Chris Eblen
Vishnu Murali
Joel Ornstein

8. Which finite abelian groups A have the property that $\mathrm{Th}(A)$ has quantifier elimination?
[Hint: Make some use of Problem 4. Prove that a finite abelian group is ultrahomogeneous iff its Sylow subgroups are ultrahomogeneous.]

The finite abelian groups whose theory have quantifier elimination are the finite groups of the form

$$\bigoplus_{\text{distinct primes } p} \left(\bigoplus_{i=1}^{n_p} \mathbb{Z}_{p^{k_p}} \right).$$

This result follows from Problem 4 that the theory of a group has quantifier elimination if and only if the group is ultrahomogeneous and the following claims prove our result.

Claim. *A finite abelian group G is ultrahomogeneous iff its Sylow subgroups are ultrahomogeneous.*

Proof. Assume that all Sylow subgroups of G are ultrahomogeneous. As G is finite abelian, it is a direct product of its Sylow subgroups. Let M and N be subgroups of G which are therefore direct products of p-subgroups. If $\varphi : M \to N$ is an isomorphism, then φ acts as a direct product of isomorphisms on each of the p-subgroups. By ultrahomogeneity of the Sylow subgroups, each component of φ can be extended into an automorphism on the Sylow subgroups, and taking the direct product of these is an extension of φ to an automorphism of G.

Assume G is ultrahomogeneous and M and N are subgroups of a Sylow p-subgroup P. Then by ultrahomogeneity of G, this isomorphism extends to an automorphism of G, which acts an an automorphism on P as G is abelian and therefore the Sylow subgroups are characteristic in G. $\square$

Claim. *The ultrahomogeneous abelian p-groups P are of the form* $\bigoplus_{i=1}^{n} \mathbb{Z}_{p^k}$.

Proof. Assume that P is ultrahomogeneous. By the classification theorem of finite abelian groups, P is a product of cyclic p-subgroups. Suppose that $P = \mathbb{Z}_{p^{k_1}} \times \cdots \times \mathbb{Z}_{p^{k_r}}$ with $k_1 \leq \cdots \leq k_r$. The sequence of elementary divisors of S are $(p^{k_1}, \dots, p^{k_r})$. Let M be the p-element subgroup of S generated by $s = (p^{k_1-1}, 0, \dots, 0)$, and let N be the p-element subgroup generated by $t = (0, 0, \dots, p^{k_r-1})$. Suppose that $\alpha : P \to P$ is an automorphism such that $\alpha(M) = N$. Then α induces an isomorphism from P/M to P/N. But the elementary divisors of these groups are $(p^{k_1-1}, \dots, p^{k_r})$ and $(p^{k_1}, \dots, p^{k_r-1})$. If these are the same sequences up to permutation, then $k_1 = k_2 = \cdots = k_r$. Hence any ultrahomogeneous abelian p-group must have the structure given in the claim.

To show that any such P is ultrahomogeneous, given an isomorphism $\varphi : M \to N$, we perform induction on the sizes of M and N to extend φ to an isomorphism between strictly larger subgroups M' and N', ultimately giving us an automorphism on P.

Assume by way of contradiction that there exist isomorphisms which cannot be extended to isomorphisms of larger subgroups. We choose an one such isomorphism $f : M \to N$

such that $|M|$ is maximal with respect to the property that f cannot be extended to an isomorphism between M' and N' properly containing M and N respectively. We observe that P has a chain of characteristic subgroups:

$$0 < p^{k-1} \cdot P < p^{k-2} \cdot P < ... < p \cdot P < P.$$

We choose $x \in P \setminus M$ of the least layer (i.e. $x \notin M$ but $p \cdot x \in M$). Hence f sends $p \cdot x$ to some element $y \in N$.

All maximal cyclic subgroups of P have the same size size p^k. Therefore y has the same number of p-th roots (z such that $p \cdot z = y$) as any generator of a cyclic subgroup of size $|\langle y \rangle| = |\langle p \cdot x \rangle|$. Specifically, y has as many p-th roots in P as $p \cdot x$ does since all p-th roots of y in N correspond to distinct p-th roots of $p \cdot x$ in M under the isomorphism f. Hence there exists $z \in P \setminus N$ that is a p-th root of y.

If we let $M' = \langle M, x \rangle$ and $N' = \langle N, z \rangle = N'$, we can extend f to an isomorphism $\tilde{f} : M' \to N'$ by letting $\tilde{f}(x) = z$, and given $m + a \cdot x \in M'$ with $m \in M$ and $a \in \mathbb{Z}$, $\tilde{f}(m + a \cdot x) = f(m) + a \cdot z$. To see that $\tilde{f}$ is well-defined, suppose $m_1 + a \cdot x = m_2 + b \cdot x$. Then $(m_1 - m_2) + (a - b) \cdot x = 0$, so that

$$0 = \tilde{f}(0) = \tilde{f}((m_1 - m_2) + (a - b) \cdot x) = f(m_1 - m_2) + (a - b) \cdot z = (f(m_1) + a \cdot z) - (f(m_2) + b \cdot z)$$

and hence $\tilde{f}(m_1 + a \cdot z) = f(m_1) + a \cdot z = f(m_2) + b \cdot z = \tilde{f}(m_2 + b \cdot z)$. That $\tilde{f}$ is an isomorphism is by construction as f is. Since $|M'| > |M|$ and $\tilde{f}$ extends f, we have a contradiction to our assumption. Hence all isomorphisms of subgroups can be extended to automorphisms of P.

$\square$