Mathematical Challenges

July 2021 - December 2021

Contents

1 December 2021

1. Let G be a group with 3129 elements. Prove it is solvable.

   Solution: $3129 = 3 \cdot 7 \cdot 149$ is the product of three distinct primes, hence solvable. See

   `https://www.physicsforums.com/threads/math-challenge-february-2021.999180/page-2#post-6462158`

2. $$I(a) := \int_0^1 \left(\frac{\log x}{a+1-x} - \frac{\log x}{a+x} \right) dx \ ; \ a \in \mathbb{C} \backslash [-1,0]$$

   Solution: Define $F\ :]0,1] \longrightarrow \mathbb{C}$ by
   $$F(x) := \frac{x \log x}{a+x} - \log(a+x)$$
   then
   $$\begin{aligned} F'(x) &= \frac{(a+x)(1+\log x) - x\log x}{(a+x)^2} - \frac{1}{a+x} \\ &= \frac{a + a\log x + x + x\log x - x\log x - a - x}{(a+x)^2} \\ &= \frac{a \log x}{(a+x)^2} \\ &\Longrightarrow \end{aligned}$$
   $$\begin{aligned} a \int_0^1 \frac{\log x}{(a+x)^2}\,dx &= F(1) - F(0^+) = -\log(a+1) - (-\log a) \\ &= \log a - \log(a+1) \end{aligned}$$
   If we define $G\ :]0,1] \longrightarrow \mathbb{C}$ by
   $$G(x) := \frac{x \log x}{a+1-x} + \log(a+1-x)$$
   then
   $$\begin{aligned} G'(x) &= \frac{(a+1-x)(1+\log x) + x\log x}{(a+1-x)^2} - \frac{1}{a+1-x} \\ &= \frac{(a+1)\log x}{(a+1-x)^2} \\ &\Longrightarrow \end{aligned}$$
   $$(a+1)\int_0^1 \frac{\log x}{(a+1-x)^2} = G(1) - G(0^+) = \log a - \log(a+1)$$

Putting those integrals together and integrating by a gives

$$\begin{aligned}
&\int \left(\int_0^1 \left(\frac{\log x}{(a+x)^2} - \frac{\log x}{(a+1-x)^2} \right) dx \right) da \\
&\int_0^1 \left(\int \left(\frac{\log x}{(a+x)^2} - \frac{\log x}{(a+1-x)^2} \right) da \right) dx \\
&\quad = \int_0^1 \left(-\frac{\log x}{a+x} + \frac{\log x}{a+1-x} + C \right) dx = I(a) + C' \\
&\quad = \int \left(\left(\frac{1}{a} - \frac{1}{a+1} \right) \cdot (\log a - \log(a+1)) \right) da \\
&\quad = \frac{1}{2} (\log a - \log(a+1))^2 + C''
\end{aligned}$$

and we get $I(a) = \frac{1}{2} (\log a - \log(a+1))^2 + C$. Note that the limit $\lim_{a\to\infty} I(a) = 0$, i.e. $C = 0$, hence

$$I(a) = \frac{1}{2} (\log a - \log(a+1))^2 = \frac{1}{2} \log^2 \frac{a}{a+1}$$

3. Let $\mathfrak{g}$ be a Lie algebra over a field of characteristic not 2. Prove that

$$\mathfrak{A}(\mathfrak{g}) = \{\alpha \in \mathfrak{gl}(\mathfrak{g}) \,|\, [\alpha(X), Y] + [X, \alpha(Y)] = 0 \text{ for all } X, Y \in \mathfrak{g}\}$$

is a Lie algebra. Determine $\mathfrak{A}(\mathfrak{B})$ for the two-dimensional non-abelian Lie algebra $\mathfrak{B}$.

Solution: $\mathfrak{B} = \langle X, Y \,|\, [X, Y] = Y \rangle$. Let $\alpha(X) = aX + bY$ and $\alpha(Y) = cX + dY$. Then the only defining equation is

$$Y = [aX + bY, cX + dY] = (ad - bc)Y \Rightarrow ad - bc = 1 \Rightarrow \mathfrak{A}(\mathfrak{B}) \cong \mathfrak{sl}(2)$$

which is a Lie algebra. To prove the general case, we only have to verify that $[\alpha, \beta] := \alpha\beta - \beta\alpha \in \mathfrak{A}(\mathfrak{g})$ since $\mathfrak{A}(\mathfrak{g})$ is obviously a vector space, and the Jacobi identity holds for the commutator multiplication.

$$\begin{aligned}
[[\alpha, \beta](X), Y] + [X, [\alpha, \beta](Y)] &= [\alpha(\beta(X)), Y] - [\beta(\alpha(X)), Y] \\
&\quad + [X, \alpha(\beta(Y))] - [X, \beta(\alpha(Y))] \\
&= -[\beta(X), \alpha(Y)] + [\alpha(X), \beta(Y)] \\
&\quad - [\alpha(X), \beta(Y)] + [\beta(X), \alpha(Y)] \\
&= 0
\end{aligned}$$

4. Show that a path connected set is connected but not vice versa and not necessarily simply connected.

Solution: A set A of a topological space X is path connected, if for any two points $a, b \in A$ there is a continuous curve $\gamma : [0,1] \to A$ with $\gamma(0) = a$ and $\gamma(1) = b$ that is entirely in A. If any such curve is null-homotopic, then A is simply connected. A is connected, if it cannot be written as disjoint union of two nonempty, open sets.

Let $A \subseteq X$ be path connected and $A = U \dot{\cup} V$ a disjoint union of open sets $U, V \neq \emptyset$. Choose $a \in U, b \in V$ and $\gamma(t)$ a continuous path that connects the two points. Then $\gamma^{-1}(U), \gamma^{-1}(V) \subseteq \mathbb{R}$ are disjoint, open sets. Since

$$[0,1] \subseteq \gamma^{-1}(U) \dot{\cup} \gamma^{-1}(V) = \gamma^{-1}(U \dot{\cup} V) = \gamma^{-1}(A)$$

is a connected interval, we have w.l.o.g. $[0,1] \subseteq \gamma^{-1}(U)$. But this contradicts $V \ni v = \gamma(1) \notin U$.

The opposite is false. Consider

$$A = \underbrace{\{(0,y) \in \mathbb{R}^2 \mid -1 \leq y \leq 1\}}_{=:U} \cup \underbrace{\{(x, \sin(x^{-1})) \in \mathbb{R}^2 \mid x > 0\}}_{=:V}$$

equipped with the standard Euclidean topology of $\mathbb{R}^2$, then there is no continuous path from $(0,0) \in U$ to $(\pi^{-1}, 0) \in V$ within A. However, every open neighborhood of $(0,0)$ always contains a point of V, hence A is connected.

The unit disc $D := \{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq 1\}$ in $\mathbb{R}^2$ is path connected, i.e. connected, too. If we cut out $B := \{(x,y) \in \mathbb{R}^2 \mid x^2 + y^2 \leq 1/4\}$, then $D \backslash B$ is still path connected, but not null-homotopic.

5.
$$\int_0^{\frac{\pi}{4}} \log(1 + \tan x)\, dx$$

Solution:

$$\begin{aligned}
\sqrt{2}\cos\left(\frac{\pi}{4} - x\right) &= \sqrt{2}\cos\left(\frac{\pi}{4}\right)\cos(x) + \sqrt{2}\sin\left(\frac{\pi}{4}\right)\sin(x) \\
&= \cos(x) + \sin(x) = \cos(x) \cdot \frac{\cos(x) + \sin(x)}{\cos(x)} \\
&= \cos(x) \cdot (1 + \tan(x)) \\
\log(1 + \tan(x)) &= -\log(\cos(x)) + \log(\sqrt{2}) + \log\left(\cos\left(\frac{\pi}{4} - x\right)\right)
\end{aligned}$$

Substitute $x \in [0, \pi/4]$ by $u = -x + \pi/4 \in [0, \pi/4]$ with $du = -dx$ so

$$\begin{aligned}\int_0^{\frac{\pi}{4}} \log\left(\cos\left(\frac{\pi}{4} - x\right)\right)\,dx &= -\int_{\frac{\pi}{4}}^{0} \log(\cos(u))\,du \\ &= \int_0^{\frac{\pi}{4}} \log(\cos(x))\,dx\end{aligned}$$

hence

$$\int_0^{\frac{\pi}{4}} \log(1 + \tan x)\,dx = \int_0^{\frac{\pi}{4}} \log(\sqrt{2}) = \frac{\pi}{8}\log(2)$$

6. There are currently about $7,808,000,000$ people on earth. If we would enumerate them all, how many of them would have a prime number?

   Solution: A little bit more than the population of the United States of America:

$$\begin{aligned}\pi(x) &\sim \frac{x}{\log(x)} \\ \pi(7,808,000,000) &\approx 342,780,659\end{aligned}$$

7. Let $M = \mathbb{R}^2$ and $G = \mathbb{R}$ and consider the map

$$\psi(\varepsilon,(x,y)) := \left(\frac{x}{1-\varepsilon x}, \frac{y}{1-\varepsilon x}\right)$$

   defined on

$$U = \left\{(\varepsilon,(x,y)) \,|\, \varepsilon < \frac{1}{x} \text{ for } x > 0, \text{ or } \varepsilon > \frac{1}{x} \text{ for } x < 0\right\} \subseteq \mathbb{R} \times \mathbb{R}^2$$

   Show that ψ defines a local group action of G on the manifold M. Does it have a global counterpart on $\mathbb{R}^2$?

   Solution: Whenever defined, we get

$$\begin{aligned}\psi(\delta,\psi(\varepsilon,(x,y))) &= \psi\left(\delta,\left(\frac{x}{1-\varepsilon x}, \frac{y}{1-\varepsilon x}\right)\right) \\ &= \left(\frac{x/(1-\varepsilon x)}{1-\delta x/(1-\varepsilon x)}, \frac{y/(1-\varepsilon x)}{1-\delta x/(1-\varepsilon x)}\right) \\ &= \left(\frac{x}{1-\varepsilon x-\delta x}, \frac{y}{1-\varepsilon x-\delta x}\right) \\ &= \left(\frac{x}{1-(\delta+\varepsilon)x}, \frac{y}{1-(\delta+\varepsilon)x}\right) = \psi(\delta+\varepsilon,(x,y))\end{aligned}$$

There is no global counterpart of this local action, because

$$\lim_{\varepsilon\to 1/x} |\psi(\varepsilon,(x,y))| = \infty \text{ for } x\neq 0$$

Note: ψ occurs in the study of the heat equation. Its orbits consists of the straight rays emanating from the origin, and the origin itself. The action is regular on the punctured plane $\mathbb{R}^2\backslash\{0\}$.

8. Give an example of a ring and a maximal ideal that isn't a prime ideal.

   Solution: If we have a commutative ring R with 1, then an ideal $P \trianglelefteq R$ is prime if R/P is an integral domain, and an ideal $M \trianglelefteq R$ is maximal if R/M is a field. Since all fields are integral domains, all maximal ideals are prime in this case. Hence we consider a ring without 1 and set $R = 2\mathbb{Z}$ and $M := 4\mathbb{Z}$.

   Let $R \neq M \trianglelefteq I \trianglelefteq R$ and $r = 2m \in I\backslash M$. Then m is odd, say $m = 2k+1$, so $I \supseteq IR = 4k\mathbb{Z} + 2\mathbb{Z} = R$, i.e. M is a maximal ideal.

   We have $2m\cdot 2n = 4nm \in M$, but $2m, 2n \notin M$ for n, m odd and neither is a unit, because R has none. This shows that M is not prime.

9. Let $U,V \subseteq \mathbb{C}$ open sets, $\varphi : U \longrightarrow V$ a holomorphic function, and $\gamma : [0,1] \longrightarrow U$ a closed, smooth path. Show that if γ is 0-homologue in U, then $\varphi\circ\gamma$ is 0-homologue in V.

   Solution: If γ is 0-homologue in U, then $\int_\gamma f(z)\,dz = 0$ by Cauchy's integral theorem. Thus

$$\begin{aligned}\int_{\varphi\circ\gamma} g(z)\,dz &= \int_0^1 g(\varphi(\gamma(t)))\cdot(\varphi\circ\gamma)'(t)\,dt\\ &= \int_0^1 (g\circ\varphi)(\gamma(t))\cdot\varphi'(\gamma(t))\cdot\gamma'(t)\,dt\\ &= \int_\gamma \underbrace{g\circ\varphi(z)\cdot\varphi'(z)}_{\text{holomorphic in U}}\,dz = 0\end{aligned}$$

   so $\varphi\circ\gamma$ is 0-homologue in V again by Cauchy's integral theorem (converse version).

   It is also possible to calculate it directly without using the backward direction of Cauchy's integral theorem. Let $z \in \mathbb{C}\backslash V$. Then

$$\begin{aligned}2\pi i \cdot \operatorname{ind}_{\varphi\circ\gamma}(z) &= \int_{\varphi\circ\gamma} \frac{1}{\zeta - z}\,d\zeta = \int_0^1 \frac{\varphi'(\gamma(t))\cdot\gamma'(t)}{\varphi(\gamma(t)) - z}\,dt \\ &= \int_\gamma \frac{\varphi'(\zeta)}{\varphi(\zeta) - z}\,d\zeta = 0\end{aligned}$$

The integration kernel $\dfrac{\varphi'(\zeta)}{\varphi(\zeta)-z}$ in the last integral is holomorphic on U since $z \notin V \supseteq \varphi(U)$ and we can use the forward direction of Cauchy's integral theorem.

10. Examine convergence:

$$\prod_{n=2}^{\infty}\left(1-\frac{1}{n}\right)\;,\;\prod_{n=3}^{\infty}\left(1-\frac{4}{n^2}\right)$$

Solution: All factors of both products are unequal zero. Set $P_n = \prod_{k=2}^n \left(1 - \dfrac{1}{k}\right)$ for $n \geq 2$.

$$\begin{aligned}P_n &= \prod_{k=2}^n \frac{k-1}{k} \stackrel{\text{telescope}}{=} \frac{1}{n} \\ &\Longrightarrow \lim_{n\to\infty} P_n = \lim_{n\to\infty}\frac{1}{n} = 0 \\ &\Longrightarrow \prod_{n=2}^{\infty}\left(1-\frac{1}{n}\right)\end{aligned}$$

does not converge, since the limit cannot be zero by definition of multiplication. (The logarithm gives a divergent series.)

Set $Q_n = \prod_{k=3}^n \left(1 - \dfrac{4}{k^2}\right)$ for $n \geq 3$.

$$\begin{aligned}Q_n &= \prod_{k=3}^n \frac{k^2-4}{k^2} = \prod_{k=3}^n \frac{k+2}{k}\cdot\frac{k-2}{k} = \prod_{k=3}^n \frac{k+2}{k+1}\cdot\frac{k+1}{k}\cdot\frac{k-1}{k}\cdot\frac{k-2}{k-1} \\ &= \prod_{k=3}^n \frac{k+2}{k+1}\cdot\prod_{k=3}^n\frac{k+1}{k}\cdot\prod_{k=3}^n\frac{k-1}{k}\cdot\prod_{k=3}^n\frac{k-2}{k} \\ &\stackrel{\text{telescope}}{=} \frac{n+2}{4}\cdot\frac{n+1}{3}\cdot\frac{2}{n}\cdot\frac{1}{n-1} = \frac{n^2+3n+2}{6n^2-6n}\end{aligned}$$

Hence

$$\prod_{n=3}^{\infty}\left(1-\frac{4}{n^2}\right)=\lim_{n\to\infty}Q_n=\lim_{n\to\infty}\frac{n^2+3n+2}{6n^2-6n}=\frac{1}{6}\,.$$

11. The Heisenberg algebra can be viewed as

$$\mathfrak{H}=\left\{\begin{bmatrix}0&x_1&x_3\\0&0&x_2\\0&0&0\end{bmatrix}\;:\;x_1,x_2,x_3\in\mathbb{R}\right\}.$$

Calculate $\exp(H)$ for a matrix $H\in\mathfrak{H}$.

Solution: Let e_{ij} be the matrix with 1 at position (i,j) and 0 elsewhere, and set $N:=x_1e_{12}+x_2e_{23}, M:=e_{13}$. Then $N^2=x_1x_2M, NM=MN=0$ and $M^2=0$. Thus

$$\begin{aligned}\exp(N+x_3M)&=\sum_{k=0}^{\infty}\frac{(N+x_3M)}{n!}\\&=\operatorname{Id}+(N+x_3M)+\frac{x_1x_2M}{2!}+\frac{0}{3!}+\ldots\\&=\begin{bmatrix}1&x_1&x_3+\dfrac{x_1+x_2}{2}\\0&1&x_2\\0&0&1\end{bmatrix}\in\left\{\begin{bmatrix}1&*&*\\0&1&*\\0&0&1\end{bmatrix}\right\}\end{aligned}$$

the Heisenberg group.

12.

$$\int_{-\infty}^{\infty}\frac{|\sin(\alpha x)|}{1+x^2}\,dx\;,\;\alpha>0$$

Solution: $|\sin(\alpha x)|$ has the Fourier series

$$|\sin(\alpha x)|=\frac{2}{\pi}+\frac{2}{\pi}\sum_{n=1}^{\infty}\left(\frac{1}{2n+1}-\frac{1}{2n-1}\right)\cos(2n\alpha x)$$

so

$$\begin{aligned}\int_{-\infty}^{\infty}\frac{|\sin(\alpha x)|}{1+x^2}\,dx &= 2+2\sum_{n=1}^{\infty}\left(\frac{1}{2n+1}-\frac{1}{2n-1}\right)\underbrace{\frac{1}{\pi}\int_{-\infty}^{\infty}\frac{\cos(2n\alpha x)}{1+x^2}\,dx}_{=e^{-2n\alpha}}\\
&= 2+2\sum_{n=1}^{\infty}\frac{(e^{-\alpha})^{2n}}{2n+1}-2\sum_{n=1}^{\infty}\frac{(e^{-\alpha})^{2n}}{2n-1}\\
&= 2\sum_{n=0}^{\infty}\frac{(e^{-\alpha})^{2n}}{2n+1}-2\sum_{n=0}^{\infty}\frac{(e^{-\alpha})^{2n+2}}{2n+1}\\
&= 2\left(e^{\alpha}-e^{-\alpha}\right)\sum_{n=0}^{\infty}\frac{(e^{-\alpha})^{2n+1}}{2n+1}\\
&= 4\sinh(\alpha)\operatorname{artanh}\left(e^{-\alpha}\right)\end{aligned}$$

13. Show that $(n-1)! \equiv -1 \mod n$ holds if and only if n is prime. Determine the first two primes for which even $(p-1)! \equiv -1 \mod p^2$ holds.

    Solution: We may assume $n > 2$. Let $n = p$ be prime. The polynomial $x^p - x = x(x^{p-1}-1)$ has exactly p roots in $\mathbb{Z}_p$. It has only simple roots, since $(x^p-x)' = px^{p-1}-1 \equiv -1 \mod p$, and there are at most p roots. Hence $x^p - x = x(x-1)\cdot\ldots\cdot(x-(p-1))$. Now

    $$\begin{aligned}&f(x) := x^{p-1}-1 = (x-1)\cdot\ldots\cdot(x-(p-1))\\ &f(p) = p^{p-1}-1 = (p-1)\cdot\ldots\cdot(p-(p-1)) = (p-1)! \equiv -1 \mod p\end{aligned}$$

    Next let $(n-1)! \equiv -1 \mod n$ and $n = a\cdot b$ with $a,b > 1$. Then

    $$\begin{aligned}a\,|\,(n-1)! &\Longrightarrow a\cdot c = (n-1)! \wedge n\cdot d = (n-1)!+1\\ &\Longrightarrow ac = nd-1 = abd-1 \Longrightarrow 0 \equiv -1 \mod a \quad ⭍\end{aligned}$$

    and n is prime.

    The small faculties are $1, 2, 6, 24, 120, \ldots$ and we see, that $24 = 5! \equiv -1 \mod 5^2$. The next one is a bit harder to find. It is

    $$\frac{(13-1)!+1}{13^2} = \frac{479{,}001{,}601}{169} = 2{,}834{,}329$$

    Up to now, there is only one more so called Wilson prime known, namely 563. It is unknown whether there are more than that. If, then they are greater than $20{,}000{,}000{,}000{,}000$. The conjecture is, that there are infinitely many Wilson primes.

14. Determine all possible topologies on $X := \{a, b\}$, and which of them are homeomorphic. Give an example of a topological space with more than one element such that all sequences converge.

    Solution: We always have the discrete topology

    $$T_d = \{\emptyset, \{a\}, \{b\}, X\} = \{\{\}, \{a\}, \{b\}, \{a, b\}\}$$

    where all subsets are open, and indiscrete or trivial topology

    $$T_t = \{\emptyset, X\} = \{\{\}, \{a, b\}\}$$

    All topologies have to be close under all unions and all intersections because we have a finite set X. Thus we get also

    $$T_a = \{\emptyset, \{a\}, X\} = \{\{\}, \{a\}, \{a, b\}\} \ , \ T_b = \{\emptyset, \{b\}, X\} = \{\{\}, \{b\}, \{a, b\}\}$$

    We want to prove, that only T_a and T_b are homeomorph by $f(a) = b\,,\, f(b) = a$. We have $f^{-1}(\emptyset) = \emptyset \in T_b$, $f^{-1}(\{a\}) = \{b\} \in T_b$, and $f^{-1}(X) = X \in T_b$. The same is true for the inverse function, so f and its inverse function are both continuous. Assume there would be a homeomorphism $f : T_t \to T_a$. Then $f^{-1}(\{a\}) \in \{\emptyset, X\}$. But f is bijective, i.e. the pre-image of a singleton has to be a singleton. This contradiction shows that $T_t \ncong T_a$ and likewise $T_t \ncong T_b$. Assume there would be a homeomorphism $f : T_a \to T_d$. Then $f^{-1}(\{b\})$ and $f^{-1}(\{a\})$ must both be singletons, and different, which is impossible. Hence $T_a \ncong T_d$ and likewise $T_b \ncong T_d$. For the same reason we get $T_t \ncong T_d$.

    Consider T_a. Each sequence in (X, T_a) converges against b because in every neighborhood of b, which is only $X = \{a, b\}$ are all sequence elements.

15. Explain the difference between $\mathbb{Z}_2 \times \mathbb{Z}_3$ and $\mathbb{Z}_2 \ltimes \mathbb{Z}_3$. Is there also a group $\mathbb{Z}_2 \rtimes \mathbb{Z}_3$?

    Solution: All these expressions have $G = \{\mathbb{Z}_2, \mathbb{Z}_3\}$ as common underlying set. It has six elements. $\mathbb{Z}_2 \times \mathbb{Z}_3$ is the direct product with the multiplication

    $$(b, c) \cdot (b', c') = (b \cdot b, c \cdot c')$$

    $\mathbb{Z}_2 \ltimes \mathbb{Z}_3$ indicates that $\mathbb{Z}_3 \trianglelefteq G$ is a normal in the resulting group. It is called semi-direct product and has the multiplication

    $$(b, c) \cdot (b', c') = (b \cdot b', c \cdot \sigma(b)(c'))$$

with a homomorphism $\sigma : \mathbb{Z}_2 \longrightarrow \operatorname{Aut}(\mathbb{Z}_3)$ into the automorphism group of the normal subgroup. It can also be written $\mathbb{Z}_3 \rtimes_\sigma \mathbb{Z}_2$ to indicate the important influence of σ. We know that there are two groups of order 6, $\mathbb{Z}_6$ and S_3. The first is abelian, as is the product $\mathbb{Z}_2 \times \mathbb{Z}_3$. Since $(1,2)$ generates $(\mathbb{Z}_2 \times \mathbb{Z}_3, +)$, it is a cyclic group and we get

$$\mathbb{Z}_2 \times \mathbb{Z}_3 \cong \mathbb{Z}_6 \,.$$

S_3 is not abelian and has subgroups $A_3 = \{(1),(123),(132)\}$ and $\{(1),(12)\}$, $\{(1),(13)\}$, $\{(1),(23)\}$ with three, two elements, resp.
Since $(123)(12)(132) = (23)$ the latter three groups are not normal in S_3. On the other hand $(12)(123)(12) = (132)$ so $A_3 \trianglelefteq S_3$ is a normal subgroup. It also shows that $\sigma : \mathbb{Z}_2 \longrightarrow \operatorname{Inn}(\mathbb{Z}_3) \trianglelefteq \operatorname{Aut}(S_3)$ defined by the conjugation with (12), i.e. $\sigma((1)) = (1)$ and $\sigma((12)) = \iota_{(12)}$ defines the required homomorphism, where $\iota_{(12)}$ is the inner automorphism conjugation with (12), and we get

$$G \cong A_3 \rtimes_\sigma \{(1),(12)\} \cong \mathbb{Z}_3 \rtimes \mathbb{Z}_2$$

Assume $\mathbb{Z}_2 \rtimes_\sigma \mathbb{Z}_3$ would be a group with non-trivial homomorphism $\sigma : \mathbb{Z}_3 \to \operatorname{Aut}(Z_2)$. However, $\operatorname{Aut}(\mathbb{Z}_2) = \{1\}$ because $\alpha(1) = 1$ which also fixes the second element by the requirement that all $\alpha \in \operatorname{Aut}(\mathbb{Z}_2)$ are bijective. Hence $\sigma(\mathbb{Z}_3) = 1$ and σ would be trivial, i.e. the product a direct one. Thus the notation $\mathbb{Z}_2 \rtimes_\sigma \mathbb{Z}_3$ makes no sense.

16. Show that 16 and 33 are Størmer numbers, but no number $2n^2 > 2$ can be one, e.g. 32.

    Solution: A Størmer number is a number for which there is a prime p such that $p > 2n$ and $p \,|\, (n^2+1)$.

    $p = 257 = 16^2 + 1$ is a prime number and $p > 2 \cdot 16 = 32$.
    $1090 = 33^2 + 1 = 2 \cdot 5 \cdot 109$ and $p = 109 > 2 \cdot 33 = 66$.
    $1025 = 32^2 + 1 = 5^2 \cdot 41$ but $p = 41 < 2 \cdot 25 = 50$.
    In general if for $n > 1$

    $$p \,|\, (2n^2)^2 + 1 = 4n^4 + 1 = (2n^2 - 2n + 1)(2n^2 + 2n + 1)$$

    then $p \,|\, (2n^2 \pm 2n + 1) < 2 \cdot 2n^2 = 4n^2$.

    Størmer numbers n are exactly those numbers for which there isn't a linear combination

    $$\operatorname{arccot} n = \sum_{k=1}^{n-1} a_k \cdot \operatorname{arccot} k \,,\; a_k \in \mathbb{Z}$$

Størmer numbers are therefore also called arc-cotangent irreducible numbers.

17. Consider a number n which is not a prime and

$$p \,|\, n \Longrightarrow p \,|\, \left(\frac{n}{p} - 1\right)$$

E.g. $30 = 2 \cdot 3 \cdot 5$ is such a number, since $2 \,|\, 14\,,\ 3 \,|\, 9\,,\ 5 \,|\, 5$.

Show that n is square-free (all prime factors have exponent 1), and no semiprime (product of exactly two primes).

Solution: Numbers with those properties are called **Giuga numbers**. Giuga conjectured 1950 that a natural number is prime, if and only if

$$\sum_{k=1}^{n-1} k^{n-1} \equiv -1 \mod n.$$

The equation follows from Fermat's little theorem if n is prime:

$$k^{p-1} \equiv 1 \mod p \Longrightarrow \sum_{k=1}^{n-1} k^{n-1} \equiv (p-1) \cdot 1 = p - 1 \equiv -1 \mod p$$

It is not clear whether the other direction holds, i.e. whether there are composite numbers with this property. It is only known that such a number has at least 10,000 decimal digits. A **Carmichael number** n is a composite, square-free number with the additional property

$$a^{n-1} \equiv 1 \mod n \text{ for all coprime } a\ ,\ (a, n) = 1.$$

Korselt had shown 1899 that a number n is a Carmichael number, if it is not prime, square-free, and for all its prime divisors $p \,|\, n$ holds $(p-1) \,|\, (n-1)$. This result can be tightened to

$$p \,|\, n \Longrightarrow (p-1) \,|\, \left(\frac{n}{p} - 1\right)$$

because $n - 1 = (n/p) - 1 + (p-1)(n/p)$, i.e. $n - 1 \equiv (n/p) - 1 \mod (p-1)$. This shows, that Carmichael numbers and Giuga numbers are closely related. Giuga's conjecture is indeed equivalent to:

No natural number is simultaneously Giuga and Carmichael number.

Another interesting theorem is, that n is a Giuga number, if and only if it is a composite, square-free number and

$$\sum_{p|n}\frac{1}{p}-\prod_{p|n}\frac{1}{p}\in\mathbb{N}.$$

This term equals 1 for all known Giuga numbers:

$$30, 858, 1722, 66198, 2214408306, 24423128562, 432749205173838,$$
$$14737133470010574, 550843391309130318,$$
$$244197000982499715087866346,$$
$$554079914617070801288578559178,$$
$$1910667181420507984555759916338506$$

Proof of the initial statements:

Let n be a Giuga number. Assume $p^2\,|\,n$. Then $p\,|\,(n/p)$ and $p\nmid (n/p)-1$ in contradiction to the defining condition.

Next assume $n=p\cdot q$ is a product of two primes with $p<q$. Then $(n/q)-1=p-1<p<q$. Hence $q\nmid ((n/q)-1)$, again a contradiction to the defining condition.

18. Prove that path integrals in $\mathbb{R}^n$ over gradient vector fields depend only on starting and endpoint, and not on the path itself.

Solution: Let $f:\mathbb{R}\longrightarrow\mathbb{R}$ a gradient vector field, i.e. there is a differentiable function $V:\mathbb{R}^n\longrightarrow\mathbb{R}$ with

$$(\operatorname{grad}V)^\tau=f.$$

Let $\gamma:[a,b]\longrightarrow\mathbb{R}^n$ be a smooth curve with $f(a)=x_0, f(b)=x_1$. Then

$$\begin{aligned}\int_\gamma\langle f,ds\rangle&=\int_a^b\langle f(\gamma(t)),\gamma'(t)\rangle\,dt=\int_a^b\langle\operatorname{grad}V(\gamma(t))^\tau,\gamma'(t)\rangle\,dt\\&=\int_a^b\operatorname{grad}V(\gamma(t))\cdot\gamma'(t)\,dt=\int_a^b\left[\frac{d}{dt}V(\gamma(t))\right]\,dt\end{aligned}$$

Now $V\circ\gamma:[a,b]\longrightarrow\mathbb{R}$ is a one-dimensional differentiable function. Thus we can apply the fundamental theorem of calculus and get

$$\int_\gamma\langle f,ds\rangle=V(\gamma(b))-V(\gamma(a))=V(x_1)-V(x_0)$$

which is independent of γ.

19. Let $P_0 = 0, P_1 = 1, P_n = 2P_{n-1} + P_{n-2}$ for all $n \in \mathbb{N}, n \geq 2$. Determine a closed form for P_n.

    Solution: All sequence elements are greater or equal zero, and the sequence is strictly monotone increasing: $0 < P_{n-1} < 2P_{n-1} + P_{n-2} = P_n$ for $n > 1$. Therefore $2 \leq P_n/P_{n-1} = 2 + P_{n-2}/P_{n-1} < 3$ for $n > 1$. Since $(P_n/P_{n-1})_{n>1}$ is bounded from below and from above, it has at least one convergent subsequence by the theorem of Bolzano-Weierstraß.

    If $(P_n/P_{n-1})_{n>1}$ converges, say against L, then

    $$L := \lim_{n\to\infty} \frac{P_n}{P_{n-1}} = 2 + \lim_{n\to\infty} \frac{P_{n-2}}{P_{n-1}} = 2 + \frac{1}{L}$$

    hence $L^2 - 2L - 1 = 0$ and $L = 1 \pm \sqrt{2}$. As each element of the sequence is greater than 2, we have $L = 1 + \sqrt{2}$.

