Problemen

| Problem Section

Edition 2016-3 We received solutions from Raymond van Bommel, Rik Bos, Alexandros Efthymiadis, Alex Heinis, Thijmen Krebs, Toshihiro Shimizu, Djurre Tijsma and Traian Viteam.

Problem 2016-3/A (folklore)

Show that a group G is torsion-free if and only if for all integers $n \geq 2$ and finite subsets $S, T \subseteq G$ with $\#S = \#T = n$ we have $\#\{st: s \in S, t \in T\} > n$.

Solution We received solutions from Raymond van Bommel, Rik Bos, Alexandros Efthymiadis, Alex Heinis, Thijmen Krebs, Toshihiro Shimizu and Djurre Tijsma. The book token is awarded to Rik Bos, the solution of whom the following is based on; the main idea below appeared in every solution received.

If G has a torsion element x, then $S = T = \langle x \rangle$ have the property that $\#(ST) = \#S = \#T$.

On the other hand, let $n \geq 2$, and let S, T be subsets of G with $\#S = \#T = n$, such that $\#(ST) = n$. Then, for every $s \in S$, we have $sT \subseteq ST$, and both sides have the same cardinality n, so $sT = ST$ for all $s \in S$. Let $s_1, s_2 \in S$ be distinct elements, and let $a = s_1^{-1} s_2$, so that $a \neq 1$. Then $aT = s_1^{-1} s_2 T = s_1^{-1} ST = s_1^{-1} s_1 T = T$, so $a^k T = T$ for all $k \geq 0$. Hence, for any $t \in T$, we have $\{a^k t: k \in \mathbb{Z}\} \subseteq T$ and therefore that a is torsion of order at most n, which contradicts G being torsion-free.

Problem 2016-3/B (proposed by Hendrik Lenstra)

Show that for all groups G the commutator subgroup $[G,G] = \langle\, xyx^{-1}y^{-1}: x,y \in G\,\rangle$ of G has order at most 2 if and only if every conjugacy class in G has at most 2 elements.

Solution We received solutions from Raymond van Bommel, Rik Bos, Alexandros Efthymiadis, Alex Heinis, Thijmen Krebs, Toshihiro Shimizu, Djurre Tijsma and Traian Viteam. The book token is awarded to Alex Heinis, the solution of whom the following is mainly based on, with some elements based on other submissions; most of the received solutions are similar.

First suppose that the order of $[G,G]$ is at most 2. Then there exists a unique $a \in G$ such that $[G,G] = \{1, a\}$. Let $x \in G$. Then we have for all $g \in G$ that $gxg^{-1} = [g,x]x \in \{x, ax\}$. Hence every conjugacy class in G has cardinality at most 2.

Now suppose that every conjugacy class in G has cardinality at most 2. Then for all $x \in G$ there exists a unique $\theta(x) \in G$ such that $\{[g,x]: g \in G\} = \{1, \theta(x)\}$, so that the conjugacy class of x is $\{x, \theta(x)x\}$. We see that θ defines a map from G to $[G,G]$ such that its image generates $[G,G]$. So it suffices to show that the image of θ has cardinality at most 2, and that the image consists of elements of order at most 2; note that the image of θ always contains 1.

First note that if $x,y \in G$ do not commute, that then $\theta(x)$ and $\theta(y)$ are both non-trivial, since $yxy^{-1} \neq x$ implies that $yxy^{-1} = \theta(x)x$, and $xyx^{-1} \neq y$ implies that $xyx^{-1} = \theta(y)y$. Next, we show that if $x,y \in G$ do not commute, that then $\theta(x) = \theta(y)$. Note that xy commutes with neither of x, y. Hence we have

$$\theta(x) = [xy,x] = [x,xy]^{-1} = \theta(xy)^{-1} = [y,xy]^{-1} = [xy,y] = \theta(y)$$

and

$$\theta(x) = [y,x] = [x,y]^{-1} = \theta(y)^{-1},$$

so in particular, $\theta(x) = \theta(y)$ is of order 2.

Note that for $x \in G$ we have $\theta(x) = 1$ if and only if $x \in Z(G)$, so θ is constant on $Z(G)$. So we are done once we show that θ is constant on $G - Z(G)$ of value of order 2. Let $x,y \in G - Z(G)$. Then the centralisers C_x, C_y of x, y respectively are proper subgroups of G, therefore $C_x \cup C_y \neq G$. Hence there exists $g \in G$ that commutes with neither of x, y. We deduce that $\theta(x) = \theta(g) = \theta(y)$, and that this element is of order 2. Therefore θ is constant on $G - Z(G)$ of value of order 2, as required.

Redactie:

Gabriele Dalla Torre
Christophe Debry
Jinbi Jin
Marco Streng
Wouter Zomervrucht

Problemenrubriek NAW
Mathematisch Instituut
Universiteit Leiden
Postbus 9512
2300 RA Leiden

problems@nieuwarchief.nl
www.nieuwarchief.nl/problems

Oplossingen | Solutions

Problem 2016-3/C (proposed by Carlo Pagano and Mima Stanojkovski)

A subgroup H of a group G is said to be *solitary* if no other subgroup of G is isomorphic to H. A group G is said to be *totally solitary* if all of its subgroups are solitary. Show that a group G is totally solitary if and only if it is isomorphic to a subgroup of $\mathbb{Q}/\mathbb{Z}$.

