

Commands mostly about generating sub-objects.

Groch, page 25:

"As an example of theorem 11, consider the following. Let A be any subset of group G . The intersection of all subgroups of G which contain A itself contains A and is, by theorem 11, also a subgroup of G . This is called the subgroup (of G) generated by the subset A . It is clearly the smallest subgroup of G containing A , in the sense that any other subgroup of G containing A also contains the subgroup generated by A . It is clear that the subgroup of G generated by A consists precisely of the elements of G which can be written as a product of elements of A and their inverses."

STOP ... Is that really clear?

Let I be the intersection of all subgroups of G containing $A \subset G$.

For $a, b, c, d \in A$, it is indeed clear that any expression such as

$$a b^{-1} c^{-1} a a d$$

must be in I because this element must be in any subgroup containing a, b, c and d . Why, however, is the set of such expressions equal to I ? It is because the set of such expressions is itself a group containing a, b, c and d and so

$$\text{Expressions} \subset I$$

and

$$I \subset \text{Expressions}$$

$$\Rightarrow I = \text{Expressions}, \text{ so Gerach is correct.}$$

What if we change this as follows:

Let I be the intersection of all normal subgroups containing $A \subset G$.

We no longer have $I = \text{expressions}(A)$, but this is often done anyway. For example, you may read something like

"Consider the group generated by x, y with $x^{10} = 1, y^2 = 1, xyxy = 1$."

That actually means the free group on $\{x, y\}$ quotiented by the normal subgroup generated by $\{x^{10} - 1, y^2 - 1, xyxy - 1\}$.

Incidentally, this is the dihedral group D_{10} which we will see later.

... Also, did you notice that I implicitly assumed that the intersection of normal subgroups is normal?

We also defined the equivalence relation generated by a relation $R \subseteq X \times X$ by

$E_g(R)$ = the intersection of all equivalence relations containing R .

To make this less abstract, let $X = \{1, 2, 3, \dots, n\}$ and let's compute $E_g(R)$ on a computer,

- Algorithm will establish

$$i E_g(R) j \Leftrightarrow e_g(i) = e_g(j)$$

- "Loop invariant"

$$i E_g(R) j \Leftrightarrow e_g(i) = e_g(j)$$

is easily established by for i in $\{1, 2, \dots, n\}$: $e_g(i) = i$

A1:

for i in $1, \dots, n$: $e_g(i) = i$

while $e_g(i) \neq e_g(j)$ for some $(i, j) \in R$:

$$e_g(i) = e_g(j)$$

If this terminates, we have $i E_g(R) j \Leftrightarrow e_g(i) = e_g(j)$.

It might not terminate as is, but this is easily fixed...

A2:

for i in $1, \dots, n$: $\text{eq}(i) := i$

while $\text{eq}(i) \neq \text{eq}(j)$ for some $(i, j) \in R$:

if $\text{eq}(i) < \text{eq}(j)$: $\text{eq}(i) := \text{eq}(j)$

if $\text{eq}(i) > \text{eq}(j)$: $\text{eq}(j) := \text{eq}(i)$

fi

This is now guaranteed to terminate because

$\sum_{i=1}^m \text{eq}(i)$ is strictly decreasing and bounded

from below.

With a bit more work, this can be
made quite efficient [$O(n \log n)$].