    If we only consider the recursion without initial conditions, then we have two possible limits and the two sequences

    $$A_0 = a \wedge A_n := a(1+\sqrt{2})^n$$
    $$B_0 = b \wedge B_n := b(1-\sqrt{2})^n$$

    are solutions to $P_n = 2P_{n-1} + P_{n-2}$ and therewith all linear comninations $a(1+\sqrt{2})^n + b(1-\sqrt{2})^n$. With $P_0 = 0, P_1 = 1$ we get

    $$P_0 = a + b$$
    $$P_1 = a(1+\sqrt{2}) + b(1-\sqrt{2})$$
    $$\begin{bmatrix} a \\ b \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1+\sqrt{2} & 1-\sqrt{2} \end{bmatrix}^{-1} \begin{bmatrix} 0 \\ 1 \end{bmatrix} = -\frac{1}{2\sqrt{2}} \begin{bmatrix} -1 \\ 1 \end{bmatrix} = \begin{bmatrix} 1/2\sqrt{2} \\ -1/2\sqrt{2} \end{bmatrix}$$

    so with our given initial conditions we have

    $$P_n = \frac{\left(1+\sqrt{2}\right)^n - \left(1-\sqrt{2}\right)^n}{2\sqrt{2}}\,.$$

    It is easy to check that P_n fulfills the recursion. It is called Pell sequence and $1 + \sqrt{2}$ the silver ratio. Finally, we have to prove that P_n/P_{n-1}

actually converges.

$$\begin{aligned}\frac{P_n}{P_{n-1}} &= \frac{\left(1+\sqrt{2}\right)^n - \left(1-\sqrt{2}\right)^n}{\left(1+\sqrt{2}\right)^{n-1} - \left(1-\sqrt{2}\right)^{n-1}} \\ &= \frac{1-\left(\dfrac{1-\sqrt{2}}{1+\sqrt{2}}\right)^n}{\dfrac{1}{1+\sqrt{2}} - \left(\dfrac{(1-\sqrt{2})^{n-1}}{(1+\sqrt{2})^n}\right)} \stackrel{n\to\infty}{\longrightarrow} \frac{1-0}{\dfrac{1}{1+\sqrt{2}}-0} = 1+\sqrt{2}\end{aligned}$$

20. Find the irreducible minimal polynomial for

$$\mathbb{Q} \subseteq \mathbb{Q}\left(\sqrt[3]{\frac{9+\sqrt{69}}{18}} + \sqrt[3]{\frac{9-\sqrt{69}}{18}}\right).$$

Solution: Set $a := \sqrt[3]{\dfrac{9+\sqrt{69}}{18}}$ and $b := \sqrt[3]{\dfrac{9-\sqrt{69}}{18}}$. Then

$$\begin{aligned}a^2b &= \sqrt[3]{\frac{(9+\sqrt{69})^2\cdot(9-\sqrt{69})}{18^3}} = \sqrt[3]{\frac{12(9+\sqrt{69})}{18^3}} \\ ab^2 &= \sqrt[3]{\frac{12(9-\sqrt{69})}{18^3}} \\ (a+b)^3 &= a^3+3a^2b+3ab^2+b^3 \\ &= 1 + \frac{\sqrt[3]{108+12\sqrt{69}}}{6} + \frac{\sqrt[3]{108-12\sqrt{69}}}{6} \\ &= 1 + \frac{\sqrt[3]{12}}{6}\left(\sqrt[3]{9+\sqrt{69}} + \sqrt[3]{9-\sqrt{69}}\right) \\ &= 1 + \sqrt[3]{\frac{1}{18}}\left(\sqrt[3]{9+\sqrt{69}} + \sqrt[3]{9-\sqrt{69}}\right) \\ &= 1+a+b\end{aligned}$$

and the minimal polynomial is therefore $x^3-x-1 \in \mathbb{Q}[x]$.

$\psi := \sqrt[3]{\dfrac{9+\sqrt{69}}{18}} + \sqrt[3]{\dfrac{9-\sqrt{69}}{18}}$ is called **plastic number**. The designation plastic number is misleading and does not correspond to van der Laan's intention, because not the material plastic, but the spatial extent (in architecture) was decisive for the name "plastic". The other two solutions of $x^3 - x - 1 = 0$ are

$$-\frac{\psi}{2} \pm i\sqrt{\frac{3-\psi}{4\psi}}$$

which can be proven by long division and Vieta's formula. ψ is the limit of the Padovan sequence, which is defined by

$$P_n := P_{n-2} + P_{n-3}\,,\; P_0 = P_1 = P_2 = 1$$

One can prove that

$$\psi = \sqrt[3]{1+\sqrt[3]{1+\sqrt[3]{1+\ldots}}} \approx 1.324717957244746025960908854\ldots$$

21. Show that the embedding $\mathbb{S}^1 \longrightarrow \mathbb{R}^2 - \{0\}$ is a homotopy equivalence, and that $\mathbb{R} \longrightarrow \mathbb{R}^2 - \{0\}$ defined by $x \mapsto (x, 1)$ is none.

    Solution: The homotopy inverse to $\mathbb{S}^1 \subseteq_\iota \mathbb{R}^2 - \{0\}$ is

    $$r\,:\,\mathbb{R}^2 - \{0\} \longrightarrow \mathbb{S}^1\,,\; x \longmapsto \frac{x}{\|x\|}$$

    so $r \circ \iota = id_{\mathbb{S}^1}$ and $\iota \circ r$ is homotope to the identity by

    $$H(x,t) := (1-t)\frac{x}{\|x\|} + tx\,.$$

    A homotopy equivalence induces an isomorphism of the fundamental groups. Now $\pi_1(\mathbb{R}^2 - \{0\}) = \pi_1(\mathbb{S}^1) = \mathbb{Z}$ while $\pi_1(\mathbb{R}) = \{1\}$, so $\mathbb{R}$ and $\mathbb{R}^2 - \{0\}$ cannot be homotopy equivalent.

22. Let $\emptyset \neq X$ be a set, $\mathcal{P}(X)$ its power set. Consider the following mappings

    $$\begin{aligned} f\,:\,X &\longrightarrow \mathcal{P}(X)\\ x &\longmapsto \{x\}\\[1ex] g\,:\,\mathcal{P}(X)\times\mathcal{P}(X) &\longrightarrow \mathcal{P}(X)\\ (A,B) &\longmapsto A\cup B \end{aligned}$$

    and decide whether they are injective, surjective, and calculate the fiber (pre-image) of the empty set.

Solution: f is injective because $f(x) = \{x\} = \{y\} = f(y)$ implies $x = y$. f is not surjective since $\emptyset \notin f(X)$. In particular $f^{-1}(\emptyset) = \emptyset$.

Let $x \in X$. Then

$$g((\{x\}, \emptyset)) = \{x\} \cup \emptyset = \{x\} = \emptyset \cup \{x\} = g((\emptyset, \{x\}))$$

which shows that g is not injective. However, g is surjective since $g((A, \emptyset)) = A \cup \emptyset = A$ for any $A \subseteq X$. The fiber of the empty set is $g^{-1}(\emptyset) = \{(\emptyset, \emptyset)\}$.

23. Find the smallest positive integer x that solves

$$\begin{aligned} x &\equiv 2 \mod 3 \\ x &\equiv 3 \mod 4 \\ x &\equiv 2 \mod 5 \end{aligned}$$

Solution: There is a solution x since $3, 4, 5$ are pairwise coprime by the Chinese remainder theorem, and all solutions are congruent modulo $M = 3 \cdot 4 \cdot 5 = 60$. The calculation is

$$\begin{aligned} 7 \cdot 3 + (-1) \cdot \frac{M}{3} &= 1 \Longrightarrow \alpha_1 = -20 \\ 4 \cdot 4 + (-1) \cdot \frac{M}{4} &= 1 \Longrightarrow \alpha_2 = -15 \\ 5 \cdot 5 + (-2) \cdot \frac{M}{5} &= 1 \Longrightarrow \alpha_3 = -24 \end{aligned}$$

which results in

$$x = 2 \cdot \alpha_1 + 3 \cdot \alpha_2 + 2 \cdot \alpha_3 = -133 \equiv 47 \mod M.$$

24. Let $\vec{u}, \vec{v}, \vec{w}$ be three different coplanar vectors of equal length, originating at a point O. Their endpoints define a triangle $\triangle UVW$. How can the barycenter S be found?

Solution: Let H be the point in which the heights intersect. $O = C$ is the circumcenter C per construction. Hence $\vec{OH} = \vec{u} + \vec{v} + \vec{w}$ by Sylvester's triangle theorem. On the other hand are O and H on the Euler straight of the triangle, and the Euler identity says $3\vec{S} = \vec{H} + 2\vec{C}$. Thus $3\vec{OS} = \vec{OH} + 2\vec{OC} = \vec{OH} = \vec{u} + \vec{v} + \vec{w}$ or $\vec{OS} = \frac{1}{3}(\vec{u} + \vec{v} + \vec{w})$.

25. Is a partially differentiable function $f : \mathbb{R}^2 \to \mathbb{R}$ at some point x_0 also continuous at x_0?

Solution: The answer is no because partial differentials are only the directional differentials in coordinate direction. There is no information about any other direction.

Consider $x_0 = (0,0)$ and $f : \mathbb{R}^2 \longrightarrow \mathbb{R}$ defined as

$$f(x,y) := \begin{cases} 0, & \text{if } x = 0 \text{ or } y = 0 \\ 1, & \text{otherwise} \end{cases}$$

Then

$$\lim_{h\to 0} \frac{f(0+h,0)-f(0,0)}{h} = \lim_{h\to 0} \frac{0-0}{h} = 0 \Longrightarrow \partial_x f(0,0) = 0$$

and the same is obviously true for the symmetric case $\partial_y f(0,0) = 0$. Thus f is partially differentiable at x_0 but not continuous, e.g.

$$\lim_{n\to\infty} f\left(\frac{1}{n}, \frac{1}{n}\right) = \lim_{n\to\infty} 1 \neq 0 = f(0,0) = f(x_0)\,.$$

26. Let $\mathfrak{g}$ be the real Lie algebra generated by

$$A_1 = \begin{bmatrix} 0 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & -1 \end{bmatrix},\ A_2 = \begin{bmatrix} 0 & 0 & 1 \\ -1 & 0 & 0 \\ 0 & 0 & 0 \end{bmatrix},\ A_3 = \begin{bmatrix} 0 & 1 & 0 \\ 0 & 0 & 0 \\ -1 & 0 & 0 \end{bmatrix}$$

Calculate its center $\mathfrak{Z}(\mathfrak{g}) = \{X \mid [A_i, X] = 0\,(i = 1,2,3)\}$, its commutator subalgebra $[\mathfrak{g},\mathfrak{g}]$, and a Cartan subalgebra $\mathfrak{h}$.

Solution: We observe that

$$\mathfrak{g} = \left\{ X = \sum_{i=1}^{3} x_i A_i \,\middle|\, \beta(X.v, w) + \beta(v, X.w) = 0 \text{ for all } v, w \in \mathbb{R}^3 \right\}$$

with respect to the bilinear form $\begin{bmatrix} 1 & 0 & 0 \\ 0 & 0 & 1 \\ 0 & 1 & 0 \end{bmatrix}$, i.e. $\mathfrak{g} \cong \mathfrak{so}(3)$. Therefore $\mathfrak{g}$ is simple, which implies that $\mathfrak{Z}(\mathfrak{g}) = \{0\}$, and $[\mathfrak{g},\mathfrak{g}] = \mathfrak{g}$. Since $\dim \mathfrak{g} = 3$ we have $\dim \mathfrak{h} = 1$, which is Abelian and thus nilpotent. We claim that $\mathfrak{h} = \mathbb{R} \cdot A_1$. It remains to show that $\mathfrak{h}$ is self-normalizing. Say $\sum_{i=1}^{3} x_i A_i \in N_{\mathfrak{g}}(A_1)$, i.e.

$$\begin{aligned} \mathfrak{h} \ni [X, A_1] &= x_2[A_2, A_1] + x_3[A_3, A_1] \\ &= x_2[e_{13} - e_{21}, e_{22} - e_{33}] + x_3[e_{12} - e_{31}, e_{22} - e_{33}] \\ &= x_2 e_{21} - x_2 e_{13} + x_3 e_{12} - x_3 e_{31} \\ &= -x_2 A_2 + x_3 A_3 \in \mathfrak{h} = \mathbb{R} \cdot A_1 \end{aligned}$$

where e_{ij} are the matrices with 1 at position (i,j) and 0 elsewhere. It follows $x_2 = x_3 = 0$ and $X \in \mathfrak{h}$, hence $\mathfrak{h}$ is self-normalizing.

27. Let $f : [a,b] \longrightarrow \mathbb{R}$ be a continuous function and $g : [a,b] \longrightarrow \mathbb{R}$ integrable with $g(x) \geq 0$ for all $x \in [a,b]$. Then there is a $\xi \in [a,b]$ such that
$$\int_a^b f(x)g(x)\,dx = f(\xi)\int_a^b g(x)\,dx$$
Solution: f assumes its minimum m and its maximum M on $[a,b]$ since f is continuous. Thus $mg(x) \leq f(x)g(x) \leq Mg(x)$ and by monotony and linearity of the Riemann integral
$$m\int_a^b g(x)\,dx \leq \int_a^b f(x)g(x)\,dx \leq M\int_a^b g(x)\,dx\,.$$
If $\int_a^b g(x)\,dx \neq 0$ then we have fo find $\xi \in [a,b]$ such that
$$f(\xi) = \frac{1}{\int_a^b g(x)\,dx}\int_a^b f(x)g(x)\,dx$$
With $g(x) \geq 0$ we have $\int_a^b g(x)\,dx > 0$ and
$$m = f(x_0) \leq \frac{1}{\int_a^b g(x)\,dx}\int_a^b f(x)g(x)\,dx \leq f(x_1) = M$$
and the intermediate value theorem for continuous functions applies, i.e. there is a $\xi \in [x_0, x_1] \subseteq [a,b]$ with the required property.
If $\int_a^b g(x)\,dx = 0$, then
$$0 = m\int_a^b g(x)\,dx \leq \int_a^b f(x)g(x)\,dx \leq M\int_a^b g(x)\,dx = 0$$
and each element of $\xi \in [a,b]$ satisfies
$$0 = \int_a^b f(x)g(x)\,dx = f(\xi)\int_a^b g(x)\,dx$$

28. Consider the circle segment above $A = (-1,0)$ and $B = (1,0)$ of
$$x^2 + \left(y + \frac{1}{\sqrt{3}}\right)^2 = \frac{4}{3}\,.$$

The point $P := \left(\dfrac{1}{\sqrt{3}}, 1-\dfrac{1}{\sqrt{3}}\right)$ lies on this segment. Calculate the height h of the circle segment, and $|AP|+|PB|$.

Solution: Set $C := (0,-\sqrt{3})$. Then $\triangle ABC$ is an equilateral triangle with side length 2. By van Schooten's theorem (a corollary of Ptolemy's theorem for concyclic quadrilaterals) we get $|AP|+|PB| = |PC|$. On the other hand

$$\begin{aligned}|PC| &= |\vec{PC}| = |\vec{PO}+\vec{OC}| = |\vec{OC}-\vec{OP}| \\ &= \left\| \begin{pmatrix} 0 \\ -\sqrt{3}\end{pmatrix} - \begin{bmatrix} 1/\sqrt{3} \\ 1-(1/\sqrt{3})\end{bmatrix} \right\| \\ &= \sqrt{\frac{1}{3}+\left(-\frac{3}{\sqrt{3}}-1+\frac{1}{\sqrt{3}}\right)^2} \\ &= \sqrt{\frac{8+4\sqrt{3}}{3}} \approx 2.231\end{aligned}$$

The height of the segment is the diameter of the circumscribed circle minus the height of equilateral $\triangle ABC$, or the $y-$coordinate of the circle at $x=0$, i.e.

$$h = \frac{4}{\sqrt{3}} - \sqrt{3} = \frac{1}{\sqrt{3}}\,.$$

29. Let $\varphi : V \longrightarrow V$ a linear mapping. Prove

$$\ker(\varphi)\cap\operatorname{im}(\varphi) = \{0\} \Longleftrightarrow \ker(\varphi\circ\varphi) = \ker(\varphi)$$

Solution: $\ker(\varphi) \subseteq \ker(\varphi\circ\varphi)$ is always true since $\varphi(0)=0$. Let $v\in\ker(\varphi\circ\varphi)$, so $\varphi(v)\in\operatorname{im}(\varphi)\cap\ker$. Hence if that intersection equals $\{0\}$, then $\ker(\varphi\circ\varphi)\subseteq\ker(\varphi)$.

Now assume $\ker(\varphi\circ\varphi)=\ker(\varphi)$ and $v\in\operatorname{im}(\varphi)\cap\ker(\varphi)=\{0\}$. Then there is a $w\in V$ such that $\varphi(w)=v$ and $\varphi(v)=0$ and $(\varphi\circ\varphi)(w)=0$. This means that $w\in\ker(\varphi)$ by assumption, i.e. $v=\varphi(w)=0$, so $\operatorname{im}(\varphi)\cap\ker(\varphi)=\{0\}$.

30. Let A by a cylindric surface (without base or cover) that rotates around the z-axis and stands on the plane $\{z=0\}$, with radius $R>0$ and height $h>0$. Give a parameterization and calculate the surface integral

$$\int_A \langle F,n\rangle\, d^2r$$

for the vector field $F : \mathbb{R}^3 \to \mathbb{R}^3$ defined by $F(x,y,z) = (xz, yz, 123)$.

Solution: One possible parameterization is

$$\begin{aligned} \phi \,:\, [0,2\pi) \times [0,h] &\longrightarrow A \\ (\varphi, z) &\longmapsto (R\cos\varphi, R\sin\varphi, z) \end{aligned}$$

The height of the cylinder is given by z, and for a fixed z we have a circle parallel to the plane $z=0$ described by polar coordinates. ϕ is a bijection because every point on A has exactly one pair of parameters (ϕ, z).

We use this parameterization ϕ to calculate the surface integral.

$$\begin{aligned} \int_A \langle F, n\rangle \, d^2r &= \int_0^{2\pi}\int_0^h \langle F\circ\phi, n\rangle \, \|\partial_\varphi\phi \times \partial_z\phi\| \, dz\, d\varphi \\ &= \int_0^{2\pi}\int_0^h \langle F\circ\phi, \partial_\varphi\phi \times \partial_z\phi\rangle \; dz\, d\varphi \\ &= \int_0^{2\pi}\int_0^h \langle \begin{pmatrix} zR\cos\varphi \\ zR\sin\varphi \\ 123 \end{pmatrix}, \begin{pmatrix} R\cos\varphi \\ R\sin\varphi \\ 0 \end{pmatrix}\rangle \; dz\, d\varphi \\ &= \int_0^{2\pi}\int_0^h zR^2\left(\cos^2\varphi + \sin^2\varphi\right)\; dz\, d\varphi \\ &= \int_0^{2\pi}\int_0^h zR^2 \, dz\, d\varphi = 2\pi R^2 \left[\frac{z^2}{2}\right]_{z=0}^{z=h} = h^2\pi R^2 \end{aligned}$$

We could alternatively use Gauß's divergence theorem. This uses closed surfaces, so we have to consider base and cover. Let C be the volume of the cylinder, D_1 its base, and D_2 its cover. Then $\partial Z = A \cup D_1 \cup D_2$. Note that the two integrals over D_1 and D_2 cancel each other since the normal vectors n are parallel to the z-axis, but pointing into opposite directions, and the third component of F is constant.

$$\begin{aligned} \int_{D_1}\langle F, n\rangle \, d^2r + \int_{D_2}\langle F, n\rangle \, d^2r &= \int_{D_1}\langle F, \begin{pmatrix} 0\\0\\1 \end{pmatrix}\rangle \, d^2r + \int_{D_2}\langle F, \begin{pmatrix} 0\\0\\-1 \end{pmatrix}\rangle \, d^2r \\ &= \int_{D_1} 123\, d^2r + \int_{D_2} -123\, d^2r \\ &= 123(\pi R^2 - \pi R^2) = 0 \end{aligned}$$

Therefore

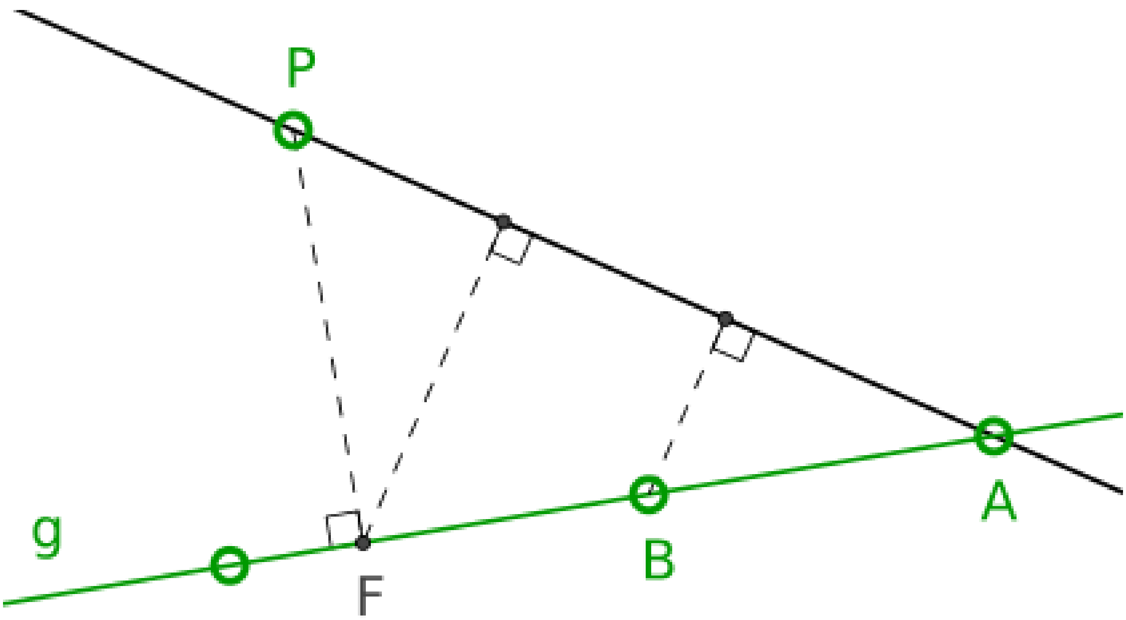
$$\int_{\partial Z}\langle F, n\rangle \, d^2r = \int_A \langle F, n\rangle \, d^2r + \int_{D_1}\langle F, n\rangle \, d^2r + \int_{D_2}\langle F, n\rangle \, d^2r = \int_A \langle F, n\rangle \, d^2r$$

Now we apply Gauß's divergence theorem

$$\begin{aligned}\int_{\partial Z} \langle F, n\rangle \, d^2r &= \int_Z \operatorname{div} F \, d^3r \\ &= \int_0^R \int_0^{2\pi} \int_0^h (\operatorname{div} F) \circ \phi \cdot |\det J_\phi| \, dz \, d\varphi \, d\rho \\ &= \int_0^R \int_0^{2\pi} \int_0^h 2z\rho \, dz \, d\varphi \, d\rho \\ &= 2 \cdot \frac{R^2}{2} \cdot \frac{h^2}{2} \cdot 2\pi = h^2 \pi R^2\end{aligned}$$

31. Let $\mathcal{P}$ be a finite set of points in a plane, that are not all collinear. Then there is a straight, that contains exactly two points.

    Solution: We consider the pairs (g, P) of a straight g through two points of $\mathcal{P}$ and a point $P \in \mathcal{P} - \{g\}$. Those points exist since not all points are collinear. The number of such pairs is finite because $\mathcal{P}$ is. Hence there is a pair (g, P), such that distance $\operatorname{dist}(g, P)$ is minimal. It remains to show that g doesn't contain a third point from $\mathcal{P}$.



`https://commons.wikimedia.org/wiki/File:Tibor_gallai_proof.svg`

Assume there are three such points. Let F be the basis point of the (minimal) perpendicular from P on g. Now there have to be two points

$A, B \in \mathcal{P}$ which lie on the same side of F by the pigeonhole principle. Say B is closer to F than P. Thus the distance $\operatorname{dist}(\overline{AP}, B)$ of B to the straight through A and P is smaller than the distance $\operatorname{dist}(g, P)$, which is as height in the right triangle $\triangle(APF)$ smaller than the cathetus $\overline{PF}$.

However, this contradicts the choice of the pair (g, P) as minimal distance $\operatorname{dist}(g, P)$, and our assumption that $\mathcal{P} \cap \{g\}$ contains three points.

2 November 2021

1. (a) Let $C \subseteq \mathbb{R}^n$ be compact and $f : C \longrightarrow \mathbb{R}^n$ continuous and injective. Show that the inverse $g = f^{-1} : f(C) \longrightarrow \mathbb{R}^n$ is continuous.

   (b) Let $S := \{x + tv \,|\, t \in (0,1)\}$ with $x, v \in \mathbb{R}^n$, and $f \in C^0(\mathbb{R}^n)$ differentiable for all $y \in S$. Show that there is a $z \in S$ such that
$$f(x+v) - f(x) = \nabla f(z) \cdot v\,.$$

   (c) Let $\gamma : [0,\pi] \longrightarrow \mathbb{R}^3$ be given as
$$\gamma(t) := \begin{pmatrix} \cos(t)\sin(t) \\ \sin^2(t) \\ \cos(t) \end{pmatrix}\,,\, t \in [0,\pi].$$
   Show that the length $L(\gamma) > \pi$.

   Reason: Calculus.

   Solution:

   (a) Let $(y_k)_{k\in\mathbb{N}} \subseteq f(C)$ a sequence such that $\lim_{k\to\infty} y_k = y \in f(C)$. There is a unique sequence $(x_k)_{k\in\mathbb{N}} \subseteq C$ and $x \in C$ such that
$$f(x_k) = y_k \;(k \in \mathbb{N}) \;\wedge\; f(x) = y$$
   since f is injective. Assume g is not continuous. Then there is a $\varepsilon > 0$ and a subsequence $(y_{k_m})_{m\in\mathbb{N}} \subseteq (y_k)_{k\in\mathbb{N}}$ with
$$|x_{k_m} - x| = |g(y_{k_m}) - g(y)| \geq \varepsilon \text{ for all } m \in \mathbb{N} \quad (*).$$
   Because C is compact, there is another convergent subsequence $(x_{k_j})_{j\in\mathbb{N}} \subseteq (x_k)_{k\in\mathbb{N}}$ with $\lim_{j\to\infty} x_{k_j} = \tilde{x}$. By continuity of f follows
$$y = \lim_{j\to\infty} y_{k_j} = \lim_{j\to\infty} f(x_{k_j}) = f(\tilde{x}),$$
   hence $f(x) = f(\tilde{x})$ and so $x = \tilde{x}$. In particular $\lim_{j\to\infty} x_{k_j} = x$ contradicting $(*)$.

   (b) Define $g : [0,1] \longrightarrow \mathbb{R}$ by
$$g(t) := f(x + tv)\,,\, t \in [0,1]$$
   Then g is continuous on $[0,1]$ and by assumption differentiable on $(0,1)$. Moreover $g(0) = f(x)$ and $g(1) = f(x+v)$. We get with the chain rule
$$g'(t) = \nabla f(x + tv) \cdot v \text{ for all } t \in (0,1)$$

and with the mean value theorem a $\tau \in (0,1)$ such that

$$g'(\tau) = \frac{g(1)-g(0)}{1-0} = \nabla f(x+\tau v)\cdot v = f(x) - f(x+v)$$

which had to be shown if we set $z := x + \tau v$.

(c)

$$\begin{aligned}
|\gamma'(t)| &= \left| \begin{pmatrix} -\sin^2(t)+\cos^2(t) \\ 2\sin(t)\cos(t) \\ -\sin(t) \end{pmatrix} \right| \\
&= \sqrt{(\cos^2(t)-\sin^2(t))^2 + 4\sin^2(t)\cos^2(t) + \sin^2(t)} \\
&= \sqrt{\cos^4(t) + 2\sin^2(t)\cos^2(t) + \sin^4(t) + \sin^2(t)} \\
&= \sqrt{(\cos^2(t)+\sin^2(t))^2 + \sin^2(t)} = \sqrt{1+\sin^2(t)} \geq 1
\end{aligned}$$

and in particular $|\gamma'(t)| > 1$ for $t \in (0,\pi)$. Hence

$$L(\gamma) = \int_0^\pi |\gamma'(t)|\,dt > \int_0^\pi dt = \pi\,.$$

2. Let g, h be two skew lines in a three-dimensional projective space $\mathcal{P} = \mathcal{P}(V)$, and P a point that is neither on g nor on h. Prove that there is exactly one straight through P that intersects g and h.

   Reason: Projective Geometry.

   Solution: The plane $\{P, g\}$ has to intersect h in a point Q for dimensional reasons. The straight $\{P, Q\}$ contains P, and intersects g and h because g and $\{P, Q\}$ are contained in a projective plane. This proves existence.

   Assume there were two transverse straights h_1, h_2 through P which both intersect g and h. Then $g \cap h_1 \neq g \cap h_2$ and $h \cap h_1 \neq h \cap h_2$ since $h_1 \neq h_2$. This means that the plane $\{h_1, h_2\}$ contains both lines g, h. However, this implies that g and h intersect, as we are in a projective space, contradicting the assumption that g, h are skew lines.

3. Let $(\mathcal{A}, e)$ be a unital C^*-algebra. A self-adjoint element $a \in \mathcal{A}$ is called positive, if its spectral values are:

$$\sigma(a) := \{\lambda \in \mathbb{C} \mid a - \lambda e \text{ is not invertible }\} \subseteq \mathbb{R}^+ := [0,\infty).$$

The set of all positive elements is written $\mathcal{A}_+$. A linear functional $f\,:\,\mathcal{A}\longrightarrow\mathbb{C}$ is called positive, if $f(a)\in\mathbb{R}^+$ for all positive $a\in\mathcal{A}_+$.

Prove that a positive functional is continuous.

Reason: C^*-algebras.

Solution: Firstly, we want to show that f is bounded on

$$M:=\{a\in\mathcal{A}_+\,|\,0\leq a\leq e\}.$$

If this wasn't the case, then there would be a sequence $(x_n)_{n\in\mathbb{N}}\subseteq M$ such that $\lim_{n\to\infty}f(x_n)=\infty$. Let $(a_n)_{n\in\mathbb{N}}\subseteq\mathbb{R}^+$ be any sequence of l^1 and set $x:=\sum_{n=1}^\infty a_nx_n$. Note that the series converges absolutely.

$$\sum_{n=1}^m a_nx_n\leq x\Longrightarrow f\left(\sum_{n=1}^m a_nx_n\right)=\sum_{n=1}^m a_nf(x_n)\leq f(x)$$

Since $f(x_n)\geq 0$, $\sum_{n=1}^\infty a_nf(x_n)$ converges for any $(a_n)_{n\in\mathbb{N}}\in l^1$.

We can find a subsequence $(f(x_{n_k}))_{k\in\mathbb{N}}\subseteq(f(x_n))_{n\in\mathbb{N}}$ such that $f(x_{n_k})\geq 2^{n_k}$ because $f(x_n)\stackrel{n\to\infty}{\longrightarrow}\infty$. Define $a\in l^1$ by $a_{n_k}=2^{-n_k}$ and $a_n=0$ otherwise. Then $\sum_{k=1}^\infty a_{n_k}f(x_{n_k})$ diverges, a contradiction. There is therefore a constant $C>0$ such that $f(x)\leq C$ for all $x\in M$.

Let x be an arbitrary self-adjoint element with $\|x\|\leq 1$. Then $x=x_+-x_-$ with positive elements $x_+,x_-\in\mathcal{A}_+$. From $x_\pm\leq|x|\leq e$ follows $x_\pm\in M$ and so $|f(x)|\leq|f(x_+)|+|f(x_-)|\leq 2C$ (Gelfand-Neumark).

If finally $x\in\mathcal{A}$ is arbitrary with $\|x\|\leq 1$, then $\left\|\frac{1}{2}(x\pm x^*)\right\|\leq 1$ and

$$|f(x)|\leq\left|f\left(\frac{1}{2}(x+x^*)\right)\right|+\left|f\left(\frac{1}{2}(x-x^*)\right)\right|\leq 4C$$

hence f is bounded with $\|f\|\leq 4C$ and therewith continuous.

4. Prove that the following groups F_1,F_2 are free groups:

   (a) Consider the functions α,β on $\mathbb{C}\cup\{\infty\}$ defined by the rules

   $$\alpha(x)=x+2\text{ and }\beta(x)=\frac{x}{2x+1}.$$

   The symbol ∞ is subject to such formal rules as $1/0=\infty$ and $\infty/\infty=1$. Then α,β are bijections with inverses

   $$\alpha^{-1}(x)=x-2\text{ and }\beta^{-1}(x)=\frac{x}{1-2x}.$$

   Thus α and β generate a group of permutations F_1 of $\mathbb{C}\cup\{\infty\}$.

(b) Define the group $F_2 := \langle A, B\rangle$ with

$$A := \begin{bmatrix} 1 & 2 \\ 0 & 1 \end{bmatrix} \text{ and } B := \begin{bmatrix} 1 & 0 \\ 2 & 1 \end{bmatrix}$$

Reason: Group Theory.

