Algebraic Crumbs

"Twinkle twinkle little star, how I wonder what you are" (Jane Taylor)

I Constructions, Nay, Properties, by Their Properties

1. ***Normal subgroup***

- Normal subgroups are precisely the ones that allow a natural group structure on the quotient.
- A subgroup H of G being normal is exactly the condition that we require so that we can put a compatible group structure on the quotient set G/H
- Why isn't a circle a ring? Why isn't R/Z a ring?

2. ***Simple group***

- Is a 'prime' 'normal' group, since it has no 'real' normal subgroups: Only itself and the trivial subgroup.
- A group that is not simple can be broken into two smaller groups, a normal subgroup and the quotient group, and the process can be repeated.
- If a group is finite, then eventually one arrives at uniquely determined simple groups (by the Jordan–Hölder theorem).

3. ***Free group***. Can these have any properties at all?

II Aren't These All the 'Same'?

4. What makes a group different from another? A finite simple group different from another?

5. TODO: where is number theory used in diff-eq, logic, etc.!!! http://mathoverflow.net/questions/90700/where-is-number-theory-used-in-the-rest-of-mathematics/90746#90746

III Stillwell's elements, Revisited

6. A revisting of the book, which we were lead to during the study of PL/QL, reveals how algebra helps us understand logic and vice versa. The realization of what the currency of studying 'abstract' systems is changes everything and explains our lack of progress at the time.

7. Once we think about 'properties' being the main currency of abstract studies, they become the replacement of 'numbers' in a symbolic game similar to arithemtic.

8. A good idea is to keep the names that are being generalised and not use 'new names', as per example we did for 'prime' for simple groups. We can use this idea during the revisiting of Stillwell's book quite effectively.

9. A short spill of this evolved point of view leads to the following notes:

- The property of 'Division with Remainder' at p.57 is a propery of 'Z', which means, an inductive (as we know, the only model of algorithm) that can be wrestled out from the axioms of Z, but not purely the axioms of a ring, which Z[x] also is. Looking at the proof for Z, we notice that order plays a role, and that is probably what is missing for Z[x]. Such 'details' would escape the attention as 'accidental' when one does not understand the 'property as currency' idiom, and focus instead on the concrete 'Z' and 'Z[x]'.

- It turns out on p.58, that the degree can be used to order polynomials, but the orders are 'set-like', not element-like.
- A good name for 'division with remainer' is 'pre-divisibility'.
- We now notice details like the essentiality of exactly the last part (the part after and including $\in$) of the following, which is something that we would have seen as not to essential in the past:

$$g \text{ divides } f \Leftrightarrow f = gh \text{ for some } h \in F[x].$$

- We now see lattice and ordering when we hear 'gcd', as in the proof of 'division with remainder' for Z, we did not before. But the (reprentation abstracting, syntactic) property is the currency that has to be wrestled into proofs, in 'proof theory'.

Bibliography

Author. ***Title***.