can erase it and use the induction hypothesis to the remaining graph, finishing the proof.

Remark 5.6. This problem was motivated by recent discoveries in graph theory, including research of one of our past tutors. In the language of research maths, what the problem asks for is a planar graph labelling scheme. What we show here is in fact that we can use labels of length $6\log_2 n$ for a given planar graph on n vertices – we first give each vertex a different, arbitrary prelabel of length $\lceil\log_2 n\rceil$. Then we combine the prelabel of each vertex with prelabels of at most 5 of its neighbors, so that for every pair of neighbors (u,v) prelabel of u is in label of v or vice versa. Thus we use at most $\sim 6\log_2 n$ digits. This is, however, not the best we can asymptotically achieve. The paper of `Kannan, Naor and Rudich (1988)` was probably the first in the area and showed a $\lceil 4\log_2\rceil$ bound for the length of label. It can be relatively quickly improved by noting that planar graphs have `arboricity` at most 3 (which is a well-known theorem in combinatorics) and trees can be labeled with $\log_2 n+o(\log_2 n)$, which gives a total label length of $3\log n+o(\log n)$. This is still not the last word: a paper from last year `Bonamy, Gavoille, Pilipczuk (2020)` (Michał Pilipczuk who co-authored this paper tutored a number of combinatorics classes during past MBLs) showed the bound of $4/3\log_2 n+o(\log_2 n)$, while this year (!) it was finally shown that $\log_2 n+o(\log_2 n)$ is achievable: `Dujmović, Esperet, Gavoille, Joret, Micek, Morin (2021)`. Note that length of label cannot be smaller than $\log n$ as we need to

have different labels for different vertices. Thus, this result essentially completes the problem, although one may wonder what is the precise size of $o(\log_2 n)$ here.

Note that the labelling scheme using labels of length $c \log_2 n$ can be restated in the following way: for any n there exists a graph $\mathcal{G}$ on $n^{c+o(1)}$ vertices such that every planar graph on n vertices is its induced subgraph. It looks even more shocking when applied for the $\log_2 n$ result: for any ε there is C such that for any n there exists a graph $\mathcal{G}$ on $Cn^{1+\varepsilon}$ vertices such that every planar graph on n vertices is its induced subgraph! Note that the number of planar graphs is at least exponential in n while $\mathcal{G}$ has nearly linear number of vertices.

Hard Division — Solutions

1. Note that exchanging signs of any two variables among (a,b,c) preserve both the assumptions and the hypothesis. Therefore, we may assume without loss of generality that $b,c\geq 0$.

Consider inequality

$$1+2xyz\geq x^2+y^2+z^2 \tag{5.1}$$

for $x,y,z\in[-1,1]$. We can treat x as a variable and y, z as parameters and use quadratic formula to show that 5.1 is equivalent to

$$x\in\left[yz-\sqrt{(1-y^2)(1-z^2)},\ yz+\sqrt{(1-y^2)(1-z^2)}\right]\cap[-1,1]\,.$$

Note that $\sqrt{(1-y^2)(1-z^2)}\geq 0$, so $yz-\sqrt{(1-y^2)(1-z^2)}\leq 1$ and $yz+\sqrt{(1-y^2)(1-z^2)}\geq -1$. Moreover if we had $yz-\sqrt{(1-y^2)(1-z^2)}<-1$, then

$$yz+1<\sqrt{(1-y^2)(1-z^2)}$$

and, since $1+yz\geq 0$, it would imply

$$(1+yz)^2<(1-y^2)(1-z^2)\,,$$

$$2yz<-y^2-z^2\,,$$

$$(y+z)^2<0$$

which is not possible. Similarly, if $yz+\sqrt{(1-y^2)(1-z^2)}>1$ then, since $1-yz\geq 0$, we would have

$$(1-y^2)(1-z^2)>(1-yz)^2\,,$$

$$-y^2-z^2>-2yz\,,$$

$$(y-z)^2<0,$$

which, again, is not possible. Therefore,

$$\begin{cases}-1 & \leq yz-\sqrt{(1-y^2)(1-z)^2}\leq 1\\ -1 & \leq yz+\sqrt{(1-y^2)(1-z)^2}\leq 1\end{cases} \tag{5.2}$$

so in particular 5.1 is equivalent to just

$$x\in\left[yz-\sqrt{(1-y^2)(1-z^2)},\ yz+\sqrt{(1-y^2)(1-z^2)}\right]$$

as this interval is contained in $[-1,1]$. Using this knowledge, we can restate the problem as follows: let $a,b,c\in[-1,1]$ and assume

$$a\in\left[bc-\sqrt{(1-b^2)(1-c^2)},\ bc+\sqrt{(1-b^2)(1-c^2)}\right]\,;$$

prove that

$$a^n\in\left[b^nc^n-\sqrt{(1-b^{2n})(1-c^{2n})},\ b^nc^n+\sqrt{(1-b^{2n})(1-c^{2n})}\right]\,.$$