Solution: Let G be a group and $X \subseteq G$ a subset of G. Assume that each element $g \in G$ can be uniquely written in the form $g = x_1^{m_1} x_2^{m_2} \cdots x_s^{m_s}$ where $x_i \in X, s \geq 0, m_i \neq 0$, and $x_i \neq x_{i+1}$. Let F be the free group on X and $\sigma : X \to F$ the associated injection. By the mapping property of free groups, there is a homomorphism $\psi : F \to G$ such that $\psi \circ \sigma : X \to G$ is the inclusion map. Since $G = \langle X\rangle$, we see that ψ is surjective. It is injective by the uniqueness of the normal form. Thus $G \cong F$ is free over X.

(a) Observe that a nonzero power of α maps the interior of the unit circle $|z| = 1$ to the exterior and a nonzero power of β maps the exterior of the unit circle to the interior with 0 removed: the second statement is most easily understood from the equation $\beta(1/x) = 1/(x + 2)$. From this it is easy to see that no nontrivial reduced word in $\{\alpha, \beta\}$ can equal 1. Hence every element of F_1 has a unique expression as a reduced word. It follows from the above that F_1 is free on $\{\alpha, \beta\}$.

(b) Consider the linear fractional transformations ($ad - bc \neq 0$)

$$\begin{aligned} \lambda(a, b, c, d) \,:\, \mathbb{C} \cup \{\infty\} &\longrightarrow \mathbb{C} \cup \{\infty\} \\ x &\longmapsto \frac{ax + b}{cx + d} \end{aligned}$$

Now

$$\begin{bmatrix} a & b \\ c & d \end{bmatrix} \stackrel{\varphi}{\longmapsto} \lambda(a, b, c, d)$$

is a homomorphism from $\operatorname{GL}(2, \mathbb{C})$ to the group of all linear fractional transformations of $\mathbb{C} \cup \{\infty\}$ in which A maps to α and B maps to β. Since no nontrivial reduced word in $\{\alpha, \beta\}$ can equal 1, the same is true of reduced words in $\{A, B\}$. Consequently the group F_2 is free on $\{A, B\}$.

5. We model the move of a chess piece on a chessboard as timely homogeneous Markov chain with the 64 squares as state space and the position of the piece at a certain (discrete) point in time as state. The transition matrix is given by the assumption, that the next possible state

is equally probable. Determine whether these Markov chains M(piece) are irreducible and aperiodic for (a) king, (b) bishop, (c) pawn, and (d) knight.

Reason: Markov Processes.

Solution: The king can reach every position on the board from any position, i.e. M(king) is irreducible. For any square we have

$$d(s_k) = \operatorname{gcd}\{n \geq 1 \,|\, (P^n)_{k,k} > 0\} = 1$$

i.e. that each state has the period 1 because the king can always get back to its starting position within 2 or 3 moves, so the greatest common divisor of all possible periods is 1. Hence M(king) is aperiodic.

M(bishop) is reducible, since we cannot reach all squares from a given starting position. With the same argument as above, we see that M(bishop) is aperiodic.

M(pawn) is reducible, since we cannot reach all squares from a given starting position, and periodic with $d(s_k) = \infty$ for all k, because a pawn can never return to its starting position.

The knight can always reach all squares from any starting point, so M(knight) is irreducible. For any square we have

$$d(s_k) = \operatorname{gcd}\{n \geq 1 \,|\, (P^n)_{k,k} > 0\} = 2$$

for the greatest common divisor of all periods with positive probability to return to the starting point. So M(knight) is periodic with period 2. The knight can always return in two moves. Since it changes the color of the square with every move, a returning path must always be of an even number of moves.

Summary:

piece	*king*	*bishop*	*pawn*	*knight*
irreducibility	1	0	0	1
period	1	1	∞	2

6. Prove that a n-dimensional manifold X is orientable if and only if
   (a) there is an atlas for which all chart changes respect orientation, i.e. have a positive functional determinant.
   (b) there is a continuous n-form which nowhere vanishes on M.

Reason: Manifolds.

Solution: Orientations of a vector space are elements from either of the two possible equivalence classes of ordered bases, i.e. $\det T \gtrless 0$ where T is the transformation matrix between bases.

An orientation μ of M is a choice of orientations μ_x for every tangent space $T_x(M)$, such that for all $x_0 \in M$ there is an open neighborhood $x_0 \in U \subseteq M$ and differentiable vector fields $\xi_1, \ldots, \xi_n$ on U with

$$[(\xi_1)_x, \ldots, (\xi_n)_x] = \mu_x$$

for all $x \in U$. The manifold M is called orientable, if an orientation for M can be chosen.

Let μ be an orientation on M. A chart (U, φ) with coordinates $x_1, \ldots, x_n$ is called positive oriented, if for all $x \in U$

$$\left[\left.\frac{\partial}{\partial x_1}\right|_x, \ldots, \left.\frac{\partial}{\partial x_n}\right|_x \right] = \mu_x$$

(a) If there is an orientation of X, we can find an atlas, that only contains positive oriented charts. Then all charts (U, φ) with $x \in U$ induce the same orientation on $T_x(M)$, hence they must have a positive functional determinant.

Let conversely be $(U_\alpha, \varphi_\alpha)$ an atlas of M, with positive functional determinant, i.e. $\det D(\varphi_\alpha \circ \varphi_\beta^{-1}) > 0$ on $\varphi_\beta(U_\alpha \cap U_\beta)$. Then all charts $(U_\alpha, \varphi_\alpha)$ with $x \in U_\alpha$ of $T_x(M)$ have the same orientation μ_x. Thus $\mu : x \longmapsto \mu_x$ defines an orientation on M because it is determined by an n-tuple of differential vector fields in a neighborhood of $x \in M$ for every chart.

(b) Let ω_0 be a nowhere vanishing n-form on M, and $(U_\iota, \varphi_\iota)_{\iota \in I}$ an atlas of M. Then there are nowhere vanishing continuous functions h_ι on $B_\iota := \varphi_\iota(U_\iota)$ for every $\iota \in I$, such that

$$(\omega_0)_\iota = h_\iota dx^1 \wedge \ldots \wedge dx^n.$$

We may assume that $h_\iota > 0$ on B_ι by changing the coordinate x^n to x^{-n} if necessary. Hence

$$\begin{aligned} h_\kappa dx^1 \wedge \ldots \wedge dx^n &= (\omega_0)_\kappa \\ &= \det\left(D\left(\varphi_\iota \circ \varphi_\kappa^{-1}\right)\right)(\omega_0)_\iota \\ &= \det\left(D\left(\varphi_\iota \circ \varphi_\kappa^{-1}\right)\right) \cdot h_\iota dx^1 \wedge \ldots \wedge dx^n \end{aligned}$$

Thus $\det\left(D\left(\varphi_\iota \circ \varphi_\kappa^{-1}\right)\right) > 0$, and the atlas is oriented.

Let M conversely be oriented with an oriented atlas (U_ι, φ_ι). Moreover let $(f_\iota)_{\iota \in I}$ a partition of unity for the cover $(U_\iota)_{\iota \in I}$. Then $dx^1 \wedge \ldots \wedge dx^n$ induces a n-form ω_ι on U_ι for every $\iota \in I$. We have $\omega_\iota = d_{\iota\kappa} \cdot \omega_\kappa$ with

$$d_{\iota\kappa} = \left(D\left(\varphi_\iota \circ \varphi_\kappa^{-1}\right)\right) \circ \varphi_\kappa > 0$$

on $U_\iota \cap U_\kappa$. The form $f_\iota \cdot \omega_\iota$ is a n-form on M with compact support $\operatorname{supp}(f_\iota \cdot \omega_\iota) \subseteq U_\iota$. We define $\omega_0 := \sum_{\iota \in I} f_\iota \cdot \omega_\iota$. Let $x \in M$, I_0 the finite set of all $\iota \in I$ with $x \in \operatorname{supp}(f_\iota)$ and $\kappa \in I_0$. Then

$$\begin{aligned}(\omega_0)_x &= \sum_{\iota \in I_0} f_\iota(x) \cdot (\omega_\iota)_x \\ &= \left(\sum_{\iota \in I_0} f_\iota(x) d_{\iota\kappa}(x)\right) \cdot (\omega_\kappa)_x\end{aligned}$$

From $f_\iota(x) > 0$, $\sum_{\iota \in I_0} f_\iota(x) = 1$, and $d_{\iota\kappa} > 0$, we get $(\omega_0)_x \neq 0$.

7. A topological vector space E over $\mathbb{K} \in \{\mathbb{R}, \mathbb{C}\}$ is normable if and only if it is Hausdorff and possesses a bounded convex neighborhood of $\vec{0}$.

   Reason: Kolmogorov's Theorem.

   Solution: If E is normable, and if $x \mapsto \|x\|$ is a norm on E that generates te topology, then $U := \{x \,:\, \|x\| \leq 1\}$ is a bounded and convex neighborhood of $\vec{0}$. As a metrizable space, E is also Hausdorff.

   Conversely, suppose E is a topological vector space, Hausdorff, and possessing a bounded convex neighborhood $\vec{0} \in U$. Let $V \subseteq U$ be a balanced neighborhood of $\vec{0}$, i.e. $\lambda V \subseteq V \subseteq U$ for all $|\lambda| \leq 1$. Then for the convex hulls holds $\operatorname{conv}(V) \subseteq \operatorname{conv}(U) = U$, where $\operatorname{conv}(V)$ is a balanced convex neighborhood of $\vec{0}$. As any subset of a bounded set is bounded, we may assume (possibly by replacing U with $\operatorname{conv}(V)$) that U is a bounded, convex, balanced neighborhood of $\vec{0}$. For $x \neq \vec{0}$, we define

   $$A(x) := \{\lambda \in \mathbb{K} \,:\, x \notin \lambda U\} \ni 0\,,\; A(\vec{0}) := \{0\}.$$

   If $x \in E - \{\vec{0}\}$, we assert that $A(x)$ contains nonzero scalars. Indeed, if $\vec{0} \in V$ is a neighborhood, $x \notin V$, and $\alpha \in \mathbb{K} - \{0\}$ such that $U \subseteq \alpha V$ (U is bounded), then $\alpha^{-1} U \subseteq V$, i.e. $x \notin \alpha^{-1} U$, hence $\alpha^{-1} \in A(x)$.

   We define now $x \longmapsto \|x\|$ for all $x \in E$ by the formula

   $$\|x\| := \sup\{|\lambda| \,:\, \lambda \in A(x)\}.$$

Clearly $\|\vec{0}\| = 0$, $\|x\| > 0$ whenever $x \neq \vec{0}$, and $A(\mu x) = \mu A(x)$, i.e. $\|\mu x\| = |\mu| \cdot \|x\|$. To show that $x \longmapsto \|x\|$ is a norm, it remains to verify that $\|x\| < \infty$ and that the triangle inequality holds.

We first show that

$$\{\lambda \,:\, |\lambda| < \|x\|\} \subseteq A(x) \qquad (*)$$

If $x = \vec{0}$ then the left side of $(*)$ is empty. Assume $x \neq \vec{0}$, and suppose $|\lambda| < \|x\|$. Since $0 \in A(x)$ we can suppose $0 < |\lambda| < \|x\|$. Then, by definition of $\|x\|$, there exists a $\mu \in A(x)$ such that $0 < |\lambda| < |\mu| \leq \|x\|$. So $x \notin \mu U$, and since U is balanced, $\lambda U \subseteq \mu U$, i.e. $x \notin \lambda U$ or $\lambda \in A(x)$, which proves $(*)$.

Let $x \in E$. We claim that $\|x\| < \infty$. As $\lambda \mapsto \lambda x$ is continuous at $\lambda = 0$, and since $0 \cdot x = \vec{0}$, there exists an $\varepsilon > 0$ such that $\lambda x \in U$ whenever $|\lambda| \leq \varepsilon$, i.e. U is absorbent. Thus $1 \notin A(\lambda x)$ and by $(*)$ we have $1 \geq \|\lambda x\| = |\lambda| \cdot \|x\|$, which implies $\|x\| < \infty$.

Let $x, y \in E$. We claim that $\|x+y\| \leq \|x\| + \|y\|$. We may assume that $x, y, x+y \neq \vec{0}$. Given any $\varepsilon > 0$, it will suffice to show that

$$\|x+y\| \leq \|x\| + \|y\| + 2\varepsilon.$$

Let $\alpha := \|x\| + \varepsilon > \|x\|$ and $\beta := \|y\| + \varepsilon > \|y\|$. This means that $\alpha \notin A(x)$ and $\beta \notin A(y)$ by the definition of $\|x\|$, i.e. $x \in \alpha U$ and $y \in \beta U$. As U is convex, it follows that

$$x + y \in \alpha U + \beta U = (\alpha + \beta)U,$$

and thus $\alpha + \beta \notin A(x+y)$, and with $(*)$ that

$$\alpha + \beta = \|x\| + \|y\| + 2\varepsilon \geq \|x+y\|$$

and the triangle inequality holds.

Summarizing, $x \longmapsto \|x\|$ is a norm on E. It remains to show that this norm topology coincides with the given topology. Since both are compatible with the additive group structure, it is sufficient to verify that their neighborhood system at $\vec{0}$ coincide.

Suppose V is any neighborhood of $\vec{0}$ for the given topology. Choose a nonzero scalar λ such that $U \subseteq \lambda V$. If $\|x\| < |\lambda|^{-1}$ then $\lambda^{-1} \notin A(x)$ by the definition of $\|x\|$, i.e. $x \in \lambda^{-1} U \subseteq V$. Thus

$$\{x \,:\, \|x\| < \lambda^{-1}\} \subseteq V$$

which shows that V is a neighborhood of $\vec{0}$ for the norm topology.

Conversely, let V be any neighborhood of $\vec{0}$ for the norm topology. Choose $\varepsilon > 0$ so that $\{x : \|x\| \leq \varepsilon\} \subseteq V$. If $x \in \varepsilon U$, then $\varepsilon \notin A(x)$, therefore $\|x\| \leq \varepsilon$ by $(*)$, hence $\varepsilon U \subseteq V$. Since εU is a neighborhood of $\vec{0}$ for the given topology, so is V.

8. (a) Determine the minimal polynomial of $\pi + e \cdot i$ over the reals.
   (b) Show that $\mathbb{F} := \mathbb{F}_7[T]/(T^3 - 2)$ is a field, and calculate the number of its elements, $(T^2 + 2T + 4)(2T^2 + 5)$, and $(T + 1)^{-1}$.
   (c) Consider $P(X) := X^{7129} + 105X^{103} + 15X + 45 \in \mathbb{F}[X]$ and determine whether it is irreducible in case
$$\mathbb{F} \in \{\mathbb{Q}, \mathbb{R}, \mathbb{F}_2, \mathbb{Q}[T]/(T^{7129} + 105T^{103} + 15T + 45)\}$$
   (d) Determine the matrix of the Frobenius endomorphism in $\mathbb{F}_{25}$ for a suitable basis.

Reason: Galois Theory.

Solution:

(a) $(\pi + e \cdot i)(\pi - e \cdot i) = \pi^2 + e^2 \in \mathbb{R}$ and $(\pi + e \cdot i) + (\pi - e \cdot i) = 2\pi \in \mathbb{R}$ so we get by Vieta's formulas $X^2 - 2\pi X + \pi^2 + e^2 \in \mathbb{R}[X]$.

(b) We have
$$\{a^3 \mid a \in \mathbb{F}_7\} = \{0, 1, 6\} \not\ni 2$$
so $T^3 - 2$ has no roots in $\mathbb{F}_7$ and is thus irreducible, i.e. $\mathbb{F}$ is a field. The equivalence classes of $1, T, T^2$ build a basis, hence $|\mathbb{F}| = |\mathbb{F}_7|^3 = 343$. Now
$$\begin{aligned}(T^2 + 2T + 4)(2T^2 + 5) &= 2T^4 + 4T^3 + 13T^2 + 10T + 20\\ &= 2T(T^3 - 2) + 4T + 4(T^3 - 2) + 8 + 13T^2 + 10T + 20\\ &= 13T^2 + 14T + 28\\ &= 6T^2\end{aligned}$$
Long division yields $(T^3 - 2) : (T + 1) = T^2 - T + 1$ remainder -3, i.e. $0 = T^3 - 2 = (T^2 + 6T + 1)(T + 1) - 3$ or $3 = (T^2 + 6T + 1)(T + 1)$. Now $3^{-1} = 5$ so we have $(T + 1)^{-1} = 5(T^2 + 6T + 1) = 5T^2 + 2T + 5$.

(c) We can use Eisenstein's criterion for $p = 5$ because
$$5|105\,,\ 5|15\,,\ 5|45\,,\ 25 \nmid 45\,,\ 5 \nmid 1$$

and conclude that $P(X)$ is irreducible over $\mathbb{Q}$.

$P(X) \in \mathbb{R}[X]$ is of odd degree and thus has a root in the real number field by the intermediate value theorem, so it cannot be irreducible.

The insertion homomorphism $X \mapsto 1$ on $\mathbb{F}_2[X]$ yields $P(1) = 166 \equiv 0 \mod 2$ so $P(X) \in \mathbb{F}_2[X]$ is reducible.

$\mathbb{F} = \mathbb{Q}[T]/(T^{7129} + 105T^{103} + 15T + 45)$ is a field. It t is the equivalence class of T then $P(t) = 0$ per construction, and $P(X) \in \mathbb{F}[X]$ is reducible.

(d) Because of

$$\{a^2 \,|\, a \in \mathbb{F}_5\} = \{0, 1, 4\} \not\ni 2$$

the polynomial $X^2 - 2 \in \mathbb{F}_5[X]$ is irreducible and

$$\mathbb{F}_{25} \cong \mathbb{F}_5[X]/(X^2 - 2)$$

so we may choose $1, x \subseteq \mathbb{F}_{25}$ as basis where x is the representative of the equivalence class of X. We have $1^5 = 1$ and $x^5 = x^2 \cdot x^2 \cdot x = 2 \cdot 2 \cdot x = 4x$. Hence the required matrix is

$$\begin{bmatrix} 1 & 0 \\ 0 & 4 \end{bmatrix}$$

9. Let V and W be finite-dimensional vector spaces over the field $\mathbb{F}$ and $f : V \otimes_{\mathbb{F}} W \longrightarrow \mathbb{F}$ a linear mapping such that

$$\forall\, v \in V - \{0\} \quad \exists\, w \in W \,:\, f(v \otimes w) \neq 0$$
$$\forall\, w \in W - \{0\} \quad \exists\, v \in V \,:\, f(v \otimes w) \neq 0$$

Show that $V \cong_{\mathbb{F}} W$.

Reason: Linear Algebra.

Solution: We get from the first condition that the mapping

$$V \longrightarrow \operatorname{Hom}_{\mathbb{F}}(W, \mathbb{F}) = W^*$$
$$v \longmapsto (w \longmapsto f(v \otimes w))$$

is injective. Since $\dim W < \infty$ we have

$$\dim_{\mathbb{F}} V \leq \dim_{\mathbb{F}} W^* = \dim_{\mathbb{F}} W.$$

The second condition yields by the analogue argument that $\dim_{\mathbb{F}} W \leq \dim_{\mathbb{F}} V$. Hence $\dim_{\mathbb{F}} V = \dim_{\mathbb{F}} W$ and $V \cong_{\mathbb{F}} W$.

10. Let $R := \mathbb{C}[X,Y]/(Y^2 - X^2)$. Describe $V_{\mathbb{R}}(Y^2 - X^2) \subseteq \mathbb{R}^2$, determine whether $\operatorname{Spec}(R)$ is finite, calculate the Krull-dimension of R, and determine whether R is Artinian.

    Reason: Commutative Algebra.

    Solution:

    (a) $V_{\mathbb{R}}(Y^2 - X^2)$ is the set of zeros of $Y^2 - X^2$, so

    $$\begin{aligned} V_{\mathbb{R}}(Y^2 - X^2) &= \{(x,y) \in \mathbb{R}^2 \mid y^2 - x^2 = 0\} \\ &= \{(x,y) \in \mathbb{R}^2 \mid y = x\} \cup \{(x,y) \in \mathbb{R}^2 \mid y = -x\} \end{aligned}$$

    and we get the diagonals in a Cartesian coordinate system.

    (b) $P_x := ([X - x], [Y - x]) \subseteq R$ is a prime ideal for every $x \in \mathbb{C}$ because

    $$R/P_x \cong_{\text{ring}} \mathbb{C}[X,Y]/(X - x, Y - x) \cong_{\text{ring}} \mathbb{C}$$

    is an integral domain. Furthermore, the well-defined insertion homomorphism $R \longrightarrow \mathbb{C}$ for $(x,x) \in \mathbb{C}^2$ shows that

    $$\forall\, x,y \in \mathbb{C} \,:\, x \neq y \Longrightarrow P_x \neq P_y\,.$$

    Therefore, $\operatorname{Spec}(R)$ cannot be finite.

    (c) Consider the canonical projection $\pi : \mathbb{C}[X,Y] \longrightarrow R$. Then

    $$\begin{aligned} \operatorname{Spec}(R) &\longrightarrow \{Q \in \operatorname{Spec}(\mathbb{C}[X,Y]) \mid (Y^2 - X^2) \subseteq Q\} \\ P &\longmapsto \pi^{-1}(P) \end{aligned}$$

    is bijective and compatible with inclusion of ideals. From

    $$(Y^2 - X^2) \subseteq (Y - X) \subsetneq (X,Y)$$

    we get $\dim R \geq 1$. Since $\dim \mathbb{C}[X,Y] = 2$, and $\{0\} \in \operatorname{Spec}(\mathbb{C}[X,Y])$ and $\{0\} \subsetneq (Y^2 - X^2)$ we conversely have $\dim R \leq 1$, hence $\dim R = 1$.

    (d) R is not Artinian because Artinian rings are zero-dimensional. Alternatively, we can also name a decreasing sequence of ideals, e.g. $(X^n)_{n\in\mathbb{N}}$, that doesn't become stationary.

11. (HS-1) Let $a \notin \{-1, 0, 1\}$ be a real number. Solve

    $$\frac{(x^4+1)(x^4+6x^2+1)}{x^2(x^2-1)^2} = \frac{(a^4+1)(a^4+6a^2+1)}{a^2(a^2-1)^2}\,.$$

Reason: Equation.

Solution: A solution x is a root of the polynomial

$$\begin{aligned}
P(x) :=\, & a^2(a^2-1)^2(x^4+1)(x^4+6x^2+1)\\
& -x^2(x^2-1)^2(a^4+1)(a^4+6a^2+1)\\
& = (a^6-2a^4+a^2)x^8-(a^8+14a^4+1)x^6+\\
& 2(a^8+7a^6+7a^2+1)x^4-(a^8+14a^4+1)x^2\\
& +a^6-2a^4+a^2\\
& = (x-a)(x+a)[(a^6-2a^4+a^2)x^6-(2a^6+13a^4+1)x^4\\
& +(a^6+13a^2+2)x^2+(-a^4+2a^2-1)]\\
& = a^2(x-a)(x+a)\left(x-\frac{1}{a}\right)\left(x+\frac{1}{a}\right)\cdot\\
& \cdot (a^4-2a^2+1)x^4-2(a^4+6a^2+1)x^2+(a^4-2a^2+1)
\end{aligned}$$

So $P(x)=0$ has the solutions $x=\pm a\,,\,\pm\dfrac{1}{a}$ and the solutions of

$$0 = x^4-2\frac{a^4+6a^2+1}{a^4-2a^2+1}x^2+1.$$

The discriminant of this quadratic equation is

$$\begin{aligned}
&\frac{(a^4+6a^2+1)^2}{(a^4-2a^2+1)^2}-1 = 16a^2\,\frac{(a^2+1)^2}{(a^2-1)^4}\\
&\Longrightarrow x^2 = \frac{a^4+6a^2+1}{(a^2-1)^2}\pm 4a\,\frac{a^2+1}{(a^2-1)^2} = \frac{(a\pm 1)^4}{(a^2-1)^2}
\end{aligned}$$

and all possible solutions are

$$\left\{a,-a,\frac{1}{a},-\frac{1}{a},\frac{a+1}{a-1},-\frac{a+1}{a-1},\frac{a-1}{a+1},-\frac{a-1}{a+1}\right\}$$

Another way is to observe

$$\frac{(x^4+1)(x^4+6x^2+1)}{x^2(x^2-1)^2} = \frac{1}{2}\left(x^2+\frac{1}{x^2}\right)\left(\left(\frac{x+1}{x-1}\right)^2+\left(\frac{x-1}{x+1}\right)^2\right)$$

and note that a polynomial of degree 8 has at most 8 roots. However, in this case we would need an argument to show that all these roots are pairwise distinct.

12. (HS-2) Define a sequence $a_1, a_2, \ldots, a_n, \ldots$ of real numbers by

$$a_1 = 1\,,\; a_{n+1} = 2a_n + \sqrt{3a_n^2 + 1} \quad (n \in \mathbb{N})\,.$$

Determine all sequence elements that are integers.

Reason: Sequence.

Solution:

$$\begin{aligned}(a_{n+1} - a_n)^2 = 3a_n^2 + 1 &\Longrightarrow a_{n+1}^2 - 4a_{n+1}a_n + a_n^2 = 1 \quad (n \geq 1)\\ &\Longrightarrow a_n^2 - 4a_na_{n-1} + a_{n-1}^2 = 1 \quad (n \geq 2)\\ &\Longrightarrow a_{n+1}^2 - a_{n-1}^2 - 4a_n(a_{n+1} - a_{n-1}) = 0\\ &\Longrightarrow (a_{n+1} - a_{n-1}) \cdot (a_{n+1} + a_{n-1} - 4a_n) = 0\end{aligned}$$

We also have $a_{n+1} > 2a_n > a_n > a_{n-1}$ for all $n \geq 2$ so that $a_{n+1} \neq a_{n-1}$, i.e. $a_{n+1} = 4a_n - a_{n-1}$. Since $a_1 = 1$ and $a_2 = 3$ are integers, this equation implies that all subsequent a_{n+1} are integers, too, so the entire sequence is in $\mathbb{Z}$.

13. (HS-3) For $n \in \mathbb{N}$ define

$$f(n) := \sum_{k=1}^{n^2} \frac{n - \left[\sqrt{k-1}\right]}{\sqrt{k} + \sqrt{k-1}}\,.$$

Determine a closed form for $f(n)$ without summation. The bracket means: $[x] = m \in \mathbb{Z}$ if $m \leq x < m+1$.

Reason: Recursion.

Solution:

$$\begin{aligned}f(n) &= \sum_{m=0}^{n-1} \sum_{k=m^2+1}^{(m+1)^2} \frac{n - \left[\sqrt{k-1}\right]}{\sqrt{k} + \sqrt{k-1}}\\ &= \sum_{m=0}^{n-1} (n-m) \sum_{k=m^2+1}^{(m+1)^2} \left(\sqrt{k} - \sqrt{k-1}\right)\\ &= \sum_{m=0}^{n-1} (n-m) \cdot \left(\sqrt{(m+1)^2} - \sqrt{m^2}\right)\\ &= \sum_{m=0}^{n-1} (n-m) = \sum_{k=1}^{n} k = \frac{n(n+1)}{2}\end{aligned}$$

14. (HS-4) Solve over the real numbers

$$\begin{array}{lll} (1) & x^4+x^2-2x & \geq 0 \\ (2) & 2x^3+x-1 & < 0 \\ (3) & x^3-x & > 0 \end{array}$$

Reason: Intervals.

Solution: All $x \geq 1$ violate the second equation, and all $x \leq -1$ violate the third, and

$$x^3-x=x(x+1)(x-1)>0$$

requires $x \notin [0,1)$ so we are left with $x \in I := (-1,0)$.

$$\begin{aligned} x^4+x^2-2x &> 0+0+0=0 \\ 2x^3+x-1 &< 0+0-1=-1<0 \\ x^3-x=x(x-1)(x+1) &= (-x)(-x+1)(x+1) > 0\cdot 0\cdot 0=0 \end{aligned}$$

and all $x \in I$ solve the equation system.

15. (HS-5) Let $f(x) := x^4-(x+1)^4-(x+2)^4+(x+3)^4$. Determine whether there is a smallest function value if $f(x)$ is defined (a) for integers, and (b) for real numbers. Which is it?

Reason: Domains.

Solution:

$$\begin{aligned} f(x) &= x^4-(x^4+4x^3+6x^2+4x+1)-(x^4+8x^3+24x^2+32x+16) \\ &\quad +(x^4+12x^3+54x^2+108x+81) \\ &= 24x^2+72x+64=24\left(x+\frac{3}{2}\right)^2+10\geq 10 \end{aligned}$$

with $f(-3/2)=10$. So $f(x)$ assumes its minimum value 10 over the reals. However, we have for all integers $x \geq -1$ and all integers $x \leq -2$

$$f(x)\geq 16 \text{ with } f(-1)=f(-2)=16.$$

Hence $f(x)$ assumes its minimum once over the reals and twice over the integers with two different function values.

3 October 2021

1. Prove that $F : L^2([0,1]) \longrightarrow (C([0,1]), \|.\|_\infty)$ defined as
$$F(x)(t) := \int_0^1 (t^2+s^2)(x(s))^2\,ds$$
is compact.

   Reason: Theorem of Arzelà-Ascoli.

   Solution: $F(x)$ are continuous functions
$$F(x)(t) = t^2\int_0^1 (x(s))^2\,ds + \int_0^1 s^2(x(s))^2\,ds = a\cdot t^2 + b$$
with $|a|, |b| \leq \|x\|_{L^2([0,1])}$. If $U \subseteq L^2([0,1])$ is bounded, then $F(U) \subseteq C([0,1])$ is bounded, too, and equicontinuous. Therefore $F(U)$ is relative compact in the supremum norm by the theorem of Arzelà-Ascoli. Hence F maps bounded sets on relative compact sets, i.e. F is a compact operator.

2. A project manager has n workers to finish the project. Let x_i be the workload of the $i-$th person, and
$$x \in S := \left\{ x \in \mathbb{R}^n \mid \sum_{i=1}^n x_i = 1\,,\, x_i \geq 0 \right\}$$
a possible partition of work. Let X_i be the set of partitions, which person i agrees upon. We may assume that he automatically agrees if $x_i = 0$, that X_i is closed, and that there is always at least one person which agrees to a given partition, i.e. $\bigcup_{i=1}^n X_i = S$.

   Prove that there is one partition that all workers agree upon.

   Reason: Project management lemma.

   Solution: Let $F_i := \{x \in S \,|\, x_i = 0\} \subseteq X_i$ be the $i-$th side of the simplex S. We have to show that $\bigcap_{i=1}^n X_i \neq \emptyset$. Assume the contrary and set $d_i(x) := \operatorname{dist}(x, X_i)$. The distances are continuous functions and $\sum_{i=1}^n d_i(x) > 0$ per assumption. Define
$$f = (f_1,\ldots,f_n) : S \longrightarrow S$$
$$f_i(x) := \frac{d_i(x)}{\sum_{i=1}^n d_i(x)}$$

Since $\bigcup_{i=1}^n X_i = S$, every $x \in S$ is part of a set X_i, i.e. $f_i(x) = 0$ for some $i \in \{1, \ldots, n\}$. f maps thus onto the boundary $\delta S = \bigcup_{i=1}^n F_i$. We also have $f(F_i) \subseteq X_i$ and so $f(F_i) \subseteq F_i$. Let $g(x)$ be the point, which is the reflexion of $f(x)$ at the center $c := (n^{-1}, \ldots, n^{-1})$. Then

$$c = \lambda(x)g(x) + (1 - \lambda(x))f(x)\,,\; 0 < \lambda(x) < 1\,,\; f(x), g(x) \in \delta S$$

with continuous functions $\lambda(x)$ and $g(x) : S \longrightarrow \delta S$. For $x \in F_i$ we get $g(x) \notin F_i$ because of the reflexion. Hence $g(x) \neq x$ for all $x \in \delta S$. Interior points of S aren't fixed points either, because they are mapped onto the boundary. This means that the continuous function $g(x)$ has no fixed point, in contradiction to Brouwer's fixed point theorem, and the assumption $\bigcap_{i=1}^n X_i = \emptyset$ was wrong.

3. Assume the axiom schema of separation for any predicate $P(x)$

$$\forall A \,:\, \exists M \,:\, \forall x \,:\, (x \in M \Longleftrightarrow x \in A \wedge P(x))$$

Show that $|A| < |\mathcal{P}(A)|$ where $\mathcal{P}(A)$ is the power set of A.

Reason: Cantor's theorem.

