MATH PROBLEMS, WITH SOLUTIONS

OVIDIU MUNTEANU

These are free online notes that I wrote to assist students that wish to test their math skills with some problems that go beyond the usual curriculum. These notes can be used as complimentary to an advanced calculus or algebra course, as training for math competitions or simply as a collection of challenging math problems. Many of these are my own creation, some from when I was a student and some from more recent times. The problems come with solutions, which I tried to make both detailed and instructive. These solutions are by no means the shortest, it may be possible that some problems admit shorter proofs by using more advanced techniques. So, in most cases, priority has been given to presenting a solution that is accessible to a student having minimum knowledge of the material. If you see a simpler, better solution and would like me to know it, I would be happy to learn about it. Of course, I will appreciate any comments you may have. I have included problems from linear algebra, group theory and analysis, which are numbered independently. In the future, I plan to expand this set and include problems from more fields as well.

1. Algebra

1. For two $n \times n$ invertible matrices A, B such that $AB + BA = O$, show that I, A, B and AB are linearly independent.

Solution: We can proceed directly: we want to show that if a, b, c, d are such that

$$aI + bA + cB + dAB = O,$$

then $a = b = c = d = 0$. Denote by $C = AB$, and observe that since $AB + BA = O$, we get $AC + CA = O$ and $BC + CB = O$ as well.
Now we multiply $aI + bA + cB + dAB = O$ to the left by A and get

$$aA + bA^2 + cAB + dAC = O,$$

which can be written as

$$(aI + bA - cB - dC)A = O.$$

As A is invertible, this implies

$$I + bA - cB - dC = O.$$

Together with $aI + bA + cB + dC = O$, it yields

$$\begin{cases} aI \ + bA = O \\ cB + dC = O \end{cases}.$$

The last equation can be simplified again, using that B is invertible. Indeed,

$$O = cB + dC = (cI + dA)B$$

implies

$$\begin{cases} aI + bA = O \\ cI + dA = O \end{cases}.$$

Each of these equations imply the coefficients are zero. Indeed, if there exist u and v so that $uI + vA = O$ and if $v \neq 0$, then $A = \lambda I$, for $\lambda = -\frac{u}{v}$. But then $O = AB + BA = 2\lambda B$, therefore $\lambda = 0$, which is a contradiction.

2. **Let A, B be two $n \times n$ matrices that commute. For any eigenvalue $\alpha \in \mathbb{C}$ of $A + B$, prove that there exists $\lambda \in \mathbb{C}$ and $\mu \in \mathbb{C}$ eigenvalues of A and B respectively, such that $\alpha = \lambda + \mu$.**

Solution: This result is well known, here we present an elementary proof. The fact that $\alpha \in \mathbb{C}$ is an eigenvalue of $A + B$ means that the system $(A + B) X = \alpha X$ has a nonzero solution, which we continue to denote with X.

Let $\lambda_1, .., \lambda_n$ and $\mu_1, .., \mu_n$ denote the eigenvalues of A and B, respectively. From $(A+B)\,X = \alpha X$ we get $BX = (\alpha I - A)\,X$, hence

$$(B - \mu_k I)\,X = ((\alpha - \mu_k)\,I - A)\,X,$$

for all $1 \leq k \leq n$. However, since $AB = BA$, it follows that:

$$\begin{aligned}
(B - \mu_2 I)\,(B - \mu_1 I)\,X &= (B - \mu_2 I)\,((\alpha - \mu_1)\,I - A)\,X \\
&= ((\alpha - \mu_1)\,I - A)\,(B - \mu_2 I)\,X \\
&= ((\alpha - \mu_1)\,I - A)\,((\alpha - \mu_2)\,I - A)\,X.
\end{aligned}$$

Continuing this argument, we obtain

$$(B - \mu_n I)\,...\,(B - \mu_1 I)\,X = CX,$$

where we have denoted

$$C := ((\alpha - \mu_n)\,I - A)\,....\,((\alpha - \mu_1)\,I - A)\,.$$

However, it is well known that B is a solution of its characteristic polynomial, therefore

$$(B - \mu_n I)\,...\,(B - \mu_1 I) = O.$$

This implies that the system $CX = 0$ has a nonzero solution, hence $\det C = 0$. Consequently, there must exist μ_k such that $\det\left((\alpha - \mu_k)\,I - A\right) = 0$, which means that $\alpha - \mu_k$ is an eigenvalue of A. This proves the statement.

3. Let A, B be two $n \times n$ invertible matrices with real entries. Prove the following claims:
(i) If $A + B$ is invertible and $(A+B)^{-1} = A^{-1} + B^{-1}$ then $\det A = \det B = \det(A+B)$.
(ii) If $n = 2$ and $\det A = \det B = \det(A+B)$ **then $A + B$ is invertible and** $(A+B)^{-1} = A^{-1} + B^{-1}$.

Solution: (i) : We use that

$$I = (A+B)(A^{-1} + B^{-1}) = 2I + AB^{-1} + BA^{-1}.$$

From here we see that $X + X^{-1} + I = O$, where $X := AB^{-1}$. This proves that X is a solution of the equation

$$X^2 + X + I = O.$$

Since the polynomial $Q(\lambda) = \lambda^2 + \lambda + 1$ is irreducible on $\mathbb{R}$, it follows that Q is the minimal polynomial of X. The characteristic polynomial and the minimal polynomial of X have the same irreducible factors over $\mathbb{R}$, hence we conclude that $n = 2k$ and the characteristic polynomial of X is $P(\lambda) = (\lambda^2 + \lambda + 1)^k$. This implies that $\det X = 1$, which means that $\det A = \det B$.

Moreover, from $X(X+I)=-I$ and $\det X=1$, we infer that $\det(X+I)=1$. This implies that

$$\det B=\det((X+I)B)=\det(A+B).$$

This proves (i).

(ii) : Using the notations at (i), it suffices to show that $X^2+X+I=O$. However, $\det A=\det B=\det(A+B)$ implies that $\det(AB^{-1})=\det(AB^{-1}+I)=1$, hence $P(0)=P(-1)=1$. In dimension $n=2$, the characteristic polynomial P of X has order 2, hence $P(\lambda)=\lambda^2+\lambda+1$. This implies $X^2+X+I=O$.

4. For n even, let A,B be two $n\times n$ matrices that commute, $AB=BA$. We assume that there exist $x_1,...,x_n$ non-negative and distinct so that $(A+x_kB)^n=O$, for all $k\in\{1,..,n\}$. Prove that $A^n=B^n=O$.

