Solutions for the AAC Competition Problems 2009

1. The sum $\frac{1}{1}+\frac{1}{2}+\cdots+\frac{1}{1200}$ is rewritten as a fraction $\frac{m}{n}$. Prove that m is divisible by 1201.

We pair up the terms of the sum as follows:

$$\sum_{k=1}^{1200}\frac{1}{k}=\sum_{k=1}^{600}\left(\frac{1}{k}+\frac{1}{1201-k}\right),$$

which yields $\frac{m}{n}=\sum_{k=1}^{600}\frac{1201}{k(1201-k)}=1201\cdot\frac{a}{1200!}$ where a is an integer. Hence $m\cdot 1200!$ is divisible by 1201. Since 1201 is a prime, it follows that m is divisible by 1201.

2. A square matrix will be called *magic* if all row sums, column sums and diagonal sums (i.e., for the main diagonal and for the secondary diagonal) are equal to each other. Find the dimension of the space of all magic $n\times n$ matrices.

Let $\mathbb{K}$ be the field that contains the entries of matrices in question. The answer may depend on $\operatorname{char}\mathbb{K}$.

For an $n\times n$ matrix $A=(a_{ij})_{i,j=1}^{n}$, consider the i-th row sum: $r_i(A)=\sum_{j=1}^{n}a_{ij}$, the j-th column sum: $c_j(A)=\sum_{i=1}^{n}a_{ij}$, and the two diagonal sums: $d(A)=\sum_{i=1}^{n}a_{ii}$ (the main diagonal) and $q(A)=\sum_{i=1}^{n}a_{i,n+1-i}$ (the secondary diagonal). Thus r_i, c_j, d and q are linear functionals on the space $\mathrm{Mat}_n(\mathbb{K})$ of $n\times n$ matrices. Then the subspace $\mathcal{M}\subset\mathrm{Mat}_n(\mathbb{K})$ of all magic $n\times n$ matrices is determined by the equations:

$$\begin{cases} r_1(A)-q(A) &= 0,\\ &\dots\\ r_n(A)-q(A) &= 0,\\ c_1(A)-q(A) &= 0,\\ &\dots\\ c_n(A)-q(A) &= 0,\\ d(A)-q(A) &= 0.\end{cases}$$

Define the linear functionals $\tilde{r}_i=r_i-q$ $(i=1,\dots,n)$, $\tilde{c}_j=c_j-q$ $(j=1,\dots,n)$, and $\tilde{d}=d-q$. Let $\mathcal{S}$ be the subspace of the dual space $\mathrm{Mat}_n(\mathbb{K})^*$

spanned by these functionals. Then the above system of equations says that $\mathcal{M} = \mathcal{S}^{\perp}$. Therefore, $\dim \mathcal{M} = \dim \mathrm{Mat}_n(\mathbb{K}) - \dim \mathcal{S}$, so it suffices to find $\dim \mathcal{S}$.

Note that the functionals $\tilde{r}_1, \ldots, \tilde{r}_n$, $\tilde{c}_1, \ldots, \tilde{c}_n$, $\tilde{d}$ are linearly dependent: the obvious relation

$$\sum_i r_i(A) = \sum_{i,j} a_{ij} = \sum_j c_j(A)$$

implies

$$\sum_{i=1}^n \tilde{r}_i - \sum_{j=1}^n \tilde{c}_j = 0. \tag{1}$$

We will now explore all possible linear relations among the functionals $\tilde{r}_1, \ldots, \tilde{r}_n$, $\tilde{c}_1, \ldots, \tilde{c}_n$, $\tilde{d}$.

Define $\epsilon_{ij}(A) = a_{ij}$. Then $\{\epsilon_{ij} \mid i, j = 1, \ldots, n\}$ is a basis for the space $\mathrm{Mat}_n(\mathbb{K})^*$, and we have

$$r_i = \textstyle\sum_{j=1}^n \epsilon_{ij}, \quad c_j = \sum_{i=1}^n \epsilon_{ij},$$
$$d = \textstyle\sum_{i=1}^n \epsilon_{ii}, \quad q = \sum_{i=1}^n \epsilon_{n+1-i,i}.$$

Now consider a linear relation

$$\sum_{i=1}^n \alpha_i \tilde{r}_i + \sum_{j=1}^n \beta_j \tilde{c}_j + \gamma \tilde{d} = 0. \tag{2}$$

Equivalently,

$$\sum_{i=1}^n \alpha_i r_i + \sum_{j=1}^n \beta_j c_j + \gamma d - \delta q = 0, \tag{3}$$

where $\delta = \sum \alpha_i + \sum \beta_j + \gamma$.

