Corrections of exercises 6-9

Exercise 6

a) As $U$ and $V$ are subgroups, they both contain the neutral element $e$ of $G$, so $e \in U \cap V$. We have to show that if $x$ and $y$ belong to $U \cap V$, then so does $xy^{-1}$. Since $U$ is a subgroup of $G$:

$$x \in U \cap V \text{ and } y \in U \cap V \Rightarrow x \in U \text{ and } y \in U \Rightarrow xy^{-1} \in U$$

and similarly, since $V$ is also a subgroup of $G$:

$$x \in U \cap V \text{ and } y \in U \cap V \Rightarrow x \in V \text{ and } y \in V \Rightarrow xy^{-1} \in V$$

Thus

$$x \in U \cap V \text{ and } y \in U \cap V \Rightarrow xy^{-1} \in U \cap V$$

b) Let $a$ be an element of $U \cap V$. Then $a \in U$ so the order of $a$ divides the order of $U$. Similarly, the order of $a$ has to divide the order of $V$. So the order of $a$ has to be a common divisor of $\#U$ and $\#V$, but the only common divisor of those two numbers is supposed to be 1, which implies that the order of $a$ is exactly 1 i.e. $a = e$. Thus

$$\gcd(\#U, \#V) = 1 \Rightarrow U \cap V = \{e\}$$

Exercise 7

a) Let $a_1$ be a generator of $G_1$ and $a_2$ be a generator of $G_2$. We claim that $(a_1, a_2)$ is a generator of $G_1 \times G_2$. As $G_1 \times G_2$ as order $n_1n_2$, it suffices to show that $(a_1, a_2)$ as order $n_1n_2$. Suppose that $(a_1, a_2)^k = (e, e)$ for some positive integer $k$. Then $(a_1^k, a_2^k) = (e, e)$ thus $a_1^k = e$ and $a_2^k = e$. But $a_1$ has order $n_1$ so $n_1$ divides $k$, and $a_2$ has order $n_2$ so $n_2$ divides $k$. Since $\gcd(n_1, n_2) = 1$, this implies that $n_1n_2$ divides $k$. Thus, the order of $(a_1, a_2) = n_1n_2$.

b) $C_2 \times C_2$ has order $2 \times 2 = 4$. If it was cyclic, it would contain an element of order 4. But for any $a$ and $b$ in $C_2$,

$$(a, b)^2 = (a^2, b^2) = (e, e)$$

because $C_2$ has order 2. Thus, any element of $C_2 \times C_2$ has order at most 2, so there is no element of order 4 in it, which implies that it cannot be cyclic.

Exercise 8 Let $a$ be a generator of $G$. If $H = \{e\}$, then $H$ is clearly cyclic. If $H \neq \{e\}$, then we can consider the smallest non-zero integer $k$ such that $a^k$ belongs to $H$. We claim that $H = \langle a^k \rangle$. Indeed, any element $b$ of $H - \{e\}$ can be written has $b = a^i$ or $a^{-i}$ for some positive integer $i$. Consider the euclidean division of $i$ by $k$:

$$i = kq + r \quad 0 \leq r < k$$

Then

$$a^r = a^{i-kq} = a^i((a^k)^{-1})^q = b^{q+1}((a^k)^{-1})^q$$

Since $b$ and $a^k$ belong to $H$, so does $a^r = b^{q+1}((a^k)^{-1})^q$. Thus $a^r \in H$ and $r < k$ so $r$ has to be zero otherwise it would be contradictory with the minimality assumption on $k$. This implies that $b = a^{q+1} = (a^k)^q$ for some $q \in \mathbb{Z}$, which implies that $H = \langle a^k \rangle$. The inverse inclusion is obvious, so $\langle a^k \rangle = H$ which proves that $H$ is cyclic, generated by $a^k$.

Exercise 9

a) Notice that $10^i = 1 \mod 3$. As $a = \sum_{i=0}^n a_i10^i$ we have

$$a = \sum_{i=0}^n a_i \mod 3$$

Thus

$$3|a \iff a = 0 \mod 3 \iff \sum_{i=0}^n a_i = 0 \mod 3 \iff 3|\sum_{i=0}^n a_i$$

b) $10^i = 1 \mod 9$ and $10^i = (-1)^i \mod 11$. 

1