Groups and Rings - SF2729

Homework 2

Jim Holmström - 890503-7571

February 22, 2012

Exercise 1. Let G be a finite group and let $H \subset G$ be a subset. Assume that for $\forall a, b \in H \Rightarrow ab \in H$.
Prove that H is a subgroup.

Solution.

$\mathcal{G}_1$	Associativity
$\mathcal{G}_2$	Existence of unit
$\mathcal{G}_3$	Existence of inverses

Table 1: Group axioms

Associativity is trivially inherited from G and therefore H satisfies $\mathcal{G}_1$.
Let $n = |H|$ and $a \in H$ then $a, a^2, \dots, a^{n+1} \in H$ since we know that H is closed under the operation. All these cannot be the same which means we have $\exists i < j : a^i = a^j$.

$$\begin{aligned} a^i &= a^j \in H \\ a^i a^{-i} &= a^j a^{-i} \in H \\ e &= a^{j-i} \in H \end{aligned}$$

Thus $e \in H$ showing that H satisfies $\mathcal{G}_2$.
$a^{-1} = ea^{-1} = a^{j-i}a^{-1} = a^{j-i-1}$ which is $\in H$ and thus $a^{-1} \in H$ which gives that H satisfies $\mathcal{G}_3$.

$\therefore H \subset G$ and H satisfying $\mathcal{G}_{1:3} \Rightarrow H < G$ $\square$

Exercise 2. Show that a group with no proper non-trivial subgroup is cyclic. Furthermore find the order of such a group.

Solution. G is a group with no proper non-trivial subgroup. In the case $G = \{e\}$ it's trivially cyclic. For the other cases we can take $a \in G, a \neq e$, we know that $< a >$ is a nontrivial subgroup of G and since G doesn't have any non-trivial proper subgroups we have $< a >= G$ and are thus cyclic. A cyclic group is isomorphic Z_n or Z, where for finite G, $n = |G|$. Since a is arbitrary the above statement most hold $\forall a \neq e \in G$. If $\gcd(a, n) \neq 1$ then $< a >\neq G$ and since this cannot be we have that $\forall a \in \{2, ..., n-1\}$ $\gcd(a, n) = 1$. Therefore n most be prime since that's the only number that has this property. $\square$

Exercise 3. Let G be a group and supposed $a \in G$ generates a cyclic group of order 2 and is the unique such element.
Show that $ax = xa \forall x \in G$. (Hint: consider $(xax^{-1})^2$).

Solution.

$$\begin{aligned} a &\neq e && \text{(Since } a \text{ is of order 2)} \\ xa &\neq x \\ xax^{-1} &\neq e \end{aligned}$$

$\forall x, (xax^{-1})^2 = xaeax^{-1} = xa^2x^{-1} = \{\text{a of order } 2 \Rightarrow a^2 = e\ \} = xex^{-1} = e$
Thus xax^{-1} is of order 2 and since a is given to be the unique element of order 2 in G we have $\forall x, xax^{-1} = a$ resulting in $\forall x, xa = ax$ $\square$

Exercise 4. Let p and q be distinct prime numbers. Find the number of generators of the cyclic group $\mathbb{Z}_{pq}$
(Assuming that we have 2 typos and are therefore following the text in the book.)

Solution. Assuming $\mathbb{Z}_{pq} =< \mathbb{Z}_{pq}, + >$
Generators $= \{a \in \mathbb{Z}^+ : a < pq \wedge sgd(a, pq) = 1\}$ This fits the definition of eulers totient function ϕ.
$|\text{Generators}| = \phi(pq) = (p-1)(q-1)$ $\square$