Note that our wlog assumption of $b,c\geq 0$ can still be made and so we will use it. We consider two separate cases.

Case I. n is odd.

Now function $f:[-1,1]\to\mathbb{R}$ defined as $f(x)=x^n$ is strictly increasing so if $a\in[X,Y]$ then $a^n\in[X^n,Y^n]$. Thus, it suffices to show that

$$\left[\left(bc-\sqrt{(1-b^2)(1-c^2)}\right)^n,\ \left(bc+\sqrt{(1-b^2)(1-c^2)}\right)^n\right]\subseteq$$
$$\subseteq\left[b^nc^n-\sqrt{(1-b^{2n})(1-c^{2n})},\ b^nc^n+\sqrt{(1-b^{2n})(1-c^{2n})}\right].$$

Firstly, we will show that

$$\left(bc-\sqrt{(1-b^2)(1-c^2)}\right)^n\geq b^nc^n-\sqrt{(1-b^{2n})(1-c^{2n})}$$

for any positive integer n. We can make the following equivalent transformations:

$$\begin{aligned}\left(bc-\sqrt{(1-b^2)(1-c^2)}\right)^n&\geq b^nc^n-\sqrt{(1-b^{2n})(1-c^{2n})}\\ sqrt(1-b^{2n})(1-c^{2n})&\geq(bc)^n-\left(bc-\sqrt{(1-b^2)(1-c^2)}\right)^n\\ \sqrt{(1-b^{2n})(1-c^{2n})}&\geq\sqrt{(1-b^2)(1-c^2)}\left((bc)^{n-1}+(bc)^{n-2}X+\cdots+X^{n-1}\right),\end{aligned}\tag{5.3}$$

where $X=bc-\sqrt{(1-b^2)(1-c^2)}$. Recall that 5.2 gives $|X|\leq 1$. As $b,c\geq 0$, we have

$$(bc)^{n-1}+(bc)^{n-2}X+\cdots+X^{n-1}\leq 1+bc+\cdots+(bc)^{n-1}$$

and by Cauchy-Schwarz inequality

$$(bc)^{n-1}+(bc)^{n-2}X+\cdots+X^{n-1}\leq 1+bc+\cdots+(bc)^{n-1}\leq\sqrt{(1+b^2+\cdots+b^{2n-2})(1+c^2+\cdots+c^{2n-2})}.$$

Thus,

$$\begin{aligned}&\sqrt{(1-b^2)(1-c^2)}\left((bc)^{n-1}+(bc)^{n-2}X+\cdots+X^{n-1}\right)\\ &\leq\sqrt{(1-b^2)(1-c^2)}\sqrt{(1+b^2+\cdots+b^{2n-2})(1+c^2+\cdots+c^{2n-2})}\\ &=\sqrt{(1-b^2)(1+b^2+\cdots+b^{2n-2})(1-c^2)(1+c^2+\cdots+c^{2n-2})}\\ &=\sqrt{(1-b^{2n})(1-c^{2n})}.\end{aligned}$$

This proves 5.3 and concludes the proof that

$$\left(bc-\sqrt{(1-b^2)(1-c^2)}\right)^n\geq b^nc^n-\sqrt{(1-b^{2n})(1-c^{2n})}.\tag{5.4}$$

Note that the proof above works also for even n (we will use it in Case II).

