2 - Group Theory

3 - Some Preliminary Lemmas

Exercise 4 (*page 35*)

Let $P(i)$ be the proposition $(ab)^i = a^i b^i$, for all a, b in G, where i is some integer. The problem can then be restated as $P(i) \wedge P(i+1) \wedge P(i+2) \Rightarrow G$is abelian.

To prove this, we begin by noting (see below for proof) that

$$P(i) \wedge P(i+1) \Rightarrow (ab)^i = (ba)^i \tag{1}$$

and similarly

$$P(i+1) \wedge P(i+2) \Rightarrow (ab)^{i+1} = (ba)^{i+1} \tag{2}$$

Now, $(ab)^i = (ba)^i \Rightarrow (ab)^{-i} = (ba)^{-i}$, applying to $(ab)^{i+1} = (ba)^{i+1}$ yields $ab = ba$. $\blacksquare$

Proof of (1)**:**

$$(ab)^i = a^i b^i$$

$$(ab)^{i+1} = a^{i+1} b^{i+1}$$

Now $(ab)^{i+1} = a(ba)^i b$, so we get $(ba)^i = a^i b^i = (ab)^i$. $\blacksquare$

Exercise 11 (*page 35*)

Suppose $a^2 \neq e$ for all $a \neq e$, i.e. $a \neq a^{-1}$ for all $a \neq e$. Since every element in G has a unique inverse and no $a \neq e$ has e as an inverse, $P = \{\{a, a^{-1}\} | a \neq e, a \in G\}$ partitions $G - \{e\}$. Now on one hand, since P partitions $G - \{e\}$, $\|G - \{e\}\|$ is even. On the other hand, since $\|G\|$ is even, $\|G - \{e\}\|$ must be odd. We have reached a contradiction!

Exercise 12 (*page 35*)

We need to show $ea = a$ and $y(a)a = e$, for all $a \in G$.

$$e = y(a)y(y(a)) = (y(a)e)y(y(a)) =$$

$$(y(a)(ay(a)))y(y(a)) =$$

$$((y(a)a)y(a))y(y(a)) =$$

$$(y(a)a)(y(a)y(y(a))) =$$
$$(y(a)a)e =$$
$$y(a)a$$

Using this we also easily have $a = ae = a(y(a)a) = (ay(a))a = ea$.

Exercise 14 (*page 36*)

Suppose $a \in G$ is an element s.t. $a^2 \neq a$. Then $\exists n \geq 1$ s.t. $a^{n+1} = a$, since G is finite. We claim that a^n satisfies $a^n b = ba^n = b$, for all $b \in G$. This is true since

$$a^{n+1} = a$$
$$a^{n+1}b = ab$$
$$a^n b = b$$

Where the last equality follows from left-cancellation.

Now $ba^n = b$ follows similarly. Therefore a^n is the identity element.

It is easy to see that a^{n-1} is both the left and right inverse of a.

5 - A Counting Principle

Exercise 2 (*page 46*)

We will show that if there is $a \in G$ of finite order, then $\cap H = \{e\}$, where H ranges over the subgroups of G such that $H \neq \{e\}$ (i.e. H is non-trivial).

Clearly $\langle a \rangle \supset \cap H$. We now show that $\cap_{H \subset \langle a \rangle} H = \{e\}$. Pick any $H \subset \langle a \rangle$. There exists a smallest $n > 0$ s.t. $a^n \in H$. Suppose $n \nmid m$ for some m. Then $x = xn + y$ for some $0 < y < n$. Thus $a^m = a^{xn+y} \Rightarrow a^{m-xn} = a^y \in G$ which contradicts minimality of n.

We can now easily state that $a^k \in G$ iff $n | k$. Thus $a^k \in \cap_{H \subset \langle a \rangle} H$ iff $p | k$ for all $p \in \mathbb{Z}$. This implies that $k = 0$, so $\cap_{H \subset \langle a \rangle} H = \{e\}$.

 ISBN10: 0-471-01090-1