Solution: $x \longmapsto \{x\}$ is an injective function from A to $\mathcal{P}(A)$, so $|A| \leq |\mathcal{P}(A)|$. We need to show that there is no surjective function. Assume

$$f \,:\, A \twoheadrightarrow \mathcal{P}(A)$$

is surjective. Set $M := \{x \in A \,|\, x \notin f(a)\}$. Then M is a set by the axiom scheme of separation, and thus $M \in \mathcal{P}(A)$. Since f is onto, there is an element $a \in A$ such that $f(a) = M$. Hence by definition of f and M

$$a \in f(a) = M \Longleftrightarrow a \notin f(a)$$

This shows that the assumption about the existence of a surjective function f is false, and in particular $|A| < |\mathcal{P}(A)|$.

4. Let $\sigma_1, \ldots, \sigma_n$ be homomorphisms from a group G into the multiplicative group $\mathbb{F}^*$ of a field $\mathbb{F}$. Show that they are $\mathbb{F}-$linearly independent if and only if they are pairwise distinct.

Reason: Dedekind's independence theorem.

Solution: If the σ_i are linearly independent, then they are certainly pairwise distinct, so assume the σ_i are all distinct. We proceed by induction on n.

Let $n = 1$ and $c\sigma_1 = 0$. Then $c\sigma_1(G) = 0$ and since $G \neq \emptyset$ there is a $g \in G$ such that $c\sigma_1(g) = 0$. As $\operatorname{im}(\sigma_1) \subseteq \mathbb{F}^*$ which has no zero divisors we conclude $c = 0$ and σ_1 is linearly independent. Assume $n > 1$ and that the statement is true for $n-1$ homomorphisms. Let $\sum_{j=1}^n c_j\sigma_j = 0$ for some $c_j \in \mathbb{F}^*$. We know from $\sigma_1 \neq \sigma_n$ that there is an element $g_0 \in G$ such that $\sigma_1(g_0) \neq \sigma_n(g_0)$.

$$
\begin{aligned}
0 &= \sum_{j=1}^n c_j\sigma_j(x) \quad \forall\, x \in G \\
\Longrightarrow 0 &= \sum_{j=1}^n c_j\sigma_j(g_0x) = c_1\sigma_1(g_0)\sigma_1(x) + \sum_{j=2}^n c_j\sigma_j(g_0)\sigma_j(x) \\
\Longrightarrow 0 &= \sigma_1(g_0)\sum_{j=1}^n c_j\sigma_j(x) = c_1\sigma_1(g_0)\sigma_1(x) + \sum_{j=2}^n c_j\sigma_1(g_0)\sigma_j(x) \\
\Longrightarrow 0 &= \sum_{j=2}^n c_j(\sigma_j(g_0) - \sigma_1(g_0))\sigma_j(x) \\
\Longrightarrow\ & c_j(\sigma_j(g_0) - \sigma_1(g_0)) = 0 \quad \forall\, j > 1 \\
\Longrightarrow\ & c_n(\sigma_n(g_0) - \sigma_1(g_0)) = 0 \\
\Longrightarrow\ & c_n = 0 \\
\Longrightarrow 0 &= \sum_{j=1}^{n-1} c_j\sigma_j \\
\Longrightarrow\ & c_1 = \ldots = c_{n-1} = 0
\end{aligned}
$$

The statement is already true for semigroups G.

5. Prove that general Heisenberg (Lie-)algebras $\mathfrak{H}$ are nilpotent.

   Reason: Engel's theorem.

   Solution: The general $n-$dimensional Heisenberg group ($n \geq 3$) is the linear algebraic group of matrices of the form $\begin{bmatrix} 1 & \vec{a}^\tau & b \\ 0 & \mathbb{I}_{n-2} & \vec{c} \\ 0 & 0 & 1 \end{bmatrix} = \exp\left(\begin{bmatrix} 0 & \vec{a}^\tau & b \\ 0 & 0_{n-2} & \vec{c} \\ 0 & 0 & 0 \end{bmatrix}\right)$. The matrices in the argument of the exponential function form their tangent space. They build a nilpotent associative algebra. To see that it is also nilpotent as a Lie algebra we set E_{ij} to be the matrix with 1 at position (i,j) and zeros elsewhere. Then

$\{E_{12},\ldots,E_{1n},E_{2n},\ldots,E_{(n-1)n}\}$ form a basis of $\mathfrak{H}$.

$$\begin{aligned}
X &= \sum_{j=2}^{n} x_j E_{1j} + \sum_{i=2}^{n-1} y_i E_{in} \\
[X,E_{1k}] &= \sum_{j=2}^{n} x_j [E_{1j},E_{1k}] + \sum_{i=2}^{n-1} y_i [E_{in},E_{1k}] = -y_k E_{1n} \\
[X,E_{kn}] &= \sum_{j=2}^{n} x_j [E_{1j},E_{kn}] + \sum_{i=2}^{n-1} y_i [E_{in},E_{kn}] = x_k E_{1n} \\
[X,E_{1n}] &= 0
\end{aligned}$$

This shows that all linear transformations $\operatorname{ad}(X)$ are nilpotent, hence $\mathfrak{H}$ is a nilpotent Lie algebra by Engel's theorem.

6. Prove that the polynomial $\mathbb{N}_0^2 \xrightarrow{P} \mathbb{N}_0$ defined as

$$P(x,y) = \frac{1}{2}\left((x+y)^2 + 3x + y\right)$$

is a bijection.

Reason: Theorem of Fueter-Pólya.

Solution:

$$\begin{aligned}
2P(x,y) &= (x+y)(x+y+1) + 2x = x^2 + 2xy + y^2 + 3x + y \\
\nabla_{(a,b)}(2P) &= (2x+2y+3, 2x+2y+1)_{(a,b)} = (2a+2b+3, 2a+2b+1) \\
\nabla_{(a,b)}(2P)(u,v) &= 2au + 2bu + 3u + 2av + 2bv + v
\end{aligned}$$

Hence $2P(x,y)$ is strictly increasing in any direction of the first quadrant and at any point in its domain, i.e. in particular injective.

$2P(0,y) = y^2 + y$ and $2P(x,0) = x^2 + 3x$. Let $N \in \mathbb{N}_0$ and

$$m := \max\{x \in \mathbb{N}_0 \,|\, x^2 + x \leq 2N\}.$$

Then $2N < (m+1)^2 + m + 1 = m^2 + 3m + 2$ or $2N \leq m^2 + 3m + 1$. The right side is always odd, whereas the left is even. Hence we may conclude that

$$m^2 + m \leq 2N \leq m^2 + 3m.$$

Set

$$2N = m^2 + 3m - k \text{ with } k \in \{0, 2, 4, \ldots, 2m\}$$

$$
\begin{aligned}
2P\left(m-\frac{k}{2},\frac{k}{2}\right) &= \left(m-\frac{k}{2}\right)^2+2\left(m-\frac{k}{2}\right)\frac{k}{2}+\left(\frac{k}{2}\right)^2+3\left(m-\frac{k}{2}\right)+\frac{k}{2}\\
&= m^2+3m-k=2N
\end{aligned}
$$

and $P(x,y)$ is surjective.

It can be shown in a rather complicated proof, that $P(x,y)$ and $P(y,x)$ are the only quadratic real polynomials that enumerate $\mathbb{N}^2$ in such a way (Theorem of Fueter-Pólya). It is not known whether the requirement quadratic can be dropped.

7. Prove that the spectrum of every element of a complex Banach algebra B with 1 is nonempty. Conclude that if B is a division ring, then $B \cong \mathbb{C}$.

   Reason: Theorem of Gelfand-Mazur.

   Solution: Assume there is an element $a \in B$ such that all $a-\lambda 1$ are invertible ($\lambda \in \mathbb{C}$). Then we have for two distinct numbers $\lambda \neq \mu$

$$
\begin{aligned}
(a-\lambda 1)^{-1}(\lambda-\mu)(a-\mu 1)^{-1} &= (a-\lambda 1)^{-1}\left[(a-\mu 1)-(a-\lambda 1)\right](a-\mu 1)^{-1}\\
&= [(a-\lambda 1)^{-1}(a-\mu 1)-1](a-\mu 1)^{-1}\\
&= (a-\lambda 1)^{-1}-(a-\mu 1)^{-1}
\end{aligned}
$$

   Let $f : B \longrightarrow \mathbb{C}$ be an arbitrary homomorphism from B^*. Then

$$
\frac{f((a-\lambda 1)^{-1})-f((a-\mu 1)^{-1})}{\lambda-\mu} = f((a-\lambda 1)^{-1}(a-\mu 1)^{-1})
$$

   The right-hand side exists for $\mu \to \lambda$ because f and all algebraic operations including the inversion in B are continuous. Hence $\lambda \stackrel{\varphi}{\longmapsto} f((a-\lambda 1)^{-1})$ is holomorph on $\mathbb{C}$. Furthermore

$$
\lim_{|\lambda|\to\infty} \|(a-\lambda 1)^{-1}\| = 0
$$

   so φ is bounded and vanishes at infinity. Now φ is constant by Liouville's theorem, i.e. identically zero. Since $f \in B^*$ has been chosen arbitrarily, the theorem of Hahn-Banach yields that $(a-\lambda 1)^{-1} = 0$ which is impossible for an invertible element.

8. Let $X_1,\ldots,X_n$ be independent random variables, such that almost certain $a_i \leq X_i - E(X_i) \leq b_i$, and let $0 < c \in \mathbb{R}$. Prove that

$$
\Pr\left(\sum_{i=1}^{n}(X_i-E(X_i)) \geq c\right) \leq \exp\left(\frac{-2c^2}{\sum_{i=1}^{n}(b_i-a_i)^2}\right).
$$

Reason: Hoeffding inequality.

Solution: Let's prove the Markov-Chebyshev inequality first. Let (Ω, Σ, ν) be a measure space, $f : \Omega \longrightarrow \mathbb{R}_0^+$ a measurable function, and $\varepsilon, p > 0$ real numbers. Then

$$\int_\Omega f^p \, d\nu \geq \int_{x \,|\, f(x) \geq \varepsilon} f^p \, d\nu \geq \int_{x \,|\, f(x) \geq \varepsilon} \varepsilon^p \, d\nu = \varepsilon^p \nu \left(x \,|\, f(x) \geq \varepsilon\right)$$

This leads to the exponential version

$$\begin{aligned} \Pr(X \geq a) &= \Pr(\exp(X) \geq \exp(a)) \\ &\leq \inf_{p>0} \frac{1}{\exp(ap)} \int_\mathbb{R} \exp(pX) \, d\Pr = \inf_{p>0} \frac{E(\exp(pX))}{\exp(pa)} \end{aligned}$$

With $\nu = \Pr$, $f = |X - E(X)|$ and $p = 2$ we get the simple version

$$\Pr(|X - E(X)| \geq k\sigma) \leq \frac{1}{k^2}$$

where $\sigma^2 = Var(X)$. This can also be seen directly by conditional probabilities

$$\begin{aligned} \sigma^2 &= E((X - E(X))^2) \\ &= E((X - E(X))^2 \,|\, k\sigma \leq |X - E(X)|) \cdot \Pr(k\sigma \leq |X - E(X)|) \\ &+ E((X - E(X))^2 \,|\, k\sigma > |X - E(X)|) \cdot \Pr(k\sigma > |X - E(X)|) \\ &\geq (k\sigma)^2 \cdot \Pr(k\sigma \leq |X - E(X)|) + 0 \cdot \Pr(k\sigma > |X - E(X)|) \\ &= k^2\sigma^2 \Pr(k\sigma \leq |X - E(X)|) \end{aligned}$$

For the matter of convenience we set $Y_i := X_i - E(X_i)$ so $E(Y_i) = 0$. Moreover, consider for $z > 0$ the strictly monotone increasing function $x \mapsto \exp(zx)$ on the real numbers.

We get from the exponential version of the Markov-Chebyshev inequality

$$\Pr\left(\sum_{i=1}^n Y_i \geq c\right) \leq \inf_{z>0} \frac{E\left(\exp\left(z \sum_{i=1}^n Y_i\right)\right)}{\exp(zc)} \leq \frac{\prod_{i=1}^n E(\exp(zY_i))}{\exp(zc)}$$

The real exponential function is convex, so by the given conditions

$$\exp(zY_i) = \exp\left(\frac{b_i - Y_i}{b_i - a_i} za_i + \frac{Y_i - a_i}{b_i - a_i} zb_i\right) \leq \frac{b_i - Y_i}{b_i - a_i} \exp(za_i) + \frac{Y_i - a_i}{b_i - a_i} \exp(zb_i)$$

and with $E(Y_i)=0$ and

$$\begin{aligned}
E(\exp(zY_i)) &\leq \frac{b_i}{b_i-a_i}\exp(za_i)-\frac{a_i}{b_i-a_i}\exp(zb_i)\\
&=\exp(-u_i\lambda_i)\left((1-\lambda_i)+\lambda_i\exp(u_i)\right)\\
&\left[1-u_i\lambda_i+\frac{u_i^2\lambda_i^2}{2}-\frac{u_i^3\lambda_i^3}{3!}\pm\ldots\right]\cdot\\
&\cdot\left[1+u_i\lambda_i+\frac{u_i^2\lambda_i}{2}+\frac{u_i^3\lambda_i}{3!}+\ldots\right]\\
&=\left[1+u_i\lambda_i+\frac{u_i^2\lambda_i}{2}+\frac{u_i^3\lambda_i}{3!}+\ldots\right]\\
&-\left[u_i\lambda_i+u_i^2\lambda_i^2+\frac{u_i^3\lambda_i^2}{2}+\ldots\right]\\
&+\left[\frac{u_i^2\lambda_i^2}{2}+\frac{u_i^3\lambda_i^3}{2}+\ldots\right]\\
&=1+\frac{u_i^2}{2}\underbrace{\left(\lambda_i-\lambda_i^2\right)}_{\leq 1/4}+\underbrace{O(\lambda_i u_i^3)}_{<0}\leq 1+\frac{\mathrm{u}_\mathrm{i}^2}{8}\leq\exp\left(\frac{\mathrm{u}_\mathrm{i}^2}{8}\right)
\end{aligned}$$

with $\lambda_i=-\dfrac{a_i}{b_i-a_i}$, $u_i=z(b_i-a_i)$.

Summing up the results, we have

$$\Pr\left(\sum_{i=1}^n Y_i\geq c\right)\leq\frac{\prod_{i=1}^n\exp(u_i^2/8)}{\exp(zc)}=\exp\left(-zc+\sum_{i=1}^n\frac{u_i^2}{8}\right)$$

which leads by the choice $z:=\dfrac{4c}{\sum_{i=1}^n(b_i-a_i)^2}$ to

$$\begin{aligned}
\Pr\left(\sum_{i=1}^n Y_i\geq c\right)&\leq\exp\left(-\frac{4c^2}{\sum_{i=1}^n(b_i-a_i)^2}+\frac{z^2}{8}\sum_{i=1}^n(b_i-a_i)^2\right)\\
&=\exp\left(\frac{-32c^2+16c^2}{8\sum_{i=1}^n(b_i-a_i)^2}\right)\\
&=\exp\left(\frac{-2c^2}{\sum_{i=1}^n(b_i-a_i)^2}\right)
\end{aligned}$$

9. Let $G\subseteq\mathbb{C}$ be a non-empty, open, connected subset, and f,g holomorphic functions on G. Show that the following statements are equivalent:

   (a) $f(z)=g(z)$ for all $z\in G$.

(b) $\{z \in G \,|\, f(z) = g(z)\}$ has a limit point.

(c) There is a $z \in G$ such that $f^{(n)}(z) = g^{(n)}(z)$ for all $n \in \mathbb{N}_0$.

Reason: Identity theorem.

Solution: Holomorphic function are analytic, i.e. can locally be represented by their Taylor series.

$(a) \Longrightarrow (b)$ is obvious since any point in G is a limit point of G.

$(b) \Longrightarrow (c)$. Let $z_0 \in G$ be a limit point of the set of coincidence points. W.l.o.g. we assume $z_0 = 0$. If (c) wasn't true, then there is a minimal $N \in \mathbb{N}_0$ such that $f^{(N)}(0) \neq g^{(N)}(0)$. We then have in a neighborhood of 0

$$f(z) - g(z) = z^N \underbrace{\sum_{n=0}^{\infty} \frac{f^{(N+n)}(0) - g^{(N+n)}(0)}{(N+n)!} z^n}_{=:h(z)}$$

and $\{z \in G \,|\, h(z) = 0\} = \{z \in G \,|\, f(z) = g(z)\}$ since $h(z)$ is continuous. In particular $0 = h(0) = \dfrac{f^{(N)}(0) - g^{(N)}(0)}{N!}$ in contradiction to the minimality of N.

$(c) \Longrightarrow (a)$. It is sufficient to show that

$$A := \{z \in G \,|\, f^{(n)}(z) = g^{(n)}(z) \;\forall\, n \in \mathbb{N}_0\}$$

is non-empty, open and closed since G is connected. $A \neq \emptyset$ by condition (c). A is also closed because

$$A = \bigcap_{i=0}^{\infty} \{z \in G \,|\, f^{(n)}(z) = g^{(n)}(z)\} = \left(f^{(n)} - g^{(n)}\right)^{-1}(\{0\})$$

it is the union of preimages of a closed set under a continuous function. $f - g$ is an analytic function and as such equal to its Taylor series in a neighborhood of $z \in A$, i.e. identically zero. However, this neighborhood is entirely contained in A, i.e. A is open.

10. Prove that π^2 is irrational.

Reason: Calculus.

Solution: Assume $\pi^2 = \dfrac{p}{q}$ with $p, q \in \mathbb{N}$ and define

$$P_n(x) := \frac{x^n(1-x)^n}{n!} \quad , \quad n! P_n(x) = \sum_{k=n}^{2n} c_k x^k \in \mathbb{Z}[x]$$

Then

$$P_n^{(j)}(0) = \begin{cases} 0 & \text{if } j < n \wedge j > 2n \\ \dfrac{j!c_j}{n!} \in \mathbb{Z} & \text{if } n \leq j \leq 2n \end{cases}$$

and $P_n^{(j)}(x) = (-1)^j P_n^{(j)}(1-x)$ so $P_n^{(j)}(1) = (-1)^j P_n^{(j)}(0) \in \mathbb{Z}$, too. Set

$$Q_n(x) := q^n \left(\pi^{2n} P_n(x) - \pi^{2n-2} P_n''(x) \pm \ldots + (-1)^n \pi^0 P_n^{(2n)}(x)\right)$$

We already know that $Q_n(0), Q_n(1) \in \mathbb{Z}$.

$$\begin{aligned} &\frac{d}{dx}\left(Q_n'(x)\sin(\pi x) - \pi Q_n(x)\cos(\pi x)\right) = \left(Q_n''(x) + \pi^2 Q_n(x)\right)\sin(\pi x) \\ &\quad = q^n \pi^{2n+2} P_n(x)\sin(\pi x) = p^n \pi^2 P_n(x)\sin(\pi x) \\ &\quad \Longrightarrow \\ &p^n \pi \int_0^1 P_n(x)\sin(\pi x)\,dx = \left[\frac{Q_n'(x)\sin(\pi x)}{\pi} - Q_n(x)\cos(\pi x)\right]_0^1 \\ &\quad = Q_n(1) + Q_n(0) \in \mathbb{Z} \end{aligned}$$

On the other hand we have by definition of $P_n(x)$ on $[0,1]$

$$0 < p^n \pi \int_0^1 P_n(x)\sin(\pi x) \leq \frac{\pi p^n}{n!} \stackrel{n\to\infty}{\longrightarrow} 0$$

and $Q_n(0) + Q_n(1)$ cannot be an integer for large enough n.

11. (HS-1) Find all functions f, g such that

$$\begin{gathered} f, g \,:\, \mathbb{R}\backslash\{-1,0,1\} \longrightarrow \mathbb{R} \\ xf(x) = 1 + \frac{1}{x} g\left(\frac{1}{x}\right) \quad \text{and} \quad \frac{1}{x^2} f\left(\frac{1}{x}\right) = x^2 g(x) \end{gathered}$$

Extra: Determine a number $r \in \mathbb{R}$ such that $|f(x) - f(x_0)| < 0.001$ whenever $|x - x_0| < r$ and $x_0 = 2$, and explain why there is no such number if we choose $x_0 = 1$ even if we artificially define some function value for $f(1)$.

Reason: Real functions.

Solution: From the second equation we get

$$\begin{aligned} xg(x) = \frac{1}{x^3} f\left(\frac{1}{x}\right) &\Longrightarrow \frac{1}{x} g\left(\frac{1}{x}\right) \\ &\Longrightarrow xf(x) = 1 + x^3 f(x) \\ &\Longrightarrow 1 = f(x)(x - x^3) = f(x)x(1-x)(1+x) \neq 0 \\ &\Longrightarrow f(x) = \frac{1}{x(1-x)(1+x)} = \frac{1}{x - x^3} \\ &\Longrightarrow g(x) = \frac{1}{x^4} f\left(\frac{1}{x}\right) \\ &\Longrightarrow g(x) = \frac{1}{x^4} \cdot \frac{1}{\frac{1}{x} - \frac{1}{x^3}} = \frac{1}{x(x^2-1)} \\ &\qquad = \frac{1}{x(x-1)(x+1)} = -f(x) \end{aligned}$$

One can easily check that the pair $\left(\frac{1}{x-x^3}, \frac{1}{x^3-x}\right)$ satisfies the two initial conditions, i.e. that this pair is a feasible solution.

Extra: Our goal is to achieve

$$|f(x) - f(2)| = \left|f(x) + \frac{1}{6}\right| = \left|\frac{6 + x - x^3}{6(x - x^3)}\right| < 0.001$$

whenever $|x - 2| < r$, i.e. $2 - r < x < 2 + r$ for some real number r. It is only asked for one such number, so we do not need to find a unique, smallest, or greatest one.

Let's start with the upper bound. Keep in mind that $x \sim 2$ and $r \sim 0$.

$$\begin{aligned} \left|\frac{6 + x - x^3}{6(x - x^3)}\right| &= \frac{|6 + x - x^3|}{6 \cdot |x| \cdot |1 - x| \cdot |1 + x|} < \frac{6 + (2 + r) + (r - 2)^3}{6 \cdot (2 - r)(r + 1)(3 - r)} \\ &= \frac{r^3 - 6r^2 + 13r}{6 \cdot (r^3 - 4r^2 + r + 6)} = \frac{r}{6} \cdot \frac{13 - 6r + r^2}{6 + r - 4r^2 + r^3} \\ &< \frac{r}{6} \cdot \frac{18}{1} = 3r < 0.001 \end{aligned}$$

for $r := 0.0001 = 10^{-4}$. Let us check the lower bound with this value.

$$\begin{aligned} \left|\frac{6 + x - x^3}{6(x - x^3)}\right| &> \frac{6 + (2 - r) - (2 + r)^3}{6 \cdot (2 + r)(1 - r)(3 + r)} = -\frac{r}{6} \cdot \frac{13 + 6r + r^2}{6 - r - 4r^2 - r^3} \\ &> -\frac{r}{6} \cdot \frac{18}{1} = -3r = -0.0003 > -0.001 \end{aligned}$$

Finally, let us define $f(1)=c\in\mathbb{R}$ for some real number $c\in\mathbb{R}$. Then for $n>10$

$$f(x)=\dfrac{1}{x(1-x)(1+x)}\begin{cases} >0 \stackrel{n\to\infty}{\longrightarrow} \infty & \text{if } x=1-\dfrac{1}{n} \\ =\dfrac{1}{c-c^3}=\text{const.} & \text{if } x=1 \\ <0 \stackrel{n\to\infty}{\longrightarrow} -\infty & \text{if } x=1+\dfrac{1}{n} \end{cases}$$

Hence the distance $|f(x)-f(1)|$ between the function values becomes arbitrary large at some location in $1-r<1-\dfrac{1}{n}<x<1+\dfrac{1}{n}<1+r$.

12. (HS-2) Solve the following equation system in $\mathbb{R}^3$

$$x^2+y^2+z^2=1 \quad \wedge \quad x+2y+3z=\sqrt{14}$$

Extra: Give an alternative solution in case you have the additional information that the solution is unique.

Reason: Non-linear equations.

Solution: Assume we have a solution (x,y,z), then

$$\begin{aligned} 0 &= (\sqrt{14}-2y-3z)^2+y^2+z^2-1 \\ &= 10z^2+12yz-6z\sqrt{14}-4y\sqrt{14}+5y^2+13 \\ &= 10\left(z+\frac{3}{5}y-\frac{3}{10}\sqrt{14}\right)^2+\frac{7}{5}y^2+\frac{2}{5}-\frac{2}{5}y\sqrt{14} \\ &= 10\left(z+\frac{3}{5}y-\frac{3}{10}\sqrt{14}\right)^2+\frac{7}{5}\left(y-\frac{1}{7}\sqrt{14}\right)^2 \\ &\Longrightarrow \\ y &= \sqrt{\frac{2}{7}} \wedge z=\frac{3}{10}\sqrt{14}-\frac{3}{5}y=\frac{3}{2}\sqrt{\frac{2}{7}}=\frac{3}{\sqrt{14}} \\ &\Longrightarrow \\ x &= 14-2\sqrt{\frac{2}{7}}-\frac{9}{\sqrt{14}}=\frac{1}{\sqrt{14}} \end{aligned}$$

It is easy to check that conversely the triple $\left(\dfrac{1}{\sqrt{14}},\dfrac{2}{\sqrt{14}},\dfrac{3}{\sqrt{14}}\right)$ satisfies the conditions of the statement.

Extra: Given that the equation system has a unique solution, we conclude that we have the equations of a sphere and a plane which intersect at exactly one point. This makes the plane a tangent space to the sphere. The tangent space of the sphere $x^2+y^2+z^2=1=1$ at $\vec{p}=(x_0,y_0,z_0)$ are all perpendicular vectors, i.e.

$$\vec{p}+\left\{\begin{bmatrix}v_x\\v_y\\v_z\end{bmatrix}\,:\,v_xx_0+v_yy_0+v_zz_0=0\right\}=\vec{p}+\alpha\begin{bmatrix}z_0\\0\\-x_0\end{bmatrix}+\beta\begin{bmatrix}0\\z_0\\-y_0\end{bmatrix}$$

This means for a point (x,y,z) on the plane that

$$\begin{aligned}x=x_0+\alpha z_0\,,\;y=y_0+\beta z_0\,,\;z&=z_0-x_0\alpha-y_0\beta\\ z_0z&=z_0^2-x_0(x-x_0)-y_0(y-y_0)\\ x_0x+y_0y+z_0z&=z_0^2+x_0^2+y_0^2=1\end{aligned}$$

Hence we get by comparison of coefficients with the given equation of the plane

$$x_0=\frac{1}{\sqrt{14}}\,,\;y_0=\frac{2}{\sqrt{14}}\,,\;z_0=\frac{3}{\sqrt{14}}$$

13. (HS-3) If $(x_n)_{n\in\mathbb{N}}\subseteq\mathbb{R}_{>0}$ is a monotone decreasing sequence of positive real numbers such that for every $n\in\mathbb{N}$

$$\frac{x_1}{1}+\frac{x_4}{2}+\frac{x_9}{3}+\ldots+\frac{x_{n^2}}{n}\leq 1$$

prove that for every $n\in\mathbb{N}$

$$\frac{x_1}{1}+\frac{x_2}{2}+\frac{x_3}{3}+\ldots+\frac{x_n}{n}\leq 3$$

Extra: Prove that both sequences converge to 0.

Reason: Sequences.

Solution: For every natural number n there is a number $k\in\mathbb{N}$ such that $k^2\leq n<(k+1)^2$. Hence

$$\begin{aligned}\sum_{i=1}^{n}\frac{x_i}{i}&\leq\sum_{i=2}^{k+1}\sum_{j=(i-1)^2}^{i^2-1}\frac{x_j}{j}\leq\sum_{i=2}^{k+1}(2i-1)\,\frac{x_{(i-1)^2}}{(i-1)^2}\\ &=\sum_{i=1}^{k}(2i+1)\frac{x_{i^2}}{i^2}\leq 3\sum_{i=1}^{k}\frac{x_{i^2}}{i}\leq 3\cdot 1=3\end{aligned}$$

by the given condition.

Extra: Assume the sequence $(x_n)_{n\in\mathbb{N}}$ becomes stationary at one point, say $x_n = a$ for all $n \geq N$. Then for any $M > N$

$$\sum_{i=1}^{M} \frac{x_i}{i} = \underbrace{\sum_{i=1}^{N-1} \frac{x_i}{i}}_{=:C_1} + \sum_{i=N}^{M} \frac{a}{i} = C_1 + a \cdot \underbrace{\sum_{i=N}^{M} \frac{1}{i}}_{=:C_M} \leq 3$$

for all M by assumption. However $\lim_{M\to\infty} C_M = \infty$, which cannot both hold. Hence the monotone decreasing sequences are strictly monotone decreasing, i.e.

$$1 \geq x_1 > x_2 > x_3 > \ldots > x_n > \ldots > 0.$$

If we now cut the interval $[0,1]$ in half, then the right half must contain infinitely many sequence members. Then we choose this half and cut it again into half. The right part has to contain infinitely many sequence members again. Going on with these nested intervals, we get interval lengths that converge to zero. If we pick one sequence member from each interval, we get a subsequence which converges to a real number (because $\mathbb{R}$ is complete). By strict monotony the sequence itself has to converge to the same number, say $L \in [0,1]$.

Assume $\lim_{n\to\infty} x_n = L > 0$. Then

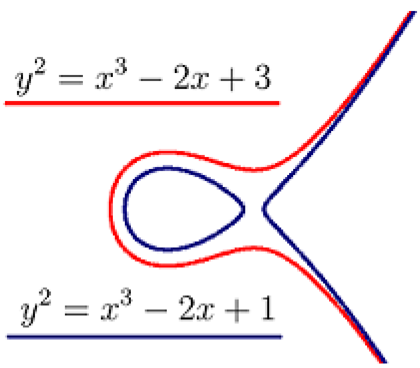
$$3 \geq \lim_{n\to\infty} \left(\frac{x_1}{1} + \ldots + \frac{x_n}{n}\right) \geq L \cdot \lim_{n\to\infty} \sum_{i=1}^{n} \frac{1}{n} = \infty$$

which cannot hold, hence our assumption was wrong and $L = 0$.

14. (HS-4) Solve the following equation system for real numbers:

$$\begin{aligned} (1) \qquad x + xy + xy^2 &= -21 \\ (2) \qquad y + xy + x^2y &= 14 \\ (3) \qquad x + y &= -1 \end{aligned}$$

Extra:



Consider the two elliptic curves and observe that one has two connection components and the other one has only one. Determine the constant $c \in [1,3]$ in $y^2 = x^3 - 2x + c$ where this behavior exactly changes. What is the left most point of this curve?

Reason: Non-linear equations.

Solution: Adding the (1) and (2) and using (3) gets

$$\begin{aligned}(x+y) + 2xy + xy(x+y) &= -7\\ \Longrightarrow xy &= -6\\ \Longrightarrow x - 6y &= -15\\ \Longrightarrow \begin{bmatrix} x\\ y\end{bmatrix} = \begin{bmatrix} 1 & -6\\ 1 & 1\end{bmatrix}^{-1} \cdot \begin{bmatrix} -15\\ -1\end{bmatrix} &= \frac{1}{7}\begin{bmatrix} 1 & 6\\ -1 & 1\end{bmatrix} \cdot \begin{bmatrix} -15\\ -1\end{bmatrix} = \begin{bmatrix} -3\\ 2\end{bmatrix}\end{aligned}$$

The pair $(-3, 2)$ conversely satisfies the required conditions, and is thus the unique solution.