To conclude Case I we also need to prove

$$\left(bc+\sqrt{(1-b^2)(1-c^2)}\right)^n\leq b^nc^n+\sqrt{(1-b^{2n})(1-c^{2n})}.\tag{5.5}$$

We will also prove this inequality for any positive integer n in a very similar way to 5.4. Define $Y = bc + \sqrt{(1-b^2)(1-c^2)}$ and recall that 5.2 shows that $|Y| \le 1$. Make the following transformations:

$$\begin{aligned}
\left(bc + \sqrt{(1-b^2)(1-c^2)}\right)^n &\le b^n c^n + \sqrt{(1-b^{2n})(1-c^{2n})} \\
\left(bc + \sqrt{(1-b^2)(1-c^2)}\right)^n - (bc)^n &\le \sqrt{(1-b^{2n})(1-c^{2n})} \\
\sqrt{(1-b^2)(1-c^2)}\left(Y^{n-1} + Y^{n-2}(bc) + \cdots + (bc)^{n-1}\right) &\le \sqrt{(1-b^{2n})(1-c^{2n})}
\end{aligned}$$

Now, it suffices to notice that $|Y| \le 1$ and we can conclude the proof by using the Cauchy-Schwarz inequality the same way as in the proof of 5.4.

Case II. n is even.

Assume first that

$$0 \in \left[bc - \sqrt{(1-b^2)(1-c^2)},\ bc + \sqrt{(1-b^2)(1-c^2)}\right],$$

that is $bc - \sqrt{(1-b^2)(1-c^2)} \le 0$. We will show that in this case also

$$0 \in \left[b^n c^n - \sqrt{(1-b^{2n})(1-c^{2n})},\ b^n c^n + \sqrt{(1-b^{2n})(1-c^{2n})}\right],$$

that is $b^n c^n - \sqrt{(1-b^{2n})(1-c^{2n})} \le 0$. As $b, c \ge 0$, we have

$$(bc)^n \le \left(\sqrt{(1-b^2)(1-c^2)}\right)^n$$

so it suffices to show that

$$\left(\sqrt{(1-b^2)(1-c^2)}\right)^n \le \sqrt{(1-b^{2n})(1-c^{2n})}.$$

This is, however, straightforward, as

$$(1-b^2)^n \le 1 - b^2 \le 1 - b^{2n}$$

because $|b| \le 1$.

Now, under the assumption of even n, $b, c \ge 0$ and

$$0, a \in \left[bc - \sqrt{(1-b^2)(1-c^2)},\ bc + \sqrt{(1-b^2)(1-c^2)}\right],$$

we observe that

$$\begin{aligned}
a^n &\in \left[0, \max\left(\left(bc - \sqrt{(1-b^2)(1-c^2)}\right)^n, \left(bc + \sqrt{(1-b^2)(1-c^2)}\right)^n\right)\right] \\
&= \left[0,\ \left(bc + \sqrt{(1-b^2)(1-c^2)}\right)^n, \right]
\end{aligned}$$

so it suffices to show that

$$\left[0,\ \left(bc + \sqrt{(1-b^2)(1-c^2)}\right)^n\right] \subseteq \left[b^n c^n - \sqrt{(1-b^{2n})(1-c^{2n})},\ b^n c^n + \sqrt{(1-b^{2n})(1-c^{2n})}\right].$$

We already know that $b^n c^n - \sqrt{(1-b^{2n})(1-c^{2n})} \le 0$ so it suffices to show that

$$\left(bc + \sqrt{(1-b^2)(1-c^2)}\right)^n \le b^n c^n + \sqrt{(1-b^{2n})(1-c^{2n})},$$

but this was already done in 5.5 in the previous case (recall that proof of this inequality was valid for any positive integer n).

Therefore we are done if $0 \in \left[bc-\sqrt{(1-b^2)(1-c^2)},\ bc+\sqrt{(1-b^2)(1-c^2)}\right]$. It remains to consider what happens if it's not the case, that is, when $0 < bc-\sqrt{(1-b^2)(1-c^2)}$. Note that $f:[-1,1]\to\mathbb{R}$ defined as $f(x)=x^n$ is strictly increasing on $(0,1]$ so, since

$$a \in \left[bc-\sqrt{(1-b^2)(1-c^2)},\ bc+\sqrt{(1-b^2)(1-c^2)}\right],$$

we must have

$$a^n \in \left[\left(bc-\sqrt{(1-b^2)(1-c^2)}\right)^n,\ \left(bc+\sqrt{(1-b^2)(1-c^2)}\right)^n\right].$$