Solution: Let $C(x)=A+xB$ where $x\in\mathbb{R}$. Clearly, we have $C^n(x)=(c_{ij}(x))_{i,j=1,..,n}$, for some polynomials $c_{ij}(x)$ of order at most n. By hypothesis, we know that $C^n(x_k)=0$, which means that each c_{ij} vanishes on $x_1,..,x_n$.
Consequently,

$$c_{ij}(x)=(x-x_1)...(x-x_n)\,d_{ij},\ \text{where } d_{ij}\in\mathbb{R}.$$

We can say now that

$$C^n(x)=(x-x_1)...(x-x_n)\,D,$$

where D is an $n\times n$ matrix. On the other hand, since A and B commute, we immediately find that

$$C^n(x)=A^n+\left(nA^{n-1}B\right)x+...+\left(nAB^{n-1}\right)x^{n-1}+B^nx^n.$$

Let us denote now

$$(x-x_1)...(x-x_n)=x^n+s_1x^{n-1}+...+s_{n-1}x+s_n,$$

where

$$\begin{aligned}
s_1 &= -(x_1+...+x_n)\\
s_{n-1} &= (-1)^{n-1}\sum_i x_1...x_{i-1}x_{i+1}..x_n\\
s_n &= (-1)^n x_1.....x_n
\end{aligned}$$

Since with this notation we also have

$$C^n(x)=s_nD+(s_{n-1}D)\,x+....+(s_1D)\,x^{n-1}+Dx^n,$$

it follows that

$$D=B^n,\ \ s_1D=nAB^{n-1},\ \ s_{n-1}D=nA^{n-1}B,\ \ s_nD=A^n.$$

Therefore, we have proved that

$$A^n=s_nB^n,\ \ nA^{n-1}B=s_{n-1}B^n,\ \ nAB^{n-1}=s_1B^n.$$

We can readily obtain from here that

$$\begin{aligned} n^2A^nB &= nA(nA^{n-1}B) = s_{n-1}nAB^n = s_{n-1}s_1B^{n+1}, \\ n^2A^nB &= n^2s_nB^{n+1} \end{aligned}$$

On the other hand, we can prove that $s_1s_{n-1} > n^2s_n$, which by above implies that $B^{n+1} = 0$. Indeed, to show that $s_1s_{n-1} > n^2s_n$, we first notice that if $s_n = 0$, the inequality to prove is trivial, as only one of the numbers x_k could be zero. On the other hand, if $s_n > 0$, the inequality to be proved becomes

$$(x_1 + .. + x_n)\left(\frac{1}{x_1} + ... + \frac{1}{x_n}\right) > n^2,$$

which is true as the numbers are distinct.
Hence, $B^{n+1} = O$, which immediately implies $B^n = O$ as well, as the minimal polynomial and the characteristic polynomial of B have the same irreducible factors. As $A^n = s_nB^n$ it follows that $A^n = O$, as well.

5. We denote by $M_n(\mathbb{R})$, the set of $n \times n$ matrices with real entries. Assume a function $f : M_n(\mathbb{R}) \to \mathbb{R}$ has the properties that $f(X) \neq 0$ for all $X \neq O$ and that

$$f(XY) = f(X)f(Y),$$

for any $X, Y \in M_n(\mathbb{R})$. Show that $f(X) = 1$, for all $X \in M_n(\mathbb{R})$.

Solution: Let us first find $f(O)$. Since $f(O) = f(O)f(O)$, it follows $f(O) \in \{0, 1\}$. Let us assume by contradiction that $f(O) = 0$. Let $A, B \in M_n(\mathbb{R})$, such that both $A, B \neq O$ but $AB = O$. For example, B could have zeros everywhere except the first row, and A could have arbitrary entries except on the first column, where all entries are taken to be zero. Then clearly $AB = O$, and $0 = f(O) = f(AB) = f(A)f(B)$, which means that $f(X) = 0$, for some nonzero X. This is a contradiction. Hence, $f(O) = 1$ and now we notice that

$$1 = f(O) = f(OX) = f(O)f(X) = f(X),$$

for all X.

6. Let A, B, C be $n \times n$ matrices. Assume that two of the matrices A, B, C commute, where $C := AB - BA$. Prove that $C^n = O$.

Solution: For simplicity, we can assume that A commutes with C. We use that for two matrices X, Y the trace $\operatorname{tr}(XY - YX) = 0$. So, $\operatorname{tr}C = 0$, and for any $k > 0$, we have:

$$C^{k+1}=C^k(AB-BA)=C^kAB-\left(C^kB\right)A=A\left(C^kB\right)-\left(C^kB\right)A.$$

Again, we get that $\mathrm{tr}C^{k+1}=0$, using the above property for $X=A$ and $Y=C^kB$. We know that if C has eigenvalues $\lambda_1,..,\lambda_n\in\mathbb{C}$, then C^k has eigenvalues $\lambda_1^k,..,\lambda_n^k$, and $\mathrm{tr}C^k=\lambda_1^k+...+\lambda_n^k$. This shows

$$\lambda_1^k+...+\lambda_n^k=0,\quad \text{for any } k>0.$$

Using the characteristic polynomial of C,

$$P(\lambda)=\det(\lambda I_n-C)=\lambda^n+c_1\lambda^{n-1}+..+c_n$$

which has roots $\lambda_1,..,\lambda_n$, we get $c_1=..=c_n=0$. So, by the Cayley-Hamilton theorem, we obtain $C^n=O$.

7. Show that there exists $C\in M_2(\mathbb{C})$ such that $A^*=CA^tC^{-1}$, for any $A\in M_2(\mathbb{C})$. Determine all matrices C with this property. Here A^* denotes the adjoint matrix of A.

Solution: Denote $A=\begin{pmatrix} a & b\\ c & d\end{pmatrix}$, then $A^*=\begin{pmatrix} d & -b\\ -c & a\end{pmatrix}$. It is easy to find for $C=\begin{pmatrix} 0 & -1\\ 1 & 0\end{pmatrix}$ that $CA^t=\begin{pmatrix} -b & -d\\ a & c\end{pmatrix}$ and $CA^tC^{-1}=\begin{pmatrix} d & -b\\ -c & a\end{pmatrix}=A^*$.
So indeed, there exists C with the required property. Now we find all such matrices. Assume $D\in M_2(\mathbb{C})$ is another matrix such that $A^*=DA^tD^{-1}$, for any $A\in M_2(\mathbb{C})$. By $DA^tD^{-1}=CA^tC^{-1}$, we get $(C^{-1}D)A^t=A^t(C^{-1}D)$. This means the matrix $C^{-1}D$ commutes with all matrices in $M_2(\mathbb{C})$. It is known that this implies $C^{-1}D=\lambda I$, for some $\lambda\in\mathbb{C}$. We have proved that $D=\lambda C$, $\lambda\in\mathbb{C}^*$, so $D=\begin{pmatrix} 0 & -\lambda\\ \lambda & 0\end{pmatrix}$.

8. Find the number of functions

$$f:M_n(\mathbb{R})\to\mathcal{P}(\{1,2,...,m\})$$

such that

$$f(XY)\subseteq f(X)\cap f(Y),$$

for any $X,Y\in M_n(\mathbb{R})$. We have denoted with $\mathcal{P}(A)$ the set of subsets of A and $M_n(\mathbb{R})$ the set of all $n\times n$ matrices with real entries.

Solution: Observe first that

$$f(X)=f(XI)\subseteq f(X)\cap f(I)\subseteq f(I),$$

hence $f(X) \subseteq f(I)$, for any $X \in M_n(\mathbb{R})$. If $Y \in M_n(\mathbb{R})$ is invertible, we have

$$f(I) = f(YY^{-1}) \subseteq f(Y) \cap f(Y^{-1}) \subseteq f(Y).$$

This proves that $f(Y) = f(I)$, for any $Y \in M_n(\mathbb{R})$ invertible. Furthermore, if A is invertible and X arbitrary, then

$$\begin{aligned} f(AX) &\subseteq f(A) \cap f(X) \subseteq f(X) \quad \text{and} \\ f(X) &= f\left(A^{-1}AX\right) \subseteq f\left(A^{-1}\right) \cap f(AX) \subseteq f(AX). \end{aligned}$$

Again, this establishes that $f(AX) = f(X)$, for any A invertible. Let us consider an arbitrary $X \in M_n(\mathbb{R})$. It is a fact that there exist R, U_r, S, such that $X = RU_rS$, where R and S are invertible and U_r has the first r elements on the diagonal equal to 1 and all other entries equal to 0.