Extra: The curves are symmetric to the $x-$axis $y = 0$. Moreover, the behavior changes at the point where the two most right extremal points coincide. Hence we have to find the points, where

$$\frac{dy}{dx} = 0$$

Now $2 \cdot y(x) \cdot y'(x) = 3x^2 - 2$ so for our points hold $x = \pm\sqrt{\frac{2}{3}}$. The negative values lead to the extremal points on the left, and the positive value is the one which we are interested in. We also know that for symmetry reasons, that

$$\begin{aligned} y^2\left(\sqrt{\frac{2}{3}}\right) = 0 = \sqrt{\frac{2}{3}}^3 - 2\sqrt{\frac{2}{3}} + c &= -\frac{4}{3}\sqrt{\frac{2}{3}} + c\\ \Longrightarrow c = \frac{4}{3}\sqrt{\frac{2}{3}} &= \sqrt{\frac{32}{27}} \approx 1.089\end{aligned}$$

To determine the left most point, we search for the points where $y = 0$, i.e. $0 = x^3 - 2x + \sqrt{\frac{32}{27}} = x^3 - 2x + \frac{4}{3}\sqrt{\frac{2}{3}}$. We know from the previous calculation that $x=\sqrt{\dfrac{2}{3}}$ is a solution. Long division shows

$$\begin{aligned}\left(x^3-2x+\frac{4}{3}\sqrt{\frac{2}{3}}\right):\left(x-\sqrt{\frac{2}{3}}\right)&=x^2+\sqrt{\frac{2}{3}}x-\frac{4}{3}\\&=\left(x+2\sqrt{\frac{2}{3}}\right)\left(x-\sqrt{\frac{2}{3}}\right)\\x^3-2x+\frac{4}{3}\sqrt{\frac{2}{3}}&=\left(x+2\sqrt{\frac{2}{3}}\right)\left(x-\sqrt{\frac{2}{3}}\right)^2\end{aligned}$$

The left most point is thus $-2\sqrt{\dfrac{2}{3}}\approx -1.633$ and the double root at $x=\sqrt{\dfrac{2}{3}}$ confirms the previous result.

15. (HS-5) Find all real numbers $m\in\mathbb{R}$, such that for all real numbers $x\in\mathbb{R}$ holds

$$f(x,m):=x^2+(m+2)x+8m+1>0 \qquad (*)$$

and determine the value of m for which the minimum of $f(x,m)$ is maximal. What is the maximum?

Extra: The set of all intersection points of two perpendicular tangents is called orthoptic of the parabola. Prove that it is the directrix, the straight parallel to the tangent at the extremum on the opposite side of the focus.

Reason: Parametric equation.

Solution: The quadratic equation $x^2+(m+2)x+8m+1=0$ has the solutions

$$-\frac{m+2}{2}\pm\frac{1}{2}\sqrt{m^2-28m}$$

If $m\leq 0$ then $m^2-28m\geq 0$ and the parabola has at least one intersection with the $x-$axis, i.e. $(*)$ cannot be greater than zero for all real numbers.

If $m\geq 28$ then the discriminant is again not negative and the parabola has at least one intersection with the $x-$axis again, i.e. $(*)$ cannot be greater than zero for all real numbers.

Hence the only possible numbers are $0 < m < 28$ in which case the discriminant is negative and the parabola does not intersect the $x-$axis:

$$\begin{aligned} x^2+(m+2)x+8m+1 &= \left(x+\frac{m+2}{2}\right)^2 - \frac{(m+2)^2}{4} + 8m+1 \\ &\geq -\frac{1}{4}\left(m^2-28m\right) = -\frac{1}{4}m(m-28) > 0 \end{aligned}$$

for all $x \in \mathbb{R}$ and $0 < m < 28$. The minimum of $f(x,m)$ for each parameter is determined by

$$\frac{d}{dx}f(x,m) = 0 = 2x+m+2 \Longrightarrow x = -\frac{m+2}{2}$$

so we want to maximize

$$\begin{aligned} f\left(-\frac{m+2}{2},m\right) &= \left(\frac{m+2}{2}\right)^2 - (m+2)\frac{m+2}{2} + 8m+1 \\ &= -\frac{1}{4}(m+2)^2+8m+1 = -\frac{1}{4}m^2+7m \end{aligned}$$

which is maximal at $-\frac{1}{2}m+7$, i.e. $m=14$ and $f(-8,14)=49$.

Extra: A parabola is defined as the set of points, that has equal distance to its focus and its directrix. We may assume that our parabola has the equation $y=ax^2$, $a \neq 0$. Then its focus is $F=\left(0,\frac{1}{4a}\right)$ and its directrix L thus $y=-\frac{1}{4a}$. This means

$$P = \{(x,y)\in\mathbb{R}^2 \,|\, y=ax^2\} = \{p\in\mathbb{R}^2 \,|\, d(F,p)=d(F,L)\}.$$

The slope of P is given by the first derivative $m=2ax$. Hence

$$P = \left\{\left(\frac{m}{2a},\frac{m^2}{4a}\right) \,\middle|\, m\in\mathbb{R}\right\}$$

and the tangent T with slope m has the equation $y = mx - \frac{m^2}{4a}$. Let $(x_0,y_0)\notin P$ be a point on T. Then $y_0 = mx_0 - \frac{m^2}{4a} \Longleftrightarrow 0 = m^2-4ax_0m+4ay_0$ which has two solutions, corresponding to the two possible tangents from (x_0,y_0). Now if the tangents meet in a right angle at (x_0,y_0), then the product of their slopes is -1. This equals the product of the solutions of the quadratic equation, i.e. by Vieta's formulas

$$-1 = 4ay_0 \Longrightarrow y_0 = -\frac{1}{4a}$$

so the set of intersection points is L, what had to be shown.

4 September 2021

1. Let f be a function defined on $(0,\infty)$ such that $f(x)>0$ for all $x>0$. Suppose that f has the following properties:

   (a) $\log f(x)$ is a convex function.

   (b) $f(x+1)=x\cdot f(x)$ for all $x>0$.

   (c) $f(1)=1$.

   Then $f(x)=\lim\limits_{n\to\infty}\dfrac{n!n^x}{x(x+1)\cdots(x+n)}=:\Gamma(x)$ for all $x>0$.

   Reason: Bohr-Mollerup theorem.

   Solution: The given conditions $(b),(c)$ allows to conclude

$$\begin{aligned} f(x+n) &= f(x+n-1+1)\\ &=(x+n-1)f(x+n-2+1)\\ &=(x+n-1)(x+n-2)f(x+n-3+1)\\ &=\\ &\vdots\\ &=\\ &=(x+n-1)(x-n-2)\cdots(x+1)xf(x)\end{aligned}$$

   This implies in particular that $f(N+1)=N!$ for all $N\in\mathbb{N}$ and if we can show $f(x)=\Gamma(x)$ for all $0<x\leq 1$ then we conclude for all $N<y=x+N\leq N+1$

$$
\begin{aligned}
f(y) = f(x+N) &= (x+N-1)(x-N-2)\cdots(x+1)\cdot x\cdot\Gamma(x)\\
&= (x+N-1)(x-N-2)\cdots(x+1)\cdot x\cdot \lim_{n\to\infty}\frac{n!n^x}{x(x+1)\cdots(x+n)}\\
&= \lim_{n\to\infty}\frac{(x+N-1)(x-N-2)\cdots(x+1)\cdot x\cdot n!n^x}{x\cdot(x+1)\cdots(x+n)}\\
&= \lim_{n\to\infty}\frac{n!n^x}{(x+N)(x+N+1)\cdots(x+n)}\\
&= \lim_{n\to\infty}\frac{n!n^{y-N}}{y(y+1)\cdots(y-N+n)}\\
&= \lim_{n\to\infty}\frac{n!n^y}{y\cdot(y+1)\cdots(y+n)}\cdot\frac{(y-N+n+1)\cdots(y+n)}{n^N}\\
&= \lim_{n\to\infty}\frac{n!n^y}{y\cdot(y+1)\cdots(y+n)}\cdot\left(\frac{y}{n}-\frac{N}{n}+\frac{n}{n}+\frac{1}{n}\right)\cdots\left(\frac{y}{n}+\frac{n}{n}\right)\\
&= \lim_{n\to\infty}\frac{n!n^y}{y\cdot(y+1)\cdots(y+n)}\cdot 1^N\\
&= \Gamma(y)
\end{aligned}
$$

Hence we may assume that $0 < x \leq 1$. Let $n > 2$ be some integer. Since $\log f(x)$ is convex, we have that the function lies beneath the secant of any two points at $a, b > 0$.

$$
\log f(x) \leq \log f(a) + \frac{\log f(b)-\log f(a)}{b-a}\cdot(x-a) \quad \text{for all } x\in(a,b)
$$

$$
\Longleftrightarrow
$$

$$
\frac{\log f(x)-\log f(a)}{x-a} \leq \frac{\log f(b)-\log f(a)}{b-a} \quad \text{for all } a<x<b
$$

Thus for $n < n+x \leq n+1$

$$
\underbrace{\frac{\log f(n+x)-\log f(n)}{(n+x)-n}}_{=\frac{\log f(n+x)-\log(n-1)!}{x}} \leq \underbrace{\frac{\log f(n+1)-\log f(n)}{(n+1)-n}}_{=\log n}
$$

and for $n-1 < n < n+x$

$$
\underbrace{\frac{\log f(n)-\log f(n-1)}{n-(n-1)}}_{=\log(n-1)} \leq \underbrace{\frac{\log f(n+x)-\log f(n-1)}{n+x-(n-1)}}_{=\frac{\log f(n+x)-\log(n-2)!}{x+1}}
$$

Thus

$$\begin{aligned}(x+1)\log(n-1)+\log(n-2)! \leq \log f(n+x) &\leq \log(n-1)!+x\log n\\ \log\left((n-1)^x(n-1)!\right) \leq \log f(n+x) &\leq \log\left(n^x(n-1)!\right)\\ \underbrace{\frac{(n-1)^x(n-1)!}{x(x+1)\cdots(x+n-1)}}_{=:L(n)} \leq f(x) &\leq \underbrace{\frac{n^x(n-1)!}{x(x+1)\cdots(x+n-1)}}_{=:R(n)}\end{aligned}$$

Since $f(x)$ in the sandwich is independent of n we may write

$$L(n{+}1)=\frac{n^x n!}{x(x+1)\cdots(x+n)} \leq f(x) \leq R(n)=\frac{n^x n!}{x(x+1)\cdots(x+n)}\cdot\frac{x+n}{n}$$

and letting $n\to\infty$ we get $\Gamma(x)\leq f(x)\leq\Gamma(x)$ which we had to show.

2. Let $T=(x_1,x_2,\ldots,x_m)$ be a sequence of not necessarily distinct reals. For any positive b, define

$$T_b := \{(x_i,x_j)\,|\,1\leq i,j\leq m, |x_i-x_j|\leq b\}.$$

Show that for any sequence T and for every integer $r>1$,

$$|T_r|<(2r-1)|T_1|.$$

Reason: Combinatorics.

Solution: We apply induction on $|T|=m$. The result is trivial for $m=1$. Assuming it holds for $m-1$, we prove it for $m>1$. Given a sequence $T=(x_1,\ldots,x_m)$ let $t+1$ be the maximum number of points of T in a closed interval of length 2 centered at a member of T. Let x_i be any rightmost point of T so that there are $t+1$ members of T in the interval $[x_i-1,x_i+1]$ and define $T':=T-\{x_i\}$. The number of members of T' in the interval $[x_i-1,x_i+1]$ is clearly t and hence x_i appears in precisely $2t+1$ ordered pairs of T_1. Thus

$$|T_1|=2t+1+|T_1'|.$$

The interval $[x_i-r,x_i+r]$ is the union of the $2r-1$ smaller intervals

$$[x_i{-}r,x_i{-}r{+}1),\ldots,[x_i{-}2,x_i{-}1),[x_i{-}1,x_i{+}1],(x_i{+}1,x_i{+}2],\ldots,(x_i{+}r{-}1,x_i{+}r].$$

By the choice of x_i, each of these smaller intervals can contain at most $t+1$ members of T, and each of the last $r-1$ ones, which lie to the right of x_i, can contain at most t members of T. Altogether there are thus at most $(r-1)(t+1)+rt$ members of T' in $[x_i - r, x_i + r]$ and hence

$$|T_r| \leq 2(r-1)(t+1) + 2rt + 1 + |T'_r| = (2r-1)(2t+1) + |T'_r|.$$

By induction hypothesis $|T'_r| < (2r-1)|T'_1|$ and hence $|T_r| < (2r-1)|T_1|$.

3. Let X, Y be two independent identically distributed real random variables. For a positive b, define $p_b := \operatorname{prob}(|X-Y| \leq b)$. Then for every integer r, $p_r \leq (2r-1)p_1$. Thus

$$\operatorname{prob}(|X-Y| \leq 2) \leq 3 \cdot \operatorname{prob}(|X-Y| \leq 1)$$

Reason: Stochastic.

Solution: Fix an integer m, and let $S := (x_1, \ldots, x_m)$ be a random sequence of m elements, where each x_i is chosen, randomly and independently, according to the distribution of X. By the previous statement

$$|S_r| < (2r-1)|S_1|.$$

Therefore, the expectation of $|S_r|$ is smaller than that of $(2r-1)|S_1|$. However, by the linearity of expectation it follows that the expectation of $|S_b|$ is precisely $m + m(m-1)p_b$ for every $b > 0$. Thus

$$m + m(m-1)p_r < (2r-1)(m + (m-1)p_1),$$

implying that for every integer m,

$$p_r < (2r-1)p_1 + \frac{2r-2}{m-1} \stackrel{m\to\infty}{\longrightarrow} (2r-1)p_1$$

It can be proven that even the strict inequality

$$\operatorname{prob}(|X-Y| \leq 2) < 3 \cdot \operatorname{prob}(|X-Y| \leq 1)$$

holds, in which case we speak of the $1-2-3$ theorem.

4. Let $\mathbb{F}$ be a field and G a finite group, such that $\operatorname{char}\mathbb{F} \nmid |G|$. Prove that $\mathbb{F}G$ is semisimple, and show that this is not true if $\operatorname{char}\mathbb{F} \mid |G|$.

Reason: Theorem of Maschke.

Solution: Let $W \subseteq V$ be finite-dimensional $\mathbb{F}G$-modules. Pick an idempotent $e \in \operatorname{End}_{\mathbb{F}}(V)$ with $eV = W$ and define

$$\overline{e} := \frac{1}{|G|}\sum_{g\in G} geg^{-1}$$

where the elements of G are considered as endomorphisms of V. Then

$$h\overline{e} = \frac{1}{|G|}\sum_{g\in G} hgeg^{-1} = \frac{1}{|G|}\sum_{g\in G}(hg)e(hg)^{-1}h = \overline{e}h$$

for all $h \in G$ and thus $\overline{e} \in \operatorname{End}_{\mathbb{F}G}(V)$. Since W is a submodule if V, the endomorphism $\overline{e}$ still satisfies $\overline{e}V \subseteq W$ and $\overline{e}|_W = \operatorname{id}_W$. Hence $\overline{e}$ is an idempotent with $\overline{e}V = W$, and we have

$$V = W \oplus (\operatorname{id}_V - \overline{e})\, V$$

i.e. every submodule splits and V is semisimple, and so is $\mathbb{F}G$.

Let $x := \sum_{g\in G} g \in \mathbb{F}G$ satisfies $gx = x$ for all $g \in G$ and $x^2 = |G|x = 0$. Thus $\mathbb{F}Gx = \mathbb{F}x$ is a submodule of $\mathbb{F}G$ which contains no idempotent. In particular, $\mathbb{F}x$ is not projective, and hence $\mathbb{F}G$ is not semisimple.

5. A group G together with a topology, such that the mapping on $G \times G$ (equipped with the product topology) to G given by $(x, y) \longmapsto xy^{-1}$ is continuous, is called a topological group (e.g. a Lie group). Prove

   (a) G is a topological group if and only if inversion and multiplication are continuous.

   (b) The mappings $x \longmapsto xg$ and $x \longmapsto gx$ are homeomorphisms for each $g \in G$.

   (c) Each open subgroup $U \leq G$ is closed, and each closed subgroup $U \leq G$ of finite index is open. If G is compact, then each open subgroup is of finite index.

   (d) Let $H \leq G$ be a subgroup equipped with the subspace topology, $K \trianglelefteq G$ a normal subgroup, and G/K equipped with the quotient space topology. Then H and G/K are again topological groups and the projection $\pi : G \twoheadrightarrow G/K$ is open.

   (e) G is Hausdorff if and only if $\{1\}$ is a closed set in G. G/K is Hausdorff for a normal subgroup $K \trianglelefteq G$, if and only if K is closed in G. If G is totally disconnected, then G is Hausdorff.

   (f) Let G be a compact topological group and $\{X_j\ (j \in I)\} \subseteq G$ a family of closed subsets such that for all $i, j \in I$ there is a $k \in I$ with $X_k \subseteq X_i \cap X_j$. Then we have for any closed subset $Y \subseteq G$

$$Y \cdot \left(\bigcap_{i\in I} X_i\right) = \bigcap_{i\in I} YX_i$$

Reason: Topological Groups.

Solution:

(a) If inversion and multiplication are continuous, then their composition is continuous, too. Now let

$$\varphi : G \times G \longrightarrow G\,,\; \varphi(x,y) := xy^{-1}$$

be continuous. Inversion ι is the composition of the continuous functions

$$G \stackrel{x\to(1,x)}{\longrightarrow} \{1\} \times G \stackrel{\varphi|_{\{1\}\times G}}{\longrightarrow} G$$

and thus continuous, too. For the multiplication we get the composition of

$$G \times G \stackrel{(\mathrm{id},\iota)}{\longrightarrow} G \times G \stackrel{\varphi}{\longrightarrow} G$$

continuous functions again.

(b) It is sufficient to prove it for $\mu_g(x) := xg$. Now

$$\mu_g \;:\; G \stackrel{x\to(g,x)}{\longrightarrow} \{g\} \times G \stackrel{\varphi|_{\{g\}\times G}}{\longrightarrow} G$$

is continuous as it is the composition of continuous functions. By $\mu_g^{-1} = \mu_{g^{-1}}$ we see that the inverse function is continuous, too.

(c) Let $U \leq G$ be a open subgroup, and $g \in G - U$. Then $gU \subseteq G - U$ is open because left multiplication is a homeomorphism, and

$$G - U = \bigcup_{g\in G-U} g = \bigcup_{g\in G-U} gU$$

is a union of open sets, i.e. open, i.e. U is closed.
Next let $A \leq G$ be a closed subgroup of finite index. Then

$$G - A = \bigcup_{g\in G-A} g = \bigcup_{g\in G-A} gA = \bigcup_{g=1}^{n} gA$$

is a finite union of closed sets, hence $G - A$ is closed and A is open.
If G is compact, and $U \leq G$ an open subgroup, then $\{gU \in G/U\}$ define an open, disjoint cover of G which has a finite subcover, i.e. G/U is of finite index.

(d) H is a topological group since the subspace topology is defined that way. Let $\overline{V} \subseteq G/K$ be an open set. Then $V := \pi^{-1}(\overline{V})$ is open by definition of the quotient topology, and $\pi(V) = VK = \overline{V}$ since π is surjective. Now let $V \subseteq G$ be open. Then Vk is open for each $k \in K$ since right multiplication is a homeomorphism and thus open, hence

$$VK = \bigcup_{k\in K} Vk = \pi(V) \subseteq G/K$$

is open. So π is continuous and open. Set

$$\varphi\,:\,G/K \times G/K \longrightarrow G/K\,,\,\varphi(gK,hK) = gh^{-1}K$$

Let $\overline{V} \subseteq G/K$ be an open set, and $(gK,hK) \in \varphi^{-1}(\overline{V})$. Since $(g,h) \longmapsto \pi(gh^{-1}) = gh^{-1}K$ is continuous, there are open neighborhoods $V_g, V_h \subseteq G$ of g,h such that $V_gV_h^{-1} \subseteq \pi^{-1}(\overline{V})$. Since π is open, $\pi(V_g) \times \pi(V_h) = V_gK \times V_hK \subseteq G/K \times G/K$ is an open neighborhood of $(gK,hK) \in G/K \times G/K$. This proves that φ is continuous since $V_gK \times V_hK \subseteq \varphi^{-1}(\overline{V})$.

(e) An equivalent definition of a Hausdorff space is, that it is a topological space in which all singleton sets are the intersection of their closed neighborhoods. In particular $\{1\} \subseteq G$ is closed if G is Hausdorff.
Now let $\{1\}$ be closed. Since right multiplication is closed, all sets $\{ab^{-1}\} = \mu_{ab^{-1}}(1)$ are closed, too. Thus there are disjoint open neighborhoods $V_{\{1\}}, V_{\{ab^{-1}\}}$ in case $a \neq b$. Since right multiplication is open, $V_b = V_{\{1\}}b$ and $V_a = V_{\{ab^{-1}\}}b$ are disjoint open neighborhoods of a and b, i.e. G is a Hausdorff space. If G/K is Hausdorff, then $\{\overline{1}\} \subseteq G/K$ is closed, and so is $K = \pi^{-1}(\{\overline{1}\}) \subseteq G$ since π is continuous. If conversely $K \subseteq G$ is closed, then $G-K$ is open. Since π is open,

$$\pi(G-K) = \pi\left(\bigcup_{g\in G-K} g\right) = \bigcup_{g\notin K} \pi(g) = \bigcup_{g\notin K} gK = \bigcup_{\overline{g}\neq 1} \overline{g} = G/K - \{\overline{1}\}$$

is open, too, and $\{\overline{1}\} \subseteq G/K$ is closed, i.e. G/K is Hausdorff.
Finally, G is totally disconnected, if the empty set and all singleton sets are the only connection components. But these are always closed, so $\{1\}$ is closed and G is Hausdorff.

(f) Clearly

$$Z := Y \cdot \left(\bigcap_{i \in I} X_i \right) \subseteq \bigcap_{i \in I} Y X_i$$

Assume there is an element $g \notin Z$, then $Y^{-1}g \cap \left(\bigcap_{i\in I} X_i g\right) = \emptyset$ since otherwise there would be an element $h = y^{-1}g$ for some $y \in Y$ and $h \in X_i$ for all $i \in I$, i.e. $g = yh \in Z$. Since G is compact and $Y^{-1}g, X_i\,(i \in I)$ are all closed with empty intersection, their complements build an open cover of G, from which finitely many will do. In any case, their complements intersect to the empty set, hence $Y^{-1}g \cap (\cap_{i=1}^n X_i) = \emptyset$. Now by our hypothesis we can recursively find a $k \in I$ such that $X_k \in X_i$ for all $i = 1, \ldots, n$. If $g = yx \in YX_k$, then $y^{-1}g \in Y^{-1}g \cap X_k \subseteq Y^{-1}g \cap (\cap_{i=1}^n X_i)$, a contradiction. Thus $g \notin YX_k$, i.e. $g \notin \bigcap_{i\in I} YX_i$ what had to be shown.

6. Let $(X_n, d_n)_{n\in\mathbb{N}_0}$ be a sequence of complete metric spaces, and let $(f_n)_{n\in\mathbb{N}_0}$ be a sequence of continuous functions $f_n : X_{n+1} \longrightarrow X_n$ such that the image $f_n(X_{n+1}) \subseteq (X_n, d_n)$ is dense for all $n \in \mathbb{N}_0$. Then

$$M_0 := \{v_0 \in X_0 \,|\, \exists\, (v_n)_{n\in\mathbb{N}} \,\forall\, n \in \mathbb{N} \,:\, v_n \in X_n \,\wedge\, f_{n-1}(v_n) = v_{n-1}\}$$

and

$$M_0 \subseteq M := \bigcap_{n=0}^{\infty} (f_0 \circ f_1 \circ \ldots \circ f_n)(X_{n+1})$$

are dense in (X_0, d_0). In particular $M \neq \emptyset$ in case $X_0 \neq \emptyset$.

Reason: Mittag-Lefler theorem.

Solution: Let $x \in X_0$ and $\varepsilon > 0$. We want to show that there is a $v_0 \in M_0$ such that $d_0(x, y) \leq \varepsilon$. We begin by constructing inductively a sequence $(y_n)_{n\in\mathbb{N}_0}$ with the properties

$$y_n \in X_n \,\wedge\, d_n(y_n, f_n(y_{n+1})) \leq \frac{\varepsilon}{2^{n+1}} \quad (1)$$

$$d_k((f_k \circ f_{k+1} \circ \ldots \circ f_{n-1})(y_n), (f_k \circ f_{k+1} \circ \ldots \circ f_n)(y_{n+1})) \leq \frac{\varepsilon}{2^{n+1}} \quad (2)$$

for all $n \in \mathbb{N}_0$ and $0 \leq k < n$. We set $y_0 := x$ and find $y_1 \in X_1$ with $d_0(y_0, f_0(y_1)) < \varepsilon/2$ by the density of $f_0(X_1) \subseteq X_0$. This satisfies both conditions in case $n = 0$.
Now assume we have constructed the points $y_0, \ldots, y_m$ for some $m \in \mathbb{N}$ such that the conditions hold for $0 \leq n < m$ and $0 \leq k < n$. Since

$f_m(X_{m+1}) \subseteq X_m$ is dense, there is a sequence $(z_j)_{j\in\mathbb{N}} \subseteq X_{m+1}$ with $\lim_{j\to\infty} f_m(z_j) = y_m$. By continuity of $f_0, f_1, \ldots$ we also have for all $k = 0, \ldots, m-1$

$$\lim_{j\to\infty} d_k((f_k \circ \ldots \circ f_{m-1})(y_m), (f_k \circ \ldots \circ f_m)(z_j)) = 0$$

Hence there is a $j_0 \in \mathbb{N}$ such that with $y_{m+1} := z_{j_0}$ both conditions hold even for $n = m$ and $0 \leq k < m$. We have thus constructed the required sequence.

For all $k, j \in \mathbb{N}_0$ define

$$u_{k,0} := y_k \ \wedge \ u_{k,j} := (f_k \circ \ldots \circ f_{k+j-1})(y_{k+j}).$$

By induction, condition (2), and the triangle inequality

$$\begin{aligned} d_k(u_{k,j}, u_{k,j+p}) &\leq \sum_{m=1}^{p} d_k(u_{k,j+m-1}, u_{k,j+m}) \\ &\leq \frac{\varepsilon}{2^{k+j}} \sum_{m=1}^{p} \frac{1}{2^m} \\ &< \frac{\varepsilon}{2^{k+j}} \xrightarrow{j\to\infty} 0 \quad (3) \end{aligned}$$

So all sequences $(u_{k,j})_{j\in\mathbb{N}_0} \subseteq (X_k, d_k)$ for $k \in \mathbb{N}_0$ are Cauchy sequences in a complete metric spaces, i.e. they converge:

$$\lim_{j\to\infty} u_{k,j} =: v_k \in X_k$$

and thus for all $k \in \mathbb{N}_0$

$$\begin{aligned} \lim_{j\to\infty} f_k(u_{k+1,j}) &= \lim_{j\to\infty} f_k(f_{k+1} \circ \ldots \circ f_{k+j})(y_{k+j+1}) \\ &= \lim_{j\to\infty} u_{k,j+1} \\ &= v_k \\ &= f_k(\lim_{j\to\infty} u_{k+1,j}) \\ &= f_k(v_{k+1}) \end{aligned}$$

In particular $v_0 \in M_0$ and by continuity of the metric d_0 and (3) for $k = j = 0$

$$d_0(x, v_0) = d_0(y_0, v_0) = \lim_{j\to\infty} d_0(u_{0,0}, u_{0,j}) \leq \limsup_{j\to\infty} \varepsilon \sum_{m=1}^{j} \frac{1}{r^m} = \varepsilon$$

7. Prove for all $x > -1$
$$x - (1+x)\log(1+x) \leq -\frac{3x^2}{2(x+3)}$$

Reason: Logarithmic inequality.

Solution:

$$\begin{aligned}
f(x) &:= x - (1+x)\log(1+x) \\
f'(x) &= 1 - \log(1+x) - (1+x)\cdot\frac{1}{1+x} = -\log(1+x) \\
f''(x) &= -\frac{1}{1+x} \\
g(x) &:= -\frac{3x^2}{2(x+3)} \\
g'(x) &= -\frac{6x\cdot 2(x+3) - 3x^2\cdot 2}{4(x+3)^2} = -\frac{3x(x+6)}{2(x+3)^2} \\
g''(x) &= -\frac{(6x+18)(2(x+3)^2) - (3x^2+18x)(4(x+3))}{4(x+3)^4} \\
&= -\frac{12(x+3)^2 - 12x^2 - 72x}{4(x+3)^3} = -\frac{27}{(x+3)^3}
\end{aligned}$$

It is $f(0) = f'(0) = g(0) = g'(0) = 0$ and for $x > -1$

$$\begin{aligned}
\frac{1}{g''(x)} &= -\frac{(x+3)^3}{27} = -\frac{1}{27}\cdot(x+3)(x^2+6x+9) \\
&= -\frac{1}{27}(x^2(x+9) + 27x + 27) < -\frac{1}{27}(27x+27) \\
&= -1 - x = \frac{1}{f''(x)} < 0 \\
f''(x) &< g''(x) < 0
\end{aligned}$$

For $x \geq 0$ is
$$f(x) = \int_0^x \int_0^t f''(s)\,ds\,dt < \int_0^x \int_0^t g''(s)\,ds\,dt = g(x)$$
which is equally true for $-1 < x < 0$ with exchanged integral limits.

8. Let $(\Omega, \mathcal{A}, \mathcal{P})$ be a probability space, B, T, σ positive real numbers, and $n \in \mathbb{N}$. For independently distributed random variables $X_1, \ldots, X_n$:

$\Omega \longrightarrow \mathbb{R}$ with expectation values $E(X_k) = 0$ and $E(X_k^2) \leq \sigma^2$, and boundary $\|X_k\|_\infty \leq B$ for all $k = 1, \ldots, n$ prove

$$P\left(\frac{1}{n}\sum_{k=1}^{n} X_k \geq \sqrt{\frac{2\sigma^2 T}{n}} + \frac{2BT}{3n}\right) \leq e^{-T}.$$

Reason: Bernstein inequality.

Solution: Set $\varepsilon := \dfrac{\sqrt{18Tn\sigma^2 + T^2B^2} + TB}{3n} = \sqrt{\dfrac{2T\sigma^2}{n} + \dfrac{T^2B^2}{9n^2}} + \dfrac{TB}{3n}$.

