Chapter 7.3 part 1

Section 7.3 Subgroups

Dfn A subset $H \subseteq G$ (G is a group) is called a subgroup if H is a group (with the same operation)

Ex $G \subseteq G$, $\{e\} \subseteq G$ - trivial all other subgroups are called proper

Ex $\mathbb{R}^{**} \subset \mathbb{R}^*$ (multiplication of reals)

$\mathbb{R} \subset \mathbb{C}$ (addition)

$\{1, -1\} \subset \mathbb{R}^*$ (multiplication) $\{1, -1\} = \langle -1 \rangle$

Th 7.11 (analogue of Th 3.6 for subrings) - criterion for a subset to be a subgroup

A subset H of a group G is a subgroup if and only if the 2 conditions are satisfied

(i) if $a, b \in H$ then $ab \in H$ (the subset is closed under the operation)

(ii) if $a \in H$ then $a^{-1} \in H$

A family of "minimalistic" examples of subgroups

Let G be a group, and let $a \in G$

If H is a subgroup of G such that $a \in H$, then by Th7.11(i) $a^n \in H$ n - any positive integer

by Th7.11(ii) $a^{-1} \in H$, and, by Th7.11(i), $a^{-n} \in H$

Also $a^0 = e \in H$

Th7.14 For a group G and any element $a \in G$

$\langle a \rangle = \{ a^n \mid n \in \mathbb{Z} \}$ is a subgroup of G

Pf - immediate from Th7.11

Terminology: $\langle a \rangle \subseteq G$ - <u>cyclic subgroup</u>

If there is $a \in G$ such that $\langle a \rangle = G$ then

G is referred to as a <u>cyclic group</u>

<u>Remark</u> $\langle a \rangle \subseteq G$, the subgroup may be finite or infinite.

$\langle 2 \rangle \subset \mathbb{Z}$ cyclic subgroup

$\langle 1 \rangle = \mathbb{Z}$ cyclic group

For $a \in G$, the order of a denoted by $|a|$

is the smallest integer k such that $a^k = e \in G$

Th 7.15 $|\langle a\rangle| = |a|$ for any $a \in G$ (G is a group)

The order of the cyclic subgroup $\langle a\rangle \subseteq G$ is equal to the order of the element $a \in G$

Remark It may happen that $\langle a\rangle = \langle b\rangle$ while $a \neq b$

Ex $\mathbb{Z}_7^*$ - group of order 6

$\langle 2\rangle = \{2, 4, 1\}$

$\langle 4\rangle = \{4, 2, 1\}$

$\langle 2\rangle = \langle 4\rangle$ - same cyclic subgroup (of order 3)

$2 \equiv 2 \pmod 7$
$2^2 \equiv 4 \pmod 7$
$2^3 \equiv 1 \pmod 7$
$2^4 \equiv 2 \pmod 7$
$2^5 \equiv 4 \pmod 7$
...

$4 \equiv 4 \pmod 7$
$4^2 \equiv 2 \pmod 7$
$4^3 \equiv 1 \pmod 7$

$\langle 3\rangle = \{3, 2, 6, 4, 5, 1\} = \mathbb{Z}_7^*$ - is a cyclic group

A generalization of cyclic subgroups as minimal subgroups containing an element

Let S be a subset of a group G

Th 7.18 Let $\langle S\rangle$ be the set of all possible products (in every order) of elements of S and their inverses.

Then:

(1) $\langle S \rangle$ is a subgroup of G

(2) If H is a subgroup of G such that $H \supset S$

then $H \supset \langle S \rangle$

Terminology: $\langle S \rangle$ is the subgroup generated by the subset S

Remark $S = \{a, b\}$

$\langle S \rangle$ - the set of all "words"

a word: $a b a^{-7} b^{3} a^{6} b^{-5} \ldots$ of finite length