Solution We received solutions from Rik Bos, Alex Heinis, Thijmen Krebs, Toshihiro Shimizu and Djurre Tijsma. The book token goes to Djurre Tijsma. All received proofs of the fact that any subgroup of $\mathbb{Q}/\mathbb{Z}$ is totally solitary are similar, and the first part of the solution is based on these. The second part of following solution is based for the most part on the submission of Raymond van Bommel.

First we show that $\mathbb{Q}/\mathbb{Z}$ is totally solitary, thereby (by definition of totally solitary) showing that all of its subgroups are. Note that $\mathbb{Q}/\mathbb{Z}$ is torsion, and that for any positive integer N, $\mathbb{Q}/\mathbb{Z}[N] = \frac{1}{N}\mathbb{Z}/\mathbb{Z}$, which is cyclic of order N. So let H_1, H_2 be two isomorphic subgroups of $\mathbb{Q}/\mathbb{Z}$, and let $\phi : H_1 \to H_2$ be an isomorphism. Then, for any $h \in H_1$, we see that $\phi(h)$ has the same order as H, say N. Hence $h = a\phi(h)$ for some integer a coprime to N, so $h \in H_2$ as well, showing that $H_1 \subseteq H_2$. The same argument shows that $H_2 \subseteq H_1$, so $H_1 = H_2$, thereby showing that $\mathbb{Q}/\mathbb{Z}$ (and each of its subgroups) is totally solitary.

Now suppose that G is totally solitary. If G were to contain an element x of infinite order, then $\langle x^2\rangle \subset \langle x\rangle$ are isomorphic subgroups of G that are not equal, which contradicts G being totally solitary. Hence G is torsion. Moreover, for any positive integer N there is at most one cyclic subgroup of G of order N, in other words, there are either 0 or $\phi(N)$ elements of G of order N, where ϕ is the Euler totient function.

Now take any finite subgroup H of G, and let N be its order. Since elements of H must have order dividing N, it follows that $N = \#H \le \sum_{d\mid n} \phi(d) = N$. Therefore, equality must hold, and H contains $\phi(N)$ elements of order N, i.e. H is cyclic.

We use this to show that G is abelian. Let $x, y \in G$ be of orders M, N, respectively. Then yxy^{-1} has the same order as x, and therefore yxy^{-1} generates the same subgroup of G as x. In other words, there exists some integer e with $\gcd(e, M) = 1$ for which $yxy^{-1} = x^e$. Now every element of $\langle x, y\rangle$ can be written in the form $x^i y^j$ for some $i = 0, 1, \ldots, M-1$ and $j = 0, 1, \ldots, N-1$, so $\langle x, y\rangle$ is finite, hence cyclic by the above, and therefore x and y commute.

Now that we have shown that G is abelian, we will write the group operation on G additively from now on.

Let us construct an injective homomorphism $G \to \mathbb{Q}/\mathbb{Z}$. First, pick an enumeration $p_1, p_2, p_3, \ldots$ of the prime numbers, and let $M_n = \prod_{i=1}^{n} p_i^n$ for $n \ge 0$ (so $M_0 = 1$). Moreover, let $H_n = G[M_n]$, so that every H_n is finite and cyclic, say of order N_n. Then $H_m < H_n$ for $m < n$, so $N_m \mid N_n$ for $m < n$, and $G = \bigcup_{n=1}^{\infty} H_n$.

Now we define recursively for every $n \ge 0$, an injective homomorphism $\phi_n : H_n \to \mathbb{Q}/\mathbb{Z}$ such that for $i < n$ and $x \in H_i$ we have $\phi_i(x) = \phi_n(x)$. This suffices, since we can define an injective homomorphism $\phi : G \to \mathbb{Q}/\mathbb{Z}$ by $x \mapsto \phi_i(x)$ for any i such that $x \in H_i$; such an i exists, and the value doesn't depend on the choice of i, by the above.

For $n = 0$, we define $\phi_0 : H_0 = 0 \to \mathbb{Q}/\mathbb{Z}$ to be the zero homomorphism. Now assume that for $n \ge 1$ and $i = 0, 1, \ldots, n-1$, injective homomorphisms $\phi_i : H_i \to \mathbb{Q}/\mathbb{Z}$ are given such that for $j < i$ and $x \in H_j$ we have $\phi_j(x) = \phi_i(x)$. Let h_{n-1} be a generator of H_{n-1}, and let h_n be a generator of H_n such that $\frac{N_n}{N_{n-1}} h_n = h_{n-1}$. Then define $\phi_n : H_n \to \mathbb{Q}/\mathbb{Z}$ to be the homomorphism sending h_n to any element $h_n' \in \mathbb{Q}/\mathbb{Z}$ such that $\frac{N_n}{N_{n-1}} h'_n = \phi_{n-1}(h_{n-1})$if $\phi_{n-1}(h_{n-1}) \ne 0$, and to $\frac{N_{n-1}}{N_n}$ otherwise. This is injective as a generator of a cyclic group of order N_n is always sent to an element of order N_n by assumption. Moreover, for all $x \in H_{n-1}$, we have $\phi_{n-1}(x) = \phi_n(x)$, so by assumption, for all $i < n$ and $x \in H_i$, we have $\phi_i(x) = \phi_n(x)$ as well, as required.