Assume $\sqrt{\alpha + \beta^2} + \beta > \sqrt{\alpha} + 2\beta$ for $\alpha, \beta > 0$. Then $\alpha + \beta^2 > \alpha + \beta^2 + 2\beta\sqrt{\alpha}$ which isn't possible for positive numbers. Thus we have

$$\varepsilon \leq \sqrt{\frac{2\sigma^2 T}{n}} + \frac{2TB}{3n}$$

Rearrangement of the definition of ε for T is

$$\begin{aligned}
(3n\varepsilon - TB)^2 = 9n^2\varepsilon^2 - 6n\varepsilon TB + T^2B^2 &= 18Tn\sigma^2 + T^2B^2 \\
3n\varepsilon^2 &= T(6\sigma^2 + 2\varepsilon B) \\
T &= \frac{3n\varepsilon^2}{6\sigma^2 + 2\varepsilon B}
\end{aligned}$$

The Markov inequality says that for a monotone increasing function $f : \mathbb{R} \longrightarrow [0, \infty)$ and a constant $a \in \mathbb{R}$

$$f(a) \cdot P(X \geq a) \leq E(f(X))$$

and in particular for $f(a) > 0$

$$P(X \geq a) \leq \frac{E(f(X))}{f(a)}.$$

Applied to $X := n^{-1}\sum_{i=1}^{n} X_i$ and $f(\varepsilon) := e^{tn\varepsilon}$ for some $t > 0$ which will be specified later in the proof, we get

$$P\left(X \geq \sqrt{\frac{2\sigma^2 T}{n}} + \frac{2TB}{3n}\right) \leq P(X \geq \varepsilon) \leq e^{-tn\varepsilon} E\left(\prod_{i=1}^{n} \exp(tX_i)\right)$$

The random variables are independent, so we may change the order of products and expectation values. $\exp(tX_i)$ is bounded by the integrable upper bound e^{tB}. Hence we can change the order of summation and expectation value, too. With $X_i^0=1$ and $E(X_i)=0$ we have

$$\begin{aligned} e^{-tn\varepsilon}E\left(\prod_{i=1}^n \exp(tX_i)\right) &= e^{-tn\varepsilon}\prod_{i=1}^n E\left(\sum_{k=0}^\infty \frac{t^k}{k!}X_i^k\right) \\ &= e^{-tn\varepsilon}\prod_{i=1}^n \left(1+\sum_{k=2}^\infty \frac{t^k}{k!}E(X_i^k)\right) \\ &\stackrel{(1)}{\leq} e^{-tn\varepsilon}\prod_{i=1}^n \left(1+\sum_{k=2}^\infty \frac{t^k}{k!}\sigma^2 B^{k-2}\right) \\ &= e^{-tn\varepsilon}\left(1+\frac{\sigma^2}{B^2}\left(e^{tB}-tB-1\right)\right)^n \\ &\stackrel{(2)}{\leq} e^{-tn\varepsilon}\cdot \exp\left(\frac{n\sigma^2}{B^2}\left(e^{tB}-tB-1\right)\right) \end{aligned}$$

$$\begin{aligned} &(1)\quad E(X_i^k)\leq E(X_i^2)B^{k-2}\leq \sigma^2 B^{k-2} \\ &(2)\quad (1+x)^n=\sum_{k=0}^n \frac{n!}{(n-k)!}\cdot\frac{x^k}{k!}\leq \sum_{k=0}^n \frac{n^kx^k}{k!}\leq e^{nx} \end{aligned}$$

Now we choose $t:=\dfrac{1}{B}\log\left(1+\dfrac{\varepsilon B}{\sigma^2}\right)>0$ and get

$$\begin{aligned} &e^{-tn\varepsilon}\cdot\exp\left(\frac{n\sigma^2}{B^2}\left(e^{tB}-tB-1\right)\right) \\ &\quad=\exp\left(-\frac{\varepsilon n}{B}\log\left(1+\frac{\varepsilon B}{\sigma^2}\right)+\frac{n\sigma^2}{B^2}\left(1+\frac{\varepsilon B}{\sigma^2}-\log\left(1+\frac{\varepsilon B}{\sigma^2}\right)-1\right)\right) \\ &\quad=\exp\left(\frac{n\sigma^2}{B^2}\left(-\frac{\varepsilon B}{\sigma^2}\log\left(1+\frac{\varepsilon B}{\sigma^2}\right)+\frac{\varepsilon B}{\sigma^2}-\log\left(1+\frac{\varepsilon B}{\sigma^2}\right)\right)\right) \end{aligned}$$

Now we get by the previous Lemma for $x:=\dfrac{\varepsilon B}{\sigma^2}>0$

$$x-(1+x)\log(1+x)\leq -\frac{3x^2}{2x+6}$$

in total

$$\begin{aligned} &P\left(X\geq\sqrt{\frac{2\sigma^2T}{n}}+\frac{2TB}{3n}\right)\leq\exp\left(-\frac{n\sigma^2}{B^2}\cdot\frac{\frac{3\varepsilon^2B^2}{\sigma^4}}{\frac{2\varepsilon B}{\sigma^2}+6}\right) \\ &\quad=\exp\left(-\frac{3\varepsilon^2 n}{2\varepsilon B+6\sigma^2}\right)=e^{-T} \end{aligned}$$

9. Let $\mathbb{P}$ be the set of all primes, $p \in \mathbb{P}$, and $n \in \mathbb{N}$ a positive integer. $\operatorname{ord}_p(N)$ denotes the number of primes p which occur as divisor in $\{1, 2, \ldots, N\}$ counted by multiplicity. E.g. $N = 24 = 4!$ and $p = 3$ yields in $\{3 = 3^1, 6 = 3^1 \cdot 2, 9 = 3^2, 12 = 3^1 \cdot 4, 15 = 3^1 \cdot 5, 18 = 3^2 \cdot 2, 21 = 3^1 \cdot 7, 24 = 3^1 \cdot 8\}$

$$\operatorname{ord}_3(24) = 1 + 1 + 2 + 1 + 1 + 2 + 1 + 1 = 10$$

Prove

(a) $\operatorname{ord}_p(n) = \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor$

(b) $2 \mid \binom{2n}{n}$ and $p \mid \binom{2n}{n}$ for all $n < p \leq 2n$

(c) $p \geq 3 \wedge 2n/3 < p \leq n \implies p \nmid \binom{2n}{n}$

(d) $p^r \mid \binom{2n}{n} \implies p^r \leq 2n$

(e) $\frac{2^{2n-1}}{n} \leq \binom{2n}{n} \leq 2^{2n-1}$

(f) $\prod_{p \leq n} p < 4^n$

Reason: Primes.

Solution:

(a) The number of numbers in $\{1, 2, \ldots, n\}$ that are divisible by p is $\lfloor n/p \rfloor$. Among them are $\lfloor n/p^2 \rfloor$ many divisible by p^2, $\lfloor n/p^3 \rfloor$ divisible by p^3 etc.

(b) $\binom{2n}{n} = \binom{2n-1}{n-1} + \binom{2n-1}{n} = 2\binom{2n-1}{n-1} \implies 2 \mid \binom{2n}{n}$

$\binom{2n}{n} = \frac{2n \cdot \ldots \cdot (n+1)}{1 \cdot \ldots \cdot n}$ and a prime $n < p \leq 2n$ in the numerator doesn't cancel.

(c) From $p > 3$ we get $p^2 > 2n$ for $1 \leq n \leq 4$ and from $p > 2n/3$ we get $p^2 > 4n^2/9 > 20n/9 > 2n$ for all $n \geq 5$. Thus

$$\begin{aligned} \operatorname{ord}_p \binom{2n}{n} &= \operatorname{ord}_p \left(\frac{(2n)!}{(n!)^2} \right) = \operatorname{ord}_p((2n)!) - 2 \operatorname{ord}_p(n!) \\ &= \sum_{k \geq 1} \left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \sum_{k \geq 1} \left\lfloor \frac{n}{p^k} \right\rfloor = \left\lfloor \frac{2n}{p} \right\rfloor - 2 \left\lfloor \frac{n}{p} \right\rfloor \\ &= 2 - 2 \cdot 1 = 0 \end{aligned}$$

which means that $p \nmid \binom{2n}{n}$

(d) Every term of the sum

$$\operatorname{ord}_p \binom{2n}{n} = \sum_{k\geq 1} \left\{ \left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right\}$$

is either 0 or 1 because for all real numbers x it is $\lfloor 2x \rfloor - 2\lfloor x \rfloor \in \{0,1\}$. Thus $\lfloor 2n/p^k \rfloor = 0$ for

$$k > r_p := \left\lfloor \log_p(2n) \right\rfloor$$

implies $\operatorname{ord}_p \binom{2n}{n} \leq r_p$, i.e. $p^r \leq p^{r_p} \leq 2n$.

(e)

$$(1+1)^{2n-1} = \binom{2n-1}{0} + \ldots + \underbrace{\binom{2n-1}{n-1} + \binom{2n-1}{n}}_{\leq \binom{2n}{n} = 2^{2n-1}} + \ldots + \binom{2n-1}{2n-1}$$

and $\binom{2n-1}{n-1} = \binom{2n-1}{n} \geq \dfrac{2^{2n-1}}{2n}$, i.e. $\binom{2n}{n} = 2\binom{2n-1}{n} \geq \dfrac{2^{2n-1}}{n}$.

(f) Set $P(n) := \prod_{p\leq n} p$. The statement is obviously true for $n = 1, 2$, so we may assume that $P(k) < 4^k$ for all $k < n$ and $n \geq 3$. If n is even, then by induction hypothesis $P(n) = P(2m) = P(2m-1) = P(n-1) < 4^{n-1} < 4^n$. So let $n = 2m-1$. we have seen that

$$\forall\, m < p \leq 2m \;:\; 2\cdot p \,|\, \binom{2m}{m} \Rightarrow 2 \left(\prod_{m<p\leq 2m} p \right) \,|\, \binom{2m}{m} \leq 2^{2m-1}$$

$$\Longrightarrow \prod_{m<p\leq 2m} p \leq 2^{2m-2} = 4^{m-1}$$

$$\Longrightarrow P(n) = P(2m-1) = P(m) \cdot \prod_{m<p<2m} p < 4^m \cdot 4^{m-1} = 4^n$$

10. Let K be compact and $C(K) := \{f : K \to \mathbb{R} \text{ or } \mathbb{C} \,|\, f \text{ is continuous}.$ A $n-$dimensional subspace $M \subseteq C(K)$ is called Haar space, if all $f \in M - \{0\}$ have at most $n-1$ zeros. Linear independent functions $S := \{\varphi_1, \ldots, \varphi_n\} \subseteq C(K)$ are called a Chebyshev- or Haar-system, if $\operatorname{span}(S)$ is a Haar space. We denote the (compact) unit circle $\mathbb{T} := \{e^{2\pi i t} \,|\, t \in [0,1)\}$. Let $K \subseteq \mathbb{R}$ be compact or $K = \mathbb{T}$, $f \in C(K)$.

    We call a point $\xi \in K$ with $f(\xi) = 0$ a simple zero of f if ξ is either on the boundary of K or f changes sign in ξ. If $f(\xi - t)f(\xi + t) > 0$ in a neighborhood of ξ, then we speak of a double zero.

(a) A subspace $M \subseteq C(K)$ with $\dim M = n$ is a Haar space if and only if each $f \in M - \{0\}$ that has $j \in \mathbb{N}_0$ simple zeros and $k \in \mathbb{N}_0$ double zeros holds
$$j + 2k < n.$$
So each element $f \in M - \{0\}$ has at most $n - 1$ different zeros.

(b) The space of all real-valued trigonometric polynomials on $[0, 1)$ of degree at most n is a Haar space of dimension $2n + 1$.

(c) Let $n \in \mathbb{N}_0,\ p \in T_n$, and $x \in \mathbb{T}$. Then
$$|p'(x)| \leq 2\pi n \sqrt{\|p\|_\infty^2 - |p(x)|^2}.$$
Remark: Consider the linear differential operator $D(p) = p'$ on T_n. From $|D(\sin(2\pi nx))| = |2\pi n \cos(2\pi nx)|$ we conclude that
$$2\pi n \leq \|D\| = \sup_{\|p\|_\infty \leq 1} \|p'\|_\infty = \sup_{\|p\|_\infty = 1} \sup_{x \in \mathbb{T}} |p'(x)| < \infty$$
because T_n is finite-dimensional.

Reason: Szegö's inequality.

Solution:

(a) We only have to show $j + 2k < n$ holds for $f \neq 0$ in a Haar space. Assume $\xi_1, \ldots, \xi_j \in K$ are the simple zeros of f and $\eta_1, \ldots, \eta_k \in K$ the double zeros, and that
$$j + 2k \geq n$$
Set $A_0(f) := \{\xi_1, \ldots, \xi_j, \eta_1, \ldots, \eta_k\}$. Then $\#A_0(f) = j + k \leq n - 1$ by definition of a Haar space. In particular $k \geq 1$. We choose an interval $[\eta_i - \delta_i, \eta_i + \delta_i] \subseteq K$ with $\delta_i > 0$ around each double zero of f, such that no further zeros are contained, and set
$$\begin{aligned} c_i &:= \operatorname{sgn} f(\eta_i - \delta_i) = \operatorname{sgn} f(\eta_i + \delta_i) \\ C &:= \min_{1 \leq i \leq k} \{|f(\eta_i - \delta_i)|\,,\, |f(\eta_i + \delta_i)|\} \end{aligned}$$
We construct an interpolation function $q \in M$ by adding arbitrary points $\theta_1, \ldots, \theta_{n-j-k} \in K - A_0(f)$ such that
$$q(\eta_i) = c_i\,(1 \leq i \leq k),\ q(\xi_i) = 0\,(1 \leq i \leq j),\ q(\theta_i) = 0\,(1 \leq i \leq n-j-k).$$

The functions $f_\alpha := f - \alpha q \in M$ for $0 < \alpha < \dfrac{C}{\|q\|_\infty}$ have function values

$$f_\alpha(\xi_i) = 0\,(1 \leq i \leq j),\; f_\alpha(\eta_i) = -\alpha c_i \neq 0\,(1 \leq i \leq k),$$

and sign changes

$$c_i = \operatorname{sgn} f_\alpha(\eta_i - \delta_i) = -\operatorname{sgn} f_\alpha(\eta_i) = \operatorname{sgn} f_\alpha(\eta_i + \delta_i).$$

Thus we have two zeros of f_α in each interval $[\eta_i - \delta_i, \eta_i + \delta_i]$, and f_α has at least $j + 2k \geq n$ zeros, contradicting the Haar condition for f_α.

(b) Set $z := e^{2\pi i x} \in \mathbb{C}$. Each trigonometric polynomial $f \in T_n - \{0\}$ has the form

$$f(x) = \sum_{k=-n}^{n} c_k e^{2\pi i k x} = \sum_{k=-n}^{n} c_k z^k = z^{-n} \sum_{k=0}^{2n+1} c_{k-n} z^k$$

with coefficient vector $(c_{-n}, \ldots, c_n) \neq 0$. The last sum is a polynomial $q \neq 0$ of degree $2n+1$. It has at most $2n$ complex zeros which may be in $\mathbb{T}$. Hence $f(x)$ has at most $2n$ zeros in $[0,1)$.

(c) Set $q(x) := \dfrac{p(x)}{\|p\|_\infty}$. Then for all $\|q\|_\infty = 1$

$$|p'(x)| \leq 2\pi n\sqrt{\|p\|_\infty^2 - |p(x)|^2} \Longleftrightarrow |q'(x)| \leq 2\pi n\sqrt{1 - |q(x)|^2}.$$

We will first show that there are no $p \in T_n, x_0 \in \mathbb{T}$ such that

$$\|p\|_\infty < 1\;,\; |p'(x_0)| = 2\pi n\sqrt{1 - |p(x_0)|^2}$$

Assume there is. We may assume w.l.o.g. that the condition holds at $x_0 = 0$, for otherwise, we shift the periodic function, and we assume $p'(x_0) = p'(0) \geq 0$ by choice of sign.

We choose an $\alpha \in \left(-\dfrac{1}{4n}, \dfrac{1}{4n}\right)$ with $p(0) = \sin(2\pi n\alpha)$ which is possible since $|p(0)| \leq \|p\|_\infty < 1$.

Now define $q(x) := \sin(2\pi n(x + \alpha)) - p(x) \in T_n$. If $q(x) \equiv 0$, then $1 > \|p\|_\infty = \|\sin(2\pi n(x+\alpha))\|_\infty = 1$ which is a contradiction. Hence $q(x) \neq 0$.

$$\begin{aligned} q(0) = q'(0) &= 2\pi n\cos(2\pi n\alpha) - p'(0) \\ &= 2\pi n\cos(2\pi n\alpha) - 2\pi n\sqrt{1 - |p(0)|^2} = 0 \end{aligned}$$

i.e. we have a double zero at $x=0$. The points

$$x_k := \alpha + \frac{2k+1}{4n}\,,\, 0 \leq k \leq 2n-1$$

are pairwise distinct in $(0,1)$. These points are extreme values of $q(x)-p(x)) = \sin(2\pi n(x-\alpha))$, so for $0 \leq k \leq 2n-1$

$$\operatorname{sgn}(q(x_k)-p(x_k)) = \operatorname{sgn}\left(\sin\left(\frac{\pi}{2}\cdot(2k+1)\right)\right) = (-1)^k$$

Since $|p(x_k)|<1$, we have $\operatorname{sgn}(q(x_k)-p(x_k)) = \operatorname{sgn}(q(x_k))$ which by the mean value theorem means that $q(x) \in T_n - \{0\}$ has at least $2n-1$ zeros in $(0,1)$, which together with the double zero at $x=0$ gives $2n+1$ zeros counted by multiplicities, and contradicting the Haar condition. We could also conclude by the previous part that

$$2n-1+2\cdot 1 = 2n+1 < 2n+1$$

which is also a contradiction.

Thus we have proven, that for all $p \in T_n - \{0\}$ that for all $x \in [0,1)$

$$\|p\|_\infty \geq 1 \;\vee\; |p'(x)| \neq 2\pi n\sqrt{1-|p(x)|^2}$$

Let $p \in T_n - \{0\}$ and $\lambda \in \left[0, \dfrac{1}{\|p\|_\infty}\right) \subseteq [0,1)$, so $\|\lambda p\|_\infty < 1$. Let

$$f(\lambda, x) := |\lambda p'(x)| - 2\pi n\sqrt{1-|\lambda p(x)|^2} \neq 0$$

because $\lambda p \in T_n$. By continuity of $f(\cdot, x)$, and $f(0,x) = -2\pi n < 0$ we get from the intermediate value theorem that $f(\lambda, x) < 0$ for all $\lambda \in \left[0, \dfrac{1}{\|p\|_\infty}\right)$ and

$$\lim_{\lambda \to \|p\|_\infty^{-1}} f(\lambda, x) \leq 0$$

i.e.

$$\left|\frac{p'(x)}{\|p\|_\infty}\right| \leq 2\pi n\sqrt{1-\left|\frac{p(x)}{\|p\|_\infty}\right|^2}$$

what had to be shown.

11. (HS-1) Let S be a set of real numbers which is closed under multiplication (that is, if a and b are in S, then so is ab). Let T and U be disjoint subsets of S whose union is S. Given that the product of any three (not necessarily distinct) elements of T is in T and that the product of any three elements of U is in U, show that at least one of the two subsets T, U is closed under multiplication.

    Reason: Logic.

    Solution: Suppose on the contrary that there exist $t_1, t_2 \in T$ with $t_1t_2 \in U$ and $u_1, u_2 \in U$ with $u_1u_2 \in T$. Then $(t_1t_2)u_1u_2 \in U$ while $t_1t_2(u_1u_2) \in T$, a contradiction.

12. (HS-2) Suppose we have a necklace of n beads. Each bead is labeled with an integer and the sum of all these labels is $n-1$. Prove that we can cut the necklace to form a string whose consecutive labels $x_1, x_2, \ldots, x_n$ satisfy

$$\sum_{i=1}^{k} x_i \leq k-1 \quad (k = 1, \ldots, n).$$

    Reason: Cycles.

    Solution: Let $S_k = x_1 + \ldots + x_k - \dfrac{k(n-1)}{n}$, so that $S_n = S_0 = 0$. These form a cyclic sequence that doesn't change when you rotate the necklace, except that the entire sequence gets translated by a constant. In particular, it makes sense to choose x_i for which S_i is maximal and make that one x_n; this way $S_i \leq 0$ for all i, and thus $x_1 + \ldots + x_i \leq i \cdot \dfrac{n-1}{n}$. However, the right side may be replaced by $i-1$ because the left side is an integer.

13. (HS-3) Let $d := d_1d_2\ldots d_9$ be a number with not necessarily distinct nine decimal digits. A number $e := e_1e_2\ldots e_9$ is such that each of the nine digit numbers formed by replacing just one of the digits d_j by the corresponding digit e_j is divisible by 7 for all $1 \leq j \leq 9$. A number $f := f_1f_2\ldots f_9$ is formed the same way by starting with e, i.e. each of the nine numbers formed by replacing a e_k by f_k is divisible by 7. Example: If $d = 20210901$ then $e_6 \in \{0, 7\}$ since $7 \mid 20210001$ and $7 \mid 20210701$. Show that, for each j, $d_j - f_j$ is divisible by 7.

    Reason: Numbers.

    Solution: We are given that for all $1 \leq j \leq 9$

$$(e_j - d_j)10^{9-j} + d \equiv 0 \equiv (f_j - e_j)10^{9-j} + e \mod 7 \quad (*)$$

Thus $\sum_{j=1}^{9}(e_j-d_j)10^{9-j}+d=e-d+9d\equiv e+d\equiv 0 \mod 7$. Now add the first and second relation from $(*)$ for any particular value j and get

$$0\equiv (f_j-d_j)10^{9-j}+e+d\equiv (f_j-d_j)10^{9-j} \mod 7$$

Because 7 is prime and $7\nmid 10^{9-j}$ this implies $7\,|\,(d_j-f_j)$.

14. (HS-4) An ellipse, whose semi-axes have lengths a and b, rolls without slipping on the curve $y=c\sin(x/a)$. How are a,b,c related, given that the ellipse completes one revolution when it traverses one period of the curve?

    Reason: Analytical geometry.

    Solution: Without slipping means that the perimeter of the ellipse equals the length of one period of the sine curve, which translates to the integral equation

    $$\int_0^{2\pi}\sqrt{(-a\sin(\theta))^2+(b\cos(\theta))^2}\,d\theta=\int_0^{2\pi a}\sqrt{1+\frac{c}{a}\cos\left(\frac{x}{a}\right)}\,dx$$

    Let $\theta=\dfrac{x}{a}$ in the second integral, $1=\sin^2\theta+\cos^2\theta$, then

    $$\int_0^{2\pi}\sqrt{a^2\sin^2(\theta)+b^2\cos^2(\theta)}\,d\theta=\int_0^{2\pi}\sqrt{a^2\sin^2\theta+(a^2+c^2)\cos^2\theta}\,d\theta$$

    Since the left side is an increasing function in b, and the right side doesn't explicitly depend on b, we must have equality if and only if $b^2=a^2+c^2$.

15. (HS-5) For a partition π of $N:=\{1,2,\ldots,9\}$, let $\pi(x)$ be the number of elements in the part containing x. Prove that for any two partitions π_1 and π_2, there are two distinct numbers x and y in N such that $\pi_j(x)=\pi_j(y)$ for $j=1,2$.

    Reason: Sets.

    Solution: For a given partition π_1, no more than three different values of $\pi_1(x)$ are possible, since four would require one part each of size at least $1,2,3,4$, and that's already more than 9 elements. If no such x,y exist, each pair $(\pi_1(x),\pi_2(x))$ occurs for at most one element of x, since there are only $3\cdot 3$ possible pairs, and each must occur exactly once. In particular, each value of $\pi_1(x)$ must occur 3 times. However, any given value of $\pi_1(x)$ occurs $C\cdot\pi(x)$ times, where C is the number of distinct partitions of that size. Thus $\pi_1(x)$ can occur 3 times only if it equals 1 or 3, but we have three distinct values for which it occurs, a contradiction.

5 August 2021

1. Let (X, ρ) be a metric space, and suppose that there exists a sequence $(f_i)_i$ of real-valued continuous functions on X with the property that a Cauchy sequence $(x_n)_n$ is convergent whenever each of the sequences $(f_i(x_n))_i$ is bounded. Then X can be remetrized (with equivalent metrics) so as to be complete.

   Reason: Metric spaces.

   Solution: Define a new distance function in X by

   $$\sigma(x,y) = \rho(x,y) + \sum_{i=1}^{\infty} \frac{1}{2^i} \min\{1, |f_i(x) - f_i(y)|\}$$

   which is a metric because the triangle axiom is satisfied by each term. The other axioms are obvious.

   For any $\varepsilon > 0$ and $x \in X$ there is an integer N such that $2^{-N} < \varepsilon$ and a positive number $\delta < \varepsilon$ such that

   $$\rho(x,y) < \delta \Longrightarrow |f_i(x) - f_i(y)| < \varepsilon \quad (i = 1, 2, \ldots, N)$$

   If $\rho(x,y) < \delta$, then

   $$\sigma(x,y) < \varepsilon + \sum_{i=1}^{N} \frac{1}{2^i} \min\{1, |f_i(x) - f_i(y)|\} + \frac{1}{2^N} < 3\varepsilon.$$

   Therefore $\sigma(x, x_n) \to 0$ whenever $\rho(x, x_n) \to 0$. The converse follows from the inequality $\rho(x,y) \leq \sigma(x,y)$. Thus σ and ρ are equivalent metrics.

   To show that (X, σ) is complete, let $(x_n)_n$ be a Cauchy sequence relative to σ. Then for any natural number k there is a natural number N such that $\sigma(x_n, x_m) < 2^{-k}$ for all $n, m \geq N$. For all $n, m \geq N$, we have

   $$1 > 2^k \sigma(x_n, x_m) \geq \min\{1, |f_k(x_n) - f_k(x_m)|\},$$

   and therefore $|f_k(x_n) - f_k(x_m)| < 1$. Let $M(k) := \max\{|f_k(x_1)|, \ldots, |f_k(x_N)|\}$.

   $$\begin{aligned} |f_k(x_n)| &= |f_k(x_n) - f_k(x_N) + f_k(x_N)| \\ &\leq |f_k(x_n) - f_k(x_N)| + |f_k(x_N)| \\ &< 1 + M(k) \end{aligned}$$

   and the sequence $(f_k(x_n))_n$ is bounded, for each k. Since $\rho(x,y) \leq \sigma(x,y)$, the sequence $(x_n)_n$ is also a Cauchy sequence relative to ρ, and by hypothesis, convergent.

2. Let $X = C([0,1])$ be the topological space of real-valued continuous functions,
$$\rho(f,g) := \sup_{x\in[0,1]} |f(x)-g(x)|$$
the uniform metric induced by the L^∞ norm,
$$\sigma(f,g) := \int_0^1 |f(x)-g(x)|\,dx$$
the L^1 induced metric, and for $n \in \mathbb{N}$
$$E_n := \{\, f \in X \mid \exists\, x \in [0,1-1/n]\ \forall\, h \in (0,1-x)\ :\ |f(x+h)-f(x)| \leq nh \}\,.$$
Show that

(a) (X,ρ) is complete.

(b) $(X,\rho) \ncong (X,\sigma)$ is not complete.

(c) $E_n \subseteq (X,\rho)$ is closed.

Reason: Topology.

Solution:

(a) ρ is called uniform metric, because convergence in this metric implies uniform convergence. Let $(f_n) \subseteq (X,\rho)$ be a Cauchy sequence, say $\rho(f_i,f_j) < \varepsilon$ for all $i,j > N(\varepsilon)$. Then
$$|f_i(x)-f_j(x)| < \varepsilon \text{ for all } i,j > N(\varepsilon) \text{ and } x \in [0,1].$$
Hence $(f_n(x)) \subseteq \mathbb{R}$ is a Cauchy sequence for all $x \in [a,b]$, and therefore converging to a limit $f(x)$. Letting $j \to \infty$ we see that $|f_i(x)-f(x)| < \varepsilon$ for all $i > N(\varepsilon)$ and all $x \in [0,1]$. Thus (f_i) converges uniformly on $[0,1]$. Let $x_0 \in [0,1]$ and $\rho(f_M,f) < \varepsilon/3$. Since f_M is continuous at x_0, there is a $\delta > 0$ such that
$$|f_M(x)-f_M(x_0)| < \varepsilon/3 \text{ for all } |x-x_0| < \delta.$$
Hence
$$\begin{aligned}|f(x)-f(x_0)| &\leq |f(x)-f_M(x)| + |f_M(x)-f_M(x_0)| + |f_M(x_0)-f(x_0)| \\ &\leq \rho(f,f_M) + \varepsilon/3 + \rho(f_M,f) < \varepsilon,\end{aligned}$$
i.e. $f(x)$ is continuous at any $x_0 \in [0,1]$ and $f_n \to f$ in C. This shows that (X,ρ) is complete.

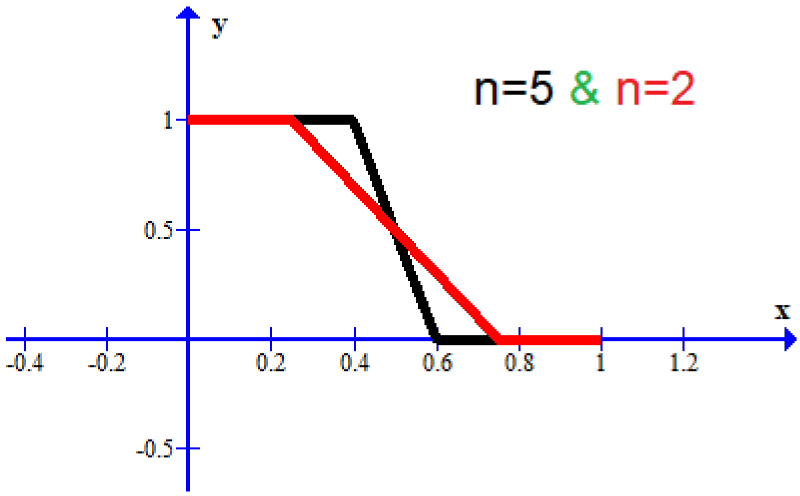
(b) Consider $f_n(x) := \max\{1 - nx, 0\}$ and let $f \equiv 0$. Then we get for $n > 1$

$$\sigma(f_n, f) = \int_0^1 |\max\{1-nx, 0\}|\, dx = \int_0^{1/n} |1-nx|\, dx = \frac{1}{n} - \frac{n}{2n^2} = \frac{1}{2n}$$

whereas $\rho(f_n, f) = 1$. Thus $f_n \to f$ in (X, σ) but not in (X, ρ), hence these spaces are not homeomorphic.

To see that (X, σ) is not complete, let

$$f_n(x) := \begin{cases} \min\left\{1\,,\, \frac{1}{2} - n\left(x - \frac{1}{2}\right)\right\} & \text{on } \left[0, \frac{1}{2}\right] \\ \max\left\{0\,,\, \frac{1}{2} - n\left(x - \frac{1}{2}\right)\right\} & \text{on } \left[\frac{1}{2}, 1\right] \end{cases}$$



$$\sigma(f_n - f_m) = \frac{1}{4} \cdot \left| \frac{1}{n} - \frac{1}{m} \right|$$

and (f_n) is a Cauchy sequence. Suppose $\sigma(f_n, f) \to 0$ as $n \to \infty$ for some $f \in C([0, 1])$. Then

$$\begin{aligned} \sigma(f_n, f) &= \int_0^1 |f_n(x) - f(x)|\, dx \\ &\geq \int_0^{\frac{1}{2}-\frac{1}{2n}} |f_n(x) - f(x)|\, dx + \int_{\frac{1}{2}+\frac{1}{2n}}^1 |f_n(x) - f(x)|\, dx \\ &\geq \int_0^{\frac{1}{2}-\frac{1}{2n}} |1 - f(x)|\, dx + \int_{\frac{1}{2}+\frac{1}{2n}}^1 |f(x)|\, dx \end{aligned}$$

Letting $n \to \infty$ it follows that

$$\int_0^{\frac{1}{2}} |1 - f(x)|\, dx = \int_{\frac{1}{2}}^1 |f(x)|\, dx = 0.$$

Since $f(x)$ is continuous, we must have $f(x) = 1$ on $[0, 1/2]$ and $f(x) = 0$ on $[1/2, 1]$, which is impossible. Therefore (X, σ) cannot be complete.

(c) Let $(f_k) \subseteq E_n$ be a sequence that converges to $f \in (X, \rho)$. This is possible because $(X, \rho) \supseteq E_n$ is complete. Be definition of E_n we have a corresponding sequence $(x_k) \subseteq [0, 1 - (1/n)]$ and

$$|f_k(x_k + h) - f_k(x_k)| \leq nh \text{ for all } 0 < h < 1 - x_k\, .$$

We may assume also that $\lim_{k\to\infty} x_k = x \in [0, 1-(1/n)]$, for some suitable x. This condition can be achieved by choosing an appropriate subsequence of (f_k) and because $[0, 1 - (1/n)]$ is compact. If $0 < h < 1 - x$, the inequality $0 < h < 1 - x_k$ holds for all sufficiently large k, and then

$$\begin{aligned} |f(x+h) - f(x)| &\leq |f(x+h) - f(x_k + h)| + |f(x_k + h) - f_k(x_k + h)| \\ &\quad + |f_k(x_k + h) - f_k(x_k)| + |f_k(x_k) - f(x_k)| \\ &\quad + |f(x_k) - f(x)| \\ &\leq |f(x+h) - f(x_k + h)| + \rho(f, f_k) + nh + \rho(f_k, f) \\ &\quad + |f(x_k) - f(x)| \end{aligned}$$

Letting $k \to \infty$, and using the fact that f is continuous at x and $x + h$, it follows that

$$|f(x+h) - f(x)| \leq nh \text{ for all } 0 < h < 1 - x.$$

Therefore $f \in E_n$ and E_n is closed.

3. Show that the set of real algebraic numbers is infinite, and denumerable.

Reason: Countability.

Solution: Let us define the weight of a polynomial $f(x) = \sum_{i=0}^n a_i x^i$ to be the number $n + \sum_{i=0}^n |a_i|$. There are only a finite number of polynomials having a given weight. Arrange these in some order, say lexicographically (first in order of n, then in order of a_0, and so on). Every non-constant polynomial has a weight at least equal to 2. Taking the polynomials of weight 2 in order, then those of weight 3, and so on, we obtain a sequence $f_1, f_2, f_3, \ldots$ in which every polynomial has at most a finite number of real zeros. Number the zeros of f_1 in order, then those of f_2, and so on, passing over any that have already been numbered. In this way we obtain a definite enumeration of all real algebraic numbers. The sequence is infinite because it includes all rational numbers.

4. A topology $\mathcal{T}$ on a vector space L over a non-discrete topological field K defines a topological vector space, i.e. addition and scalar multiplication are continuous, if and only if $\mathcal{T}$ is translation-invariant (all mappings $x \mapsto x + x_0$ are homeomorphisms) and possesses a $0-$neighborhood base $\mathcal{B}$ with the following properties:

   (a) For each $V \in \mathcal{B}$, there exists $U \in \mathcal{B}$ such that $U + U \subseteq V$.

   (b) Every $V \in \mathcal{B}$ is radial (i.e. there exists a $\lambda_0 \in K$ such that whenever $|\lambda| \geq |\lambda_0|$ we have $F \subseteq \lambda V$ for each finite subset $F \subseteq L$) and circled ($\lambda V \subseteq V$ whenever $|\lambda| \leq 1$).

