Problemen

| Problem Section

This Problem Section is open to everyone; everybody is encouraged to send in solutions and propose problems. Group contributions are welcome. We will select the most elegant solutions for publication. For this, solutions should be received before **15 January 2025**. The solutions of the problems in this issue will appear in one of the subsequent issues.

Problem A (proposed by Hendrik Lenstra)

Let r,k,n be integers with $0<k<n-1$ such that the set of remainders of $r,2r,\cdots,kr$ upon division by n equals the set $\{1,\cdots,k\}$. Prove that $r\equiv 1 \bmod n$ or give a counterexample.

Problem B (proposed by ...)

Let $n\geq 2$ be an integer, let $P\in\mathbb{R}[X]$ be a polynomial of degree $n-2$, and suppose that there exist $0\leq x_1<\cdots<x_n\leq n\pi$ with $P(x_i)=\sin(x_i)$ for all $i\in\{1,\cdots,n\}$. Prove that there exist distinct $i,j\in\{1,\cdots,n\}$ with $|x_i-x_j|<\pi$.

Problem C (proposed by Hendrik Lenstra)

Let $k,n>0$ be integers and let R be a commutative ring whose additive group is isomorphic to $\mathbb{Z}^n$. Let $a_1,\cdots,a_k\in R$. Prove that

$$S=\{f(a_1,\cdots,a_k)\mid f\in\mathbb{Z}[X_1,\cdots,X_k],\deg(f)<n\}$$

is a subring of R.

Edition 2024-3 We received solutions from Pieter de Groen and Carsten Dietzel

Problem 2024-1/A

Prove that for all three line segments of length 1 in a disc of radius 1 there are two of those line segments with distance at most 1.

Solution We received solutions from Pieter de Groen and Carsten Dietzel
Divide the disk into 6 equal closed pie slices. Any of the line segments contained within a slice intersects at least 3 slices: the segment either has to be a radius and thus contains the center point shared by all slices, or must be the chord between the sides of the slice and thus intersects (the boundary of) both neighboring slices. Consequently, each line segment intersects at least 2 slices. We may choose the orientation of the slices so that a given line segment intersects at least 3 slices, by placing one of the end points of the segment on the boundary of a slice. By the pigeonhole principle there is a slice with at least two line segments intersecting it, and these two segments then have distance at most 1.

Problem 2024-1/B (proposed by Hendrik Lenstra)

Let A be an abelian group and write $\mathrm{End}(A)$ for the ring of group homomorphisms from A to A. Show that A is free as $\mathrm{End}(A)$-module if and only if A admits a commutative ring structure so that the Cayley map $A\to\mathrm{End}(A)$ given by $x\mapsto(y\mapsto xy)$ is an A-module isomorphism. Show that for all subrings of $\mathbb{Q}$ and rings $\mathbb{Z}/p\mathbb{Z}$ with p a prime the Cayley map is an isomorphism, and give an example of an uncountable ring with this property.

Solution We received solutions from Carsten Dietzel
Suppose A is a commutative ring such that $\phi:\mathrm{End}(A)\to A$ given by $f\mapsto f(1)$, the in-

Redactie: Onno Berrevoets en Daan van Gent
problems@nieuwarchief.nl
www.nieuwarchief.nl/problems

Oplossingen | Solutions

verse of the Cayley map, is an A-module isomorphism. For $f,g \in \mathrm{End}(A)$ we have $\phi(fg) = f(g(1)) = f\phi(g)$, so ϕ is an $\mathrm{End}(A)$-module homomorphism. In particular, A is free as $\mathrm{End}(A)$-module.

Write $R = \mathrm{End}(A)$ and suppose we have an isomorphism $b: R^{(S)} \to A$ of (left) R-modules. Hence we have a isomorphism $R = \mathrm{End}(A) \to \mathrm{End}\big(R^{(S)}\big)$ of groups given by $f \mapsto b^{-1} \circ f \circ b$. For $f \in R$ and $g = (g_i)_i \in R^{(S)}$ we have

$$(b^{-1} \circ f \circ b)(g) = b^{-1} \circ (f \cdot b(g)) = b^{-1}(b(fg)) = fg = (fg_i)_i.$$

