Problemen

| Problem Section

Edition 2022-1 We received solutions from Brian Gilding, Pieter de Groen en Nicky Hekster.

Problem 2022-1/A (proposed by Hendrik Lenstra)

Let R be a ring. We say $x \in R$ is a *unit* if there exists some $y \in R$ such that $xy = yx = 1$ and write R^* for the set of units of R. Show that $1 < \#(R \setminus R^*) < \infty$ implies $1 < \#R < \infty$.

Solution As solved by Nicky Hekster. Since $1 < \#(R \setminus R^*)$, we may pick some non-zero $a \in R \setminus R^*$. If $Ra = aR = R$, then a is a unit, which is a contradiction. So suppose without loss of generality that $Ra \subsetneq R$. In particular $Ra \cap R^* = \emptyset$. Hence $Ra \subseteq R \setminus R^*$ is finite. Consider $\mathrm{Ann}(a) = \{r \in R : ra = 0\}$. Since $\mathrm{Ann}(a) \cap R^* = \emptyset$, we again have that $\mathrm{Ann}(a)$ is finite. Finally, the left R-module homomorphism $R \to R$ given by $r \mapsto ra$ induces an isomorphism $R/\mathrm{Ann}(a) \cong Ra$, from which it follows that R is also finite.

Problem 2022-1/B (proposed by Hendrik Lenstra)

Let G be a group. For $n \in \mathbb{Z}_{>0}$ write $G[n] = \{g \in G \mid g^n = 1\}$ and $G^n = \{g^n \mid g \in G\}$.

1. Suppose G is abelian and $m, n \in \mathbb{Z}_{>0}$. Show that $G[n] \subseteq G^m$ if and only if $G[m] \subseteq G^n$.
2. Show that there exist $m, n \in \mathbb{Z}_{>0}$ such that the above is false when we drop the assumption that G is abelian.

Solution 1. We will use additive notation. By symmetry it suffices to show that $G[n] \subseteq mG$ implies $G[m] \subseteq nG$. For a prime p and abelian group H write $H[p^\infty] = \{h \in H : (\exists k \geq 0)\ p^k h = 0\}$ and $H[\infty] = \{h \in H : (\exists n > 0)\ nh = 0\}$.

Claim 1. For all $n > 0$ and primes p we have $G[n][p^\infty] = G[p^\infty][n]$ and $(nG)[p^\infty] = n(G[p^\infty])$.

Proof. The first equality is trivial, as well as the inclusion $n(G[p^\infty]) \subseteq (nG)[p^\infty]$. Suppose $x \in (nG)[p^\infty]$. Then $ny = x$ for some $y \in G$ and $p^k x = 1$ for some $k \geq 0$. Write $n = p^s u$ for some $s \geq 0$ and $(u,p) = 1$, and let v be an inverse of u modulo p^k. Then $p^{k+s}(uvy) = p^k vx = 1$, so $uvy \in G[p^\infty]$, and $nuvy = uvx = x$, so $x \in n(G[p^\infty])$. □

Claim 2. With p ranging over the primes we have $\sum_p G[p^\infty] = G[\infty]$.

Proof. This follows from the Chinese remainder theorem. □

We reduce to the case $G = G[p^\infty]$ for some prime p. Suppose $G[n] \subseteq mG$. Then $G[p^\infty][n] = G[n][p^\infty] \subseteq (mG)[p^\infty] = m(G[p^\infty])$ by Claim 1. Assuming we have solved the case $G = G[p^\infty]$ we get $G[m][p^\infty] \subseteq (nG)[p^\infty]$. From Claim 2 it then follows that $G[m] \subseteq (nG)[\infty] \subseteq nG$, as was to be shown.

Thus we assume $G = G[p^\infty]$. Consequently, we may assume $m = p^a$ and $n = p^b$. Furthermore, the statement is clearly true when $a = 0$ or $b = 0$, so suppose neither is the case. Let $x \in G[p^a]$. We distinguish two cases.

Case $a \leq b$: It suffices to show inductively for all $0 \leq k \leq b$ that there exists a $y_k \in G$ such that $x = p^k y_k$. For $k \leq a$ we have $x \in G[p^a] \subseteq G[p^b] \subseteq p^a G$, so we may write $x = p^a y_a$ and $y_k = p^{a-k} y_a$. Suppose $a < k \leq b$ and $p^{k-a} y_{k-a} = x$. Then $p^k y_{k-a} = 0$, so $y_{k-a} \in G[p^k] \subseteq G[p^b] \subseteq p^a G$. Hence $y_{k-a} = p^a y_k$ for some $y_k \in G$ and $p^k y_k = x$, as was to be shown.

Case $b \leq a$: It suffices to show inductively for all $0 \leq k \leq b$ that there exists a $y_k \in G$ such that $p^k x = p^b y_k$. For $k = b$ we may take $y_k = x$. Suppose $0 < k \leq b$ and $p^k x = p^b y_k$. Then $0 = p^{b-k}(p^k x - p^b y_k) = p^b(x - p^{2b-k} y_k)$, so $x - p^{2b-k} y_k \in G[p^b] \subseteq p^a G$ for some $z \in G$. It follows that

$$p^{k-1} x = p^{a+k-1} z + p^{2b-1} y_k = p^b(p^{a-b+k-1} z + p^{b-1} y_k) =: p^b y_{k-1},$$

as was to be shown.

2. Consider the non-trivial semi-direct product $G = (\mathbb{Z}/3\mathbb{Z}) \rtimes (\mathbb{Z}/4\mathbb{Z})$. Then $G[2] = \{(0,0),(0,2)\} = G^6$, while $G[6] = \{(a,b) : b \in 2\mathbb{Z}\} \not\subseteq \{(0,0),(1,0),(2,0),(0,2)\} = G^2$.

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

Oplossingen

| Solutions

Problem 2022-1/C (proposed by Onno Berrevoets)

Let $f:\mathbb{R}\to\mathbb{R}$ be a twice differentiable function. Suppose that $a<b<c$ are real numbers such that $f(a)=f(b)=f(c)=0$. Prove that there exists $x\in(a,c)$ such that

$$f'(x)+f''(x)=f(x)^2+2f(x)f'(x)\,.$$

Solution Solved Brian Gilding, partially solved by Pieter de Groen. Proof from Brian Gilding: Define two functions $\mathbb{R}\to\mathbb{R}$ by the following:

$$g(x)=f(x)\exp\left(-\int_b^x f(t)\,\mathrm{d}t\right) \quad \text{and} \quad h(x)=e^x(f'-f^2)(x)\,.$$

Notice that g and h are differentiable on $\mathbb{R}$. Since $g(a)=g(b)=g(c)=0$, by Rolle's theorem there exists $u\in(a,b)$ and $v\in(b,c)$ such that $g'(u)=g'(v)=0$. The last two equalities imply that $h(u)=h(v)$. Hence, by Rolle's theorem, $h'(x)=0$ for some $x\in(u,v)$. This yields $(f'+f''-f^2-2ff')\,(x)=0$.