Expanding the left-hand side of (3) and using the notation $m = (n+1)/2$ and

$$\Delta = \{(i, j) \mid i = j \text{ or } i + j = n + 1\},$$

we obtain

$$\begin{aligned} &\sum_{(i,j)\notin\Delta} (\alpha_i + \beta_j)\epsilon_{ij} \\ &+ \sum_{i\neq m} (\alpha_i + \beta_i + \gamma)\epsilon_{ii} + \sum_{i\neq m} (\alpha_i + \beta_{n+1-i} - \delta)\epsilon_{i,n+1-i} \\ &+ (\alpha_m + \beta_m + \gamma - \delta)\epsilon_{m,m} \ = \ 0, \end{aligned}$$

where the last term should be omitted if n is even. Since the elements $\epsilon_{1,j}$ for $j = 2, \ldots, n-1$ appear in the first sum, it follows that $\beta_2 = \cdots = \beta_{n-1} = -\alpha_1$. Similarly, we obtain $\beta_2 = \cdots = \beta_{n-1} = -\alpha_n$ and $\alpha_2 = \cdots = \alpha_{n-1} = -\beta_1 = -\beta_n$. Thus all α's and β's can be expressed through, say, α_1 and α_2.

If $n > 4$, then, say, $\epsilon_{2,3}$ appears in the first sum, so $\beta_3 = -\alpha_2$, which yields $\alpha_1 = \alpha_2$. We conclude that $\alpha_i = \alpha_1$ and $\beta_i = -\alpha_1$ for all i, j. Looking at $\epsilon_{1,1}$ in the second sum, we see that $\gamma = 0$. Therefore, relation (2) is a scalar multiple of relation (1). Hence in this case $\dim \mathcal{S} = (2n+1) - 1 = 2n$ and $\dim \mathcal{M} = n^2 - 2n$, regardless of $\operatorname{char} \mathbb{K}$.

If $n = 4$, then looking at $\epsilon_{1,1}$ and $\epsilon_{2,2}$ (in the second sum), we obtain $\alpha_1 + \beta_1 = -\gamma = \alpha_2 + \beta_2$, which yields $\alpha_1 - \alpha_2 = \alpha_2 - \alpha_1$. If $\operatorname{char} \mathbb{K} \neq 2$, then this implies $\alpha_1 = \alpha_2$ and hence relation (2) is a scalar multiple of relation (1), as before. If $\operatorname{char} \mathbb{K} = 2$, then α_1 and α_2 remain independent. Since $\gamma = \alpha_1 - \alpha_2$, we see that relation (2) is a linear combination of (1) and the following relation:

$$\tilde{r}_1 + \tilde{r}_4 + \tilde{c}_2 + \tilde{c}_3 + \tilde{d} = 0, \tag{4}$$

which is obtained by setting $\alpha_1 = 1$ and $\alpha_2 = 0$. It is easy to verify that (4) indeed holds if $\operatorname{char} \mathbb{K} = 2$. So in this case $\dim \mathcal{S} = (2n+1) - 2 = 2n - 1$ and $\dim \mathcal{M} = n^2 - 2n + 1 = 9$.

If $n = 3$, then looking at $\epsilon_{1,1}$ and $\epsilon_{1,3}$, we obtain:

$$\alpha_1 - \alpha_2 + \gamma = \alpha_1 - \alpha_2 - \delta = 0,$$

whence $\gamma = -\delta = \alpha_2 - \alpha_1$. Now recall that $\delta = \sum \alpha_i + \sum \beta_j + \gamma$. It follows that $\delta = \alpha_1 - \alpha_2 + \gamma = 0$ and hence $\gamma = 0$ and $\alpha_1 = \alpha_2$. Therefore, relation (2) is a scalar multiple of relation (1), and $\dim \mathcal{M} = n^2 - 2n = 3$, regardless of $\operatorname{char} \mathbb{K}$.

If $n \leq 2$, it is easy to see that $\dim \mathcal{M} = 1$.

Answer: $\dim \mathcal{M} = 1$ if $n = 1$ or 2; $\dim \mathcal{M} = 9$ if $n = 4$ and $\operatorname{char} \mathbb{K} = 2$; $\dim \mathcal{M} = n^2 - 2n$ in all other cases.

