

## Chapter 8

# Conclusion

We have given a new quantum Fourier sampling theorem and a new quantum Fourier transform algorithm for abelian groups. These results are based on the robustness of the Fourier transform with respect to changes in the underlying group – a property which might play a useful role in future quantum algorithms – for example, in the context of the Unique Shortest Vector Problem, where there is an underlying abelian group.

We have studied how the existing algorithm for the Hidden Subgroup Problem over abelian groups generalizes to the nonabelian case. This is motivated by the reduction of graph isomorphism to the HSP over the symmetric group. We characterize how the algorithm works and show that normal subgroups can be found. We have also shown that the algorithm cannot distinguish between a trivial and a nontrivial subgroup when the group is the symmetric group, so more must be done to solve graph isomorphism.

Finally, we solved the Shifted Legendre Symbol Problem, which appears to go beyond the framework of the HSP. The structure of the algorithm is different from that of

the HSP algorithm, and may provide a starting point for new quantum algorithms.