   (c) There exists $\lambda \in K$, $0 < |\lambda| < 1$, such that $V \in \mathcal{B}$ implies $\lambda V \in \mathcal{B}$.

   If K is an Archimedean valuated field, e.g. $K \in \{\mathbb{R}, \mathbb{C}\}$, then the last condition is dispensable.

   Reason: Topological vector spaces.

   Solution: First let $(L, \mathcal{T})$ be a topological vector space. We note that for each $x_0 \in L$ and each $\lambda_0 \in K - \{0\}$, the mapping $x \longmapsto \lambda_0 x + x_0$ is a homeomorphism of L onto itself. It is clearly onto L and, by continuity of scalar multiplication and addition, continuous with continuous inverse $y \longmapsto \lambda_0^{-1}(y - x_0)$. Given a $0-$neighborhood W in L, there exists a $0-$neighborhood U and a real number $\varepsilon > 0$ such that $\lambda U \subseteq W$ whenever $|\lambda| < \varepsilon$ since scalar multiplication is continuous; hence since K is non-discrete, $V := \cup\{\lambda U \,|\, |\lambda| < \varepsilon\}$ is a $0-$neighborhood which is contained in W, and obviously circled. This the family $\mathcal{B}$ of all circled $0-$neighborhoods in L is a base at 0. The continuity at $\lambda = 0$ of $(\lambda, x_0) \longrightarrow \lambda x_0$ for each $x_0 \in L$ implies that every $V \in \mathcal{B}$ is radial. It is obvious from continuity of addition that $\mathcal{B}$ satisfies the first condition. Given $V \in \mathcal{B}$, and since K is non-discrete, there is a $\lambda \in K, 0 < |\lambda| < 1$, such that λV is a $0-$neighborhood by our initial statement, and which is circled. Again by our initial statement, we observe that the topology in translation-invariant.

   Conversely let $\mathcal{T}$ be a translation-invariant topology on L possessing a

$0-$neighborhood base $\mathcal{B}$ with the three properties as stated. We need to show continuity of addition and scalar multiplication. It is clear that $\{x_0 + V \,|\, V \in \mathcal{B}\}$ is a neighborhood base of $x_0 \in L$, hence if $V \in \mathcal{B}$ is given, and $U \in \mathcal{B}$ can be selected such that $U + U \subseteq V$, then $x - x_0, y - y_0 \in U$ implies that $x + y \in x_0 + y_0 + V$, so addition is continuous. Now let $\lambda_0 \in K, x_0 \in L$ be any fixed points. If $V \in \mathcal{B}$ is given, then there is a $U \in \mathcal{B}$ such that $U + U \subseteq V$. By radiality of U, there is a real number $\varepsilon > 0$ such that $(\lambda - \lambda_0)x_0 \in U$ whenever $|\lambda - \lambda_0| < \varepsilon$. Let $\mu \in K$ satisfy the third condition. Then there exists a natural number $n \in \mathbb{N}$ such that $|\mu^{-n}| = \infty\mu|^{-n} > |\lambda_0| + \varepsilon$. Set $W := \mu^n U \in \mathcal{B}$. Now since U is circled, the relations $x - x_0 \in W$ and $|\lambda - \lambda_0| < \varepsilon$ imply $\lambda(x - x_0) \in U$, and hence with

$$\lambda x = \lambda_0 x_0 + (\lambda - \lambda_0)x_0 + \lambda(x - x_0)$$

that $\lambda x \in \lambda_0 x_0 + U + U \subseteq \lambda_0 x_0 + V$, i.e. scalar multiplication is continuous.

Finally, if K is an Archimedean valuated field, then $|2| > 1$ for $2 = 1 + 1 \in K$ and thus $|2^n| = |2|^n > \lambda_0 + \varepsilon$ for a suitable $n \in \mathbb{N}$. By repeated application of the second condition, we can select a $W_1 \in \mathcal{B}$ such that

$$2^n W_1 \subseteq W_1 + \ldots + W_1 \subseteq U$$

Since W_1 and hence $2^n W_1$ are circled, W_1 can be substituted for W in the preceding proof, so the third condition is dispensable in this case.

5. Let $L \xrightarrow{\mu} M$ be locally convex topological vector spaces, $\mathcal{P}$ a family of semi-norms ($\|\alpha x\|_p = |\alpha| \cdot \|y\|_p$ and $\|x+y\|_p \leq \|x\|_p + \|y\|_p$) generating the topology of L and μ algebraically homomorph, i.e. linear. Then μ is continuous if and only if for each continuous semi-norm q on M, there exists a finite subset $\{p_j \,|\, j = 1, \ldots, n\} \subseteq \mathcal{P}$ and a number $c > 0$ such that $\|\mu(x)\|_q < c \cdot \sup_j p_j(x)$ for all $x \in L$.

   Reason: Continuity of Linear Maps.

   Solution: Necessity. Let V be the $0-$neighborhood $\{y \,|\, \|y\|_q < 1\}$, where q is a given continuous semi-norm on M. Since μ is continuous and $\mathcal{P}$ generates the topology of L, there exist $0-$neighborhoods $U_j = \{x \,|\, \|x\|_{p_j} < \varepsilon_j\}$ where $\varepsilon_j > 0$ and $p_j \in \mathcal{P}$ for $j = 1, \ldots, n$, such that $\mu\left(\cap_{j=1}^n U_j\right) \subseteq V$. Hence, letting $\varepsilon := \min\{\varepsilon_1, \ldots, \varepsilon_n\}$, the relation $\sup\{p_1(x), \ldots, p_n(x)\} < \varepsilon$ implies $\mu(x) \in V$, thus $\|\mu(x)\|_q < \varepsilon^{-1} \sup\{p_1(x), \ldots, p_n(x)\}$ for all $x \in L$.

   Sufficiency. If V is a given convex circled $0-$neighborhood in M, its gauge function $q : x \longmapsto \|q(x)\| = \inf\{\lambda > 0 \,|\, x \in \lambda M\}$ is a continuous semi-norm. Thus if $\|\mu(x)\|_q < c \cdot \sup\{p_1(x), \ldots, p_n(x)\}$, where $c > 0$ and $p_j \in \mathcal{P}$ for $j = 1, \ldots, n$, it follows that $\mu(U) \subseteq V$ for the $0-$neighborhood $U = \{x \,|\, cp_j(x) < 1\,,\, j = 1, \ldots, n\}$ in L.

An important corollary is:

If $(L, \|.\|_L) \xrightarrow{\mu} (M, \|.\|_M)$ is a linear map between normed spaces, i.e. a linear operator, then μ is continuous if and only if μ is bounded: $\|\mu(x)\|_M < c\|x\|_L$ for some $c > 0$ and all $x \in L$.

6. Let $\mathbb{F}_q$ be a finite field of characteristic p. Show that it's multiplicative group $\mathbb{F}_q^* = \mathbb{F}_q - \{0\}$ is cyclic.

   Reason: Finite fields.

   Solution: If $n \in \mathbb{N}$ and φ denotes the Euler φ-function, then
$$n = \sum_{d\,|\,n} \varphi(d).$$
   If $d\,|\,n$, let C_d be the unique subgroup of $\mathbb{Z}_n$ of order d, and let $\Phi(d)$ be the set of generators of C_d. Since all elements of $\mathbb{Z}_n$ generate one of the C_d, the group $\mathbb{Z}_n$ is the disjoint union of the $\Phi(d)$ and we have
$$n = \operatorname{card}(\mathbb{Z}_n) = \sum_{d\,|\,n} \operatorname{card}(\Phi(d)) = \sum_{d\,|\,n} \varphi(d).$$
   Let H be any finite group of order n. Suppose that, for all divisors d of n, the set of $x \in H$ such that $x^d = 1$ has at most d elements. Then H is cyclic.

   Let $d\,|\,n$ and $x \in H$ of order d. Then all elements $y \in H$ with $y^d = 1$ are at most d many by the hypothesis. They form a group that contains x, hence
$$\langle x \rangle = \left\{ y \in H \,|\, y^d = 1 \right\} \cong C_d$$
   In particular, all elements of H of order d are generators of $\langle x \rangle$ and these are in number $\varphi(d)$. Hence, the number of elements of H of order d is 0 or $\varphi(d)$. If it were zero for a value of d, the formula $n = \sum_{d\,|\,n} \varphi(d)$ would show that the number of elements H is less that n, contrary to hypothesis. In particular, there exists an element $x \in H$ of order n and $H = \langle x \rangle$, i.e. H is a cyclic group.

   Finally, we set $H = \mathbb{F}_q^*$ and $n = q - 1$. The polynomial $X^d - 1 \in \mathbb{F}_q[X]$ has at most d solutions in $\mathbb{F}_q$, so we can apply what we just have proven and conclude that $H = \mathbb{F}_q^*$ is cyclic.

7. Let $\mathbb{F}_q$ be a finite field of characteristic p and $f_\alpha \in \mathbb{F}_q[X_1,\ldots,X_n]$ polynomials such that $\sum_\alpha \deg f_\alpha < n$, and $V \subseteq \mathbb{F}_q^n$ be the set of their common zeros. Then
$$p \,|\, \operatorname{card}(V)$$

Reason: Polynomials over finite fields.

Solution: We first observe that for an integer $n \geq 0$
$$S_n(X) := \sum_{x\in\mathbb{F}_q} x^n = \begin{cases} -1 & \text{if } n \geq 1 \,\wedge\, (q-1)\,|\, n \\ 0 & \text{otherwise} \end{cases}$$
with the convention $0^0 = 1$. The case $n = 0$ is obvious since $q \equiv 0\,(p)$ so we may assume $n \geq 1$. The multiplicative group of $\mathbb{F}_q$ is cyclic of order $q-1$, so in case n is divisible by $q-1$, we have $S_n(X) = 0^n + \sum_{x\neq 0} (x^{q-1})^e = 0 + \sum_{x\neq 0} 1^e = q-1 = -1$ for some $e \in \mathbb{N}$. Next assume $(q-1) \nmid n$. Then there exists a $y \in \mathbb{F}_q - \{0\}$ with $y^n \neq 1$ and
$$\begin{aligned} S_n(X) &= \sum_{x\in\mathbb{F}_q} x^n = \sum_{x\neq 0} x^n = \sum_{x\neq 0} y^n x^n = y^n \sum_{x\neq 0} x^n = y^n S_n(X) \\ &\Longrightarrow (1-y^n)S_n(X) = 0 \\ &\Longrightarrow S_n(X) = 0 \end{aligned}$$
Let $P(X) := \prod_\alpha (1-f_\alpha)^{q-1}$ and $x \in \mathbb{F}_q^n$. If $x \in V$ then all $f_\alpha(x) = 0$ and $P(x) = 1$; if $x \notin V$, we have one of the f_α with $f_\alpha \neq 0$ but $f_\alpha^{q-1} = 1$, hence $P(x) = 0$. Thus $P(X)$ is the characteristic function of V. If, for every polynomial f, we put $S(f) := \sum_{x\in\mathbb{F}_q^n} f(x)$, we have
$$\operatorname{card}(V) \equiv S(P)\,(p)$$
and we have to show that $S(P) = 0$. The hypothesis $\sum_\alpha \deg f_\alpha < n$ implies that $\deg P < n(q-1)$. Thus $P(X)$ is a linear combination of monomials $X^v = X_1^{u_1}\cdots X_n^{u_n}$ with $\sum u_j < n(q-1)$. This means that at least one $0 \leq u_j < q-1$ and $S(X_j^{u_j}) = 0$ by our initial observation. Now
$$S(X^v) = \sum_{x\in\mathbb{F}_q^n} X^v(x) = \sum_{x\in\mathbb{F}_q^n} x_1^{u_1}\cdots x_n^{u_n} = 0 \Longrightarrow S(P) = 0$$

8. A linear fractional transformation $S : \mathbb{C}_\infty \longrightarrow \mathbb{C}_\infty$ defined by $S(z) = \dfrac{az+b}{cz+d}$ is called a Möbius transformation if $ad - bc \neq 0$. Here $S(\infty) =$

a/c and $S(-d/c) = \infty$. Show that Möbius transformations form a group by composition, and that there is a unique Möbius transformation $S(z)$ which takes (z_1, z_2, z_3) to $(1, 0, \infty)$. Which one?

Reason: Möbius transformation.

Solution: Associativity is guaranteed by taking composition as multiplication, multiplicative closure and the identity element are obvious, so only the existence of an inverse has to be shown. Set

$$S^{-1}(z) := \frac{dz - b}{-cz + a}$$

$$S(S^{-1}(z)) = \frac{a\dfrac{dz-b}{-cz+a} + b}{c\dfrac{dz-b}{-cz+a} + d} = \frac{adz - ab - bcz + ab}{cdz - cb - cdz + ad} = z$$

$$S^{-1}(S(z)) = \frac{d\dfrac{az+b}{cz+d} - b}{-c\dfrac{az+b}{cz+d} + a} = \frac{adz + bd - bcz - bd}{-acz - bc + acz + ad} = z$$

Let $S \not\equiv 1$ and $S(z) = z$. Then $0 = cz^2 + (d-a)z - b$ which has at most two different solutions. If $a, b, c \in \mathbb{C}_\infty$ are three different points such that $S(a) = T(a), S(b) = T(b), S(c) = T(c)$ for two Möbius transformations S, T. Then $T^{-1} \circ S$ has three fixed points, i.e. $T^{-1}S \equiv 1$ and $S = T$. Hence, a Möbius map is uniquely determined by its action on any three distinct given points in $\mathbb{C}_\infty$. Set

$$S(z) := \begin{cases} \dfrac{\dfrac{z-z_2}{z-z_3}}{\dfrac{z_1-z_2}{z_1-z_3}} & \text{if } z_1, z_2, z_3 \in \mathbb{C} \\[2ex] \dfrac{z-z_2}{z-z_3} & \text{if } z_1 = \infty \\[2ex] \dfrac{z_1-z_3}{z-z_3} & \text{if } z_2 = \infty \\[2ex] \dfrac{z-z_2}{z_1-z_2} & \text{if } z_3 = \infty \end{cases}$$

Then $S(z_1) = 1\,,\ S(z_2) = 0\,,\ S(z_3) = \infty$.

9. Let G be a connected open set and let $f : G \longrightarrow \mathbb{C}$ be an analytic function. Show that the following statements are equivalent:

   (a) $f \equiv 0$

   (b) There is a point $a \in G$ such that $f^{(n)}(a) = 0$ for each $n \geq 0$.

   (c) $\{z \in G \,|\, f(z) = 0\}$ has a limit point in G.

   Reason: Function theory.

   Solution: It is sufficient to show that $(c) \Rightarrow (b)$ and $(b) \Rightarrow (a)$.

   Let $a \in G$ be a limit point of $Z := \{z \in G \,|\, f(z) = 0\}$, and let $R > 0$ be such that $B(a;R) \subseteq G$. Since f is continuous, it follows $f(a) = 0$. Suppose there is an integer $n \geq 1$ such that $f(a) = f^{'}(a) = \cdots = f^{(n-1)}(a) = 0$ and $f^{(n)}(a) \neq 0$. Expanding f in power series about a gives that
$$f(z) = \sum_{k=n}^{\infty} a_k (z-a)^k$$
   for $|z-a| < R$. If
$$g(z) := \sum_{k=n}^{\infty} a_k (z-a)^{k-n}$$
   then g is analytic in $B(a;R)$, $f(z) = (z-a)^n g(z)$, and $g(a) = a_n \neq 0$. Since g is continuous in $B(a;R)$ we can find an $0 < r < R$, such that $g(z) \neq 0$ for $|z-a| < r$. But since a is a limit point of Z there is a point $b \in Z$ with $0 < |b-a| < r$. This gives $0 = (b-a)^n g(b)$ and so $g(b) = 0$, a contradiction. Hence no such integer n can be found, which proves (b).

   Let $A := \{z \in G \,|\, f^{(n)}(z) = 0 \text{ for all } n \geq 0\}$. From the hypothesis (b) we have that $A \neq \emptyset$. We will show that A is both open and closed in G; by connectedness of G it will follow that $A = G$ and so $f \equiv 0$.
   To see that $A$is closed, let $z \in \overline{A}$ and let (a_k) be a sequence in A such that $z = \lim a_k$. Since $f^{(n)}$ is continuous it follows that $f^{(n)}(z) = \lim f^{(n)}(a_k) = 0$. So $z \in A$ and A is closed.
   To see that A is open, let $a \in A$ and let $R > 0$ be such that $B(a;R) \subseteq G$. Then $f(z) = \sum a_n (z-a)^n$ for $|z-a| < R$ where $a_n = (n!)^{-1} f^{(n)}(a) = 0$ for each $n \geq 0$. Hence $f(z) = 0$ for all $z \in B(a;R)$ and, consequently, $B(a;R) \subseteq A$. Thus A is open and this completes the proof.

10. Suppose f and g are meromorphic in a neighborhood of $\overline{B}(a;R)$ with no zeros (Z) or poles (P) on the circle $\gamma = \{z \in \mathbb{C} \,|\, |z-a| = R\}$. If

Z_f, Z_g, P_f, P_g are the numbers of zeros, resp. poles, of f and g inside γ counted according to their multiplicities and if

$$|f(z) + g(z)| < |f(z)| + |g(z)|$$

on γ, then

$$Z_f - P_f = Z_g - P_g \ .$$

Reason: Rouché's theorem.

Solution: From the hypothesis

$$\left| \frac{f(z)}{g(z)+1} \right| < \left| \frac{f(z)}{g(z)} \right| + 1$$

on γ. If $\lambda := f(z)/g(z)$ and if λ is a positive real number then this inequality becomes $\lambda + 1 < \lambda + 1$, a contradiction. Hence the meromorphic function f/g maps γ onto $\Omega := \mathbb{C} - [0, \infty)$. If L is a branch of the logarithm on Ω then $L(f(z)(g(z))$ is a well-defined primitive for $(f/g)'(f/g)^{-1}$ in a neighborhood of γ. Thus

$$\begin{aligned} 0 &= \frac{1}{2\pi i} \int_\gamma (f/g)'(f/g)^{-1} \\ &= \frac{1}{2\pi i} \int_\gamma \left(\frac{f'}{f} - \frac{g'}{g} \right) \\ &= (Z_f - P_f) - (Z_g - P_g). \end{aligned}$$

11. (HS-1) A gardener holds a water hose horizontally and wants to water a bed 6 m away. The water exits the hose at a speed of 8 m/s . Calculate the minimum height the gardener needs to hold the hose for the water to reach the bed, the speed at which the water droplets hit the bed, and the angle at which the water droplets hit the bed.

    Reason: Projectile motion.

    Solution: It is a uniformly motion, i.e. $x_0 = v_x \cdot t_0$. We have also an acceleration towards earth the whole time, i.e.

$$y_0 = \frac{g}{2} \cdot t_0^2 = \frac{g}{2} \cdot \left(\frac{x_0}{v_x} \right)^2 = \frac{9.8\,\dfrac{\mathrm{m}}{\mathrm{s}^2}}{2} \cdot \left(\frac{6\,\mathrm{m}}{8\,\dfrac{\mathrm{m}}{\mathrm{s}}} \right)^2 = 2.76\,\mathrm{m}$$

For the y-component of the velocity we have $v_y = g \cdot t_0$ so

$$v = \sqrt{v_x^2 + v_y^2} = \sqrt{v_x^2 + g^2 \cdot \left(\frac{x_0}{v_x}\right)^2}$$
$$= \sqrt{64\,\frac{\mathrm{m}^2}{\mathrm{s}^2} + 96.04\,\frac{\mathrm{m}^2}{\mathrm{s}^4} \cdot \left(\frac{6\,\mathrm{m}}{8\,\frac{\mathrm{m}}{\mathrm{s}}}\right)^2} = 10.86\,\frac{\mathrm{m}}{\mathrm{s}}$$

Finally we have for the angle

$$\tan\alpha = \frac{v_y}{v_x} = \frac{g \cdot \frac{x_0}{v_x}}{v_x} = \frac{g \cdot x_0}{v_x^2} = 9.8\,\frac{\mathrm{m}}{\mathrm{s}^2} \cdot \frac{6\,\mathrm{m}}{64\,\frac{\mathrm{m}^2}{\mathrm{s}^2}} = 0.91875$$

which results in $\alpha \approx 42.6°$

12. (HS-2) A faucet delivers a volume flow of $V' = 6\,\frac{l}{\mathrm{min}}$. The connected garden hose has an inner diameter of $d_1 = 18\,\mathrm{mm}$, the nozzle a cross-section of $d_2 = 5\,\mathrm{mm}$. Calculate the mass flow in the garden hose, the speed of the water in the garden hose, and the speed of the water at the nozzle. It is observed that the water jet widens after the nozzle. Why?

    Reason: Fluid dynamics.

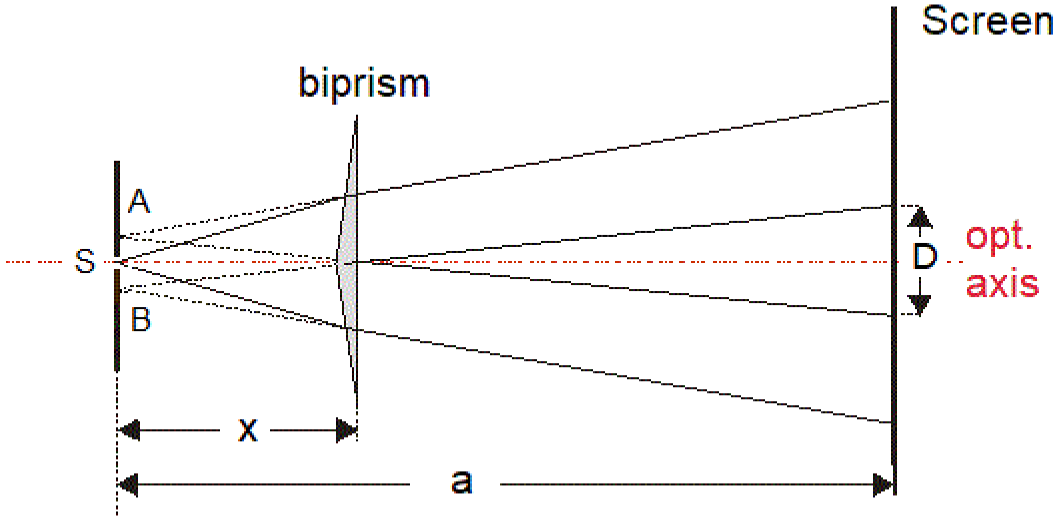
    Solution: Water is an incompressible fluid and has a density of $\rho = 1,000\,\frac{\mathrm{kg}}{\mathrm{m}^3}$ under standard conditions. We have by hypothesis a flow of volume
    $$V' = 6\,\frac{l}{\mathrm{min}} = \frac{6 \cdot 10^{-3}\,\mathrm{m}^3}{60\,\mathrm{s}} = 10^{-4}\,\frac{\mathrm{m}^3}{\mathrm{s}}$$
    From $m = \rho \cdot V$ for the mass of incompressible fluids we get
    $$m' = \rho V' = 1000\,\frac{\mathrm{kg}}{\mathrm{m}^3} \cdot 10^{-4}\,\frac{\mathrm{m}^3}{\mathrm{s}} = 0.1\,\frac{\mathrm{kg}}{\mathrm{s}}$$
    The cross-section of the hose has a radius $r_1 = d_1/2 = 9\,\mathrm{mm} = 0.009\,\mathrm{m}$ and so an area of $A_1 = \pi r_1^2 = 2.545 \cdot 10^{-4}\,\mathrm{m}^2$. This results in a velocity of
    $$v_1 = \frac{V'}{A_1} = \frac{10^{-4}\,\frac{\mathrm{m}^3}{\mathrm{s}}}{2.545 \cdot 10^{-4}\,\mathrm{m}^2} = 0.393\,\frac{\mathrm{m}}{\mathrm{s}}.$$

The cross-section of the nozzle is $A_2 = \pi r_2^2 = \pi \frac{d_2^2}{4} = 0.2 \cdot 10^{-4}\,\mathrm{m}^2$, hence the velocity at the nozzle is

$$v_2 = \frac{V'}{A_2} = \frac{10^{-4}\,\frac{\mathrm{m}^3}{\mathrm{s}}}{0.2 \cdot 10^{-4}\,\mathrm{m}^2} = 5\,\frac{\mathrm{m}}{\mathrm{s}}.$$

The velocity of the water is slowed down due to friction and air resistance. However, mass and volume stay the same, such that velocity times cross-section is constant. That is why the beam widens.

13. (HS-3) As a result of the refraction, the light bundle emanating from the slit S produces two bundles which overlap in the screen area of width D and appear to arise from two virtual slit images A and B. Since the two virtual slit images originate from the same slit, the light emanating from them is coherent and can interfere in the area of overlap.



Calculate the wavelength if monochromatic light is used from the quantities given in the sketch and the distance Δy between two adjacent interference strips? Assume that the dimensions parallel to the optical axis can be viewed as large compared to those perpendicular to the optical axis.

Reason: Optics.

Solution: Let b be the distance between the two virtual slit images A, B. The intercept theorem yields

$$\frac{b}{D} = \frac{x}{a-x} \Longrightarrow b = \frac{Dx}{a-x}$$

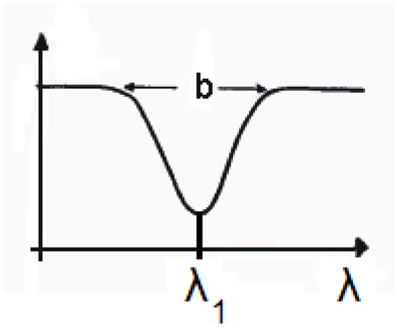
For $a \gg b$ we may assume that the beams that run from A and B in direction P on the screen are approximately parallel. For the interference at the k-th maximum, and small angles, we have

$$\Delta s_k = b \cdot \sin \alpha_k = k \cdot \lambda \Longrightarrow \sin \alpha_k = \frac{k\lambda}{b} \approx \tan \alpha_k = \frac{y_k}{a}$$

By the same arguments we get $\dfrac{(k+1)\lambda}{b} = \dfrac{y_{k+1}}{a}$ and thus

$$\lambda = \frac{b}{a}(y_{k+1} - y_k) = \frac{b}{a} \cdot \Delta y \ .$$

14. (HS-4) A galaxy is 42 MLy away and oriented in space, such that its rotation axis is perpendicular to the line of sight. The α line of hydrogen is measured to occur at $\lambda_1 = 658.003\,\text{nm}$ instead of $\lambda_0 = 656.28\,\text{nm}$



widened to $b = 0.438\,\text{nm}$. Assume that the main cause of the widening is the rotation of the stars around the center of the galaxy. Assume further that the different wavelength is only due to the radial motion of the galaxy compared to our solar system.

What is the maximal rotational velocity of the observed stars, and what is the maximal velocity the galaxy is moving and in which direction as seen from our solar system?

Reason: Astronomy.

Solution: If we consider the rotational velocity v, we have $v = \dfrac{\Delta\lambda}{\lambda_1} \cdot c$ and with $\Delta\lambda = 0.5\,b$

$$v = \frac{0.219\,\text{nm}}{658.003\,\text{nm}} \cdot 3 \cdot 10^8\,\frac{\text{m}}{\text{s}} = 99778.5\,\frac{\text{m}}{\text{s}} \approx 100\,\frac{\text{km}}{\text{s}}$$

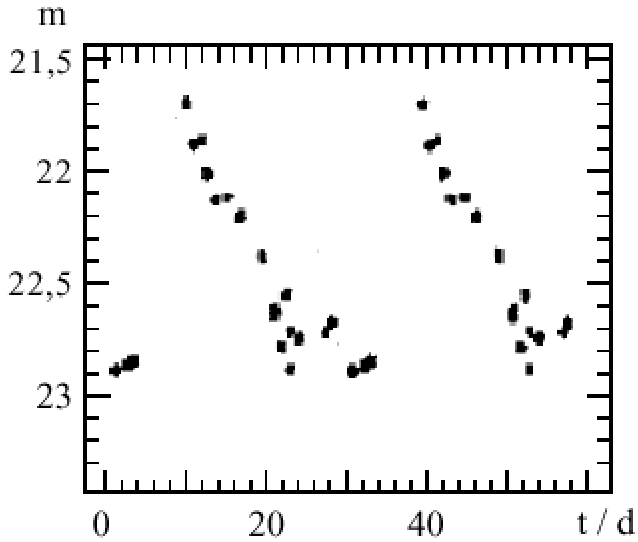
The calculation of the galaxy's relative motion to us is

$$v = \frac{\Delta\lambda}{\lambda_1} \cdot c = \frac{\lambda_1 - \lambda_0}{\lambda_1} \cdot c = \frac{1.723\,\text{nm}}{656.28\,\text{nm}} \cdot 3 \cdot 10^8\,\frac{\text{m}}{\text{s}} = 787,076\,\frac{\text{m}}{\text{s}} \approx 790\,\frac{\text{km}}{\text{s}} \ .$$

Since $\lambda_1 > \lambda_0$ the galaxy is moving at around $790\,\frac{\text{km}}{\text{s}}$ away from us.

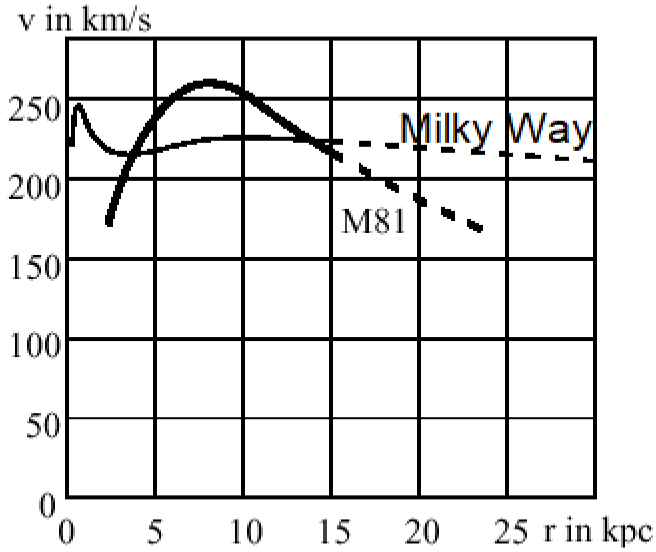
15. (HS-5) The spiral galaxy M81 near Ursa Major can already be viewed by a small telescope. It has an apparent magnitude of $M = 6.9$. The angle to the celestial pole is about $21°$. Is it possible to observe M81 the entire year, if you live in Toronto?

    The following diagram shows data-points of light from the cepheid C27 in M81.



    Calculate our distance from M81 in lightyears. (Use an average value of magnitude 22.3 at a pulsation rate of 30 per day and the relation $M = -1.67 - 2.54 \cdot \log_{10} p$.)

    The second diagram is a comparison between M81 and Milky Way. It shows the radial orbit velocity v of the stars in relation to their distance r from the galaxy center. Optical wavelengths are hardly to observe from around $16\,kpc$ on, so radio wavelengths are used.



Verify that if a celestial body orbits a center of great mass, then we can calculate the central mass approximately by $M = \dfrac{v^2 \cdot r}{G}$. Show by choosing two data-points that the rotation curve of M81 is approximately $v \sim \dfrac{1}{\sqrt{r}}$ for $r = 10\,\text{kpc}$. What does that mean for the mass distribution in M81 ? Estimate the mass of M81 within the optical spectrum in units of sun masses.

The rotation curves of M81 and the Milky Way differ a lot for great distances from the center. What does that mean for the mass distribution in our Milky Way?

The wavelength of the α-line of hydrogen from the optical center of M81 is measured to be $\lambda_1 = 656.38\,\text{nm}$ in comparison to $\lambda_0 = 656.28\,\text{nm}$. Can we apply Hubble's law to M81?

Reason: M81.

Solution:

(a) An observer in the Northern hemisphere can see all stars (or galaxies) whose angular distance from the celestial pole is less than its geographical latitude. Toronto is at 43° 39' 40,86" N, 79° 22' 59,11" W, which is significantly greater than 21°, hence M81 can be seen at any time of the year.