We may assume $A \neq 0$, hence $R \neq 0$ and $S \neq \emptyset$, otherwise all holds trivially. Choose $j \in S$ and let $x, y \in R$ be distinct. Consider the the element of $\varphi \in \mathrm{End}\big(R^{(S)}\big)$ that multiplies on the *right* by x at index j and by y elsewhere. Then by the previous there is some $f \in R$ such that φ is given by $(g_i)_i \mapsto (fg_i)_i$. At index j this gives $fg_j = g_j x$ for all $g_j \in R$, so in particular $f = x$ when taking $g_j = 1$, from which it then also follows that R is commutative. At any index different from j we have similarly that $f = y$, so $x = y$, which is a contradiction. Hence $\#S = 1$ and $b: R \to A$ is an isomorphism of R-modules. If we transport the ring structure of R along b to A, then the Cayley map is an A-module isomorphism.

Let R be a subring of $\mathbb{Q}$, or $\mathbb{Z}/p\mathbb{Z}$ for some prime p. For each $f \in \mathrm{End}(R)$ and $a, b \in \mathbb{Z}$ such that the image of a/b in R is well-defined, we have $bf(a/b) = f(a) = af(1)$, so $f(a/b) = f(1) \cdot (a/b)$. With $x = f(1) \in R$ we have $f = y \mapsto xy$, so indeed $R \to \mathrm{End}(R)$ is an isomorphism.

Consider $R = \prod_p (\mathbb{Z}/p\mathbb{Z})$ and note that it is uncountable. Then we have an isomorphism $\mathrm{End}(R) \cong \prod_p \mathrm{Hom}(R, \mathbb{Z}/p\mathbb{Z})$, where $\mathrm{Hom}(R, \mathbb{Z}/p\mathbb{Z})$ are the group homomorphisms from R to $\mathbb{Z}/p\mathbb{Z}$. It suffices to show that the natural injection $\varphi: \mathrm{End}(\mathbb{Z}/p\mathbb{Z}) = \mathrm{Hom}(\mathbb{Z}/p\mathbb{Z}, \mathbb{Z}/p\mathbb{Z}) \to \mathrm{Hom}(R, \mathbb{Z}/p\mathbb{Z})$ is surjective for all primes p. Suppose $f \in \mathrm{Hom}(R, \mathbb{Z}/p\mathbb{Z})$. For $x \in R$ we have $0 = pf(x) = f(px)$, so $\{(x_q)_q \in R : x_p = 0\} = pR \subseteq \ker(f)$. Hence f is in the image of φ.

Problem 2024-1/C (proposed by Albert Visser)

A *Gollum ring* is a ring that is isomorphic to the subring $\mathbb{Z} + 2R$ of a commutative ring R. Show that there is a sentence in first-order logic in the language of rings that is true in all Gollum rings, but not true in all commutative rings.

Solution We received solutions from Carsten Dietzel. Clarification: $\mathbb{Z}$ in $\mathbb{Z} + 2R$ refers to the image of $\mathbb{Z} \to R$.

Note that the statement $r \in 2R$ can be expressed as the proposition $\exists s \in R : 2s = r$. Let G be the Gollum ring with ambient ring R, i.e., $G = 2R + \mathbb{Z}$. An element $r \in G$ can be written as $r = 2s + m$ with $s \in R, m \in \mathbb{Z}$. As either $m \in 2\mathbb{Z}$ or $m - 1 \in 2\mathbb{Z}$, we see that either $r \in 2R$ or $r - 1 \in 2R$. Therefore, $r(r-1) \in 2R$. It follows that $r^2(r-1)^2 \in 4R = 2(2R) \subseteq 2G$, proving the following first-order formula:

$$\forall r \in G, \exists s \in G : r^2(r-1)^2 = 2s.$$

This formula does not hold in general! The ring $R = \mathbb{Z}[x]/(x^2(x-1)^2 - 1)$ is an integral extension of $\mathbb{Z}$. Then $r = \overline{x}$, the class of x, clearly satisfies the equation $r^2(r-1)^2 = 1$. An element s satisfying $2s = r^2(r-1)^2$ would therefore satisfy $2s - 1 = 0$ and can thus not be integral over $\mathbb{Z}$. The formula can therefore not hold in R.

In Problem 2023-2/C, the statement $c_{[p]} = \mathrm{gcd}\{s \in S : v_p(s) > 0\}$ is incorrect. Instead, one could prove $c_{[p]} \in \langle S \rangle$ inductively.