Notes

September 24, 2014

assignment

assignment 3.1 no 23, 3.2no 3,6,7

if $(G,\cdot), a \in G$ then the cyclic subgroup generated by a is $< a >= \{\dots, a^{-2}, a^{-1}, e, a, a^2, a^3, \dots\} \subseteq G$.

$< a >$ is a subgroup of G and if H is a subgroup of G and $a \in H$ then $< a > \subseteq H$, hence $< a >$ is the smallest subgroup of G

example: $(\mathbb{Z}, +) \rightarrow < n >= n\mathbb{Z}$

$< 1 >=< -1 >= \mathbb{Z}$

we say that the group G is cyclic if there exists $a \in G$ such that $< a >= G$. So $(\mathbb{Z}, +)$ is cyclic because $< 1 >= \mathbb{Z}$

another example $(\mathbb{Z}_n, +)$, $< [1] >= \mathbb{Z}_n$.

definition

if there exists $n > 0, n \in \mathbb{Z}$ such that $a^n = e$ we say that a has finite order and $\mathrm{ord}(a) = \min\{n|n > 0, n \in \mathbb{Z}, a^n = e\}$. otherwise it has infinite order

proposition

if G is a finite group, $a \in G$ then a has finite order. $\{e, a, a^2, a^3, \dots\} \in G$. Since G is finite, we have some m,n where $a^m = a^n$ wlog $m > n$, $a^m a^- n = a^n a^- n = e = a^{m-n}$

examples

$(\mathbb{Q}^*, \cdot)$, $\mathrm{ord}(-1) = 2, \mathrm{ord}(1) = 1, \mathrm{ord}(2) = \infty$

proof for proposition3.2.8ii

use division algorithm, $k = ord(a) \cdot q + r$ with $0 \leq r < ord(a)$

then $e = a^k = a^{ord(a)q+r=[a^{ord(a)}]^q} a^r = a^r$

excercise, complete this proof