Therefore it suffices to show that

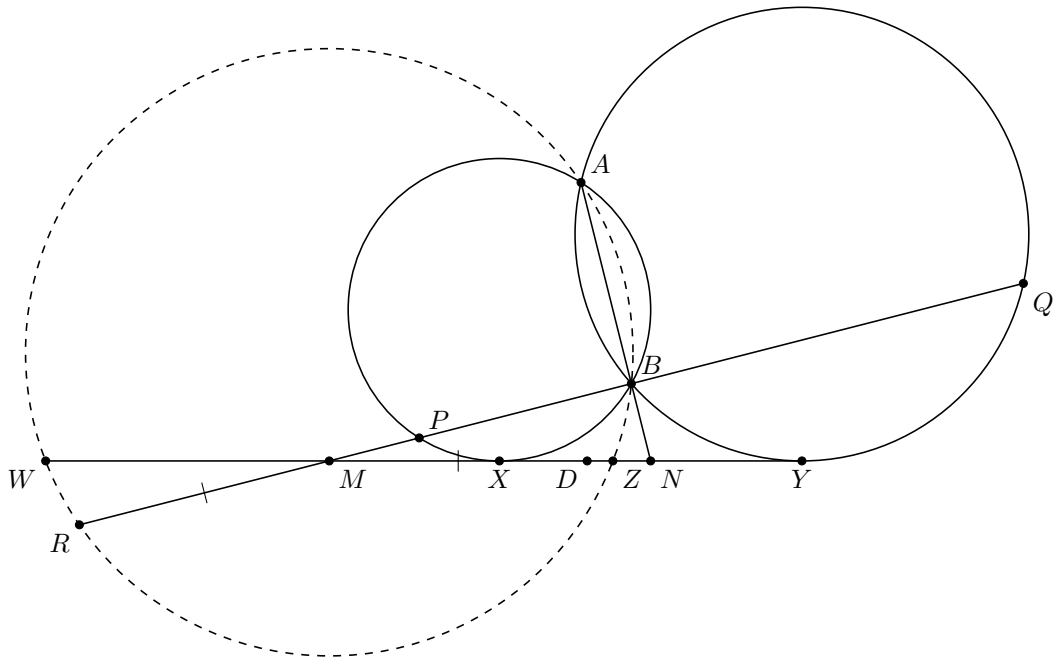
$$\left[\left(bc-\sqrt{(1-b^2)(1-c^2)}\right)^n,\ \left(bc+\sqrt{(1-b^2)(1-c^2)}\right)^n\right] \subseteq$$
$$\subseteq \left[b^nc^n-\sqrt{(1-b^{2n})(1-c^{2n})},\ b^nc^n+\sqrt{(1-b^{2n})(1-c^{2n})}\right],$$

that is

$$\left(bc-\sqrt{(1-b^2)(1-c^2)}\right)^n \geq b^nc^n-\sqrt{(1-b^{2n})(1-c^{2n})},$$
$$\left(bc+\sqrt{(1-b^2)(1-c^2)}\right)^n \leq b^nc^n+\sqrt{(1-b^{2n})(1-c^{2n})},$$

but this was already done in Case I (5.4 and 5.5 did not rely on parity assumptions on n). This finishes the solution.

2. (proposed by Daniel Goc)



By power of point, we just need to prove that $MD^2 = MP \cdot MQ$. This is equivalent to $MR^2 = MP \cdot MQ$. By multiplying both sides by MB^2 and using power of point, we get

$$MX^2 \cdot MY^2 = (MP \cdot MB) \cdot (MQ \cdot MB) = (MR \cdot MB)^2 = (MW \cdot MZ)^2.$$

Thus, it suffices to prove $MX \cdot MY = MW \cdot MZ$. Let N be the intersection of AB with XY. Then $NX^2 = NA \cdot NB = NY^2$, so N is the midpoint of XY. Moreover, $NX^2 = NA \cdot NB = NZ \cdot NW$ by power of point. Expanding it further,

$$NX^2 = NZ \cdot NW = (NM - MZ)(NM + MW) = NM^2 - MZ^2,$$

so $NX^2 + MZ^2 = NM^2$. We can see that this formula possesses some kind of symmetry, as we can transform it also in the opposite direction, now in M:

$$MZ^2 = NM^2 - NX^2 = (NM - NX)(NM + NY) = MX \cdot MY,$$

so $MZ \cdot MW = MX \cdot MY$, which ends the proof.