3. Let $\mathbb{K}$ be a field.

a) For any $f, g \in \mathbb{K}[x]$, prove that $f(x)g(y) - f(y)g(x) \in \mathbb{K}[x, y]$ is divisible by $x - y$.

b) Define $[f, g] = \frac{f(x)g(y) - f(y)g(x)}{x - y}|_{x=y}$. Show that $\mathbb{K}[x]$ with operation $[f, g]$ is a *Lie algebra*, i.e., the antisymmetry identity $[f, f] = 0$ and Jacobi identity $[[f, g], h] + [[g, h], f] + [[h, f], g] = 0$ hold.

c) Prove that if $\mathbb{K}$ has characteristic zero, then the Lie algebra $L = \mathbb{K}[x]$ defined in (b) is *simple*, i.e., for any ideal I of L (a subspace $I \subset L$ with $[L, I] \subset I$), we have either $I = 0$ or $I = L$.

a) Denote $\{f, g\} = f(x)g(y) - f(y)g(x)$. Clearly, this expression is linear in f and in g, so we can expand: $\{\sum_i a_i x^i, \sum_j b_j x^j\} = \sum_{i,j} a_i b_j \{x^i, x^j\}$. Therefore, it suffices to prove that $\{f, g\}$ is divisible by $x - y$ in the case $f = x^i$ and $g = x^j$. But then

$$\{f,g\} = x^i y^j - x^j y^i = \begin{cases} x^i y^i (y^{j-i} - x^{j-i}) & \text{if} \quad i < j; \\ 0 & \text{if} \quad i = j; \\ x^j y^j (x^{i-j} - y^{i-j}) & \text{if} \quad i > j. \end{cases}$$

In all cases, the result is divisible by $x - y$.

Another way to see that $\{f, g\}$ is divisible by $x - y$ is to consider the natural homomorphism $\pi : \mathbb{K}[x, y] \to \mathbb{K}[x, y]/(x - y)$. Since $\pi(x) = \pi(y)$, it follows that $\pi(h(x)) = \pi(h(y))$ for any polynomial h. Hence $\pi(\{f, g\}) = 0$, which means that $\{f, g\}$ is divisible by $x - y$.

b) The antisymmetry identity $[f, f] = 0$ is clear, because if $g = f$, then $f(x)g(y) - f(y)g(x) = 0$. To prove Jacobi identity, we can use linearity in f, g and h. Hence it suffices to consider the case $f = x^i$, $g = x^j$ and $h = x^k$. Then using the formula in part (a), we obtain:

$$\frac{f(x)g(y) - f(y)g(x)}{x - y} = \begin{cases} -x^i y^i \sum_{k=1}^{j-i} x^{k-1} y^{j-i-k} & \text{if} \quad i < j; \\ 0 & \text{if} \quad i = j; \\ x^j y^j \sum_{k=1}^{i-j} x^{k-1} y^{i-j-k} & \text{if} \quad i > j. \end{cases}$$

In all cases, substituting $y = x$ yields $(i - j)x^{i+j-1}$, so we obtain:

$$[x^i, x^j] = (i - j)x^{i+j-1}.$$

Now we can verify Jacobi identity:

$$\begin{aligned}
&[[f, g], h] + [[g, h], f] + [[h, f], g] \\
&= [(i-j)x^{i+j-1}, x^k] + [(j-k)x^{j+k-1}, x^i] + [(k-i)x^{k+i-1}, x^j] \\
&= \big((i-j)(i+j-k-1) + (j-k)(-i+j+k-1) + (k-i)(i-j+k-1)\big)x^{i+j+k-2} \\
&= \big((i+j+k-1)(i-j+j-k+k-i) - 2(i-j)k - 2(j-k)i - 2(k-i)j\big)x^{i+j+k-2} \\
&= \big(0 - 2ik + 2jk - 2ij + 2ik - 2jk + 2ij\big)x^{i+j+k-2} = 0.
\end{aligned}$$

It is useful to note that

$$[f,g] = f'g - fg' \tag{5}$$

where f' denotes the derivative of f. Indeed, using linearity of both sides in f and in g, it suffices to consider the case $f = x^i$ and $g = x^j$. Then both sides equal $(i-j)x^{i+j-1}$.