Now, from $X = RU_rS$ we get $f(X) = f(U_r)$. So the question reduces to computing $f(U_r)$. We first notice that $U_rU_{r+1} = U_r$ implies $f(U_r) \subseteq f(U_{r+1})$. We can in fact show that such an increasing sequence of subsets of $\{1, 2, ..., m\}$ characterizes a function f as in the problem. Indeed, if $(A_i)_{i=0,n}$ is an increasing subsequence of parts of $\{1, .., m\}$, we can define f by $f(X) = A_r$, if $\operatorname{rank}(X) = r$. This immediately implies that f satisfies

$$f(XY) \subseteq f(X) \cap f(Y), \text{ for any } X, Y \in M_n(\mathbb{R}),$$

as $\operatorname{rank}(XY) \leq \min\{\operatorname{rank}(X), \operatorname{rank}(Y)\}$. So to count the number of functions f, we need to compute the number of increasing sequences $(A_i)_{i=0,n}$, where $A_i \in \mathcal{P}(\{1, 2, .., m\})$. Let $k_0 := |A_0|$. To choose A_0 we have $\binom{m}{k_0}$ choices. For A_0 given, we choose $A_1 \backslash A_0$ from the $m - k_0$ remaining elements. So, if $k_1 := |A_1| - |A_0|$, with $k_1 \geq 0$, we have $\binom{m-k_0}{k_1}$ possibilities to choose $A_1 \backslash A_0$. By this reasoning, the number of sequences $(A_i)_i$ is

$$N := \sum_{0 \leq k_0 + ... + k_n \leq m} \binom{m}{k_0} \binom{m-k_0}{k_1} \cdots\cdots \binom{m-(k_0+k_1+...+k_{n-1})}{k_n}$$

We use that

$$\sum_{k_n=0}^{m-(k_0+...+k_{n-1})} \binom{m-(k_0+k_1+...+k_{n-1})}{k_n} = 2^{m-(k_0+..+k_{n-1})}$$

and

$$\sum_{k_{n-1}=0}^{m-(k_0+...+k_{n-2})} \binom{m-(k_0+k_1+...+k_{n-2})}{k_{n-1}} 2^{m-(k_0+..+k_{n-2})-k_{n-1}} = 3^{m-(k_0+..+k_{n-2})}.$$

Continuing, we get $N = (n+2)^m$.

1. Let $(G,\cdot)$ be a group. We assume that G has an odd number of elements and that there exists $a \in G$ and $n \in \mathbb{N}$, such that:

$$a^n \cdot x = x \cdot a,$$

for all $x \in G \backslash \{a^k \mid k \in \mathbb{N}\}$. Show that $ax = xa$, for any $x \in G$.

Solution: Let us denote with $H := \{a^k \mid k \in \mathbb{N}\}$. We know that $a^n = xax^{-1}$, for any $x \in G\backslash H$. Since H is a subgroup of G, this implies that if $x \notin H$, then $x^{-1} \notin H$ as well.
From above, this means that we also have $a^n = x^{-1}ax$, for any $x \in G\backslash H$. Therefore, this means $x^{-1}ax = xax^{-1}$, which implies that $x^2 a = ax^2$, for any $x \in G\backslash H$.
Now let's fix $x \in G\backslash H$, and assume by contradiction that $x^2 \in H$. We know that G has an odd number of elements, say that G has $= 2p+1$ elements. If $x^2 \in H$, it follows that $(x^2)^p \in H$. Since $x \in G\backslash H$, we see that $x^{2p+1} = x^{2p} \cdot x \in G\backslash H$. However, $x^{2p+1} = e \in H$, because G has order $2p+1$. This provides a contradiction, hence the assumption that $x^2 \in H$ is false. We have showed that $x \in G\backslash H$ implies $x^2 \in G\backslash H$ as well. It results that $a^n = x^2 a (x^2)^{-1}$. Since x^2 and a commute, this implies $a^n = a$. This immediately implies that $ax = xa$, for any $x \in G\backslash H$, which solves the problem.

2. Let $(G,\cdot)$ be a group with n elements, where n is not a multiple of 3. For a subset H of G we assume that $x^{-1}y^3 \in H$, for any $x, y \in G$. Prove that H is a subgroup of G.

Solution. Consider an element $a \in H$. We then have that $a^{-1}a^3 \in H$, so $a^2 \in H$. Continuing this, we get $(a^2)^{-1}(a^2)^3 \in H$, which means that $a^4 \in H$. From $a^4 \in H$ and $a \in H$ it follows that $(a^4)^{-1}a^3 \in H$, therefore $a^{-1} \in H$.
We have thus established that $a^{-1} \in H$, for any $a \in H$.
Now consider any two $x, y \in H$. Since $x \in H$, we know that $x^{-1} \in H$ as well. Now $x^{-1} \in H$ and $y \in H$ imply that $(x^{-1})^{-1}y^3 \in H$. This proves that $xy^3 \in H$, for any $x, y \in H$. Now we use induction on $p \in \mathbb{N}$ to prove that

$$xy^{3p} \in H, \quad \text{for any } x, y \in H.$$

Indeed, by induction we have that $xy^{3(p-1)} \in H$, and since $y \in H$, we get that

$$xy^{3p} = \left(xy^{3(p-1)}\right) \cdot y^3 \in H.$$

We discuss two cases:
Case I: $n = 3k+1$, for some $k \in \mathbb{N}$. Taking $p = k$ above we get, for any $x, y \in H$

$$xy^{-1} = xy^{n-1} \in H.$$

Indeed, we have used that $y^n = e$, as G has n elements. This proves H is a subgroup of G.
Case II: $n = 3k+2$, for some $k \in \mathbb{N}$. Taking $p = k+1$ we get for any $x, y \in H$ that

$$xy = xy^{n+1} = xy^{3k+3} \in H.$$

Again, this proves that H is a subgroup of G, because we have already established that $a^{-1} \in H$, for any $a \in H$.

3. Let G be a group. We assume there exists an homomorphism of groups $f : G \times G \to G$ and $a \in G$ such that

$$f(a, x) = f(x, a) = x,$$

for any $x \in G$. Prove that G is abelian.

Solution: Recall that $G \times G$ is a group with respect to

$$(x, y) \cdot (z, w) = (xz, yw).$$

Since f is a homomorphism, we have

$$f(xz, yw) = f(x, y) \cdot f(z, w).$$

It follows therefore that

$$f(x, e) \cdot f(a, a) = f(xa, ea) = f(xa, a) = xa,$$

where e denotes the identity element in G. Moreover, we also know by hypothesis that $f(a, a) = a$, which by above implies that

$$f(x, e) = x, \text{ for any } x \in G.$$

Similarly,

$$f(e, x) \cdot f(a, a) = f(a, xa) = xa,$$

which then implies that

$$f(x, e) = f(e, x) = x, \quad \text{for any } x \in G.$$

In

$$f(xz, yw) = f(x, y) \cdot f(z, w)$$

we first take $z = e$ and $y = e$ to get that

$$f(x, w) = x \cdot w$$

and now take $x = e$ and $w = e$ to get that

$$f(z, y) = y \cdot z.$$

This clearly implies G is abelian and also that

$$f(x,y) = x \cdot y, \text{ for any } x, y \in G.$$

4. Let $(G,\cdot)$ be a group with identity $e \in G$. We assume that there exists a surjective endomorphism $f : G \to G$, such that $H := \{x \in G \mid f(x) = e\}$ has the property that if K is a subgroup of G with $H \subseteq K \subseteq G$, then either $K = H$ or $K = G$. Prove that $G \simeq \mathbb{Z}$ or $G \simeq \mathbb{Z}_p$, for p prime.