3. (adapted from solution by Kosma Kasprzak)

Lemma 5.7. A minor of a happy graph is happy.

Proof. Let G be a happy graph with n vertices. We will prove that G remains happy after any of a vertex deletion, an edge deletion or an edge contraction. Let H be a graph obtained from G by a vertex deletion, an edge deletion or an edge contraction. We will prove that H is also happy. Since for any graph $\hat{G}$ we have $P_{\hat{G}}(x_1, x_2, \ldots, x_m) \geq P_{\hat{G}}(|x_1|, |x_2|, \ldots, |x_m|)$, we will assume that all x_i's are non-negative.

1. If H is obtained from G by erasing a vertex, say v_n, then $P_H(x_1, x_2, \ldots, x_{n-1}) = P_G(x_1, x_2, \ldots, x_{n-1}, 0)$.
2. Erasing an edge removes exactly one non-positive term from $P_G(x_1, \ldots, x_n)$, so the sum remains positive.
3. If H is obtained from G by contracting an edge, say (x_{n-1}, x_n), then $P_H(x_1, x_2, \ldots, x_{n-1}) \geq P_G(x_1, x_2, \ldots, x_{n-1}, x_{n-1})$ (these expressions are equal if x_{n-1} and x_n have no common neighbours, otherwise we have some additional terms $-x_i x_j$ on the right-hand side).

□

Let us first note that a graph is happy if and only if all its connected components are happy, so it suffices to consider only connected graphs.

Let's take an arbitrary connected happy graph G. Clearly, a clique on three vertices is not happy (take $x_1 = x_2 = x_3 = 1$), and since its a minor of any graph with at least one cycle and taking a minor preserves happiness, G is a tree. Moreover, a star on five vertices (v_1 is connected to v_2, v_3, v_4, v_5, and there are no other edges) is not happy – take for example $x_1 = 2$, $x_2 = x_3 = x_4 = x_5 = 1$. Therefore, all vertices of G have order at most three, and there is at most one vertex of degree three – if not, after contracting the path between two of them we get a vertex of degree four. Thus, G is either a path, or is a graph consisting of a central vertex v, and three paths of length

k, l, m going out of it. The path case can be seen as a degenerate case of the latter one, with $m = 0$.

For clarity, we will change the variables to $(d, a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_l, c_1, c_2, \ldots, c_m)$, where d corresponds to v, a_1, b_1, c_1 to its neighbours, and $(a_1, \ldots, a_k)$, $(b_1, \ldots, b_k l$, $(c_1, \ldots, c_m)$ correspond to the paths coming out of v.

Let's consider the function P_G on the sphere $x_1^2 + x_2^2 + \ldots + x_n^2 = 1$. It has to attain a minimum, since this is a compact set. Let $(d, a_1, a_2, \ldots, a_k, b_1, b_2, \ldots, b_l, c_1, c_2, \ldots, c_m)$ be that minimum. We can see that for any $1 < j < k$ replacing $a_j \to \frac{a_{j-1}+a_{j+1}}{2}$ decreases the value of P_G, unless $a_j = \frac{a_{j-1}+a_{j+1}}{2}$ (this is just taking the minimum of a quadratic function), so we need to have all these equalities, as we are investigating the minimum. For $j = 1, k$ we can get the same results, but we need to take $a_0 = d$, $a_{k+1} = 0$. This means that $0, a_k, a_{k-1}, \ldots, a_1, d$ is an arithmetic progression, so $a_{k+1-r} = \frac{rd}{k+1}$. We can derive similar results for b_i and c_1 the same way. Using the assumption about sum of squares being 1 we could now calculate the value of d, so we see that this is the minimum of P_G for any k, l, m, and G is happy only if the value there is positive. To calculate this value, let's temporarily add $2d^2$ – now we can split it into values for three paths. The value of one of the paths is

$$d^2 \left(\frac{1^2}{(k+1)^2} + \frac{2^2}{(k+1)^2} + \ldots + \frac{(k+1)^2}{(k+1)^2} - \frac{1 \cdot 2}{(k+1)^2} - \frac{2 \cdot 3}{(k+1)^2} - \ldots - \frac{k \cdot (k+1)}{(k+1)^2} \right)$$
$$= d^2 \frac{k+2}{2(k+1)} = \frac{d^2}{2} \left(1 + \frac{1}{k+1} \right),$$

so the total value of P_G is

$$\frac{d^2}{2} \left(3 + \frac{1}{k+1} + \frac{1}{l+1} + \frac{1}{m+1} \right) - 2d^2 = \frac{d^2}{2} \left(\frac{1}{k+1} + \frac{1}{l+1} + \frac{1}{m+1} - 1 \right).$$