Another way to obtain (5) is to use the following fact: over any commutative ring R, for any polynomial $\varphi(y) \in R[y]$ and any $a \in R$, we have $\varphi(y) = \varphi(a) + \varphi'(a)(y-a) + \psi(y)(y-a)^2$, where $\psi(y)$ is a polynomial depending on φ and a. It follows that $\varphi(y) - \varphi(a)$ is divisible by $y - a$ in $R[y]$, with the quotient equal to $\varphi'(a) + \psi(y)(y-a)$. Now we regard $f(x)g(y) - f(y)g(x)$ as a polynomial in y with coefficients in $R = \mathbb{K}[x]$, and take $a = x$. Since $\frac{d}{dy}(f(x)g(y) - f(y)g(x)) = f(x)g'(y) - f'(y)g(x)$, we obtain: $\frac{f(x)g(y)-f(y)g(x)}{y-x} = f(x)g'(x) - f'(x)g(x) + \psi(y)(y-x)$ for some $\psi \in R[y]$. Substituting $y = x$ yields: $-[f,g] = f(x)g'(x) - f'(x)g(x)$, as desired.

Using (5), Jacobi identity is easy to verify:

$$\begin{aligned}
&[[f,g],h] + [[g,h],f] + [[h,f],g] \\
&= [f'g - fg', h] + [g'h - gh', f] + [h'f - hf', g] \\
&= (f''g' - fg'')h - (f'g - fg')h' \\
&+ (g''h - gh'')f - (g'h - gh')f' \\
&+ (h''f - hf'')g - (h'f - hf')g' \\
&= 0.
\end{aligned}$$

c) Observe that (5) implies $[f,1] = f'$ for all $f \in L$. Suppose $I \subset L$ is a nonzero ideal. Pick a nonzero element $f \in I$. By our observation, all derivatives of f are in I. Let n be the degree of f, so $f = a_n x^n + \cdots$ where $0 \neq a_n \in \mathbb{K}$ and the dots denote terms of lower degree. Then the n-th derivative of f is $f^{(n)} = n!a_n$, so $n!a_n \in I$. Since we assume $\operatorname{char}\mathbb{K} = 0$, it follows that $1 \in I$. Finally, for any $g \in L$ there exists $h \in L$ such that $h' = g$ (here we again use the assumption $\operatorname{char}\mathbb{K} = 0$), so $g = [h,1] \in I$. We have proved that $I = L$.

4. A finite abelian group will be called *balanced* if the sum of its elements is equal to zero. Which is greater: the number of balanced groups or unbalanced groups of order ≤ 2009?

If A is a finite abelian group, we let $A_2 = \{a \in A \mid 2a = 0\}$. Since an element plus its inverse equals 0, we see that

$$A \text{ is balanced } \iff A_2 \text{ is balanced.}$$

Now $A_2 \cong C_2 \oplus \cdots \oplus C_2$ where C_2 denotes the cyclic group of order 2. If the number of summands is $n > 1$, then A_2 is balanced. This can be shown by induction on n, with basis $n = 2$. Assuming the result for $n = k \geq 2$, we have for $n = k + 1$ that $A_2 \cong \langle x \rangle \oplus B$ where B is balanced. Then the sum of the elements of A_2 is equal to $|B|x$, which is zero since $|B|$ is even. Clearly, C_2 is unbalanced. We have shown the following:

$$A \text{ is unbalanced } \iff A_2 \cong C_2.$$

Using the Fundamental Theorem on finite abelian groups, this can be restated as follows:

$$A \text{ is unbalanced } \iff A \cong C_{2^m} \oplus B \text{ where } m \geq 1 \text{ and } |B| \text{ is odd.}$$

Let $\mathcal{U}$, resp. $\mathcal{B}$, be the set of (isomorphism classes of) unbalanced, resp. balanced, abelian groups of order ≤ 2009. Define a map $\alpha : \mathcal{U} \to \mathcal{B}$ by

$$\alpha(C_{2^m} \oplus B) = \begin{cases} B & \text{if} \quad m = 1; \\ C_2 \oplus C_{2^{m-1}} \oplus B & \text{if} \quad m > 1. \end{cases}$$

The Fundamental Theorem on finite abelian groups implies that α is injective. However, α is not surjective, since, for example, the cyclic group of order 1005 is not in $\alpha(\mathcal{U})$. We conclude that there are more balanced groups than unbalanced.