Solution: We first show that $H = \{e\}$. Assuming there exists $x_0 \in H \backslash \{e\}$, we can let $K := \{x \in G \mid (f \circ f)(x) = e\}$ and $L := \{x \in G \mid (f \circ f \circ f)(x) = e\}$. These are both subgroups of G as $f \circ f$ and $f \circ f \circ f$ are endomorphisms of G. Furthermore, we can show $H \subset K \subset L$, with strict inclusions. Indeed, as f is onto, there exists $x_1 \in G$ such that $f(x_1) = x_0$. It follows that $(f \circ f)(x_1) = f(x_0) = e$, so $x_1 \in K$. Since $f(x_1) = x_0 \neq e$ it follows that $x_1 \in K \backslash H$. Similarly, there exists $x_2 \in G$ such that $f(x_2) = x_1$, and the same argument as above implies $x_2 \in L \backslash K$.
By hypothesis, this is a contradiction. The contradiction is to the assumption that there exists $x_0 \in H \backslash \{e\}$. Therefore, $H = \{e\}$ and G has no proper subgroups. This implies the conclusion.

5. Assume $(G,\cdot)$ is a group with an odd number of elements and there exist $x, y \in G$ such that $yxy = x$. Prove that $y = e$, where e is the identity in G.

Solution: From $yxy = x$ we successively get that $y = (yx)^{-1}x$, and $y = x(xy)^{-1}$. Equalizing the two formulas we get $(yx)^{-1}x = x(xy)^{-1}$. This is equivalent to $x(xy) = (yx)x$, so we have established that $x^2y = yx^2$. By induction, we can show that $x^{2p}y = yx^{2p}$. Indeed, $p = 1$ is already checked. If we assume now that $x^{2p}y = yx^{2p}$, we checked immediately that

$$\begin{aligned} x^{2(p+1)}y &= (x^{2p}x^2)y = x^{2p}(x^2y) \\ &= x^{2p}(yx^2) = yx^{2p}x^2 \\ &= yx^{2(p+1)}. \end{aligned}$$

Since G has an odd number of elements, we get from here that $xy = yx$. By hypothesis, we obtain $y^2 = e$. However, using again that G has an odd number of elements, we get $y = e$.

6. Let $(G,\cdot)$ be a group with identity e and $a \in G\backslash\{e\}$. We assume there exists an integer $n \geq 2$ such that $x^{n+1}a = ax$, for any $x \in G$. Prove that $x^{n^2} = e$, for any $x \in G$.

Solution: In $x^{n+1}a = ax$, we let substitute xa for x to get:

$$(xa)^{n+1}a = axa.$$

Simplifying, we get $(xa)^{n+1} = ax$. Since $ax = x^{n+1}a$, it follows that $(xa)^{n+1} = x^{n+1}a$. We rewrite this as $x(ax)^n a = xx^n a$, which simplifying again, implies $(ax)^n = x^n$. We have proved that

$$\begin{cases} (ax)^{n+1} = (ax)^n ax = x^n ax \\ (ax)^{n+1} = ax(ax)^n = axx^n \end{cases}$$

This implies $x^n ax = axx^n$, which gives $x^n a = ax^n$. Hence, x^n and a commute, for any $x \in G$. In $x^{n+1}a = ax$ we substitute x^n for x to see that $(x^n)^{n+1}a = ax^n$. Since $x^n a = ax^n$, this implies $x^{n(n+1)}a = x^n a$. We obtain that $x^{n^2} = e$, for any $x \in G$.

7. Find all groups $(G,\cdot)$ that are the union of three proper subgroups, one of which has a prime number of elements.

Solution: We know $G = H_1 \cup H_2 \cup H_3$, where $|H_3| = p$ for a prime number p. Let

$$\begin{aligned} x_1 &\in H_1\backslash(H_2 \cup H_3) \\ x_2 &\in H_2\backslash(H_1 \cup H_3). \end{aligned}$$

For example, such x_1 exists, as otherwise it will imply that $H_1 \subset (H_2 \cup H_3)$ so $G = H_2 \cup H_3$. However, it is known that a group cannot be written as the union of two proper subgroups. The existence of x_2 is established similarly.
Now, if $x_1x_2 \in H_1$, since $x_1 \in H_1$ we get $x_2 \in H_1$ as well. This is a contradiction to the definition of x_2. Similarly, one can see that $x_1x_2 \in H_2$ is not possible either. Hence, this leaves us with $x_1x_2 \in H_3\backslash(H_1 \cup H_2)$. Let us denote

$$a = x_1x_2.$$

Since $|H_3| = p$ and p is prime, it follows that

$$H_3 = \{e, a, a^2, ..., a^{p-1}\}.$$

Furthermore, for any $k \in \{1, ..., p-1\}$,

$$a^k \in H_3\backslash(H_1 \cup H_2).$$

Indeed, if $b := a^k$, then we have $H_3 = \{e, b, ..., b^{p-1}\}$. This shows that if $b \in H_1 \cup H_2$, then $H_3 \subset (H_1 \cup H_2)$, which is a contradiction because G would be the union of H_1 and H_2.

Now let $x \in H_1 \cap H_2$. The same as above, we can see that $ax \in H_3 \backslash (H_1 \cup H_2)$. It means there exists k such that $ax = a^k$, therefore $x = a^{k-1}$, and we must have $k = 1$. This proves that $H_1 \cap H_2 = \{e\}$. Obviously, we also have $H_2 \cap H_3 = \{e\}$ and $H_1 \cap H_3 = \{e\}$.Since

$$H_1 = \{H_1 \backslash (H_2 \cup H_3)\} \cup \{H_1 \cap H_2\} \cup \{H_1 \cap H_3\}$$

it remains to find $H_1 \backslash (H_2 \cup H_3)$. Let $x \in H_1 \backslash (H_2 \cup H_3)$, then $xx_2 \in H_3 \backslash (H_1 \cup H_2)$. Hence, there exists k so that $xx_2 = a^k$. We first suppose $k > 1$. Then,

$$xx_2 = a^{k-1} x_1 x_2$$

thus $x = a^{k-1} x_1$, and $a^{k-1} = xx_1^{-1} \in H_1$, contradiction. We further notice that $k = 0$ is impossible as well because it would imply $x_2 = x^{-1} \in H_1$. We must have $xx_2 = x_1 x_2$, so $x = x_1$. This shows $H_1 = \{e, x_1\}$, and similarly $H_2 = \{e, x_2\}$, with $x_1^2 = x_2^2 = e$. This shows

$$G = \{e, x_1, x_2, a, a^2, ..., a^{p-1}\}.$$

Since $ax_1 \in G \backslash \{e, x_1, a, ..., a^{p-1}\}$, we have $ax_1 = x_2$. It then results $x_1 x_2 = x_2 x_1$ and $a^2 = e$. This proves G is Klein's group of four elements.

8. Let $(G, \cdot)$ be a group and $n \in \mathbb{N}$, $n \equiv 2 (\mathrm{mod}\ 3)$ so that $(xy)^n = x^n y^n$ and $x^3 y^3 = y^3 x^3$, for any $x, y \in G$.
Show that $(G, \cdot)$ is abelian.