Clearly this value is positive if and only if $\frac{1}{k+1} + \frac{1}{l+1} + \frac{1}{m+1} > 1$. This is true if at least one of k, l, m is zero, which corresponds to a path. To derive other solutions, suppose $1 \le k \le l \le m$. Clearly we need $k = 1$. Now, if $l = 1$ then any m works; if $l = 3$ then no m works; and if $l = 2$ then $m + 1 < 6$. This way we get solutions corresponding to $(1, 1, m)$, $(1, 2, 2)$, $(1, 2, 3)$ and $(1, 2, 4)$ which, along with all paths, constitute all happy connected graphs. The algebraic transformations above indeed show that all of those graphs are happy. Therefore, a general graph is happy if and only if all its connected components are happy connected graphs of the form described above, which finishes the solution.

Remark 5.8. Connected graphs that are solutions to our problem are *Dynkin diagrams* A_n, D_n, E_6, E_7 and E_8. They arise in many areas of mathematics, such as representation theory or classification of semisimple Lie algebras. E_8 is also connected to the recent solution of Kepler's conjecture about sphere packing in eight dimensions.

4. Suppose the equation is satisfied for some k, l, m. Let's replace $\sqrt{2}$ with x. Then the polynomial $P(x) := (3-x)^k + (4+x)^l - (5-x)^m$ is divisible by $x^2 - 2$. Indeed, $P(\sqrt{2}) = 0$, so P has to be divisible by minimal polynomial of $\sqrt{2}$, which is exactly $x^2 - 2$. Thus, $P(x) = (x^2 - 2)Q(x)$ for some polynomial Q with integer coefficients. Now, let's substitute 3 for x. We get $P(3) = 7Q(3)$, so $P(3)$ is divisible by 7. But $P(3) = 7^l - 2^m$ and 2^m is not divisible by 7. We get a contradiction, which means the given equation has no solutions.

5. We will prove that now Bob has a winning strategy that starts with him playing 43. Since 2021 is divisible by 43, the forbidden numbers are now exactly multiples of 43, and Alice has to play some number a coprime with 43. By a well-known solution to the postage stamp problem (with two stamps) $N := 43a - 43 - a$ becomes the greatest number that is not forbidden. In particular, this means that there is only a finite number of possible moves and this number decreases after every turn, so the game will end and either Alice or Bob has a winning strategy.

We claim that regardless of Bob's next move, the number N will be forbidden afterwards. This would allow us to perform a strategy stealing proof. Indeed, suppose that Alice has a winning strategy. After Bob plays N, Alice has some winning move c. But then, Bob could just have played c in the first place, and get to the same situation, with Alice in the losing position. This is a contradiction with the fact that Alice has a winning strategy, so it's actually Bob who has a winning strategy.

It suffices to prove the above claim. Suppose Bob plays c. We claim that $N - c$ was already a forbidden number, which would mean that N is also forbidden, since both c and $N - c$ are. Choose d so that $c \equiv ad \pmod{43}$ and $0 \le d \le 42$. If $c \ge ad$ then it would be a forbidden number, so $c \le ad - 43$. We have $N - c = 43a - 43 - a - c \ge a(42 - d)$ and $N - c = a(42 - d) + (ad - 43 - c)$, where both summands are nonnegative, the first one is divisible by a and the second one by 43. Therefore, $N - c$ is forbidden, which finishes the proof.

Remark 5.9. The game described in the problem (without the first move) is called Sylver Coinage. R. L. Hutchings proved that moves being prime numbers greater of equal to 5 are winning. Cases of moves of a form $2^a 3^b$ are generally open; Conway in 2017 offered \$1000 for determining if 16 is a winning move for Alice.

Qualifying Quiz

Problems

Applicants were asked to attempt **three** out of five *olympic* problems (i.e. problems 1-5) and **three** *exploratory* ones (i.e. problems 6-8). At `https://mathsbeyondlimits.eu/mbl-2021/` you can find solutions to the former, as well as some cool, fun and neat ideas for the latter.

