Reminder: Group Theory

Let's get some help with computers. What are the groups of order $|G| = 400$? Here is the computer program.[1]

```
G := AllSmallGroups(400);;
List(G, g -> StructureDescription(g));
[ "C25 : C16", "C400", "C25 : C16", "C25 : Q16", "C8 x D50",
  "C25 : (C8 : C2)", "C25 : QD16", "D400", "C2 x (C25 : C8)",
  "C25 : (C8 : C2)", "C4 x (C25 : C4)", "C25 : (C4 : C4)",
  "C25 : (C4 : C4)", "C25 : ((C4 x C2) : C2)", "C25 : QD16", "C25 : D1
  "C25 : Q16", "C25 : QD16", "C25 : ((C4 x C2) : C2)", "C100 x C4",
  "C25 x ((C4 x C2) : C2)", "C25 x (C4 : C4)", "C200 x C2",
  "C25 x (C8 : C2)", "C25 x D16", "C25 x QD16", "C25 x Q16",
  "C25 : (C8 x C2)", "C25 : (C8 : C2)", "C4 x (C25 : C4)",
  "C25 : (C4 : C4)", "C2 x (C25 : C8)", "C25 : (C8 : C2)",
  "C25 : ((C4 x C2) : C2)", "C2 x (C25 : Q8)", "C2 x C4 x D50",
  "C2 x D200", "C25 : ((C4 x C2) : C2)", "D8 x D50",
  "C25 : ((C4 x C2) : C2)", "Q8 x D50", "C25 : ((C4 x C2) : C2)",
  ...
]
```

Notice there is is both $C_{25} \times QD_{16}$ and $C_{25} \ltimes QD_{16}$.

In more commom notation we can write with the symbols $\times$ (direct product) and $\ltimes$ (indirect product):

- $G = (C_5 \ltimes Q_8) \times D_{10}$
- $G = (C_5 \ltimes C_5) \ltimes (C_4 \times C_4)$
- $G = C_2 \times ((C_5 \times C_5) \ltimes C_8)$
- $G = D_8 \times ((C_5 \times C_5) \ltimes C_2)$

Once we have these explicit descriptions of groups, we look at the representation theory of finite groups. Example, the Peter-Weyl theorem:

[1] https://math.stackexchange.com/questions/4108993/the-221-groups-of-order-g-400
https://www.gap-system.org/

Approximate Groups Does "commutativity" matter? We've been studying the equation $ab = ba$. It certainly works for numbers $2 \times 3 = 3 \times 2$ and we can describe when it fails:

$$\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 2 & 1 \\ 1 & 0 \end{bmatrix} \neq \begin{bmatrix} 1 & 2 \\ 1 & 0 \end{bmatrix} = \begin{bmatrix} 1 & 1 \\ 1 & 0 \end{bmatrix} \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$$

so we have lots of examples of non-commutativity.

Lemma Let G be an aribtary group. Let $A \subset G$ be a subset with $|A^2| \leq K|A|$. Then $|A^{-1}A| \leq K^2|A|$ and $|AA^{-1}| \leq K^2 A$.

In my experience the proofs not very exciting. Counting he possibilities on both sides and making sure both sides are equal. Here's the counter-example the book has provided: Let H be a finite group and $G = H * \langle x \rangle$, the free-product of H and the infinite cyclic group one generatory (basically $\mathbb{Z}$). Set $A = H \cup \{x\}$. Then

$$|A^2 \leq 3|A| \tag{$*$}$$

but $HxH \subseteq A^3$ and yet $|HxH| = |H|^2 \asymp |A|^2$.

This is their instance of **small tripling**. We could imamgine $A \subseteq \mathbb{Z}$ then:

$$A = A + A + A \text{ or } |3A| \leq 3|A|$$

so once we throw away the exact relation $A + A = A$ (such as the arithmetic progression or a **subgroup** or **coset** of $\mathbb{Z}$) we get to consider small-doubling or small-tripliing moves.

Ex $(A \cup \{1\} \cup A^{-1})^2$ is an $O(K^9)$-approximate group.

References

[1]