Solution: Let's use that $x^n y^n = (xy)^n = x(yx)^{n-1} y$, so $(yx)^{n-1} = x^{n-1} y^{n-1}$. From here we have

$$\begin{aligned} y^n x^n &= (yx)^n = yx(yx)^{n-1} \\ &= yxx^{n-1} y^{n-1} = yx^n y^{n-1}. \end{aligned}$$

This implies that

$$x^n y^{n-1} = y^{n-1} x^n.$$

Therefore, it follows that

$$\begin{aligned} x^{n(n-1)} y^{n(n-1)} &= (x^{n-1})^n (y^n)^{n-1} \\ &= (y^n)^{n-1} (x^{n-1})^n \\ &= y^{n(n-1)} x^{n(n-1)}. \end{aligned}$$

Furthermore, we have

$$\begin{aligned} (xy)^{n(n-1)} &= ((xy)^n)^{n-1} \\ &= (x^n y^n)^{n-1} \\ &= y^{n(n-1)} x^{n(n-1)}. \end{aligned}$$

This shows that
$$(yx)^{n(n-1)} = x^{n(n-1)}y^{n(n-1)}.$$
From here we get:
$$(xy)^{n(n-1)} = (yx)^{n(n-1)}, \text{ for any } x, y \in G.$$
Since $n \equiv 2 \pmod 3$ it follows that $n(n-1)+1 \equiv 0 \pmod 3$ hence $x^{n(n-1)+1}y^{n(n-1)+1} = y^{n(n-1)+1}x^{n(n-1)+1}$. Moreover, we have:
$$\begin{aligned} (xy)^{n(n-1)+1} &= x(yx)^{n(n-1)}y \\ &= xx^{n(n-1)}y^{n(n-1)}y \\ &= x^{n(n-1)+1}y^{n(n-1)+1} \end{aligned}$$
and the same as above it follows that
$$(xy)^{n(n-1)+1} = (yx)^{n(n-1)+1}, \text{ for any } x, y \in G.$$
If we denote by $m = n(n-1)$, then we have proved that
$$\begin{cases} (xy)^m = (yx)^m \\ (xy)^{m+1} = (yx)^{m+1} \end{cases}$$
Since now we have
$$(xy)^{m+1} = (yx)^{m+1} = (yx)^m (yx) = (xy)^m (yx),$$
we immediately get $xy = yx$, proving that G is abelian.

9. Determine all groups $(G, \cdot)$ with 2002 elements so that $f : G \to G$, defined by $f(x) = x^4$ is a group homomorphism.

Solution: We use that
$$x^4y^4 = (xy)^4 = x(yx)^3y$$
which implies $(yx)^3 = x^3y^3$. Hence, we have
$$\begin{aligned} y^4x^4 &= (yx)^4 = yx(yx)^3 \\ &= yxx^3y^3 = yx^4y^3. \end{aligned}$$
Simplifying this implies
$$x^4y^3 = y^3x^4.$$
This proves that
$$x^{12}y^{12} = (x^3)^4(y^4)^3 = (y^4)^3(x^3)^4 = y^{12}x^{12}.$$
We now observe that
$$(xy)^{12} = ((xy)^4)^3 = (x^4y^4)^3 = y^{12}x^{12},$$
therefore
$$(xy)^{12} = x^{12}y^{12} = y^{12}x^{12}, \text{ for any } x, y \in G.$$

Finally, this implies that

$$\begin{aligned}(xy)^{2004} &= ((xy)^{12})^{167} = (x^{12}y^{12})^{167} \\ &= (x^{12})^{167}(y^{12})^{167} = x^{2004}y^{2004}.\end{aligned}$$

Now we use that G has 2002 elements, so $a^{2004} = a^2$, for any $a \in G$. By above, this yields that: $(xy)^2 = x^2y^2$, for any $x, y \in G$. This immediately implies G is abelian. Since $|G| = 2002 = 2 \cdot 11 \cdot 91$, so $|G|$ is a free of squares it follows by a know result that G is isomorphic to $\mathbb{Z}_{2002}$.

10. Let $(A, +, \cdot)$ be a ring with an odd number of elements. We denote by $I := \{a \in A \mid a^2 = a\}$. Prove the following:
a) $|A| \geq 3\,|I| - 3$.
b) Determine A provided $|A| = 3\,|I| - 3$.

Solution:
a) We know A has an odd number of elements, say $|A| = 2n + 1$. Then we see that $2 \cdot (n + 1) = 1$, so $x = 2$ is invertible in A. Let us denote by $M := \{x \in A \mid x^2 = 1\}$. For any $x \in M$, we have

$$\big(2^{-1}(1 + x)\big)^2 = 4^{-1}(1 + 2x + 1) = 2^{-1}(1 + x),$$

hence $2^{-1}(1+x) \in I$. We define the function $f : M \to I$ by $f(x) := 2^{-1}(1+x)$, which is obviously bijective. Hence, $|M| = |I|$. Define also $J := \{a \in A \mid -a \in I\}$. Let us observe that

$$I \cap J = \{0\};\ I \cap M = \{1\} \ \text{ and } \ J \cap M = \{-1\}.$$

Indeed, if $a \in I \cap J$, then $a = -a = a^2$. As 2 is invertible, it results that $a = 0$. Now if $a \in I \cap M$, we get $a^2 = 1$ and $a^2 = a$, so $a = 1$. Since I, J, M have the same number of elements, this yields that $|A| \geq 3\,|I| - 3$.
b) If A has exactly three elements, it follows that A is isomorphic to $\mathbb{Z}_3$. Assuming $|A| > 3$, we can show that A is isomorphic to $\mathbb{Z}_3 \times \mathbb{Z}_3$. From the proof of a), we know that $A = I \cup J \cup M$.
Therefore, for any $x \in A$, we have that

$$x^2 \in \{1, x, -x\}.$$

Since 2 is invertible in A, from here we immediately get that $3 = 0$. Furthermore, we observe that the invertible elements of A must belong to M, so $(M, \cdot)$ forms an abelian group. Choose any $a \in I \backslash \{0, 1\}$. Since f is bijective, there exists a corresponding $y \in M$ such that $a = -y - 1$. Now let $x \in M$ be arbitrary. Since x and y commute, we see that x and a commute. If ax is invertible, it would mean a is invertible as well, so $a = 1$. This is a contradiction, which means $ax \in I \cup J$. Let us assume $ax \in I$, therefore

$$ax = (ax)^2 = a^2x^2 = a.$$

Now notice that

$$(a-x)^2 = a - 2a + 1 = 1 - a;$$

and on the other hand, $(a-x)^2 \in \{1, a-x, x-a\}$. This implies that $x \in \{1, -a-1\}$. In the second case, when $ax \in J$, a similar computation gives that $x \in \{-1, a+1\}$. Since a was fixed, it follows that

$$M \subset \{-1, 1, -a-1, a+1\}.$$

It is easy to check the converse inclusion is true as well, therefore $|M| = 4$, and now $A \simeq \mathbb{Z}_3 \times \mathbb{Z}_3$ follows directly from here.

11. Let $(A, +, \cdot)$ be a commutative ring, having $2n+1$ elements, where $n \neq 4$. Let us assume that if $a \in A$ is not invertible, then $a^2 \in \{-a, a\}$. Prove that A is a field.