(b) We read an average of magnitude $m = 22.3$ at a pulsation rate of 30 per day. With the given relation we calculate $M = -5.42$. The distance is given by

$$m - M = 5 \cdot \log_{10}\left(\frac{d}{10\,\text{pc}}\right) \Longrightarrow d = 10^{(m-M)/5} \cdot 10\,\text{pc}$$
$$d = 10^{(22.3+5.42)/5} \cdot 10\,\text{pc} = 350,000 \cdot 10\,\text{pc}$$
$$\approx 10,798,258 \cdot 10^{16}\,\text{m} \approx 11.4\,\text{MLy}$$

(c) $F_G = F_C \Longrightarrow G \cdot \dfrac{m \cdot M}{r^2} = \dfrac{m \cdot v^2}{r} \Longrightarrow M = \dfrac{v^2 \cdot r}{G}$

(d) The diagram gives us two data-points $r_1 = 10\,\text{kpc}\,,\ \text{v}_1 = 250\,\text{kms}^{-1}$ and $r_2 = 20\,\text{kpc}\,,\ \text{v}_2 = 185\,\text{kms}^{-1}$. Hence

$$\frac{v_1}{v_2} = \frac{250}{185} = 1.35 \text{ and } \frac{\sqrt{r_2}}{\sqrt{r_1}} = \sqrt{2} = 1.41 \Longrightarrow v \sim \frac{1}{\sqrt{r}}.$$

This is almost the proportion we have for a single large central mass, which in return means that almost the entire mass of M81 is within 10 kpc of range. The optical limit is the point $r = 16\,\text{kpc}\,,\ \text{v} = 210\,\text{kms}^{-1}$.

$$m_{M81} = \frac{\left(210\,\dfrac{\text{km}}{\text{s}}\right)^2 \cdot 16\,\text{kpc}}{6.673 \cdot 10^{-11}\,\dfrac{\text{m}^3}{\text{kg}\,\text{s}^2}} = \frac{44,100 \cdot 10^6 \cdot 16,000 \cdot 3.0857 \cdot 10^{16}\,\text{m}^3\text{s}^{-2}}{6.673 \cdot 10^{-11}\,\dfrac{\text{m}^3}{\text{kg}\,\text{s}^2}}$$
$$= 3.2628 \cdot 10^{41}\,\text{kg} \approx 164 \cdot 10^9\,\text{m}_{\text{sun}}$$

(e) The orbital velocity of the Milky Way is almost constant for large distances from its center. So there must be considerable (non-luminous) masses at these distances.

(f) Since the α-line of hydrogen is blue-shifted, $\lambda_1 > \lambda_0$, Hubble's law does not apply. M81 is approaching the Milky Way.

6 July 2021

1. Suppose that G is a finite group such that for each subgroup H of G there exists a homomorphism $\varphi : G \longrightarrow H$ such that $\varphi(h) = h$ for all $h \in H$. Show that G is a product of groups of prime order.

   Reason: Group Theory.

   Solution: We proceed by induction on $|G|$. The base case $|G| = 1$ is trivial (empty product), as are $|G| = 2, 3$. Suppose that $|G| > 3$ and that the statement is true for all smaller groups. Choose a subgroup H of G of prime order p. Such a subgroup exists by the first Sylow theorem. By assumption, there is a homomorphism $\varphi : H \longrightarrow H$ such that $\varphi(h) = h$ for all $h \in H$. Let $K := \ker \varphi$. By induction hypothesis, K is a product of groups of prime order. Let $\sigma : G \longrightarrow K$ be a homomorphism which is constant on K, i.e. $\sigma(k) = k$ for all $k \in K$, which exists by assumption. Now we define

   $$\alpha : G \longrightarrow K \times H \ , \ \alpha(g) := (\sigma(g), \varphi(g))$$

   Since σ restricted to K equals the identity, the kernel of α is trivial, i.e. α is injective and thus $|G| = |K| \cdot |H|$. But then α is an isomorphism, K a product of subgroups of prime order by induction hypothesis, and H was of prime order p.

2. Let G be a finite group that operates on a set X. Then the number of orbits is

   $$|X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|$$

   where $X^g = \{ x \in X \ : \ g.x = x \}$ are the fixed points in X.

   Reason: Burnside's Lemma (Frobenius-Cauchy Lemma).

   Solution: Long version.

   $G_x = \{ g \in G \,|\, g.x = x \} \leqslant G$ is the stabilizer of x.
   $G(x) = \{ g.x \,|\, g \in G \} \subseteq X$ is the orbit of x under G.

   Step 1: Stabilizer-Orbit Formula: $|G| = |G_x| \cdot |G(x)|$

   Consider the relation $R = \{ (g, y) \in G \times X \,|\, y = g.x \}$. For each $g \in G$ there is exactly one $y = g.x \in X$, hence $|R| = |G|$. On the other hand, we have for $y \in G(x)$, say $y = g_0.x$, exactly $|G_x|$ many elements $h \in G$ with $h.x = y$, because these are exactly all elements $h = g_0 g$ with

$g \in G_x$. In case $y \notin G(x)$ there is no element $(g, y) \in R$. Therefore

$$|R| = |G| = \sum_{y \in G(x)} |G_x| = |G(x)| \cdot |G_x|$$

Step 2: $\displaystyle\sum_{g \in G} |X^g| = \sum_{x \in X} |G_x|$

This time we use the double count argument on the relation $S = \{\, (g, x) \in G \times X \,|\, g.x = x \,\}$. For a fixed element $h \in G$ the set $\{\, (h, x) \,|\, x \in X^h \,\}$ is the set of pairs in S which have h as their first coordinate. On the other hand we have for a given $z \in X$ the set of pairs in S with second coordinate z the set $\{\, (g, z) \,|\, g \in G_z \,\}$. Hence

$$\sum_{h \in G} |X^h| = |S| = \sum_{z \in X} |G_z|$$

Step 3: $\displaystyle |X/G| = \frac{1}{|G|} \sum_{g \in G} |X^g|$

We use the stabilizer-orbit formula and sort the summands on the RHS with equal stabilzers; especially all elements $y \in G(x)$ have stabilizers G_x of equal size:

If $g \in G_x$ and $y = g_0.x \in G(x)$ then $g.x = x$ and thus $(g_0 g.x = g_0.x = y)$, i.e. $(g_0 g g_0^{-1}).(g_0.x) = g_0.x = y$. If g runs through the stabilizer G_x, then $g_0 G_x g_0^{-1}$ runs through the stabilizer of $y = g_0.x$. But both sets are of equal size $|G_x|$. With the previous steps, especially with $|G_x| = |G|/|G(x)| = |G|$, we get

$$\begin{aligned} \sum_{g \in G} |X^g| &= \sum_{x \in X} |G_x| = \sum_{A \in X/G} \sum_{x \in A} |G_x| \\ &= \sum_{A \in X/G} |A| \cdot \frac{|G|}{|A|} = \sum_{A \in X/G} |G| = |X/G| \cdot |G| \end{aligned}$$

Note: William Burnside wrote this formula down around 1900. Historians of mathematics, however, found this formula already from Cauchy (1845) and Frobenius (1887). Therefore the formula is sometimes referred to as the Lemma which is not from Burnside.

3. Prove that there is a Lie algebra monomorphism $\mathfrak{g} \hookrightarrow \mathfrak{gl}(\mathfrak{g})$ if $\mathfrak{g}$ is a semisimple Lie algebra. Is this also a necessary condition?

   Reason: Adjoint Representation and Center.

Solution: A semisimple Lie algebra has no Abelian ideals. Its center, however, is an Abelian ideal. Thus we have

$$\begin{aligned}\mathfrak{Z}(\mathfrak{g}) &= \{\, Z \in \mathfrak{g} \,|\, [X,Z]=0 \;\forall\, X \in \mathfrak{g}\,\} \\ &= \bigcap_{X\in\mathfrak{g}} \ker \mathfrak{ad} X = \ker \mathfrak{ad} = \{\,0\,\}\end{aligned}$$

This means that $\mathfrak{ad} \, : \, \mathfrak{g} \longrightarrow \mathfrak{gl}(\mathfrak{g})$ is a monomorphism of Lie algebras and

$$\mathfrak{g} \cong \mathfrak{ad}(\mathfrak{g}) \cong \mathfrak{Der}(\mathfrak{g}) \subseteq \mathfrak{gl}(\mathfrak{g})$$

The adjoint representation cannot be onto, since the center of $\mathfrak{gl}(\mathfrak{g})$ are all multiples of the identity matrix.

If we consider the non Abelian two dimensional Lie algebra defined by $[X,Y]=Y$, which is the Borel subalgebra of the simple Lie algebra $\mathfrak{sl}(2)$, or the Lie algebra of matrices $\begin{bmatrix} * & * \\ 0 & 0 \end{bmatrix}$, then we have a solvable and therewith no semisimple Lie algebra which has only a trivial center, too. Hence the condition of semisimplicity is not necessary.

4. If $n>1$ is a square-free natural number, prove for all $k>1$

$$\sum_{d|n} \sigma(d^{k-1})\,\varphi(d) = n^k$$

Remark: φ is Euler's phi-function and $\sigma(m)$ the sum of divisors of m.

Reason: Number Theory.

Solution: Let $n=p_1p_2\ldots p_r>1$ a square-free number. The function $f(m)=\sigma(m^t)\varphi(m)$ with $t\geq 1$ is build of multiplicative functions and as such multiplicative, too. This means for coprime numbers a,b we have $f(ab)=f(a)f(b)$. The function $F(n)=\sum_{d|n} f(d) = \sum_{d|n}\sigma(d^{k-1})\varphi(d)$ is also multiplicative:

$$F(ab)=\sum_{d|ab} f(ab) = \sum_{d|a}\sum_{e|b} f(a)f(b) = \sum_{d|a} f(a) \sum_{e|b} f(b) = F(a)F(b)$$

Thus it is sufficient to show $F(p)=p^k$ since as n is square-free and $F(n)=F(p_1\ldots p_r)=p_1^k\ldots p_r^k=n^k$

$$F(p)=\sum_{d|p}\sigma(d^{k-1})\varphi(d) = 1+\sigma(p^{k-1})\varphi(p) = 1+\frac{p^k-1}{p-1}\cdot(p-1)=p^k$$

5. Show that

$$M := \{\, x \in \mathbb{R}^3 \,|\, x_1+x_2+x_3 = 0\,,\; x_1^2+2x_2^2+x_3^2-2x_2(x_1+x_3) = 9\,\} \subseteq \mathbb{R}^3$$

is a manifold, and determine the tangent space T_pM and the normal space N_pM at $p = (2, -1, -1) \in M$.

Reason: Manifolds.

Solution: We consider the function $f : \mathbb{R}^3 \longrightarrow \mathbb{R}^2$ defined by

$$\begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \stackrel{f}{\longrightarrow} \begin{bmatrix} x_1 + x_2 + x_3 \\ x_1^2 + 2x_2^2 + x_3^2 - 2x_2(x_1 + x_3) - 9 \end{bmatrix}$$

such that $M = f^{-1}(\{(0,0)\})$. Its Jacobi matrix is

$$J_xf = \begin{bmatrix} 1 & 1 & 1 \\ 2(x_1 - x_2) & 2(2x_2 - x_1 - x_3) & 2(x_3 - x_2) \end{bmatrix}$$

$\operatorname{rk} J_xf = 1$ if $x_1 - x_2 = 2x_2 - x_1 - x_3 = x_3 - x_2$ or $x_1 = x_2 = x_3$. Since $f(t,t,t) = (3t, -9) \neq 0$, $(0,0)$ is a regular value of f and M a submanifold of dimension $3 - 1 - 1 = 1$.

For $p = (2, -1, -1)$ we have $J_pf = \begin{bmatrix} 1 & 1 & 1 \\ 6 & -6 & 0 \end{bmatrix}$, hence $T_pM = \ker D_pf = \mathbb{R} \cdot \begin{bmatrix} 1 & 1 & -2 \end{bmatrix}$ and $N_pM = (T_pM)^{\perp} = \mathbb{R} \cdot \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} + \mathbb{R} \cdot \begin{bmatrix} 1 \\ -1 \\ 0 \end{bmatrix}$, which is the row space of J_pf.

6. Two persons P and Q play the following game:

P starts by selecting exactly one real value for a, b, or c in the equation

$$x^3 + ax^2 + bx + c = 0$$

Then Q does the same for one of the remaining coefficients, before P finally chooses the last value. P wins if and only if the equation has three different real roots. Is there a winning strategy for one of the players?

Reason: Mean Value Theorem.

Solution: P has the following winning strategy:

P chooses $c = 1$ in his first move. In case Q sets a value for a, then P

finally sets $b < -a-2$; whereas in case Q sets a value for b, P finally sets $a < -b-2$. We now have to show that the equation has three distinct real roots. Let $f(x) = x^3 + ax^2 + bx + 1$. Since $\lim_{x\to\infty} f(x) = +\infty$ and $\lim_{x\to-\infty} f(x) = -\infty$ there is a real number $k > 1$ such that

$$f(k) > 0\,,\; f(0) = 1\,,\; f(-k) < 0\,,\; f(1) = a + b + 2 < 0$$

By the mean value theorem, there have to be roots $f(\xi_j) = 0$ with

$$-k < \xi_1 < 0 < \xi_2 < 1 < \xi_3 < k$$

7. What are the composition factors of $\mathrm{GL}(2, \mathbb{F}_{19})$?

   Reason: Group Theory.

   Solution: We know that

$$\mathrm{GL}(2, \mathbb{F}_{19})/\mathrm{SL}(2, \mathbb{F}_{19}) \cong \mathbb{F}_{19}^{\times} \cong \mathbb{Z}_{18} \cong \mathbb{Z}_2 \times \mathbb{Z}_9$$

   $\mathbb{Z}_9$ has the composition factor $\mathbb{Z}_3$ twice and $\mathbb{Z}_2$ is simple. We know further that

$$\mathrm{SL}(2, \mathbb{F}_{19})/\mathrm{Z}(\mathrm{SL}(2, \mathbb{F}_{19})) \cong \mathrm{PSL}(2, \mathbb{F}_{19})$$

   which is simple, too. With Iwasawa's criterion for simplicity, it can be shown that all groups $\mathrm{PSL}(\mathrm{m}, \mathbb{F}_{\mathrm{p}^\mathrm{k}})$ are simple, except of $\mathrm{PSL}(2, \mathbb{F}_2)$ and $\mathrm{PSL}(2, \mathbb{F}_3)$.

$$|\mathrm{PSL}(\mathrm{m}, \mathbb{F}_{\mathrm{p}^\mathrm{k}})\| = \mathrm{d}^{-1}\mathrm{q}^{\frac{\mathrm{m(m-1)}}{2}} \prod_{\mathrm{j=2}}^{\mathrm{m}} (\mathrm{q}^\mathrm{j} - 1)\,,\; \mathrm{d} := \gcd(\mathrm{m}, \mathrm{q}-1)\,,\; \mathrm{q} = \mathrm{p}^\mathrm{k}$$

   Thus in our case we have $|\mathrm{PSL}(2, \mathbb{F}_{19})| = \dfrac{19}{2}(19^2-1) = 3420$. $\mathrm{PSL}(2, \mathbb{F}_{19})$ is the Chevalley group $A_1(19)$. The remaining composition factors are provided by

$$\mathrm{Z}(\mathrm{SL}(2, \mathbb{F}_{19}))/\{\,\mathbf{1}\,\} \cong \mathrm{Z}(\mathrm{SL}(2, \mathbb{F}_{19})) \cong \mathbb{Z}_2$$

   such that we have the following list:

$$\mathbb{Z}/2\mathbb{Z}\ \text{(twice)}\ ,\ \mathbb{Z}/3\mathbb{Z}\ \text{(twice)}\ ,\ \mathrm{PSL}(2, \mathbb{F}_{19})$$

8. A group G of order 70 has always a normal subgroup of order 5.

   Reason: Group Theory.

Solution: According to Sylow's first theorem, there is at least one subgroup $U \leqslant G$ of order 5. According to his third theorem the number s of such subgroups satisfies

$$s \equiv 1 \mod 5\,,\; s \,|\, |G| = 70$$

If $s \cdot \alpha = 70 = 5 \cdot 14$ and $5 \nmid s$, then $5 \,|\, \alpha$, say $\alpha = 5\beta$ and so $s \cdot \beta = 14$ and $s \,|\, 14 = 2 \cdot 7$. However, $2 \equiv 2 \not\equiv 1 \mod 5$, $7 \equiv 2 \not\equiv 1 \mod 5$ and $14 \equiv 4 \not\equiv 1 \mod 5$, a contradiction except for $s = 1$. As all gUg^{-1} are Sylow 5-subgroups, too, they are already contained in the only one U, which means that U is a normal subgroup.

9. Let X, Y, Z be topological spaces, X covering compact (not necessarily Hausdorff), and Z Hausdorff. Let $g : X \longrightarrow Y$ be continuous, and $h : X \longrightarrow Z$ surjective and continuous. Show that the following statements are equivalent:

   (a) $g(x) = g(x')$ for all $x, x' \in X$ with $h(x) = h(x')$.

   (b) There is a continuous function $f : Z \longrightarrow Y$ with $g = f \circ h$.

   (c) There is a unique continuous function $f : Z \longrightarrow Y$ with $g = f \circ h$.

   Reason: Topology.

   Solution: $(a) \Longrightarrow (b)$: Since h is surjective, we have for any $z \in Z$ an element $x \in X$ such that $z = h(x) = h(x')$, hence $g(x) = g(x')$ by assumption. Therefore there is a well-defined function $f : Z \longrightarrow Y$ with $f(z) := f(h(x)) = g(x)$ for all $z \in Z$, i.e. $g = f \circ h$.

   Given a closed set $A \subseteq X$, means that A is covering compact as X is, hence $h(A) \subseteq Z$ is covering compact, too, because h is continuous. Since Z is Hausdorff, $h(A)$ is closed and so is h.

   Now let $B \subseteq Y$ be closed. Then $g^{-1}(B) = h^{-1}(f^{-1}(B))$, i.e. $f^{-1}(B) \stackrel{(*)}{=} h(h^{-1}(f^{-1}(B))) = h(g^{-1}(B))$. Since g is continuous and h closed, we have that $f^{-1}(B)$ is closed, which means f in continuous.

   $(*)$ h is surjective, so $h(h^{-1}(M)) = M$ for all sets $M \subseteq Z$.
   This property is equivalent to surjectivity.

   $(b) \Longrightarrow (c)$: If $f_1, f_2 : Z \longrightarrow Y$ with $f_1h = g = f_2h$, then $f_1 = f_2$ because surjectivity of h allows us a right cancellation.
   This property is equivalent to surjectivity.

   $(c) \Longrightarrow (a)$: Be $x, x' \in X$ with $h(x) = h(x')$ then $g(x) = f(h(x)) = f(h(x')) = g(x')$.

10. Given $y''' = y'' + y' - y$. Determine a fundamental system, and solve the initial value problem $y(0) = 1$, $y'(0) = 0$, $y''(0) = 3$.

    Reason: Differential Equation.

    Solution: The characteristic polynomial $p\left(\dfrac{d}{dx}\right)(y) = 0$ is given by $p(x) = x^3 - x^2 - x + 1 = (x-1)^2(x+1)$ with a double root at $c_1 = 1$ and a simple root at $c_2 = -1$. With $D = \dfrac{d}{dx}$ we verify

$$\begin{aligned}(D-1)(D-1)(e^x) &= (D-1)(e^x - e^x) = D(0) - 0 = 0\\ (D-1)(D-1)(xe^x) &= (D-1)(xe^x + e^x) = (e^x + xe^x) - (xe^x + e^x) = 0\\ (D+1)(e^{-x}) &= -e^{-x} + e^{-x} = 0\end{aligned}$$

    so we get three linear independent solutions and a basis by the fundamental system

$$\{\, \varphi_1 = e^x \,,\, \varphi_2 = xe^x \,,\, \varphi_3 = e^{-x} \,\}$$

    With the initial values for $y = \sum_{k=1}^{3} a_k \varphi_k(x) = a_1 e^x + a_2 x e^x + a_3 e^{-x}$

$$\begin{aligned}y(0) = 1 &\Longrightarrow a_1 + a_3 = 0\\ y'(0) = 0 &\Longrightarrow a_1 + a_2 - a_3 = 0\\ y''(0) = 3 &\Longrightarrow a_1 + 2a_2 + a_3 = 3\end{aligned}$$

    which results in $(a_1, a_2, a_3) = (0, 1, 1)$ and $y(x) = xe^x + e^{-x}$.

11. (HS-1) Assume we have put a Cartesian coordinate system on France and got the following positions: Paris $(0, 0)$, Lyon $(3, -8)$ and Marseille $(4, -12)$. Look up the definitions and calculate the distance between Lyon and Marseille according to

    (a) the Euclidean metric.
    (b) the maximum metric.
    (c) the French railway metric.
    (d) the Manhattan metric.
    (e) the discrete metric.

    Reason: Internet search for the metrics.

    Solution: We have $P = (0, 0), L = (3, -8), M = (4, -12)$.

    (a) the Euclidean metric.
    $|LM| = \sqrt{(4-3)^2 + (-12-(-8))^2} = \sqrt{17} \approx 4.123.$

(b) the maximum metric.

$|LM| = \max\{\,|4-3|\,,\,|-12-(-8)|\,\} = \max\{\,1,4\,\} = 4.$

(c) the French railway metric.

Paris isn't on the direct line between Lyon and Marseille, so $|LM| = |LP| + |PM| = \sqrt{3^2+(-8)^2} + \sqrt{4^2+(-12)^2} = \sqrt{73} + \sqrt{160} \approx 21.193.$

(d) the Manhattan metric.

$|LM| = |4-3| + |-12-(-8)| = 1+4 = 5.$

(e) the discrete metric.

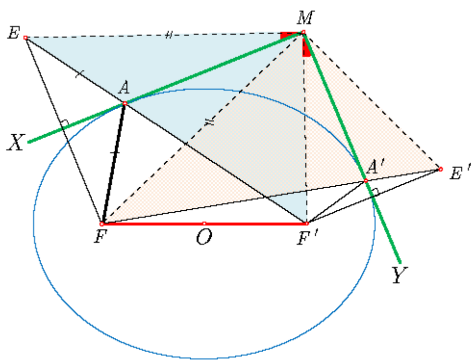
$|LM| = 1.$

12. (HS-2) Consider the ellipse in the first quarter of a Cartesian coordinate system

$$\frac{(x-2)^2}{4} + (y-1)^2 = 1$$

and rotate it such that the coordinate axes are always tangents to the ellipse. Which locus describes the center of the ellipse during a full rotation?

Reason: Geometry.



Solution:
Consider an Ellipse of foci F and F' and semi axis $a=2, b=1$. Let M be a point outside the ellipse. The tangents from M touch the Ellipse at A and A'. Let E be the symmetric of F with respect to MA and define E' similarly.

Step1. The points F', A and E are aligned. Indeed, by the optical property of the ellipse $\angle MAF' = \angle FAX = \angle XAE$. Similarly, the F, A' and F' are also aligned.

Step2. $\triangle FE'M$ and $\triangle F'EM$ are congruent. Because, $EF' = EA +$

$AF' = FA + AF' = 2a$ and similarly, $FE' = 2a$. Moreover, $ME = MF$ and $ME' = MF'$.

Step3. $\angle AMA' = \angle F'ME$. Indeed, from the previous step we conclude that

$$\angle XME = \frac{1}{2}\angle EMF = \frac{1}{2}\angle E'MF' = \angle YMF'.$$

Step4. It follows that $MA \perp MA'$ if and only if $\angle EMF' = \frac{\pi}{2}$, and (since $EM = FM$,) this equivalent to

$$FM^2 + F'M^2 = F'E^2 = 4a^2 \quad (*)$$

But using the parallelogram identity we know that

$$FM^2 + F'M^2 = 2OM^2 + 2OF^2 = 2OM^2 + 2e^2 = 2OM^2 + 2(a^2 - b^2)$$

Thus, $(*)$ is equivalent to $OM^2 = a^2 + b^2 = 5$, which is the desired conclusion, a segment of circle of radius $\sqrt{5}$ and center $(0,0)$ between $(2,1)$ and $(1,2)$.

13. (HS-3) Maximize $f(x,y,z) = 4x^2y^2 - (x^2+y^2-z^2)^2$ under the conditions $x + y + z = c$ and that $x, y, z > 0$.

Reason: Heron's Theorem.

Solution: In case x, y, z are the side lengths of a triangle, we have $f(x,y,z) = c(c-2x)(c-2y)(c-2z) > 0$ if we label the longest side z. Since the geometric mean is less or equal the arithmetic mean, we have

$$c(c-2x)(c-2y)(c-2z) \leq c\left((c-2x) + (c-2y) + (c-2z)\right)^3 = c^4$$

where equality holds if $c - 2x = c - 2y = c - 2z$, i.e. $x = y = z$.

The theorem of Heron says that $f(x,y,z) = 16\,F^2$ where F is the area of the triangle with side lengths x, y, z . The triangle with the maximal area by constant circumference is the equilateral triangle.

Now assume that $c > z \geq x + y > y \geq x > 0$. Then $f(x,y,z) \leq 0$ because $c, c-2x, c-2y > 0, c - 2z = (x+y) - z \leq 0$. We can achieve the maximal value 0 by setting $z = c/2$ such that $f(x,y,c/2) = 0$. In order to match the restrictions on x, y, we could set $x = y = c/4$. The solution, however, isn't unique since e.g. $x = c/6, y = c/3$ match the requirements, too.

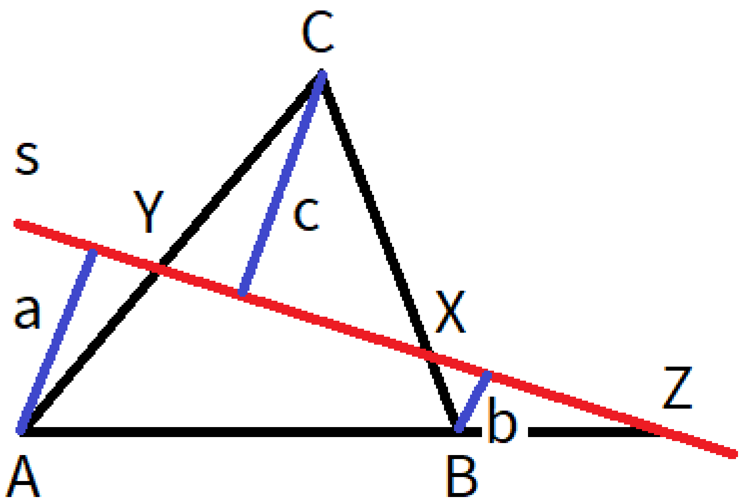
14. (HS-4) Let $\triangle ABC$ be a triangle and s a straight which intersects all three sides (or their prolongations), say $X \in BC$, $Y \in CA$, $Z \in AB$ are the intersection points. Prove

$$\overline{AZ} \cdot \overline{BX} \cdot \overline{CY} = \overline{AY} \cdot \overline{BZ} \cdot \overline{CX}$$

Reason: Menelaus's Theorem.

Solution: Let a, b, c be the perpendiculars in A, B, C resp. on s. From the intercept theorem we get

$$\overline{AZ} : \overline{BZ} = a : b\,,\ \overline{BX} : \overline{CX} = b : c\,,\ \overline{CY} : \overline{AY} = c : a$$



Multiplication yields

$$\frac{\overline{AZ}}{\overline{BZ}} \cdot \frac{\overline{BX}}{\overline{CX}} \cdot \frac{\overline{CY}}{\overline{AY}} = \frac{a}{b} \cdot \frac{b}{c} \cdot \frac{c}{a} = 1$$

15. (HS-5) Otto von Guericke, who invented the air pump, led an experiment in Berlin in 1654. Two groups of eight horses tried in vain to pull apart two bronze hemispheres between which a vacuum was created. Assume that the radius R of the hemispheres is so thin that we can neglect the difference between inner and outer radius.

Show that the force required to tear apart the hemispheres is $F =$

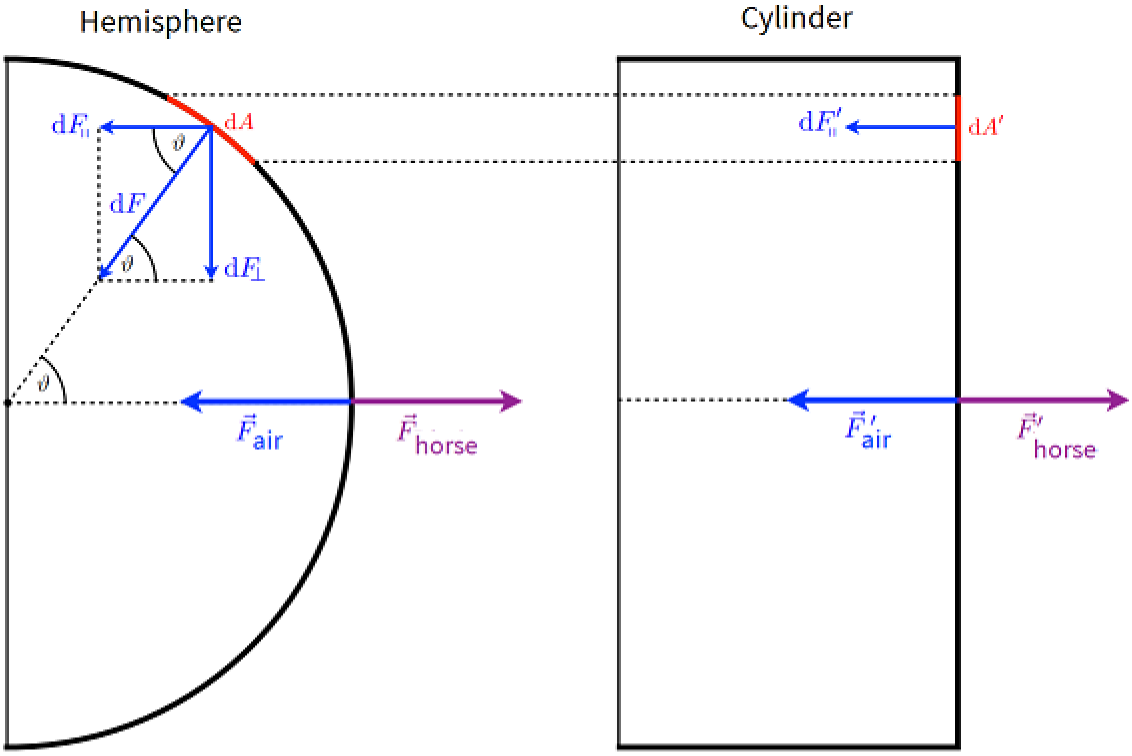
$\pi R^2 \cdot \Delta p$ where Δp is the difference of air pressure within and outside the hemispheres. Next assume $R = 30\,cm$, an inner pressure of $0.1\,bar$ and an outer pressure of $1.013\,bar$ Which force had each group of horses to apply in order to separate the hemispheres?

Reason: Magdeburg Hemispheres. Physics.

Solution: The evacuated Magdeburg hemispheres are affected by the difference of external and internal air pressure Δp which presses them together. To calculate the total force on one of the two hemispheres, we consider a surface element dA. The ambient air exerts a force $d\vec{F}$ on this area that is perpendicular to the surface element and of an amount $dF = \Delta p\,dA$. However, we are only interested in the horizontal part of this force $\vec{F}_{\|}$ which is parallel to the direction to which the horses pull, i.e. parallel to the horizontal symmetry axis of the hemisphere. The perpendicular components $\vec{F}_{\perp}$ cancel themselves out. If we denote the angle φ between the normal to the surface and the direction of pull, then the parallel component has an amount of

$$dF_{\|} = dF \cdot \cos\varphi = \Delta p \; dA \cdot \cos\varphi =: \Delta p \; dA' =: dF'_{\|}$$

The quantity $dA' = dA \cdot \cos\varphi$ can be viewed as parallel projection ot the surface area dA onto a cylinder (see the figure).



The parallel component $dF'_{\|}$ of the force which the air pressure exerts onto the projected surface area element dA' is thus of the same amount as the parallel component $dF_{\|}$ of the original force exerts on the original surface element dA.

The total amount of force exerted by the air pressure onto the hemisphere is the sum of all forces over the surface elements which compose the hemisphere. Since $dF_{\|} = dF'_{\|}$ we have for the total amount $F_{air} = F'_{air}$, the force onto the projection. So the two hemispheres are pressed together as two cylinders were, whose diameters correspond to the section of the hemispheres: R. The force of air pressure on a cylinder is easy to calculate. It's simply the product of pressure and circle area:

$$F_{air} = F'_{air} = \Delta p \; A_{\circ} = \pi R^2 \Delta p$$

The example then calculates to a force of

$$F_{air} = \pi \cdot (0.3)^2 (1.013 - 0.1) \; 10^5 \; N \approx 26 \; kN$$

which each group of horses has to come up with in order to separate the hemispheres. For comparison: One horsepower is approximately

735.5 Watt, so 30 horses would produce 22 kW. A horse pulls with approximately $10 - 12\,\%$ of its weight, i.e. with ca. 700 N or 21 kN for 30 horses.