---

1. Nonzero real numbers a, b, c satisfy the condition $a+b+c=-abc=-1$. Show that $\frac{1}{a}+\frac{1}{b}+\frac{1}{c}\leq -1$.

2. Players $A_1, A_2, \ldots, A_{2020}$ competed in a chess tournament. Each player played exactly one match against every other player and there were no ties. We call a pair of players (A_i, A_j) *victorious* if there is no player A_k, who won with both A_i and A_j. Determine whether it is possible that pairs $(A_1, A_2), (A_2, A_3), \ldots, (A_{2019}, A_{2020}), (A_{2020}, A_1)$ are all victorious.

3. Positive integers $x,\ y,\ n$ satisfy $x \neq y$ and $x+y \mid x^{2n}+y^{2n}$. Prove that $(x-y)^{4n} > xy$.

4. A triangle ABC is given with $\sphericalangle BAC = 60°$. Let E and F be feet of angle bisectors from B and C respectively, and I be the intersection of BE and CF. M and N are midpoints of AE and AF, while P and Q are midpoints of IE and IF, respectively. Prove that I lies on a line through circumcenters of triangles CMQ and BPN.

5. We call a positive rational number $\frac{p}{q}$ $(\gcd(p,q)=1;\ p,\ q\neq 1)$ *balanced* if p and q are products of the same number of prime numbers (not necessarily distinct). Prove that for every positive integer k we may find two distinct positive integers x and y such that numbers

$$\frac{x+1}{y+1},\ \frac{x+2}{y+2},\ \ldots,\frac{x+k}{y+k}$$

are all balanced.

---

6. Ania has a very large collection of finite 0-1 sequences.[1] In fact, her collection is infinite and she can't remember it. She wants to be able to quickly tell if any given 0-1 sequence is in her collection. She knows that for any sequence t in her collection, all subsequences of t also belong to it.

She wants you to find a finite set S of 0-1 sequences such that any 0-1 sequence is in Ania's collection if and only if it does not contain any sequence from S as a subsequence.

a) Can you help Ania no matter what is her collection of sequences?

b) If we would change all words "subsequence" to "substring", will the answer change?

Here we assume definitions of `subsequence` and `substring` as on Wikipedia.

[1] A 0-1 sequence is a sequence whose all elements are equal to either 0 or 1.

7. In a convex n-gon $A_1A_2\ldots A_n$ equalities

$$A_1A_3 = A_2A_4 = \ldots = A_{n-1}A_1 = A_nA_2 \quad \text{and} \quad A_1A_4 = A_2A_5 = \ldots = A_{n-1}A_2 = A_nA_3$$

hold.

For which n do they imply that this n-gon is regular? Investigate this question in cases

a) $n = 6$,

b) $n = 7$,

c) $n = 11$.

Any progress in case of general n will be also warmly welcomed.

8. Let n be a given positive integer. Justyna draws n distinct circles on a plane and colours every circle with a different colour. Then she draws a line l such that all circles are on one side of the line. Let P be an arbitrary point on l. If there exists a point A with colour c on some circle, such that $AP \perp l$ and segment AP does not contain points of any other colour, then paint P with colour c. After repeating such operation for every point on l, this line is split to some segments of various colours (some points of the line will remain uncoloured though).

a) What is the greatest number of these segments, in terms of n?

b) Tomek wanted to do the same thing as Justyna, however instead of circles he chose to use equilateral triangles. Moreover he placed his triangles and line l so that each triangle has a side parallel to l (i.e. all triangles are placed either as Δ, or as ∇). What will be the greatest possible number of segments this time?

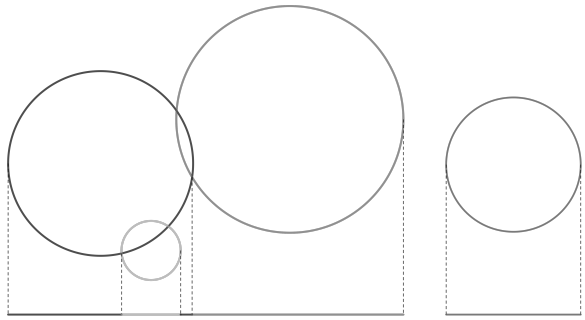


Figure 5.1: In this case we have five segments.

Contents