Solution. Let us assume by contradiction that A is not a field. Then there exists $a \in I \backslash \{0, 1\}$, where $I := \{a \in A : a^2 = a\}$. Indeed, we know there exists $x \in A \backslash \{0, 1\}$, which is not invertible. By hypothesis, it follows that $x^2 \in \{-x, x\}$. Then, for either $a = x$ or $a = -x$, we can arrange that $a^2 = a$. So the set I has at least three elements. Now take any $x \in A$, which is invertible. The element ax cannot be invertible, because a is not. Therefore, $(ax)^2 \in \{ax, -ax\}$. Using that A is commutative, it follows that $ax \in \{a, -a\}$.
We now use that the group $(A, +)$ has $2n+1$ elements, which in particular implies that $2(n+1) = 1$. Hence, this shows that 2 is invertible in A, which from above we know it implies that $2a = -a$. This means that $3 \in A$ is not invertible, which by hypothesis it implies that $3^2 \in \{3, -3\}$. In both cases we get that $3 = 0$.
Recall that for any $x \in A$ invertible, we have $ax \in \{a, -a\}$. If $ax = a$, it follows that

$$\begin{aligned}
(x-a)^2 &= x^2 - 2ax + a^2 \\
&= x^2 - 2a + a^2 \\
&= x^2 - a^2 \\
&= (x-a)(x+a).
\end{aligned}$$

We see that $x - a$ cannot be invertible, as otherwise we get $x - a = x + a$, so $a = 0$. Hence, since $x - a$ is not invertible, we get $(x-a)^2 \in \{x-a, -x+a\}$. Consequently, this means that $x^2 - a \in \{x-a, -x+a\}$. If $x^2 - a = x - a$, then $x = 1$, as x is invertible. If $x^2 - a = -x + a$ then $x(x+1) = -a$ which implies that $x + 1$ is not invertible. In this case, we use the hypothesis again to conclude that $(x+1)^2 \in \{x+1, -x-1\}$, which now implies that $x^2 = 1$. Indeed, if $(x+1)^2 = x+1$, then $x^2 + x = 0$, which

implies $x = -1$. If $(x+1)^2 = -x - 1$, we find that $x^2 + 3x + 2 = 0$. Using that $3 = 0$ in A, it follows that $x^2 = 1$. As we have established above that $x^2 + x + a = 0$, using $x^2 = 1$, we get that $x = -a - 1$. Concluding, this shows that if $ax = a$, then $x \in \{1, -a-1\}$.
On the other hand, if $ax = -a$, then we proceed similarly for $(x+a)^2 = x^2 - a^2$, and get that $x \in \{-1, a+1\}$.
This proves that any invertible element of A belongs to $\{-1, 1, -a-1, a+1\}$ and the converse is easily checked as well. Certainly, if $b \in I \backslash \{0, 1\}$ is different from a, the argument above shows that

$$\{-1, 1, -a-1, a+1\} = \{-1, 1, -b-1, b+1\},$$

thus $b = 1 - a$. Therefore,

$$A = \{0, -1, 1, -a, a, -a-1, a+1, a-1, -a+1\}$$

which is a contradiction because A cannot have 9 elements. Thus A is a field.

12. Let $(A, +, \cdot)$ be a ring without zero divisors and $a \in A \backslash \{0\}$. Assume that there exists $n \in \mathbb{N}$ so that $x^{n+1}a = ax$, for any $x \in A$. Prove that A is a field.

Solution: In $x^{n+1}a = ax$, we take $x = xa$ and get: $(xa)^{n+1}a = axa$. Simplifying by a, as A does not have zero divisors, we get $(xa)^{n+1} = ax$. Moreover, we have $ax = x^{n+1}a$, which yields $(xa)^{n+1} = x^{n+1}a$. We rewrite this as $x\left((ax)^n - x^n\right)a = 0$. Again, simplifying by a and x, we see that $(ax)^n = x^n$, for any $x \in A \backslash \{0\}$. This proves that

$$\begin{cases} (ax)^{n+1} = (ax)^n ax = x^n ax \\ (ax)^{n+1} = ax(ax)^n = axx^n \end{cases}$$

which implies that

$$x^n ax = axx^n.$$

We rewrite this as $(x^n a - ax^n)x = 0$, which implies that $x^n a = ax^n$, for any $x \in A \backslash \{0\}$. In $x^{n+1}a = ax$ we now make $x = x^n$ to obtain:

$$(x^n)^{n+1}a = ax^n.$$

By this, we get $x^{n(n+1)}a = x^n a$, which means $x^n(x^{n^2} - 1)a = 0$. Now we notice that if $x \in A \backslash \{0\}$, then $x^n \in A \backslash \{0\}$ as well. We can therefore conclude that

$$x^{n^2} = 1, \text{ for any } x \in A \backslash \{0\}.$$

This means A is a field.

2. Analysis

1. Let $f : [0,\infty) \to \mathbb{R}$ be smooth such that $f^{(n)}(x) \geq 1$, for any $x \geq 0$ and $n \in \mathbb{N}$. Prove that $f^{(n)}(x) \geq e^x$, for any $x \geq 0$ and $n \in \mathbb{N}$.

Solution: We show that $f(x) \geq e^x$, for any $x \geq 0$. Let $n \in \mathbb{N}$ and $g : [0,\infty) \to \mathbb{R}$ defined by $g(x) = f(x) - \left(1 + \frac{x}{1!} + ... + \frac{x^n}{n!}\right)$. By induction after $k \in \mathbb{N}$ one computes

$$g^{(k)}(x) = f^{(k)}(x) - \left(1 + \frac{x}{1!} + ... + \frac{x^{(n-k)}}{(n-k)!}\right),$$

so $g^{(n)}(x) = f^{(n)}(x) - 1 \geq 0$. This means $g^{(n-1)}$ is increasing. However, $g^{(n-1)}(x) = f^{(n-1)}(x) - \left(1 + \frac{x}{1!}\right)$, therefore $g^{(n-1)}(0) = f^{(n-1)}(0) - 1 \geq 0$. Hence, this shows that $g^{(n-1)}$ is nonnegative. It follows that $g^{(n-2)}$ in increasing. Continuing, we eventually get that g' nonnegative, hence g increasing. But $g(0) = f(0) - 1 \geq 0$, so g nonnegative. This argument shows $f(x) \geq 1 + \frac{x}{1!} + ... + \frac{x^n}{n!}$, for any $n \in \mathbb{N}$. Taking a limit as $n \to \infty$ we obtain $f(x) \geq e^x$, for any $x \in [0,\infty)$. For $p \in \mathbb{N}$ arbitrary, we let $h : [0,\infty) \to \mathbb{R}$, $h(x) = f^{(p)}(x)$. Then h is smooth and $h^{(n)}(x) \geq 1$, for any n. The above argument shows $h(x) \geq e^x$.

2. Assume $f : (-2,2) \to \mathbb{R}$ is bounded and has the property that for any $x, y \in (-2,2)$, $x \neq y$, there exists $z \in (-2,2)$ such that

$$f(x) - f(y) = (x-y)f(z).$$

a) Is f differentiable on $(-2,2)$?
b) If, in addition, we know that z is always between x and y, find f.