5.

a) Help Professor A. B. Normal to prove the following important result: Theorem 3. *If a finite group contains exactly 3 non-normal subgroups, then its order is divisible by 3.*

b) Can one replace the 3's in this theorem by 4's?

c) The groups S_3 and D_4 have, respectively, 3 and 4 non-normal subgroups. Does there exist a finite group with exactly 2 non-normal subgroups?

a) Assume a finite group G contains a non-normal subgroup H. This means that H has a conjugate, $gHg^{-1} \neq H$, which is also non-normal. It follows that if G contains exactly 3 non-normal subgroups, then they must all be conjugates of each other. Hence $[G : N_G(H)] = 3$, and the result follows.

b) Yes. If the 4 non-normal subgroups are conjugate to each other and H is one of them, then $[G : N_G(H)] = 4$ and we are done. So assume that the 4 non-normal subgroups are not all conjugate. Then they fall into two conjugacy classes: H_1 with its conjugate $\tilde{H}_1$ and H_2 with its conjugate $\tilde{H}_2$. Note that the normalizers of these 4 groups have index 2. Since the intersection of two distinct subgroups of index 2 is a subgroup of index 4, we may assume without loss of generality that $N_G(H_1) = N_G(\tilde{H}_1) = N_G(H_2) = N_G(\tilde{H}_2)$. Denote this subgroup by N. If $|N|$ is even, we are done. Assume that $|N|$ is odd. Pick an element $x \notin N$. Since $[G : N] = 2$, the element x has even order. Then some power of x has order 2. So let $x \in G$ be an element of order 2. It follows that $x \notin N$. The cyclic group $\langle x \rangle$ cannot be one of the 4 non-normal subgroups of G (they are all contained in N), so $\langle x \rangle$ is normal. It follows that x is a central element and hence normalizes H_1, i.e., $x \in N$. This is a contradiction, which shows that $|N|$ cannot be odd.

c) We will construct a group G of order 16 that has exactly 2 non-normal subgroups. Let H be a cyclic group of order 8 and let σ be a generator of H. Let G be the semidirect product $H \rtimes \langle x \rangle$ where x has order 2 and acts on H by sending σ to σ^5. (Note that $5^2 \equiv 1 \bmod 8$, so this is a well-defined action of $\langle x \rangle$ by automorphisms of H.) In other words,

$$G = \langle \sigma, x \mid \sigma^8 = 1, x^2 = 1, x\sigma x^{-1} = \sigma^5 \rangle.$$

Every element of G can be written uniquely in the form $\sigma^i x^j$ where $0 \leq i < 8$ and $0 \leq j < 2$. Let $y = \sigma^4 x$. Then $y = \sigma x \sigma^{-1}$, so $\langle x \rangle$ and $\langle y \rangle$ are two conjugate (non-normal) subgroups of G. We will show that all other subgroups are normal.

Since H is normal in G and contains a unique subgroup of each order dividing 8, all subgroups of H are normal in G. One checks that the cyclic subgroups $\langle \sigma^i x \rangle$ are normal for $i \neq 0, 4$. We have proved that all cyclic subgroups except $\langle x \rangle$ and $\langle y \rangle$ are normal. Since any subgroup of index 2 is normal, the only remaining possibility for a non-normal subgroup of G is to be isomorphic to $C_2 \times C_2$. But the only elements of order 2 in G are x, y

and σ^4. Hence G has a unique subgroup isomorphic to $C_2 \times C_2$, and this subgroup is normal.

6. Show that for real matrices A the following implication holds:

$$A^{2008} = A^T \quad \Longrightarrow \quad A^{2010} = A.$$

Since A is real, the Hermitian adjoint is equal to the transpose: $A^* = A^T$. It follows that $AA^* = A^{2009} = A^*A$, so A is normal. By Spectral Theorem, A is unitarily diagonalizable, i.e., there exists a unitary matrix U such that $U^{-1}AU = D$ where $D = \operatorname{diag}(\lambda_1, \ldots, \lambda_n)$ and $\lambda_1, \ldots, \lambda_n$ are the eigenvalues of A (repeated according to multiplicity). Now it suffices to show that $D^{2010} = D$, i.e., that every eigenvalue of A satisfies the equation

$$\lambda^{2010} = \lambda. \tag{6}$$

Since $U^{-1} = U^*$, we have $U^{-1}A^*U = D^*$ (i.e., A and A^* are diagonalized with respect to the same basis). Therefore, $A^{2008} = A^T$ implies $D^{2008} = D^*$, which in its turn yields

$$\lambda^{2008} = \bar{\lambda}. \tag{7}$$

Since $A^{2008^2} = (A^T)^T = A$, we see that for any eigenvalue λ of A, either $\lambda = 0$ or $|\lambda| = 1$. In either case, $\lambda^2\bar{\lambda} = \lambda$. Equation (6) now follows from (7).