Solution:
a). Define $f : (-2,2) \to \mathbb{R}$ by

$$f(x) = \begin{cases} \frac{1}{2}x, & x \in (-2,0) \\ x, & x \in (0,2) \end{cases}$$

We prove that for any $x, y \in (-2,2), x \neq y$, there exists $z \in (-2,2)$ such that

$$f(x) - f(y) = (x-y)f(z).$$

However, it is clear that f is not differentiable at $x = 0$.
We have the following cases:
If $x, y \in (0,2)$, then $f(x) = x$ and $f(y) = y$, so

$$\frac{f(x) - f(y)}{x-y} = 1 = f(1)$$

If $x \in (-2,0]$, $y \in (0,2)$ then $f(x) = \frac{1}{2}x$ and $f(y) = y$. Denoting $a := -x$ we have

$$\frac{f(x)-f(y)}{x-y} = \frac{\frac{1}{2}x - y}{x-y} = \frac{y+\frac{1}{2}a}{y+a}.$$

Let us observe that

$$0 < \frac{y+\frac{1}{2}a}{y+a} \leq 1.$$

Since $f : (-2,2) \to (-1,2)$ is onto, it follows that there exists $z \in (-2,2)$ such that

$$f(z) = \frac{y+\frac{1}{2}a}{y+a} = \frac{f(x)-f(y)}{x-y}.$$

If $x, y \in (-2,0]$ then

$$\frac{f(x)-f(y)}{x-y} = \frac{1}{2}$$

and

$$f(\frac{1}{2}) = \frac{1}{2} = \frac{f(x)-f(y)}{x-y}.$$

This shows f has the required property, but it is not differentiable in zero.
b). Since f is bounded, we have $|f(z)| \leq M$, for any $z \in (-2,2)$. In particular,

$$|f(x)-f(y)| \leq M\,|x-y|\,,$$

which shows f is continuous. Furthermore, for $x \in (-2,2)$ arbitrary, we show $f'(x) = f(x)$. Let $y \in (-2,2)$, $y \neq x$. There exists z between x and y so that

$$f(z) = \frac{f(y)-f(x)}{y-x}.$$

When $y \to x$ we have $z \to x$, as well. Since f is continuous in x we get that f is differentiable in x and $f'(x) = f(x)$. This proves $f(x) = ce^x$.

3. Let $f : [0,1] \to [0,1]$ be continuous such that for any $x \in [0,1]$,

$$f(x) \in \{\sin(f(x)),\ f(\sin(x))\}$$

Prove that f is constant.

Solution: Let $x \in [0,1]$. If $f(x) = \sin(f(x))$, since $f(x) \in [0,1]$ and $\sin y = y$ has a unique solution $y = 0$ for $y \in [0,1]$, it follows that $f(x) = 0$. Of course, if $f = 0$ the problem is solved. We may assume there exists $a \in [0,1]$ such that $f(a) \neq 0$. From what we proved above we infer that $f(a) = f(\sin a)$. Let $b = \sin a$, then $f(b) = f(a) \neq 0$ and $f(b) \in \{\sin(f(b), f(\sin(b))\}$. As above we can deduce that $f(b) = f(\sin b)$. Hence, $f(a) = f(\sin(\sin a))$. Continuing, we get

$$f(a) = f(\sin \circ \ldots. \circ \sin(a)),$$

for any $n \in \mathbb{N}$. However, let us show that
But

$$\lim_{n\to\infty} \sin \circ .... \circ \sin a = 0.$$

Indeed, let $a_n := \sin a_{n-1}$,and $a_0 := a \in [0,1]$. We find that $a_n = \sin a_{n-1} \leq a_{n-1}$, so a_n is decreasing. Furthermore, $a_n \in [0,1]$, hence a_n is convergent, being monotone and bounded. Denoting $l := \lim_{n\to\infty} a_n$, the fact that $a_n = \sin a_{n-1}$ implies in the limit that $l = \sin l$. Since $l \in [0,1]$, we conclude that $l = 0$.
Hence, we have that

$$f(a) = \lim_{n\to\infty} f(\sin \circ ... \circ \sin a) = f(\lim_{n\to\infty} \sin \circ .... \circ \sin a) = f(0),$$

where we have used that f is continuous in 0. We now let $\alpha := f(0)$. From what we have showed so far, we have that $f(x) \in \{0, \alpha\}$, for any $x \in [0,1]$. Now f must be constant, as it is continuous.

4. Let $a, b \in \mathbb{R}$, such that $a^2 + b^2 < 1$. Define

$$I(a,b) = \int_0^{2\pi} \frac{1}{\sqrt{1 + a\cos t + b\sin t}} dt$$

Prove that $I(a,b) \geq 2\pi$, and equality holds if and only if $a = b = 0$.

Solution: Define

$$F(x) = \int_0^x \frac{1}{\sqrt{1 + q\cos s}} ds,$$

where $q = \sqrt{a^2 + b^2} \in [0,1)$. There exists $\theta \in [0, 2\pi)$, such that $a = q\cos\theta$ and $b = -q\sin\theta$. We have that I depends on both q and θ, and

$$I(q,\theta) = \int_0^{2\pi} \frac{1}{\sqrt{1 + q\cos(t+\theta)}} dt.$$

Here we make the change of variable $t + \theta = s$ to get

$$I(q,\theta) = \int_\theta^{\theta+2\pi} \frac{1}{\sqrt{1 + q\cos s}} ds = F(\theta + 2\pi) - F(\theta).$$

Consequently, for $q \in [0,1)$ fixed, we have that

$$\frac{dI}{d\theta} = F'(\theta + 2\pi) - F'(\theta) = \frac{1}{\sqrt{1 + q\cos(\theta + 2\pi)}} - \frac{1}{\sqrt{1 + q\cos\theta}} = 0.$$

This shows that I is independent of θ, and depends only on q. Hence,

$$I(q,\theta) = I(q,0) = \int_0^{2\pi} \frac{1}{\sqrt{1 + q\cos t}} dt.$$

We now observe that

$$\begin{aligned} I(q,0) &= \int_0^{2\pi} \frac{1}{\sqrt{1+q\cos t}}dt = 2\int_0^{\frac{\pi}{2}} \left(\frac{1}{\sqrt{1+q\cos t}} + \frac{1}{\sqrt{1-q\cos t}} \right) dt \\ &\geq 4\int_0^{\frac{\pi}{2}} \frac{1}{(1-q^2\cos^2 t)^{\frac{1}{4}}}dt \geq 4\frac{\pi}{2} = 2\pi. \end{aligned}$$

Above, we used that

$$\begin{aligned} \frac{1}{\sqrt{1+q\cos t}} + \frac{1}{\sqrt{1-q\cos t}} &\geq 2\sqrt{\frac{1}{\sqrt{1+q\cos t}\sqrt{1-q\cos t}}} \\ &= \frac{2}{(1-q^2\cos^2 t)^{\frac{1}{4}}} \end{aligned}$$

and that

$$1 - q^2\cos^2 t \leq 1,$$

respectively. It is obvious from here that equality here holds only if $q = 0$.

5. We let

$$F = \{f : [0,1] \to (0,\infty), \;\; f \text{ is increasing on } [0,1]\}.$$

For $n \in \mathbb{N}$, **find**

$$\min_{f\in F} \frac{\int_0^1 tf^n(t)dt}{\left(\int_0^1 f(t)dt\right)^n}.$$

Solution: As f is increasing and positive, f^n is increasing as well, for any $n \in \mathbb{N}$. We can apply Chebyshev's inequality to get:

$$\begin{aligned} \int_0^1 tf^n(t)dt &\geq \left(\int_0^1 tdt\right)\left(\int_0^1 f^n(t)dt\right) \\ &= \frac{1}{2}\int_0^1 f^n(t)dt. \end{aligned}$$

From Hölder's inequality, it follows, for any $n \geq 2$

$$\left(\int_0^1 f(t)dt\right)^n \leq \int_0^1 f^n(t)dt,$$

which yields

$$\int_0^1 tf^n(t)dt \geq \frac{1}{2}\left(\int_0^1 f(t)dt\right)^n, \;\; \text{for any } n \in \mathbb{N}.$$

This proves that

$$\frac{\int_0^1 t f^n(t)dt}{\left(\int_0^1 f(t)dt\right)^n} \geq \frac{1}{2}.$$

Since the value $\frac{1}{2}$ is achieved for $f = 1 \in F$, it means the desired value is $\frac{1}{2}$.

6. Let $f : [0,1] \to \mathbb{R}$ be differentiable so that

$$f'(x) + e^{f(x)} = e^x \text{ , for any } x \in [0,1].$$

Assuming $f(0) \in [0,1]$, prove that $f(x) \in [0,1]$, for any $x \in [0,1]$.

Solution: Let

$$g : [0,1] \to \mathbb{R}, \quad g(x) = \begin{cases} \frac{e^{f(x)}-1}{f(x)} & \text{if } f(x) \neq 0 \\ 1 & \text{if } f(x) = 0 \end{cases}$$

Notice that g is continuous, as if $f(a) = 0$ then

$$\lim_{x\to a} g(x) = \lim_{x\to a} \frac{e^{f(x)}-1}{f(x)} = \lim_{y\to 0} \frac{e^y - 1}{y} = 1,$$

Now the function

$$u : [0,1] \to \mathbb{R}, \quad u(x) = f(x)e^{\int_0^x g(t)dt}$$

is differentiable and

$$\begin{aligned} u'(x) &= e^{\int_0^x g(t)dt}\left(f'(x) + f(x)g(x)\right) \\ &= e^{\int_0^x g(t)dt}\left(f'(x) + f(x)\frac{e^{f(x)}-1}{f(x)}\right) \\ &= e^{\int_0^x g(t)dt}\left(e^x - 1\right) \geq 0. \end{aligned}$$

This shows u is increasing. But $u(0) = f(0) \geq 0$, hence $u(x) \geq 0$, and this proves $f(x) \geq 0$.

Now we show $f(x) \leq 1$, for any $x \in [0,1]$. In this sense, we define:

$$h : [0,1] \to \mathbb{R}, \quad h(x) = \begin{cases} \frac{e-e^{f(x)}}{1-f(x)} & \text{if } f(x) \neq 1 \\ e & \text{if } f(x) = 1 \end{cases}$$

which is also continuous. Then the function

$$v : [0,1] \to \mathbb{R}, \quad v(x) = (1 - f(x))\, e^{\int_0^x h(t)dt}.$$

is differentiable and

$$\begin{aligned} v'(x) &= e^{\int_0^x h(t)dt}\left(-f'(x) + h(x)(1-f(x))\right) \\ &= e^{\int_0^x h(t)dt}\left(-f'(x) + e - e^{f(x)}\right) \\ &= e^{\int_0^x h(t)dt}\left(e - e^{x}\right) \geq 0. \end{aligned}$$

So v is increasing, and since $v(0) = 1 - f(0) \geq 0$, this shows $v(x) \geq 0$, i.e., $f(x) \leq 1$.

7. Let us define the sequence $f_n : [0,1] \to \mathbb{R}$ of continuous functions by:

$$f_{n+1}(x) = \int_0^1 \frac{\ln(1+tx)}{t} f_n(t)dt \ , \text{ where } n \in \mathbb{N}.$$

Prove that

$$\lim_{n\to\infty} f_n(x) = 0, \text{ for any } x \in [0,1] \, .$$

Solution: For any $x \in [0,1]$, we have

$$\ln(1+tx) \leq \ln(1+t),$$

which shows

$$\int_0^1 \frac{\ln(1+tx)}{t} dt \leq \int_0^1 \frac{\ln(1+t)}{t} dt.$$

Let us denote by

$$M = \int_0^1 \frac{\ln(1+t)}{t} dt.$$

We can show that $M < 1$. Indeed, it is known that $\ln(1+t) < t$, for any $t \in (0,1]$. Integrating, we have

$$\int_0^1 \frac{\ln(1+t)}{t} dt < 1,$$

so $M < 1$. We have thus proved that

$$\int_0^1 \frac{\ln(1+tx)}{t} dt \leq M < 1, \text{ for any } x \in [0,1].$$

Let us denote now

$$M_n := \sup_{t\in[0,1]} f_n(t).$$

For $x \in [0,1]$ fixed, we have:

$$\begin{aligned} |f_{n+1}(x)| &\leq \int_0^1 \frac{\ln(1+tx)}{t} |f_n(t)|\, dt \\ &\leq M_n \int_0^1 \frac{\ln(1+tx)}{t} dt \\ &\leq MM_n. \end{aligned}$$

Maximizing in x, this implies that

$$M_{n+1} \leq MM_n.$$

We iterate this to find

$$M_n \leq MM_{n-1} \leq M^2 M_{n-2} \leq .... \leq M^n M_0$$

and since $M < 1$, we get

$$\lim_{n\to\infty} M_n = 0.$$

Since $|f_{n+1}(x)| \leq MM_n$, we obtain

$$\lim_{n\to\infty} f_n(x) = 0.$$

8. Let $f : \mathbb{R} \to \mathbb{R}$ be continuous. We assume there exists a divergent sequence $(a_n)_{n\in\mathbb{N}}$ so that $(f(a_n))_{n\in\mathbb{N}}$ is convergent and

$$\lim_{n\to\infty} f(a_n) \in \mathrm{Im}\,(f)\,.$$

Show that f is not one to one.
Here we have denoted $\mathrm{Im}(f) := \{y \in \mathbb{R} : \ y = f\,(x) \quad$ **for some** $x \in \mathbb{R}\}$.

Solution: We assume by contradiction that f is injective. Since f is continuous and injective, it results that f is monotone. Hence, the following limit exists:

$$L := \lim_{x\to\infty} f(x).$$

Let us observe that $(a_n)_{n\in\mathbb{N}}$ is not bounded. Indeed, if (a_n) were bounded, since it is divergent, it must have two subsequences $(a_{n_k})_{k\in\mathbb{N}} \to a$ and $\exists (a_{n'_k})_{k\in\mathbb{N}} \to b$, where $a \neq b$. Since f is continuous, it follows that

$$\lim_{k\to\infty} f(a_{n_k}) = f(a) \text{ and } \lim_{k\to\infty} f(a_{n'_k}) = f(b).$$

Since $\left(f\,(a_n)\right)_n$ is convergent, the limit must be the same, so $f(a) = f(b)$. This contradicts that f is injective.

Therefore, $(a_n)_n$ is unbounded, which without loss of generality means we can extract a subsequence $(a_{n_k})_{k\in\mathbb{N}}$ of a_n, so that

$$\lim_{k\to\infty} a_{n_k} = \infty.$$

We have

$$\begin{aligned} L &= \lim_{x\to\infty} f(x) = \lim_{k\to\infty} f(a_{n_k}) \\ &= \lim_{n\to\infty} f(a_n) \in \operatorname{Im}(f). \end{aligned}$$

This proves that there exists $a \in \mathbb{R}$ so that $L = f(a)$. This contradicts f is injective.